FEMP

FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

_ens

Esquema Nacional de Seguridad

TOMO 2

GUÍA PARA ENTIDADES LOCALES DE MENOS DE 2.000 HABITANTES

ESQUEMA NACIONAL DE SEGURIDAD (ENS)

Cuaderno de Recomendaciones

Presentación

Ramón Fernández Pacheco Monterreal

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

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.

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

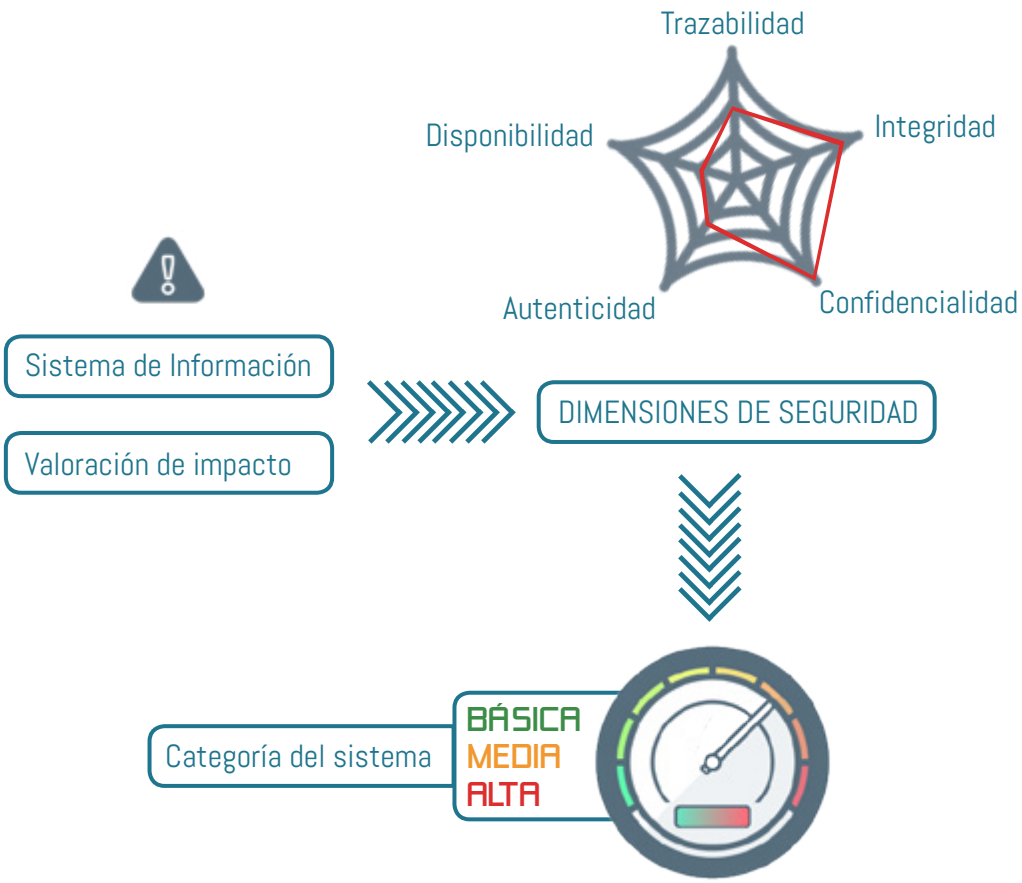
1 | El Sistema de Información Local

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

3 Ámbito de aplicación

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.

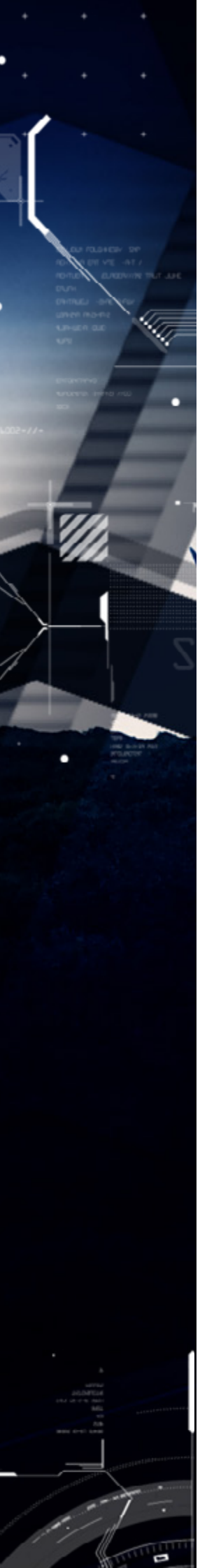
Conociendo la complejidad del nombramiento de todas estas figuras, principalmente porque estos ayuntamientos disponen, en la mayoría de los casos, de un único trabajador que realiza tareas administrativas, las figuras anteriormente nombradas confluirán en el nombramiento de un ***Responsable de Seguridad 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]

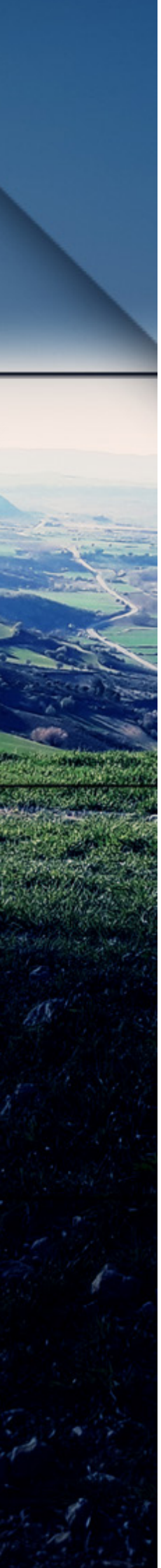
1. Objetivo
2. Ámbito de aplicación
3. Vigencia
4. Revisión y evaluación
5. Referencias
6. Normas previas
7. La confidencialidad de la información
8. Ámbito de la confidencialidad
    - 8.1 Deber de confidencialidad
    - 8.2 Difusión de la información
    - 8.3 Información comprendida en el deber de 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