Administración Electrónica

Esquema Nacional de Seguridad

RD 3/2010

tiThink

Esquema Nacional de Seguridad
RD 3/2010

Editado por tiThink
José María Rodríguez e Ignacio Peralta

En colaboración con Symantec.

Esta publicación incluye información obtenida de los documentos y guías técnicas publicadas por el Centro de Criptografía Nacional CCN, relativas a la adecuación de las Administraciones Públicas al Real Decreto RD 3/2010 que regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Esta publicación tiene el propósito general de divulgar dicho Real Decreto y sus implicaciones prácticas a la hora de abordar su implementación. Antes de tomar cualquier decisión práctica en el momento de implementar cualquier iniciativa de las descritas en este documento se debe consultar los documentos y guías oficiales del CCN y/o asesores profesionales especializados en el Esquema Nacional de Seguridad.

Presentación

La Ley 11/2007 de "Acceso Electrónico de los Ciudadanos" reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos. La ley regula los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa, en las relaciones entre las Administraciones Públicas, así como en las relaciones de los ciudadanos con las mismas.

La Administración General del Estado garantiza así el acceso de todos los ciudadanos a los servicios electrónicos bajo su responsabilidad a través de un sistema de varios canales que cuente, al menos, con los siguientes medios:

- oficinas de atención presencial,
- puntos de acceso electrónico, y
- servicios de atención telefónica.

Entre los fines de la ley se incluye el de crear las condiciones de confianza y seguridad en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de los derechos fundamentales. En especial, los relacionados con la intimidad y la protección de datos de carácter personal, garantizando la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.

En este contexto aparece el Real Decreto 3/2010, de 8 de Enero, por el que se regula el ESQUEMA NACIONAL DE SEGURIDAD en el ámbito de la ADMINISTRACIÓN ELECTRÓNICA. Tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, y en él se definen los principios básicos y requisitos mínimos que permiten una protección adecuada de la información.

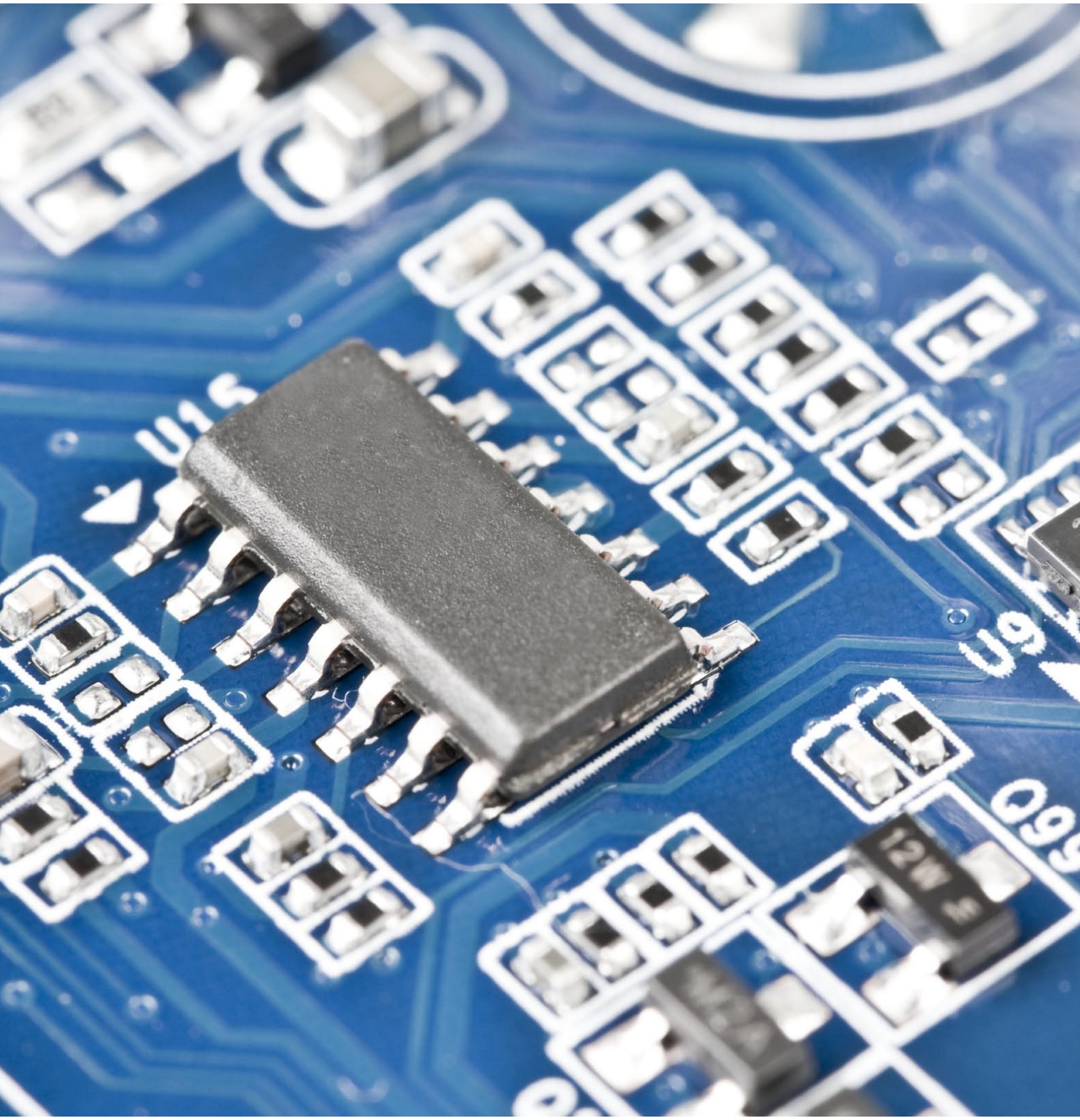
La aparición de este RD, y la documentación técnica proporcionada por el Centro Criptológico Nacional, supusieron el pistoletazo de salida para el proceso de adecuación a las recomendaciones y medidas que se definen en esta regulación, avanzando en los procesos de gestión de seguridad al mismo ritmo que las Administraciones Públicas lo están haciendo en proporcionar servicios electrónicos avanzados.

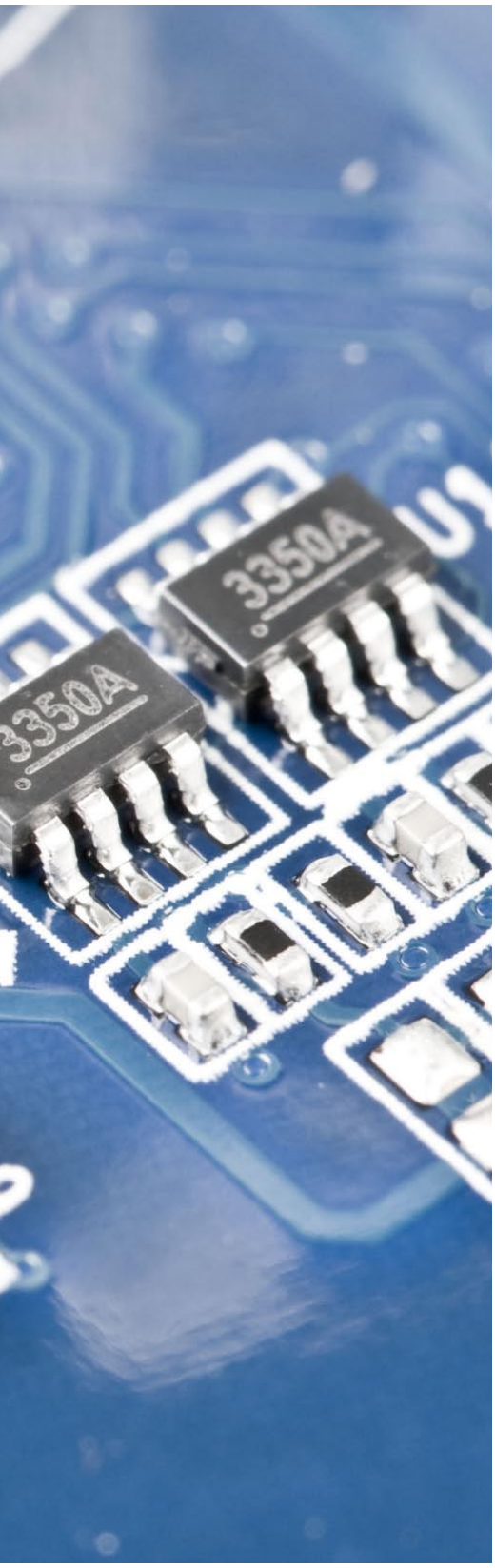
El Real Decreto establece enero del 2014 como el plazo máximo para la adecuación de todas las Administraciones Electrónicas al Esquema Nacional de Seguridad, y es una línea de trabajo que está en la agenda de todos los responsables técnicos en la Administración.

En esta línea presentamos este documento, en el que resaltamos los aspectos fundamentales del Real Decreto, el cual confiamos que sea de utilidad para todos los que nos vemos involucrados en hacer frente a los retos planteados en este proceso de cambio.

Contenido

Figuras y Tablas


U15
Q9



Introducción al Esquema Nacional de Seguridad

Los ciudadanos confían que los servicios disponibles por medios electrónicos se presten en unas condiciones de seguridad equivalentes a las que se encuentran cuando se acercan personalmente a las oficinas de la Administración. Además, buena parte de la información contenida en los sistemas de información de las AA.PP. y los servicios que prestan constituyen activos nacionales estratégicos. La información y los servicios prestados están sometidos a amenazas y riesgos provenientes de acciones malintencionadas o ilícitas, errores o fallos y accidentes o desastres.

La Ley 11/2007, de "Acceso electrónico de los ciudadanos a los Servicios Públicos", establece los principios relativos a la seguridad de las administraciones electrónicas, y en su artículo 42 crea el Esquema Nacional de Seguridad.

El Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010 determina la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos.

El ENS está constituido por los principios básicos y requisitos mínimos para una protección adecuada de la información. Será aplicado por las AA.PP. 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.

El Esquema Nacional de Seguridad 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 Administraciones Públicas, 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 en el ámbito de la Ley 11/2007, que estará constituida por los **principios básicos y** los **requisitos mínimos** para una protección adecuada de la información.
- Introducir los elementos comunes que han de **guiar** la actuación de las Administraciones Públicas en materia de seguridad de las tecnologías de la información.
- Aportar un **lenguaje común** para facilitar la interacción de las Administraciones Públicas y la comunicación de los requisitos de seguridad de la información a la Industria.
- Aportar un tratamiento homogéneo de la seguridad que facilite la **cooperación** en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- Facilitar un **tratamiento continuado** de la seguridad.

Se limita a establecer los principios básicos y requisitos mínimos, 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 protocolo de la capacidad de respuesta ante incidentes de seguridad en el Centro Criptológico Nacional y se hace una referencia expresa a la formación.

Adecuación al Esquema nacional de Seguridad

En la disposición transitoria del Real Decreto 3/2010 se establece un mecanismo escalonado para la adecuación a lo indicado en el Esquema Nacional de Seguridad, de manera que los sistemas de las administraciones deberán estar adecuados a este Esquema en unos plazos no superiores a 48 meses desde la entrada en vigor del mismo. El plazo de adecuación **vence el 30 de enero de 2014**.

La adecuación ordenada al Esquema Nacional de Seguridad requiere el tratamiento de las siguientes cuestiones:

- Preparar y aprobar la **Política de Seguridad**, incluyendo la definición de roles y la asignación de responsabilidades.
- **Categorizar** los sistemas atendiendo a la valoración de la información manejada y de los servicios prestados.
- Realizar el **análisis de riesgos**, incluyendo la valoración de las medidas de seguridad existentes.
- Preparar y aprobar la **Declaración de Aplicabilidad** de las medidas del Anexo II del ENS. (Medidas de Seguridad).
- **Implantar**, operar y monitorizar las medidas de seguridad a través de la gestión continuada de la seguridad.
- **Auditar** la seguridad de los sistemas.
- **Informar** sobre el estado de la seguridad.

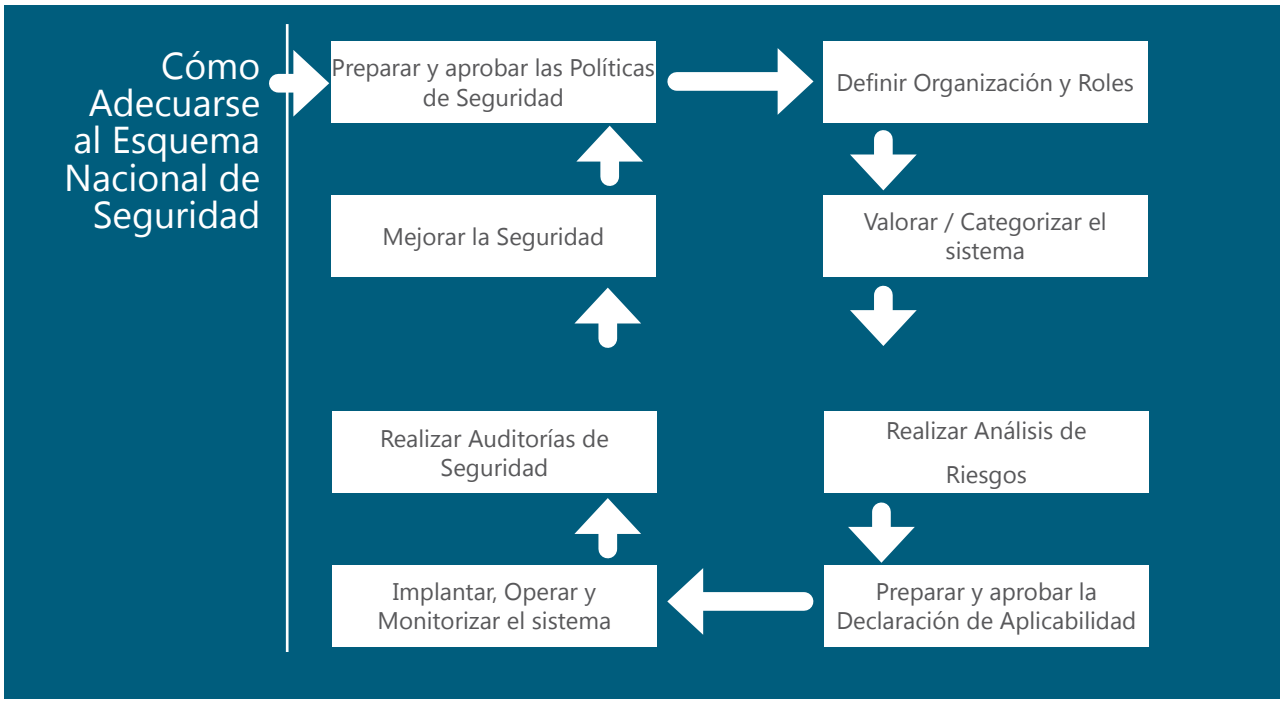


Fig. 1. Proceso de adecuación al ENS

Los sistemas existentes a la entrada en vigor del Real Decreto se adaptarán al Esquema Nacional de Seguridad para el cumplimiento de lo establecido en la regulación. Para los nuevos sistemas, se aplicará lo establecido en el presente Real Decreto desde su concepción.

Si a los doce meses de la entrada en vigor del Esquema Nacional de Seguridad hubiera circunstancias que impidan la plena aplicación de lo exigido en el mismo, es obligatorio disponer de un **plan de adecuación** que marque los plazos de ejecución y que en ningún caso, serán superiores a 48 meses desde la entrada en vigor del ENS.

El plan indicado en el párrafo anterior debe ser elaborado por el Responsable de Seguridad y aprobado por los órganos superiores competentes.

Este plan de adecuación incluirá la siguiente información:

Política de Seguridad

Si el organismo dispone de una **Política de Seguridad** se identificará y anexará al plan de adecuación. Si se dispone de una Política de Seguridad, pero no satisface los requisitos, o no se dispone de ella, se hará constar cómo se planea adaptar o desarrollar la política.

La Información y su valoración

Se deberá detallar la **información** que se maneja y los **servicios** que se prestan, junto con la **valoración** por su responsable. Si se carece de una Política de Seguridad, o no está nombrado el responsable de alguna de las informaciones o servicios, o no está aprobada formalmente la valoración, será realizada por el Responsable de Seguridad a su mejor criterio, dejando constancia de los motivos de dicha valoración. Se deberá indicar un plazo límite para disponer de la valoración formal de los servicios que se prestan, con su valoración, bajo el mismo tratamiento que la información valorada.

Si el sistema maneja datos de carácter personal, el plan de adecuación incluirá una relación detallada de dichos datos. Bastará una referencia al Documento de Seguridad requerido por el RD 1720 de 2007 referente a LOPD.

Categoría del sistema

El Responsable de Seguridad establecerá la **categoría del sistema.** Si lo considera oportuno, puede fragmentar el sistema en varios subsistemas a fin de acotar las exigencias de medidas de protección y, en última instancia, reducir los recursos necesarios.

Análisis de riesgos

El plan de adecuación incorporará un **análisis de riesgos**, según los requisitos para la categoría establecida para el sistema. En el análisis de riesgos se valorarán las salvaguardas y los **riesgos residuales** presentes en la fecha de aprobación del plan de adecuación.

Declaración de Aplicabilidad

Se elaborará una relación de las **medidas que son de aplicación** al sistema. Cuando una medida requerida no se considere aplicable, esta no-aplicabilidad debe estar justificada. Cuando se recurra a medidas alternativas, se indicará el motivo, así como las medidas que sustituye.

Insuficiencias del sistema

Pueden detectarse insuficiencias en el sistema por el **incumplimiento** formal de las medidas de seguridad o por la existencia de **riesgos no asumibles** por el organismo. Formalmente, los riesgos residuales deben ser aceptados por los Responsables de la Información y Servicios afectados, y en su defecto por el Responsable de Seguridad.

Plan de mejora de la seguridad

Se indicarán las **actuaciones destinadas a subsanar las insuficiencias** detectadas. Cada actuación prevista incluirá las insuficiencias que resuelve, el plazo previsto de ejecución, indicando fecha de inicio y fecha de terminación, y una estimación del coste que supondrá.

Las Políticas de Seguridad

La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa 'seguridad de la información' en una organización. El documento debe estar accesible para todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible. Conviene que sea breve, dejando los detalles técnicos para otros documentos normativos. La Política de Seguridad deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización.

La Política de Seguridad será aprobada por el órgano superior competente que corresponda, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

- Los objetivos o misión de la organización.
- El marco legal y regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación.
- La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización.
- Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Secciones típicas de una Política de Seguridad de la Información:

1. **Misión u objetivos del organismo**. Se describirá la razón de la existencia del organismo y los servicios que presta.

2. **Marco normativo**. Se plasmará por escrito las responsabilidades que el organismo pueda tener por su naturaleza legal, por su obligación de atender normativa nacional o sectorial y por obligaciones contraídas con terceros, con indicación de las normas correspondientes.

3. **Organización de seguridad**. Se debe describir cómo se coordina el organismo para atender a las necesidades de seguridad, tanto TIC como en otras materias y cómo se distribuye la información y se toman las decisiones corporativas. Se deben describir los roles unipersonales en materia de seguridad de la información, en particular la figura del Responsable de Seguridad, detallando sus funciones y responsabilidades:

    - Definición de comités y roles unipersonales.
    - Funciones.
    - Responsabilidades.
    - Mecanismos de coordinación.
    - Procedimientos de designación de personas.

4. **Concienciación y formación**. El objetivo es lograr la plena conciencia respecto a que la seguridad de la información afecta a todos los miembros del organismo y a todas las actividades, de acuerdo al principio de Seguridad Integral. Así como la articulación de los medios necesarios para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

5. Postura ante la **gestión de riesgos**. El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar, además de los mínimos establecidos por el Esquema Nacional de Seguridad. En esta sección se debe plasmar el compromiso y la obligación de los responsables de los sistemas de realizar análisis de riesgos y atender a sus conclusiones. El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente.

6. **Proceso de revisión** de la Política de Seguridad. La Política de Seguridad de la Información es un documento que será aprobado formalmente por la Alta Dirección de la Organización y tendrá carácter imperativo sobre toda la organización. Estará sujeto a un proceso de revisión regular que lo adapte a nuevas circunstancias, técnicas u organizativas, y evite que quede obsoleto.

    Se establecerá un proceso organizativo que asegure que regularmente se revisa la completitud y precisión de lo que la Política establezca y sea sometido a aprobación formal por la Alta Dirección. El proceso de elaboración y aprobación debe explicitarse en la misma Política.

El texto será claro en los objetivos que se persiguen y evitar referencias a soluciones tecnológicas concretas, de tal forma que la evolución tecnológica no requiera la revisión de la Política.
Debe garantizar que se mantiene la posición de la organización en materia de seguridad independientemente de los recursos que se empleen en cada momento.

Aunque el texto deba revisarse regularmente, estas revisiones tendrán por lo general un carácter marcadamente continuista, limitándose a mejorar expresiones ambiguas, mejorar la claridad y atajar situaciones no previstas que han ocurrido en la utilización del sistema. No se puede cambiar de Política alegremente; pero si **se debe ir adaptando continuamente a la realidad**.

Fig. 2. Políticas de Seguridad

Organización: roles y funciones

En la estructura organizativa establecida se identificará al Responsable de la Información, al Responsable del Servicio y al Responsable de la Seguridad (CISO - *Chief Information Security Officer*).

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 garantizar la seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará claramente diferenciada de la responsabilidad sobre la prestación de los servicios, normalmente identificada sobre el Responsable del Sistema.

Nivel Organizativo	Opción A	Opción B
Órganos de Gobierno	Comité de Seguridad Corporativa / Responsable Seguridad Corporativa (CSO)	
	Comité de Seguridad de la Información	Responsable de la Información
		Responsable del Servicio
Ejecutivo	Responsable de la Seguridad (CISO)	
Operaciones	Responsable del Sistema	

Fig. 3. Roles Seguridad

Opcionalmente, algunas organizaciones tendrán un Administrador de la Seguridad del Sistema (ASS) encargado de operar las herramientas y procedimientos de seguridad. Podrá depender del Responsable de Seguridad o del Responsable del Sistema, pero siempre estará vinculado a las dos funciones.

Las funciones se describen en la siguiente matriz RACI:

Nivel Organizativo	CSO	RInf	RServ	CISO	RSis	ASeg
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		A	A	R	I	
Documentación de seguridad				A/R	C	I
Política de seguridad	A			R	C	
Normativa de seguridad				A/R	C	I
Procedimientos de seguridad				C	A/R	I
Implantación de las medidas de seguridad		I	I	C	A/R	R
Supervisión de las medidas de seguridad				A o C	C o A	R
Estado de seguridad del sistema	I	I	I	A	I	R
Planes de mejora de la seguridad				A/R	C	
Planes de concienciación y formación				A/R	C	
Planes de continuidad				C	A/R	
Suspensión temporal del servicio	A	C	C	C	R	
Seguridad en el ciclo de vida				C	A/R	

Fig. 4. Responsabilidades Seguridad

(Responsable / Aprueba / Consultado / Informado)

Elementos principales de Esquema Nacional de Seguridad

Los elementos principales del ENS son los siguientes:

- 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** proporcionales a la naturaleza de la información y los servicios a proteger.
- Las comunicaciones electrónicas, los sistemas e infraestructuras.
- La **auditoría** de la seguridad.
- La **respuesta ante incidentes** de seguridad.
- La **certificación** de la seguridad.
- La **conformidad**.

El aspecto principal del ENS es que todos los órganos superiores de las AA.PP. deberán disponer de su Política de Seguridad, que se establecerá en base a los principios básicos y que se desarrollará aplicando los requisitos mínimos.

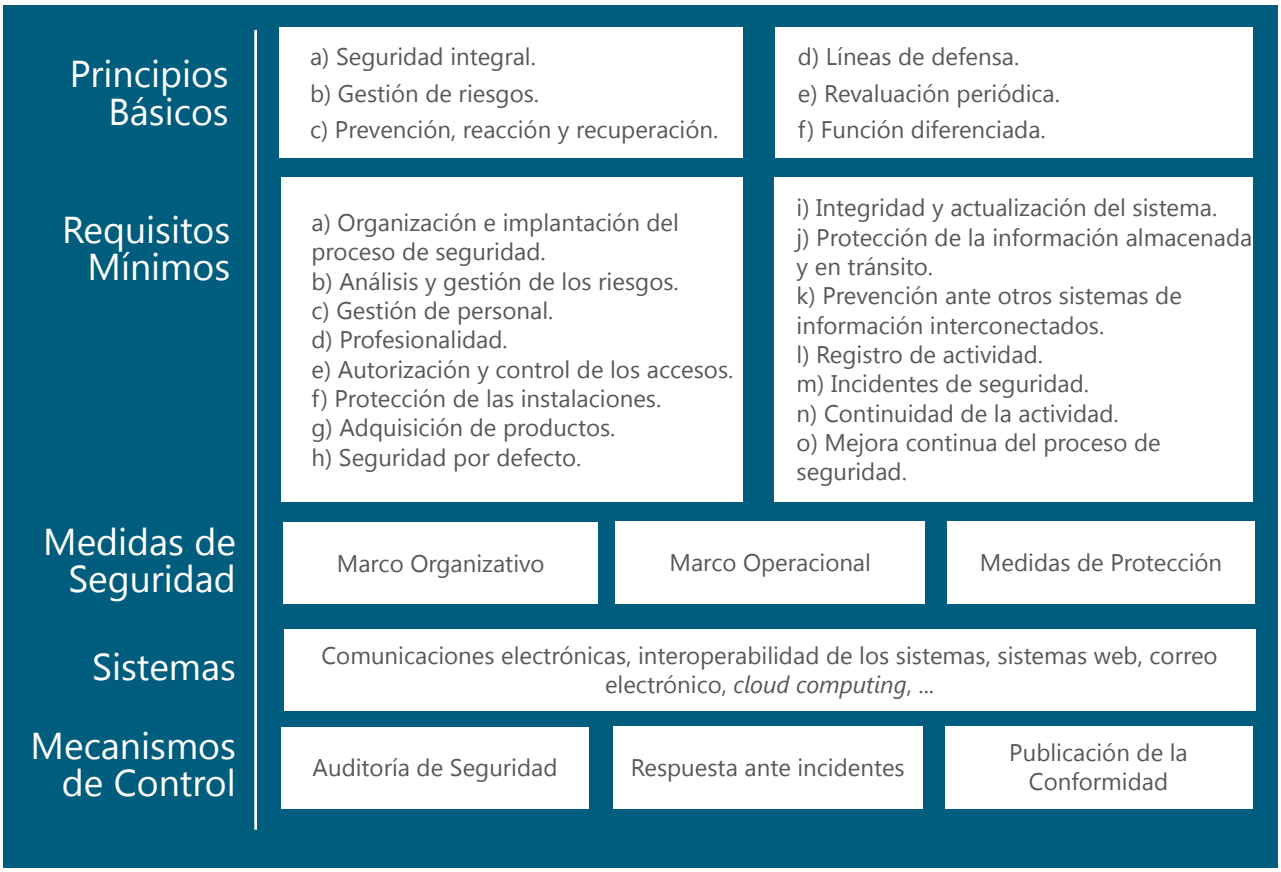


Fig. 5. Elementos principales del ENS

Principios Básicos

Cualquier decisión en materia de seguridad deberá alinearse con los siguientes principios básicos:

Seguridad Integral

La seguridad se entenderá como un **proceso integral** constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. Se prestará la máxima atención a la **concienciación** de las personas. Se concibe la seguridad 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.

Gestión de riesgos

El análisis y **gestión de riesgos** será parte esencial del proceso de seguridad y deberá mantenerse **permanentemente actualizado**. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables.

Prevención, reacción y recuperación

Las **medidas de prevención** deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Estas medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Las **medidas de detección** estarán acompañadas de **medidas de reacción**, de forma que los incidentes de seguridad se atajen a tiempo.

Las **medidas de recuperación** permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

Líneas de defensa

El sistema ha de disponer de una estrategia de protección constituida por **múltiples capas de seguridad**. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Revaluación periódica

Las medidas de seguridad se revaluarán y actualizarán periódicamente, para **adecuar** su **eficacia** a la constante evolución de los riesgos y sistemas de protección, llegando incluso a un replanteamiento de la seguridad, si fuese necesario.

Función diferenciada

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

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

Requisitos Mínimos

Todos los órganos superiores de las Administraciones Públicas **deberán aplicar los siguientes requisitos mínimos** a la hora de desarrollar su Política de Seguridad:

Organización

La seguridad deberá comprometer a todos los miembros de la organización.

Gestión de los riesgos

Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.

Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

Gestión de personal

Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.

Profesionalidad

La seguridad de los sistemas estará atendida, revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: instalación, mantenimiento, gestión de incidencias y desmantelamiento.

Control de los accesos

El acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

Protección de las instalaciones

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Adquisición de productos

En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que vayan a ser utilizados por las Administraciones Públicas se valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

Seguridad por defecto

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto: el sistema proporcionará la mínima funcionalidad requerida; las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y sólo serán accesibles por las personas; se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés; el uso ordinario del sistema ha de ser sencillo y seguro.

Integridad del sistema

Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Información almacenada y en tránsito

Se prestará especial atención a la información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil.

Otros sistemas interconectados

Se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Registro de actividad

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.

Incidentes de seguridad

Se establecerá un sistema de detección y reacción frente a código dañino. Se registrarán los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan. Estos registros se emplearán para la mejora continua de la seguridad del sistema.

Continuidad de la actividad

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Mejora continua del proceso de seguridad

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 gestión de las tecnologías de la información.

Medidas de Seguridad

Para dar cumplimiento a estos requisitos mínimos las Administraciones Públicas aplicarán las medidas de seguridad indicadas teniendo en cuenta los activos que constituyen el sistema, la categoría del sistema, y las decisiones que se adopten para gestionar los riesgos identificados.

Cuando un sistema al que afecte el ENS maneje datos de carácter personal le será de aplicación lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normativa de desarrollo, sin perjuicio de los requisitos establecidos en el Esquema Nacional de Seguridad.

Los medidas definidas en el ENS **tendrán la condición de mínimos exigibles**, y podrán ser ampliados por la organización. A priori se establecen 75 medidas, que engloban el Marco Organizativo, el Marco Operacional y las Medidas de Protección.

El detalle de estas medidas se podrá ver en un capítulo específico de este documento.

Sistemas de Aplicación

La seguridad de las sedes y registros electrónicos, así como la del acceso electrónico de los ciudadanos a los servicios públicos, se regirán por lo establecido en el Esquema Nacional de Seguridad.

Para el mejor cumplimiento de lo establecido en el ENS el Centro Criptológico Nacional, en el ejercicio de sus competencias, elabora y difunde las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones. Haciendo especial hincapié en los principales tipos de sistemas afectados:

- Seguridad en Sistemas web.
- Seguridad en el Correo Electrónico.
- Seguridad en entornos de *Cloud Computing*.
- Tipificación y aplicación de Herramientas de Seguridad.
- etc.

Sistemas no afectados

En capítulos posteriores se resumen las principales guías aportadas por el CCN. Las Administraciones Públicas podrán determinar aquellos sistemas de información a los que no les sea de aplicación lo dispuesto en el Real Decreto por tratarse de sistemas no relacionados con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo.

Mecanismos de Control

Cada órgano de la Administración pública o Entidad de Derecho Público establecerá sus mecanismos de control para **garantizar** de forma real y efectiva **el cumplimiento** del Esquema Nacional de Seguridad.

No obstante en el ENS se establecen unas actuaciones concretas para asegurar el control de las medidas de seguridad definidas.

Auditorías de Seguridad

Los sistemas estarán sujetos, en función de su categoría, a realizar auditorías de seguridad específicas para verificar el cumplimiento de las medidas del ENS. En un capítulo posterior se especifica el contenido y objetivo de este tipo de auditorías.

Respuesta ante incidentes de Seguridad

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (CERT - *Computer Emergency Response Team*). Desarrollará un programa que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las Administraciones Públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad. Siendo el CCN-CERT coordinador a nivel público estatal.

Informe del estado de Seguridad

El Comité Sectorial de Administración Electrónica articulará los procedimientos necesarios para conocer regularmente el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el Real Decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones Públicas.

Publicación 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.

Estas declaraciones de conformidad deberán ser publicadas en las correspondientes sedes electrónicas y situadas en lugar de fácil acceso para los usuarios.

La base por la que se declara la conformidad con los requisitos esenciales del ENS, es la superación en conformidad de la evaluación efectuada, realizada por el Responsable de Seguridad.

Contenido declaración de Conformidad

Constará de tres cuerpos. En el primer cuerpo se identificará el declarante, en el segundo se indicará el contenido de la declaración y, en el tercero, se señalará en base a qué se declara la conformidad y con qué finalidad.

El órgano o entidad de derecho público titular del sistema, que se declara conforme, se identificará de forma inequívoca en la declaración escrita, señalando grupos operativos, departamentos o Administración a la que pertenece, o los datos que fuesen necesarios para proporcionar la identificación concreta del organismo público a que se refiere.

La descripción del objeto se hará mediante la manifestación expresa que el sistema cumple los requerimientos establecidos en el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, de forma que recoja constancia expresa de lo siguiente:

- Que las sedes y registros electrónicos, así como el acceso electrónico de los ciudadanos a los mismos y a los servicios que proporcionan, cumplen las exigencias de seguridad del ENS.
- Que las especificaciones de seguridad están incluidas en el ciclo de vida de los servicios y sistemas, acompañadas del correspondiente procedimiento de control.
- Que existe mecanismo de control para garantizar el cumplimiento del ENS, establecido por el órgano o entidad de derecho público que efectúa la declaración.

La identificación del sistema se efectuará mediante su descripción de forma que pueda ser reconocido indubitadamente y, contendrá, al menos, el nombre del sistema, objeto y servicios que presta. Los servicios se identificarán con nombres comprensibles para los ciudadanos.

Fig. 6. Declaración de Conformidad

Gestión de Riesgos con Magerit

Hay dos grandes tareas a realizar:

- Análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.
- Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente.

Los **Activos** son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización.

Las **Amenazas** son cosas que les pueden pasar a los activos causando un perjuicio a la Organización

Los Activos tienen un valor para la Organización que puede verse alterado por las amenazas. Las amenazas actúan de dos formas diferentes sobre el valor del activo. Por un lado con la capacidad de degradación de de dicho valor si la amenaza ocurre. Esa medida es el **Impacto**.

Por otro lado con la probabilidad de que la amenaza ocurra. Si ponderamos el impacto por la probabilidad de ocurrencia, tendremos el **Riesgo** potencial del Activo.

Las Salvaguardas son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño. Actúan modificando la capacidad de degradación y la probabilidad de una amenaza, modificando consecuentemente el impacto y el riesgo. Las nuevas medidas, tras aplicar las salvaguardas, son conocidas como impacto residual y riesgo residual.

Los valores de impacto y riesgo (residual y potencial) son **evaluados** por la dirección junto con otros factores más cualitativos (intangibles, normativos, etc.) para aceptar el riesgo o realizar tratamientos sobre él.

Los **tratamientos** pueden ser de eliminación, mitigación, compartición y/o financiación. En los tres primeros casos, al modificarse bien los activos, bien las amenazas, o bien las salvaguardas es necesario volver a realizar un nuevo análisis de riesgos.

Análisis del Riesgo

Tratamiento del Riesgo

Fig. 7. Magerit

Categorización de los Sistemas de Información

La categoría de un sistema de información en materia de seguridad, modulará el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el **principio de proporcionalidad**.

La facultad para determinar la categoría del sistema corresponderá al Responsable de Seguridad.

La determinación de la categoría de un sistema se basa en la valoración del impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información o de los servicios.

Se entiende que un servicio queda afectado cuando: no se alcancen sus objetivos, queden desprotegidos los activos a su cargo, no se cumplan las obligaciones diarias de servicio o no se respeten la legalidad vigente y los derechos de los ciudadanos.

A fin de poder determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de sistemas, y de poder establecer la categoría del mismo, se tendrán en cuenta las siguientes **dimensiones de la seguridad**, que serán identificadas por sus correspondientes iniciales en mayúsculas:

- Disponibilidad [D].
- Autenticidad [A].
- Integridad [I].
- Confidencialidad [C].
- Trazabilidad [T].

Una información o un servicio pueden verse afectados en una o más de sus dimensiones de seguridad. Cada **dimensión** de seguridad afectada se adscribirá a uno de los siguientes niveles: **BAJO, MEDIO o ALTO**. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

Para determinar la categoría de un sistema de información se definen tres **categorías**: **BÁSICA, MEDIA y ALTA**.

- Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
- Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel MEDIO, y ninguna alcanza un nivel superior.
- Un sistema de información será de categoría BÁSICA si alguna de sus dimensiones de seguridad alcanza el nivel BAJO, y ninguna alcanza un nivel superior.

La secuencia de actuaciones para determinar la categoría de un sistema se resume en:

Identificación del nivel correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en la tabla de la siguiente página.

Determinación de la categoría del sistema, según la categoría de sus dimensiones

Categorización del Sistema de Información	Disponibilidad RTO.- Recovery Time Objective Si el uso de la información es a través de servicios contemplados en el sistema de información, basta valorar dichos servicios e imputar los mismos valores a la información necesaria	Autenticidad Aplica por igual a la información y/o servicios
Nivel Alto	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la indisponibilidad de la información/detención del servicio causaría un grave daño, de difícil o imposible reparación • porque la indisponibilidad de la información/detención del servicio supondría el incumplimiento grave de una norma • porque la indisponibilidad de la información/detención del servicio causaría un daño reputacional grave con los ciudadanos o con otras organizaciones • porque la indisponibilidad de la información/detención del servicio podría desembocar en protestas masivas (alteración seria del orden público) • cuando el RTO es inferior a 4 horas	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible reparación • porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas • porque la falsedad en su origen o en su destinatario causaría un daño reputacional grave con los ciudadanos o con otras organizaciones • porque la falsedad en su origen o en su destinatario podría desembocar en protestas masivas (alteración seria del orden público)
Nivel Medio	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la indisponibilidad de la información/detención del servicio causaría un daño importante aunque subsanable • porque la indisponibilidad de la información/detención del servicio supondría el incumplimiento material o formal de una norma • porque la indisponibilidad de la información/detención del servicio causaría un daño reputacional importante con los ciudadanos o con otras organizaciones • porque la indisponibilidad de la información/detención del servicio podría desembocar en protestas públicas (alteración del orden público) • cuando el RTO se sitúa entre 4 y 24 horas (un día)	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable • porque la falsedad en su origen o en su destinatario causaría pérdidas económicas importantes • porque la falsedad en su origen o en su destinatario causaría un daño reputacional importante con los ciudadanos o con otras organizaciones • porque la falsedad en su origen o en su destinatario podría desembocar en protestas públicas (alteración del orden público)
Nivel Bajo	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la indisponibilidad de la información/detención del servicio causaría algún perjuicio • porque la indisponibilidad de la información/detención del servicio supondría el incumplimiento leve de una norma • porque la indisponibilidad de la información/detención del servicio causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones • porque la indisponibilidad de la información/detención del servicio podría desembocar en múltiples protestas individuales • cuando el RTO se sitúa entre 1 y 5 días (una semana)	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la falsedad en su origen o en su destinatario causaría algún perjuicio • porque la falsedad en su origen o en su destinatario causaría pérdidas económicas apreciables • porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones • porque la falsedad en su origen o en su destinatario podría desembocar en múltiples protestas individuales
Sin Valorar	• cuando la información/servicio es prescindible por tiempo indefinido • cuando el RTO es superior a 5 días laborables (una semana)	• cuando el origen es irrelevante o ampliamente conocido por otros medios • cuando el destinatario es irrelevante, por ejemplo por tratarse de información/servicios de difusión anónima

Integridad	Confidencialidad	Trazabilidad
Los requisitos de integridad sobre un servicio derivan de la información que maneja. Esto incluye la posibilidad de que la información quede en un estado impropio porque el servicio no se complete adecuadamente.	Los requisitos de confidencialidad sobre un servicio derivan de la información que maneja	Aplica por igual a la información y/o servicios
• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible reparación • porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas • porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones • porque su manipulación o alteración no autorizada	• porque la información debe conocerla un número muy reducido de personas • por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque su revelación causaría un grave daño, de difícil o imposible reparación • porque su revelación supondría el incumplimiento grave de una norma • porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas • porque su revelación causaría un daño reputacional grave con los ciudadanos o con otras organizaciones • porque su revelación podría desembocar en protestas masivas (alteración seria del orden público)	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la incapacidad para rastrear un acceso a la información/servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave • porque la incapacidad para rastrear un acceso a la información/servicio dificultaría notablemente la capacidad para perseguir delitos • porque la incapacidad para rastrear un acceso a la información/servicio facilitaría enormemente la comisión de delitos graves
• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable • porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma • porque su manipulación o modificación no autorizada causaría pérdidas económicas importantes • porque su manipulación o modificación no autorizada causaría un daño reputacional importante con los ciudadanos o con otras organizaciones • porque su manipulación o modificación no autorizada podría desembocar en protestas públicas (alteración del orden público)	• porque la información deben conocerla sólo quienes lo necesiten para su trabajo, con autorización explícita • por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque su revelación causaría un daño importante aunque subsanable • porque su revelación supondría el incumplimiento material o formal de una norma • porque su revelación causaría pérdidas económicas importantes • porque su revelación causaría un daño reputacional importante con los ciudadanos o con otras organizaciones • porque su revelación podría desembocar en protestas públicas (alteración del orden público)	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la incapacidad para rastrear un acceso a la información/servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante • porque la incapacidad para rastrear un acceso a la información/servicio dificultaría notablemente la capacidad para perseguir delitos • porque la incapacidad para rastrear un acceso a la información/servicio facilitaría la comisión de delitos
• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque su manipulación o modificación no autorizada causaría algún perjuicio • porque su manipulación o modificación no autorizada supondría el incumplimiento leve de una norma • porque su manipulación o modificación no autorizada supondría pérdidas económicas apreciables • porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones • porque su manipulación o modificación no autorizada podría desembocar en múltiples protestas individuales	• porque la información no deben conocerla personas ajenas a la organización • por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque su revelación causaría algún perjuicio • porque su revelación supondría el incumplimiento leve de una norma • porque su revelación supondría pérdidas económicas apreciables • porque su revelación causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones • porque su revelación podría desembocar en múltiples protestas individuales	• por disposición legal o administrativa: ley, decreto, orden, reglamento, ... • porque la incapacidad para rastrear un acceso a la información/servicio dificultaría la capacidad de subsanar errores • porque la incapacidad para rastrear un acceso a la información/servicio dificultaría la capacidad para perseguir delitos
• cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables	• información de carácter público, accesible por cualquier persona	• cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios • cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios


SPYWARE
UPDATE
VIRUS
SECURITY
HACKER
PHISHING
INTERNET
PASSW

Las Medidas de Seguridad y la Declaración de Aplicabilidad

El Esquema Nacional de Seguridad establece una serie de medidas de seguridad que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría del sistema de información de que se trate.

Estas medidas **constituyen un mínimo** que se debe implementar, o justificar los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios.

La relación de **medidas seleccionadas** se formalizará en un documento denominado **Declaración de Aplicabilidad**, firmado por el Responsable de Seguridad del sistema.

Esta Declaración de Aplicabilidad será posteriormente revisada y auditada en los procedimientos correspondientes.

Las medidas de seguridad se dividen en tres grupos:

- **Marco organizativo** [org]. Constituido por el conjunto de medidas (4) relacionadas con la organización global de la seguridad.
- **Marco operacional** [op]. Formado por las medidas a tomar para proteger la operación del sistema . Se clasifican en:
  - Planificación (5)
  - Control de Acceso (7)
  - Explotación (11)
  - Servicios Externos (3)
  - Continuidad del Servicio (3)
  - Monitorización del Sistema (2)
- **Medidas de protección** [mp]. Se centran en proteger activos concretos:
  - Instalaciones e Infraestructuras (8)
  - Gestión del Personal (5)
  - Protección de los Equipos (4)
  - Telecomunicaciones (5)
  - Soportes de Información (5)
  - Aplicaciones Informáticas (2)
  - Protección de la Información (7)
  - Protección de los Servicios (4)

Para la selección de las medidas de seguridad se seguirán los pasos siguientes:

- Identificación de los tipos de activos presentes.
- Determinación de las dimensiones de seguridad relevantes y su nivel, y determinación de la categoría del sistema.
- Selección de las medidas de seguridad apropiadas de entre las contenidas en este capítulo, de acuerdo con las dimensiones de seguridad y sus niveles.

La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad, se indican en las tablas siguientes, utilizando las siguientes convenciones:

- Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad en algún nivel determinado se utiliza la voz «aplica».
- «n.a.» significa «no aplica».
- Para indicar que las exigencias de un nivel son iguales a los del nivel inferior se utiliza el signo "=".
- Para indicar el incremento de exigencias graduado en función del nivel de la dimensión de seguridad, se utilizan los signos "+" y "++".
- Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial.

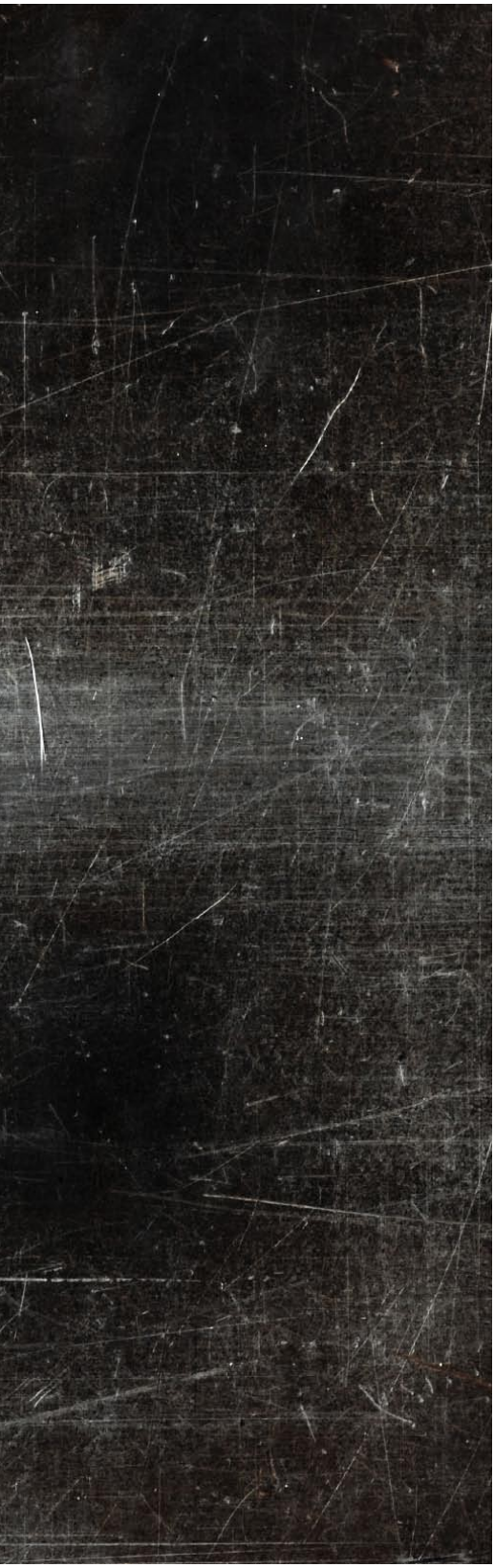
Dimensiones				Marco Organizativo
Afectadas	BAJO	MEDIO	ALTO	
categoría	aplica	=	=	org.1 Política de seguridad
categoría	aplica	=	=	org.2 Normativa de seguridad
categoría	aplica	=	=	org.3 Procedimientos de seguridad
categoría	aplica	=	=	org.4 Proceso de autorización

Dimensiones				Marco Operacional
Afectadas	BAJO	MEDIO	ALTO	
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
ICAT	aplica	=	=	op.acc.2 Requisitos de acceso
ICAT	n.a.	aplica	=	op.acc.3 Segregación de funciones y tareas
ICAT	aplica	=	=	op.acc.4 Proceso de gestión de derechos de acceso
ICAT	aplica	+	++	op.acc.5 Mecanismo de autenticación
ICAT	aplica	+	++	op.acc.6 Acceso local (local logon)
ICAT	aplica	+	=	op.acc.7 Acceso remoto (remote login)
op.exp Explotación				
categoría	aplica	=	=	op.exp.1 Inventario de activos
categoría	aplica	=	=	op.exp.2 ConfIguración de seguridad
categoría	n.a.	aplica	=	op.exp.3 Gestión de la configuración
categoría	aplica	=	=	op.exp.4 Mantenimiento
categoría	n.a.	aplica	=	op.exp.5 Gestión de cambios
categoría	aplica	=	=	op.exp.6 Protección frente a código dañino
categoría	n.a.	aplica	=	op.exp.7 Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8 Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9 Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10 Protección de los registros de actividad
categoría	aplica	+	=	op.exp.11 Protección de claves criptográficas
op.ext Servicios externos				
categoría	n.a.	aplica	=	op.ext.1 Contratación y acuerdos de nivel de servicio
categoría	n.a.	aplica	=	op.ext.2 Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9 Medios alternativos
op.cont Continuidad del servicio				
D	n.a.	aplica	=	op.cont.1 Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2 Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3 Pruebas periódicas
op.mon Monitorización del sistema				
categoría	n.a.	n.a.	aplica	op.mon.1 Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2 Sistema de métricas

Dimensiones				Medidas de Protección
Afectadas	BAJO	MEDIO	ALTO	
mp.if Protección a las instalaciones e infraestructuras				
categoría	aplica	=	=	mp.if.1 Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2 Identificación de las personas
categoría	aplica	=	=	mp.if.3 Acondicionamiento de los locales
D	aplica	+	=	mp.if.4 Energía eléctrica
D	aplica	=	=	mp.if.5 Protección frente a incendios
D	n.a.	aplica	=	mp.if.6 Protección frente a inundaciones
categoría	aplica	=	=	mp.if.7 Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9 Instalaciones alternativas
mp.per Gestión del personal				
categoría	n.a.	aplica	=	mp.per.1 Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2 Deberes y obligaciones
categoría	aplica	=	=	mp.per.3 Concienciación
categoría	aplica	=	=	mp.per.4 Formación
D	n.a.	n.a.	aplica	mp.per.9 Personal alternativo
mp.eq Protección de los equipos				
categoría	aplica	+	=	mp.eq.1 Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2 Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3 Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9 Medios alternativos
mp.com Protección de las comunicaciones				
categoría	aplica	=	+	mp.com.1 Perímetro seguro
C	n.a.	aplica	+	mp.com.2 Protección de la confidencialidad
IA	aplica	+	++	mp.com.3 Protección de la autenticidad y de la integridad
categoría	n.a.	n.a.	aplica	mp.com.4 Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9 Medios alternativos
mp.si Protección de los soportes de información				
C	aplica	=	=	mp.si.1 Etiquetado
IC	n.a.	aplica	+	mp.si.2 Criptografía
categoría	aplica	=	=	mp.si.3 Custodia
categoría	aplica	=	=	mp.si.4 Transporte
C	n.a.	aplica	=	mp.si.5 Borrado y destrucción
mp.sw Protección de las aplicaciones informáticas				
categoría	n.a.	aplica	=	mp.sw.1 Desarrollo
categoría	aplica	+	++	mp.sw.2 Aceptación y puesta en servicio
mp.info Protección de la información				
categoría	aplica	=	=	mp.info.1 Datos de carácter personal
C	aplica	+	=	mp.info.2 Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3 Cifrado
IA	aplica	+	++	mp.info.4 Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5 Sellos de tiempo
C	aplica	=	=	mp.info.6 Limpieza de documentos
D	n.a.	aplica	=	mp.info.9 Copias de seguridad (backup)
mp.s Protección de los servicios				
categoría	aplica	=	=	mp.s.1 Protección del correo electrónico
categoría	aplica	=	=	mp.s.2 Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8 Protección frente a denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9 Medios alternativos

Fig. 9. Medidas de Seguridad


www.



Aplicación del ENS en entornos y aplicaciones web

Dada la criticidad tanto de los entornos de producción como de los dispositivos embebidos, se hace necesario establecer una metodología que permita evaluar y reforzar la seguridad de los entornos y aplicaciones Web asociados a éstos.

Desde el punto de vista de la seguridad, todos los elementos que conforman el entorno o aplicación Web deben ser tenidos en cuenta a la hora de evaluar y diseñar los mecanismos de protección.

Existen dos procedimientos para mejorar la seguridad de las aplicaciones y entornos Web:

- **Durante el proceso de diseño y desarrollo** de la aplicación, estableciendo unos requisitos y controles de seguridad que debe cumplir tanto el código de la aplicación, como el entorno de desarrollo utilizado.
- Posteriormente, **tras la puesta en producción**, realizando el análisis de seguridad de la aplicación Web mediante auditorías de seguridad, análisis de vulnerabilidades y pruebas de intrusión.

Las **grandes amenazas** de seguridad de las aplicaciones Web están asociadas a las características intrínsecas a este tipo de entornos:

- Las aplicaciones Web en Internet están **públicamente disponibles**, en prácticamente cualquier entorno de computación.
- Los firewalls tradicionales deben dejar pasar el **tráfico** hacia puertos estándares **HTTP**, **SSL** y **TLS**, y son de poca utilidad en el filtrado de ataques directos sobre la aplicación Web.
- Los ataques desde Internet conllevan un **anonimato** muy elevado por parte del atacante.
- Las técnicas y **herramientas de ataque** necesarias para explotar vulnerabilidades en los entornos Web son **muy sencillas**, siendo en algunos casos más que suficiente el uso exclusivo de un navegador Web estándar.
- Las capacidades de autentificación y mantenimiento de sesiones en HTTP son muy limitadas, y es necesario desarrollar un sistema de autentificación y de **gestión de sesiones**. Este desarrollo puede introducir nuevas vulnerabilidades.

Adicionalmente a los diferentes elementos que forman parte de una arquitectura Web, existen otros elementos que son potenciales objetivos para los atacantes, tales como el **tráfico Web** intercambiado entre clientes y servidores, y la posibilidad de realizar ataques de **denegación de servicio (DoS)**.

Algunas de las vulnerabilidades de seguridad más comunes y relevantes en aplicaciones Web en los últimos años son: Cross-Site Scripting, Cross-Site Request Forgery, Inyección SQL/XPath/LDAP, HTTP Response Splitting, Path traversal, ...

Los incidentes de mayor relevancia son publicados en la *WHID,* **Web Hacking Incidents Database**. Se recomienda su consulta para disponer de una visión actualizada de los ataques que se están llevando a cabo.

Uno de los objetivos fundamentales de todo responsable de seguridad debe ser el evitar aparecer en estas bases de datos de incidentes, dónde se reflejaría su dominio o entorno Web como vulnerable.

Estrategia y Metodología de Seguridad de Aplicaciones Web

La estrategia de seguridad de un entorno o aplicación Web debe incluir:

- Formación en seguridad de aplicaciones Web.
- Arquitectura e infraestructura (sistemas y redes) segura: servidor Web y de aplicación, framework de desarrollo, etc.
- Metodología de seguridad de desarrollo de aplicaciones Web, gestión de versiones y actualizaciones.
- Metodología de análisis de seguridad de aplicaciones Web.
- Web Application Firewalls (WAF's).
- Auditorías de seguridad:
  - Caja negra: pruebas de intrusión y Web Application Security Scanners (WASS)
  - Caja blanca: revisión de código manual y automático.
- Mecanismos de Respuesta ante incidentes.

Para alcanzar un nivel de seguridad adecuado en el entorno o aplicación Web es necesario **involucrar tanto a administradores como a desarrolladores**.

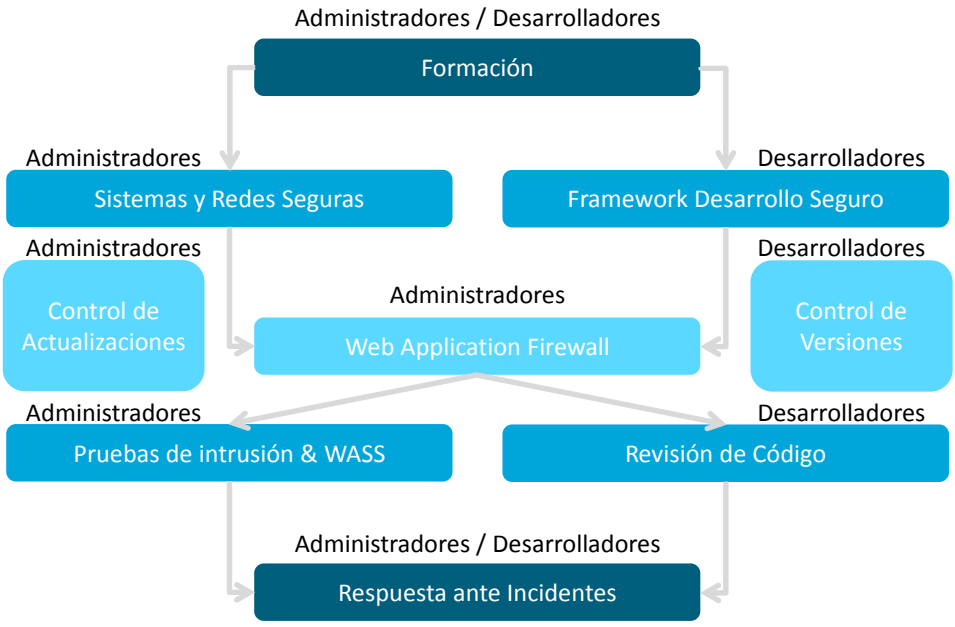


Fig. 10. Componentes de Seguridad en entornos web

Respuestas ante incidentes

En el caso de identificar un incidente de seguridad en un entorno Web, uno de los recursos de mayor relevancia es el **CCN-CERT**. La finalidad principal del CCN-CERT es contribuir a la mejora del nivel de seguridad de los sistemas de información en las Administraciones Públicas españolas.

La comunidad a la que presta servicio el CCN-CERT está constituida por el conjunto de organismos de la Administración: General, Autonómica y Local.

Arquitecturas de seguridad en entornos web

Existen fundamentalmente dos modelos de arquitectura de aplicaciones Web:

- En dos capas: donde el servidor Web y de aplicación conviven en el mismo sistema.
- En tres capas: donde cada elemento (servidor Web, servidor de aplicación y servidor de base de datos) corresponde a un sistema independiente.

Modelo de 3 capas

Desde el punto de vista de la seguridad, **el modelo en tres capas es preferible** ya que ofrece separación entre los distintos componentes y un mayor aislamiento frente a incidentes de seguridad en cualquiera de los elementos. Adicionalmente, la arquitectura de tres capas, aunque más compleja, ofrece:

- **Mayor escalabilidad** para poder gestionar un mayor número de peticiones y usuarios.
- La posibilidad de introducir **controles de acceso** avanzados, como filtrado del tráfico, y elementos avanzados de **monitorización**, como sistemas de detección de intrusos, entre los elementos de la arquitectura.
- Permite aplicar una **securización más estricta** sobre cada uno de los componentes, ya que cada uno tiene asignada una funcionalidad y tareas claramente definidas.

Web App Firewalls

Uno de los elementos principales empleados en la protección de entornos y aplicaciones Web son los cortafuegos (firewalls) de aplicaciones Web, también conocidos como ***WAF, Web Application Firewall.***

En arquitecturas Web de tres capas (servidor Web, servidor de aplicación y base de datos), existe la posibilidad de emplear WAF's dedicados entre cada una de las capas.

En el caso de ser necesario asegurar la confidencialidad de las comunicaciones Web, es necesario hacer uso de la versión segura del protocolo, HTTPS y utilizar SSL (Secure Socket Layer) o TLS (Transport Layer Security) para cifrar las comunicaciones entre el navegador Web y el servidor Web.

Protección de los componentes del sistema web

Adicionalmente a los elementos de seguridad propios de un entorno Web, es necesario proteger todos los elementos de la infraestructura en la que reside la aplicación Web, tales como dispositivos de comunicaciones (routers, switches, etc) o la infraestructura de servidores de nombres (DNS).

Las guías CCN-STIC proporcionan las mejores prácticas de seguridad para cada uno de los elementos que conforman el entorno Web. Los mecanismos de protección a implementar deben proteger los diferentes equipos frente a:

- **Ataques directos**, tales como accesos no autorizados sobre cualquiera de los elementos que conforman el entorno o aplicación Web.
- **Ataques indirectos**, dónde cualquiera de los elementos es empleado como herramienta en el ataque. Por ejemplo, un ataque sobre los servidores de DNS podría permitir redireccionar el tráfico de los clientes Web hacia un entorno malicioso que suplante la aplicación Web real.
- Ataques de **denegación de servicio** (DoS).

Desarrollo seguro de software de aplicaciones web

Uno de los elementos fundamentales en la estrategia de seguridad de aplicaciones Web pasa por incluir todos los aspectos de **seguridad en el ciclo de vida de desarrollo** de software. Desde el diseño y definición de requisitos hasta el pase a producción de las nuevas versiones.

En este sentido, la **formación** en seguridad que deben tener los **desarrolladores** web debe ser la apropiada.

Existen multitud de recomendaciones y frameworks de desarrollo para garantizar un entorno seguro. En la guía CCN-STIC-812 se describen numerosas recomendaciones con tal efecto. Vamos a resaltar algunas de ellas.

Recomendaciones generales

Todos los mecanismos de interacción entre los distintos componentes del entorno Web (servidor Web, de aplicación y base de datos) deben realizarse de forma segura. Las **comunicaciones** entre estos elementos deberán estar **cifradas**, autentificadas y asegurar su integridad.

El **almacenamiento** de información sensible, tanto propia de la lógica de la aplicación como las credenciales de acceso, debe de almacenarse **cifrada** en todos los servidores, y especialmente en el de base de datos.

Filtrado de datos de entrada

Algunos de los ataques Web habituales, como por ejemplo XSS o inyección SQL, pueden ser mitigados filtrando los datos maliciosos (código HTML o sentencias SQL) en la entrada de la aplicación. Se recomienda, aplicando criterios de defensa en profundidad, aplicar los mecanismos de filtrado tanto en la entrada como en la salida.

Los datos de entrada proporcionados por el usuario (o atacante) deben ser considerados dañinos por naturaleza, por ello es necesaria su verificación y análisis antes de ser procesados por la aplicación.

Existen **dos modelos para el filtrado** de datos de entrada:

- Eliminar los caracteres maliciosos y permitir el resto.
- Permitir sólo los caracteres válidos para cada entrada en la aplicación. Este modelo es el más restrictivo y seguro aunque no siempre puede ser implementado.

El filtrado de los datos de entrada del usuario se debería realizar tanto en el cliente como en el servidor. En caso de ser necesario un único nivel de validación, por ejemplo por motivos de rendimiento, este siempre se llevará a cabo en el servidor, ya que la validación en el cliente puede ser fácilmente manipulada por parte del atacante.

Control de mensajes de error

El entorno Web debe considerar una **gestión de errores adecuada**, minimizando la cantidad de información que se proporciona al usuario o atacante ante fallos en la aplicación.

La información contenida en los errores puede ser empleada durante el reconocimiento del entorno, y proporcionar información del software y las versiones empleadas, información del sistema de ficheros y detalles de dónde se encuentran ubicados los recursos empleados por la aplicación Web. Adicionalmente puede contener información más detallada de la base de datos que puede ser empleada por un atacante para ejecutar ataques de inyección de código más efectivos.

Es necesario en todo momento capturar las condiciones de error y mostrar mensajes de error personalizados con la mínima cantidad de información posible.

Autentificación y gestión de sesiones

En ningún caso la aplicación debe desvelar los detalles sobre qué componentes de las credenciales de acceso no son válidos. Por ejemplo, mensajes de error indicando que el usuario es válido, pero la clave no, facilitan enormemente a un atacante las tareas de adivinación de claves.

El mecanismo de **autentificación** debe proporcionar capacidades para definir una política de acceso, definir la longitud y complejidad de las claves, los mecanismos de log de acceso, y la política de bloqueo temporal de cuentas en base al tiempo tras un número de intentos de acceso fallidos.

La **gestión de sesiones** en la aplicación Web debe realizarse empleando identificadores de sesión o tokens no predecibles (es decir, suficientemente aleatorios), de suficiente longitud para que no puedan ser adivinados mediante técnicas de fuerza bruta, y que caduquen tras cierto tiempo.

Gestión de logs

Existen numerosos motivos para la generación, almacenamiento y gestión de logs, tales como motivos legales y/o de regulación, de contabilidad, para la resolución problemas, auditoría, estadísticas, respuesta ante incidentes y análisis forense.

Se recomienda la aplicación de las **mejores prácticas en la gestión de logs**, no sólo a nivel de los diferentes elementos que componen la plataforma del entorno Web, tales como los dispositivos de red, firewalls, IDS, WAF, servidor Web, servidor de aplicación o servidor de base de datos, sino también en el propio código de la aplicación Web.

Dentro de las mejores prácticas de gestión de logs es necesario considerar su **rotación**, **ubicación** (local y remota), espacio necesario en disco, **permisos**, rendimiento política de retención de logs, centralización y correlación de logs, y las herramientas y soluciones para su análisis detallado (automático y manual).

Análisis de seguridad de aplicaciones web

Una vez se ha implementado una metodología de desarrollo de software para aplicaciones Web que contempla los aspectos de seguridad pertinentes, es necesario complementarla con análisis y auditorías del entorno y la aplicación Web.

Caja Negra y Caja Blanca

La metodología de análisis debe incluir dos enfoques:

- **Caja negra.** El análisis de caja negra se centra en estudiar las vulnerabilidades de seguridad de la aplicación Web desde el punto de vista de un **atacante externo**. El analista, actuando como atacante, no dispone de ningún tipo de información previa relativa a la aplicación y mucho menos del código de la misma. La metodología a seguir es similar a la empleada en las pruebas de intrusión, donde el análisis desde el punto de vista del atacante se divide en varias fases que permiten obtener información de la aplicación y sus posibles vulnerabilidades. Las fases típicas de este proceso son:
  - Reconocimiento, también conocida como descubrimiento o identificación.
  - Enumeración o escaneo.
  - Detección y verificación de vulnerabilidades.

  Existen numerosas herramientas que permiten analizar e identificar vulnerabilidades en aplicaciones Web de forma automática. Las revisiones automáticas deben complementarse con análisis manuales, por la complejidad de las pruebas a acometer.
- **Caja blanca.** El análisis de caja blanca se centra en estudiar las vulnerabilidades de seguridad de la aplicación Web desde el **punto de vista del desarrollador**. Dentro de las áreas de revisión de código se deberá analizar el código de la aplicación Web en busca de vulnerabilidades.

Requisitos de auditorías de seguridad en entornos web

Los requisitos necesarios para que una auditoría de seguridad realizada por terceras partes sobre los entornos Web de la Administración son:

- **Completitud**: la auditoría debe reflejar el estado real y completo de la seguridad de los servicios Web ofrecidos por el entorno objetivo, sin importar su base tecnológica a efectos de alcance.
- **Relevancia**: la auditoría deberá reflejar, de forma concisa y práctica, las posibilidades, teóricas o prácticas, de que un atacante altere las características de Disponibilidad, Integridad, Confidencialidad, Autenticidad, y Trazabilidad ofrecidas por los servicios Web.
- **Secreto**: se deberá comunicar toda la identificación de los terceros implicados en la auditoría. Los auditores tendrán un acuerdo de confidencialidad que reforzará en lo posible la legislación de referencia, con penalización económica en caso de incumplimiento y avales suficientes.

Los **resultados** de la auditoría deben ser **reproducibles**.

Es recomendable disponer en el informe de resultados de una **lista detallada de las vulnerabilidades** y problemas de seguridad encontrados, clasificados por orden de criticidad.

De forma complementaria es necesario analizar la inclusión de pruebas de denegación de servicio y de ingeniería social.

El análisis de seguridad debe identificar complementariamente alguno de los aspectos asociados a la gestión del entorno e infraestructura Web, tales como:

- La política de actualizaciones de software.
- El ciclo de vida de la aplicación Web y la metodología de actualizaciones, resolución de errores (bugs), e inclusión de nuevas funcionalidades.
- Los mecanismos de copia de seguridad (backup) y su cifrado.

Alcance de la auditoría

El determinar y cerrar el ámbito o alcance de la auditoría de seguridad de un entorno Web no es una tarea sencilla debido a las relaciones existentes entre múltiples dominios y aplicaciones Web.

Se recomienda **cerrar el alcance inicialmente** mediante una lista de dominios objetivo de la auditoría. Todas las aplicaciones Web existentes en el dominio o los dominios del alcance, serían objeto de las pruebas englobadas dentro de la auditoría.

Adicionalmente, es posible limitar aún más el alcance en entornos muy complejos mediante la definición de un límite máximo en la profundidad del número de enlaces recorridos desde la página Web principal.

Fases de la auditoría

Las **fases** de la metodología de análisis recomendada son:

- **Reconocimiento**, también conocida como descubrimiento o identificación.
- **Enumeración** o escaneo.
- **Análisis** (detección y verificación) de vulnerabilidades.

Cada una de estas fases deben incluir información detallada sobre los elementos y fuentes de datos relacionadas con el entorno o aplicación Web objetivo de la auditoría de seguridad.

A continuación se desarrolla brevemente el alcance de cada fase.

Reconocimiento

En la fase de Reconocimiento es necesario analizar en detalle toda la información disponible en los servicios de **registro de dominios y rangos de direcciones IP**, además de:

- Información confidencial y sensible en buscadores accesibles públicamente (Google, Yahoo, etc) mediante técnicas de búsqueda avanzadas, conocidas como "Google Hacking".
- Identificación de relaciones con otras organizaciones, entornos Web y dominios.
- Obtención de un **mapa Web completo** en modo texto y/o gráfico del entorno objetivo, separando claramente partes estáticas y dinámicas.
- Análisis de correspondencias y discrepancias entre el mapa Web obtenido previamente y el mapa descrito en el sitio Web objetivo.
- Información de la ubicación en la red del entorno Web objetivo y tráfico ICMP permitido.
- Identificación de los **sistemas de comunicaciones y dispositivos de red:** routers, balanceadores, etc.
- Identificación de los **sistemas de protección de perímetro** (firewalls, IDS, etc).

Enumeración

En la fase de Enumeración es necesario obtener la mayor i**nformación posible sobre los servicios y recursos** del entorno Web objetivo, incluyendo tanto su ubicación en la red como los detalles de los elementos que lo conforman:

- Enumeración de los **servicios disponibles** en el entorno objetivo, obtenida mediante escaneos de puertos (TCP y UDP) exhaustivos.
- Identificación de la **plataforma y sistema operativo** (OS fingerprinting) de los servidores objetivo, al menos, servidor Web, servidor de aplicación y base de datos.
- Identificación de la política de **tráfico permitido** en los sistemas de protección de perímetro.
- Identificación de los **contenidos**:
  - Identificación de recursos existentes en el entorno Web, tanto enlazados como adivinados/obtenidos por fuerza bruta o técnicas de diccionario.
  - Información de la estructura de la Web de los dominios objetivo, diferenciando contenidos y recursos estáticos y dinámicos.
  - Listado de las páginas dinámicas detectadas, sus parámetros de entrada, los tipos de los parámetros y el método de transferencia al servidor.
  - Identificación de los lenguaje(s) y entorno(s) de programación empleado(s).
  - Acceso y análisis de los códigos de error generados por la aplicación Web.
  - Identificación de las extensiones de ficheros empleadas en los recursos Web y la gestión de las diferentes extensiones de ficheros.
  - Identificación de contenidos por defecto propios de las tecnologías empleadas en el entorno Web.
  - Acceso público a páginas administrativas, de gestión, estadísticas, etc.
  - Identificación de recursos con control de accesos, es decir, que requieren autentificación (páginas de login).
  - Identificación de copias de seguridad/versiones anteriores de recursos

accesibles, tanto enlazadas como adivinadas/obtenidas por fuerza bruta o técnicas de diccionario.

- Identificación de relaciones con otros entornos y aplicaciones Web, y análisis de seguridad en la invocación y referencias a servicios Web tanto internos y externos.
- Análisis de los mecanismos de control de almacenamiento de contenidos en cachés y dispositivos de red intermedios, tales como proxies.
- Análisis de los mecanismos de control de publicación de contenidos en los servidores de búsqueda de Internet: Google, Yahoo, etc.
- Análisis de los mecanismos existentes centrados en ofrecer una superficie de exposición mínima a la totalidad del entorno Web.
- Identificación de las capacidades de la base de datos, contenidos y funcionalidad disponible por defecto.

Vulnerabilidades

En la fase de Análisis se realiza la **identificación de vulnerabilidades de filtrado** mediante el chequeo de parámetros de entrada en los componentes dinámicos de la aplicación (Inyección SQL, Inyección SQL ciega, Inyección LDAP y XPath, XSS, reflejado y persistente, CSRF, HTTP Response Splitting, Inyección de comandos en el sistema operativo, ...). Además de:

- Identificación de vulnerabilidades en los **mecanismos de autentificación**.
- Análisis de seguridad en los mecanismos de **control de sesiones**.
- Análisis de los mecanismos de **control de acceso** (ACLs).

En todos aquellos entornos Web dónde existe el concepto de usuarios autentificados, se recomienda la realización de los análisis de seguridad desde dos vertientes:

- Mediante un usuario externo **sin credenciales** de acceso.
- Mediante un usuario **con credenciales** de acceso, y que por tanto puede acceder a contenidos protegidos o privados.

Denegación de servicio DoS

Se recomienda incluir en el alcance de la auditoría, como elemento opcional, la realización de **pruebas de carga** que podrían provocar una denegación de servicio (DoS) sobre el entorno objetivo. Este tipo de pruebas debe de ser meticulosamente planeado, especialmente sobre entornos en producción, para evitar problemas de disponibilidad en el servicio del entorno Web.

Pueden realizarse dos tipos de pruebas de carga:

- **DoS simple**: empleando un único cliente, y definiendo el ancho de banda disponible, por ejemplo 20Mbps.
- **DoS distribuida** (DDoS): empleando múltiples clientes, por ejemplo 20, y definiendo el ancho de banda disponible para cada uno de ellos, por ejemplo 20Mbps.


Health
Greenings
Phair macy

Aplicación del Esquema Nacional de Seguridad en el uso del Correo Electrónico

Nadie duda de la revolución que el correo electrónico ha supuesto a la hora de trabajar en cualquier organismo, introduciendo innumerables ventajas de entre las que destaca la rapidez de comunicación y envío de datos; pero como cualquier cambio, **el correo electrónico introduce** una serie de **riesgos** que es necesario conocer y, hasta donde sea posible, mitigar, para garantizar la confidencialidad, integridad y disponibilidad de la información corporativa.

Por este motivo, el Esquema Nacional de Seguridad introduce medidas de seguridad que, con independencia de la categoría del sistema, especifica la obligatoriedad de proteger la información transmitida tanto en el cuerpo como en los anexos de un mensaje, de proteger la información de encaminamiento y establecimiento de conexiones y de proteger a la organización frente a las amenazas especialmente vinculadas al correo electrónico, como el spam, el software dañino o el código activo.

La organización debe ejecutar un **análisis de riesgos** que evalúe amenazas, probabilidades, impactos, riesgos efectivos, salvaguardas y riesgos residuales que afecten a los sistemas corporativos de correo electrónico.

Dicho análisis debe estar contenido en un análisis global de riesgos para la organización, y permitirá conocer los principales riesgos a los que está expuesto el correo corporativo y las salvaguardas aplicadas para mitigarlos.

Entre los principales riesgos se encuentran:

- **Software Dañino**. Para evitar la contaminación del receptor de un correo electrónico es necesaria la utilización de sistemas antivirus, tanto en el equipo donde se lee el mensaje como en servidores de correo intermedios, así como un uso correcto del correo electrónico por parte del usuario.
- **SPAM**. Bajo la denominación SPAM se identifica el correo no deseado por el usuario. Normalmente tratan de ofrecer servicios fraudulentos y es habitual que bajo la etiqueta de correo no deseado se reciban ataques de phising.
- **Fugas de Información**. El correo electrónico es una potencial fuente de fugas de información, ya que permite remitir volúmenes relativamente importantes de datos a un tercero de una forma que no siempre es posible detectar; sobre todo si consideramos la facilidad con la que los usuarios pueden acceder a correos personales externos (gmail, outlook, etc.) a través del navegador.
- **Ingeniería Social**. Suelen tener como objetivo usuarios concretos que bien por su trabajo, bien por su nivel de privilegios en la red, pueden facilitar al atacante datos relevantes sin ellos saberlo, derivando en problemas de fugas de información, malware, etc.
- **Daños a la Imagen**. Un uso inadecuado de las direcciones de correo electrónico propias de una organización puede perjudicar seriamente a su imagen: correos insultantes, de contenido ilícito, que fomenten actitudes contrarias a la convivencia,... no sólo perjudican la imagen de esta persona, sino la de la organización en su conjunto;
- **Bulos**. Noticias falsas que intentan pasar por reales ante sus receptores; a diferencia de los fraudes, como el phishing, los bulos no tienen por qué tener propósito delictivo o de lucro, aunque pueden implicar impactos muy dañinos contra una organización.

Políticas en el Uso del Correo Electrónico

Las organizaciones deben regular, en forma de **normativa específica**, el uso del correo electrónico corporativo por parte de sus empleados.

Normativa de Obligado Cumplimiento

Esta normativa debe contener:

- **Uso adecuado**, racional y leal del correo electrónico corporativo, en especial en lo relativo a la confidencialidad de los datos.
- **Regulación** del envío de **información sensible** o de datos de carácter personal a través del correo electrónico.
- **Prohibición** expresa del uso del correo corporativo con **fines personales**, con la posible excepción del uso razonable del mismo siempre que éste no introduzca riesgos significativos en la organización.
- **Garantía reputacional**. Prohibición expresa del uso del correo electrónico corporativo en cualquier forma que degrade o pueda degradar la reputación de la organización o de las personas que la componen.
- Directrices de **almacenamiento y eliminación** del correo en servidores corporativos.
- Directrices de **actuación ante correos electrónicos recibidos** por el usuario que puedan suponer un riesgo para la seguridad de la organización.
- **Medidas disciplinarias** a que haya lugar en caso de incumplimientos de los deberes y obligaciones en el uso del correo electrónico.

Recomendaciones y directrices

Además, se deben facilitar **recomendaciones** o restricciones directas en la utilización del correo; estas directrices, siempre dependientes de la regulación anterior, tienen como objetivo la **mayor concienciación** en temas referentes a la seguridad en el uso del correo electrónico:

- Prohibición de ejecución de ficheros adjuntos provenientes de fuentes no confiables.
- Prohibición de envío de información sensible fuera de las premisas de la organización sin cumplir las medidas de seguridad oportunas.
- Prohibición de respuesta a cualquier mensaje considerado sospechoso, incluyendo los mensajes de SPAM que requieren de un correo para dar de baja la dirección de una lista de distribución concreta.
- Restricción en el uso de correos personales para envío de información sensible.
- Recomendaciones para identificar ataques de phishing contra la organización.

Factores a analizar en la selección de una solución de correo

Cifrado. El sistema debe proporcionar cifrado robusto y basado en estándares internacionales.

Tránsito de datos. Si en la solución se produce tránsito de datos en texto claro es necesario garantizar que dicho tránsito no afecta a la confidencialidad de la información corporativa y que se cumplen las restricciones legales de aplicación, en especial las relativas a datos de carácter personal.

Costes. Es necesario analizar en términos económicos diferentes alternativas y aplicar la más adecuada en cada caso. El factor coste no debe anteponerse bajo ninguna condición al factor seguridad.

Además de los tradicionales de **Facilidad de uso**, **Capacidad de integración** y **Monitorización**.

Fig. 11. Selección de una solución de correo

Medidas de Seguridad en el Servidor de Correo

Arquitectura de Red

El servidor de correo electrónico corporativo debe estar ubicado en una **zona desmilitarizada (DMZ)** aislada tanto de Internet como de la red interna de la organización mediante un cortafuegos correctamente configurado.

Habitualmente, existen dos aproximaciones para configurar una zona desmilitarizada; en la primera de ellas la DMZ corporativa se configura con dos elementos cortafuegos, uno para aislar dicha zona de la red interna y otro para aislarla de la externa, preferiblemente de tecnologías diferentes para evitar que un problema de seguridad concreto en uno de ellos repercuta en el otro y por tanto en toda la organización.

La segunda aproximación para la definición de una DMZ se basa en el uso de un único elemento cortafuegos (redundado o no) para separar zonas de red (interna/ DMZ/Internet), mediante el uso de tarjetería de red adicional en el sistema (se requiere al menos una tarjeta por cada zona de la red).

En el caso de sistemas evaluados de categoría ALTA, el ENS especifica como obligatoria la utilización de **dos o más equipos de diferente fabricante en cascada** y con sistemas redundantes que garanticen la continuidad en caso de fallo técnico.

En los entornos de categoría ALTA la organización debe implantar en la arquitectura de red sistemas de detección o prevención de intrusiones basados en red (NIDS/ NIPS) que permitan identificar o incluso detener ataques o tráficos anómalos contra la plataforma de correo corporativo.

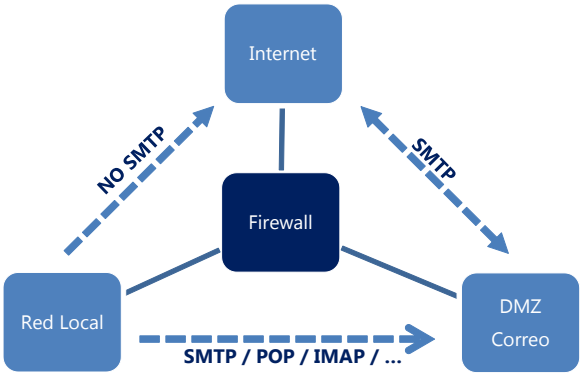


Fig. 12. Arquitectura de Red de Correo

Bastionado del Sistema

Los servidores de correo deben estar **correctamente bastionados** a nivel de sistema operativo. El servidor o servidores de correo corporativo deben estar en **sistemas dedicados**, no compartiendo su funcionalidad con otros entornos de la organización para evitar que vulnerabilidades en éstos afecten al correo electrónico.

En términos generales, debemos considerar siempre los siguientes extremos:

- **Aplicación de parches** y actualizaciones de seguridad en el sistema tan pronto como sea posible. Regulado en la normativa de aplicación de Parches y Vulnerabilidades.
- **Eliminación de los servicios no necesarios** para el funcionamiento correcto del sistema: Servicios de impresión de documentos (CUPS, LPD...), Servicios de compartición de ficheros (NFS, SMB...), Servidores web o de aplicaciones (Apache,

IIS, Tomcat…), Servicios simples TCP (chargen, echo, daytime…), Servicios de gestión remota (SSH, VNC, Terminal Remota…).

- **Restricciones de acceso** adecuadas, tanto desde la red interna como desde Internet: tráfico externo SMTP, tráfico interno POP/ IMAP, tráfico administrativo autorizado, bloqueo de tráfico no autorizado, etc.
- Políticas de **gestión de usuarios y contraseñas** robustas. El acceso para gestión del servidor debe estar limitado a unos pocos usuarios de las áreas técnicas correspondientes, siempre con usuarios nominales y registrando hasta donde técnicamente sea posible las acciones ejecutadas en dichos accesos .
- Permisos correctos en todo el sistema de archivos, pero prestando especial atención a las carpetas de correo de los usuarios. El **acceso privilegiado** al entorno de correo debe permanecer **restringido** a unas pocas personas del área técnica correspondiente y las acciones de dichos accesos deben ser convenientemente trazadas, y supervisadas por los responsables de seguridad, para detectar cualquier situación anómala, en especial aquellas que puedan implicar pérdidas de confidencialidad.
- **Monitorización y control** de parámetros que impliquen anomalías en la seguridad.

Seguridad en los Servicios de Correo

Los servicios asociados al correo electrónico deben también configurarse de manera segura. Es especialmente importante garantizar que las versiones de las diferentes aplicaciones utilizadas para la gestión del correo en el servidor sean correctas tanto desde el punto de vista funcional como desde el punto de vista de seguridad, aplicando las actualizaciones proporcionadas por el fabricante siempre que sea necesario.

Se debe **evaluar** muy cuidadosamente los riesgos asociados a permitir el **acceso** a los servicios de correo **desde toda Internet**. En caso de que sea necesario, es necesario garantizar en el tiempo que el servidor de correo no permite ser utilizado para el envío de correo no deseado.

Si esta situación se produce, aparte del problema de seguridad asociado y del impacto directo en la organización, es posible que el servidor corporativo sea incorporado a una lista negra y por tanto bloqueado automáticamente. Esto implica un elevado riesgo reputacional y un problema operativo que se puede llegar a producir al no poder enviar correos.

Independientemente de desde dónde esté permitido el acceso vía web al correo, el servidor web no debe estar ubicado en el propio servidor corporativo, sino en un **servidor independiente**. Todas la comunicaciones deben estar obligatoriamente cifradas y el servidor web debe proporcionar mecanismos de terminación automática de la sesión.

Administración del Servidor

La administración de los entornos de correo, al igual que el resto de componentes del sistema, debe basarse obligatoriamente en **procedimientos documentados** y aprobados por la organización y contener las definiciones pertinentes para los controles de acceso y la gestión de usuarios, las copias de seguridad y la continuidad del servicio, acorde a los requerimientos del ENS en función de la categorización del sistema.

Registros y Auditorías del Sistema

Los registros de actividad del sistema y sus copias deben **protegerse convenientemente** en los términos definidos en el ENS, garantizando que los registros no puedan ser modificados ni eliminados de forma no controlada. Estos

registros deben ser procesados, automática y/o manualmente, de forma periódica buscando anomalías, que deberán ser reportadas al Responsable de Seguridad, con objeto de emprender las acciones pertinentes. Ejemplos de anomalías pueden ser:

- **Intentos de accesos fallidos** al sistema o aplicaciones de correo por parte de usuarios privilegiados.
- **Conexiones** al sistema o aplicaciones de correo **fuera de horario** por parte de usuarios privilegiados.
- **Número excesivo de conexiones** legítimas al sistema fuera del horario habitual de trabajo.
- Indicios de **actividad excesiva en horario no laboral** (consumo de CPU, E/S, memoria…).
- **Accesos simultáneos** o cercanos en el tiempo con diferentes nombres de usuario desde un mismo origen.
- Número elevado de intentos de acceso fallido y posteriormente accesos legítimos desde un mismo origen.

Los sistemas involucrados en la gestión del correo electrónico deben ser analizados técnicamente por un **equipo de seguridad independiente** de los administradores de sistemas o redes; para ello debe establecerse una política de auditorías técnicas que contemple:

- Un conjunto de **pruebas automáticas** ejecutadas con una frecuencia alta o muy alta.
- Complementadas con **análisis manuales** ejecutados por el equipo de seguridad corporativo (internos o externos), desde la propia red y desde internet, simulando ataques externos.

Estas pruebas técnicas tienen que estar institucionalizadas en una metodología de auditoría basada en los estándares del mercado.

Roles a implementar en la gestión de la seguridad del correo electrónico

Para maximizar los controles de seguridad en los sistemas de correo corporativos, un aspecto clave es la separación de tareas en los entornos de correo electrónico, como un medio para prevenir o mitigar el riesgo asociado a errores, vulnerabilidades o compromisos de seguridad en general. Independientemente del sistema elegido, deben diferenciarse como mínimo los siguientes roles:

Administrador de Sistema

Administrador de Red

Administrador de Seguridad

El Rol de Administrador de Seguridad debe tener independencia absoluta –incluyendo línea de mando- de los roles anteriores. Este rol recae habitualmente en departamentos de seguridad corporativa, auditoría o control interno.

Esta estructura debe garantizar que las acciones del personal son controladas y auditadas de forma correcta, minimizando así el riesgo de fraudes o fugas de información.

Fig. 13. Roles de gestión del correo electrónico

Medidas de Seguridad en el Cliente de Correo

Equipos de usuario y clientes de correo

Para garantizar la seguridad del correo electrónico corporativo, como elemento clave en el flujo de mensajes, es necesario garantizar la **seguridad de los equipos de usuario** utilizados para procesar dicho correo:

- Actualización correcta del sistema operativo en cuanto a releases y parches de seguridad.
- Utilización de herramientas antimalware en el equipo.
- El usuario, en su trabajo habitual, no debe disponer de privilegios de root o administrador.
- Se debe evaluar la conveniencia de utilizar cortafuegos en los equipos personales.
- El equipo personal, fuera de los horarios de trabajo, debe permanecer apagado.
- Si el equipo de usuario almacena correo electrónico, es necesario analizar la conveniencia de cifrar el directorio donde se ubiquen los mensajes; esta conveniencia debe considerarse obligatoria en equipos portátiles.
- Desactivar características de interpretación de contenido activo (Active X, Javascript) en los clientes de correo.
- Desactivación de acciones automáticas del cliente de correo sobre el contenido.
- Incorporar capacidades antispam.

La organización debe **auditar** el cumplimiento de las directrices de seguridad en equipos de usuario –incluyendo dispositivos portátiles- de forma periódica, **mediante muestreo significativo** de los equipos corporativos.

Clientes Móviles

Estos dispositivos introducen en la organización una serie de riesgos asociados a la movilidad, además de los controles habituales de seguridad.

En el caso de dispositivos móviles la organización debe considerar las salvaguardas adecuadas desde el punto de vista físico, como la correcta **protección frente a robos o pérdidas**, así como restricciones desde el punto de vista lógico:

- Control de acceso al dispositivo mediante **contraseña**.
- **Cifrado** de la información almacenada.
- Cifrado de la información transmitida.
- **Borrado seguro**, local y remoto.
- Sistemas de control de **software dañino**.

En función del tipo de dispositivo móvil corporativo (BlackBerry, iPhone…), la organización debe definir las **directrices de bastionado y configuración** segura correspondientes.

Clientes web

Además de las medidas de aplicación para el resto de clientes, los clientes web tienen unas medidas especiales asociadas a sus características.

- Los **navegadores** utilizados para acceder a correo vía web deben estar permanentemente **actualizados** a su última versión, al menos en cuanto a parches de seguridad, así como **correctamente configurados**.
- Es obligatorio que una vez ha finalizado la sesión web, el usuario se desconecte

del servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.

- **Desactivación** de las características de **recordar contraseñas** para el navegador.
- **Borrado automático**, al cerrar el navegador, de la información sensible registrada por el mismo: histórico de navegación, histórico de descargas, histórico de formularios, caché, cookies, contraseñas, etc.
- **Instalación de complementos** para el navegador **prohibida** o, al menos, notificación al usuario en caso de intento de instalación de un addon.

Las organizaciones deben evaluar la posibilidad de utilizar POP3S e IMAPS, que no son más que la denominación habitual de los protocolos clásicos POP3 e IMAP pero a través de túneles de cifrado SSL.

Acceso Seguro al Servidor

En el caso de acceso vía web al correo electrónico, debe considerarse obligatorio el **uso de SSL/TLS** tanto para la autenticación del usuario como para la sesión en general.

Si el acceso al correo electrónico se produce desde **equipos ajenos a la organización** (típicamente accesos desde Internet), debe considerarse obligatorio que el usuario verifique que las características de seguridad del navegador son aceptables, en particular las referentes a recordar contraseñas y a borrado de cookies.

En cualquier caso, volvemos a insistir en que proporcionar este tipo de accesos es un riesgo muy considerable para la organización, ya que el equipo cliente, no controlado, puede estar comprometido y por tanto la información que trata puede ser interceptada independientemente de la configuración de un navegador o cliente concretos, por lo que es necesario **evaluar muy cuidadosamente** si permitimos estos accesos.

Medidas de Seguridad centradas en el contenido

Cifrado y Firma de datos

Las organizaciones deben analizar la conveniencia de implantar controles y herramientas para el cifrado (y firma) del correo electrónico de acreditada robustez, que empleen algoritmos acreditados por el Centro Criptológico Nacional y preferentemente **productos certificados** en el caso de **entornos de nivel alto**.

Es necesario tener siempre en consideración, en las políticas y normativas de seguridad corporativa, los siguientes aspectos relativos al cifrado de datos en el correo electrónico:

- **Las cabeceras** de un correo electrónico, en términos generales, **no pueden ser cifradas**, por lo que un ataque de interceptación puede tener acceso a estos datos, que en ocasiones proporcionan información técnica significativa.
- En especial **el asunto** de un correo con información sensible **no debe proporcionar información significativa** del contenido, ya que este es un campo que no se cifrará habitualmente.
- Si ciframos un fichero adjunto con un programa que añada una extensión al nombre del fichero, un ataque de interceptación puede tener acceso a dicho nombre, por lo que debemos **utilizar nombres de archivo poco significativos** o incluso completamente asépticos: aa.doc, 123.xls…
- El uso de criptografía de clave privada no es aceptable para correspondencia electrónica habitual debido a las potenciales debilidades en la transmisión de la clave, por lo que debemos implantar y **utilizar** un esquema basado en **criptografía de clave pública**.
- **El cifrado** de los datos por sí mismo **no garantiza la autenticidad** del emisor si no va acompañado de firma digital, por lo que no debemos considerar válida cualquier información que nos llegue simplemente cifrada.

Correo No Corporativo

Es necesario que la política corporativa de uso del correo electrónico indique que el uso del correo con fines personales sea razonable, y por supuesto que no viole ninguno de los principios expuestos en dicha política.

Es mucho más peligroso el uso del **correo personal con fines profesionales**, con situaciones de:

- Uso malintencionado. Un usuario puede utilizar un servicio de correo externo a la organización, típicamente un webmail, para **robar datos corporativos**, por ejemplo enviando la información desde un correo externo a otro, también externo, fuera del control de la organización.
- Uso bienintencionado. Un usuario se envía información corporativa a sí mismo, utilizando como origen su cuenta de correo en la organización (escenario habitual) y como destino su cuenta de correo personal con una buena intención. Típicos ejemplos de esta situación se producen para poder trabajar en casa con informes, documentos, etc.

Es necesario **prohibir** expresamente en la Política de Seguridad corporativa el uso de **direcciones de correo personales para la gestión de información sensible**.

La organización debe **evaluar** la conveniencia de **denegar** técnicamente la conexión de la organización con los **webmails habituales** (Hotmail, GMail, etc.).

También es necesario evaluar la posibilidad de **monitorizar el tráfico** saliente por los protocolos habituales en el uso de webmails, típicamente HTTP y HTTPS.

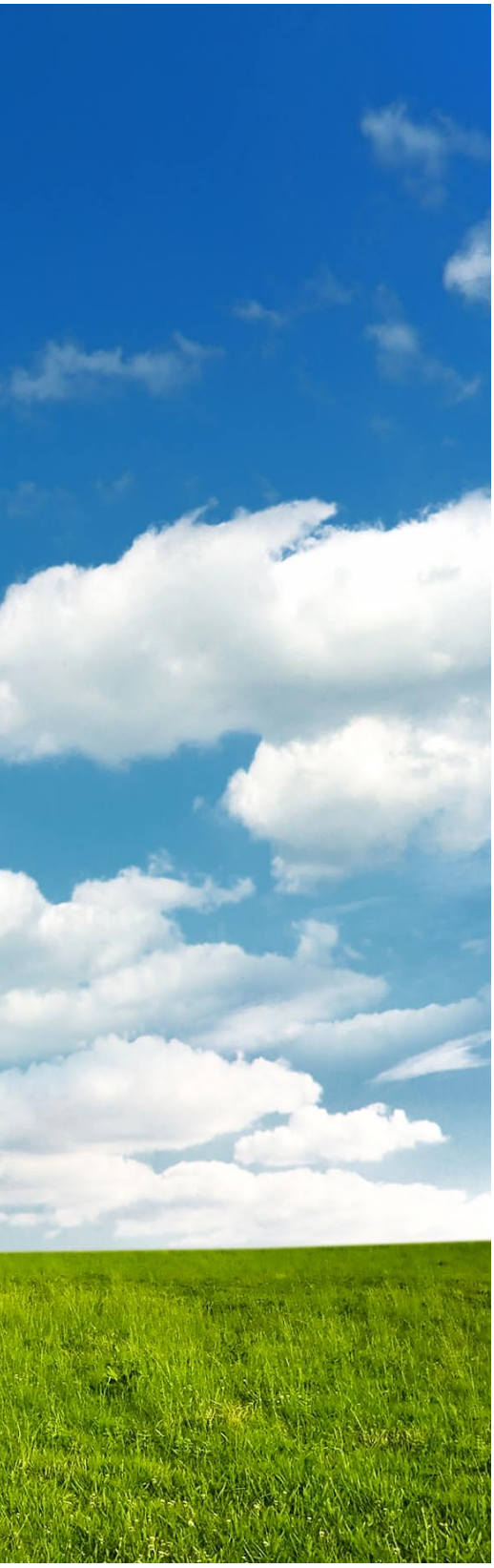
Técnicas antimalware y antispam

La organización debe considerar obligatorio, el uso de al menos **dos niveles de protección** frente a software dañino y antispam (servidor de correo y equipo de usuario) y, si es posible, el uso de productos de diferente fabricante en cada uno de estos puntos.

Es obligatorio que la organización conciencie a los usuarios en general sobre la importancia de su actitud a la hora de evitar ataques víricos.

En el caso de sistemas antispam, es obligatorio en todos los entornos la implantación de listas blancas para evitar la pérdida de mensajes.

Se debe proporcionar a sus usuarios **mecanismos de reporte de alertas o anomalías** que puedan suponer potenciales riesgos para la seguridad de la información corporativa, haciendo que estas alertas lleguen al personal de la organización con capacidad para mitigar dichos riesgos en un tiempo mínimo.



Aplicación del Esquema Nacional de Seguridad en el uso de Cloud Computing

La migración a entornos web ha sido un catalizador para la externalización de los sistemas de información de un amplio número de organizaciones. Como consecuencia de esta situación surge el modelo de *cloud computing* o computación en la nube, como una propuesta tecnológica capaz de ofrecer servicios a través de Internet de forma ágil y flexible.

Existen diversas modalidades de servicios en el ámbito *cloud computing*, tanto en lo referente al tipo de despliegue (privada, pública, comunitaria o híbrida) como en los modelos de servicio que se ofrecen (*Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) o Software-as-a-Service (SaaS)*).

Cabe destacar la posible **dependencia de terceros** en los servicios de *cloud computing*. La tendencia mayoritaria apunta hacia externalizar los servicios de computación en la nube a terceros delegando en ellos todas las tareas de mantenimiento, adquisición de sistemas, gestión de la capacidad, etc.

Si bien esto es considerado generalmente como una ventaja, debe tenerse en cuenta que esta opción **nunca debe conllevar una pérdida del control** de la información, o una despreocupación por la seguridad, debido a que la responsabilidad final siempre recae en el organismo contratante. A la hora de contratar estos servicios es fundamental estudiar adecuadamente las condiciones del servicio y las medidas de seguridad aplicadas.

En términos generales, en función del tipo de servicio contratado, conforme va incrementándose el nivel de abstracción (IaaS -> PaaS -> SaaS) disminuye el control que el cliente tiene sobre la infraestructura. Del mismo modo cuanto mayor control tiene la organización cliente sobre la infraestructura que proporciona el servicio, mayor nivel de seguridad y control puede aplicar sobre ésta y por tanto sobre la información tratada.

La adopción de este nuevo paradigma tecnológico introduce nuevos riesgos que es necesario controlar para poder prestar un servicio que garantice los requisitos exigibles por el ENS.

En el supuesto de que sea el organismo el propietario y administrador de la infraestructura sobre la que se despliegan los servicios *cloud computing*, la completa adecuación efectiva a la normativa vigente recae en dicho organismo, mientras que en el caso de estar la infraestructura operada por un tercero, éste deberá cumplir los requisitos establecidos en la normativa de seguridad que sea de aplicación en lo que respecta a prestadores de servicios, detallado más adelante en esta guía.

En cualquier caso, **la responsabilidad del cumplimiento del ENS** o de cualesquiera otras normas de aplicación, así como del correcto tratamiento de los datos en términos generales desde el punto de vista de su seguridad, **recaerá siempre sobre el organismo propietario de la información**.

Como referencia principal para identificar las medidas a tener en cuenta se seguirán los aspectos que son de aplicación en el ENS: la gestión de riesgos, la gestión de servicios externos, el cumplimiento de las medidas que sean de aplicación y otros requisitos legales como los provenientes de la LOPD.

A pesar de que las medidas definidas en gestión de servicios externos son solo de aplicación a los sistemas categorizados de nivel MEDIO o superior, la organización debe evaluar la conveniencia de su implantación en los sistemas categorizados de nivel básico.

Gestión de Riesgos en Cloud Computing

La utilización de servicios de *cloud computing*, en cualquiera de sus modalidades IaaS, PaaS o SaaS provistos por un tercero para soportar los sistemas de información de un organismo, introduce una serie de riesgos que deberán ser objeto de estudio pormenorizado. Al igual que cualquier cambio significativo sobre los sistemas de información, **previo a la contratación**, se deberá **revisar el análisis de riesgos** existente de la entidad.

Esta revisión deberá identificar las dependencias de los servicios que vayan a verse afectados por este cambio y las amenazas inherentes a la delegación del servicio en un tercero. A continuación se detallan las amenazas propias de los tipos de servicios de *cloud computing* y que están asociadas al proveedor y no al organismo contratante:

Amenaza / Tipo de Servicios	SaaS	PaaS	IaaS
(E.2) Errores del administrador del sistema/de la seguridad	√	√	
(E.3) Errores de monitorización	√	√	√
(E.4) Errores de configuración	√	√	
(E.15) Alteración de la información	√	√	√
(E.18) Destrucción de la información	√	√	√
(E.19) Fugas de información	√	√	√
(E.20) Vulnerabilidades de los programas	√	√	
(E.23) Errores de mantenimiento de los programas (software)	√	√	
(E.24) Caída del sistema por agotamiento de recursos	√	√	√
(A.3) Manipulación de los registros de actividad (log)	√	√	
(A.4) Manipulación de los ficheros de configuración	√	√	
(A.5) Suplantación de la identidad del usuario	√	√	√
(A.6) Abuso de privilegios de acceso	√	√	√
(A.11) Acceso no autorizado	√	√	√
(A.12) Análisis de tráfico	√	√	√
(A.13) Repudio (negación de actuaciones)	√	√	√
(A.14) Interceptación de información	√	√	√
(A.15) Modificación de la información	√	√	√
(A.18) Destrucción de la información	√	√	√
(A.19) Revelación de la información	√	√	√
(A.22) Manipulación de programas	√	√	
(A.24) Denegación de servicio	√	√	

Fig. 14. Riesgos en Cloud Computing

La organización deberá realizar una identificación de amenazas correcta que permita la ejecución de un análisis de riesgos o la revisión del ya existente, en función de la categoría del sistema o sistemas que se ubiquen en la nube.

Los riesgos residuales deben ser aceptados por la organización

La adopción del *cloud computing* dependerá de los niveles de riesgo residuales resultantes tras la aplicación de salvaguardas, los criterios de aceptación de riesgos existentes y la disposición de la Dirección para tomar las medidas adecuadas para reducir dicho nivel de riesgo.

Contratación y SLA en Cloud Computing

La primera medida a implantar del ENS es la relativa al proceso de "Contratación y acuerdos de nivel de servicio". Esta medida recoge la necesidad de establecer una serie de **requisitos contractuales** en la prestación del servicio, debiendo contemplar las características del servicio prestado y las responsabilidades de ambas partes.

Estos contratos deberán reflejar al menos los siguientes aspectos.

Descripción detallada

Una descripción detallada del servicio que incluya los acuerdos de nivel de servicio y todas las especificaciones del mismo. Por otra parte el contratante deberá reflejar la **categoría del sistema** que albergará en la nube en los requisitos facilitados al proveedor, de forma que éste conozca esta información y aplique las medidas de seguridad correspondientes en cada caso.

Tipo de Servicio

Las soluciones SaaS proporcionan un software como servicio, integrando una gran cantidad de funciones y herramientas. La implementación del ENS se delega en el proveedor, así como gran parte de las medidas de seguridad a implantar.

Las soluciones PaaS proporcionan entornos para desplegar aplicaciones desarrolladas. La organización cliente dispone de más control sobre el entorno y por tanto es responsable final de la seguridad de las aplicaciones.

Por último las soluciones IaaS proporcionan una infraestructura, por norma general virtualizada, en la que el cliente es responsable del software que esa infraestructura soportará, incluyendo los sistemas operativos y aplicaciones base. En este modelo la implementación de la seguridad de la información en su mayor parte es responsabilidad de la organización cliente, por lo que a priori puede considerarse el modelo de servicio *cloud* que mayor nivel de control proporciona a la organización.

Tipo de Infraestructura

La selección del tipo de infraestructura vendrá condicionado por la **categorización** de la información gestionada por el Sistema, en su parámetro de **confidencialidad**:

Infraestructura	N/A	Bajo	Medio	Alto
Nube pública	√	√		
Nube comunitaria externalizada	√	√	√	
Nube comunitaria interna	√	√	√	√
Nube privada externalizada	√	√	√	
Nube privada interna	√	√	√	√

Fig. 15. Infraestructuras Cloud vs Categoría del sistema

A la vista de esta tabla, es necesario hacer hincapié en que para sistemas cuyo parámetro de confidencialidad sea ALTO los únicos entornos *cloud* aceptables son los internos (nube privada o comunitaria, a determinar por cada organización).

Capacidad del Servicio

La capacidad del servicio deberá figurar expresamente en el acuerdo, así como las **medidas de penalización** a adoptar en el caso de que los parámetros de capacidad no se cumplan. Con independencia de la forma de medir la capacidad del servicio, es necesario especificar las condiciones bajo las que se podrá modificar la capacidad contratada, ya sea para aumentarla o reducirla, incluso en tiempo real según la demanda de cada momento. El *cloud provider* debe proporcionar herramientas u otros recursos que permitan a la organización contratante medir la capacidad del servicio y su rendimiento,

Confidencialidad

El proveedor debe comprometerse en el contrato a mantener la confidencialidad en el tratamiento de la información proporcionada por la organización cliente. Esto implica,

además del cumplimiento legal en materia de protección de datos, que el *cloud provider* debe comprometerse por escrito a **no divulgar o acceder indebidamente** a la información sin la autorización expresa de su propietario (la organización cliente), más allá de las necesidades que se requieran para ofrecer los servicios prestados.

Acuerdos de Nivel de Servicio

Se deben incluir los ANS (niveles, tiempos de respuesta, penalizaciones, etc.). Estos ANS deben ser aceptables para la organización cliente y deberán reflejar aspectos referentes a capacidad, disponibilidad, continuidad o gestión de incidencias, así como peticiones de cambio, entre otros, con al menos los siguientes criterios:

- **Capacidad**: se definirán desviaciones de carga que el proveedor deberá asumir.
- **Disponibilidad**: se establecerán porcentajes de disponibilidad del servicio en función de la criticidad del mismo.
- **Continuidad**: se definirán tiempos de recuperación para los sistemas de información en línea con los criterios de valoración de disponibilidad.
- **Peticiones de cambio e incidencias**: se definirán los tiempos de respuesta y resolución.
- Se definirá la periodicidad de los **informes de cumplimiento** de los SLA, así como las penalizaciones por incumplimiento de los mismos.

Modo de acceso al servicio

El acceso al servicio *cloud* se realizará siempre a través de entornos seguros, haciendo uso de protocolos que garanticen la confidencialidad de las comunicaciones. Para proteger la confidencialidad en sistemas de nivel MEDIO o ALTO se incorporará **cifrado de datos** para la información en tránsito.

Responsabilidades y obligaciones

Por parte del proveedor se deben considerar las siguientes responsabilidades mínimas:

- **Cumplir con las medidas de seguridad** requeridas y notificar todos los incidentes que pueden comprometer la seguridad del servicio o de la información de la organización cliente.
- Realizar la entrega de informes en la monitorización de servicios y **realizar auditorías** que demuestren el adecuado cumplimiento normativo.
- Garantizar el correcto funcionamiento de los servicios contratados cumpliendo con los niveles de servicio fijados en los SLAs.
- Mantener el principio de confidencialidad durante y tras la finalización de la relación contractual.

Por parte del cliente se considerarán las siguientes responsabilidades mínimas:

- **Designar representantes** del cliente con autoridad y capacitación para la toma de decisiones ante cambios.
- **Notificar las incidencias** y las peticiones de servicio al proveedor haciendo uso de los canales establecidos para tal fin.
- **Revisar** el cumplimiento de los **niveles de servicio** contratados y solicitar las auditorías realizadas por el proveedor.

Finalización del servicio

La finalización del servicio deberá estar **recogida en la descripción** del propio servicio, identificando la necesidad de que el proveedor elimine o devuelva la información a la finalización de la relación contractual y debiendo constar esto en una cláusula junto al tiempo que tardará el proveedor en realizar la destrucción o migración de los datos, definiendo así el periodo de tiempo para la ejecución de la migración o destrucción de la información tras la rescisión del contracto.

Requerimientos legales en la contratación en Cloud Computing

El servicio estará expuesto a determinados riesgos con potenciales implicaciones legales, como son los siguientes:

- Incumplimiento de SLA.
- Incumplimiento de acuerdo de confidencialidad.
- Incumplimiento de la legislación aplicable.

Requisitos para el cumplimiento del ENS

Los proveedores deberán cumplir lo estipulado en el apartado Servicios externos, de acuerdo lo establecido en el ENS. El Organismo solicitante deberá notificar al proveedor la categoría del sistema que va a albergar la nube, indicando tanto el nivel final del sistema como la categorización que se ha realizado de los parámetros DICAT.

El proveedor de servicios deberá **garantizar el cumplimiento de las medidas** que son de aplicación a dicho sistema. El cumplimiento de estas medidas deberá ser reflejado en el contrato o pliego de condiciones suscrito entre ambas entidades. La organización deberá evaluar la conveniencia de disponer del **derecho de auditoría**, con la profundidad correspondiente, sobre el proveedor de servicios o de solicitar a éste la siguiente documentación siempre que lo considere necesario:

- Una Declaración de Aplicabilidad de las medidas a aplicar.
- Una auditoría que verifique mediante evidencias el cumplimiento de las medidas.

En ocasiones los proveedores de servicios *cloud* disponen de Sistemas de Gestión de Seguridad de la Información certificados de acuerdo con referentes internacionales, como la norma **ISO 27001**, cuyo alcance incluye los servicios de *cloud computing*; aunque la organización cliente debe evaluar en cada caso la conveniencia de que sus proveedores dispongan de estas acreditaciones, es necesario recordar que disponer de éstas **NO garantiza** en ningún momento **el cumplimiento del ENS** por parte del proveedor.

Análisis de riesgos

El *cloud provider* deberá disponer de un análisis de riesgos realizado siguiendo una metodología reconocida internacionalmente cuyo alcance incluya los servicios objeto de la prestación. El *cloud provider* deberá **aportar evidencia** de la existencia de dicho análisis de riesgos actualizado, así como de una correcta gestión de los riesgos resultantes.

Gestión del personal

Además de las funciones y obligaciones que se deberán establecer entre cliente y **proveedor**, este último deberá designar un **Responsable de Seguridad** de la organización que haga las funciones de interlocutor directo con el Responsable de Seguridad del organismo cliente. Del mismo modo se deberá garantizar que todo el personal participante en la provisión del servicio mantenga la confidencialidad de la información tratada tanto de forma directa durante la prestación del servicio como a la finalización de éste.

Autorización y control de acceso

El acceso a la información en plataforma *cloud* debe limitarse en todo momento al personal debidamente autorizado y se realizará siempre bajo la premisa del ***need to know***. Para ello la plataforma *cloud* puesta a disposición del cliente deberá contar con controles de acceso lógico que contemplen: identificadores únicos de usuario, mecanismos de autenticación de acuerdo con el nivel de seguridad del sistema y limitación de acceso a recursos por parte de usuarios de acuerdo con las funciones asignadas al usuario.

Protección de las instalaciones

Se deberá solicitar al proveedor información referente a las medidas de seguridad implantadas en el Centro de Proceso de Datos para confirmar que son acordes a los requisitos de seguridad de la organización cliente.

Seguridad por defecto

Deberá realizarse un **bastionado de los sistemas** de información de manera que se implemente una configuración segura por defecto:

- Se limitarán todas las funcionalidades técnicas de los sistemas que no sean requeridas.
- Se limitará el acceso a la administración y al registro de actividad únicamente al personal autorizado.
- Se inhabilitarán cuentas de usuario innecesarias.
- Se establecerán bloqueos de sesión por tiempo de inactividad.
- Se establecerá un límite de número de intentos de acceso fallidos.
- La organización solicitará al proveedor de servicios la documentación que defina el proceso de bastionado.

Integridad del sistema

El *cloud provider* deberá garantizar que se identifican y gestionan las vulnerabilidades de la infraestructura que da soporte a los servicios de *cloud*, llevando a cabo las actualizaciones pertinentes. Para ello deberá disponer de un procedimiento de gestión de parches y vulnerabilidades definido, implantado y auditado sobre los sistemas que darán servicio a la organización. Este procedimiento o las **evidencias de cumplimiento** deberá ser facilitado a la organización.

Gestión de Cambios

La Gestión de Cambios es una medida exigible para todos los sistemas que sean categorizados con un **nivel MEDIO o superior**, aunque la organización debe evaluar la conveniencia de implementar la medida en los sistemas de nivel básico. El *cloud provider* deberá informar a la organización cliente de, al menos, los siguientes aspectos:

- Notificación de los cambios que puedan afectar al servicio.
- Procedimiento de solicitud de cambios.
- Proceso de autorización de cambios.
- Asignación de responsabilidades referentes a cambios.
- Tareas de mantenimiento y actualización de recursos.

Información almacenada y en tránsito

Para garantizar la confidencialidad y la integridad de la información albergada en la nube, se deberán implantar medidas de cifrado tanto por parte del proveedor de *cloud computing* como por parte del cliente. El **cifrado** deberá realizarse en los sistemas de información donde se ubica la **información**, en el **tránsito** de esta información y en los soportes empleados para el **respaldo** de la misma. El cifrado de la información solo es de aplicación a los sistemas cuya confidencialidad haya sido clasificada de nivel ALTO, mientras que las restantes medidas son de aplicación a sistemas categorizados de nivel MEDIO.

En cuanto al cifrado de las comunicaciones, se deberá garantizar en todo momento la confidencialidad de las mismas.

Otros sistemas interconectados

Los servicios prestados por un *cloud provider* externo a la organización hacen habitualmente uso de redes públicas. El proveedor deberá dar garantías de que la infraestructura está debidamente protegida frente a accesos indebidos o potenciales ataques externos. Como evidencia de que se ha definido un perímetro seguro se solicitará al proveedor el documento que defina la arquitectura de seguridad o un esquema que resuma los dispositivos (cortafuegos, IPS, IDS, WAF, etc.) para proteger la infraestructura donde se hospedarán los datos de la organización cliente.

Registro de actividad

Los sistemas proporcionados por el *cloud provider* deberán disponer de registros de acceso que permitan **monitorizar, analizar, investigar y documentar acciones indebidas o no autorizadas,** tanto a nivel operativo como de administración. Dentro del seguimiento y monitorización que el proveedor deberá entregar a la organización, se proporcionará un registro de los accesos realizados a las plataformas puestas a disposición del cliente.

Gestión de incidencias

El proveedor deberá disponer de un procedimiento de gestión de incidencias. Se deberá informar a la organización cliente de:

- Procedimiento de **notificación de incidencias**.
- **Tipología** de incidencias incluidas en el servicio.
- Procedimientos específicos ante **incidentes de seguridad**.
- **Tiempos de respuesta** y resolución de incidencias/incidentes.
- Mantenimiento y gestión del **registro de incidencias**.

Procedimiento de borrado de información

Los sistemas sobre los que se aplique esta regulación deberán disponer de medidas para el borrado y destrucción de soportes de información con independencia de un servicio *cloud* o prestado de forma convencional. En entornos *cloud* la compartición de recursos puede implicar que la información que los sistemas han albergado llegue a ser comprometida, por lo que deberán llevarse a cabo procedimientos de borrado seguro siempre que se realice una modificación sustancial o terminación contractual. Esta medida es exigible para todos los sistemas cuya confidencialidad haya sido categorizada con un **nivel MEDIO o superior**, y el proveedor deberá informar a la organización cliente de: procedimiento de borrado seguro, notificación y certificación de borrados acometidos.

Respaldo y recuperación de datos

En línea con lo especificado por el ENS y por el RD LOPD, el proveedor deberá disponer de un **procedimiento de copias de respaldo** que garantice la restauración de la información. Esta medida es exigible para todos los sistemas, y el proveedor deberá informar a la organización cliente de: alcance de los respaldos, política de copias de seguridad, medidas de cifrado de información en respaldo, procedimiento de solicitud de restauraciones de respaldo, realización de pruebas de restauración y traslado de copias de seguridad (si aplica).

Continuidad del servicio

Se deberá solicitar al proveedor **evidencia de la existencia de un plan de continuidad** de negocio que garantice la restauración de los servicios. Esta medida es exigible para todos los sistemas cuya disponibilidad haya sido categorizada con un nivel ALTO, y el proveedor deberá informar a la organización cliente de: existencia de plan de continuidad de negocio y evidencia satisfactoria de la ejecución periódica de pruebas de continuidad. Se deberá disponer de medios para aprovisionar el servicio en caso de caída del mismo. Esta medida es aplicable para todos los sistemas cuya disponibilidad haya sido categorizada con nivel ALTO, aunque la organización debe evaluar la conveniencia de su aplicación a los sistemas categorizados de nivel MEDIO. Se deberá requerir al proveedor evidencia de la existencia de un plan de continuidad de negocio cuyo alcance incluya los servicios objeto de la prestación.

En caso de que el proveedor disponga de un Sistema de Gestión de la Continuidad de Negocio basado en las normas ISO 22301, BS25999 o UNE 71599 cuyo alcance incluya la prestación de servicios en modalidad *cloud* y a su vez se encuentre certificado, la organización debe evaluar si considera esta certificación una prueba suficiente de que los planes de continuidad definidos se someten a pruebas periódicas. En caso contrario se solicitará al proveedor evidencia de la realización de estas pruebas periódicas.

Seguimiento del Servicio de Cloud Computing

En los servicios prestados por terceros a la organización, tan importante es el acuerdo contractual con el proveedor de servicios como el seguimiento a realizar sobre el servicio prestado. Para poder tener el control de los servicios, y por tanto también poder exigirle al proveedor el cumplimiento de las medidas de seguridad aplicables, es necesaria una monitorización de los mismos.

Este punto especifica tres aspectos principales a seguir:

- **La medición del cumplimiento del servicio** y el procedimiento para restaurar las desviaciones estipuladas contractualmente.
- El proceso de coordinación para el **mantenimiento de los sistemas** implicados.
- El proceso de **coordinación ante incidencias** o desastres.

La organización debe monitorizar de forma independiente el cumplimiento de los términos establecidos en el contrato, bien a través de controles técnicos propios o a través de la revisión y aprobación periódica de los informes de servicio proporcionados por el *cloud provider*.

Consideraciones del servicio de correo electrónico en plataformas de *Cloud Computing*

Cuando se utilice el correo electrónico como servicio interno, que es la mayor parte de situaciones en las Administraciones Públicas, deberá requerirse el cumplimiento del ENS en función de los niveles de confidencialidad y trazabilidad que requiera la información tratada por la entidad y los servicios prestados que hagan uso de este servicio interno, eligiendo el tipo de despliegue y de servicio de acuerdo con lo recogido a continuación.

Respecto al tipo de despliegue y en función del nivel de confidencialidad de la información tratada en el sistema:

- Para nivel bajo, podrá estar ubicada en cualquier tipo de nube.
- Para nivel medio, no podrá ubicarse en una nube pública.
- Para nivel alto, deberá ubicarse en nubes internas ya sean comunitarias o privadas.

Además, en función del tipo de servicio:

- Si es SaaS, se deberá exigir al proveedor, que el software cumpla las medidas de seguridad requeridas por el ENS referentes a confidencialidad y trazabilidad aplicables de acuerdo con los niveles de los sistemas de información del contratante.
- Si es PaaS o IaaS, la entidad será la encargada de configurar o implantar las medidas de seguridad requeridas por el ENS aplicables en función nivel de confidencialidad y trazabilidad de los sistemas de información propios.

Dada la particular casuística del correo electrónico corporativo, en el que por la diversidad de la información tratada (transmitida, almacenada...) no es fácil identificar unívocamente el nivel de confidencialidad de dicha información, se deberá considerar ésta en su conjunto como la de mayor nivel de confidencialidad que se gestione a través del correo electrónico (esto implicará nivel ALTO en la mayor parte de situaciones), por lo que se deben aplicar las salvaguardas correspondientes a este nivel, en concreto en lo relativo a la ubicación en nubes internas a la organización.

Fig. 16. Correo electrónico en Cloud Computing

Herramientas de Seguridad

El Esquema Nacional de Seguridad establece una serie de requisitos para cuyo cumplimento resulta de gran importancia contar con las herramientas adecuadas.

Las herramientas de seguridad pueden describirse como el conjunto de **hardware o software** que proporcionan servicios orientados a reforzar y dar soporte a la seguridad de los sistemas.

El Esquema Nacional de Seguridad indica la tipología de herramientas a usar en la interconexión de sistemas en función de la clasificación de los mismos.

El **Responsable de Seguridad**, **determinará** el alcance de **su aplicación**, considerando la Política de Seguridad de la Organización y los requisitos de obligado cumplimiento definidos por el Esquema Nacional de Seguridad.

Las herramientas de seguridad deben implementar funcionalidades que permitan facilitar y reforzar al menos los siguientes aspectos:

- Identificación y autenticación.
- Control de acceso (protección de datos de usuario en terminología Common Criteria).
- Registro de los eventos y auditoría.
- Integridad.
- Disponibilidad.
- Gestión de la configuración.
- Gestión de la seguridad.
- Garantía.

Dada la naturaleza de su funcionalidad, las herramientas de seguridad pueden constituirse en **punto de acceso a información de carácter sensible**, es por ello que deben cumplir los siguientes requisitos:

- **Control de acceso** a la información/ recursos granular y basado en perfiles: de manera que cada usuario sólo pueda acceder a aquellos que esté autorizado y siempre con el nivel de acceso adecuado, para aquellas herramientas que sean utilizadas por varios usuarios.
- **Explotación de la información**: las herramientas dispondrán de la capacidad de elaborar informes en múltiples formatos y en base a distintos criterios, los cuales permitirán facilitar la correcta interpretación de la información y su posterior tratamiento.
- **Trazabilidad**: las herramientas deben generar registros (logs) de su actividad y la de sus usuarios, de manera que pueda identificarse de manera inequívoca las acciones de los mismos.

Las herramientas de seguridad pueden agruparse en las siguientes áreas principales de actividad:

- **Gestión de la seguridad**: utilizadas habitualmente para labores de certificación y acreditación, de análisis y gestión de riesgos, análisis de vulnerabilidades, inspecciones periódicas o respuesta a incidentes.
- **Administración de la seguridad del Sistema:** cubrirán aspectos como comprobaciones de integridad de sistemas de ficheros, filtrado o supervisión de recursos, revisión automática de logs y comprobaciones de configuración.

Y suelen clasificarse como:

- **Auditoría**.
- **Protección**.
- **Detección**.
- **Reacción**.

La tecnología en general y de manera especialmente acentuada en lo referente a la seguridad, evoluciona a gran velocidad, por lo que la clasificación dada pretende ser más una guía de referencia que una foto exacta del estado del arte actual.

Selección, Control de la Configuración y Operación

Selección y contratación

Es condición indispensable que las herramientas de seguridad que se utilicen sean **aprobadas por el Responsable de Seguridad** y cumplan la Política de Seguridad TIC de la Organización.

Se valorará positivamente, como garantía, que las herramientas de seguridad dispongan, o estén en proceso de hacerlo, de certificaciones según Criterios Comunes (Common Criteria, CC) o equivalente (ITSEC, TCSEC, etc.). En cualquier caso, el nivel de certificación mínimo dependerá del resultado del análisis de riesgos que se lleve a cabo y de la categoría del sistema conforme al ENS.

La aprobación de una herramienta de seguridad por parte de la Autoridad correspondiente para un sistema de nivel de protección Alto, cuando no esté certificada o en proceso de certificación, debería basarse en un Plan de Evaluación y Pruebas de Seguridad.

La autorización de uso dependerá de la criticidad del Sistema y de la ausencia de herramientas con este tipo de certificación en el mercado.

En la planificación y adquisición se debe tener en cuenta al menos lo siguiente:

- Los Pliegos de Prescripciones Técnicas (PPT) deben contemplar los requisitos obligatorios definidos en esta guía para las herramientas de seguridad.
- Los PPT deben especificar de manera detallada los requisitos hardware y software de las herramientas de seguridad correspondientes.
- Los recursos adicionales que se consideren necesarios para la adecuada explotación de las herramientas de seguridad, deben estar reflejados y tenidos en cuenta.

Control de la Configuración

El control de la configuración de las herramientas de seguridad debe realizarse conforme a los procedimientos de control de la configuración aplicables a los Sistemas de Producción, los cuales a su vez dependerán de la categoría asignada a los mismos conforme a los criterios del ENS.

A la hora de aplicar cambios en la configuración, requeridos por actualizaciones del proveedor, deberemos tener en cuenta la necesidad o no de nuevas funcionalidades y, en cualquier caso, **debe acordarse con el Responsable de Seguridad la idoneidad del cambio**.

Operación

Las herramientas de seguridad deben ser operadas conforme a los procedimientos definidos en la documentación de seguridad aprobada para el sistema. Como mínimo deberían cubrir los siguientes aspectos:

- Configuración y gestión de la herramienta: roles y perfiles a implementar, a fin de garantizar que los usuarios tienen el nivel de acceso adecuado.
- Análisis y protección de datos: cómo manejar los datos que se obtengan a partir de la operación de la herramienta.
- Definición de operación básica, la cual debe cubrir la mayor parte del día a día de la operación de la herramienta.
- Gestión de incidentes derivados del uso de la herramienta.

En el caso de herramientas capaces de explotar vulnerabilidades del sistema, solo podrán ser utilizadas por **personal autorizado**.

Criterios para el empleo de herramientas de seguridad según la clasificación del sistema

Tipo de herramienta	Nivel	Herramientas	Categoría		
			Baja	Media	Alta
Auditoría	Red	Escáner de Red	N.A	N.A	Aplica
	Sistema	Revisión de la configuración	N.A.	Aplica	Aplica
		Revisión de consumo de recursos	N.A.	Aplica	Aplica
	Usuario	Auditoría de contraseñas	Aplica	Aplica	Aplica
	Aplicación	Control y calidad en el desarrollo	Aplica	Aplica	Aplica
		Auditoría de código	Aplica	Aplica	Aplica
		Análisis de metadatos	Aplica	Aplica	Aplica
	Multinivel	Análisis de vulnerabilidades	N.A.	N.A.	Aplica
Protección	Red	Dispositivos de protección perimetral	Aplica	Aplica	Aplica
		Detección y prevención de intrusiones	Aplica	Aplica	Aplica
		Gestión de red	Aplica	Aplica	Aplica
	Sistema	Configuraciones de seguridad	Aplica	Aplica	Aplica
		Herramientas de actualizaciones	Aplica	Aplica	Aplica
		Detección y prevención de intrusiones	Aplica	Aplica	Aplica
	Usuario	Contraseñas	Aplica	Aplica	Aplica
		Antivirus	Aplica	Aplica	Aplica
		Filtros Antispam	Aplica	Aplica	Aplica
		Cifrado	Aplica	Aplica	Aplica
		Borrado Seguro	Aplica	Aplica	Aplica
	Aplicación	Cortafuegos de aplicación	N.A.	Aplica	Aplica
		Limpieza de metadatos	N.A.	Aplica	Aplica
Detección	Red	Captura, monitorización y análisis de tráfico	N.A.	Recomendado	Aplica
		Monitorización y supervisión de dispositivos de red	N.A.	Recomendado	Aplica
	Multinivel	Monitorización y análisis de registros del sistema	N.A.	Recomendado	Aplica
Reacción	Multinivel	Análisis forense	N.A.	Aplica	Aplica
		Análisis de código dañino	N.A.	Aplica	Aplica
		Gestión de incidencias	N.A.	Aplica	Aplica
	Datos	Backup	Recomendado	Aplica	Aplica

Fig. 17. Herramientas de seguridad vs clasificación del sistema

En los documentos técnicos del CCN (CCN-STIC-818) se pueden encontrar una descripción detallada del objetivo de cada tipo de herramienta, así como las principales y más significativas referencias de productos de mercado para cada grupo.

El proceso de auditoría en el ámbito del Esquema Nacional de Seguridad

Los sistemas de información deberán ser objeto de una **auditoría regular ordinaria**, al menos cada dos años (para los sistemas de categoría media y alta), que verifique el cumplimiento de los requerimientos del ENS. Se deberán realizar **auditorías de carácter extraordinario**, cuando se produzcan modificaciones al sistema.

El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del ENS, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias necesarias, así como las recomendaciones que se consideren oportunas. El objeto de la auditoría será emitir una opinión independiente y objetiva sobre este cumplimiento de tal forma que permita a los responsables correspondientes, tomar las medidas oportunas para subsanar las deficiencias identificadas.

El objetivo de la auditoría es calibrar la capacidad del sistema para garantizar la integridad, disponibilidad, autenticidad, confidencialidad y trazabilidad de los servicios prestados y la información tratada, almacenada o transmitida.

Los informes de auditoría **serán presentados al Responsable del Sistema y al Responsable de Seguridad** competentes, para que tomen las medidas oportunas.

La auditoría se realizará en los siguientes términos:

- Que la política de seguridad define los roles y funciones, los servicios, los activos y la seguridad del sistema de información.
- Que existen procedimientos para resolución de conflictos entre dichos responsables.
- Que se han designado personas para dichos roles bajo el principio de «separación de funciones».
- Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- Que se cumplen las actividades de protección descritas en el ENS sobre Medidas de Seguridad.
- Que existe un sistema de gestión de la seguridad de la información, documentado y aprobación por la dirección.

La auditoría **requiere la existencia de evidencias** que permitan sustentar cumplimiento de los puntos indicados, con documentación de los procedimientos, registro de incidencias y examen del personal afectado en conocimiento y ejecución de las medidas que le afectan.

En función de la categoría del sistema los requisitos de auditoría son diferentes.

- Los sistemas de **categoría BÁSICA** no necesitarán realizar una auditoría. Bastará una **autoevaluación interna**. El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada con sus evidencias. Se entregará al Responsable de Seguridad.
- En sistemas de **categoría MEDIA o ALTA,** el **informe de auditoría** identificará las deficiencias y sugerirá las posibles medidas correctoras o complementarias que sean necesarias, así como las recomendaciones que se consideren oportunas. Los informes de auditoría serán analizados por el Responsable de Seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

Estándares metodológicos en el proceso de auditoría

El proceso de auditoría de la seguridad, acorde a los requerimientos de ENS, requiere que se realice de una forma metodológica que permita identificar claramente los apartados definidos a continuación.

Alcance y objetivo de la auditoría

El Alcance y Objetivo de la Auditoría deben estar claramente **definidos, documentados y consensuados** entre el equipo auditor y el órgano de las Administraciones Públicas.

Considerando que las redes de comunicaciones y sistemas de la administración pública, tienen interconexiones con entidades publicas y privadas, la descripción detallada del alcance de la auditoría y establecer claramente el límite hasta dónde se audita es esencial.

Es imprescindible que se defina, preliminarmente, si existe alguna información que, por indicación del Responsable del Sistema, del Servicio o del de Seguridad, no estará accesible a los auditores, y ni siquiera al Jefe del equipo de auditoría, debiendo éste evaluar si es una limitación para realizar la auditoría. Si es así, y se decide continuar con el proceso de auditoría, esta limitación debe reflejarse en el Informe. Las tareas de auditoría no incluirán en ningún caso la ejecución de acciones que puedan ser consideradas como responsabilidades de consultoría o similares.

Recursos necesarios

El **equipo auditor** deberá estar compuesto por un equipo de profesionales (Jefe del equipo de auditoría, auditores, y expertos, tanto internos como externos) que garantice que se dispone de los **conocimientos suficientes** para asegurar la adecuada y ajustada realización de la auditoría.

Si el equipo de auditoría es interno, éste deberá ser totalmente independiente de la organización, sistemas o servicios que sean o puedan ser objeto de la auditoría. Si participan auditores internos y externos, se debe establecer qué equipo es responsable de la supervisión y realización de la auditoría, y de la emisión del informe, y consecuentemente, de los resultados de la auditoría.

Planificación y requisitos de información

Para la realización de la auditoría es necesario realizar una planificación preliminar que, fundamentalmente, consiste en establecer los **requisitos de información y documentación** necesarios e imprescindibles para:

- Establecer y desarrollar el programa de auditoría.
- Concretar los conocimientos necesarios del equipo de auditoría.
- Definir la agenda de revisiones, reuniones y entrevistas.
- Definir las revisiones y pruebas a realizar.
- Adjudicar las tareas a los componentes del equipo de auditores y expertos.

La documentación mínima a requerir para concretar la planificación en detalle de la auditoría del cumplimiento, es entre otras:

- Documentos firmados por el órgano superior correspondiente que muestren el conocimiento y la aprobación formal de las decisiones en materia de **política de seguridad**.
- **Organigrama** de los servicios o áreas afectadas, con descripción de funciones y responsabilidades. Identificación de los responsables: de la información, de los servicios, de la seguridad y del sistema.
- **Descripción** detallada **del sistema de información** a auditar e identificación de

la categoría del sistema.

- Niveles de seguridad definidos.
- La **Política de Seguridad**, de Firma electrónica y certificados (si se emplean estas tecnologías), **y la normativa de seguridad**.
- Descripción detallada del sistema de gestión de la seguridad y la documentación que lo sustancia.
- Informes de **análisis de riesgos y la Declaración de Aplicabilidad**, junto con las decisiones adoptadas para gestionar los riesgos.
- Relación de las **medidas de seguridad implantadas** y su registro.
- Informes de otras **auditorías previas**.
- Lista de **proveedores externos** que entran dentro del alcance de la auditoría, y evidencias del control realizado sobre estos servicios.

Programa detallado

Cada entorno a auditar será diferente y con sus propias configuraciones y estructura organizativa, por lo tanto, es necesario tenerlas en cuenta a la hora de:

- diseñar las revisiones y pruebas de auditoría,
- definir en qué consistirá cada una de ellas, y
- establecer los recursos necesarios (del equipo de auditoría y de los servicios auditados).

Los elementos a incluir en la planificación de la auditoría, como elementos mínimos a considerar son los siguientes:

- Análisis y Gestión de riesgos.
- El marco organizativo y la segregación de funciones.
- El marco operacional (Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, y Monitorización del Sistema).
- La Declaración de Aplicabilidad que recoge las medidas de seguridad que son relevantes para el sistema de información sujeto a la auditoría.
- Los procesos de mejora continua de la seguridad.

Para definir la tipología de pruebas a realizar (verificación de las medidas de seguridad), el equipo auditor puede utilizar guías, y cuestionarios de auditoría disponibles en asociaciones y colectivos de auditores, y las guías STIC proporcionadas por el CCN.

Presentación de resultados

La presentación, de los resultados individuales de las pruebas, a las personas involucradas con estos resultados, para su confirmación sin valoraciones con respecto a los resultados finales.

El objetivo principal de la presentación de los resultados de las revisiones y pruebas, antes de la emisión del informe de auditoría, es **confirmar los hechos y las situaciones detectadas** o identificadas como resultado de las pruebas y revisiones realizadas. Es fundamental para la eficacia del informe de auditoría posterior, al confirmar que los resultados, de las revisiones y las pruebas, son ciertos.

Evaluación global e Informe de Auditoría

Una vez confirmados los hechos y deficiencias resultados de las revisiones y pruebas de auditoría se realizará la evaluación global de los resultados de la auditoría en relación al objetivo y alcance definidos y a los requisitos del ENS y se ejecutará la confección, presentación y emisión formal del Informe de Auditoría. Este informe

deberá presentarse al **Responsable del Sistema y al Responsable de Seguridad**.

Los informes de auditoría serán analizados por el Responsable de Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.

El equipo auditor no entregará ni concederá acceso al informe de auditoría a terceros distintos de los indicados en el párrafo anterior, salvo por imperativo legal o mandato judicial.

El informe de auditoría deberá dictaminar sobre la adecuación de las medidas exigidas por el ENS, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. El informe incluirá una opinión sobre si:

- La Política de Seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- Existen procedimientos para la resolución de conflictos entre dichos responsables.
- Se han designado personas para dichos roles a la luz del principio de "separación de funciones".
- Existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.
- Se ha realizado un análisis de riesgos, con revisión y aprobación regular, según lo establecido en las medidas aplicables del Anexo II del RD 3/2010.
- Se cumplen las medidas de seguridad descritas en el Anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- Existe un sistema de gestión de mejora continua.

Si la auditoría se realizara conjuntamente con la requerida por el RD 1720/2007, es necesario que el informe indique con claridad cuando una deficiencia de seguridad o incumplimiento, o una mejora recomendada está, individualmente, relacionada con ambas normas, o bien con una en concreto.

Deberá entregarse en soporte papel y debidamente firmado, o bien en soporte electrónico con firma electrónica. **Las recomendaciones en ningún caso deberán ser cerradas, sino sugerencias** de las distintas alternativas posibles, cuando sea aplicable, a considerar por los responsables de seguridad. Las recomendaciones estarán siempre basadas en la existencia de un riesgo y sustentadas debidamente, o bien relacionadas con un incumplimiento.

Informe Ejecutivo

Se incluirá un **informe ejecutivo** en el que no incluirán términos o acrónimos informáticos, ya que el informe podrá ser leído por directores y gerentes, o terceros, que no tengan el conocimiento informático adecuado. Tampoco se deberán incluir nombres de personas concretas, solo funciones o puestos desempeñados.

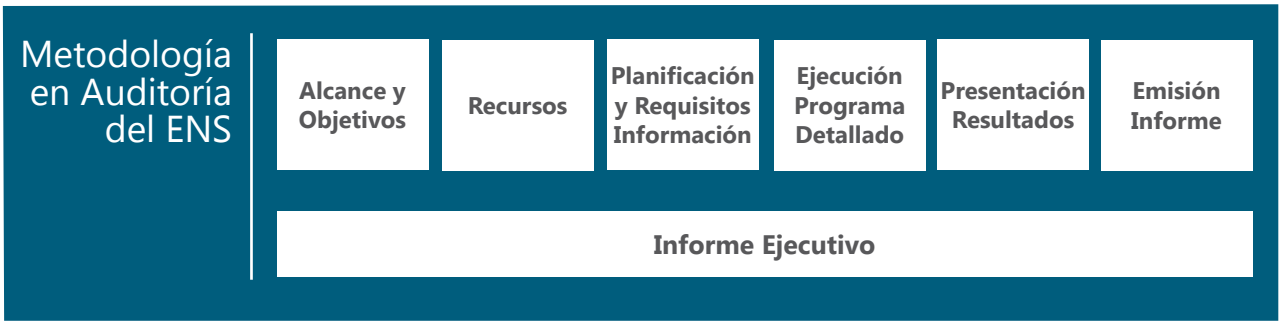


Fig. 18. Metodología de Auditoría del ENS

Guías CCN-STIC y relación del ENS con otras normas

El art. 29 del ENS señala la utilidad de las Guías CCN-STIC. En concreto, dice: "Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones."

No se trata, por tanto, de normas imperativas, sino de la expresión de metodologías y recomendaciones para el adecuado cumplimiento de lo dispuesto en el ENS. Recomendaciones que tendrán especial significación para aquel organismo administrativo afectado por un incidente grave de seguridad, motivado por la inobservancia de las recomendaciones descritas.

El CCN mantiene el repositorio de Guías STIC, permanentemente actualizado, en el siguiente enlace: **https://www.ccn-cert.cni.es/**. Las relativas al Esquema Nacional de Seguridad, identificadas como la serie 800 son actualmente:

- **CCN-STIC-800 Glosario de términos y abreviaturas del ENS**. Recoge aquellos términos y abreviaturas utilizados en las guías de desarrollo del ENS.
- **CCN-STIC-801 Responsabilidades y Funciones en el ENS**. El objeto de esta guía es crear un marco de referencia que establezca las responsabilidades generales en la gestión de la seguridad de los Sistemas, así como proponer las figuras o roles de seguridad que las implementen.
- **CCN-STIC-802 Auditoría del Esquema Nacional de Seguridad**. El objeto de esta guía es describir las premisas, objetivos y métodos a desarrollar a la hora de realizar las auditorías de seguridad del sistema.
- **CCN-STIC-803 Valoración de Sistemas en el ENS**. El Esquema Nacional de Seguridad establece una serie de medidas de protección en su Anexo II que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares.
- **CCN-STIC-804 Medidas de Implantación del ENS**. El Esquema Nacional de Seguridad establece una serie de medidas de seguridad en su Anexo II que están condicionadas a la valoración del nivel de seguridad en cada dimensión, y a la categoría (artículo 43) del sistema de información de que se trate.
- **CCN-STIC-805 Política de Seguridad de la Información**. La Política de Seguridad de la Información es un documento de alto nivel que define lo que significa seguridad de la información en una organización. El documento debe estar accesible por todos los miembros de la organización y redactado de forma sencilla, precisa y comprensible.
- **CCN-STIC-806 Plan de Adecuación del ENS**. Los sistemas existentes a la entrada en vigor del RD 3/2010, de 8 de enero, deberán adecuarse al Esquema Nacional de Seguridad de forma que permitan el cumplimiento de lo establecido en la disposición final tercera de la Ley 11/2007, de 22 de junio. Esta guía establece unas pautas de carácter general que son aplicables a entidades de distinta naturaleza, dimensión y sensibilidad sin entrar en casuísticas particulares.

- **CCN-STIC-807 Criptología de Empleo en el ENS**. Esta guía desarrolla las recomendaciones sobre algoritmos y parámetros criptológicos recogidas en el Esquema Nacional de Seguridad.
- **CCN-STIC-808 Verificación del Cumplimiento de las Medidas en el ENS**. El objeto de esta guía es que sirva tanto de itinerario, como de registro, a aquella persona designada como auditor de los requisitos del Esquema Nacional de Seguridad para un sistema.
- **CCN-STIC-809 Declaración de conformidad del ENS**. La presente guía tiene por objeto dar pautas generales para redacción de la declaración de conformidad al ENS, sin perjuicio de la particularización de cada organismo.
- **CCN-STIC-810 Guía de Creación de CERT,s**. Esta guía forma parte del desarrollo del RD 3/2010 del ENS, según se alude en el artículo 37 sobre prestación de servicios de respuesta a incidentes de seguridad en las Administraciones Públicas, y específicamente, en su punto número 2 sobre el programa desarrollado por el CCN para que las Administraciones Públicas puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad.
- **CCN-STIC-811 Interconexión en el ENS**. El Esquema Nacional de Seguridad, en su artículo 22, establece la obligatoriedad de proteger el perímetro de los sistemas a interconectar, (en particular si se utilizan redes públicas total o parcialmente) y de analizar los riesgos derivados de la interconexión de los sistemas, controlando además su punto de unión.
- **CCN-STIC-812 Seguridad en Servicios Web en el ENS**. Guía de referencia en la identificación y el análisis de los requisitos de seguridad asociados a las aplicaciones y entornos Web en el ámbito del Esquema Nacional de Seguridad, con el objetivo de reducir las posibles amenazas de seguridad asociadas a estos entornos y aplicaciones durante su diseño y antes de su paso a producción.
- **CCN-STIC-813 Componentes Certificados en el ENS**. Esta guía introduce los conceptos y define los criterios específicos que deben guiar y ayudar en la aplicación de los requisitos de adquisición y uso de componentes certificados en el Esquema Nacional de Seguridad.
- **CCN-STIC-814 Seguridad en Servicio de Correo en el ENS**. Guía de configuración segura del correo electrónico en el ámbito del Esquema Nacional de Seguridad, con el objetivo de reducir las posibles amenazas de seguridad asociadas a estos entornos.
- **CCN-STIC-815 Indicadores y Métricas en el ENS**. Esta guía persigue proponer un conjunto de datos a registrar del sistema de información a fin de poder derivar métricas posteriormente, tanto locales del sistema, como del conjunto de la Administración; un conjunto amplio de métricas o indicadores para caracterizar los puntos del Anexo II del ENS; un conjunto reducido de métricas o indicadores para caracterizar la posición del sistema de información en materia de seguridad de la información y cuadros de mando para escenarios típicos.
- **CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS** . En desarrollo.
- **CCN-STIC-817 Gestión de Incidentes de Seguridad en el ENS**. Con el fin de comunicar y compartir información con claridad sobre incidentes es necesario adoptar una terminología común que describa todos aquellos que son posible que se materialicen. Sólo partiendo de las mismas premisas y siguiendo las mismas definiciones se puede coordinar una respuesta rápida y eficaz. Esta guía recoge un conjunto de conceptos y descripciones de alto nivel que permiten mejorar las comunicaciones entre los distintos responsables de seguridad de las AA.PP.

- **CCN-STIC-818 Herramientas de seguridad en el ENS**. Persigue el doble objetivo de describir y clasificar las diferentes herramientas de seguridad existentes, así como establecer los requisitos relativos a la selección, aprobación, implementación, uso y mantenimiento de dichas herramientas de seguridad en los Sistemas.
- **CCN-STIC-819 Guía de contratos en el marco del ENS**. En desarrollo.
- **CCN-STIC-820 Guía de protección contra Denegación de Servicio**. En desarrollo.
- **CCN-STIC-821 Ejemplos de Normas de Seguridad**. El objetivo de esta Guía es proponer a los organismos de las Administraciones Públicas españolas una relación de Normas de Seguridad, recogiendo lo exigido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS, en adelante).
- **CCN-STIC-822 Ejemplos de Procedimientos de Seguridad**. El objetivo de esta Guía es proponer a los organismos de las Administraciones Públicas españolas una relación de Procedimientos de Seguridad, recogiendo lo exigido por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica. La normativa contenida en la esta Guía resulta de aplicación a cualquier entidad del sector público del ámbito de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos: Administración General del Estado, Administración de las Comunidades Autónomas y Administración de las Entidades Locales.
- **CCN-STIC-823 Requisitos de seguridad en entornos CLOUD**. Esta guía recoge los aspectos de seguridad necesarios que deberán contemplarse para la adopción del *cloud computing* como paradigma tecnológico para la disposición de servicios con las garantías de seguridad pertinentes. Se han identificado las medidas de seguridad y los requisitos que deben cumplir los proveedores de servicios para dar cumplimiento tanto a los marcos legislativos aplicables, en especial el ENS o la normativa vigente en materia de protección de datos personales, como a los códigos de buenas prácticas o estándares reconocidos internacionalmente.
- **CCN-STIC-824 Informe del estado de seguridad**. Este documento describe una serie de medidas e indicadores con 2 destinatarios: el propio organismo propietario del sistema de información y el informe anual del estado de seguridad de la administración pública española. En ambos casos se busca una estimación preventiva de la seguridad, vía análisis del cumplimiento de determinados aspectos que se han estimado críticos para cualquier organismo; una estimación de la eficacia y eficiencia de las actividades en materia de seguridad y una estimación del esfuerzo humano y económico dedicado a seguridad TIC.

De forma complementaria el resto de series STIC (000,100,200,300,400,500,600 y 900) pueden ser utilizadas como guías de referencia para profundizar en determinadas materias enunciadas en el ENS.

Relación con otras normas y estándares de Seguridad

El RD en realidad presenta **analogías** constantes con la norma **ISO 27001:2007**, Gestión de la Seguridad de la Información, pero determina de manera específica controles a implementar en la administración electrónica.

El ENS presenta un esquema basado en el análisis de los riesgos, el concepto de seguridad integral, la organización de la misma como instrumento para la gestión y por el desarrollo de procesos de revaluación, prevención, reacción y recuperación mediante la implantación de medidas de seguridad según la naturaleza y servicios de la organización.

Por ello el Real Decreto 3/2010 representa una especie de SGSI con sus buenas prácticas incluido (Medidas de Seguridad), y auditable.

El ENS es una norma jurídica de aplicación obligatoria a todas las Administraciones Públicas. El ENS que trata la 'protección' de la información y los servicios, contempla y exige la gestión continuada de la seguridad, para lo cual cabe aplicar un sistema de gestión.

Una ISO 27001 para la Administración Pública

La normalización nacional e internacional, **de cumplimiento voluntario**, ofrece herramientas como la norma **UNE ISO/IEC 27001:2007** que es una norma de 'gestión' que contiene los requisitos para la construcción de un sistema de gestión de seguridad de la información, contra la que puede, en su caso, de forma voluntaria, certificarse una entidad (pública o privada) mediante un proceso de auditoría realizado por un auditor certificado externo.

Si bien cabe señalar que aquellas organizaciones que se encuentren certificadas contra ISO 27001 tienen una buena parte del camino recorrido para lograr su conformidad con el ENS, toda vez que **las medidas de protección que señala el ENS coinciden, en lo sustancial, con los controles que prevé la norma internacional**.

Por tanto, el Esquema Nacional de Seguridad y la norma UNE ISO/IEC 27001:2007 **difieren en su naturaleza, en su ámbito de aplicación, en su obligatoriedad y en los objetivos que persiguen**.

Relación entre el ENS y la norma UNE-ISO/IEC 27002:2009

La norma UNE-ISO/IEC 27002:2009 es un conjunto de controles de seguridad para sistemas de información genéricos.

Aunque muchas de las medidas de seguridad indicadas en el anexo II del ENS coinciden con controles de UNE-ISO/IEC 27002:2009, **el ENS es más preciso** y establece un sistema de protección proporcionado a la información y servicios a proteger para racionalizar la implantación de medidas de seguridad y reducir la discrecionalidad.

La norma UNE-ISO/IEC 27002:2009 carece de esta proporcionalidad, quedando a la mejor opinión del auditor que certifica la conformidad con la norma UNE ISO/IEC 27001:2007.

Por otra parte, el ENS contempla diversos aspectos de especial interés en relación con la protección de la información y los servicios de administración electrónica (por ejemplo, aquellos relativos a la firma electrónica) no recogidos en la norma UNE-ISO/IEC 27002:2009.

Certificación 27001 y ENS

ISO 27001 es una norma de gestión que indica cómo llegar a tener un Sistema de Gestión de Seguridad de la Información (para ello se apoya en las recomendaciones de ISO 27002). La norma UNE ISO/IEC 27001:2007, de carácter voluntario, es una norma de 'gestión' que contiene los requisitos para la construcción de un sistema de

gestión de seguridad de la información, contra la que puede, en su caso, de forma voluntaria, certificarse una entidad.

Sin embargo, cabe precisar que **quién haya certificado su Servicio/Sistema conforme a la norma UNE ISO/IEC 27001:2007 está muy cerca de asegurar el cumplimiento del ENS**, cuya conformidad debe alcanzarse siguiendo la metodología descrita en los Anexos I, II y III del Real Decreto 3/2010.

ITIL vs ENS

El Esquema Nacional de Seguridad se basa en procesos ITIL, aunque sin nombrarlos directamente. Principios básicos como la Seguridad diferenciada y la Gestión de Riegos, y en grupos de Medidas de Seguridad como son la Continuidad de la actividad, Gestión de cambios, Acuerdos de nivel de servicio y Proceso de Autorización, son en si mismos procesos identificados como mejores prácticas en ITIL.

Por ello es completamente factible la convivencia e integración con procesos ITIL y sistemas de gestión ITSM sobre, por ejemplo, ISO 20000.

Gestión integral de las certificaciones

Para aquellos organismos que deban implantar el ENS y estén inmersos en otras certificaciones 27001, ISO 9000, etc. cuyo objetivo final es disponer de un sistema de gestión integral de la seguridad, sería recomendable abordar ambos procedimientos de adecuación de una forma coordinada para no entrar en contradicciones y reducir esfuerzos a la hora de su implementación.

No obstante cabe reforzar la obligatoriedad jurídica del ENS frente a la voluntariedad del resto de certificaciones.

Preguntas frecuentes

¿Cuál es el origen del ENS?, ¿quiénes han participado en su elaboración?

El ENS nace en el artículo 42 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. El ENS es el resultado de un trabajo coordinado por el Ministerio de la Presidencia, asumido posteriormente por el Ministerio de Hacienda y Administraciones Públicas, con el apoyo del Centro Criptológico Nacional (CCN) y la participación de todas las Administraciones Públicas, incluyendo las universidades públicas, a través de los órganos colegiados con competencias en materia de administración electrónica: Consejo Superior de Administración Electrónica, Comité Sectorial de Administración Electrónica, Comisión Nacional de Administración Local. Participación que incluyó los informes preceptivos de: Ministerio de Política Territorial, Ministerio de la Presidencia, Agencia Española de Protección de Datos y Consejo de Estado.

También se ha tenido presente la opinión de las asociaciones de la Industria del sector TIC y las aportaciones recibidas tras la publicación del borrador en el sitio web del Consejo Superior de Administración Electrónica el 3 de septiembre de 2009.

¿Para qué sirven los Principios Básicos enunciados en el ENS?

Son los fundamentos que deben regir toda acción o decisión orientada a asegurar la información y los servicios.

¿Qué hay que hacer con los Requisitos Mínimos que se expresan en el ENS?

Los Requisitos Mínimos deben cumplirse siempre. Lo más habitual es que se plasmen por medio de la aplicación de las medidas de seguridad; pero si, por alguna razón, motivada y documentada, las medidas de seguridad son sustituidas por otras medidas compensatorias, los requisitos mínimos, en todo caso, deben cumplirse igualmente.

¿Es el ENS de obligado cumplimiento para todas las Administraciones Públicas?

El ámbito de aplicación del Esquema Nacional de Seguridad es el establecido en el artículo 2 de la Ley 11/2007, de manera que es de aplicación:

- A la Administración General del Estado, Administraciones de las Comunidades.
- Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

Están excluidos del ámbito de aplicación del ENS los sistemas que tratan información clasificada regulada por Ley 9/1968 de 5 de abril, de Secretos Oficiales y sus normas de desarrollo.

¿Qué aplicaciones, servicios o sistemas están comprendidos en el ámbito de aplicación del ENS?

Como regla general, podemos afirmar que el ENS es de aplicación a:

- Sedes electrónicas.
- Registros electrónicos.

- Sistemas de Información accesibles electrónicamente por los ciudadanos.
- Sistemas de Información para el ejercicio de derechos.
- Sistemas de Información para el cumplimiento de deberes.
- Sistemas de Información para recabar información y estado del procedimiento administrativo.

Cualquier caso que se aleje de la lista anterior conviene examinarlo con detalle y determinar si se encuentra o no comprendido dentro del marco de la Ley 11/2007 y por defecto lo dispuesto en el ENS.

¿Cuándo un sistema no estaría comprendido dentro del ámbito de aplicación del ENS?

Sólo en el caso de que el sistema:

- no esté relacionado con el ejercicio de derechos por medios electrónicos, o
- no esté relacionado con un cumplimiento de deberes por medios electrónicos, o
- no esté relacionado con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo.

Las AA.PP. podrán determinar incluir tal sistema en el ámbito de aplicación del ENS. En cualquier otro caso, la aplicación del ENS al sistema en cuestión es obligatoria.

¿Qué responsabilidades se derivan del incumplimiento del ENS?

Las responsabilidades derivadas del incumplimiento del ENS serían las que correspondieren a cada caso concreto, en virtud de lo dispuesto en la Ley 30/1992, de 6 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

¿Es el ENS de aplicación a las entidades vinculadas o dependientes de las Administraciones Públicas?

El ENS es aplicable a las entidades de derecho público vinculadas o dependientes de las Administraciones Públicas (AGE, CC.AA. y EE.LL.), aunque puede ser necesario un análisis caso por caso.

Las Universidades Públicas son Administración Pública vinculada (que no dependiente) a las administraciones de las Comunidades Autónomas y, por tanto, les aplica el ENS.

En el caso de los órganos constitucionales (Casa Real, Congreso, Senado, Consejo General del Poder Judicial, Tribunal Constitucional, Defensor del Pueblo, Tribunal de Cuentas, Consejo Económico y Social) la aplicación del ENS, o no, sería una decisión propia.

¿En qué medida debemos tener en cuenta el ENS cuando las actividades de los Sistemas de Información tienen lugar fuera de las dependencias de nuestro organismo o están subcontratados con empresas externas?

El ENS es una norma de obligado cumplimiento para todos los Sistemas de Información de las AA.PP., independientemente de su ubicación. Por tanto, debemos exigir el cumplimiento del ENS no sólo a los Sistemas de Información que estén operados por personal de las AA.PP. y/o en dependencias de las AA.PP., sino también a aquellos otros que, estando operados por terceros –e, incluso, en dependencias de terceros- desarrollan funciones, misiones, cometidos o servicios para las AA.PP.

¿Cuál es el "órgano superior" al que se alude en el ENS ?

A efectos del ENS, debemos entender por órgano superior, los siguientes:

- En la Administración General del Estado: Ministros y, en su caso, Secretarios de Estado.
- En la Administración de las Comunidades Autónomas: Consejeros y, en su caso, Viceconsejeros.
- En la Administración Local: Presidentes de Diputaciones Provinciales, Alcaldes y, en su caso, Tenientes de Alcalde.

Obsérvese que los órganos superiores que menciona el ENS se corresponden con aquellos órganos administrativos entre cuyas competencias se encuentra la determinación y asignación presupuestaria del organismo, circunstancia lógica, a la vista de que el cumplimiento del ENS supondrá, en la mayoría de los casos, la debida asignación presupuestaria que requiere su implantación.

¿Cómo debemos entender la Sede Electrónica, desde el punto de vista del ENS? ¿Es un Sistema de Información o es un derecho de los ciudadanos? ¿Hay que colgar en la Sede Electrónica la declaración de conformidad con el ENS?

La seguridad de la Sede Electrónica debe contemplarse, conjuntamente, desde su doble función: como punto de acceso (requiriendo medidas de seguridad diferenciadas) y como elemento a partir del cual los ciudadanos pueden tener acceso a una multiplicidad de servicios (que requerirán, cada uno de ellos, el tratamiento diferenciado que aconseje su preceptivo análisis de riesgos).

Así pues, la Sede Electrónica, requerirá de cautelas de seguridad diferenciadas, particulares y, en general, distintas, de cada uno de los servicios a los que puedan accederse a

través de ella.

Finalmente, en la Sede Electrónica nunca se deberá publicar información o documentos que puedan evidenciar vulnerabilidades o brechas de seguridad que puedan ser explotadas por agentes externos/internos.

¿Quedarían excluidos del ámbito de aplicación del ENS aquellos sistemas no relacionados con los ciudadanos *stricto sensu* como, por ejemplo, los implicados en la gestión de recursos humanos (función pública)?

La gestión de Recursos Humanos de un organismo público no goza de ese carácter "público" de sus actuaciones administrativas, puesto que se trata, más bien, de una relación "privada" entre el propio funcionario y el organismo del que depende o en el que presta sus servicios.

¿Se considerarían incluidos en el ámbito del ENS medios como la atención telefónica?

La atención telefónica (usada con las debidas garantías), está comprendida dentro de los canales que podrán ser utilizados por los ciudadanos para el ejercicio de sus derechos.

Por tanto, si un incidente de seguridad sobre los canales de atención telefónica pudiera tener repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos, nos encontraríamos con que tales canales estarían dentro del ámbito contemplado en el ENS.

¿Afecta el ENS a las relaciones entre distintos organismos de las AA.PP., entendidas como intercambio de información entre los mismos?

El ENS afecta, especialmente, a las Sedes y Registros Electrónicos, los Sistemas de Información accesibles electrónicamente por los ciudadanos, los Sistemas de Información para el ejercicio de derechos o para el cumplimiento de deberes y los Sistemas de Información para recabar información y estado del procedimiento administrativo.

Por tanto, si el intercambio de información entre distintos organismos de las AA.PP. tiene como objetivo último estos fines, tal intercambio deberá estar sometido a lo dispuesto en el ENS.

Un sistema de back-office (no visible desde el exterior) utilizado para, por ejemplo, gestionar procedimientos sancionadores de los ciudadanos, ¿quedaría dentro del alcance del ENS?

En el caso descrito, el ejercicio de los derechos de los ciudadanos quedaría limitado si, debido a algún incidente de seguridad en tal sistema, se impidiera o perturbara la interposición del correspondiente recurso, conocer el estado de su tramitación, alteración del cómputo de los plazos, etc.

Aunque se trate de un Sistema de Información no visible desde el exterior, su correcto funcionamiento incide directamente en el normal desenvolvimiento del procedimiento administrativo. Por tanto, le es de aplicación plena lo dispuesto en el ENS.

¿Es aplicable el ENS a los Hospitales públicos? ¿Y a las Universidades públicas?

Si el Hospital o Universidad de que se trate posee la consideración de entidad de derecho público (vinculada o dependiente, de la Administración General del Estado, de las Comunidades Autónomas o de las Entidades Locales), le será de plena aplicación lo dispuesto en el ENS en aquellas actividades que no desarrolle en régimen de derecho privado.

Los Colegios Profesionales, ¿están sujetos a lo dispuesto en el ENS?

Si entre las funciones, servicios o actividades que desarrollan, prestan o acometen se encuentran aquellos que están relacionados con:

- Sedes electrónicas.
- Registros electrónicos.
- Sistemas de Información accesibles electrónicamente por los ciudadanos.
- Sistemas de Información para el ejercicio de derechos.
- Sistemas de Información para el cumplimiento de deberes.
- Sistemas de Información para recabar información y/o estado del procedimiento administrativo.

Entonces, a tales servicios o actividades, le será de plena aplicación lo dispuesto en el ENS, no siendo aplicable, sin embargo, a aquellas otras actividades que desarrollaran al margen de las enumeradas o al amparo del derecho privado.

¿Cuáles son las medidas de seguridad que deben adoptar los proveedores externos que proporcionen servicios informáticos a las AA.PP.?, ¿deben cumplir con el ENS? (Por ejemplo: servicios de alojamiento de servidores, servicios *cloud computing*, etc.)

Las medidas de seguridad que deben adoptar los proveedores de servicios no las fija el propio proveedor, sino que serán las determinadas por la Administración contratante, en virtud de la naturaleza de los servicios prestados.

Es responsabilidad de la Administración contratante la suscripción del correspondiente contrato de prestación del servicio que deberá contener todas las estipulaciones necesarias para dar cumplimiento a lo dispuesto en el ENS, en virtud de la naturaleza del servicio prestado.

¿Cómo se realiza el control de la correcta aplicación del ENS?

Existen varios controles:

- Los ordinarios de cumplimiento de cada unidad administrativa (art. 40).
- Los que pueda articular el Comité Sectorial de Administración Electrónica para conocer el estado de las principales variables de seguridad (art. 35).
- Los derivados de las auditorías (art. 34).
- Eventualmente, los que pudieran emanar del CCN, en el ámbito de sus competencias.

¿Se pueden entender equivalentes los niveles LOPD con los niveles ENS?

Las denominaciones BÁSICO/MEDIO/ALTO, que utilizan tanto el ENS como la LOPD no poseen la misma semántica. No son intercambiables ni significan lo mismo.

¿Cuáles son las funciones que debe desarrollar el Responsable del Sistema, según el ENS? ¿Quién debe ser esta persona?

El Responsable del Sistema es un puesto operativo, no un cargo directivo o de gobierno. Suele recibir también la denominación de Responsable de Producción o Explotación, de manera que en él viene a recaer la responsabilidad de la prestación material del servicio.

¿Cuáles son las funciones que debe desarrollar el Responsable de la Información según el ENS?, ¿quién debe ser?

Según se manifiesta en la Guía CCN-STIC-801, , el Responsable de la Información es la persona (u órgano colegiado con responsabilidad unitaria identificable) que tiene la potestad de establecer los requisitos de la información en materia de seguridad, o, en terminología del ENS, la persona que determina los niveles de seguridad de la información.

Por tanto, lo lógico será que el Responsable de la Información se corresponda con algún funcionario o empleado público (de carrera o de libre designación, según los casos) perteneciente a los niveles de gobierno del organismo público en cuestión.

¿Puede designarse al Responsable de Seguridad como un Comité en el que se contemplen distintos roles: técnico, organizativo y legal?, ¿tiene sentido que el Responsable de Seguridad sea un alto cargo?, ¿cuál es el perfil más idóneo para esta función?

La finalidad última del ENS en relación con este asunto es evitar que la responsabilidad se diluya en comités o unidades administrativas más o menos formales, sino que, por el contrario, la responsabilidad última deber recaer sobre una persona física (que podrá ser, nada lo impide, el Presidente de un Comité de Seguridad).

El Responsable de Seguridad no es un cargo de gobierno.

Su función esencial es planificar lo que se ha de hacer en materia de seguridad, así como supervisar que se haya hecho adecuadamente. Suele poseer un perfil técnico.

Aunque es frecuente que el Responsable de Seguridad posea un nivel administrativo inferior al Responsable del Sistema, lo idóneo sería que ambas figuras se mantuvieran en el mismo nivel administrativo.

¿Es obligatoria la división de responsabilidades citada en la Guía CCN-STIC-801?

La división de responsabilidades enunciada en la Guía CCN-STIC-801 es una recomendación, desarrollada para el mejor cumplimiento de lo dispuesto en el ENS, recomendación que se contiene de nuevo en la medida de seguridad “Segregación de funciones y tareas [op. acc.3].”

¿El Responsable de Seguridad del ENS puede ser la misma persona que el Responsable de Seguridad de la LOPD?

Formalmente nada lo impide.

¿Puede una misma persona ser Responsable de la Información, Responsable del Servicio y Responsable de Seguridad?, ¿qué roles son incompatibles en una misma persona?

El ENS prohíbe, explícitamente, que el Responsable del Sistema sea la misma persona que el Responsable de Seguridad.

Hecha esta salvedad, nos preguntamos hasta qué punto el resto de las responsabilidades enunciadas en el ENS son

susceptibles de ser asumidas de manera unificada.

Desde el punto de vista formal, nada lo impide. Sin embargo, desde el punto de vista funcional, esta coincidencia no es lógica.

Habiendo concluido el plazo previsto en el ENS para redactar y aprobar el Plan de Adecuación al ENS, ¿es necesaria su realización?

Naturalmente. Siempre constituye el punto de partida de todo proceso de adecuación legal de los Sistemas de Información de las organizaciones públicas a lo dispuesto en el ENS.

¿Se puede hacer un Plan de Adecuación sin incluir la Política de Seguridad?

Rotundamente, no. La redacción –y aprobación- de la Política de Seguridad de la organización es una condición previa e indispensable para abordar un proceso de conformidad legal al ENS coherente y con garantías de éxito.

¿Se puede aprobar una Política de Seguridad sin contemplar la Estructura de Seguridad de la Organización de la Seguridad?

No tendría sentido. Obsérvese que una Política de Seguridad contiene, necesariamente, la estructura organizativa encargada de dirigir y materializar su implantación, y velar por su cumplimiento.

¿Debe publicarse en la Sede Electrónica del organismo en cuestión el Plan de Adecuación al ENS?

Sería claramente contraproducente desde el punto de vista de la seguridad, toda vez que se estarían dando "pistas" respecto del nivel de seguridad de los sistemas de información del organismo, cuestión nada deseable y que vendría a introducir riesgos adicionales.

¿Es obligatorio para las AA.PP. seguir lo que se indica en las Guías STIC del CCN?

No se trata de normas imperativas, sino de la expresión de metodologías y recomendaciones para el adecuado cumplimiento de lo dispuesto en el ENS.

Recomendaciones que tendrán especial significación para aquel organismo administrativo afectado por un incidente grave de seguridad, motivado por la inobservancia de las recomendaciones descritas.

¿Es necesario realizar un Análisis de Riegos, en sentido estricto? ¿No bastaría con usar la experiencia de los técnicos del organismo para determinar qué medidas son las más oportunas en cada caso?

La excesiva confianza en las capacidades personales y en la experiencia es, en sí misma, un riesgo. Podemos afirmar que el Análisis y la Gestión de Riesgos son la base de la Seguridad TIC. Realizar un Análisis y Gestión de Riesgos no es, por tanto, una medida opcional: es una exigencia de obligado cumplimiento.

¿Es necesario utilizar herramientas para el Análisis de Riesgos?

Usar una herramienta, que nos sirva de ayuda para desarrollar eficazmente un Análisis de Riesgos, es sin duda una buena opción. En el caso de las AA.PP. es especialmente importante que tales herramientas estén basadas en la metodología MAGERIT. En este sentido, debemos señalar que la herramienta PILAR, suministrada gratuitamente por el CCN a todas las AA.PP. españolas, se ha mostrado como una ayuda extraordinariamente eficaz en tal sentido.

La preceptiva Declaración de Aplicabilidad, ¿ha de realizarse por Sistema de Información o por Áreas de Negocio?

Deberá aplicarse al Sistema de Información que le ha dado origen.

¿Es necesario realizar la auditoría de la seguridad por un auditor independiente de la organización?

Cuando se están evaluando sistemas/servicios cuya categoría sea de nivel MEDIO o ALTO, la norma señala que se hace necesario pasar una auditoría bienal, realizada por personal cualificado e independiente del servicio/sistema que esté auditando En sistemas categorizados como de nivel BAJO, el ENS prescribe una autoevaluación.

¿Existe alguna certificación que acredite la adecuación al ENS por parte de un organismo público?

En la actualidad no existe tal certificación, emitida por un organismo público.

Nada impide, sin embargo, que empresas privadas especializadas, con la cualificación adecuada, a instancias del organismo público de que se trate, y tras pasar con éxito el organismo público la Auditoría a que se refiere el ENS, puedan emitir un certificado de conformidad , con el alcance temporal y ámbito que se determine.

Contactos Symantec

Jesús Herranz
jesus_herranz@symantec.com

Antonio Cortés
antonio_cortes@symantec.com

Juan Aguilo
juan_aguilo@symantec.com

Sobre Symantec

Symantec se fundó en 1982 por un grupo de especialistas en informática con visión de futuro. La empresa ha evolucionado y se convirtió en una de las empresas de software más grandes del mundo, con más de 18.500 empleados en más de 50 países. Brindamos soluciones de seguridad, almacenamiento y administración de sistemas que ayudan a nuestros clientes, desde consumidores y pequeñas empresas hasta las más grandes corporaciones internacionales, a administrar su información y protegerla contra más riesgos, en más puntos y de manera más completa y eficiente que cualquier otra empresa.

Hoy en día, la información es el valor más valioso de la economía mundial. Las personas y las empresas confían en ella para gobernar naciones, llevar a cabo operaciones comerciales y tomar decisiones personales.

Sin embargo, la información con la que contamos cada vez corre más riesgos. Amenazas cibernéticas, desastres naturales, errores de usuarios y fallas en los sistemas ponen en peligro la seguridad y la disponibilidad de la valiosa y crucial información. Las personas y organizaciones están buscando un socio que pueda ayudarlos a comprender y administrar los riesgos de la información, ya sea protegiendo información personal en su equipo o al construir una infraestructura global de TI que sea segura, resistente y flexible.

Symantec es el líder mundial en soluciones que ayudan a los usuarios individuales y a las empresas a garantizar la seguridad, la disponibilidad y la integridad de su información.

Symantec protege la información del mundo, y es el líder global en soluciones de seguridad, copias de seguridad y disponibilidad. Nuestros productos y servicios innovadores protegen a las personas y a la información en cualquier entorno – desde el dispositivo móvil más pequeño, al centro de datos empresarial, y a los sistemas basados en la nube. Nuestra experiencia líder del sector protegiendo datos, identidades e interacciones proporciona a nuestros clientes confianza en un mundo conectado.

De este modo, en el marco específico de regulación del Esquema Nacional de Seguridad, Symantec aporta soluciones líderes de seguridad que permiten:

- tener una visión integral de la seguridad de estos nuevos servicios, considerando todos los medios necesarios a nivel técnico, humano, material y de organización;
- la adecuación de los controles de seguridad a un entorno evolutivo y cambiante, tanto por parte de los sistemas de información, como de sus amenazas y vulnerabilidades;
- y el cumplimiento particular y concreto de los requisitos propios del Esquema Nacional de Seguridad;

y todo ello, siempre incorporando el conocimiento y desarrollo obtenido desde una visión global de Internet, y por tanto de estos nuevos servicios.

Para más información, visite www.symantec.com o conecte con Symantec en: go.symantec.com/socialmedia.

Contactos

José María Rodríguez
Socio
+34 650 592 012
jmrodriguez@tithink.com
@chemapostigo

Ignacio Peralta
Socio
+34 608 791 117
iperalta@tithink.com
@iperaltal

Sobre tiThink

En tiThink enfocamos nuestro asesoramiento hacia la Transformación del Comportamiento Tecnológico de las compañías, ayudándolas a alcanzar la madurez corporativa en la aplicación eficiente de las Tecnologías.

Somos una compañía de consultoría estratégica y servicios de seguridad de información, que ayuda a proteger y generar valor a sus clientes apalancando el cumplimiento de sus objetivos estratégicos, mediante el uso de metodologías estructuradas y adaptables.

Tenemos como meta, ser reconocidos como una empresa de consultoría con un portafolio de servicios de calidad, excelencia y respuesta integral. Además, deseamos ser percibidos como un aliado estratégico, representado en un excelente retorno de la inversión a través de la generación de valor y con un alto nivel de satisfacción de sus clientes, empleados y socios.

En el ámbito del Esquema Nacional de Seguridad desde tiThink te podemos ayudar en:

- Evaluar el "estado del arte" y definir el plan director o la hoja de ruta para la adecuación al ENS.
- Definir y formalizar las Políticas de Seguridad de la información, sus normas y su modelo organizativo.
- Catalogar los sistemas y servicios bajo tu responsabilidad y definir la Declaración de Aplicabilidad de medidas.
- Implantar la metodología de gestión de riesgos tecnológicos.
- Acompañar en el proceso de implantación de medidas de seguridad: selección de herramientas, definición de procedimientos, supervisión de proyectos de implantación de herramientas, etc.
- Realizar auditorías y pruebas de seguridad de los sistemas.
- Tutelar el proceso de adecuación al ENS bajo la figura de Oficina de Proyectos.

www.tithink.com