MINISTERIO
DE HACIENDA Y
ADMINISTRACIONES PÚBLICAS

(17-11-2014)

REF.:
REF.C.M.:

PROYECTO DE REAL DECRETO …/…, de …, MODIFICACIÓN DEL 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 Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, establece en su artículo 1.2 que las Administraciones públicas utilizarán las tecnologías de la información de acuerdo con lo previsto en la misma, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

Entre los principios de la Ley 11/2007 figuran los relativos al respeto al derecho a la protección de los datos de carácter personal en los términos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de carácter personal, a la seguridad en la implantación y utilización de los medios electrónicos por las Administraciones Públicas y a la proporcionalidad, en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones. También figura la seguridad entre los derechos de los ciudadanos recogidos en la citada Ley, de forma que se contempla el derecho a la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Asimismo, la Ley 11/2007, en su artículo 42.2, establece que el Esquema Nacional de Seguridad, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto mantener la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

Además, la Ley 11/2007, en su artículo 42.3, establece que el Esquema Nacional de Seguridad debe mantenerse actualizado de manera permanente y, en desarrollo de este precepto, el Real Decreto 3/2010, establece que el Esquema Nacional de Seguridad se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de Administración electrónica, la evolución de la tecnología, los nuevos estándares internacionales

sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo, manteniéndose actualizado de manera permanente.

En efecto, los ciudadanos confían en que los servicios públicos disponibles por el medio electrónico se presten en unas condiciones de seguridad equivalentes a las que 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 administraciones públicas y los servicios que prestan constituyen activos nacionales estratégicos.

Por otra parte, las ciberamenazas, que constituyen riesgos que afectan singularmente a la Seguridad Nacional, se han convertido en un potente instrumento de agresión contra particulares y entidades públicas y privadas, de manera que la ciberseguridad figura entre los doce ámbitos prioritarios de actuación de la Estrategia de Seguridad Nacional como instrumento actualizado para encarar el constante y profundo cambio mundial en el que nos hayamos inmersos y como garantía de la adecuada actuación de España en el ámbito internacional. En particular, dicho ámbito de actuación de ciberseguridad se refiere a la garantía de la seguridad de los sistemas de información y las redes de comunicaciones e infraestructuras comunes a todas las Administraciones Públicas y a que se finalizará la implantación del Esquema Nacional de Seguridad, previsto en la Ley 11/2007, de 22 de junio. Profundizando en la cuestión, la Estrategia de Ciberseguridad Nacional en su Objetivo I se refiere a "*Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia*" y en su línea de acción 2, titulada "*Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas*", se incluye la medida relativa a "*Asegurar la plena implantación del Esquema Nacional de Seguridad y articular los procedimientos necesarios para conocer regularmente el estado de las principales variables de seguridad de los sistemas afectados*".

La rápida evolución de las tecnologías de aplicación, la experiencia derivada de la implantación del Esquema Nacional de Seguridad y el mejor cumplimiento de los artículos indicados, aconsejan la actualización de esta norma.

Para aportar una mayor concreción y detalle, se introducen mejoras en el artículo 11 relativo a los requisitos mínimos de seguridad, en el 15 relativo a la profesionalidad, en el 18 relativo a la adquisición de productos de seguridad, en el 19 relativo a la seguridad por defecto, en el artículo 27 relativo al cumplimiento de los requisitos mínimos; se introducen en el artículo 29 las instrucciones técnicas de seguridad; en lo referido al informe del estado de la seguridad, se modifica el artículo 35 mediante el añadido de referencias expresas a la articulación de los procedimientos necesarios para la recogida y consolidación de la información y aspectos metodológicos y organismos responsables de su realización; se introduce en el artículo 36 la obligación de notificar incidentes de seguridad que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados; mientras que en el artículo 37 se precisan los elementos necesarios para la investigación de incidentes de seguridad; finalmente, en el texto del Anexo II se introducen precisiones que aumentan la eficacia de ciertas medidas de seguridad, en particular, en relación con el Reglamento nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se

deroga la Directiva 1999/93/CE; a la vez que se realizan algunas otras mejoras en los anexos III, IV y V.

Las entidades del ámbito de aplicación del 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, dispondrán de un plazo de veinticuatro meses para la adecuación de sus sistemas a lo dispuesto en el presente real decreto.

En su virtud, a propuesta conjunta de la Ministra de la Presidencia y del Ministro de Hacienda y Administraciones Públicas,…, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día…

DISPONGO

Artículo único. *Modificación del 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.*

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 será modificado en el siguiente sentido:

Uno. El apartado 1 del artículo 11 queda redactado como sigue:
«Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad de la organización que articule la gestión continuada de la seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:»

Dos. Los apartados 1 y 3 del artículo 15 quedan redactados como sigue:
« 1. 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 incidentes y desmantelamiento.»
«3. Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con unos niveles idóneos de gestión y madurez en los servicios prestados y con profesionales cualificados.»

Tres. El título del artículo 18 queda modificado como ‘Adquisición de productos y contratación de servicios de seguridad’.
Los apartados 1 y 2 del artículo 18 quedan redactados como sigue:
«1. 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 utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos

asumidos no lo justifiquen a juicio del Responsable de Seguridad. Una Instrucción Técnica de Seguridad detallará los criterios exigibles.
2. La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares reconocidos internacionalmente, en el ámbito de la seguridad funcional.»
Se añade un nuevo apartado 4 redactado como sigue:
«4. Para la contratación de servicios de seguridad se estará a lo dispuesto en los apartados anteriores y en el artículo 15.»

Cuatro. El apartado a) del artículo 19 queda redactado como sigue:
«a) El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos. »

Cinco. Se añaden dos nuevos apartado 4 y 5 al artículo 27 redactados como sigue:
«4. La relación de medidas seleccionadas del anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de seguridad.
5. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de seguridad. »

Seis. El título del artículo 29 queda modificado como ‘Instrucciones y guías de seguridad’.
Se añaden dos apartados, 2 y 3, con la siguiente redacción:
«2. El Ministerio de Hacienda y Administraciones Públicas, a propuesta del Comité Sectorial de Administración Electrónica previsto en el artículo 40 de la Ley 11/2007, de 22 de junio, y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento y se publicarán mediante Resolución de la Secretaria de Estado de Administraciones Públicas. Para la redacción y mantenimiento de las instrucciones técnicas de seguridad se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.
3. Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas a nivel europeo que resulten de aplicación.»

Siete. El apartado 4 del artículo 34 queda redactado como sigue:
«4. En la realización de esta auditoría se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de auditorías de sistemas de información. Una instrucción técnica de seguridad regulará el desarrollo de las auditorías previstas en el presente real decreto. »

Ocho. El artículo 35 queda redactado como sigue:

«El Comité Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere el presente Real Decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.
El Centro Criptológico Nacional articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en el Comité Sectorial de Administración Electrónica y en la Comisión de Estrategia TIC para la Administración General del Estado. »

Nueve. En el artículo 36 se añade un segundo párrafo con la siguiente redacción:
«Las Administraciones Públicas notificarán al Centro Criptológico Nacional aquellos incidentes que tengan un impacto significativo en la seguridad de la información manejada y de los servicios prestados. Mediante la correspondiente instrucción técnica de seguridad se determinarán las características de los incidentes sujetos a notificación y el procedimiento para realizarlo. »

Diez. En el artículo 37, el apartado 1. a) queda redactado como sigue:
«a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.
El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas.
Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar evidencias tales como informes de auditoría de los sistemas afectados, registros de auditoría, configuraciones y otra información relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, atendiendo, cuando sea de aplicación, a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, y su normativa de desarrollo, así como a la posible confidencialidad de datos de carácter institucional u organizativo.»

Once. Se elimina la Disposición adicional segunda. Instituto Nacional de Tecnologías de la Comunicación (INTECO) y organismos análogos.

Doce. Se añade una nueva disposición adicional redactada como sigue:
«Disposición adicional quinta. Desarrollo del Esquema Nacional de Seguridad
1. Sin perjuicio de las propuestas que pueda acordar el Comité Sectorial de Administración Electrónica según lo establecido en el artículo 29, apartado 2, se desarrollarán las siguientes instrucciones técnicas de seguridad que serán de obligado cumplimiento por parte de las Administraciones públicas:
a) Informe del estado de la seguridad.
b) Notificación de incidentes de seguridad.

c) Auditoría de la seguridad.
d) Conformidad con el Esquema Nacional de Seguridad.
e) Adquisición de productos de seguridad.
f) Criptología de empleo en el Esquema Nacional de Seguridad.
g) Interconexión en el Esquema Nacional de Seguridad.
h) Requisitos de seguridad en entornos externalizados.
2. La aprobación de estas instrucciones se realizará de acuerdo con el procedimiento establecido en el citado artículo 29 apartados 2 y 3. »

Trece. El apartado 3.4 Proceso de autorización [org.4] del Anexo II queda como sigue:

«**3.4 Proceso de autorización [org.4].**

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información:
a) Utilización de instalaciones, habituales y alternativas.
b) Entrada de equipos en producción, en particular, equipos que involucren criptografía.
c) Entrada de aplicaciones en producción.
d) Establecimiento de enlaces de comunicaciones con otros sistemas.
e) Utilización de medios de comunicación, habituales y alternativos.
f) Utilización de soportes de información.
g) Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, PDA, u otros de naturaleza análoga.
h) Utilización de servicios de terceros, bajo contrato o Convenio. »

Catorce. El apartado 4.1.2. Arquitectura de seguridad [op.pl.2] del Anexo II queda como sigue:

«**4.1.2 Arquitectura de seguridad [op.pl.2].**

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	+

La seguridad del sistema será objeto de un planteamiento integral detallando, al menos, los siguientes aspectos:

Categoría BÁSICA
a) Documentación de las instalaciones:
   1. Áreas.
   2. Puntos de acceso.
b) Documentación del sistema:

1. Equipos.
2. Redes internas y conexiones al exterior.
3. Puntos de acceso al sistema (puestos de trabajo y consolas de administración).

c) Esquema de líneas de defensa:
1. Puntos de interconexión a otros sistemas o a otras redes, en especial si se trata de Internet o redes públicas en general.
2. Cortafuegos, DMZ, etc.
3. Utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

d) Sistema de identificación y autenticación de usuarios:
1. Uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga.
2. Uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Categoría MEDIA

e) Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Categoría ALTA

f) Sistema de gestión de seguridad de la información con actualización y aprobación periódica.

g) Controles técnicos internos:
1. Validación de datos de entrada, salida y datos intermedios. »

Quince. El apartado 4.1.5. Componentes certificados [op.pl.5] del Anexo II, queda como sigue:

«**4.1.5 Componentes certificados [op.pl.5].**

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

Categoría ALTA

Se utilizarán sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas.

Tendrán la consideración de entidades independientes de reconocida solvencia las recogidas en los acuerdos o arreglos internacionales de reconocimiento mutuo de los certificados de la seguridad de la tecnología de la información u otras de naturaleza análoga.

Una instrucción técnica de seguridad detallará los criterios exigibles. »

Dieciséis. El apartado 4.2.1. Identificación [op.acc.1] del Anexo II queda redactado como sigue:

« **4.2.1. Identificación [op.acc.1].**

dimensiones	A T		
nivel	bajo	medio	alto
	aplica	=	=

La identificación de los usuarios del sistema se realizará de acuerdo con lo que se indica a continuación:

a) Se asignará un identificador singular para cada entidad (usuario o proceso) que accede al sistema, de tal forma que:
   1º Se puede saber quién recibe y qué derechos de acceso recibe.
   2º Se puede saber quién ha hecho algo y qué ha hecho.

b) Las cuentas de usuario se gestionarán de la siguiente forma:
   1º Cada cuenta estará asociada a un identificador único.
   2º Las cuentas deben ser inhabilitadas en los siguientes casos: cuando el usuario deja la organización; cuando el usuario cesa en la función para la cual se requería la cuenta de usuario; o, cuando la persona que la autorizó, da orden en sentido contrario.
   3º Las cuentas se retendrán durante el periodo necesario para atender a las necesidades de trazabilidad de los registros de actividad asociados a las mismas. A este periodo se le denominará periodo de retención.

c) En los supuestos contemplados en el Capítulo IV relativo a “Comunicaciones Electrónicas”, las partes intervinientes se identificarán de acuerdo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Si se requiere un nivel BAJO en la dimensión de autenticidad (Anexo I)
- nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento nº 910/2014)

Si se requiere un nivel MEDIO en la dimensión de autenticidad (Anexo I)
- nivel de seguridad sustancial o alto (artículo 8 del Reglamento nº 910/2014)

Si se requiere un nivel ALTO en la dimensión de autenticidad (Anexo I)
- nivel de seguridad alto (artículo 8 del Reglamento nº 910/2014) »

Diecisiete. El apartado 4.2.5. Mecanismo de autenticación [op.acc.5] del Anexo II, queda como sigue:

«**4.2.5. Mecanismo de autenticación [op.acc.5].**

dimensiones	ICAT		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:
- “algo que se sabe”: contraseñas o claves concertadas.
- “algo que se tiene”: componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, *tokens*).
- “algo que se es”: elementos biométricos.

Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte.

Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel.

Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán credenciales.

Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios:

- Mediante la presentación física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello.
- De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado.
- De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.

Nivel BAJO

a) Como principio general, se admitirá el uso de cualquier mecanismo de autenticación sustentado en un solo factor.

b) En el caso de utilizarse como factor “algo que se sabe”, se aplicarán reglas básicas de calidad de la misma.

c) Se atenderá a la seguridad de las credenciales de forma que:

1. Las credenciales se activarán una vez estén bajo el control efectivo del usuario.
2. Las credenciales estarán bajo el control exclusivo del usuario.
3. El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad e información inmediata en caso de pérdida.
4. Las credenciales se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5. Las credenciales se retirarán y serán deshabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) Se exigirá el uso de al menos dos factores de autenticación.

b) En el caso de utilización de “algo que se sabe” como factor de autenticación, se establecerán exigencias rigurosas de calidad y renovación.

c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo:

1. Presencial.
2. Telemático usando certificado electrónico cualificado.
3. Telemático mediante una autenticación con una credencial electrónica obtenida tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.

Nivel ALTO

a) Las credenciales se suspenderán tras un periodo definido de no utilización.

b) En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.

c) Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma. »

Dieciocho. El apartado 4.3.3 Gestión de la configuración [op.exp.3], del anexo II queda como sigue:

«**4.3.3. Gestión de la configuración [op.exp.3].**

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se gestionará de forma continua la configuración de los componentes del sistema de forma que:

a) Se mantenga en todo momento la regla de «funcionalidad mínima» ([op.exp.2]).

b) Se mantenga en todo momento la regla de «seguridad por defecto» ([op.exp.2]).

c) El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).

d) El sistema reaccione a vulnerabilidades reportadas ([op.exp.4]).

e) El sistema reaccione a incidentes (ver [op.exp.7]). »

Diecinueve. El apartado 4.3.7 Gestión de incidencias [op.exp.7], del anexo II queda como sigue:

«4.3.7 Gestión de incidentes [op.exp.7].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema, incluyendo:

a) Procedimiento de reporte de incidentes reales o sospechosos, detallando el escalado de la notificación.

b) Procedimiento de toma de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.

c) Procedimiento de asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.

d) Procedimientos para informar a las partes interesadas, internas y externas.

e) Procedimientos para:

1. Prevenir que se repita el incidente.

2. Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.

3. Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y normas de desarrollo, sin perjuicio de cumplir, además, las medidas establecidas por este real decreto. »

Veinte. El apartado 4.3.8 Registro de la actividad de los usuarios [op.exp.8], del Anexo II queda como sigue:

«4.3.8 Registro de la actividad de los usuarios [op.exp.8].

dimensiones	T		
nivel	bajo	medio	alto
	aplica	+	++

Se registrarán las actividades de los usuarios en el sistema, de forma que:

a) El registro indicará quién realiza la actividad, cuándo la realiza y sobre qué información.

b) Se incluirá la actividad de los usuarios y, especialmente, la de los operadores y administradores en cuanto puedan acceder a la configuración y actuar en el mantenimiento del sistema.

c) Deberán registrarse las actividades realizadas con éxito y los intentos fracasados.

d) La determinación de qué actividades deben registrarse y con qué niveles de detalle se adoptará a la vista del análisis de riesgos realizado sobre el sistema ([op.pl.1]).

Nivel BAJO
Se activarán los registros de actividad en los servidores.

Nivel MEDIO
Se revisarán informalmente los registros de actividad buscando patrones anormales.

Nivel ALTO

Se dispondrá de un sistema automático de recolección de registros y correlación de eventos; es decir, una consola de seguridad centralizada. »

Veintiuno. El apartado 4.3.9 Registro de la gestión de incidencias [op.exp.9], del Anexo II queda como sigue:

«4.3.9 Registro de la gestión de incidentes [op.exp.9].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, de forma que:

a) Se registrará el reporte inicial, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

b) Se registrará aquella evidencia que pueda, posteriormente, sustentar una demanda judicial, o hacer frente a ella, cuando el incidente pueda llevar a actuaciones disciplinarias sobre el personal interno, sobre proveedores externos o a la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.

c) Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables. »

Veintidós. El apartado 4.3.11 Protección de claves criptográficas [op.exp.11], del Anexo II queda como sigue:

«4.3.11 Protección de claves criptográficas [op.exp.11].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	=

Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.

Categoría BÁSICA

a) Los medios de generación estarán aislados de los medios de explotación.

b) Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

Categoría MEDIA

a) Se usarán programas evaluados o dispositivos criptográficos certificados conforme a lo establecido en [op.pl.5].

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional. »

Veintitrés. El apartado 4.4.2. Gestión diaria [op.ext.2] del Anexo II queda como sigue:

«4.4.2 Gestión diaria [op.ext.2].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA

Para la gestión diaria del sistema, se establecerán los siguientes puntos:

a) Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio y el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).

b) El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas afectados por el acuerdo.

c) El mecanismo y los procedimientos de coordinación en caso de incidentes y desastres (ver [op.exp.7]). »

Veinticuatro. El apartado 4.6.1. Detección de intrusión [op.mon.1] del Anexo II queda como sigue:

«4.6.1 Detección de intrusión [op.mon.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Categoría MEDIA
Se dispondrán de herramientas de detección o de prevención de intrusión. »

Veinticinco. El apartado 4.6.2 Sistema de métricas [op.mon.2] queda como sigue:

«4.6.2 Sistema de métricas [op.mon.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA:
Se recopilarán los datos necesarios atendiendo a la categoría del sistema para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35.

Categoría MEDIA:
Además, se recopilaran datos para valorar el sistema de gestión de incidentes, permitiendo conocer
- número de incidentes de seguridad tratados
- tiempo empleado para cerrar el 50% de los incidentes
- tiempo empleado para cerrar el 90% de las incidentes

Categoría ALTA
Se recopilarán datos para conocer la eficiencia del sistema de seguridad TIC:
- recursos consumidos: horas y presupuesto »

Veintiséis. El apartado 5.2.3 Concienciación [mp.per.3] queda como sigue:

«**5.2.3 Concienciación [mp.per.3].**

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

a) La normativa de seguridad relativa al buen uso de los sistemas.

b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas. »

Veintisiete. El apartado 5.3.3 Protección de portátiles [mp.eq.3] queda como sigue:

«**5.3.3 Protección de portátiles [mp.eq.3].**

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	+

Categoría BÁSICA

Los equipos que sean susceptibles de salir de las instalaciones de la organización y no puedan beneficiarse de la protección física correspondiente, con un riesgo manifiesto de pérdida o robo, serán protegidos adecuadamente.

Sin perjuicio de las medidas generales que les afecten, se adoptarán las siguientes:

a) Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.

b) Se establecerá un canal de comunicación para informar, al servicio de gestión de incidentes, de pérdidas o sustracciones.

c) Cuando un equipo portátil se conecte remotamente a través de redes que no están bajo el estricto control de la entidad, el lado servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de Internet y otras redes que no sean de confianza.

d) Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

Categoría ALTA

a) Se dotará al dispositivo de detectores de violación que permitan saber el equipo ha sido manipulado y activen los procedimientos previstos de gestión del incidente.

b) La información de nivel alto almacenada en el disco se protegerá mediante cifrado. »

Veintiocho. El apartado 5.4.2 Protección de la confidencialidad [mp.com.2] queda como sigue:

«**5.4.2 Protección de la confidencialidad [mp.com.2].**

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	aplica	+

Nivel MEDIO

a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.

b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

Nivel ALTO

a) Se emplearán, preferentemente, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5]. »

Veintinueve. El apartado 5.4.3 Protección de la autenticidad y de la integridad [mp.com.3] queda como sigue:

«**5.4.3 Protección de la autenticidad y de la integridad [mp.com.3].**

dimensiones	I A		
nivel	Bajo	medio	Alto
	aplica	+	++

Nivel BAJO

a) Se asegurará la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información (ver [op.acc.5]).
b) Se prevendrán ataques activos, garantizando que al menos serán detectados. y se activarán los procedimientos previstos de tratamiento del incidente Se considerarán ataques activos:
    1. La alteración de la información en tránsito
    2. La inyección de información espuria
    3. El secuestro de la sesión por una tercera parte
c) Se aceptará cualquier mecanismo de autenticación de los previstos en la Ley 11/2007.

Nivel MEDIO

a) Se emplearán redes privadas virtuales cuando la comunicación discurra por redes fuera del propio dominio de seguridad.
b) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
c) Se aceptará cualquier mecanismo de autenticación de los previstos en la Ley 11/2007. En caso de uso de claves concertadas se aplicarán exigencias medias en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta.

Nivel ALTO

a) Se valorará positivamente el empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.
b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5].
c) Se aceptará cualquier mecanismo de autenticación de los previstos en la Ley 11/2007. En caso de uso de claves concertadas se aplicarán exigencias altas en cuanto a su calidad frente a ataques de adivinación, diccionario o fuerza bruta. »

Treinta. El apartado 5.5.2 Criptografía [mp.si.2] del Anexo II queda como sigue:

«5.5.2 Criptografía [mp.si.2].

dimensiones	I C		
nivel	bajo	medio	alto
	no aplica	aplica	+

Esta medida se aplica, en particular, a todos los dispositivos removibles. Se entenderán por dispositivos removibles, los CD, DVD, discos USB, u otros de naturaleza análoga.

Nivel MEDIO

Se aplicarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.

Nivel ALTO

a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

b) Se emplearán productos certificados conforme a lo establecido en [op.pl.5]. »

Treinta y uno. El apartado 5.5.5. Borrado y destrucción [mp.si.5] del Anexo II queda como sigue:

«5.5.5 Borrado y destrucción [mp.si.5].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	+	=

La medida de borrado y destrucción de soportes de información se aplicará a todo tipo de equipos susceptibles de almacenar información, incluyendo medios electrónicos y no electrónicos.

Nivel BAJO

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido.

Nivel MEDIO

b) Se destruirán de forma segura los soportes, en los siguientes casos:
   1. Cuando la naturaleza del soporte no permita un borrado seguro.
   2. Cuando así lo requiera el procedimiento asociado al tipo de información contenida.

c) Se emplearán productos certificados conforme a lo establecido en [[op.pl.5]]. »

Treinta y dos. El apartado 5.7.4. Firma electrónica [mp.info.4] del Anexo II, queda como sigue:

«**5.7.4 Firma electrónica [mp.info.4].**

dimensiones	I A		
nivel	bajo	medio	Alto
	aplica	+	++

Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio.
La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema.

En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del artículo 27.

Nivel BAJO
Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

a) Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.
b) Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.
c) Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:
d) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:
    1. Certificados.
    2. Datos de verificación y validación.
e) El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2.
f) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.

Nivel ALTO
1. Se usará firma electrónica cualificada, incorporando certificados cualificados y dispositivos cualificados de creación de firma.
2. Se emplearán productos certificados conforme a lo establecido en [op.pl.5]. »

Treinta y tres. El apartado 5.7.5 Sellos de tiempo [mp.info.5] del Anexo II queda como sigue:

«5.7.5 Sellos de tiempo [mp.info.5].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO
Los sellos de tiempo prevendrán la posibilidad del repudio posterior:
1. Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
2. Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.
3. Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte.
4. Se utilizarán productos certificados (según [op.pl.5]) o servicios externos admitidos (véase [op.exp.10]).
5. Se emplearán "sellos cualificados de tiempo electrónicos" acordes con la normativa europea en la materia. »

Treinta y cuatro. El apartado 5.7.7. Copias de seguridad *(backup)* [mp.info.9] del Anexo II queda como sigue:

«**5.7.7 Copias de seguridad *(backup)* [mp.info.9].**

dimensiones	D		
Nivel	bajo	medio	alto
	aplica	=	=

Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente con una antigüedad determinada.

Estas copias poseerán el mismo nivel de seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad, según proceda, de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de seguridad deberán abarcar:

g) Información de trabajo de la organización.
h) Aplicaciones en explotación, incluyendo los sistemas operativos.
i) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
j) Claves utilizadas para preservar la confidencialidad de la información. »

Treinta y cinco. El apartado 5.8.2 Protección de servicios y aplicaciones web [mp.s.2] del Anexo II queda como sigue:

«5.8.2 Protección de servicios y aplicaciones web [mp.s.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	+

Los subsistemas dedicados a la publicación de información deberán ser protegidos frente a las amenazas que les son propias.
a) Cuando la información tenga algún tipo de control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:
1.º Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
2.º Se prevendrán ataques de manipulación de URL.
3.º Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como «cookies».
4.º Se prevendrán ataques de inyección de código.
b) Se prevendrán intentos de escalado de privilegios.
c) Se prevendrán ataques de «cross site scripting».
d) Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como «proxies» y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como «cachés».

Nivel BAJO
Se emplearán “certificados de autenticación de sitio web” acordes a la normativa europea en la materia.

Nivel ALTO
Se emplearán “certificados cualificados de autenticación del sitio web” acordes a la normativa europea en la materia. »

Treinta y seis. El apartado 5.8.4. Medios alternativos [mp.s.9] del Anexo II queda como sigue:

«5.8.4 Medios alternativos [mp.s.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Nivel ALTO

Se garantizará la existencia y disponibilidad de alternativas para prestar los servicios en el caso de que fallen los medios habituales. La prestación alternativa estará sujeta a las mismas garantías de protección que la habitual. »

Treinta y siete. Por todo ello, la tabla general del apartado 2.4 del Anexo II, queda como sigue:

«

Dimensiones				MEDIDAS DE SEGURIDAD	
Afectadas	**B**	**M**	**A**		
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	aplica	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	+	++	op.pl.2	Arquitectura de seguridad
categoría	aplica	=	=	op.pl.3	Adquisición de nuevos componentes
D	n.a.	aplica	=	op.pl.4	Dimensionamiento / Gestión de capacidades
categoría	n.a.	n.a.	aplica	op.pl.5	Componentes certificados
				op.acc	Control de acceso
A T	aplica	=	=	op.acc.1	Identificación
I C A T	aplica	=	=	op.acc.2	Requisitos de acceso
I C A T	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
I C A T	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
I C A T	aplica	+	++	op.acc.5	Mecanismo de autenticación
I C A T	aplica	+	++	op.acc.6	Acceso local (*local logon*)
I C A T	aplica	+	=	op.acc.7	Acceso remoto (*remote login*)
				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 incidentes
T	aplica	+	++	op.exp.8	Registro de la actividad de los usuarios
categoría	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidentes
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.	aplica	=	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas
				mp	**Medidas de protección**
				mp.if	Protección de 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
I A	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
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	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
I A	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	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 la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

»

Treinta y ocho. El anexo III Auditoría de la seguridad queda como sigue:
«1. Objeto de la auditoría
1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos:
a) Que 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.
b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
c) Que se han designado personas para dichos roles a la luz del principio de «separación de funciones».
d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.
1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:
a) Documentación de los procedimientos.
b) Registro de incidentes.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el Artículo 18 relativo a productos certificados.

2. Niveles de auditoría
Los niveles de auditoría que se realizan a los sistemas de información, serán los siguientes:
2.1 Auditoría a sistemas de categoría BÁSICA.
a) Los sistemas de información de categoría BÁSICA, o inferior, no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.
El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.
b) Los informes de autoevaluación serán analizados por el responsable de seguridad competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.
2.2 Auditoría a sistemas de categoría MEDIA O ALTA.
a) El informe de auditoría dictaminará sobre el grado de cumplimiento del presente real decreto, identificará sus deficiencias y sugerirá las posibles medidas correctoras o complementarias que sean necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen en que se basen las conclusiones formuladas.
b) 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.

3. Interpretación

La interpretación del presente anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en la instrucción técnica CCN-STIC correspondiente, atendiendo al espíritu y finalidad de aquellas. »

Treinta y nueve. Glosario. La definición de Gestión de incidentes queda como sigue:
« Gestión de incidentes. Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.»

Cuarenta. Anexo V Modelo de cláusula administrativa particular. Queda redactada como sigue:

«Cláusula administrativa particular.–En cumplimiento con lo dispuesto en el artículo 115.4 del Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público, y en el artículo 18 del 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, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo indicado en la medida op.pl.5 sobre componentes certificados, recogida en el apartado 4.1.5 del Anexo II del citado Real Decreto 3/2010.

Cuando estos sean empleados para el tratamiento de datos de carácter personal, el licitador incluirá, también, lo establecido en la Disposición adicional única del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.»

Disposición transitoria única.

Las entidades del ámbito de aplicación del 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, dispondrán de un plazo de veinticuatro meses para la adecuación de sus sistemas a lo dispuesto en el presente real decreto.

Disposición final

Única. Entrada en vigor. El presente real decreto entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del Estado.

…