I. DISPOSICIONES GENERALES

MINISTERIO DE LA PRESIDENCIA

1330 *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.*

I

La necesaria generalización de la sociedad de la información es subsidiaria, en gran medida, de la confianza que genere en los ciudadanos la relación a través de medios electrónicos.

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

A ello ha venido a dar respuesta el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, mediante la creación del Esquema Nacional de Seguridad, cuyo objeto es el establecimiento de los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información.

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

El Esquema Nacional de Seguridad persigue fundamentar la confianza en que los sistemas de información prestarán sus servicios y custodiarán la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas. Se desarrollará y perfeccionará en paralelo a la evolución de los servicios y a medida que vayan consolidándose los requisitos de los mismos y de las infraestructuras que lo apoyan.

Actualmente los sistemas de información de las administraciones públicas están fuertemente imbricados entre sí y con sistemas de información del sector privado: empresas y administrados. De esta manera, la seguridad tiene un nuevo reto que va más allá del aseguramiento individual de cada sistema. Es por ello que cada sistema debe tener claro su perímetro y los responsables de cada dominio de seguridad deben coordinarse efectivamente para evitar «tierras de nadie» y fracturas que pudieran dañar a la información o a los servicios prestados.

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

II

El Esquema Nacional de Seguridad tiene presentes las recomendaciones de la Unión Europea (Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001, por la que se modifica su Reglamento interno y Decisión 2001/264/CE del Consejo, de 19 de marzo de 2001, por la que se adoptan las normas de seguridad del Consejo), la situación tecnológica de las diferentes Administraciones públicas, así como

cve: BOE-A-2010-1330

los servicios electrónicos existentes en las mismas, la utilización de estándares abiertos y, de forma complementaria, estándares de uso generalizado por los ciudadanos.

Su articulación se ha realizado atendiendo a la normativa nacional sobre Administración electrónica, protección de datos de carácter personal, firma electrónica y documento nacional de identidad electrónico, Centro Criptológico Nacional, sociedad de la información, reutilización de la información en el sector público y órganos colegiados responsables de la Administración Electrónica; así como la regulación de diferentes instrumentos y servicios de la Administración, las directrices y guías de la OCDE y disposiciones nacionales e internacionales sobre normalización.

La Ley 11/2007, de 22 de junio, posibilita e inspira esta norma, a cuyo desarrollo coadyuva, en los aspectos de la seguridad de los sistemas de tecnologías de la información en las Administraciones públicas, contribuyendo al desarrollo de un instrumento efectivo que permite garantizar los derechos de los ciudadanos en la Administración electrónica.

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y sus normas de desarrollo, determinan las medidas para la protección de los datos de carácter personal. Además, aportan criterios para establecer la proporcionalidad entre las medidas de seguridad y la información a proteger.

La Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, referente legal imprescindible de cualquier regulación administrativa, determina la configuración de numerosos ámbitos de confidencialidad administrativos, diferentes a la información clasificada y a los datos de carácter personal, que necesitan ser materialmente protegidos. Asimismo determina el sustrato legal de las comunicaciones administrativas y sus requisitos jurídicos de validez y eficacia, sobre los que soportar los requerimientos tecnológicos y de seguridad necesarios para proyectar sus efectos en las comunicaciones realizadas por vía electrónica.

La Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público que determina la regulación básica del régimen jurídico aplicable a la reutilización de documentos elaborados en el sector público, que configura un ámbito excepcionado de su aplicación, en el que se encuentra la información a la que se refiere el Esquema Nacional de Seguridad.

Junto a las disposiciones indicadas, han inspirado el contenido de esta norma, documentos de la Administración en materia de seguridad electrónica, tales como los Criterios de Seguridad, Normalización y Conservación, las Guías CCN-STIC de Seguridad de los Sistemas de Información y Comunicaciones, la Metodología y herramientas de análisis y gestión de riesgos o el Esquema Nacional de Interoperabilidad, también desarrollado al amparo de lo dispuesto en la Ley 11/2007, de 22 de junio.

III

Este real decreto se limita a establecer los principios básicos y requisitos mínimos que, de acuerdo con el interés general, naturaleza y complejidad de la materia regulada, permiten una protección adecuada de la información y los servicios, lo que exige incluir el alcance y procedimiento para gestionar la seguridad electrónica de los sistemas que tratan información de las Administraciones públicas en el ámbito de la Ley 11/2007, de 22 de junio. Con ello, se logra un común denominador normativo, cuya regulación no agota todas las posibilidades de normación, y permite ser completada, mediante la regulación de los objetivos, materialmente no básicos, que podrán ser decididos por políticas legislativas territoriales.

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

cve: BOE-A-2010-1330

La norma se estructura en diez capítulos, cuatro disposiciones adicionales, una disposición transitoria, una disposición derogatoria y tres disposiciones finales. A los cuatro primeros anexos dedicados a la categoría de los sistemas, las medidas de seguridad, la auditoría de la seguridad, y el glosario de términos, se les une un quinto que establece un modelo de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes.

En este real decreto 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. La información tratada en los sistemas electrónicos a los que se refiere este real decreto estará protegida teniendo en cuenta los criterios establecidos en la Ley Orgánica 15/1999, de 13 de diciembre.

El presente real decreto se aprueba en aplicación de lo dispuesto en la disposición final octava de la Ley 11/2007, de 22 de junio y, de acuerdo con lo dispuesto en el artículo 42 apartado 3 y disposición final primera de dicha norma, se ha elaborado con la participación de todas las Administraciones públicas a las que les es de aplicación, ha sido informado favorablemente por la Comisión Permanente del Consejo Superior de Administración Electrónica, la Conferencia Sectorial de Administración Pública y la Comisión Nacional de Administración Local; y ha sido sometido al previo informe de la Agencia Española de Protección de Datos. Asimismo, se ha sometido a la audiencia de los ciudadanos según las previsiones establecidas en el artículo 24 de la Ley 50/1997, de 27 de noviembre, del Gobierno.

En su virtud, a propuesta de la Ministra de la Presidencia, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día 8 de enero de 2010,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad establecido en el artículo 42 de la Ley 11/2007, de 22 de junio, y determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada ley.

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

Artículo 2. *Definiciones y estándares.*

A los efectos previstos en este real decreto, las definiciones, palabras, expresiones y términos han de ser entendidos en el sentido indicado en el Glosario de Términos incluido en el anexo IV.

Artículo 3. *Ámbito de aplicación.*

El ámbito de aplicación del presente real decreto será el establecido en el artículo 2 de la Ley 11/2007, de 22 de junio.

cve: BOE-A-2010-1330

Están excluidos del ámbito de aplicación indicado en el párrafo anterior los sistemas que tratan información clasificada regulada por Ley 9/1968, de 5 de abril, de Secretos Oficiales y normas de desarrollo.

CAPÍTULO II

Principios básicos

Artículo 4. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. En las decisiones en materia de seguridad deberán tenerse en cuenta los siguientes principios básicos:

a) Seguridad integral.
b) Gestión de riesgos.
c) Prevención, reacción y recuperación.
d) Líneas de defensa.
e) Reevaluación periódica.
f) Función diferenciada.

Artículo 5. *La seguridad como un proceso integral.*

1. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema. La aplicación del Esquema Nacional de Seguridad estará presidida por este principio, que excluye cualquier actuación puntual o tratamiento coyuntural.
2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Artículo 6. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

Artículo 7. *Prevención, reacción y recuperación.*

1. La seguridad del sistema debe contemplar los aspectos de prevención, detección y corrección, para conseguir que las amenazas sobre el mismo no se materialicen, no afecten gravemente a la información que maneja, o los servicios que se prestan.
2. 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.
3. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo.
4. 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.
5. Sin merma de los demás principios básicos y requisitos mínimos establecidos, el sistema garantizará la conservación de los datos e informaciones en soporte electrónico.

cve: BOE-A-2010-1330

De igual modo, el sistema mantendrá disponibles los servicios durante todo el ciclo vital de la información digital, a través de una concepción y procedimientos que sean la base para la preservación del patrimonio digital.

Artículo 8. *Líneas de defensa.*

1. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuesta de forma que, cuando una de las capas falle, permita:

a) Ganar tiempo para una reacción adecuada frente a los incidentes que no han podido evitarse.
b) Reducir la probabilidad de que el sistema sea comprometido en su conjunto.
c) Minimizar el impacto final sobre el mismo.

2. Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

Artículo 9. *Reevaluación periódica.*

Las medidas de seguridad se reevaluarán 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.

Artículo 10. *La seguridad como función diferenciada.*

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

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

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

CAPÍTULO III

Requisitos mínimos

Artículo 11. *Requisitos mínimos de seguridad.*

1. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente. Esta política de seguridad, se establecerá en base a los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.

cve: BOE-A-2010-1330

l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

2. A los efectos indicados en el apartado anterior, se considerarán órganos superiores, los responsables directos de la ejecución de la acción del gobierno, central, autonómico o local, en un sector de actividad específico, de acuerdo con lo establecido en la Ley 6/1997, de 14 de abril, de organización y funcionamiento de la Administración General del Estado y Ley 50/1997, de 27 de noviembre, del Gobierno; los estatutos de autonomía correspondientes y normas de desarrollo; y la Ley 7/1985, de 2 de abril, reguladora de las bases del Régimen Local, respectivamente.

Los municipios podrán disponer de una política de seguridad común elaborada por la Diputación, Cabildo, Consejo Insular u órgano unipersonal correspondiente de aquellas otras corporaciones de carácter representativo a las que corresponda el gobierno y la administración autónoma de la provincia o, en su caso, a la entidad comarcal correspondiente a la que pertenezcan.

3. Todos estos requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, pudiendo algunos no requerirse en sistemas sin riesgos significativos, y se cumplirán de acuerdo con lo establecido en el artículo 27.

Artículo 12. *Organización e implantación del proceso de seguridad.*

La seguridad deberá comprometer a todos los miembros de la organización. La política de seguridad según se detalla en el anexo II, sección 3.1, deberá identificar unos claros responsables de velar por su cumplimiento y ser conocida por todos los miembros de la organización administrativa.

Artículo 13. *Análisis y gestión de los riesgos.*

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

2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.

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

Artículo 14. *Gestión de personal.*

1. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad. Sus actuaciones deben ser supervisadas para verificar que se siguen los procedimientos establecidos.

2. El personal relacionado con la información y los sistemas, ejercitará y aplicará los principios de seguridad en el desempeño de su cometido.

3. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad.

4. Para corregir, o exigir responsabilidades en su caso, cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

Artículo 15. *Profesionalidad.*

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 incidencias y desmantelamiento.

cve: BOE-A-2010-1330

2. El personal de las Administraciones públicas recibirá la formación específica necesaria para garantizar la seguridad de las tecnologías de la información aplicables a los sistemas y servicios de la Administración.

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.

Artículo 16. *Autorización y 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.

Artículo 17. *Protección de las instalaciones.*

Los sistemas se instalarán en áreas separadas, dotadas de un procedimiento de control de acceso. Como mínimo, las salas deben estar cerradas y disponer de un control de llaves.

Artículo 18. *Adquisición de productos de seguridad.*

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 valorarán positivamente aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. La certificación indicada en el apartado anterior deberá estar de acuerdo con las normas y estándares de mayor reconocimiento internacional, en el ámbito de la seguridad funcional.

3. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información, constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, y regulado por la orden PRE/2740/2007, de 19 de septiembre, dentro de sus competencias, determinará el criterio a cumplir en función del uso previsto del producto a que se refiera, en relación con el nivel de evaluación, otras certificaciones de seguridad adicionales que se requieran normativamente, así como, excepcionalmente, en los casos en que no existan productos certificados. El proceso indicado, se efectuará teniendo en cuenta los criterios y metodologías de evaluación, determinados por las normas internacionales que recoge la orden ministerial citada.

Artículo 19. *Seguridad por defecto.*

Los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.

b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

c) En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés, sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

d) El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

Artículo 20. *Integridad y actualización del sistema.*

1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.

cve: BOE-A-2010-1330

2. 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.

Artículo 21. *Protección de información almacenada y en tránsito.*

1. En la estructura y organización de la seguridad del sistema, 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.

2. Forman parte de la seguridad los procedimientos que aseguren la recuperación y conservación a largo plazo de los documentos electrónicos producidos por las Administraciones públicas en el ámbito de sus competencias.

3. Toda información en soporte no electrónico, que haya sido causa o consecuencia directa de la información electrónica a la que se refiere el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello se aplicarán las medidas que correspondan a la naturaleza del soporte en que se encuentren, de conformidad con las normas de aplicación a la seguridad de los mismos.

Artículo 22. *Prevención ante otros sistemas de información interconectados.*

El sistema ha de proteger el perímetro, en particular, si se conecta a redes públicas. Se entenderá por red pública de comunicaciones la red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público, de conformidad a la definición establecida en el apartado 26 del anexo II, de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

Artículo 23. *Registro de actividad.*

Con la finalidad exclusiva de lograr el cumplimiento del objeto del presente real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, 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.

Artículo 24. *Incidentes de seguridad.*

1. Se establecerá un sistema de detección y reacción frente a código dañino.

2. 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.

Artículo 25. *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.

Artículo 26. *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.

cve: BOE-A-2010-1330

Artículo 27. *Cumplimiento de requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las Administraciones públicas aplicarán las medidas de seguridad indicadas en el Anexo II, teniendo en cuenta:

a) Los activos que constituyen el sistema.
b) La categoría del sistema, según lo previsto en el artículo 43.
c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Cuando un sistema al que afecte el presente real decreto 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.

3. Los medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados por causa de la concurrencia indicada o del prudente arbitrio del responsable de la información, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos.

Artículo 28. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el presente real decreto en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración.

Artículo 29. *Guías de seguridad.*

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.

Artículo 30. *Sistemas de información no afectados.*

Las Administraciones públicas podrán determinar aquellos sistemas de información a los que no les sea de aplicación lo dispuesto en el presente de real decreto por tratarse de sistemas no relacionados con el ejercicio de derechos ni con el cumplimiento de deberes por medios electrónicos ni con el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, de acuerdo con lo previsto en la Ley 11/2007, de 22 de junio.

CAPÍTULO IV

Comunicaciones electrónicas

Artículo 31. *Condiciones técnicas de seguridad de las comunicaciones electrónicas.*

1. Las condiciones técnicas de seguridad de las comunicaciones electrónicas en lo relativo a la constancia de la transmisión y recepción, de sus fechas, del contenido integro de las comunicaciones y la identificación fidedigna del remitente y destinatario de las mismas, según lo establecido en la Ley 11/2007, de 22 de junio, serán implementadas de acuerdo con lo establecido en el Esquema Nacional de Seguridad.

2. Las comunicaciones realizadas en los términos indicados en el apartado anterior, tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que resulte de aplicación.

cve: BOE-A-2010-1330

Artículo 32. *Requerimientos técnicos de notificaciones y publicaciones electrónicas.*

1. Las notificaciones y publicaciones electrónicas de resoluciones y actos administrativos se realizarán de forma que cumplan, de acuerdo con lo establecido en el presente real decreto, las siguientes exigencias técnicas:

a) Aseguren la autenticidad del organismo que lo publique.
b) Aseguren la integridad de la información publicada.
c) Dejen constancia de la fecha y hora de la puesta a disposición del interesado de la resolución o acto objeto de publicación o notificación, así como del acceso a su contenido.
d) Aseguren la autenticidad del destinatario de la publicación o notificación.

Artículo 33. *Firma electrónica.*

1. Los mecanismos de firma electrónica se aplicarán en los términos indicados en el Anexo II de esta norma y de acuerdo con lo preceptuado en la política de firma electrónica y de certificados, según se establece en el Esquema Nacional de Interoperabilidad.
2. La política de firma electrónica y de certificados concretará los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas, sin perjuicio de lo previsto en el Anexo II, que deberá adaptarse a cada circunstancia.

CAPÍTULO V

Auditoría de la seguridad

Artículo 34. *Auditoría de la seguridad.*

1. Los sistemas de información a los que se refiere el presente real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del presente Esquema Nacional de Seguridad.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en el sistema de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoria extraordinaria determinará la fecha de cómputo para el cálculo de los dos años, establecidos para la realización de la siguiente auditoría regular ordinaria, indicados en el párrafo anterior.

2. Esta auditoría se realizará en función de la categoría del sistema, determinada según lo dispuesto en el anexo I y de acuerdo con lo previsto en el anexo III.
3. En el marco de lo dispuesto en el artículo 39, de la ley 11/2007, de 22 de junio, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante, dentro del alcance establecido para la auditoría.
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.
5. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto, identificar sus deficiencias y sugerir las posibles medidas correctoras o complementarias 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 las conclusiones formuladas.
6. Los informes de auditoría serán presentados al responsable del sistema y al responsable de seguridad competentes. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

cve: BOE-A-2010-1330

7. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.

8. Los informes de auditoría podrán ser requeridos por los responsables de cada organización con competencias sobre seguridad de las tecnologías de la información.

CAPITULO VI

Estado de seguridad de los sistemas

Artículo 35. *Informe del estado de la 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 presente real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las Administraciones públicas.

CAPÍTULO VII

Respuesta a incidentes de seguridad

Artículo 36. *Capacidad de respuesta a incidentes de seguridad de la información.*

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Artículo 37. *Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.*

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

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 los informes de auditoría de los sistemas afectados.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.

c) Formación destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de

cve: BOE-A-2010-1330

conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

d) Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN 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, y en el que, aquél, será coordinador a nivel público estatal.

CAPÍTULO VIII

Normas de conformidad

Artículo 38. *Sedes y registros electrónicos.*

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.

Artículo 39. *Ciclo de vida de servicios y sistemas.*

Las especificaciones de seguridad se incluirán en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

Artículo 40. *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.

Artículo 41. *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.

CAPÍTULO IX

Actualización

Artículo 42. *Actualización permanente.*

El Esquema Nacional de Seguridad se deberá mantener actualizado de manera permanente. Se desarrollará y perfeccionará a lo largo del tiempo, en paralelo al progreso de los servicios de Administración electrónica, de la evolución tecnológica y nuevos estándares internacionales sobre seguridad y auditoría en los sistemas y tecnologías de la información y a medida que vayan consolidándose las infraestructuras que le apoyan.

cve: BOE-A-2010-1330

CAPÍTULO X

Categorización de los sistemas de información

Artículo 43. *Categorías.*

1. 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 criterio del principio de proporcionalidad.

2. La determinación de la categoría indicada en el apartado anterior se efectuará en función de la valoración del impacto que tendría un incidente que afectara a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I.

3. La valoración de las consecuencias de un impacto negativo sobre la seguridad de la información y de los servicios se efectuará atendiendo a su 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.

Artículo 44. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 43, así como la modificación posterior, en su caso, corresponderá, dentro del ámbito de su actividad, al responsable de cada información o servicio.

2. La facultad para determinar la categoría del sistema corresponderá al responsable del mismo.

Disposición adicional primera. *Formación.*

El personal de las Administraciones públicas recibirá, de acuerdo con lo previsto en la disposición adicional segunda de la Ley 11/2007, de 22 de junio, la formación necesaria para garantizar el conocimiento del presente Esquema Nacional de Seguridad, a cuyo fin los órganos responsables dispondrán lo necesario para que la formación sea una realidad efectiva.

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

El Instituto Nacional de Tecnologías de la Comunicación (INTECO), como centro de excelencia promovido por el Ministerio de Industria, Turismo y Comercio para el desarrollo de la sociedad del conocimiento, podrá desarrollar proyectos de innovación y programas de investigación dirigidos a la mejor implantación de las medidas de seguridad contempladas en el presente real decreto.

Asimismo, las Administraciones públicas podrán disponer de entidades análogas para llevar a cabo dichas actividades u otras adicionales en el ámbito de sus competencias.

Disposición adicional tercera. *Comité de Seguridad de la Información de las Administraciones Públicas.*

El Comité de Seguridad de la Información de las Administraciones Públicas, dependiente del Comité Sectorial de Administración electrónica, contará con un representante de cada una de las entidades presentes en dicho Comité Sectorial. Tendrá funciones de cooperación en materias comunes relacionadas con la adecuación e implantación de lo previsto en el Esquema Nacional de Seguridad y en las normas, instrucciones, guías y recomendaciones dictadas para su aplicación.

cve: BOE-A-2010-1330

Disposición adicional cuarta. *Modificación del Reglamento de desarrollo de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.*

Se modifica la letra b) del apartado 5 del artículo 81 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal aprobado por Real Decreto 1720/2007, de 21 de diciembre, que pasa a tener la siguiente redacción:

«b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.»

Disposición transitoria. *Adecuación de sistemas.*

1. Los sistemas existentes a la entrada en vigor del presente real decreto se adecuarán 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. Los nuevos sistemas aplicarán lo establecido en el presente real decreto desde su concepción.
2. 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, se dispondrá de un plan de adecuación que marque los plazos de ejecución los cuales, en ningún caso, serán superiores a 48 meses desde la entrada en vigor.

El plan indicado en el párrafo anterior será elaborado con la antelación suficiente y aprobado por los órganos superiores competentes.

3. Mientras no se haya aprobado una política de seguridad por el órgano superior competente serán de aplicación las políticas de seguridad que puedan existir a nivel de órgano directivo.

Disposición derogatoria única.

Quedan derogadas las disposiciones de igual o inferior rango que se opongan a lo dispuesto en el presente reglamento.

Disposición final primera. *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en el artículo 149.1.18.ª de la Constitución, que atribuye al Estado la competencia sobre las bases del régimen jurídico de las Administraciones públicas.

Disposición final segunda. *Desarrollo normativo.*

Se autoriza al titular del Ministerio de la Presidencia, para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

Disposición final tercera. *Entrada en vigor.*

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

Dado en Madrid, el 8 de enero de 2010.

JUAN CARLOS R.

La Vicepresidenta Primera del Gobierno
y Ministra de la Presidencia,
MARÍA TERESA FERNÁNDEZ DE LA VEGA SANZ

cve: BOE-A-2010-1330

ANEXOS

ANEXO I

Categorías de los sistemas

1. Fundamentos para la determinación de la categoría de un sistema.

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 sistemas, con repercusión en la capacidad organizativa para:

a) Alcanzar sus objetivos.
b) Proteger los activos a su cargo.
c) Cumplir sus obligaciones diarias de servicio.
d) Respetar la legalidad vigente.
e) Respetar los derechos de las personas.

La determinación de la categoría de un sistema se realizará de acuerdo con lo establecido en el presente real decreto, y será de aplicación a todos los sistemas empleados para la prestación de los servicios de la Administración electrónica y soporte del procedimiento administrativo general.

2. Dimensiones de la seguridad.

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

a) Disponibilidad [D].
b) Autenticidad [A].
c) Integridad [I].
d) Confidencialidad [C].
e) Trazabilidad [T].

3. Determinación del nivel requerido en una dimensión de seguridad.

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.

a) Nivel BAJO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio limitado sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.
Se entenderá por perjuicio limitado:

1.º La reducción de forma apreciable de la capacidad de la organización para atender eficazmente con sus obligaciones corrientes, aunque estas sigan desempeñándose.
2.º El sufrimiento de un daño menor por los activos de la organización.
3.º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.
4.º Causar un perjuicio menor a algún individuo, que aún siendo molesto pueda ser fácilmente reparable.
5.º Otros de naturaleza análoga.

cve: BOE-A-2010-1330

b) Nivel MEDIO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio grave:

1.º La reducción significativa la capacidad de la organización para atender eficazmente a sus obligaciones fundamentales, aunque estas sigan desempeñándose.
2.º El sufrimiento de un daño significativo por los activos de la organización.
3.º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.
4.º Causar un perjuicio significativo a algún individuo, de difícil reparación.
5.º Otros de naturaleza análoga.

c) Nivel ALTO. Se utilizará cuando las consecuencias de un incidente de seguridad que afecte a alguna de las dimensiones de seguridad supongan un perjuicio muy grave sobre las funciones de la organización, sobre sus activos o sobre los individuos afectados.

Se entenderá por perjuicio muy grave:

1.º La anulación de la capacidad de la organización para atender a alguna de sus obligaciones fundamentales y que éstas sigan desempeñándose.
2.º El sufrimiento de un daño muy grave, e incluso irreparable, por los activos de la organización.
3.º El incumplimiento grave de alguna ley o regulación.
4.º Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.
5.º Otros de naturaleza análoga.

Cuando un sistema maneje diferentes informaciones y preste diferentes servicios, el nivel del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

4. Determinación de la categoría de un sistema de información.

1. Se definen tres categorías: BÁSICA, MEDIA y ALTA.

a) Un sistema de información será de categoría ALTA si alguna de sus dimensiones de seguridad alcanza el nivel ALTO.
b) 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.
c) 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.

2. La determinación de la categoría de un sistema sobre la base de lo indicado en el apartado anterior no implicará que se altere, por este hecho, el nivel de las dimensiones de seguridad que no han influido en la determinación de la categoría del mismo.

5. Secuencia de actuaciones para determinar la categoría de un sistema:

1. Identificación del nivel correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3.
2. Determinación de la categoría del sistema, según lo establecido en el apartado 4.

cve: BOE-A-2010-1330

ANEXO II

Medidas de seguridad

1. Disposiciones generales

1. Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplicarán las medidas de seguridad indicadas en este anexo, las cuales serán proporcionales a:

a) Las dimensiones de seguridad relevantes en el sistema a proteger.
b) La categoría del sistema de información a proteger.

2. Las medidas de seguridad se dividen en tres grupos:

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

2. Selección de medidas de seguridad

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

a) Identificación de los tipos de activos presentes.

b) Determinación de las dimensiones de seguridad relevantes, teniendo en cuenta lo establecido en el anexo I.
c) Determinación del nivel correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
d) Determinación de la categoría del sistema, según lo establecido en el Anexo I.
e) Selección de las medidas de seguridad apropiadas de entre las contenidas en este Anexo, de acuerdo con las dimensiones de seguridad y sus niveles, y, para determinadas medidas de seguridad, de acuerdo con la categoría del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan sistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse la información y los servicios afectados.
3. La relación de medidas seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad del sistema.
4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad, es la que se indica en la tabla siguiente:

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	n.a.	+	++	op.pl.1	Análisis de riesgos
categoría	aplica	=	=	op.pl.2	Arquitectura de seguridad

cve: BOE-A-2010-1330

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 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

				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

cve: BOE-A-2010-1330

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	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
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	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 la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

En las tablas del presente Anexo se emplean las siguientes convenciones:

a) 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».

b) «n.a.» significa «no aplica».

c) Para indicar que las exigencias de un nivel son iguales a los del nivel inferior se utiliza el signo «=».

d) Para indicar el incremento de exigencias graduado en función de del nivel de la dimensión de seguridad, se utilizan los signos «+» y «++».

e) Para indicar que una medida protege específicamente una cierta dimensión de seguridad, ésta se explicita mediante su inicial.

3. **Marco organizativo [org]**

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad.

3.1 Política de seguridad [org.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

cve: BOE-A-2010-1330

La política de seguridad será aprobada por el órgano superior competente que corresponda, de acuerdo con lo establecido en el artículo 11, y se plasmará en un documento escrito, en el que, de forma clara, se precise, al menos, lo siguiente:

a) Los objetivos o misión de la organización.
b) El marco legal y regulatorio en el que se desarrollarán las actividades.
c) 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.
d) 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.
e) Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

La política de seguridad debe referenciar y ser coherente con lo establecido en el Documento de Seguridad que exige el Real Decreto 1720/2007, en lo que corresponda.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se dispondrá de una serie de documentos que describan:

a) El uso correcto de equipos, servicios e instalaciones.
b) Lo que se considerará uso indebido.
c) La responsabilidad del personal con respecto al cumplimiento o violación de estas normas: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se dispondrá de una serie de documentos que detallen de forma clara y precisa:

a) Cómo llevar a cabo las tareas habituales.
b) Quién debe hacer cada tarea.
c) Cómo identificar y reportar comportamientos anómalos.

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.

cve: BOE-A-2010-1330

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.

4. **Marco operacional [op]**

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Bastará un análisis informal, realizado en lenguaje natural. Es decir, una exposición textual que describa los siguientes aspectos:

a) Identifique los activos más valiosos del sistema.
b) Identifique las amenazas más probables.
c) Identifique las salvaguardas que protegen de dichas amenazas.
d) Identifique los principales riesgos residuales.

Categoría MEDIA

Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:

a) Identifique y valore cualitativamente los activos más valiosos del sistema.
b) Identifique y cuantifique las amenazas más probables.
c) Identifique y valore las salvaguardas que protegen de dichas amenazas.
d) Identifique y valore el riesgo residual.

Categoría ALTA

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

a) Identifique y valore cualitativamente los activos más valiosos del sistema.
b) Identifique y cuantifique las amenazas posibles.
c) Identifique las vulnerabilidades habilitantes de dichas amenazas.
d) Identifique y valore las salvaguardas adecuadas.
e) Identifique y valore el riesgo residual.

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

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

cve: BOE-A-2010-1330

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

a) Documentación de las instalaciones:

1.º Áreas.
2.º Puntos de acceso.

b) Documentación del sistema:

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

c) Esquema de líneas de defensa:

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

d) Sistema de identificación y autenticación de usuarios:

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

e) Controles técnicos internos:

1.º Validación de datos de entrada, salida y datos intermedios.

f) Sistema de gestión con actualización y aprobación periódica.

4.1.3 Adquisición de nuevos componentes [op.pl.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se establecerá un proceso formal para planificar la adquisición de nuevos componentes del sistema, proceso que:

a) Atenderá a las conclusiones del análisis de riesgos: [op.pl.1].
b) Será acorde a la arquitectura de seguridad escogida: [op.pl.2].
c) Contemplará las necesidades técnicas, de formación y de financiación de forma conjunta.

4.1.4 Dimensionamiento / gestión de capacidades [op.pl.4].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Con carácter previo a la puesta en explotación, se realizará un estudio previo que cubrirá los siguientes aspectos:

cve: BOE-A-2010-1330

a) Necesidades de procesamiento.
b) Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
d) Necesidades de comunicación.
e) Necesidades de personal: cantidad y cualificación profesional.
f) Necesidades de instalaciones y medios auxiliares.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

Se utilizarán preferentemente sistemas, productos o equipos cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y que estén certificados por entidades independientes de reconocida solvencia.

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.

4.2 Control de acceso. [op.acc].

El control de acceso cubre el conjunto de actividades preparatorias y ejecutivas para que una determinada entidad, usuario o proceso, pueda, o no, acceder a un recurso del sistema para realizar una determinada acción.

El control de acceso que se implante en un sistema real será un punto de equilibrio entre la comodidad de uso y la protección de la información. En sistemas de nivel Bajo, se primará la comodidad, mientras que en sistemas de nivel Alto se primará la protección.

En todo control de acceso se requerirá lo siguiente:

a) Que todo acceso esté prohibido, salvo concesión expresa.
b) Que la entidad quede identificada singularmente [op.acc.1].
c) Que la utilización de los recursos esté protegida [op.acc.2].
d) Que se definan para cada entidad los siguientes parámetros: a qué se necesita acceder, con qué derechos y bajo qué autorización [op.acc.4].
e) Serán diferentes las personas que autorizan, usan y controlan el uso [op.acc.3].
f) Que la identidad de la entidad quede suficientemente autenticada [mp.acc.5].
g) Que se controle tanto el acceso local ([op.acc.6]) como el acceso remoto ([op.acc.7]).

Con el cumplimiento de todas las medidas indicadas se garantizará que nadie accederá a recursos sin autorización. Además, quedará registrado el uso del sistema ([op.exp.8]) para poder detectar y reaccionar a cualquier fallo accidental o deliberado.

Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, en los casos en que sea necesario, las medidas de seguridad locales se acompañarán de los correspondientes acuerdos de colaboración que delimiten mecanismos y procedimientos para la atribución y ejercicio efectivos de las responsabilidades de cada sistema ([op.ext]).

4.2.1 Identificación [op.acc.1].

dimensiones	A T		
nivel	bajo	medio	alto
	aplica	=	=

cve: BOE-A-2010-1330

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:

1.º Se puede saber quién recibe y qué derechos de acceso recibe.
2.º Se puede saber quién ha hecho algo y qué ha hecho.

b) Las cuentas de usuario se gestionarán de la siguiente forma:

1.º Cada cuenta estará asociada a un identificador único.
2.º 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.
3.º 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.

4.2.2 Requisitos de acceso [op.acc.2].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	=	=

Los requisitos de acceso se atenderán a lo que a continuación se indica:

a) Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.
b) Los derechos de acceso de cada recurso, se establecerán según las decisiones de la persona responsable del recurso, ateniéndose a la política y normativa de seguridad del sistema.
c) Particularmente se controlará el acceso a los componentes del sistema y a sus ficheros o registros de configuración.

4.2.3 Segregación de funciones y tareas [op.acc.3].

dimensiones	I C A T		
nivel	bajo	medio	alto
	no aplica	aplica	=

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos para cometer alguna acción ilícita.
En concreto, se separarán al menos las siguientes funciones:

a) Desarrollo de operación.
b) Configuración y mantenimiento del sistema de operación.
c) Auditoría o supervisión de cualquier otra función.

4.2.4 Proceso de gestión de derechos de acceso [op.acc.4].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	=	=

cve: BOE-A-2010-1330

Los derechos de acceso de cada usuario, se limitarán atendiendo a los siguientes principios:

a) Mínimo privilegio. Los privilegios de cada usuario se reducirán al mínimo estrictamente necesario para cumplir sus obligaciones. De esta forma se acotan los daños que pudiera causar una entidad, de forma accidental o intencionada.
b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.
c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello, podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos por su propietario.

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

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen.
Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados a cada nivel.

Nivel BAJO

a) Se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, o dispositivos físicos (en expresión inglesa »tokens») o componentes lógicos tales como certificados software u otros equivalentes o mecanismos biométricos.
b) En el caso de usar contraseñas se aplicarán reglas básicas de calidad de las mismas.
c) Se atenderá a la seguridad de los autenticadores de forma que:

1.º Los autenticadores se activarán una vez estén bajo el control efectivo del usuario.
2.º Los autenticadores estarán bajo el control exclusivo del usuario.
3.º El usuario reconocerá que los 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.º Los autenticadores se cambiarán con una periodicidad marcada por la política de la organización, atendiendo a la categoría del sistema al que se accede.
5.º Los autenticadores se retirarán y serán deshabilitados cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.

Nivel MEDIO

a) No se recomendará el uso de claves concertadas.
b) Se recomendará el uso de otro tipo de mecanismos del tipo dispositivos físicos (tokens) o componentes lógicos tales como certificados software u otros equivalentes o biométricos.
c) En el caso de usar contraseñas se aplicarán políticas rigurosas de calidad de la contraseña y renovación frecuente.

Nivel ALTO

a) Los autenticadores se suspenderán tras un periodo definido de no utilización.
b) No se admitirá el uso de claves concertadas.

cve: BOE-A-2010-1330

c) Se exigirá el uso de dispositivos físicos (tokens) personalizados o biometría.
d) En el caso de utilización de dispositivos físicos (tokens) se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
e) Se emplearán, preferentemente, productos certificados [op.pl.5].

Tabla resumen de mecanismos de autenticación admisibles

		Nivel		
		BAJO	MEDIO	ALTO
algo que se sabe	claves concertadas	sí	Con cautela	no
algo que se tiene	Tokens	si	sí	criptográficos
algo que se es	Biometría	sí	sí	+ doble factor

4.2.6 Acceso local [op.acc.6].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	++

Se considera acceso local al realizado desde puestos de trabajo dentro de las propias instalaciones de la organización. Estos accesos tendrán en cuenta el nivel de las dimensiones de seguridad:

Nivel BAJO

a) Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo. La información revelada a quien intenta acceder, debe ser la mínima imprescindible (los diálogos de acceso proporcionarán solamente la información indispensable).
b) El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez efectuados un cierto número de fallos consecutivos.
c) Se registrarán los accesos con éxito, y los fallidos.
d) El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

Nivel MEDIO

Se informará al usuario del último acceso efectuado con su identidad.

Nivel ALTO

a) El acceso estará limitado por horario, fechas y lugar desde donde se accede.
b) Se definirán aquellos puntos en los que el sistema requerirá una renovación de la autenticación del usuario, mediante identificación singular, no bastando con la sesión establecida.

4.2.7 Acceso remoto [op.acc.7].

dimensiones	I C A T		
nivel	bajo	medio	alto
	aplica	+	=

cve: BOE-A-2010-1330

Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros.

Se garantizará la seguridad del sistema cuando accedan remotamente usuarios u otras entidades, lo que implicará proteger tanto el acceso en sí mismo (como [op.acc.6]) como el canal de acceso remoto (como en [mp.com.2] y [mp.com.3]).

Nivel MEDIO

Se establecerá una política específica de lo que puede hacerse remotamente, requiriéndose autorización positiva.

4.3 Explotación [op.exp].

4.3.1 Inventario de activos [op.exp.1].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su propietario; es decir, la persona que es responsable de las decisiones relativas al mismo.

4.3.2 Configuración de seguridad [op.exp.2].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	=	=

Se configurarán los equipos previamente a su entrada en operación, de forma que:

a) Se retiren cuentas y contraseñas estándar.
b) Se aplicará la regla de «mínima funcionalidad»:

1.º El sistema debe proporcionar la funcionalidad requerida para que la organización alcance sus objetivos y ninguna otra funcionalidad,
2.º No proporcionará funciones gratuitas, ni de operación, ni de administración, ni de auditoría, reduciendo de esta forma su perímetro al mínimo imprescindible.
3.º Se eliminará o desactivará mediante el control de la configuración, aquellas funciones que no sean de interés, no sean necesarias, e incluso, aquellas que sean inadecuadas al fin que se persigue.

c) Se aplicará la regla de «seguridad por defecto»:

1.º Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.
2.º Para reducir la seguridad, el usuario tiene que realizar acciones conscientes.
3.º El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

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

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

cve: BOE-A-2010-1330

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 incidencias (ver [op.exp.7]).

4.3.4 Mantenimiento [op.exp.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Para mantener el equipamiento físico y lógico que constituye el sistema, se aplicará lo siguiente:

a) Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas.
b) Se efectuará un seguimiento continuo de los anuncios de defectos.
c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Se mantendrá un control continuo de cambios realizados en el sistema, de forma que:

a) Todos los cambios anunciados por el fabricante o proveedor serán analizados para determinar su conveniencia para ser incorporados, o no.
b) Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario. El equipo de pruebas será equivalente al de producción en los aspectos que se comprueban.
c) Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados.
d) Mediante análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel alto serán aprobados explícitamente de forma previa a su implantación.

4.3.6 Protección frente a código dañino [op.exp.6].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

cve: BOE-A-2010-1330

Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como «spyware», y en general, todo lo conocido como «malware».

Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

4.3.7 Gestión de incidencias [op.exp.7].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

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.º Prevenir que se repita el incidente.

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

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

La gestión de incidentes que afecten a datos de carácter personal tendrá en cuenta lo dispuesto en el Real Decreto 1720 de 2007, en lo que corresponda.

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

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

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

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

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

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

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

4.3.9 Registro de la gestión de incidencias [op.exp.9].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

cve: BOE-A-2010-1330

Se registrarán todas las actuaciones relacionadas con la gestión de incidencias, 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 las incidencias, se revisará la determinación de los eventos auditables.

4.3.10 Protección de los registros de actividad [op.exp.10].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Se protegerán los registros del sistema, de forma que:

a) Se determinará el periodo de retención de los registros.
b) Se asegurará la fecha y hora. Ver [mp.info.5].
c) Los registros no podrán ser modificados ni eliminados por personal no autorizado.
d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

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

4.4 Servicios externos [op.ext].

Cuando se utilicen recursos externos a la organización, sean servicios, equipos, instalaciones o personal, deberá tenerse en cuenta que la delegación se limita a las funciones.

La organización sigue siendo en todo momento responsable de los riesgos en que se incurre en la medida en que impacten sobre la información manejada y los servicios finales prestados por la organización.

La organización dispondrá las medidas necesarias para poder ejercer su responsabilidad y mantener el control en todo momento.

cve: BOE-A-2010-1330

4.4.1 Contratación y acuerdos de nivel de servicio [op.ext.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

Previa a la utilización de recursos externos se establecerán contractualmente las características del servicio prestado y las responsabilidades de las partes. Se detallará lo que se considera calidad mínima del servicio prestado y las consecuencias de su incumplimiento.

4.4.2 Gestión diaria [op.ext.2].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

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 incidencias y desastres (ver [op.exp.7]).

4.4.3 Medios alternativos [op.ext.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Estará prevista la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio contratado. El servicio alternativo disfrutará de las mismas garantías de seguridad que el servicio habitual.

4.5 Continuidad del servicio [op.cont].

4.5.1 Análisis de impacto [op.cont.1].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Se realizará un análisis de impacto que permita determinar:

a) Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo.
b) Los elementos que son críticos para la prestación de cada servicio.

cve: BOE-A-2010-1330

4.5.2 Plan de continuidad [op.cont.2].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Este plan contemplará los siguientes aspectos:

a) Se identificarán funciones, responsabilidades y actividades a realizar.
b) Existirá una previsión de los medios alternativos que se va a conjugar para poder seguir prestando los servicios.
c) Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
d) Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
e) El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

4.5.3 Pruebas periódicas [op.cont.3].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Se realizarán pruebas periódicas para localizar y, corregir en su caso, los errores o deficiencias que puedan existir en el plan de continuidad

4.6 Monitorización del sistema [op.mon].

El sistema estará sujeto a medidas de monitorización de su actividad.

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

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

Se dispondrán de herramientas de detección o de prevención de intrusión.

4.6.2 Sistema de métricas [op.mon.2].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

Se establecerá un conjunto de indicadores que mida el desempeño real del sistema en materia de seguridad, en los siguientes aspectos:

a) Grado de implantación de las medidas de seguridad.
b) Eficacia y eficiencia de las medidas de seguridad.
c) Impacto de los incidentes de seguridad.

cve: BOE-A-2010-1330

5. Medidas de protección [mp]

Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

5.1 Protección de las instalaciones e infraestructuras [mp.if].

5.1.1 Áreas separadas y con control de acceso [mp.if.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El equipamiento de instalará en áreas separadas específicas para su función.
Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas y vigiladas.

5.1.2 Identificación de las personas [mp.if.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El mecanismo de control de acceso se atendrá a lo que se dispone a continuación:

a) Se identificará a todas las personas que accedan a los locales donde hay equipamiento que forme parte del sistema de información.
b) Se registrarán las entradas y salidas de personas.

5.1.3 Acondicionamiento de los locales [mp.if.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Los locales donde se ubiquen los sistemas de información y sus componentes, dispondrán de elementos adecuados para el eficaz funcionamiento del equipamiento allí instalado. Y, en especial:

a) Condiciones de temperatura y humedad.
b) Protección frente a las amenazas identificadas en el análisis de riesgos.
c) Protección del cableado frente a incidentes fortuitos o deliberados.

5.1.4 Energía eléctrica [mp.if.4].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	+	=

Los locales donde se ubiquen los sistemas de información y sus componentes dispondrán de la energía eléctrica, y sus tomas correspondientes, necesaria para su funcionamiento, de forma que en los mismos:

a) Se garantizará el suministro de potencia eléctrica.
b) Se garantizará el correcto funcionamiento de las luces de emergencia.

cve: BOE-A-2010-1330

Nivel MEDIO

Se garantizará el suministro eléctrico a los sistemas en caso de fallo del suministro general, garantizando el tiempo suficiente para una terminación ordenada de los procesos, salvaguardando la información.

5.1.5 Protección frente a incendios [mp.if.5].

dimensiones	D		
nivel	bajo	medio	alto
	aplica	=	=

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incendios fortuitos o deliberados, aplicando al menos la normativa industrial pertinente.

5.1.6 Protección frente a inundaciones [mp.if.6].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

Los locales donde se ubiquen los sistemas de información y sus componentes se protegerán frente a incidentes fortuitos o deliberados causados por el agua.

5.1.7 Registro de entrada y salida de equipamiento [mp.if.7].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se llevará un registro pormenorizado de toda entrada y salida de equipamiento, incluyendo la identificación de la persona que autoriza de movimiento.

5.1.8 Instalaciones alternativas [mp.if.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Se garantizará la existencia y disponibilidad de instalaciones alternativas para poder trabajar en caso de que las instalaciones habituales no estén disponibles. Las instalaciones alternativas disfrutarán de las mismas garantías de seguridad que las instalaciones habituales.

5.2 Gestión del personal [mp.per].

5.2.1 Caracterización del puesto de trabajo [mp.per.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

cve: BOE-A-2010-1330

Cada puesto de trabajo se caracterizará de la siguiente forma:

a) Se definirán las responsabilidades relacionadas con cada puesto de trabajo en materia de seguridad. La definición se basará en el análisis de riesgos.
b) Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad.
c) Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar dicho puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias.

5.2.2 Deberes y obligaciones [mp.per.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

1. Se informará a cada persona que trabaje en el sistema, de los deberes y responsabilidades de su puesto de trabajo en materia de seguridad.

a) Se especificarán las medidas disciplinarias a que haya lugar.
b) Se cubrirá tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
c) Se contemplará el deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que estén adscritos al puesto de trabajo, como posteriormente a su terminación.

2. En caso de personal contratado a través de un tercero:

a) Se establecerán los deberes y obligaciones del personal.
b) Se establecerán los deberes y obligaciones de cada parte.
c) Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

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 incidencias de seguridad, sean reales o falsas alarmas.

5.2.4 Formación [mp.per.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

cve: BOE-A-2010-1330

Se formará regularmente al personal en aquellas materias que requieran para el desempeño de sus funciones, en particular en lo relativo a:

a) Configuración de sistemas.
b) Detección y reacción a incidentes.
c) Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.

5.2.5 Personal alternativo [mp.per.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Se garantizará a existencia y disponibilidad de otras personas que se puedan hacer cargo de las funciones en caso de indisponibilidad del personal habitual. El personal alternativo deberá estar sometido a las mismas garantías de seguridad que el personal habitual.

5.3 Protección de los equipos [mp.eq].

5.3.1 Puesto de trabajo despejado [mp.eq.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	=

Se exigirá que los puestos de trabajo permanezcan despejados, sin más material encima de la mesa que el requerido para la actividad que se está realizando en cada momento

Categoría MEDIA

Este material se guardará en lugar cerrado cuando no se esté utilizando.

5.3.2 Bloqueo de puesto de trabajo [mp.eq.2].

dimensiones	A		
nivel	bajo	medio	alto
	no aplica	aplica	+

El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

Categoría ALTA

Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

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

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	+

cve: BOE-A-2010-1330

Los equipos que abandonen 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 incidencias, de pérdidas o sustracciones.

c) Se establecerá un sistema de protección perimetral que minimice la visibilidad exterior y controle las opciones de acceso al interior cuando el equipo se conecte a redes, en particular si el equipo se conecta a redes públicas.

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.

5.3.4 Medios alternativos [mp.eq.9].

dimensiones	D		
nivel	bajo	medio	alto
	No aplica	aplica	=

Se garantizará la existencia y disponibilidad de medios alternativos de tratamiento de la información para el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección.

Igualmente, se establecerá un tiempo máximo para que los equipos alternativos entren en funcionamiento.

5.4 Protección de las comunicaciones [mp.com].

5.4.1 Perímetro seguro [mp.com.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	+

Se dispondrá un sistema cortafuegos que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejara transitar los flujos previamente autorizados.

Categoría ALTA

a) El sistema de cortafuegos constará de dos o más equipos de diferente fabricante dispuestos en cascada.

b) Se dispondrán sistemas redundantes.

cve: BOE-A-2010-1330

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, preferentemente, productos certificados [op.pl.5].

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 alguna (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.º La alteración de la información en transito
2.º La inyección de información espuria
3.º El secuestro de la sesión por una tercera parte

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 valorará positivamente en empleo de dispositivos hardware en el establecimiento y utilización de la red privada virtual.
b) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.4.4 Segregación de redes [mp.com.4].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

cve: BOE-A-2010-1330

La segregación de redes acota el acceso a la información y, consiguientemente, la propagación de los incidentes de seguridad, que quedan restringidos al entorno donde ocurren.

La red se segmentará en segmentos de forma que haya:

a) Control de entrada de los usuarios que llegan a cada segmento.
b) Control de salida de la información disponible en cada segmento.
c) Las redes se pueden segmentar por dispositivos físicos o lógicos. El punto de interconexión estará particularmente asegurado, mantenido y monitorizado (como en [mp.com.1]).

5.4.5 Medios alternativos [mp.com.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Se garantizará la existencia y disponibilidad de medios alternativos de comunicación para el caso de que fallen los medios habituales. Los medios alternativos de comunicación:

a) Estarán sujetos y proporcionar las mismas garantías de protección que el medio habitual.
b) Garantizarán un tiempo máximo de entrada en funcionamiento.

5.5 Protección de los soportes de información [mp.si].

5.5.1 Etiquetado [mp.si.1].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	=	=

Los soportes de información se etiquetarán de forma que, sin revelar su contenido, se indique el nivel de seguridad de la información contenida de mayor calificación.

Los usuarios han de estar capacitados para entender el significado de las etiquetas, bien mediante simple inspección, bien mediante el recurso a un repositorio que lo explique.

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.

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, preferentemente, productos certificados [op.pl.5].

cve: BOE-A-2010-1330

5.5.3 Custodia [mp.si.3].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, mediante las siguientes actuaciones:

a) Garantizando el control de acceso con medidas físicas ([mp.if.1] y [mpl.if.7]) ó lógicas ([mp.si.2]), o ambas.
b) Garantizando que se respetan las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agresores medioambientales.

5.5.4 Transporte [mp.si.4].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El responsable de sistemas garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro.
Para ello:

a) Se dispondrá de un registro de salida que identifique al transportista que recibe el soporte para su traslado.
b) Se dispondrá de un registro de entrada que identifique al transportista que lo entrega.
c) Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
d) Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al nivel de calificación de la información contenida de mayor nivel.
e) Se gestionarán las claves según [op.exp.11].

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

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	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.

a) Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su anterior contenido.
b) Se destruirán de forma segura los soportes, en los siguientes casos:

1.º Cuando la naturaleza del soporte no permita un borrado seguro.
2.º Cuando así lo requiera el procedimiento asociado al tipo de la información contenida,.

c) Se emplearán, preferentemente, productos certificados [op.pl.5].

cve: BOE-A-2010-1330

5.6 Protección de las aplicaciones informáticas [mp.sw].

5.6.1 Desarrollo de aplicaciones [mp.sw.1].

dimensiones	todas		
categoría	básica	media	alta
	no aplica	aplica	=

a) El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción.

b) Se aplicará una metodología de desarrollo reconocida que:

1.º Tome en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.

2.º Trate específicamente los datos usados en pruebas.

3.º Permita la inspección del código fuente.

c) Los siguientes elementos serán parte integral del diseño del sistema:

1.º Los mecanismos de identificación y autenticación.

2.º Los mecanismos de protección de la información tratada.

3.º La generación y tratamiento de pistas de auditoría.

d) Las pruebas anteriores a la implantación o modificación de los sistemas de información no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

5.6.2 Aceptación y puesta en servicio [mp.sw.2].

dimensiones	todas		
categoría	básica	media	alta
	aplica	+	++

Categoría BÁSICA

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación.

a) Se comprobará que:

1.º Se cumplen los criterios de aceptación en materia de seguridad.

2.º No se deteriora la seguridad de otros componentes del servicio.

b) Las pruebas se realizarán en un entorno aislado (pre-producción).

c) Las pruebas de aceptación no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Categoría MEDIA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de vulnerabilidades.

b) Pruebas de penetración.

cve: BOE-A-2010-1330

Categoría ALTA

Se realizarán las siguientes inspecciones previas a la entrada en servicio:

a) Análisis de coherencia en la integración en los procesos.
b) Se considerará la oportunidad de realizar una auditoría de código fuente.

5.7 Protección de la información [mp.info].

5.7.1 Datos de carácter personal [mp.info.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	aplica	aplica

Cuando el sistema trate datos de carácter personal, se estará a 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.

Lo indicado en el párrafo anterior también se aplicará, cuando una disposición con rango de ley se remita a las normas sobre datos de carácter personal en la protección de información.

5.7.2 Calificación de la información [mp.info.2].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	+	=

1. Para calificar la información se estará a lo establecido legalmente sobre la naturaleza de la misma.
2. La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
3. La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 43 y los criterios generales prescritos en el Anexo I.
4. El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
5. El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

Nivel MEDIO

Se redactarán los procedimientos necesarios que describan, en detalle, la forma en que se ha de etiquetar y tratar la información en consideración al nivel de seguridad que requiere; y precisando cómo se ha de realizar:

a) Su control de acceso.
b) Su almacenamiento.
c) La realización de copias.
d) El etiquetado de soportes.
e) Su transmisión telemática.
f) Y cualquier otra actividad relacionada con dicha información.

cve: BOE-A-2010-1330

5.7.3 Cifrado de la información [mp.info.3].

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Para el cifrado de información se estará a lo que se indica a continuación:

a) La información con un nivel alto en confidencialidad se cifrará tanto durante su almacenamiento como durante su transmisión. Sólo estará en claro mientras se está haciendo uso de ella.
b) Para el uso de criptografía en las comunicaciones, se estará a lo dispuesto en [mp.com.2].
c) Para el uso de criptografía en los soportes de información, se estará a lo dispuesto en [mp.si.2].

5.7.4 Firma electrónica [mp.info.4].

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+	++

La firma electrónica es un mecanismo de prevención del repudio; es decir, previene frente a la posibilidad de que en el futuro el signatario pudiera desdecirse de la información firmada.
La firma electrónica garantiza la autenticidad del signatario y la integridad del contenido.
Cuando se emplee firma electrónica:

a) El signatario será la parte que se hace responsable de la información, en la medida de sus atribuciones.
b) Se dispondrá de una Política de Firma Electrónica, aprobada por el órgano superior competente que corresponda.

Nivel BAJO

Se empleará cualquier medio de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

1. Los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso:

a) Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.
b) Se emplearán, preferentemente, certificados reconocidos.
c) Se emplearán, preferentemente, dispositivos seguros de firma.

2. 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:

a) Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación:

1.º Certificados.
2.º Datos de verificación y validación.

cve: BOE-A-2010-1330

b) Se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.

c) 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 a) y b).

d) La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes a) y b).

Nivel ALTO

Se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en la nivel Medio, además de las siguientes:

a) Se usarán certificados reconocidos.
b) Se usarán dispositivos seguros de creación de firma.
c) Se emplearán, preferentemente, productos certificados [op.pl.5].

5.7.5 Sellos de tiempo [mp.info.5].

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

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].

5.7.6 Limpieza de documentos [mp.info.6].

dimensiones	C		
nivel	bajo	medio	alto
	aplica	=	=

En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, meta-datos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

Esta medida es especialmente relevante cuando el documento se difunde ampliamente, como ocurre cuando se ofrece al público en un servidor web u otro tipo de repositorio de información.

Se tendrá presente que el incumplimiento de esta medida puede perjudicar:

a) Al mantenimiento de la confidencialidad de información que no debería haberse revelado al receptor del documento.
b) Al mantenimiento de la confidencialidad de las fuentes u orígenes de la información, que no debe conocer el receptor del documento.
c) A la buena imagen de la organización que difunde el documento por cuanto demuestra un descuido en su buen hacer.

cve: BOE-A-2010-1330

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

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	=

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

Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

Las copias de respaldo deberán abarcar:

a) Información de trabajo de la organización.
b) Aplicaciones en explotación, incluyendo los sistemas operativos.
c) Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
d) Claves utilizadas para preservar la confidencialidad de la información.

5.8 Protección de los servicios [mp.s].

5.8.1 Protección del correo electrónico (e-mail) [mp.s.1].

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

a) La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.
b) Se protegerá la información de encaminamiento de mensajes y establecimiento de conexiones.
c) Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:

1.º Correo no solicitado, en su expresión inglesa «spam».
2.º Programas dañinos, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
3.º Código móvil de tipo «applet».

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:

1.º Limitaciones al uso como soporte de comunicaciones privadas.

2.º Actividades de concienciación y formación relativas al uso del correo electrónico.

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

dimensiones	todas		
categoría	básica	media	alta
	aplica	=	=

cve: BOE-A-2010-1330

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».

5.8.3 Protección frente a la denegación de servicio [mp.s.8].

dimensiones	D		
nivel	bajo	medio	alto
	No aplica	aplica	+

Nivel MEDIO

Se establecerán medidas preventivas y reactivas frente a ataques de denegación de servicio (DOS Denial of Service). Para ello:

a) Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.
b) Se desplegarán tecnologías para prevenir los ataques conocidos.

Nivel ALTO

a) Se establecerá un sistema de detección de ataques de denegación de servicio.
b) Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.
c) Se impedirá el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

5.8.4 Medios alternativos [mp.s.9].

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

Se garantizará la existencia y disponibilidad de medios alternativos para prestar los servicios en el caso de que fallen los medios habituales. Estos medios alternativos estarán sujetos a las mismas garantías de protección que los medios habituales.

cve: BOE-A-2010-1330

6. Desarrollo y complemento de las medidas de seguridad

Las medidas de seguridad se desarrollarán y complementarán según lo establecido en la disposición final segunda.

7. 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 las instrucciones técnicas CCN-STIC correspondientes a la implementación y a diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.

ANEXO III

Auditoría de la seguridad

1. *Objeto de la auditoría*

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.

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 incidencias.
c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.

2. *Niveles de auditoría*

Los niveles de auditoría que se realizan a los sistemas de información, serán los siguientes:

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.

cve: BOE-A-2010-1330

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.

ANEXO IV

Glosario

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Análisis de riesgos. Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de los controles del sistema, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.

Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

Categoría de un sistema. Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.

Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

Firma electrónica. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Gestión de incidentes. Plan de acción para atender a las incidencias que se den. Además de resolverlas 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.

Gestión de riesgos. Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad. Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

cve: BOE-A-2010-1330

Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

Política de firma electrónica. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.

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

Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Proceso. Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.

Proceso de seguridad. Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.

Requisitos mínimos de seguridad. Exigencias necesarias para asegurar la información y los servicios.

Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización.

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

Servicios acreditados. Servicios prestados por un sistema con autorización concedida por la autoridad responsable, para tratar un tipo de información determinada, en unas condiciones precisas de las dimensiones de seguridad, con arreglo a su concepto de operación.

Sistema de gestión de la seguridad de la información (SGSI). Sistema de gestión que, basado en el estudio de los riesgos, se establece para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

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

Trazabilidad. Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Vulnerabilidad. Una debilidad que puede ser aprovechada por una amenaza.

Acrónimos

CCN: Centro Criptológico Nacional.
CERT: Computer Emergency Reaction Team.
INTECO: Instituto Nacional de Tecnologías de la Comunicación.
STIC: Seguridad de las Tecnologías de Información y Comunicaciones.

cve: BOE-A-2010-1330

ANEXO V

Modelo de cláusula administrativa particular

«Cláusula administrativa particular.–En cumplimiento con lo dispuesto en el artículo 99.4 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público, y el artículo 18 del Real Decreto ……/……, de …… de …… por el que se regula el Esquema Nacional de Seguridad, el licitador incluirá referencia precisa, documentada y acreditativa de que los productos de seguridad, equipos, sistemas, aplicaciones o sus componentes, han sido previamente certificados por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

En el caso de que no exista la certificación indicada en el párrafo anterior, o esté en proceso, se incluirá, igualmente, referencia precisa, documentada y acreditativa de que son los más idóneos.

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.»

cve: BOE-A-2010-1330