

§ 17 Sistema Español de Archivos y Sistema de Archivos de la Administración del Estado

a) El establecimiento de políticas de prevención del deterioro de los documentos de archivo utilizando sistemas de instalación adecuados y con especial atención sobre los documentos con formatos y soportes más vulnerables.

b) El fomento de la creación y dotación de talleres de restauración en los centros de Archivo que se estime conveniente con el fin de abordar la conservación activa de los documentos.

c) El desarrollo de planes de preservación, restauración y criterios de cooperación entre los Archivos del Sistema en materia de conservación.

Artículo 17. *Enriquecimiento del patrimonio documental.*

1. El Ministerio de Cultura promoverá:

a) Las transferencias periódicas regulares de las fracciones de serie o series documentales de carácter histórico desde los archivos intermedios al archivo histórico que corresponda.

b) La incorporación de documentos o agrupaciones documentales de interés histórico e informativo, por medio de compra, depósito, comodato, donación o cualquier otra figura legal contemplada en el ordenamiento jurídico.

c) La reproducción de documentos custodiados en otros centros nacionales o internacionales mediante la suscripción de convenios de colaboración, acuerdos y contratos cumpliendo los requisitos legalmente establecidos.

2. A los archivos y fondos adquiridos con base en lo dispuesto en el apartado anterior se les aplicarán las mismas condiciones de custodia, conservación, reproducción y difusión que al resto de sus fondos documentales, sin perjuicio de su titularidad y conforme a lo establecido en el correspondiente contrato o instrumento jurídico.

3. Entre los compromisos del Ministerio de Cultura se incluye la permanencia conjunta e indivisible de los documentos adquiridos en el archivo o centro de titularidad estatal, en el que se determine su custodia.

Artículo 18. *Medidas de fomento del patrimonio documental.*

1. El Ministerio de Cultura, de acuerdo con la normativa vigente, arbitrará medios económicos y técnicos para colaborar con los poseedores y propietarios privados de Patrimonio Documental en el mantenimiento, tratamiento y conservación adecuada de dicho Patrimonio.

2. A tal fin, podrá realizar convocatorias periódicas de ayudas en régimen de concurrencia competitiva dirigidas a entidades privadas sin ánimo de lucro para la mejora de sus instalaciones o equipamiento de sus archivos, así como para el desarrollo de proyectos archivísticos, con el fin de fomentar la conservación y difusión del patrimonio documental de carácter privado con arreglo a las normas y estándares internacionales.

Los beneficiarios de las citadas ayudas quedarán obligados a:

a) Garantizar el acceso público a sus fondos en las condiciones que se establezcan conjuntamente.

b) Ceder, cuando así lo previera la convocatoria de ayudas, los derechos de reproducción, comunicación pública y transformación en Internet, de todos los elementos que constituyen el resultado del proyecto realizado, independientemente del soporte en que se entregue.

c) Autorizar la difusión a través de Internet y de la plataforma institucional del Ministerio de Cultura de la información proporcionada como resultado de la realización de los proyectos subvencionados. La difusión de la información en ningún caso supondrá merma o menoscabo de los derechos de propiedad intelectual que puedan existir.

Artículo 19. *Difusión de los documentos de archivo y de otros recursos culturales o informativos del Sistema español de archivos.*

El Ministerio de Cultura impulsará programas dinámicos encaminados a asegurar la difusión al conjunto de la sociedad, de los contenidos y de los servicios telemáticos y

§ 17 Sistema Español de Archivos y Sistema de Archivos de la Administración del Estado

presenciales que ofrecen los centros de archivo del Sistema Español de Archivos, a través de:

a) El desarrollo del Portal de Archivos Españoles que pone en Internet y al servicio de los ciudadanos, las bases de datos descriptivas y las imágenes digitalizadas de los documentos de los centros de archivo del Ministerio de Cultura y de cualquier otro centro de archivo del Sistema Español de Archivos que quiera adherirse a la mencionada plataforma, con el fin de fomentar el acceso libre y gratuito de los usuarios a los contenidos culturales e informativos que se custodian.

b) El impulso a través del Centro de Información Documental de Archivos, del Censo Guía de Archivos, como guía electrónica y directorio de los archivos de España e Iberoamérica, que permite a los ciudadanos la localización inmediata de los centros de archivo así como los fondos y colecciones que custodian y los servicios que éstos prestan.

c) La elaboración de un catálogo colectivo accesible por Internet, que incluya información de los ejemplares bibliográficos y hemerográficos de las bibliotecas históricas y las bibliotecas especializadas o auxiliares de los archivos del Ministerio de Cultura, coordinado desde el Centro de Información Documental de Archivos.

d) El diseño y desarrollo de estrategias de comunicación y marketing y la utilización de la Web como instrumento inmediato de información.

e) La programación y el diseño de exposiciones presenciales y visitas y exposiciones virtuales que permitan divulgar los documentos de archivo así como su interés histórico, científico y cultural.

f) El impulso de actividades pedagógicas que acerquen los archivos y el contexto histórico de producción de los documentos, a los estudiantes de los diferentes ciclos formativos.

g) El desarrollo de programas de edición electrónica y en papel, de instrumentos de referencia, catálogos, boletines informativos y de cualquier otra obra de interés para el conocimiento y difusión del patrimonio documental.

h) El apoyo y fomento de jornadas, conferencias, congresos y actividades culturales relacionadas con el ámbito de los archivos.

Sección 4.ª Documentos electrónicos y preservación digital.

Artículo 20. *Condiciones para la recuperación y conservación del documento electrónico.*

1. Las disposiciones del presente Real Decreto relativas a los documentos integrantes del Sistema de Archivos de la Administración General del Estado, serán de aplicación también a los documentos en soporte electrónico, con las especialidades derivadas de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, de los Esquemas Nacionales de Seguridad e Interoperabilidad, y demás normativa de desarrollo.

2. Los Departamentos Ministeriales y las entidades de derecho público vinculadas o dependientes de los mismos, adoptarán las decisiones organizativas y las medidas técnicas necesarias con el fin de garantizar la recuperación y conservación de los documentos electrónicos a lo largo de su ciclo de vida. Entre éstas:

a) La identificación clara y precisa de cada uno de los documentos mediante un código unívoco que permita su identificación en un entorno de intercambio interadministrativo.

b) La asociación de los metadatos mínimos obligatorios y, en su caso, complementarios asociados al documento electrónico.

c) La inclusión, en el caso de los expedientes electrónicos, de un índice electrónico firmado por el órgano o entidad actuante que garantice la integridad del mismo y permita su recuperación.

d) La recuperación completa e inmediata de los documentos a través de métodos de consulta en línea a los datos que permita la visualización de los documentos de modo que sean legibles e identificables.

e) La adopción de medidas para garantizar la conservación de la memoria e identificación de los órganos que ejercen la competencia sobre el documento o expediente para que el ciudadano de hoy y del futuro pueda comprender el contexto en el que se creó.

§ 17 Sistema Español de Archivos y Sistema de Archivos de la Administración del Estado

f) El mantenimiento del valor probatorio de los documentos y expedientes y de las evidencias electrónicas como prueba de las actividades y procedimientos, así como la observancia de las obligaciones jurídicas que incumban a los servicios.

g) La transferencia de los expedientes electrónicos a los archivos históricos para la conservación permanente, de acuerdo con lo establecido en la normativa vigente, de manera que se pueda asegurar su conservación y accesibilidad a medio y largo plazo.

h) El borrado de la información, en su caso, o si procede la destrucción física de los soportes, de acuerdo con un procedimiento regulado y dejando registro de su eliminación.

i) La valoración y el establecimiento de las estrategias que se pueden aplicar para la conservación a medio y largo plazo de los documentos, tales como procedimientos de emulación, migración y conversión de formatos.

Artículo 21. *Aplicación de las tecnologías de la información y comunicaciones en la gestión y tratamiento de los documentos.*

Los Departamentos Ministeriales y sus organismos vinculados o dependientes promoverán en todo momento el uso de las tecnologías de la información y el conocimiento en el tratamiento archivístico de los documentos de su competencia y en todo lo relativo a las funciones de conservación, gestión, acceso y difusión que tiene encomendadas, mediante:

a) La utilización de sistemas de gestión, de acuerdo con los requisitos establecidos en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y su normativa de desarrollo.

b) El desarrollo de archivos digitales o repositorios de documentos en soporte electrónico estableciendo formatos de intercambio de documentos o expedientes electrónicos definiendo unos metadatos y clasificaciones comunes que permitan la reutilización y el intercambio de información entre los distintos órganos de la Administración.

c) La aplicación de los principios básicos y los requisitos mínimos requeridos para una protección adecuada de la información con el fin de 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.

d) El desarrollo de Sistemas Integrales de Información y Gestión de Archivos y su implementación en plataformas informáticas compartidas, con procedimientos de actualización en línea y accesibles por Internet.

e) La implantación progresiva de los servicios telemáticos que permitan recoger, gestionar y dar respuesta al conjunto de solicitudes, reclamaciones y sugerencias que realicen los ciudadanos sobre acceso, localización, reproducción, u otras cuestiones relacionadas con los documentos o los servicios que prestan los archivos del Sistema.

Artículo 22. *Documentos en formato electrónico transferidos al Archivo Intermedio de la Administración General del Estado.*

Las decisiones organizativas y medidas técnicas previstas en este capítulo no supondrán para la documentación transferida al Archivo Intermedio de la Administración General del Estado por los distintos Ministerios y Organismos, obligaciones adicionales a las previstas en la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en los Esquemas Nacionales de Seguridad e Interoperabilidad y demás normativa de desarrollo.

CAPÍTULO IV

Procedimiento de acceso a documentos y archivos

Artículo 23. *Derecho de acceso a documentos y archivos.*

1. Toda persona tiene derecho a acceder a los documentos conservados en los archivos incluidos en el ámbito de aplicación de esta norma, en los términos establecidos en el

§ 17 Sistema Español de Archivos y Sistema de Archivos de la Administración del Estado

presente capítulo sin perjuicio de las exclusiones y limitaciones previstas en la Constitución y en las leyes.

2. El presente Capítulo tiene por objeto regular el procedimiento común para el acceso a los documentos obrantes en los archivos de la Administración General del Estado, así como de las entidades de Derecho público vinculadas o dependientes de ella, que no tengan la consideración de archivos de oficina o gestión.

3. El responsable del archivo ofrecerá la asistencia que sea necesaria para facilitar el ejercicio del derecho de acceso, teniendo en cuenta las necesidades especiales de algunos colectivos.

4. Los sistemas de información archivística deberán garantizar el uso de las lenguas cooficiales del Estado en los términos previstos en la Ley 30/1992, de 26 de noviembre, y en la normativa que resulte de aplicación.

Artículo 24. *Solicitud de acceso.*

1. La solicitud de acceso a documentos podrá presentarse a través de los medios y en los términos establecidos en la Ley 30/1992, de 26 de noviembre, y en la Ley 11/2007, de 22 de junio, y se dirigirá al responsable del archivo que los custodia. En todos los archivos existirá un modelo normalizado de solicitud a disposición de los interesados, que igualmente estará disponible en la sede electrónica del correspondiente Departamento o entidad de Derecho Público.

2. En la solicitud deberá indicarse con claridad el documento o conjunto de documentos a los que se refiere, así como la identidad del solicitante y una dirección, a efectos de comunicaciones.

3. No será necesario motivar la solicitud de acceso a documentos. No obstante, el solicitante podrá exponer los motivos de su petición, que se tendrán en cuenta en la tramitación y resolución de la solicitud.

4. Con el fin de facilitar la identificación de los documentos solicitados, el responsable del archivo pondrá a disposición del público los instrumentos de referencia y descripción de los fondos documentales que lo integran, con excepción de los que en aplicación de las limitaciones legalmente previstas no deban constar.

5. Las entidades públicas incluidas en el ámbito de aplicación de este Real Decreto informarán del órgano competente para resolver las solicitudes de acceso. En ausencia de previsión expresa, se entenderá competente aquél del que dependa orgánicamente el archivo que custodia los documentos cuya consulta se solicita.

Artículo 25. *Autorización de entrada a los archivos y de consulta de documentos originales.*

1. La entrada en la zona de depósito de los archivos estará reservada a personal autorizado. Quienes acrediten un interés histórico, científico, estadístico o cultural relevante podrán solicitar al responsable del archivo autorización de entrada para el examen de la documentación obrante. La autorización, que podrá denegarse en razón de las necesidades de organización de los servicios o de la garantía del carácter restringido de determinados fondos obrantes en los archivos, determinará las condiciones en que deba realizarse la entrada.

2. Cuando en el archivo existan reproducciones de los documentos solicitados, se dará acceso a éstas como norma general; en estos casos, sólo cuando la materia o circunstancias de la investigación lo justifiquen y el estado de conservación de los documentos lo permita, se autorizará el acceso a los originales previa presentación de la correspondiente solicitud de autorización.

Artículo 26. *Acceso restringido.*

1. Los documentos conservados en los archivos incluidos en el ámbito de aplicación de esta norma serán de libre acceso, salvo cuando les afecte alguna de las limitaciones previstas en la Constitución y en las Leyes. En particular, serán de acceso restringido los documentos clasificados según lo dispuesto en la normativa sobre secretos oficiales, los documentos que contengan información cuya difusión pudiera entrañar riesgos para la seguridad y la defensa del Estado o interferir en la averiguación de los delitos o la tutela

§ 17 Sistema Español de Archivos y Sistema de Archivos de la Administración del Estado

judicial efectiva de ciudadanos e instituciones, así como los declarados reservados por una norma con rango de Ley y aquellos que contengan datos personales a los que se refiere el artículo 28.

2. El responsable del archivo, siempre que sea posible, tendrá a disposición del público la relación de los documentos y series documentales de acceso restringido, con exclusión de aquellos que en atención a los intereses protegidos no deban ser objeto de publicidad.

3. El acceso a documentos excluidos de pública consulta será restringido y quedará condicionado, con las excepciones y especialidades previstas en la Ley, a la obtención de autorización previa.

4. Con carácter excepcional, el responsable del archivo podrá restringir cautelarmente el acceso a aquellos documentos o series documentales que, sin haber sido objeto de exclusión de consulta pública, pudieran incurrir, a su juicio y a la vista de su contenido, en alguna de las limitaciones previstas en las leyes.

Toda alteración en el régimen de acceso a documentos deberá ser puesta en conocimiento de la Comisión Superior Calificadora de Documentos Administrativos, que será la encargada de informar con carácter previo los casos de modificación del régimen de libre acceso.

Artículo 27. *Solicitud de consulta de documentos de acceso restringido por razones de seguridad y defensa del Estado.*

1. Los documentos clasificados de conformidad con lo previsto en la normativa sobre secretos oficiales del Estado estarán excluidos de la consulta pública, sin que pueda concederse autorización para el acceso en tanto no recaiga una decisión de desclasificación por el órgano competente para realizarla.

2. Cuando la solicitud de consulta se refiera a documentos o series documentales que incorporen marcas de reserva o confidencialidad, el órgano competente para resolver remitirá la solicitud a su superior jerárquico o, según lo que establezcan las normas de organización de los respectivos Departamentos Ministeriales y entidades de Derecho Público, al órgano que realizó la declaración de reserva o confidencialidad, para que decidan sobre la concesión de autorización de la consulta.

Artículo 28. *Solicitud de consulta de documentos de acceso restringido por contener datos personales.*

1. La solicitud de acceso a documentos que contengan datos personales referidos exclusivamente al propio solicitante se regirá por la normativa de protección de datos personales.

2. El acceso a los documentos que contengan datos personales que puedan afectar a la intimidad o a la seguridad de las personas, o que tengan la consideración de especialmente protegidos en los términos de la normativa de protección de datos personales, incluyendo los que se encuentren en procedimientos o expedientes sancionadores, será posible siempre que medie el consentimiento expreso y por escrito de los afectados.

No obstante, serán accesibles los documentos con datos personales que puedan afectar a la seguridad o intimidad de las personas cuando hayan transcurrido veinticinco años desde el fallecimiento de los afectados. Si éste dato no constara, el interesado deberá aportar la correspondiente certificación expedida por el Registro Civil.

Cuando no fuera posible conocer la fecha o el hecho del fallecimiento y el documento o documentos solicitados posean una antigüedad superior a cincuenta años, el acceso se concederá si, atendidas las circunstancias del caso, se entiende razonablemente excluida la posibilidad de lesión del derecho a la intimidad personal y familiar o el riesgo para la seguridad del afectado y siempre de conformidad con la normativa de protección de datos.

3. El acceso a documentos que contengan datos nominativos o meramente identificativos de las personas que no afecten a su seguridad o su intimidad, será posible cuando el titular de los mismos haya fallecido o cuando el solicitante acredite la existencia de un interés legítimo en el acceso.

A estos efectos, se entenderá que poseen interés legítimo quienes soliciten el acceso para el ejercicio de sus derechos y los investigadores que acrediten que el acceso se produce con una finalidad histórica, científica o estadística.

§ 17 Sistema Español de Archivos y Sistema de Archivos de la Administración del Estado

4. Se concederá el acceso a documentos que contengan datos de carácter personal, sin necesidad de consentimiento de sus titulares, cuando se proceda previamente a la oportuna disociación, de los datos de modo que se impida la identificación de las personas afectadas.

5. La información que contenga datos de carácter personal únicamente podrá ser utilizada para las finalidades que justificaron el acceso a la misma y siempre de conformidad con la normativa de protección de datos.

Artículo 29. *Tramitación y resolución.*

1. Las resoluciones de las solicitudes de acceso y de consulta directa se notificarán por escrito al solicitante, con indicación de los recursos que procedan contra las mismas, el órgano administrativo o judicial ante el que deban interponerse y el plazo para hacerlo. En el supuesto de ser estimatorias, especificarán la forma y, en su caso, el plazo en el que se facilitarán al interesado los documentos solicitados o será posible la consulta directa. Las resoluciones denegatorias serán motivadas.

2. En caso de que la solicitud se refiera a documentos que no obren en poder del órgano al que se dirige, será remitida de oficio al que los posea, si se conoce, dando cuenta de ello al solicitante.

3. Cuando la indicación de la existencia o no del documento solicitado suponga incurrir en alguna de las limitaciones al acceso, se desestimarán la solicitud, informando al interesado de esta circunstancia.

4. Se tramitarán con carácter preferente las solicitudes que tengan por objeto el acceso a documentos necesarios para el ejercicio de derechos.

5. Serán inadmitidas las solicitudes que se consideren abusivas por su carácter manifiestamente irrazonable o repetitivo.

Artículo 30. *Plazo para resolver y sentido del silencio.*

1. La resolución de la solicitud de acceso o de consulta deberá adoptarse y notificarse lo antes posible y, en todo caso, en el plazo máximo de un mes desde la recepción por el órgano competente para tramitarla.

2. En el caso de solicitud de acceso a documentos, cuando el volumen de lo solicitado, su emplazamiento o las dificultades para su reproducción así lo justifiquen, el plazo para resolver podrá ampliarse por otro mes, informando de esta circunstancia al solicitante.

3. El cómputo del plazo para resolver se interrumpirá en los siguientes supuestos:

a) Cuando se requiera al solicitante la subsanación de deficiencias y la aportación de documentos, especialmente los relativos al consentimiento de los afectados.

b) Cuando una norma exija autorización específica.

La interrupción del plazo será debidamente comunicada al interesado.

4. Transcurrido el plazo máximo para resolver sin haberse notificado resolución expresa, la solicitud de acceso se entenderá estimada.

Artículo 31. *Obtención de copias.*

1. La estimación de la solicitud de acceso o de consulta conllevará el derecho a obtener copia de los documentos solicitados, salvo en los siguientes supuestos:

a) Cuando los documentos no sean de libre consulta.

b) Cuando no resulte posible realizar la copia en un formato determinado debido a la carencia de equipos apropiados o al excesivo coste de la misma.

c) Cuando la reproducción suponga vulneración de los derechos de propiedad intelectual.

2. La resolución que conceda el acceso expresará si es posible la obtención de copias y las condiciones de uso de las mismas.

3. La expedición de certificaciones y copias y la transposición a formatos diferentes del original podrá someterse al previo pago de las exacciones que estén legalmente establecidas en la normativa sobre tasas y precios públicos.

Artículo 32. *Régimen de impugnaciones.*

Contra toda resolución, expresa o presunta, recaída en el procedimiento regulado en este Real Decreto podrán interponerse los recursos administrativos y contencioso-administrativos que resulten procedentes de conformidad con la legislación aplicable.

Disposición adicional primera. *Constitución del Consejo de Cooperación Archivística y de la Comisión de Archivos de la Administración General del Estado.*

En el plazo de tres meses desde la fecha de la entrada en vigor de este Real Decreto se procederá a convocar la reunión constitutiva del Consejo de Cooperación Archivística y a la designación de sus componentes.

La Comisión de Archivos de la Administración General del Estado y de sus organismos públicos asumirá las funciones de la Junta Superior de Archivos y se constituirá en el plazo máximo de seis meses desde la entrada en vigor de este Real Decreto.

Disposición adicional segunda. *Regulación de las Comisiones Calificadoras de Documentos Administrativos.*

Las Comisiones Calificadoras de Documentos Administrativos de los departamentos ministeriales que no hayan sido suprimidas por el Real Decreto 776/2011, de 3 de junio, por el que se suprimen determinados órganos colegiados y se establecen criterios para la normalización en la creación de órganos colegiados en la Administración General del Estado y sus Organismos Públicos, se regirán por su normativa específica.

Disposición adicional tercera. *Archivo Histórico de la Nobleza.*

Mediante Real Decreto y en el plazo de tres meses desde la fecha de la entrada en vigor de este Real Decreto, se aprobarán los órganos rectores del Archivo Histórico de la Nobleza, con sede en Toledo, quedando suprimida la Sección Nobleza del Archivo Histórico Nacional.

Disposición adicional cuarta. *Sistema Archivístico de la Defensa.*

El Sistema Archivístico de la Defensa se rige por su normativa específica. No obstante, el régimen de acceso a los documentos obrantes en el mismo será el establecido en el presente Real Decreto.

Disposición adicional quinta. *Documentación que afecta a las relaciones internacionales de España.*

Con el fin de adaptar lo previsto en el presente Real Decreto a las características de la documentación que afecta a las relaciones internacionales de España, podrá crearse un sistema archivístico propio del Ministerio de Asuntos Exteriores y de Cooperación, mediante Real Decreto de iniciativa conjunta de los Ministros de Cultura y de Asuntos Exteriores y de Cooperación.

A estos efectos, en el plazo de tres meses se constituirá un grupo de trabajo integrado por los Ministerios citados, de composición paritaria y cuyos miembros serán designados por las Subsecretarías respectivas.

En todo caso, el régimen de acceso a los documentos obrantes en dicho sistema archivístico será el establecido en el presente Real Decreto.

Disposición adicional sexta. *Régimen de acceso a los Archivos Históricos de titularidad y gestión estatal.*

Las disposiciones del presente Real Decreto se aplicarán sin perjuicio de las reglas específicas de acceso a los fondos de los Archivos Históricos de titularidad y gestión estatal, en razón de su carácter de archivos abiertos al público, siempre que resulten más favorables al derecho de acceso.

Disposición adicional séptima. *Régimen de acceso a los archivos y documentos adquiridos por negocio jurídico.*

El derecho de acceso a archivos y documentos custodiados por el Ministerio de Cultura en virtud de compra, comodato, depósito, donación o cualquier otra figura jurídica, se someterá a las condiciones establecidas en el título en el que se materialice dicho negocio jurídico.

Disposición adicional octava.

El acceso a los documentos de las instituciones europeas que se encuentren en los archivos incluidos en el ámbito de aplicación de este Real Decreto se realizará sin perjuicio de las previsiones contenidas en la normativa europea y, en particular, de lo dispuesto en el Reglamento (CE) n.º 1049/2001 del Parlamento y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

Disposición adicional novena. *Cláusula de no incremento del gasto público.*

La aplicación de este Real Decreto se hará sin aumento del coste de funcionamiento de los respectivos órganos directivos y no supondrá aumento del gasto público.

Disposición transitoria primera. *Normas y plazos de transferencias.*

Las normas y plazos de transferencias de documentos de los Departamentos ministeriales al Archivo General de la Administración establecidos en el Decreto 914/1969, de 8 de mayo de 1969, por el que se crea el Archivo General de la Administración, serán sustituidos progresivamente por los calendarios de conservación y normas técnicas de transferencia que se aprueben en el marco del Sistema de Archivos de la Administración General del Estado.

Disposición transitoria segunda. *Comisión Superior Calificadora de Documentos Administrativos.*

La Comisión Superior Calificadora de Documentos Administrativos seguirá desarrollando sus funciones como órgano superior consultivo de la Administración General del Estado en la toma de decisiones sobre la conservación permanente y utilización de sus documentos, hasta la constitución de la Comisión de Archivos de la Administración General del Estado, momento en que se hará efectiva su condición de órgano superior consultivo de éste, con idénticas funciones.

Disposición derogatoria única. *Derogación normativa.*

Quedan derogadas todas las normas de igual e inferior rango en cuanto contradigan o se opongan a lo dispuesto en el presente real decreto y, en particular, las siguientes:

- a) El Decreto de 22 de noviembre de 1901, por el que se aprueba el Reglamento de Archivos del Estado.
- b) El Decreto de 24 de julio de 1947, sobre ordenación de los Archivos y Bibliotecas y del Tesoro Histórico-documental y Bibliográfico.
- c) La Orden de 25 de noviembre de 1996, por la que se regula la composición y funciones de la Junta Superior de Archivos.

Disposición final primera. *Modificación del Real Decreto 1401/2007, de 29 de octubre.*

El artículo 2.1.a) del Real Decreto 1401/2007, de 29 de octubre, por el que se regula la composición, funcionamiento y competencias de la Comisión Superior Calificadora de Documentos Administrativos, queda redactado como sigue:

«a) Presidente: La persona titular de la Subsecretaría de Cultura, que podrá delegar en el Vicepresidente Primero.»

Disposición final segunda. *Título competencial.*

Este Real Decreto se dicta al amparo de lo dispuesto en la regla 28.^a del apartado primero del artículo 149 de la Constitución, que atribuye al Estado la competencia exclusiva sobre los archivos de titularidad estatal. Se exceptúan de lo anterior los capítulos I y II, que se dictan al amparo de lo dispuesto en el artículo 149.2 de la Constitución, en virtud del cual, sin perjuicio de las competencias que podrán asumir las Comunidades Autónomas, el Estado considerará el servicio de la cultura como deber y atribución esencial y facilitará la comunicación cultural entre las Comunidades Autónomas, de acuerdo con ellas.

Disposición final tercera. *Organización archivística departamental.*

Los titulares de los departamentos ministeriales adoptarán las previsiones necesarias para asegurar la plena aplicación de las previsiones de este Real Decreto referidas a la organización de los archivos de su competencia en el plazo de seis meses desde su entrada en vigor, excepto en aquellos supuestos en que los correspondientes Ministerio u Organismo no dispongan de Archivo Central, en cuyo caso el plazo será de un año.

Disposición final cuarta. *Habilitación para el desarrollo reglamentario.*

Se autoriza a los titulares de los departamentos ministeriales, en el ámbito de sus competencias, para que adopten las medidas necesarias para el desarrollo y ejecución de lo establecido en este real decreto, siempre que no supongan incremento global del gasto público ni de las estructuras orgánicas de los departamentos ministeriales.

Disposición final quinta. *Entrada en vigor.*

El presente Real Decreto entrará en vigor el día 1 de enero de 2012.

NORMATIVA PARA INGRESO EN EL CUERPO GENERAL ADMINISTRATIVO DE LA ADMINISTRACIÓN DEL ESTADO

§ 18

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

Ministerio de Asuntos Económicos y Transformación Digital
«BOE» núm. 106, de 4 de mayo de 2022
Última modificación: 6 de noviembre de 2024
Referencia: BOE-A-2022-7191

I

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (en adelante, ENS) tenía por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que han venido garantizando adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades.

El ENS, cuyo ámbito de aplicación comprendía todas las entidades de las administraciones públicas, perseguía fundamentar la confianza en que los sistemas de información prestan sus servicios adecuadamente y custodian la información sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar a personas no autorizadas, estableciendo medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, de forma que se facilite a los ciudadanos y a las administraciones públicas el ejercicio de sus derechos y el cumplimiento de sus obligaciones a través de medios electrónicos.

Desde 2010 se han producido notables cambios en España y en la Unión Europea, incluidos la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad y el avance de las tecnologías de aplicación. Asimismo, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, advirtiéndose un notable incremento de los ciberataques, tanto en volumen y frecuencia como en sofisticación, con agentes y actores con mayores capacidades técnicas y operativas; amenazas que se producen en un contexto de alta dependencia de las tecnologías de la información y de las comunicaciones en nuestra sociedad y de gran interconexión de los sistemas de información. Todo ello afecta significativamente a un número cada vez mayor de entidades públicas y privadas, a sus cadenas de suministro, a los ciudadanos y, por ende, a la ciberseguridad nacional, lo que compromete el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos, como reconocen tanto la Estrategia de Ciberseguridad Nacional de 2013 como, particularmente, la Estrategia Nacional de Ciberseguridad 2019.

El Real Decreto 3/2010, de 8 de enero, establecía que el ENS debía desarrollarse y perfeccionarse manteniéndose actualizado de forma permanente conforme al progreso de los servicios de la administración electrónica, de la evolución de la tecnología, de los nuevos

§ 18 Esquema Nacional de Seguridad

estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo.

En el plano normativo, acompasado a dichos cambios y en ocasiones como origen de los mismos, desde 2010 se han modificado tanto el marco europeo (con cuatro Reglamentos y una Directiva) como el español, referido a la seguridad nacional, regulación del procedimiento administrativo y el régimen jurídico del sector público, de protección de datos personales y de la seguridad de las redes y sistemas de información, y se ha evolucionado el marco estratégico de la ciberseguridad.

Así, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, considera a la ciberseguridad como un ámbito de especial interés de la Seguridad Nacional tal como señala su artículo 10, y que, por ello, requiere una atención específica por resultar básica para preservar los derechos y libertades y el bienestar de los ciudadanos y para garantizar el suministro de los servicios y recursos esenciales. De acuerdo con las previsiones de su artículo 4.3 se aprobó el Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017, y posteriormente, el Real Decreto 1150/2021, de 28 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2021, identificando en ambas al ciberespacio como un espacio común global, que la Estrategia 2021 describe como espacio de conexión caracterizado por su apertura funcional, la carencia de fronteras físicas y su fácil accesibilidad, añadiendo que en los espacios comunes globales resulta difícil la atribución de cualquier acción irregular o delictiva, dada su extensión, su débil regulación y la ausencia de soberanía.

Por otra parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ha ampliado el ámbito de aplicación del ENS a todo el sector público, estableciendo en su artículo 3, que regula los principios generales, la necesidad de que las administraciones públicas se relacionen entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que garanticen la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas y la protección de los datos personales, y faciliten la prestación de servicios a los interesados preferentemente por dichos medios, señalando al ENS como instrumento fundamental para el logro de dichos objetivos en su artículo 156.

Asimismo, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, entre los derechos de las personas en sus relaciones con las administraciones públicas previstos en el artículo 13 incluye el relativo a la protección de los datos personales y, en particular, el derecho a la seguridad de los datos que figuren en los ficheros, sistemas y aplicaciones de las administraciones públicas.

En desarrollo de las dos leyes anteriores, el Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, concreta en diferentes preceptos la obligación del cumplimiento de las medidas de seguridad previstas en el ENS, como los referidos al intercambio electrónico de datos en entornos cerrados de comunicación, los sistemas de clave concertada y otros sistemas de identificación de las personas interesadas, el archivo electrónico único o los portales de internet, entre otros.

Coincidente en el tiempo con la aprobación de las tres leyes mencionadas, el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizó el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de la ciberseguridad del momento, y de la evolución del marco legal, para adecuarse a lo previsto en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (conocido como «Reglamento eIDAS»).

Con relación a las medidas de seguridad del ENS en el tratamiento de datos personales, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ordenó en su disposición adicional primera que dichas medidas de seguridad se implanten en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679, del

Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). De otra parte, la disposición adicional primera también prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público y a las del sector privado que colaboren con estas en la prestación de servicios públicos que involucren el tratamiento de datos personales. Por último, y en el mismo sentido, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, ha establecido en su artículo 37 la obligación de aplicar las medidas del ENS a los tratamientos de datos personales por parte de las autoridades públicas competentes.

Por otra parte, con relación a la seguridad de redes y sistemas de información, desde la entrada en vigor del Real Decreto 3/2010, de 8 de enero, se han aprobado en la Unión Europea dos Reglamentos y una Directiva que han fijado el marco de actuación en los ordenamientos nacionales.

Así, en primer lugar, el Reglamento (UE) N.º 526/2013 del Parlamento Europeo y del Consejo de 21 de mayo de 2013 relativo a la Agencia de Seguridad de las Redes de la Información de la Unión Europea (ENISA) y por el que se deroga el Reglamento (CE) N.º 460/2004. En segundo lugar, el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad»).

En tercer lugar, la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como «Directiva NIS (*Security of Network and Information Systems*)», que ha sido objeto de transposición en España por medio del Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, señalando la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas aplicables a entidades del ámbito de aplicación de este. Este Real Decreto-ley 12/2018, de 7 de septiembre, ha sido desarrollado por el Real Decreto 43/2021, de 26 de enero, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad. Así, el Real Decreto 43/2021, de 26 de enero, establece que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero.

Tal como estableció la Estrategia de Seguridad Nacional de 2017, España precisa garantizar un uso seguro y responsable de las redes y sistemas de información y comunicaciones a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques potenciando y adoptando medidas específicas para contribuir a la promoción de un ciberespacio seguro y fiable. En este sentido, el Consejo de Seguridad Nacional aprobó el 12 de abril de 2019 la Estrategia Nacional de Ciberseguridad 2019, publicada por Orden PCI/487/2019, de 26 de abril, con el propósito de fijar las directrices generales en el ámbito de la ciberseguridad de manera que se alcanzasen los objetivos previstos en la Estrategia de Seguridad Nacional de 2017.

La Estrategia Nacional de Ciberseguridad 2019, contiene un objetivo general y cinco objetivos específicos, y, para alcanzarlos, se proponen siete líneas de acción con un total de 65 medidas. El primero de estos objetivos es la seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales y se desarrolla a través de dos líneas de acción y veinticuatro medidas específicas entre las que figura la de asegurar la plena implantación del Esquema Nacional de Seguridad. Para desarrollar esta Estrategia, el Consejo de Ministros ha aprobado el 29 de marzo de 2022 el

§ 18 Esquema Nacional de Seguridad

Plan Nacional de Ciberseguridad, que prevé cerca de 150 iniciativas, entre actuaciones y proyectos, para los próximos tres años.

Asimismo, la Estrategia Nacional de Ciberseguridad 2019 señala entre sus objetivos la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y de los datos personales tratados por los sistemas y redes del sector público y de los servicios, sean o no esenciales, recogiendo que su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, mediante el desarrollo de nuevas soluciones, y el refuerzo de la coordinación y la adaptación del ordenamiento jurídico.

II

La evolución de las amenazas, los nuevos vectores de ataque, el desarrollo de modernos mecanismos de respuesta y la necesidad de mantener la conformidad y el alineamiento con las regulaciones europeas y nacionales de aplicación, exigen adaptar las medidas de seguridad a esta nueva realidad. Fortalecer la ciberseguridad demanda recursos económicos, humanos y tecnológicos que se han de dimensionar atendiendo al principio de proporcionalidad y al nivel de seguridad requerido, de acuerdo con una adecuada planificación y contando con la participación de los agentes involucrados, según una dinámica de mejora continua adaptativa.

Por ello, en un mundo hiperconectado como el actual, implementar la seguridad en el ciberespacio se ha convertido en una prioridad estratégica. Sin embargo, el riesgo en el ciberespacio es demasiado grande para que el sector público o las empresas lo aborden por sí solos, pues ambos comparten el interés y la responsabilidad de enfrentar juntos ese reto. A medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

De hecho, el pasado 9 de marzo, el Parlamento Europeo ha aprobado por amplísima mayoría una Resolución sobre injerencias extranjeras en todos los procesos democráticos de la Unión Europea, en particular la desinformación. Tal como señala dicha Resolución en sus considerandos, las injerencias extranjeras constituyen un patrón de conducta que amenaza o afecta negativamente a valores, procedimientos democráticos, procesos políticos, la seguridad de Estados y ciudadanos y la capacidad de hacer frente a situaciones excepcionales. Las tácticas de injerencia extranjera, que se combinan a menudo para tener un mayor efecto, adoptan, entre otras formas, los ciberataques, la asunción del control de infraestructuras críticas, la desinformación, supresión de información, manipulación de plataformas de redes sociales y de sus algoritmos, operaciones de pirateo y filtración, amenazas y acoso para acceder a información sobre los votantes e interferir en la legitimidad del proceso electoral, personalidades e identidades falsas, ejercicio de presiones sobre ciudadanos extranjeros que viven en la Unión, instrumentalización de migrantes y espionaje.

Al tiempo que el escenario descrito ha venido consolidándose, se ha ido extendiendo la implantación del ENS, resultando de ello una mayor experiencia acumulada sobre su aplicación, a la vez que un mejor conocimiento de la situación gracias a las sucesivas ediciones del Informe Nacional del Estado de la Seguridad (INES), del cuerpo de guías de seguridad CCN-STIC y de los servicios y herramientas proporcionados por la capacidad de respuesta a incidentes de seguridad de la información, el CCN-CERT, del Centro Criptológico Nacional (CCN).

En definitiva, por todas las razones anteriormente expuestas es necesario actualizar el ENS para cumplir tres grandes objetivos.

En primer lugar, alinear el ENS con el marco normativo y el contexto estratégico existente para garantizar la seguridad en la administración digital. Se trata de reflejar con claridad el ámbito de aplicación del ENS en beneficio de la ciberseguridad y de los derechos de los ciudadanos, así como de actualizar las referencias al marco legal vigente y de revisar la formulación de ciertas cuestiones a la luz de éste, conforme a la Estrategia Nacional de Ciberseguridad 2019 y el Plan Nacional de Ciberseguridad, de forma que se logre simplificar, precisar o armonizar los mandatos del ENS, eliminar aspectos que puedan considerarse excesivos, o añadir aquellos otros que se identifican como necesarios.

§ 18 Esquema Nacional de Seguridad

En segundo lugar, introducir la capacidad de ajustar los requisitos del ENS, para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza que presentan una multiplicidad de entidades o servicios en cuanto a los riesgos a los que están expuestos sus sistemas de información y sus servicios. Ello aconseja la inclusión en el ENS del concepto de «perfil de cumplimiento específico» que, aprobado por el Centro Criptológico Nacional, permita alcanzar una adaptación del ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua mediante la revisión de los principios básicos, de los requisitos mínimos y de las medidas de seguridad.

Por último, la aprobación de este real decreto se incardina también en la ejecución del Plan de Digitalización de las Administraciones Públicas 2021-2025, uno de los instrumentos principales para el cumplimiento del Plan de Recuperación, Transformación y Resiliencia y su Componente 11 denominado «Modernización de las Administraciones Públicas», así como para el desarrollo de las inversiones y reformas previstas en la agenda España Digital 2025. Dicho Plan de Digitalización contempla expresamente, entre sus reformas, la actualización del ENS con el fin de hacer evolucionar la política de seguridad de todas las entidades del sector público español, tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Dicha reforma se ve complementada con la constitución del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos que servirá de referencia para las demás administraciones públicas y contribuirá a mejorar el cumplimiento del ENS de las entidades en su alcance de servicio. Esta previsión ha sido respaldada por el Acuerdo de Consejo de Ministros de 25 de mayo de 2021 sobre actuaciones urgentes en materia de ciberseguridad que mandata la tramitación y aprobación de un real decreto que sustituya al Real Decreto 3/2010, de 8 de enero, como medida de refuerzo del marco normativo.

III

El real decreto se estructura en cuarenta y un artículos distribuidos en siete capítulos, tres disposiciones adicionales, una disposición transitoria, una disposición derogatoria, tres disposiciones finales y cuatro anexos.

El capítulo I comprende las disposiciones generales que regulan el objeto de la norma, su ámbito de aplicación, la referencia a los sistemas de información que traten datos personales y las definiciones aplicables. El ámbito de aplicación es el previsto en el artículo 2 de la Ley 40/2015, de 1 de octubre, al que se añaden los sistemas que tratan información clasificada, sin perjuicio de la normativa que resulte de aplicación, pudiendo resultar necesario complementar las medidas de seguridad de este real decreto con otras específicas para tales sistemas, derivadas de los compromisos internacionales contraídos por España o su pertenencia a organismos o foros internacionales en la materia. Asimismo los requisitos del ENS serán de aplicación a los sistemas de información de las entidades del sector privado, cuando de acuerdo con la normativa aplicable y en virtud de una relación contractual presten servicios a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas. Como se ha señalado anteriormente, considerando que la transformación digital ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y que el sector privado se encuentra igualmente inmerso en la transformación digital de sus procesos de negocio, ambos tipos de sistemas de información se encuentran expuestos al mismo tipo de amenazas y riesgos. Por ello, los operadores del sector privado que prestan servicios a las entidades del sector público, por razón de la alta imbricación de unos y otras, han de garantizar el mismo nivel de seguridad que se aplica a los sistemas y a la información en el ámbito del sector público, todo ello de conformidad, además, con los especiales requerimientos establecidos tanto en la Ley Orgánica 3/2018, de 5 de diciembre, como en la Ley Orgánica 7/2021, de 26 de mayo. Por otra parte, cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo

§ 18 Esquema Nacional de Seguridad

establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

El capítulo II, que comprende los artículos 5 a 11, regula los principios básicos que deben regir el ENS y que enumera en su artículo 5: seguridad integral; gestión de la seguridad basada en los riesgos; prevención, detección, respuesta y conservación; existencia de líneas de defensa; vigilancia continua y reevaluación periódica; y diferenciación de responsabilidades.

El capítulo III se refiere a la Política de Seguridad y los requisitos mínimos para permitir una protección adecuada de la información y los servicios. En los artículos 12 a 27 se definen tales requisitos: organización e implantación del proceso de seguridad; gestión de riesgos, consistente en un proceso de identificación, análisis, evaluación y tratamiento de los mismos; gestión de personal; profesionalidad; autorización y control de los accesos; protección de las instalaciones; adquisición de productos de seguridad y contratación de servicios de seguridad; mínimo privilegio; integridad y actualización del sistema; protección de la información almacenada y en tránsito; prevención ante otros sistemas de información interconectados; registro de la actividad y detección de código dañino; incidentes de seguridad; continuidad de la actividad; y mejora continua del proceso de seguridad. Seguidamente, el artículo 28 indica que para el cumplimiento de tales requisitos mínimos deberán adoptarse las medidas recogidas en el anexo II, conforme a una serie de consideraciones al efecto. No obstante, tales medidas de seguridad podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que la protección que aportan es, al menos, equivalente, y satisfacen los principios básicos y requisitos mínimos indicados previamente. En el artículo 29 se hace un llamamiento a la utilización de infraestructuras y servicios comunes de las administraciones públicas en aras de lograr una mayor eficiencia y retroalimentación de las sinergias de cada colectivo. Por último, el artículo 30 establece la posibilidad de implementar perfiles de cumplimiento específicos, así como esquemas de acreditación de entidades de implementación de configuraciones seguras.

El capítulo IV versa sobre la auditoría de la seguridad, el informe del estado de la seguridad y la respuesta a incidentes de seguridad. La auditoría de la seguridad se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes. Por su parte, el artículo 32, relativo al informe del estado de la seguridad, destaca el papel de la Comisión Sectorial de Administración Electrónica en este ámbito, así como del CCN y los órganos colegiados competentes en el ámbito de la administración digital en la Administración General del Estado.

La prevención, detección y respuesta a incidentes de seguridad se regula en los artículos 33 y 34, separando, por un lado, los aspectos relativos a la capacidad de respuesta y, por otro, los relativo a la prestación de los servicios de respuesta a incidentes de seguridad, tanto a las entidades del Sector Público como a las organizaciones del sector privado que les presten servicios.

En el capítulo V, artículos 35 a 38, se definen las normas de conformidad, que se concretan en cuatro: Administración Digital, ciclo de vida de servicios y sistemas, mecanismos de control y procedimientos de determinación de la conformidad con el ENS.

Por su parte, el capítulo VI, compuesto por su único artículo, el 39, establece la obligación de actualización permanente, de acuerdo con el marco jurídico vigente en cada momento, la evolución de la tecnología y los estándares en materia de seguridad y sistemas, así como de las ya mencionadas nuevas amenazas y vectores de ataque.

Concluye el articulado de la parte dispositiva con el capítulo VII, que desarrolla el procedimiento de categorización de los sistemas de información, definiendo en el artículo 40 las categorías de seguridad y en el artículo 41 las facultades al respecto.

En cuanto a las tres disposiciones adicionales, la primera regula los programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público que desarrollarán el CCN y el Instituto Nacional de Administración Pública.

§ 18 Esquema Nacional de Seguridad

La segunda disposición adicional regula las instrucciones técnicas de seguridad, de obligado cumplimiento y las guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC).

Por último, la tercera disposición adicional establece el cumplimiento del llamado principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH, por sus siglas en inglés, *Do No Significant Harm*) y las condiciones del etiquetado climático y digital.

La disposición transitoria única fija un plazo de veinticuatro meses para que los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, alcancen su plena adecuación al ENS.

La disposición derogatoria suprime el Real Decreto 3/2010, de 8 de enero, así como cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este real decreto.

Por último, la norma cuenta con tres disposiciones finales. La primera de ellas enumera los títulos competenciales; la segunda disposición final habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la su aplicación y desarrollo, sin perjuicio de las competencias de las comunidades autónomas para el desarrollo y ejecución de la legislación básica del Estado, y la disposición final tercera ordena la entrada en vigor el día siguiente al de su publicación en el «Boletín Oficial del Estado».

El real decreto se complementa con cuatro anexos: el anexo I regula las categorías de seguridad de los sistemas de información, detallando la secuencia de actuaciones para determinar la categoría de seguridad de un sistema; el anexo II detalla las medidas de seguridad; el anexo III se ocupa del objeto, niveles e interpretación de la Auditoría de la seguridad y, por último, el anexo IV incluye el glosario de términos y definiciones.

Con relación, en particular, al anexo II, este detalla las medidas de seguridad estructuradas en tres grupos: el marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; el marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y las medidas de protección, que se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas. Como se ha dicho, la modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas ha obligado a actualizar el elenco de medidas de seguridad del anexo II, con objeto de añadir, eliminar o modificar controles y sub-controles, al tiempo que se incluye un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y de unos posibles refuerzos, alineados con el nivel de seguridad perseguido. Todo ello se efectúa con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, y facilitar su implantación y auditoría.

IV

El real decreto, cuya aprobación está incluida en el Plan Anual Normativo de la Administración General del Estado para el año 2022, se ajusta a los principios de buena regulación contenidos en el artículo 129 de la Ley 39/2015, de 1 de octubre (principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia).

Así, la norma es acorde con los principios de necesidad y eficacia en tanto que persigue un interés general al concretar la regulación del ENS desarrollando en este aspecto la Ley 40/2015, de 1 de octubre y otros aspectos concretos de la normativa nacional y de la Unión Europea mencionada en este preámbulo. La norma es también acorde con el principio de proporcionalidad, al contener la regulación imprescindible para la consecución de los objetivos previamente mencionados. Igualmente, se ajusta al principio de seguridad jurídica, siendo coherente con el resto del ordenamiento, estableciéndose un marco normativo estable, integrado y claro. Durante el procedimiento de elaboración de la norma y aún en el contexto de la aplicación de las previsiones del artículo 27 de la Ley 50/1997, de 27 de noviembre, del Gobierno, por tratarse de una tramitación de urgencia acordada por el Consejo de Ministros, se han formalizado los trámites de audiencia e información pública, conforme a lo previsto en el artículo 133 de la Ley 39/2015, de 1 de octubre, y el artículo 26 de la Ley 50/1997, de 27 de noviembre, en cumplimiento del principio de transparencia,

quedando además justificados en el preámbulo los objetivos que persigue este real decreto. El proyecto se ha sometido a consulta a las comunidades autónomas y a la Federación Española de Municipios y Provincias a través de la Comisión Sectorial de Administración Electrónica y ha sido informado por la Comisión Nacional de los Mercados y la Competencia A.A.I. y la Agencia Española de Protección de Datos A.A.I.

Por último, en virtud del principio de eficiencia la norma no introduce ninguna variación en materia de cargas administrativas, respecto de la normativa que desarrolla.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18.^a, 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, sobre las telecomunicaciones y sobre la seguridad pública, respectivamente.

En su virtud, a propuesta de la Ministra de Asuntos Económicos y Transformación Digital, con la aprobación previa de la Ministra de Hacienda y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 3 de mayo de 2022,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

1. Este real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el artículo 156.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

2. El ENS está constituido por los principios básicos y requisitos mínimos necesarios para una protección adecuada de la información tratada y los servicios prestados por las entidades de su ámbito de aplicación, con objeto de asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos que gestionen en el ejercicio de sus competencias.

3. Lo dispuesto en este real decreto, por cuanto afecta a los sistemas de información utilizados para la prestación de los servicios públicos, deberá considerarse comprendido en los recursos y procedimientos integrantes del Sistema de Seguridad Nacional recogidos en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.

Artículo 2. *Ámbito de aplicación.*

1. El presente real decreto es de aplicación a todo el sector público, en los términos en que este se define por el artículo 2 de la Ley 40/2015, de 1 de octubre, y de acuerdo con lo previsto en el artículo 156.2 de la misma.

2. Asimismo, sin perjuicio de la aplicación de la Ley 9/1968, de 5 de abril, de Secretos Oficiales y otra normativa especial, este real decreto será de aplicación a los sistemas que tratan información clasificada, pudiendo resultar necesario adoptar medidas complementarias de seguridad, específicas para dichos sistemas, derivadas de los compromisos internacionales contraídos por España o de su pertenencia a organismos o foros internacionales.

3. Este real decreto también se aplica a los sistemas de información de las entidades del sector privado, incluida la obligación de contar con la política de seguridad a que se refiere el artículo 12, cuando, de acuerdo con la normativa aplicable y en virtud de una relación contractual, presten servicios o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

La política de seguridad a que se refiere el artículo 12 será aprobada en el caso de estas entidades por el órgano que ostente las máximas competencias ejecutivas.

Los pliegos de prescripciones administrativas o técnicas de los contratos que celebren las entidades del sector público incluidas en el ámbito de aplicación de este real decreto

§ 18 Esquema Nacional de Seguridad

contemplarán todos aquellos requisitos necesarios para asegurar la conformidad con el ENS de los sistemas de información en los que se sustenten los servicios prestados por los contratistas, tales como la presentación de las correspondientes Declaraciones o Certificaciones de Conformidad con el ENS.

Esta cautela se extenderá también a la cadena de suministro de dichos contratistas, en la medida que sea necesario y de acuerdo con los resultados del correspondiente análisis de riesgos.

4. Cuando las entidades del sector público lleven a cabo la instalación, despliegue y explotación de redes 5G o la prestación de servicios 5G, además de las previsiones de este real decreto será de aplicación lo establecido en el Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, en particular, lo dispuesto en su artículo 17 relativo a la gestión de seguridad por las administraciones públicas, así como su normativa de desarrollo.

Artículo 3. *Sistemas de información que traten datos personales.*

1. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto.

2. En estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

3. En todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto a los que se refiere el apartado anterior, en caso de resultar agravadas respecto de las previstas en el presente real decreto.

Artículo 4. *Definiciones.*

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.

CAPÍTULO II

Principios básicos

Artículo 5. *Principios básicos del Esquema Nacional de Seguridad.*

El objeto último de la seguridad de la información es garantizar que una organización podrá cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información. Por ello, en materia de seguridad de la información deberán tenerse en cuenta los siguientes principios básicos:

- a) Seguridad como proceso integral.
- b) Gestión de la seguridad basada en los riesgos.
- c) Prevención, detección, respuesta y conservación.
- d) Existencia de líneas de defensa.
- e) Vigilancia continua.
- f) Reevaluación periódica.
- g) Diferenciación de responsabilidades.

§ 18 Esquema Nacional de Seguridad

Artículo 6. *La seguridad como un proceso integral.*

1. La seguridad se entiende como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación del ENS 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 la de los responsables jerárquicos, para evitar que, la ignorancia, la falta de organización y de coordinación o de instrucciones adecuadas, constituyan fuentes de riesgo para la seguridad.

Artículo 7. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y la gestión de los riesgos es parte esencial del proceso de seguridad, debiendo constituir una actividad continua y permanentemente actualizada.

2. La gestión de los riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos a niveles aceptables. La reducción a estos niveles se realizará mediante una apropiada aplicación de medidas de seguridad, de manera equilibrada y proporcionada a la naturaleza de la información tratada, de los servicios a prestar y de los riesgos a los que estén expuestos.

Artículo 8. *Prevención, detección, respuesta y conservación.*

1. La seguridad del sistema debe contemplar las acciones relativas a los aspectos de prevención, detección y respuesta, al objeto de minimizar sus vulnerabilidades y lograr que las amenazas sobre el mismo no se materialicen o que, en el caso de hacerlo, no afecten gravemente a la información que maneja o a los servicios que presta.

2. Las medidas de prevención, que podrán incorporar componentes orientados a la disuasión o a la reducción de la superficie de exposición, deben eliminar o reducir la posibilidad de que las amenazas lleguen a materializarse.

3. Las medidas de detección irán dirigidas a descubrir la presencia de un ciberincidente.

4. Las medidas de respuesta, que se gestionarán en tiempo oportuno, estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad.

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

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

Artículo 9. *Existencia de líneas de defensa.*

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

a) Desarrollar una reacción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad de que el sistema sea comprometido en su conjunto.

b) 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 10. *Vigilancia continua y reevaluación periódica.*

1. La vigilancia continua permitirá la detección de actividades o comportamientos anómalos y su oportuna respuesta.

2. La evaluación permanente del estado de la seguridad de los activos permitirá medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

§ 18 Esquema Nacional de Seguridad

3. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

Artículo 11. *Diferenciación de responsabilidades.*

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

2. La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la explotación de los sistemas de información concernidos.

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

CAPÍTULO III

Política de seguridad y requisitos mínimos de seguridad

Artículo 12. *Política de seguridad y requisitos mínimos de seguridad.*

1. La política de seguridad de la información es el conjunto de directrices que rigen la forma en que una organización gestiona y protege la información que trata y los servicios que presta. A tal efecto, el instrumento que apruebe dicha política de seguridad deberá incluir, como mínimo, los siguientes extremos:

- a) Los objetivos o misión de la organización.
- b) El marco regulatorio en el que se desarrollarán las actividades.
- c) Los roles o funciones de seguridad, definiendo para cada uno, sus deberes y responsabilidades, así como el procedimiento para su designación y renovación.
- d) La estructura y composición del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad 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.
- f) Los riesgos que se derivan del tratamiento de los datos personales.

2. Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.

No obstante, la totalidad o una parte de los sujetos de un sector público institucional podrán quedar incluidos en el ámbito subjetivo de la política de seguridad aprobada por la Administración con la que guarden relación de vinculación, dependencia o adscripción, cuando así lo determinen los órganos competentes en el ejercicio de las potestades de organización.

3. En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento. Los organismos públicos y entidades pertenecientes al sector público institucional estatal podrán contar con su propia política de seguridad, aprobada por el órgano competente, que será coherente con la del Departamento con el que mantenga la relación de vinculación, dependencia o adscripción, o bien quedar comprendidos en el ámbito subjetivo de la política de seguridad de este. También podrán contar con su propia política de seguridad, aprobada por el órgano competente, coherente con la del Departamento del que dependan o al que estén adscritos, los centros directivos de la propia Administración General del Estado que gestionen servicios bajo la declaración de servicios compartidos.

4. La Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital dispondrá de su propia política de seguridad, que será aprobada por la persona titular de la misma.

5. Los municipios podrán disponer de una política de seguridad común elaborada por la entidad local comarcal o provincial que asuma la responsabilidad de la seguridad de la información de los sistemas municipales.

§ 18 Esquema Nacional de Seguridad

6. La política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II 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 de seguridad y contratación de servicios de seguridad.
- h) Mínimo privilegio.
- i) Integridad y actualización del sistema.
- j) Protección de la información almacenada y en tránsito.
- k) Prevención ante otros sistemas de información interconectados.
- l) Registro de la actividad y detección de código dañino.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- ñ) Mejora continua del proceso de seguridad.

7. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos.

Artículo 13. *Organización e implantación del proceso de seguridad.*

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

2. La política de seguridad, en aplicación del principio de diferenciación de responsabilidades a que se refiere el artículo 11 y según se detalla en la sección 3.1 del anexo II, deberá ser conocida por todas las personas que formen parte de la organización e identificar de forma inequívoca a los responsables de velar por su cumplimiento, los cuales tendrán las siguientes funciones:

- a) El responsable de la información determinará los requisitos de la información tratada
- b) El responsable del servicio determinará los requisitos de los servicios prestados.
- c) El responsable de la seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones.
- d) El responsable del sistema, por sí o a través de recursos propios o contratados, se encargará de desarrollar la forma concreta de implementar la seguridad en el sistema y de la supervisión de la operación diaria del mismo, pudiendo delegar en administradores u operadores bajo su responsabilidad.

3. El responsable de la seguridad será distinto del responsable del sistema, no debiendo existir dependencia jerárquica entre ambos. En aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que ambas funciones recaigan en la misma persona o en distintas personas entre las que exista relación jerárquica, deberán aplicarse medidas compensatorias para garantizar la finalidad del principio de diferenciación de responsabilidades previsto en el artículo 11.

4. Una Instrucción Técnica de Seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles a esta figura.

5. En el caso de servicios externalizados, salvo por causa justificada y documentada, la organización prestataria de dichos servicios deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.

§ 18 Esquema Nacional de Seguridad

Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

Artículo 14. *Análisis y gestión de los riesgos.*

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información o la prestación de servicios 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 15. *Gestión de personal.*

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en este real decreto, deberá ser formado e informado de sus deberes, obligaciones y responsabilidades en materia de seguridad. Su actuación, que deberá ser supervisada para verificar que se siguen los procedimientos establecidos, aplicará las normas y procedimientos operativos de seguridad aprobados en el desempeño de sus cometidos.
2. El significado y alcance del uso seguro del sistema se concretará y plasmará en unas normas de seguridad que serán aprobadas por la dirección o el órgano superior correspondiente.

Artículo 16. *Profesionalidad.*

1. La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.
2. Las entidades del ámbito de aplicación de este real decreto exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
3. Las organizaciones determinarán los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

Artículo 17. *Autorización y control de los accesos.*

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación de este real decreto deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

Artículo 18. *Protección de las instalaciones.*

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Artículo 19. *Adquisición de productos de seguridad y contratación de servicios de seguridad.*

1. En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los

§ 18 Esquema Nacional de Seguridad

sistemas de información del ámbito de aplicación de este real decreto, se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición.

2. El Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del Centro Criptológico Nacional (en adelante, CCN), constituido al amparo de lo dispuesto en el artículo 2.2.c) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo y en función del uso previsto del producto o servicio concreto dentro de sus competencias, determinará los siguientes aspectos:

- a) Los requisitos funcionales de seguridad y de aseguramiento de la certificación.
- b) Otras certificaciones de seguridad adicionales que se requieran normativamente.
- c) Excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

3. Para la contratación de servicios de seguridad se estará a lo señalado en los apartados anteriores y a lo dispuesto en el artículo 16.

Artículo 20. *Mínimo privilegio.*

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño, lo que implica incorporar los siguientes aspectos:

- a) El sistema proporcionará la funcionalidad imprescindible para que la organización alcance sus objetivos competenciales o contractuales.
- b) Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son desarrolladas por las personas autorizadas, desde emplazamientos o equipos asimismo autorizados; pudiendo exigirse, en su caso, restricciones de horario y puntos de acceso facultados.
- c) Se eliminarán o desactivarán, mediante el control de la configuración, las funciones que sean innecesarias o inadecuadas al fin que se persigue. El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.
- d) Se aplicarán guías de configuración de seguridad para las diferentes tecnologías, adaptadas a la categorización del sistema, al efecto de eliminar o desactivar las funciones que sean innecesarias o inadecuadas.

Artículo 21. *Integridad y actualización del sistema.*

1. La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

2. La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

Artículo 22. *Protección de información almacenada y en tránsito.*

1. En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

2. Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

3. Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que

§ 18 Esquema Nacional de Seguridad

correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

Artículo 23. *Prevención ante otros sistemas de información interconectados.*

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, tal y como se definen en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad correspondiente.

Artículo 24. *Registro de actividad y detección de código dañino.*

1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

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

Artículo 25. *Incidentes de seguridad.*

1. La entidad titular de los sistemas de información del ámbito de este real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con lo previsto en el artículo 33, la Instrucción Técnica de Seguridad correspondiente y, en caso de tratarse de un operador de servicios esenciales o de un proveedor de servicios digitales, de acuerdo con lo previsto en el anexo del Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.

2. Asimismo, se dispondrá de mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como de los cauces de comunicación a las partes interesadas y el registro de las actuaciones. Este registro se empleará para la mejora continua de la seguridad del sistema.

Artículo 26. *Continuidad de la actividad.*

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

§ 18 Esquema Nacional de Seguridad

Artículo 27. *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 la gestión de la seguridad de las tecnologías de la información.

Artículo 28. *Cumplimiento de los requisitos mínimos.*

1. Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:

- a) Los activos que constituyen los sistemas de información concernidos.
- b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
- c) Las decisiones que se adopten para gestionar los riesgos identificados.

2. Las medidas a las que se refiere el apartado 1 tendrán la condición de mínimos exigibles, siendo ampliables a criterio del responsable de la seguridad, quien podrá incluir medidas adicionales, habida cuenta del estado de la tecnología, la naturaleza de la información tratada o los servicios prestados y los riesgos a que están expuestos los sistemas de información afectados. La relación de medidas de seguridad seleccionadas se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

3. Las medidas de seguridad referenciadas en el anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, del riesgo sobre los activos (anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III. Como parte integral de la Declaración de Aplicabilidad se indicará, de forma detallada, la correspondencia entre las medidas compensatorias implantadas y las medidas del anexo II que compensan. El conjunto será objeto de la aprobación formal por parte del responsable de la seguridad. Una Guía CCN-STIC de las previstas en la disposición adicional segunda guiará en la selección de dichas medidas, así como su registro e inclusión en la Declaración de Aplicabilidad.

Artículo 29. *Infraestructuras y servicios comunes.*

La utilización de infraestructuras y servicios comunes de las administraciones públicas, incluidos los compartidos o transversales, facilitará el cumplimiento de lo dispuesto en este real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada administración pública.

Artículo 30. *Perfiles de cumplimiento específicos y acreditación de entidades de implementación de configuraciones seguras.*

1. En virtud del principio de proporcionalidad y buscando una eficaz y eficiente aplicación del ENS a determinadas entidades o sectores de actividad concretos, se podrán implementar perfiles de cumplimiento específicos que comprenderán aquel conjunto de medidas de seguridad que, trayendo causa del preceptivo análisis de riesgos, resulten idóneas para una concreta categoría de seguridad.

2. De forma análoga a lo dispuesto en el apartado anterior, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades comprendidas en el ámbito de aplicación de este real decreto, se podrán implementar esquemas de acreditación de entidades y validación de personas, que garanticen la seguridad de dichas soluciones o plataformas y la conformidad con lo dispuesto en este real decreto.

3. El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los antedichos esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad aprobadas conforme a lo previsto en la disposición adicional segunda.

4. Las correspondientes instrucciones técnicas de seguridad o, en su caso, las guías de Seguridad CCN-STIC, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente

prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.

CAPÍTULO IV

Seguridad de los sistemas: auditoría, informe e incidentes de seguridad

Artículo 31. *Auditoría de la seguridad.*

1. Los sistemas de información comprendidos en el ámbito de aplicación de este real decreto serán objeto de una auditoría regular ordinaria, al menos cada dos años, que verifique el cumplimiento de los requerimientos del ENS.

Con carácter extraordinario, deberá realizarse dicha auditoría siempre que se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La realización de la auditoría 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.

El plazo de dos años señalado en los párrafos anteriores podrá extenderse durante tres meses cuando concurren impedimentos de fuerza mayor no imputables a la entidad titular del sistema o sistemas de información concernidos.

2. La auditoría se realizará en función de la categoría del sistema y, en su caso, del perfil de cumplimiento específico que corresponda, según lo dispuesto en los anexos I y III y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

3. En la realización de las auditorías de la seguridad se utilizarán los criterios, métodos de trabajo y de conducta generalmente reconocidos, así como la normalización nacional e internacional aplicables a este tipo de actividades.

4. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento de este real decreto identificando los hallazgos de cumplimiento e incumplimiento detectados. 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, todo ello de conformidad con la citada Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

5. Los informes de auditoría serán presentados al responsable del sistema y al responsable de la seguridad. Estos informes serán analizados por este último que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

6. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría y atendiendo a una eventual gravedad de las deficiencias encontradas, el responsable del sistema podrá suspender temporalmente el tratamiento de informaciones, la prestación de servicios o la total operación del sistema, hasta su adecuada subsanación o mitigación.

7. Los informes de auditoría podrán ser requeridos por los responsables de cada organización, con competencias sobre seguridad de las tecnologías de la información, y por el CCN.

Artículo 32. *Informe del estado de la seguridad.*

1. La Comisión Sectorial de Administración Electrónica recogerá la información relacionada con el estado de las principales variables de la seguridad en los sistemas de información a los que se refiere este real decreto, de forma que permita elaborar un perfil general del estado de la seguridad en las entidades titulares de los sistemas de información comprendidos en el ámbito de aplicación del artículo 2, que se plasmará en el informe correspondiente.

2. El CCN articulará los procedimientos necesarios para la recogida y consolidación de la información, así como los aspectos metodológicos para su tratamiento y explotación, a través de los correspondientes grupos de trabajo que se constituyan al efecto en la Comisión Sectorial de Administración Electrónica y en los órganos colegiados competentes en el ámbito de la Administración General del Estado.

§ 18 Esquema Nacional de Seguridad

3. Los resultados del informe serán utilizados por las autoridades competentes que impulsarán las medidas oportunas que faciliten la mejora continua del estado de la seguridad utilizando en su caso, cuadros de mando e indicadores que contribuyan a la toma de decisiones mediante el uso de las herramientas que el CCN provea para tal efecto.

Artículo 33. *Capacidad de respuesta a incidentes de seguridad.*

1. El CCN articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (por su acrónimo en inglés de *Computer Emergency Response 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.

2. Sin perjuicio de lo establecido en el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre, las entidades del sector público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, de acuerdo con la correspondiente Instrucción Técnica de Seguridad.

3. Cuando un operador esencial que haya sido designado como operador crítico sufra un incidente, los CSIRT de referencia se coordinarán con el Ministerio del Interior, a través de su Oficina de Coordinación de Ciberseguridad, según lo previsto en el artículo 11.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, éste pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará a la capacidad de respuesta e incidentes de seguridad de referencia para el ámbito de la Defensa nacional, denominada ESPDEF-CERT, del Mando Conjunto del Ciberespacio (MCCE) a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente y podrá colaborar en la supervisión con la autoridad competente.

5. De conformidad con lo dispuesto en el Real Decreto-ley 12/2018, de 7 de septiembre, el CCN ejercerá la coordinación nacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática (denominados por su acrónimo en inglés *Computer Security Incident Response Team*, en adelante, CSIRT) en materia de seguridad de las redes y sistemas de información del sector público.

6. Tras un incidente de seguridad, el CCN-CERT determinará técnicamente el riesgo de reconexión del sistema o sistemas afectados, indicando los procedimientos a seguir y las salvaguardas a implementar con objeto de reducir el impacto para, en la medida de lo posible, evitar que vuelvan a darse las circunstancias que lo propiciaron.

Tras un incidente de seguridad, la Secretaría General de Administración Digital, sin perjuicio de la normativa que regula la continuidad de los sistemas de información implicados en la seguridad pública o la normativa que regule la continuidad de los sistemas de información militares implicados en la Defensa Nacional que requieran la participación del ESPDEF-CERT del Mando Conjunto del Ciberespacio, autorizará la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales, si un informe de superficie de exposición del CCN-CERT hubiere determinado que el riesgo es asumible.

En caso de que se trate de un incidente de seguridad que afecte a un medio o servicio común bajo ámbito de responsabilidad de la Intervención General de la Administración del Estado, esta participará en el proceso de autorización de la reconexión a que se refiere el párrafo anterior.

7. Las organizaciones del sector privado que presten servicios a las entidades públicas notificarán al INCIBE-CERT, centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE) dependiente del Ministerio de Asuntos Económicos y Transformación Digital, los incidentes que les afecten a través de su equipo de respuesta a incidentes de seguridad informática, quien, sin perjuicio de sus competencias y de lo previsto en los artículos 9, 10 y 11 del Real Decreto 43/2021, de

§ 18 Esquema Nacional de Seguridad

26 de enero, en relación con la Plataforma de Notificación y Seguimiento de Ciberincidentes, lo pondrá inmediatamente en conocimiento del CCN-CERT.

Artículo 34. *Prestación de servicios de respuesta a incidentes de seguridad a las entidades del sector público.*

1. De acuerdo con lo previsto en el artículo 33, el CCN-CERT prestará los siguientes servicios:

a) Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad que tengan las entidades del ámbito de aplicación de este real decreto.

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 afectados.

Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar informes, registros de auditoría y configuraciones de los sistemas afectados y cualquier otra información que se considere relevante, así como los soportes informáticos que se estimen necesarios para la investigación del incidente de los sistemas afectados, sin perjuicio de lo dispuesto en la normativa de protección de datos que resulte de aplicación, así como de la posible confidencialidad de datos de carácter institucional u organizativo.

b) Investigación y divulgación de las mejores prácticas sobre seguridad de la información entre todos los miembros de las entidades del sector público. Con esta finalidad, las series de documentos CCN-STIC (CCN-Seguridad de las Tecnologías de Información y la Comunicación), elaboradas por el CCN, ofrecerán normas, instrucciones, guías, recomendaciones y mejores prácticas para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación de este real decreto.

c) Formación destinada al personal del sector público especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos y de lograr la sensibilización y mejora de sus capacidades para la prevención, 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 entidades del sector público puedan desarrollar sus propias capacidades de respuesta a incidentes de seguridad, y en el que, aquel, será coordinador a nivel público estatal.

CAPÍTULO V

Normas de conformidad

Artículo 35. *Administración digital.*

1. La seguridad de los sistemas de información que sustentan la administración digital se regirá por lo establecido en este real decreto.

2. El CCN es el órgano competente para garantizar la debida interoperabilidad en materia de ciberseguridad y criptografía, en relación con la aplicación del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica.

Artículo 36. *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 37. *Mecanismos de control.*

Cada entidad titular de los sistemas de información comprendidos en el ámbito de aplicación de este real decreto y, en su caso, sus organismos, órganos, departamentos o

§ 18 Esquema Nacional de Seguridad

unidades, establecerán sus mecanismos de control para garantizar de forma real y efectiva el cumplimiento del ENS.

Artículo 38. *Procedimientos de determinación de la conformidad con el Esquema Nacional de Seguridad.*

1. Los sistemas de información comprendidos en el ámbito del artículo 2 serán objeto de un proceso para determinar su conformidad con el ENS. A tal efecto, los sistemas de categoría MEDIA o ALTA precisarán de una auditoría para la certificación de su conformidad, sin perjuicio de la auditoría de la seguridad prevista en el artículo 31 que podrá servir asimismo para los fines de la certificación, mientras que los sistemas de categoría BÁSICA solo requerirán de una autoevaluación para su declaración de la conformidad, sin perjuicio de que se puedan someter igualmente a una auditoría de certificación.

Tanto el procedimiento de autoevaluación como la auditoría de certificación se realizarán según lo dispuesto en el artículo 31 y el anexo III y en los términos que se determinen en la correspondiente Instrucción Técnica de Seguridad, que concretará asimismo los requisitos exigibles a las entidades certificadoras.

2. Los sujetos responsables de los sistemas de información a que se refiere el apartado anterior darán publicidad, en los correspondientes portales de internet o sedes electrónicas a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada Instrucción Técnica de Seguridad.

CAPÍTULO VI

Actualización del Esquema Nacional de Seguridad

Artículo 39. *Actualización permanente.*

El ENS se mantendrá actualizado de manera permanente, desarrollándose y perfeccionándose a lo largo del tiempo, en paralelo al avance de los servicios prestados por las entidades del sector público, la evolución tecnológica, la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría y los riesgos a los que estén expuestos los sistemas de información concernidos.

CAPÍTULO VII

Categorización de los sistemas de información

Artículo 40. *Categorías de seguridad.*

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

2. La determinación de la categoría de seguridad se efectuará en función de la valoración del impacto que tendría un incidente que afectase a la seguridad de la información o de los servicios con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, siguiendo el procedimiento descrito en el anexo I.

Artículo 41. *Facultades.*

1. La facultad para efectuar las valoraciones a las que se refiere el artículo 40, así como, en su caso, su posterior modificación, corresponderá al responsable o responsables de la información o servicios afectados.

2. Con base en las valoraciones señaladas en el apartado anterior, la determinación de la categoría de seguridad del sistema corresponderá al responsable o responsables de la seguridad.

§ 18 Esquema Nacional de Seguridad

Disposición adicional primera. Formación.

El CCN y el Instituto Nacional de Administración Pública desarrollarán programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público, para asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos, y para garantizar el conocimiento permanente del ENS entre dichas entidades.

Disposición adicional segunda. Desarrollo del Esquema Nacional de Seguridad.

En desarrollo de lo dispuesto en este real decreto, la persona titular del Ministerio para la Transformación Digital y de la Función Pública, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de la persona titular de la Secretaría de Estado de Función Pública.

Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea aplicables. Para su redacción y mantenimiento se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración digital.

Para el mejor cumplimiento de lo establecido en este real decreto, el CCN, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y la comunicación (guías CCN-STIC), particularmente de la serie 800, que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

Disposición adicional tercera. Respeto del principio de «no causar un perjuicio significativo» al medioambiente.

En cumplimiento con lo dispuesto en el Plan de Recuperación, Transformación y Resiliencia (PRTR) y en el Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia, todas las actuaciones que se lleven a cabo en el marco del PRTR en cumplimiento del presente real decreto deben respetar el principio de «no causar un perjuicio significativo» al medioambiente (principio DNSH por sus siglas en inglés, *Do No Significant Harm*) y las condiciones del etiquetado climático y digital.

Disposición transitoria única. Adecuación de sistemas.

1. Los sistemas de información del ámbito de aplicación de este real decreto, preexistentes a su entrada en vigor, incluidos aquellos de los que sean titulares los contratistas del sector privado en los términos señalados en el artículo 2, dispondrán de veinticuatro meses para alcanzar su plena adecuación al ENS, circunstancia que se manifestará con la exhibición del correspondiente distintivo de conformidad, atendiendo lo dispuesto en el artículo 38.

2. Durante los antedichos veinticuatro meses, los sistemas de información preexistentes a la entrada en vigor de este real decreto que dispusieren de los correspondientes Distintivos de Conformidad, derivados de Declaraciones o Certificaciones de conformidad con el ENS, podrán mantener su vigencia procediendo a su renovación de conformidad y en los términos señalados por el Real Decreto 3/2010, de 8 de enero, del que trajeron causa.

3. Los nuevos sistemas de información aplicarán lo establecido en este real decreto desde su concepción.

Disposición derogatoria única. Derogación normativa.

Queda derogado el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, así como cuantas disposiciones de igual o inferior rango que se opongan a lo dispuesto en este real decreto.

Disposición final primera. *Títulos competenciales.*

Este real decreto se dicta en virtud de lo establecido en los artículos 149.1.18.^a, 149.1.21.^a y 149.1.29.^a de la Constitución, que atribuyen al Estado la competencia exclusiva sobre las bases del régimen jurídico de las administraciones públicas, las telecomunicaciones y la seguridad pública, respectivamente.

Disposición final segunda. *Desarrollo normativo.*

Se habilita a la persona titular del Ministerio de Asuntos Económicos y Transformación Digital para dictar las disposiciones necesarias para la aplicación y desarrollo de lo establecido en este 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.*

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

ANEXO I**Categorías de seguridad de los sistemas de información****1. Fundamentos para la determinación de la categoría de seguridad de un sistema de información**

La determinación de la categoría de seguridad de un sistema de información se basará en la valoración del impacto que tendría sobre la organización un incidente que afectase a la seguridad de la información tratada o de los servicios prestados para:

- a) Alcanzar sus objetivos.
- b) Proteger los activos a su cargo.
- c) Garantizar la conformidad con el ordenamiento jurídico.

Anualmente, o siempre que se produzcan modificaciones significativas en los citados criterios de determinación, deberá re-evaluarse la categoría de seguridad de los sistemas de información concernidos.

2. Dimensiones de la seguridad

A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas:

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

3. Determinación del nivel de seguridad 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 de seguridad: BAJO, MEDIO o ALTO. Si una dimensión de seguridad no se ve afectada, no se adscribirá a ningún nivel.

a) Nivel BAJO. Se aplicará 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.

§ 18 Esquema Nacional de Seguridad

Se entenderá por perjuicio limitado:

- 1.º La reducción de forma apreciable de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
- 2.º Causar un daño menor en 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 pese a resultar molesto, pueda ser fácilmente reparable.
- 5.º Otros de naturaleza análoga.

b) Nivel MEDIO. Se aplicará 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 de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias, aunque estas sigan desempeñándose.
- 2.º Causar un daño significativo en 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 aplicará 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 efectiva de la capacidad de la organización para desarrollar eficazmente sus funciones y competencias.
- 2.º Causar un daño muy grave, e incluso irreparable, de 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 de información trate diferentes informaciones y preste diferentes servicios, el nivel de seguridad del sistema en cada dimensión será el mayor de los establecidos para cada información y cada servicio.

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

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

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

b) Un sistema de información será de categoría MEDIA si alguna de sus dimensiones de seguridad alcanza el nivel de seguridad MEDIO, y ninguna alcanza un nivel de seguridad 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 seguridad de un sistema de información sobre la base de lo indicado en el apartado anterior, no implicará que se altere, por este hecho, el nivel de seguridad de las dimensiones de seguridad que no han influido en la determinación de la categoría de seguridad del mismo.

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

1. Identificación del nivel de seguridad correspondiente a cada información y servicio, en función de las dimensiones de seguridad, teniendo en cuenta lo establecido en el apartado 3 anterior.

§ 18 Esquema Nacional de Seguridad

2. Determinación de la categoría de seguridad del sistema, según lo establecido en el apartado 4 anterior.

Las guías CCN-STIC, del CCN, precisarán los criterios necesarios para una adecuada categorización de seguridad de los sistemas de información.

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 de seguridad 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 de seguridad correspondiente a cada dimensión de seguridad, teniendo en cuenta lo establecido en el anexo I.
- d) Determinación de la categoría de seguridad del sistema, según lo establecido en el anexo I.
- e) Selección de las medidas de seguridad, junto con los refuerzos apropiados, de entre las contenidas en este anexo, de acuerdo con las dimensiones y sus niveles de seguridad y para determinadas medidas de seguridad, de acuerdo con la categoría de seguridad del sistema.

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este anexo, cuando en un sistema de información existan subsistemas 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 con los refuerzos correspondientes, y siempre que puedan delimitarse la información y los servicios afectados.

3. Las guías CCN-STIC, del CCN, podrán establecer perfiles de cumplimiento específicos, según el artículo 30 de este real decreto, para entidades o sectores concretos, que incluirán la relación de medidas y refuerzos que en cada caso resulten aplicables o los criterios para su determinación.

4. La correspondencia entre los niveles de seguridad exigidos en cada dimensión y las medidas de seguridad con sus refuerzos, es la que se indica en la tabla siguiente:

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org	Marco organizativo				
org.1	Política de seguridad	Categoría	aplica	aplica	aplica
org.2	Normativa de seguridad	Categoría	aplica	aplica	aplica

§ 18 Esquema Nacional de Seguridad

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
org.3	Procedimientos de seguridad	Categoría	aplica	aplica	aplica
org.4	Proceso de autorización	Categoría	aplica	aplica	aplica
op	Marco operacional				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Categoría	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Categoría	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Categoría	n.a.	aplica	aplica
op.acc	Control de acceso				
op.acc.1	Identificación	T A	aplica	+ R1	+ R1
op.acc.2	Requisitos de acceso	C I T A	aplica	aplica	+ R1
op.acc.3	Segregación de funciones y tareas	C I T A	n.a.	aplica	+ R1
op.acc.4	Proceso de gestión de derechos de acceso	C I T A	aplica	aplica	aplica
op.acc.5	Mecanismo de autenticación (usuarios externos)	C I T A	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	Explotación				
op.exp.1	Inventario de activos	Categoría	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Categoría	aplica	aplica	aplica
op.exp.3	Gestión de la configuración de seguridad	Categoría	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Categoría	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Categoría	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
op.exp.7	Gestión de incidentes	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3
op.exp.8	Registro de la actividad	T	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Categoría	aplica	aplica	aplica
op.exp.10	Protección de claves criptográficas	Categoría	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Categoría	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Categoría	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Categoría	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Categoría	n.a.	aplica	+ R1
op.nub	Servicios en la nube				
op.nub.1	Protección de servicios en la nube	Categoría	aplica	+ R1	+ R1 + R2
op.cont	Continuidad del servicio				
op.cont.1	Análisis de impacto	D	n.a.	aplica	aplica
op.cont.2	Plan de continuidad	D	n.a.	n.a.	aplica
op.cont.3	Pruebas periódicas	D	n.a.	n.a.	aplica
op.cont.4	Medios alternativos	D	n.a.	n.a.	aplica
op.mon	Monitorización del sistema				
op.mon.1	Detección de intrusión	Categoría	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Categoría	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Categoría	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
mp	Medidas de protección				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Categoría	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Categoría	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Categoría	aplica	aplica	aplica
mp.if.4	Energía eléctrica	D	aplica	+ R1	+ R1
mp.if.5	Protección frente a incendios	D	aplica	aplica	aplica
mp.if.6	Protección frente a inundaciones	D	n.a.	aplica	aplica
mp.if.7	Registro de entrada y salida de equipamiento	Categoría	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Categoría	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Categoría	aplica	+ R1	+ R1
mp.per.3	Concienciación	Categoría	aplica	aplica	aplica
mp.per.4	Formación	Categoría	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Categoría	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Categoría	aplica	aplica	+ R1 + R2
mp.eq.4	Otros dispositivos conectados a la red	C	aplica	+ R1	+ R1
mp.com	Protección de las comunicaciones				
mp.com.1	Perímetro seguro	Categoría	aplica	aplica	aplica
mp.com.2	Protección de la confidencialidad	C	aplica	+ R1	+ R1 + R2 + R3
mp.com.3	Protección de la integridad y de la autenticidad	I A	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4
mp.com.4	Separación de flujos de información en la red	Categoría	n.a.	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
mp.si	Protección de los soportes de información				
mp.si.1	Marcado de soportes	C	n.a.	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1 + R2
mp.si.3	Custodia	Categoría	aplica	aplica	aplica
mp.si.4	Transporte	Categoría	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	+ R1	+ R1

§ 18 Esquema Nacional de Seguridad

Medidas de Seguridad		Por categoría o dimensión(es)	Nivel de las dimensiones de seguridad		
			BAJO	MEDIO	ALTO
			Categoría de seguridad del sistema		
			BÁSICA	MEDIA	ALTA
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Categoría	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Categoría	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Categoría	aplica	aplica	aplica
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.3	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4
mp.info.4	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.5	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.6	Copias de seguridad	D	aplica	+ R1	+ R1 + R2
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Categoría	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Categoría	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Categoría	aplica	aplica	+ R1
mp.s.4	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

5. En las tablas del presente anexo se han empleado las siguientes convenciones:

a) La tercera columna indica si la medida se exige atendiendo al nivel de seguridad de una o más dimensiones de seguridad, o atendiendo a la categoría de seguridad del sistema. Cuando se exija por nivel de seguridad de las dimensiones, se indican cuales afectan utilizando sus iniciales.

b) Para indicar que una determinada medida de seguridad se debe aplicar a una o varias dimensiones de seguridad, en algún nivel de seguridad determinado, se utiliza la voz «aplica».

c) «n.a.» significa «no aplica» a efectos de cumplimiento normativo, por lo que no es exigible, sin perjuicio de que su implantación en el sistema pudiera ser beneficioso técnicamente.

d) Para indicar una mayor exigencia se emplean los refuerzos de seguridad (R) que se suman (+) a los requisitos base de la medida pero que no siempre son incrementales entre sí.

e) Para señalar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes y separados por «o» [Rn o Rn+1].

f) Se han empleado los colores verde, amarillo y rojo con el siguiente código: verde para indicar que una medida se aplica en sistemas de categoría BÁSICA o superior; el amarillo para indicar qué medidas y refuerzos empiezan a aplicar en categoría MEDIA o superior; y el rojo para indicar qué medidas o refuerzos son solo de aplicación en categoría ALTA o requieren un esfuerzo en seguridad superior al de categoría MEDIA.

6. A continuación, se describen individualmente cada una de las medidas organizadas de la siguiente forma:

a) Primero, una tabla resumen con las exigencias de seguridad de la medida en función de la categoría de seguridad del sistema y de las dimensiones de seguridad afectadas.

b) A continuación, una descripción con el cuerpo de la medida que desglosa los requisitos de base.

c) Posteriormente, podrán aparecer una serie de refuerzos adicionales que complementan a los requisitos de base, no en todos los casos requeridos o exigidos, y que podrían aplicarse en determinados perfiles de cumplimiento específicos.

d) Además, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría de seguridad del sistema, según corresponda. En los casos en los que se pueda elegir entre aplicar un refuerzo u otro, además de indicarlo entre corchetes [Rm o Rn], se incluirá un diagrama de flujo explicativo.

e) Por último, algunos refuerzos son de carácter opcional, no siendo requeridos en todos los sistemas de información. Se aplicarán como medidas adicionales cuando el análisis de riesgos así lo recomiende.

§ 18 Esquema Nacional de Seguridad

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	aplica	aplica

Requisitos.

La política de seguridad, que se aprobará de conformidad con lo dispuesto en el artículo 12 de este real decreto, se plasmará en un documento en el que, de forma clara, se precise, al menos, lo siguiente:

- [org.1.1] Los objetivos o misión de la organización.
- [org.1.2] El marco legal y regulatorio en el que se desarrollarán las actividades.
- [org.1.3] 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.
- [org.1.4] La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, las personas integrantes y la relación con otros elementos de la organización.
- [org.1.5] Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.

Aplicación de la medida.

- Categoría BÁSICA: org.1.
- Categoría MEDIA: org.1.
- Categoría ALTA: org.1.

3.2 Normativa de seguridad [org.2].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se dispondrá de una serie de documentos que describan:

- [org.2.1] El uso correcto de equipos, servicios e instalaciones, así como lo que se considerará uso indebido.
- [org.2.2] La responsabilidad del personal con respecto al cumplimiento o violación de la normativa: derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.

Refuerzo R1-Documentos específicos.

[org.2.r1.1] Se dispondrá de una documentación de seguridad, desarrollada según lo reflejado en las guías CCN-STIC que resulten de aplicación.

Aplicación de la medida.

- Categoría BÁSICA: org.2.
- Categoría MEDIA: org.2.
- Categoría ALTA: org.2.

3.3 Procedimientos de seguridad [org.3].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA

§ 18 Esquema Nacional de Seguridad

	aplica	aplica	aplica
--	--------	--------	--------

Requisitos.

Se dispondrá de una serie de documentos que detallen de forma clara y precisa cómo operar los elementos del sistema de información:

- [org.3.1] Cómo llevar a cabo las tareas habituales.
- [org.3.2] Quién debe hacer cada tarea.
- [org.3.3] Cómo identificar y reportar comportamientos anómalos.
- [org.3.4.] La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere, precisando cómo efectuar:

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

Refuerzo R1-Validación de procedimientos.

[org.3.r1.1] Se requerirá la validación de los procedimientos de seguridad por la autoridad correspondiente.

Aplicación de la medida.

- Categoría BÁSICA: org.3.
- Categoría MEDIA: org.3.
- Categoría ALTA: org.3.

3.4 Proceso de autorización [org.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

Se establecerá un proceso formal de autorizaciones que cubra todos los elementos del sistema de información concernidos:

- [org.4.1] Utilización de instalaciones, habituales y alternativas.
- [org.4.2] Entrada de equipos en producción, en particular, equipos que involucren criptografía.
- [org.4.3] Entrada de aplicaciones en producción.
- [org.4.4] Establecimiento de enlaces de comunicaciones con otros sistemas.
- [org.4.5] Utilización de medios de comunicación, habituales y alternativos.
- [org.4.6] Utilización de soportes de información.
- [org.4.7] Utilización de equipos móviles. Se entenderá por equipos móviles ordenadores portátiles, tabletas, teléfonos móviles u otros de naturaleza análoga.
- [org.4.8] Utilización de servicios de terceros, bajo contrato o convenio, concesión, encargo, etc.

Aplicación de la medida.

- Categoría BÁSICA: org.4.
- Categoría MEDIA: org.4.
- Categoría ALTA: org.4.

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.

§ 18 Esquema Nacional de Seguridad

4.1 Planificación [op.pl].

4.1.1 Análisis de riesgos [op.pl.1].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+ R2

Requisitos.

Se realizará un análisis de riesgos informal, realizado en lenguaje natural. Es decir, una exposición textual que:

- [op.pl.1.1] Identifique los activos más valiosos del sistema. (Ver op.exp.1).
- [op.pl.1.2] Identifique las amenazas más probables.
- [op.pl.1.3] Identifique las salvaguardas que protegen de dichas amenazas.
- [op.pl.1.4] Identifique los principales riesgos residuales.

Refuerzo R1-Análisis de riesgos semiformal.

Se deberá realizar un análisis de riesgos semiformal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que:

- [op.pl.1.r1.1] Valore cualitativamente los activos más valiosos del sistema.
- [op.pl.1.r1.2] Cuantifique las amenazas más probables.
- [op.pl.1.r1.3] Valore las salvaguardas que protegen de dichas amenazas.
- [op.pl.1.r1.4] Valore el riesgo residual.

Refuerzo R2-Análisis de riesgos formal.

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente, que:

- [op.pl.1.r2.1] Valore cualitativamente los activos más valiosos del sistema.
- [op.pl.1.r2.2] Cuantifique las amenazas posibles.
- [op.pl.1.r2.3] Valore y priorice las salvaguardas adecuadas.
- [op.pl.1.r2.4] Valore y asuma formalmente el riesgo residual.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.1.
- Categoría MEDIA: op.pl.1 + R1.
- Categoría ALTA: op.pl.1 + R2.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

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

- [op.pl.2.1] Documentación de las instalaciones, incluyendo áreas y puntos de acceso.
- [op.pl.2.2] Documentación del sistema, incluyendo equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema (puestos de trabajo y consolas de administración).
- [op.pl.2.3] Esquema de líneas de defensa, incluyendo puntos de interconexión a otros sistemas o a otras redes (en especial, si se trata de internet o redes públicas en general); cortafuegos, DMZ, etc.; y la utilización de tecnologías diferentes para prevenir vulnerabilidades que pudieran perforar simultáneamente varias líneas de defensa.

§ 18 Esquema Nacional de Seguridad

– [op.pl.2.4] Sistema de identificación y autenticación de usuarios, incluyendo el uso de claves concertadas, contraseñas, tarjetas de identificación, biometría, u otras de naturaleza análoga, y el uso de ficheros o directorios para autenticar al usuario y determinar sus derechos de acceso.

Refuerzo R1-Sistema de gestión.

[op.pl.2.r1.1] Sistema de gestión, relativo a la planificación, organización y control de los recursos relativos a la seguridad de la información.

Refuerzo R2-Sistema de gestión de la seguridad con mejora continua.

[op.pl.2.r2.1] Sistema de gestión de la seguridad de la información, con actualización y aprobación periódica.

Refuerzo R3-Validación de datos.

[op.pl.2.r3.1] Controles técnicos internos, incluyendo la validación de datos de entrada, salida y datos intermedios.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.2.
- Categoría MEDIA: op.pl.2 + R1.
- Categoría ALTA: op.pl.2 + R1 + R2 + R3.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

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

- [op.pl.3.1] Atenderá a las conclusiones del análisis de riesgos ([op.pl.1]).
- [op.pl.3.2] Será acorde a la arquitectura de seguridad escogida ([op.pl.2]).
- [op.pl.3.3] Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

Aplicación de la medida.

- Categoría BÁSICA: op.pl.3.
- Categoría MEDIA: op.pl.3.
- Categoría ALTA: op.pl.3.

4.1.4 Dimensionamiento / gestión de la capacidad [op.pl.4].

dimensiones	D		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

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

- [op.pl.4.1] Necesidades de procesamiento.
- [op.pl.4.2] Necesidades de almacenamiento de información: durante su procesamiento y durante el periodo que deba retenerse.
- [op.pl.4.3] Necesidades de comunicación.
- [op.pl.4.4] Necesidades de personal: cantidad y cualificación profesional.
- [op.pl.4.5] Necesidades de instalaciones y medios auxiliares.

§ 18 Esquema Nacional de Seguridad

Refuerzo R1 –Mejora continua de la gestión de la capacidad.

- [op.pl.4.r1.1] Se realizará una previsión de la capacidad y se mantendrá actualizada durante todo el ciclo de vida del sistema.
- [op.pl.4.r1.2] Se emplearán herramientas y recursos para la monitorización de la capacidad.

Aplicación de la medida (por disponibilidad):

- Nivel BAJO: op.pl.4.
- Nivel MEDIO: op.pl.4 + R1.
- Nivel ALTO: op.pl.4 + R1.

4.1.5 Componentes certificados [op.pl.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	aplica

Requisitos.

- [op.pl.5.1]. Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) del CCN, para seleccionar los productos o servicios suministrados por un tercero que formen parte de la arquitectura de seguridad del sistema y aquellos que se referencien expresamente en las medidas de este real decreto.

En caso de que no existan productos o servicios en el CPSTIC que implementen las funcionalidades requeridas, se utilizarán productos certificados de acuerdo a lo descrito en el artículo 19.

Una Instrucción Técnica de Seguridad detallará los criterios relativos a la adquisición de productos de seguridad.

- [op.pl.5.2] Si el sistema suministra un servicio de seguridad a un tercero bajo el alcance del ENS, el producto o productos que en los que se sustente dicho servicio debe superar un proceso de cualificación y ser incluido en el CPSTIC, o aportar una certificación que cumpla con los requisitos funcionales de seguridad y de aseguramiento de acuerdo a lo establecido en el artículo 19.

Refuerzo R1-Protección de emisiones electromagnéticas.

[op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de acuerdo con la normativa en vigor.

Refuerzo R2 - Lista de componentes software.

[op.pl.5.r2.1] Cada producto y servicio incluirá en su descripción una lista de componentes software, acorde a lo especificado en [mp.sw.1.r5].

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.pl.5.
- Categoría ALTA: op.pl.5.

4.2 Control de acceso [op.acc].

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas tendentes a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

Los mecanismos de control de acceso deberán equilibrar la facilidad de uso y la protección de la información y los servicios, primando una u otra característica atendiendo a la categoría de seguridad del sistema.

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

§ 18 Esquema Nacional de Seguridad

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	T A		
nivel	BAJO	MEDIO	ALTO
	aplica	+ R1	+ R1

Requisitos.

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

– [op.acc.1.1] Se podrá utilizar como identificador único los sistemas de identificación previstos en la normativa de aplicación, entre ellos, los sistemas de clave concertada y cualquier otro sistema que las administraciones consideren válido en los términos y condiciones establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

– [op.acc.1.2] Cuando el usuario tenga diferentes roles frente al sistema (como ciudadano o usuario final, como trabajador del organismo o como administrador de los sistemas, por ejemplo) recibirá identificadores singulares para cada perfil, de forma que se recaben siempre los correspondientes registros de actividad, delimitándose los privilegios correspondientes a cada perfil.

– [op.acc.1.3] Cada entidad (entidad, usuario o proceso) que accede al sistema, contará con un identificador singular que permita conocer el destinatario de los mismos y los derechos de acceso que recibe, así como las acciones realizadas por cada entidad.

– [op.acc.1.4] Las cuentas de usuario se gestionarán de la siguiente forma:

a) Cada cuenta (de entidad, usuario o proceso) estará asociada a un identificador único.

b) 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.

c) 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».

– [op.acc.1.5] En los supuestos de comunicaciones electrónicas, las partes intervinientes se identificarán atendiendo a los mecanismos previstos en la legislación europea y nacional en la materia, con la siguiente correspondencia entre los niveles de la dimensión de autenticidad de los sistemas de información a los que se tiene acceso y los niveles de seguridad (bajo, sustancial, alto) de los sistemas de identificación electrónica previstos en el Reglamento (UE) n.º 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE y sus normas de desarrollo o ejecución que resulten de aplicación:

a) Si se requiere un nivel BAJO en la dimensión de autenticidad (anexo I): Nivel de seguridad bajo, sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

b) Si se requiere un nivel MEDIO en la dimensión de autenticidad (anexo I): Nivel de seguridad sustancial o alto (artículo 8 del Reglamento (UE) n.º 910/2014).

c) Si se requiere un nivel ALTO en la dimensión de autenticidad (anexo I): Nivel de seguridad alto (artículo 8 del Reglamento (UE) n.º 910/2014).

Refuerzo R1-Identificación avanzada.

– [op.acc.1.r1.1] La identificación del usuario permitirá al Responsable del Sistema, al Responsable de la Seguridad o a sus respectivos administradores delegados, singularizar a la persona asociada al mismo, así como sus responsabilidades en el sistema.

§ 18 Esquema Nacional de Seguridad

– [op.acc.1.r1.2] Los datos de identificación serán utilizados por el sistema para determinar los privilegios del usuario conforme a los requisitos de control de acceso establecidos en la documentación de seguridad.

– [op.acc.1.r1.3] Se asegurará la existencia de una lista actualizada de usuarios autorizados y mantenida por el administrador del sistema/de la seguridad del sistema.

Aplicación de la medida (por trazabilidad y autenticidad).

– Nivel BAJO: op.acc.1.

– Nivel MEDIO: op.acc.1 +R1.

– Nivel ALTO: op.acc.1+ R1.

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

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	+ R1

Requisitos.

– [op.acc.2.1] Los recursos del sistema se protegerán con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de derechos de acceso suficientes.

– [op.acc.2.2] 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.

– [op.acc.2.3] Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

Refuerzo R1-Privilegios de acceso.

– [op.acc.2.r1.1] Todos los usuarios autorizados deben tener un conjunto de atributos de seguridad (privilegios) que puedan ser mantenidos individualmente.

– [op.acc.2.r1.2] Los privilegios de acceso se implementarán para restringir el tipo de acceso que un usuario puede tener (lectura, escritura, modificación, borrado, etc.).

Refuerzo R2-Control de acceso a dispositivos.

– [op.acc.2.r2.1] Se dispondrá de soluciones que permitan establecer controles de acceso a los dispositivos en función de la política de seguridad de la organización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.2.

– Nivel MEDIO: op.acc.2.

– Nivel ALTO: op.acc.2+ R1.

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

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	n.a.	aplica	+ R1

Requisitos.

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 o no autorizada.

– [op.acc.3.1] Siempre que sea posible, las capacidades de desarrollo y operación no recaerán en la misma persona.

– [op.acc.3.2] Siempre que sea posible, las personas que autorizan y controlan el uso serán distintas.

Refuerzo R1-Segregación rigurosa.

- [op.acc.3.r1.1] Siempre que sea posible, la misma persona no aunar funciones de configuración y mantenimiento del sistema.
- [op.acc.3.r1.2] La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función.

Refuerzo R2-Privilegios de auditoría.

- [op.acc.3.r2.1] Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas.

Refuerzo R3-Acceso a la información de seguridad.

- [op.acc.3.r3.1] El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.).

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: no aplica.
- Nivel MEDIO: op.acc.3.
- Nivel ALTO: op.acc.3 + R1.

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

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	aplica	aplica	aplica

Requisitos.

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

- [op.acc.4.1] Todo acceso estará prohibido, salvo autorización expresa.
- [op.acc.4.2] Mínimo privilegio: los privilegios de cada entidad, usuario o proceso se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.
- [op.acc.4.3] Necesidad de conocer y responsabilidad de compartir: los privilegios se asignarán de forma que las entidades, usuarios o procesos sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio del organismo y toda aquella que resulte necesaria para el usuario estará a su disposición.
- [op.acc.4.4] Capacidad de autorizar: 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 responsable. Los permisos de acceso se revisarán de forma periódica.
- [op.acc.4.5] Se establecerá una política específica de acceso remoto, requiriéndose autorización expresa.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

Nivel BAJO: op.acc.4.

Nivel MEDIO: op.acc.4.

Nivel ALTO: op.acc.4.

4.2.5 Mecanismo de autenticación (usuarios externos) [op.acc.5].

Referente a usuarios que no son usuarios de la organización.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A
-------------	---------

§ 18 Esquema Nacional de Seguridad

nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4]	+ [R2 o R3 o R4] + R5	+ [R2 o R3 o R4] + R5

Requisitos.

- [op.acc.5.1] Antes de proporcionar las credenciales de autenticación a las entidades, usuarios o procesos, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un Prestador Cualificado de Servicios de Confianza o un proveedor de identidad electrónica reconocido por las administraciones públicas, de conformidad con lo dispuesto en la Ley 39/2015, de 1 de octubre.
- [op.acc.5.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.
- [op.acc.5.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
- [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.
- [op.acc.5.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.
- [op.acc.5.6] Las credenciales serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentica termina su relación con el sistema.
- [op.acc.5.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.
- [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.
- [op.acc.5.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

- [op.acc.5.r1.1] Se empleará una contraseña como mecanismo de autenticación.
- [op.acc.5.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + OTP.

- [op.acc.5.r2.1] Se requerirá una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario.

Refuerzo R3-Certificados.

- [op.acc.5.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.
- [op.acc.5.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.
- [op.acc.5.r3.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando un certificado electrónico cualificado.

Refuerzo R4-Certificados en dispositivo físico.

- [op.acc.5.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.
- [op.acc.5.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

§ 18 Esquema Nacional de Seguridad

– [op.acc.5.r4.3] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial, o bien telemático, usando certificado electrónico cualificado.

Refuerzo R5-Registro.

– [op.acc.5.r5.1] Se registrarán los accesos con éxito y los fallidos.

– [op.acc.5.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.5.r6.1] 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.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.5.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

– Nivel BAJO: op.acc.5 + [R1 o R2 o R3 o R4].

– Nivel MEDIO: op.acc.5 + [R2 o R3 o R4] + R5.

– Nivel ALTO: op.acc.5 + [R2 o R3 o R4] + R5.

4.2.6 Mecanismo de autenticación (usuarios de la organización) [op.acc.6].

Esta medida se refiere a personal del organismo, propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en el sistema.

Las guías CCN-STIC desarrollarán los mecanismos y calidades exigibles a cada tipo de factor de autenticación, en función de los niveles de seguridad requeridos por el sistema de información el que se accede y los privilegios concedidos al usuario.

dimensiones	C I T A		
nivel	BAJO	MEDIO	ALTO
	+ [R1 o R2 o R3 o R4] + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R8 + R9	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9

Requisitos.

– [op.acc.6.1] Antes de proporcionar las credenciales a los usuarios, estos deberán conocer y aceptar la política de seguridad del organismo en los aspectos que les afecten.

– [op.acc.6.2] Antes de activar el mecanismo de autenticación, el usuario reconocerá que ha recibido las credenciales de acceso y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, la protección de su confidencialidad y el deber de notificación inmediata en caso de pérdida.

– [op.acc.6.3] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.

– [op.acc.6.4] Las credenciales se cambiarán con una periodicidad marcada por la política de seguridad de la organización.

– [op.acc.6.5] Las credenciales serán inhabilitadas -pudiendo ser regeneradas, en su caso-, cuando conste o se sospeche su pérdida, compromiso o revelación a entidades (personas, equipos o procesos) no autorizadas.

– [op.acc.6.6] Las credenciales serán inhabilitadas cuando el usuario que autentica termina su relación con el sistema.

– [op.acc.6.7] Antes de autorizar el acceso, la información presentada por el sistema será la mínima imprescindible para que el usuario se autentique, evitando todo aquello que pueda, directa o indirectamente, revelar información sobre el sistema o la cuenta, sus características, su operación o su estado. Las credenciales solamente se validarán cuando se tengan todos los datos necesarios y, si se rechaza, no se informará del motivo del rechazo.

§ 18 Esquema Nacional de Seguridad

– [op.acc.6.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, y requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

– [op.acc.6.9] El sistema informará al usuario de sus derechos u obligaciones inmediatamente después de obtener el acceso.

Refuerzo R1-Contraseñas.

– [op.acc.6.r1.1] Se empleará una contraseña como mecanismo de autenticación cuando el acceso se realiza desde zonas controladas y sin atravesar zonas no controladas (véase refuerzo R8).

– [op.acc.6.r1.2] Se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

Refuerzo R2-Contraseña + otro factor de autenticación.

– [op.acc.6.r2.1] Se requerirá un segundo factor tal como «algo que se tiene», es decir, un dispositivo, una contraseña de un solo uso (OTP, en inglés) como complemento a la contraseña de usuario, o «algo que se es».

Refuerzo R3-Certificados.

– [op.acc.6.r3.1] Se emplearán certificados cualificados como mecanismo de autenticación.

– [op.acc.6.r3.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R4-Certificados en dispositivo físico.

– [op.acc.6.r4.1] Se emplearán certificados cualificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

– [op.acc.6.r4.2] El uso del certificado estará protegido por un segundo factor, del tipo PIN o biométrico.

Refuerzo R5-Registro.

– [op.acc.6.r5.1] Se registrarán los accesos con éxito y los fallidos.

– [op.acc.6.r5.2] Se informará al usuario del último acceso efectuado con su identidad.

Refuerzo R6-Limitación de la ventana de acceso.

– [op.acc.6.r6.1] 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.

Refuerzo R7-Suspensión por no utilización.

– [op.acc.6.r7.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

Refuerzo R8-Doble factor para acceso desde o a través de zonas no controladas.

Se denomina «zona controlada» aquella que no es de acceso público, requiriéndose que el usuario, antes de tener acceso al equipo, se haya autenticado previamente de alguna forma (control de acceso a las instalaciones), diferente del mecanismo de autenticación lógica frente al sistema. Un ejemplo de zona no controlada es Internet.

– [op.acc.6.r8.1] Para el acceso desde o a través de zonas no controladas se requerirá un doble factor de autenticación: R2, R3 o R4.

Refuerzo R9-Acceso remoto (todos los niveles).

– [op.acc.6.r9.1] Será de aplicación la ITS de Interconexión de sistemas de información.

– [op.acc.6.r9.2] El acceso remoto deberá considerar los siguientes aspectos:

a) Ser autorizado por la autoridad correspondiente.

b) El tráfico deberá ser cifrado.

§ 18 Esquema Nacional de Seguridad

c) Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.

d) Deberán recogerse registros de auditoría de este tipo de conexiones.

Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad).

- Nivel BAJO: $\text{op.acc.6} + [\text{R1 o R2 o R3 o R4}] + \text{R8} + \text{R9}$.
- Nivel MEDIO: $\text{op.acc.6} + [\text{R1 o R2 o R3 o R4}] + \text{R5} + \text{R8} + \text{R9}$.
- Nivel ALTO: $\text{op.acc.6} + [\text{R1 o R2 o R3 o R4}] + \text{R5} + \text{R6} + \text{R7} + \text{R8} + \text{R9}$.

4.3 Explotación [op.exp].

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

[op.exp.1.1] Se mantendrá un inventario actualizado de todos los elementos del sistema, detallando su naturaleza e identificando a su responsable; es decir, la persona que toma las decisiones relativas al mismo.

Refuerzo R1-Inventario de etiquetado.

– [op.exp.1.r1.1] El etiquetado del equipamiento y del cableado formará parte del inventario.

Refuerzo R2-Identificación periódica de activos.

– [op.exp.1.r2.1] Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

Refuerzo R3-Identificación de activos críticos.

– [op.exp.1.r3.1] Se dispondrá de herramientas que permitan categorizar los activos críticos por contexto de la organización y riesgos de seguridad.

Refuerzo R4-Lista de componentes software.

– [op.exp.1.r4.1] Se mantendrá actualizada una relación formal de los componentes software de terceros empleados en el despliegue del sistema. Esta lista incluirá librerías software y los servicios requeridos para su despliegue (plataforma o entorno operacional). El contenido de la lista de componentes será equivalente a lo requerido en [mp.sw.1.r5].

Aplicación de la medida.

- Categoría BÁSICA: op.exp.1.
- Categoría MEDIA: op.exp.1.
- Categoría ALTA: op.exp.1.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	aplica	aplica

Requisitos.

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

- [op.exp.2.1] Se retiren cuentas y contraseñas estándar.
- [op.exp.2.2] Se aplicará la regla de «mínima funcionalidad», es decir:

§ 18 Esquema Nacional de Seguridad

a) El sistema debe proporcionar la funcionalidad mínima imprescindible para que la organización alcance sus objetivos.

b) No proporcionará funciones injustificadas (de operación, administración o auditoría) al objeto de reducir al mínimo su perímetro de exposición, eliminándose o desactivándose aquellas funciones que sean innecesarias o inadecuadas al fin que se persigue.

– [op.exp.2.3] Se aplicará la regla de «seguridad por defecto», es decir:

a) Las medidas de seguridad serán respetuosas con el usuario y protegerán a éste, salvo que se exponga conscientemente a un riesgo.

b) Para reducir la seguridad, el usuario tendrá que realizar acciones conscientes.

c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

– [op.exp.2.4] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parcheado, cuentas de usuarios, software antivirus, etc. se realizará como si se tratara de máquinas físicas, incluyendo la máquina anfitriona.

Aplicación de la medida.

– Categoría BÁSICA: op.exp.2.

– Categoría MEDIA: op.exp.2.

– Categoría ALTA: op.exp.2.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2+R3

Requisitos.

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

– [op.exp.3.1] Se mantenga en todo momento la regla de "funcionalidad mínima" ([op.exp.2]).

– [op.exp.3.2] Se mantenga en todo momento la regla de "mínimo privilegio" ([op.exp.2]).

– [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas. (Ver [op.acc.4]).

– [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas. (Ver [op.exp.4]).

– [op.exp.3.5] El sistema reaccione a incidentes. (Ver [op.exp.7]).

– [op.exp.3.6] La configuración de seguridad solamente podrá editarse por personal debidamente autorizado.

Refuerzo R1-Mantenimiento regular de la configuración.

– [op.exp.3.r1.1] Existirán configuraciones hardware/software, autorizadas y mantenidas regularmente, para los servidores, elementos de red y estaciones de trabajo.

– [op.exp.3.r1.2] Se verificará periódicamente la configuración hardware/software del sistema para asegurar que no se han introducido ni instalado elementos no autorizados.

– [op.exp.3.r1.3] Se mantendrá una lista de servicios autorizados para servidores y estaciones de trabajo.

Refuerzo R2-Responsabilidad de la configuración.

– [op.exp.3.r2.1] La configuración de seguridad del sistema operativo y aplicaciones, tanto de estaciones y servidores como de la electrónica de red del sistema, será responsabilidad de un número muy limitado de administradores del sistema.

Refuerzo R3-Copias de seguridad.

– [op.exp.3.r3.1] Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

§ 18 Esquema Nacional de Seguridad

Refuerzo R4-Aplicación de la configuración.

– [op.exp.3.r4.1] La configuración de seguridad del sistema operativo y de las aplicaciones se mantendrá actualizada a través de una aplicación o procedimiento manual que permita la instalación de las correspondientes modificaciones de versión y actualizaciones de seguridad oportunas.

Refuerzo R5-Control del estado de seguridad de la Configuración.

– [op.exp.3.r5.1] Se dispondrá de herramientas que permitan conocer de forma periódica el estado de seguridad de la configuración de los dispositivos de red y, en el caso de que resulte deficiente, permitir su corrección.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.3.
- Categoría MEDIA: op.exp.3 + R1.
- Categoría ALTA: op.exp.3 + R1 + R2 + R3.

4.3.4 Mantenimiento y actualizaciones de seguridad [op.exp.4].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1	+R1+R2

Requisitos.

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

- [op.exp.4.1] Se atenderá a las especificaciones de los fabricantes en lo relativo a instalación y mantenimiento de los sistemas, lo que incluirá un seguimiento continuo de los anuncios de defectos.
- [op.exp.4.2] 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 implantación o no de la actualización.
- [op.exp.4.3] El mantenimiento solo podrá realizarse por personal debidamente autorizado.

Refuerzo R1-Pruebas en preproducción.

[op.exp.4.r1.1] Antes de poner en producción una nueva versión o una versión parcheada, se comprobará en un entorno de prueba controlado y consistente en configuración al entorno de producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

Refuerzo R2-Prevención de fallos.

[op.exp.4.r2.1] Antes de la aplicación de las configuraciones, parches y actualizaciones de seguridad se preverá un mecanismo para revertirlos en caso de aparición de efectos adversos.

Refuerzo R3-Actualizaciones y pruebas periódicas.

[op.exp.4.r3.1] Se deberá comprobar de forma periódica la integridad del firmware utilizado en los dispositivos hardware del sistema (infraestructura de red, BIOS, etc.). La periodicidad de estas comprobaciones seguirá las recomendaciones de la Guía CCN-STIC que sea de aplicación.

Refuerzo R4 - Monitorización continua.

[op.exp.4.r4.1] Se desplegará a nivel de sistema una estrategia de monitorización continua de amenazas y vulnerabilidades. Esta estrategia detallará:

1. Los indicadores críticos de seguridad a emplear.

§ 18 Esquema Nacional de Seguridad

2. La política de aplicación de parches de seguridad de los componentes software relacionados en las listas de [op.exp.1.r4], [op.ext.3.r3] y [mp.sw.1.r5]).

3. Los criterios de revisión regular y excepcional de las amenazas sobre el sistema.

Aplicación de la medida.

- Categoría BÁSICA: op.exp.4.
- Categoría MEDIA: op.exp.4 + R1.
- Categoría ALTA: op.exp.4 + R1 + R2.

4.3.5 Gestión de cambios [op.exp.5].

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	n.a.	aplica	+ R1

Requisitos.

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

– [op.exp.5.1] Los cambios se planificarán para reducir el impacto sobre la prestación de los servicios afectados. Para ello, todas las peticiones de cambio se registrarán asignando un número de referencia que permita su seguimiento, de forma equivalente al registro de los incidentes.

– [op.exp.5.2] La información a registrar para cada petición de cambio será suficiente para que quien deba autorizarlos no tenga dudas al respecto y permita gestionarlo hasta su desestimación o implementación.

– [op.exp.5.3] Las pruebas de preproducción, siempre que sea posible realizarlas, se efectuarán en equipos equivalentes a los de producción, al menos en los aspectos específicos del cambio.

– [op.exp.5.4] Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados, explícitamente, de forma previa a su implantación, por el Responsable de la Seguridad.

– [op.exp.5.5] Una vez implementado el cambio, se realizarán las pruebas de aceptación convenientes. Si son positivas, se actualizará la documentación de configuración (diagramas de red, manuales, el inventario, etc.), siempre que proceda.

Refuerzo R1-Prevención de fallos.

– [op.exp.5.r1.1] Antes de la aplicación de los cambios, se deberá tener en cuenta la posibilidad de revertirlos en caso de la aparición de efectos adversos.

– [op.exp.5.r1.2] Todos los fallos en el software y hardware deberán ser comunicados al responsable designado en la organización de la seguridad.

– [op.exp.5.r1.3] Todos los cambios en el sistema deberán documentarse, incluyendo una valoración del impacto que dicho cambio supone en la seguridad del sistema.

Aplicación de la medida.

- Categoría BÁSICA: no aplica.
- Categoría MEDIA: op.exp.5.
- Categoría ALTA: op.exp.5+ R1.

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

dimensiones	Todas		
categoría	BÁSICA	MEDIA	ALTA
	aplica	+ R1+R2	+R1+R2+R3+R4

Requisitos.