



## PROYECTO DE REAL DECRETO POR EL QUE SE REGULA EL ESQUEMA NACIONAL DE SEGURIDAD

(V-1) (14-6-21)

I

El Esquema Nacional de Seguridad (en adelante ENS), regulado por el Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Su aprobación en 2010, con todas las entidades de las Administraciones públicas en su alcance subjetivo, perseguía fundamentar la confianza en que los sistemas de información prestaran sus servicios y custodiaran la información sin interrupciones o modificaciones fuera de control, y sin que la información pudiera llegar a personas no autorizadas, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permitiera a los ciudadanos y a las Administraciones públicas, el ejercicio de sus derechos y el cumplimiento de sus deberes a través de estos medios.

Posteriormente, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público ampliaba el ámbito de aplicación del ENS a todo el sector público; establecía en su artículo 3, que regula los principios generales, que las Administraciones públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos personales, y facilitarán preferentemente la prestación conjunta de servicios a los interesados; y, más adelante, recogía el ENS en su artículo 156.

Por otra parte, la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, recogía en su artículo 13 sobre derechos de las personas en sus relaciones con las Administraciones públicas el relativo a la protección de 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.

El Real Decreto 951/2015, de 23 de octubre vino a actualizar el ENS a la luz de la experiencia y conocimiento en su aplicación, de la situación de ciberseguridad del momento, y de la evolución del marco legal, particularmente europeo, para adecuarse a lo previsto en el Reglamento 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.



A lo anterior se añadió la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales que establece que el ENS incluirá aquellas medidas que deberán implantarse 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); y que prescribe la implantación de las medidas de seguridad del ENS a las entidades del sector público e, indirectamente, a las del Sector Privado que colaboren con aquellas en la prestación de servicios públicos que involucren el tratamiento de datos personales.

Además, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, como respuesta al mandato de transposición de 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, señalaba la necesidad de tener en cuenta el ENS en el momento de elaborar las disposiciones reglamentarias, instrucciones y guías, y adoptar las medidas correspondientes, a las que estuvieran sometidas las entidades de su ámbito de aplicación. Su desarrollo, el 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, señala que las medidas para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esencial 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.

El ENS, con vocación europeísta ha tomado asimismo en consideración otras regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información, tal como 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) Nº 526/2013 («Reglamento sobre la Ciberseguridad»).

Además, la Estrategia Nacional de Ciberseguridad, publicada en 2019 persigue la consolidación de un marco nacional coherente e integrado que garantice la protección de la información y, por consiguiente, de los datos personales, manejados por el sector público y por los servicios, sean o no esenciales, de sus sistemas, así como de las redes que los soportan. Su cumplimiento requiere la implantación de medidas de seguridad enfocadas a mejorar las capacidades de prevención, detección y respuesta ante incidentes, desarrollando nuevas soluciones, reforzando la coordinación y adaptando el ordenamiento jurídico.

Finalmente, el Plan de Digitalización de las Administraciones Públicas, uno de los instrumentos principales para la ejecución de los fondos del Componente 11 «Modernización de las Administraciones Públicas» del Plan de Recuperación, Transformación y Resiliencia, así como para el desarrollo de las inversiones y reformas



previstas en la agenda España Digital 2025, contempla la actualización del ENS entre las reformas normativas a abordar con el fin de evolucionar la política de seguridad de las Administraciones Públicas españolas (que alcanza a todas las entidades del sector público), tomando en cuenta las regulaciones de la Unión Europea dirigidas a incrementar el nivel de ciberseguridad de los sistemas de información. Se trata de una reforma que se ve complementada con la inversión destinada a constituir el 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 en 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.

## II

El Real Decreto 3/2010, de 8 de enero, establece que el ENS se desarrollará y perfeccionará a lo largo del tiempo en paralelo al progreso de los servicios de administración electrónica, la evolución de la tecnología, los nuevos estándares internacionales sobre seguridad y auditoría, y la consolidación de las infraestructuras que le sirven de apoyo, manteniéndose actualizado de manera permanente.

Desde la aparición del ENS en 2010, la realidad nos muestra un escenario de incremento de los ciberataques, en número, frecuencia y sofisticación, con agentes y actores de la amenaza que han ampliado sus capacidades técnicas y su operativa; y que, aprovechando la dependencia de las tecnologías de la información y las comunicaciones de nuestra sociedad y la interconexión de los sistemas, vienen afectando, incesantemente, 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, comprometiendo el normal desenvolvimiento social y económico del país y el ejercicio de los derechos y libertades de los ciudadanos.

Las amenazas son sofisticadas y están evolucionando continuamente sus tácticas, técnicas, métodos y procedimientos. Por ello, en un mundo hiperconectado como el actual, implementar seguridad en el ciberespacio, al tiempo que se garantiza la privacidad y la protección de los datos de los ciudadanos, se ha convertido en una prioridad estratégica.

En este sentido, la amenaza de ataques cibernéticos es un riesgo demasiado grande para que el Gobierno o las empresas lo aborden por sí solos. Los gobiernos y el sector privado comparten el interés y la responsabilidad de enfrentarse juntos a la ciberamenaza dado que a medida que aumenta el papel de la tecnología en la sociedad, la ciberseguridad se convierte en un desafío cada vez mayor.

Desde la publicación del ENS, y tras su actualización en 2015, se han producido notables cambios: la progresiva transformación digital de nuestra sociedad, el nuevo escenario de la ciberseguridad o el avance de las tecnologías de aplicación. Todo ello, con modificaciones del marco legal en materia de procedimiento administrativo y régimen jurídico del sector público, seguridad de las redes y sistemas de información, así como el de protección de datos y del marco estratégico de ciberseguridad, con la Estrategia de 2019. Además, se ha extendido la implantación del ENS con 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 el CCN-CERT, del Centro Criptológico Nacional (CCN).

Durante todo este periodo, la transformación digital de las Administraciones públicas españolas, y del sector público en general, ha progresado significativamente, suponiendo una mejora en la prestación de sus servicios y un mayor acercamiento a los ciudadanos. Ahora bien, la transformación digital también ha supuesto un incremento de los riesgos asociados a los sistemas de información que sustentan los servicios públicos y, por tanto, a la información que manejan. El Sector Privado está igualmente inmerso en la transformación digital de sus procesos de negocio, de forma que sus sistemas de información están expuestos al mismo tipo de amenazas y riesgos. Por ello, particularmente aquellos 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 requieren los sistemas y la información concernidos en el servicio, atendiendo, además, a los especiales requerimientos establecidos en la Ley Orgánica 3/2018, de 5 de diciembre.

De hecho, desde entonces, se ha evidenciado que los sistemas de información están expuestos de forma cada vez más intensa a la materialización de amenazas del ciberespacio, a los ciberincidentes, que siguen una pauta de crecimiento en frecuencia, sofisticación, alcance y severidad del impacto. Diversos organismos internacionales y del ámbito de la Unión Europea, así como las sucesivas estrategias de ciberseguridad, de 2013 y, particularmente la Estrategia Nacional de Ciberseguridad 2019, reconocen que los ciberincidentes que se materializan en los sistemas de información de las organizaciones constituyen una de las amenazas más significativas para el normal desenvolvimiento de las sociedades, instituciones, empresas y ciudadanos. 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 nacionales y europeas 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 último, los postulados recogidos en el reciente 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, exigen la recepción de un actualizado marco de la ciberseguridad pública, pretensión de la que asimismo trae causa este renovado ENS.

A la luz de todo lo anterior se suscita la conveniencia, cuando no necesidad, de actualizar el ENS atendiendo a tres grandes cuestiones.

En primer lugar, se persigue alinear el ENS con el marco normativo y el contexto estratégico existente para facilitar 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, actualizar referencias al marco legal actualizado y revisar la formulación de ciertas cuestiones a la luz del mismo, alinearlos con el contexto establecido en la Estrategia Nacional de Ciberseguridad 2019 y mejorar diversos aspectos del cuerpo



para simplificar, precisar o armonizar, eliminar aspectos excesivos, o añadir aquellos que se identifican como necesarios.

En segundo lugar, se persigue introducir la capacidad de ajustar los requisitos del ENS para adaptarse 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 servicios, que aconseja la inclusión en el ENS del concepto de “perfil de cumplimiento específico” que, aprobado por el Centro Criptológico Nacional (CCN), permitan alcanzar una adaptación al ENS más eficaz y eficiente, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.

En tercer lugar, se persigue actualizar el ENS para facilitar una mejor respuesta a las tendencias en ciberseguridad, reducir vulnerabilidades y promover la vigilancia continua, mediante la revisión, a la luz del estado del arte, de los principios básicos, los requisitos mínimos y las medidas de seguridad.

La evolución de las amenazas, los nuevos vectores de ataque y el desarrollo de nuevos mecanismos de respuesta a los mismos, así como la necesidad de mantener la conformidad y el alineamiento con las regulaciones nacionales y europeas de aplicación, exigen actualizar las medidas de seguridad a esta nueva realidad, tratando al tiempo de acompañar la determinación de los controles de protección de los sistemas con el esfuerzo económico y de recursos requerido, buscando siempre la proporcionalidad de los medios empleados al nivel de seguridad demandado.

La modificación del marco táctico y operativo en el que se desenvuelven las ciberamenazas y sus correlativas salvaguardas obliga, más allá de los siempre presentes ajustes editoriales, a actualizar igualmente el elenco de medidas de seguridad contenidas en el Anexo II, añadiendo, eliminando o modificando controles y sub-controles, e incluyendo un nuevo sistema de referencias más moderno y adecuado, sobre la base de la existencia de un requisito general y unos posibles refuerzos, alineados con el nivel de seguridad perseguido, todo ello con el objetivo de afianzar de manera proporcionada la seguridad de los sistemas de información concernidos, facilitando su implantación y auditoría.

### III

El real decreto se estructura en nueve capítulos, cuatro 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, ámbito de aplicación, las definiciones y estándares aplicables para las que se remite al anexo IV y las Instrucciones técnicas de seguridad y guías de seguridad. El ámbito de aplicación se remite al ámbito del artículo 2 de la Ley 40/2015, de 1 de octubre y, se añade que también será de aplicación a los sistemas que manejan o tratan información clasificada, sin perjuicio de que pudiera resultar necesario complementar las medidas de seguridad previstas en el presente 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. Por su parte, en el artículo 4 se prevé que en desarrollo de lo



dispuesto en el real decreto, el Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del CCN, aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de la Secretaría de Estado Digitalización e Inteligencia Artificial. Asimismo, 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).

El Capítulo II regula en cada uno de sus diferentes artículos los principios básicos que deben regir el ENS, enumerados en su artículo 5, a saber: 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 13 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, en su artículo 28, se indica que para dar cumplimiento a tales requisitos mínimos se deberán adoptar las medidas referidas en el Anexo II apreciando 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 son igual o más eficaces 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 retroalimentarse 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, que se desarrolla íntegramente en el artículo 31, detallando las características del procedimiento de auditoría, así como de los correspondientes informes.

El Capítulo V relativo al Estado de la Seguridad de los sistemas, se desarrolla íntegramente en el artículo 32, destacando 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.

El Capítulo VI regula la prevención, detección y respuesta a incidentes de seguridad, separando por un lado los aspectos relativos a la capacidad de respuesta (artículo 33) y, por otro, lo relativo a la prestación de los servicios de respuesta a incidentes de seguridad a las entidades del Sector Público (artículo 34).



En el Capítulo VII, que ocupa los artículos 35 a 38, se definen las normas de conformidad. Dichas normas 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.

El Capítulo VIII compuesto por su único artículo 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 los nuevos vectores de ataque y amenazas.

Por último, el Capítulo IX 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.

Por su parte, las cuatro disposiciones adicionales regulan, respectivamente, 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; la habilitación a la Comisión Sectorial de Administración Electrónica para proponer el desarrollo de las instrucciones técnicas de seguridad para lograr la mejor implantación del ENS; la tercera prevé la 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 y, la cuarta, la aplicación de los requisitos del ENS a los sistemas de información que permitan los tratamientos de datos personales de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre.

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

Por último, el real decreto cuenta con tres disposiciones finales. La primera enumera los títulos competenciales; la segunda 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 el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado y la disposición final tercera ordena la entrada en vigor al 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 diferentes medidas de seguridad estructuradas en tres grupos: marco organizativo, constituido por el conjunto de medidas relacionadas con la organización global de la seguridad; marco operacional, formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin; y 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; el Anexo III trata la Auditoría de la seguridad y el Anexo IV incluye el glosario de términos y definiciones.



El real decreto 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), 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 los otros aspectos concretos de la normativa mencionada en este preámbulo. La norma es 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 jurídico, estableciéndose un marco normativo estable, integrado y claro.

Durante el procedimiento de elaboración de la norma, se han formalizado los trámites de consulta pública e información pública, que establece la Ley en cumplimiento del principio de transparencia, quedando además justificados en el preámbulo los objetivos que persigue este real decreto. 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.

Asimismo, el proyecto ha sido informado por la Agencia Española de Protección de Datos y 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 a informe de los diferentes ministerios.

El real decreto se aprueba en ejercicio de las competencias previstas en los artículos 149.1.18<sup>a</sup>, 149.1.21<sup>a</sup> y 149.1.29.<sup>a</sup> 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 Vicepresidenta Segunda y Ministra de Asuntos Económicos y Transformación Digital, de acuerdo con el Consejo de Estado y previa deliberación del Consejo de Ministros en su reunión del día de de 2021,

DISPONGO:

## ÍNDICE

### **CAPÍTULO I. Disposiciones generales**

Artículo 1. Objeto

Artículo 2. Ámbito de aplicación

Artículo 3. Definiciones y estándares

Artículo 4. Instrucciones técnicas de seguridad y guías de seguridad

### **CAPÍTULO II. Principios básicos**

Artículo 5. Principios básicos del Esquema Nacional de Seguridad



Artículo 6. La seguridad como un proceso integral

Artículo 7. Gestión de la seguridad basada en los riesgos

Artículo 8. Prevención, detección y respuesta

Artículo 9. Existencia de líneas de defensa

Artículo 10. Vigilancia continua y reevaluación periódica

Artículo 11. Diferenciación de responsabilidades

### **CAPÍTULO III. Política de seguridad y requisitos mínimos de seguridad**

Artículo 12. Política de seguridad y requisitos mínimos de seguridad

Artículo 13. Organización e implantación del proceso de seguridad

Artículo 14. Análisis y gestión de riesgos

Artículo 15. Gestión de personal

Artículo 16. Profesionalidad

Artículo 17. Autorización y control de los accesos

Artículo 18. Protección de las instalaciones

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

Artículo 20. Mínimo privilegio

Artículo 21. Integridad y actualización del sistema

Artículo 22. Protección de información almacenada y en tránsito

Artículo 23. Prevención ante otros sistemas de información interconectados

Artículo 24. Registro de actividad y detección de código dañino

Artículo 25. Incidentes de seguridad

Artículo 26. Continuidad de la actividad

Artículo 27. Mejora continua del proceso de seguridad

Artículo 28. Cumplimiento de los requisitos mínimos

Artículo 29. Infraestructuras y servicios comunes

Artículo 30. Perfiles de cumplimiento específicos.



#### **CAPÍTULO IV. Auditoría de la seguridad**

Artículo 31. Auditoría de la seguridad

#### **CAPÍTULO V. Estado de la seguridad de los sistemas**

Artículo 32. Informe del estado de la seguridad

#### **CAPÍTULO VI. Prevención, detección y respuesta a incidentes de seguridad**

Artículo 33. Capacidad de respuesta a incidentes de seguridad de la información

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

#### **CAPÍTULO VII. Normas de conformidad**

Artículo 35. Administración Digital

Artículo 36. Ciclo de vida de servicios y sistemas

Artículo 37. Mecanismos de control

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

#### **CAPÍTULO VIII. Actualización del Esquema Nacional de Seguridad**

Artículo 39. Actualización permanente

#### **CAPÍTULO IX. Categorización de los sistemas de información**

Artículo 40. Categorías de seguridad

Artículo 41. Facultades

Disposición adicional primera. Formación

Disposición adicional segunda. Desarrollo del Esquema Nacional de Seguridad.

Disposición adicional tercera. Conformidad con el Esquema Nacional de Seguridad de los servicios prestados por terceros pertenecientes al sector privado.

Disposición adicional cuarta. Aplicación de los requisitos del Esquema Nacional de Seguridad a los sistemas de información que permitan los tratamientos de datos personales de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Disposición transitoria única. Adecuación de sistemas



Disposición derogatoria única. Derogación normativa

Disposición final primera. Título habilitante

Disposición final segunda. Desarrollo normativo

Disposición final tercera. Entrada en vigor

## **ANEXOS**

ANEXO I. Categorías de los sistemas

ANEXO II. Medidas de seguridad

ANEXO III. Auditoría de la seguridad

ANEXO IV. Glosario

## **CAPÍTULO I**

### **Disposiciones generales**

#### **Artículo 1. Objeto.**

1. El presente real decreto tiene por objeto regular el Esquema Nacional de Seguridad (en adelante, ENS), establecido en el apartado 2 del artículo 156 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, para asegurar el acceso, confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

#### **Artículo 2. Ámbito de aplicación.**

1. El ámbito de aplicación del presente real decreto es el comprendido en el artículo 2 de la Ley 40/2015, de 1 de octubre, de acuerdo con lo previsto en el apartado 2 del artículo 156 de la misma.

2. Asimismo será de aplicación a los sistemas que manejan o tratan información clasificada, sin perjuicio de que pudiera resultar necesario complementar las medidas de seguridad previstas en el presente 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.

#### **Artículo 3. Definiciones y estándares.**



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

**Artículo 4.** *Instrucciones técnicas de seguridad y guías de seguridad.*

1. En desarrollo de lo dispuesto en el presente real decreto, el Ministerio de Asuntos Económicos y Transformación Digital, a propuesta de la Comisión Sectorial de Administración Electrónica y a iniciativa del Centro Criptológico Nacional (en adelante, CCN), aprobará las instrucciones técnicas de seguridad de obligado cumplimiento, que se publicarán mediante Resolución de la Secretaría de Estado Digitalización e Inteligencia Artificial.

Para la redacción y mantenimiento de las instrucciones técnicas de seguridad se constituirán los correspondientes grupos de trabajo en los órganos colegiados con competencias en materia de administración electrónica.

2. Las instrucciones técnicas de seguridad tendrán en cuenta las normas armonizadas por la Unión Europea que resulten de aplicación.

3. Para el mejor cumplimiento de lo establecido en el presente 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), que se incorporarán al conjunto documental utilizado para la realización de las auditorías de seguridad.

## 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 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.

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

1. La seguridad es un proceso integral constituido por todos los elementos técnicos, humanos, materiales 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 coordinación o instrucciones inadecuadas, 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, los servicios a prestar y 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 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 informaciones 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.

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 prestación de los servicios.

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 y los servicios que consideran críticos. 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, los deberes y responsabilidades del cargo, 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.

2. Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad que articule la gestión continuada de la seguridad y que será aprobada por el titular del órgano superior correspondiente.

En el caso de los organismos públicos y entidades de derecho público vinculados o dependientes, su política de seguridad será aprobada por la persona titular de la Presidencia o de la Dirección.

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.

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.

3. 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.
- 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.
- m) Incidentes de seguridad.
- n) Continuidad de la actividad.
- ñ) Mejora continua del proceso de seguridad.

4. Los requisitos mínimos se exigirán en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28 del presente real decreto, 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 de este real decreto, deberá identificar inequívocamente a los responsables de



velar por su cumplimiento y ser conocida por todos los miembros de la organización, distinguiendo los siguientes roles:

- 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 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, 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, salvo en aquellas situaciones excepcionales en las que la ausencia justificada de recursos haga necesario que, de manera temporal, ambas funciones recaigan en la misma persona.
4. Una instrucción técnica de seguridad regulará el Esquema de Certificación de Responsables de la Seguridad, que recogerá las condiciones y requisitos exigibles en 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) de Seguridad de la información, 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, así como la gestión de los incidentes para el ámbito del servicio que provea.
- Este POC de seguridad, será el propio Responsable de Seguridad de la organización contratada o 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 y las comunicaciones realizará su propia gestión de riesgos.
2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.
3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.



#### **Artículo 15. Gestión de personal.**

1. El personal, propio o ajeno, relacionado con los sistemas de información sujetos a lo dispuesto en el presente real decreto, deberá ser formado e informado de sus deberes y obligaciones 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 del presente 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 el diseño curricular y experiencia necesaria del personal para el desarrollo de su puesto trabajo.

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

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación del presente 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.

#### **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 sistemas de información del ámbito de aplicación del presente 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 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 de que se trate, determinará dentro de sus competencias:

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

El proceso indicado se efectuará teniendo en cuenta los criterios y metodologías de evaluación nacionales e internacionales reconocidas por este organismo.

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, es decir:

- a) El sistema proporcionará la funcionalidad exclusivamente 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, modificación o retirada de cualquier elemento físico o lógico, que se incorporará al catálogo actualizado de activos del sistema, 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.

#### **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 el presente real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, 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, en particular, si se conecta a redes públicas, y se reforzarán las tareas de prevención, detección y respuesta a incidentes de seguridad.

De acuerdo con lo previsto en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, se entiende por red pública aquella red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

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 la actividad y detección de código dañino.*

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

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 (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), los sujetos comprendidos en el artículo 2 de este real decreto podrán analizar las comunicaciones entrantes o salientes, 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.

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 del presente real decreto dispondrá de procedimientos de gestión de incidentes de seguridad de acuerdo con la correspondiente instrucción técnica de seguridad y, en caso de tratarse de un operador de servicios esenciales, 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 los mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como 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.

**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 relativos a 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. Cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en especial su Disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el presente real decreto.



3. Las medidas a las que se refieren los apartados 1 y 2 tendrán la condición de mínimos exigibles, y podrán ser ampliados al prudente arbitrio del responsable de la seguridad, incluyendo alguno de los refuerzos no exigidos inicialmente que se relacionan en algunas medidas, 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 y los refuerzos correspondientes del Anexo II seleccionados se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el responsable de la seguridad.

4. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias, siempre y cuando se justifique documentalmente que protegen, igual o mejor, el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del presente real decreto. 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 el artículo 4 de este real decreto facilitará la implementación 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 el presente real decreto. Los supuestos concretos de utilización de estas infraestructuras y servicios serán determinados por cada Administración.

**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. Análogamente, para posibilitar la adecuada implantación y configuración de soluciones o plataformas suministradas por terceros, que vayan a ser usadas por las entidades del ámbito de aplicación del presente 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 el presente 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 lo establecido en el artículo 4 de este real decreto sobre instrucciones técnicas de seguridad y guías de seguridad.

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

### **Auditoría de la seguridad**

#### **Artículo 31. Auditoría de la seguridad.**

1. Los sistemas de información comprendidos en el ámbito de aplicación del presente 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 el Anexo I y Anexo III del presente real decreto y de conformidad con lo regulado en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de la Información.

3. En el marco de lo dispuesto en el artículo 41 de la Ley 40/2015, de 1 de octubre, la auditoría profundizará en los detalles del sistema hasta el nivel que considere que proporciona evidencia suficiente y relevante, dentro del alcance establecido para la auditoría.

4. En la realización de 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.

5. El informe de auditoría deberá dictaminar sobre el grado de cumplimiento del presente real decreto identificando los hallazgos de cumplimiento o 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 Auditoría de la Seguridad de los Sistemas de Información.

6. 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.

7. 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.

8. 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.

## CAPITULO V

### Estado de la seguridad de los sistemas

**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 el presente 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 presente real decreto, 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 Digital en la Administración General del Estado.

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.

## CAPÍTULO VI

### Prevención, detección y respuesta a incidentes de seguridad

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

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. 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 (CSIRT, por su acrónimo en inglés de *Computer Security Incident Response Team*) en materia de seguridad de las redes y sistemas de información del sector público comprendido en la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, y en la Ley 40/2015, de 1 de octubre.

4. El CCN-CERT determinará técnicamente el riesgo de reconexión de un sistema, tras un incidente de seguridad, indicando los procedimientos a seguir y las salvaguardas a implementar para reducir el impacto para, en la manera de lo posible, evitar que se den las circunstancias que lo propiciaron.

No obstante lo anterior, para poder autorizar a interconectar de nuevo, es preceptivo un informe de superficie de exposición del CCN-CERT que determine que el sistema está recuperado y que el riesgo de infección es asumible.

La Secretaría General de Administración Digital, tomando en consideración dicho informe de superficie de exposición del CCN-CERT, decidirá sobre la reconexión a los medios y servicios comunes comprendidos bajo su ámbito de responsabilidad, incluidos los compartidos o transversales.

5. 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 el Instituto Nacional de Ciberseguridad 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 (Computer Security Incident Response Team, CSIRT), quien, sin perjuicio de sus competencias, lo pondrá inmediatamente en conocimiento del CCN-CERT, así mismo sin perjuicio de lo previsto sobre la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes en los artículos 9, 10 y 11 del Real Decreto 43/2021, de 26 de enero.

**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 del presente 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 y registros de auditoría de los sistemas afectados, configuraciones 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 y recomendaciones para aplicar el ENS y para garantizar la seguridad de los sistemas de información del ámbito de aplicación del presente 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 VII

### 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 el presente real decreto.

2. 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, el órgano competente será el CCN.

#### **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 del presente real decreto y, en su caso, sus organismos, órganos, departamentos o 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 y la disposición adicional tercera de este real decreto 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 formal para la certificación de su conformidad, 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 formal de certificación.

Tanto el procedimiento de autoevaluación como la auditoría formal de certificación se realizarán según lo dispuesto en el artículo 31 y el Anexo III de este real decreto 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 a las declaraciones y certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la mencionada instrucción técnica de seguridad.

## CAPÍTULO VIII

### **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 y la aparición o consolidación de nuevos estándares internacionales sobre seguridad y auditoría.

## CAPÍTULO IX

### **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 criterio del 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 afectará 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 del presente real decreto.

#### **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 cada información o servicio afectados.

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

La Comisión Sectorial de Administración Electrónica, con el objetivo de lograr la mejor implantación del ENS, propondrá el desarrollo de las instrucciones técnicas de seguridad, que se aprobarán conforme al procedimiento señalado en el artículo 4 del presente real decreto.

#### **Disposición adicional tercera. Conformidad con el Esquema Nacional de Seguridad de los servicios prestados por terceros pertenecientes al sector privado.**

El presente real decreto resulta 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 o provean soluciones a las entidades del sector público para el ejercicio por estas de sus competencias y potestades administrativas.

Los Pliegos de Prescripciones Administrativas y/o Técnicas que regulen los procedimientos de contratación que publiquen las entidades del ámbito de aplicación del presente real decreto, 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 terceros.

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



**Disposición adicional cuarta.** *Aplicación de los requisitos del Esquema Nacional de Seguridad a los sistemas de información que permitan los tratamientos de datos personales de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

En aplicación de lo dispuesto en el artículo 28.2 de este real decreto, los requisitos establecidos en el mismo se aplicarán a los sistemas de información que permitan los tratamientos de datos personales en el ámbito subjetivo y con el alcance al que se refieren el artículo 77.1 y la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre.

**Disposición transitoria única.** *Adecuación de sistemas.*

1. Los sistemas de información del ámbito de aplicación del presente real decreto, preexistentes a su entrada en vigor, 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 del presente real decreto.

2. Los nuevos sistemas de información aplicarán lo establecido en el presente 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 el presente real decreto.

**Disposición final primera.** *Título habilitante.*

El presente real decreto se dicta en virtud de lo establecido en los artículos 149.1.18<sup>a</sup>, 149.1.21.<sup>a</sup> y 149.1.29.<sup>a</sup> 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 autoriza 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 el presente real decreto, sin perjuicio de las competencias de las comunidades autónomas de desarrollo y ejecución de la legislación básica del Estado.

**Disposición final tercera.** *Entrada en vigor.*

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



## **ANEXOS**

### **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 afectará 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 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.

Se entenderá por perjuicio limitado:

1º La reducción de forma apreciable de la capacidad de la organización para



desarrollar eficazmente sus competencias, aunque estas sigan desempeñándose.

2º Causar un daño menor en los activos de la organización.

3º El incumplimiento formal de alguna ley o regulación, que tenga carácter de subsanable.

4º Causar un perjuicio menor a algún individuo, que pese a resultar molesto, pueda ser fácilmente reparable.

5º 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:

1º La reducción significativa de la capacidad de la organización para desarrollar eficazmente sus competencias, aunque estas sigan desempeñándose.

2º Causar un daño significativo en los activos de la organización.

3º El incumplimiento material de alguna ley o regulación, o el incumplimiento formal que no tenga carácter de subsanable.

4º Causar un perjuicio significativo a algún individuo, de difícil reparación.

5º 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:

1º. La anulación efectiva de la capacidad de la organización para desarrollar eficazmente sus competencias.

2º. Causar un daño muy grave, e incluso irreparable, de los activos de la organización.

3º. El incumplimiento grave de alguna ley o regulación.

4º. Causar un perjuicio grave a algún individuo, de difícil o imposible reparación.

5º. 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.

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

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 del sistema de información a proteger.

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

a) Marco organizativo [org]. Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

b) Marco operacional [op]. Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

c) Medidas de protección [mp]. Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

#### 2. Selección de medidas de seguridad

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

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

2. A los efectos de facilitar el cumplimiento de lo dispuesto en este Anexo, cuando en un sistema de información existan sistemas que requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad 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 4 del presente 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		Dimensiones de seguridad afectadas	NIVEL DE LAS DIMENSIONES DE SEGURIDAD		
			BAJO	MEDIO	ALTO
			CATEGORÍA DEL SISTEMA		
			BÁSICA	MEDIA	ALTA
<b>org</b>	<b>Marco organizativo</b>				
org.1	Política de seguridad	Todas	aplica	aplica	aplica
org.2	Normativa de seguridad	Todas	aplica	aplica	aplica
org.3	Procedimientos de seguridad	Todas	aplica	aplica	aplica
org.4	Proceso de autorización	Todas	aplica	aplica	aplica
<b>op</b>	<b>Marco operacional</b>				
op.pl	Planificación				
op.pl.1	Análisis de riesgos	Todas	aplica	+ R1	+ R2
op.pl.2	Arquitectura de Seguridad	Todas	aplica	+ R1	+ R1 + R2 + R3
op.pl.3	Adquisición de nuevos componentes	Todas	aplica	aplica	aplica
op.pl.4	Dimensionamiento/gestión de la capacidad	D	aplica	+ R1	+ R1
op.pl.5	Componentes certificados	Todas	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	Protección 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]	+ [R1 o R2 o R3]	+ [R2 o R3] + R4
op.acc.6	Mecanismo de autenticación (usuarios de la organización)	C I T A	+ [R1 o R2 o R3]	+ [R2 o R3] + R4	+ R3 + R4 + R5
op.exp	Explotación				
op.exp.1	Inventario de activos	Todas	aplica	aplica	aplica
op.exp.2	Configuración de seguridad	Todas	aplica	+ R1	+ R1
op.exp.3	Gestión de la configuración de seguridad	Todas	aplica	+ R1	+ R1 + R2 + R3
op.exp.4	Mantenimiento y actualizaciones de seguridad	Todas	aplica	+ R1	+ R1 + R2
op.exp.5	Gestión de cambios	Todas	n.a.	aplica	+ R1
op.exp.6	Protección frente a código dañino	Todas	aplica	+ R1	+ R1 + R2 + R3
op.exp.7	Gestión de incidentes	Todas	aplica	+ R1 + R2	+ R1 + R2
op.exp.8	Registro de la actividad	Todas	aplica	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4 + R5
op.exp.9	Registro de la gestión de incidentes	Todas	aplica	aplica	aplica
op.exp.11	Protección de claves criptográficas	Todas	aplica	+ R1	+ R1
op.ext	Recursos externos				
op.ext.1	Contratación y acuerdos de nivel de servicio	Todas	n.a.	aplica	aplica
op.ext.2	Gestión diaria	Todas	n.a.	aplica	aplica
op.ext.3	Protección de la cadena de suministro	Todas	n.a.	n.a.	aplica
op.ext.4	Interconexión de sistemas	Todas	n.a.	aplica	+ R1
op.nub	Servicio en la nube				
op.nub.1	Protección de servicios en la nube	Todas	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	Todas	aplica	+ R1	+ R1 + R2
op.mon.2	Sistema de métricas	Todas	aplica	+ R1 + R2	+ R1 + R2
op.mon.3	Vigilancia	Todas	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4 + R5 + R6
<b>mp</b>	<b>Medidas de protección</b>				
mp.if	Protección de las instalaciones e infraestructuras				
mp.if.1	Áreas separadas y con control de acceso	Todas	aplica	aplica	aplica
mp.if.2	Identificación de las personas	Todas	aplica	aplica	aplica
mp.if.3	Acondicionamiento de los locales	Todas	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	Todas	aplica	aplica	aplica
mp.per	Gestión del personal				
mp.per.1	Caracterización del puesto de trabajo	Todas	n.a.	aplica	aplica
mp.per.2	Deberes y obligaciones	Todas	aplica	+ R1	+ R1
mp.per.3	Concienciación	Todas	aplica	aplica	aplica
mp.per.4	Formación	Todas	aplica	aplica	aplica
mp.eq	Protección de los equipos				
mp.eq.1	Puesto de trabajo despejado	Todas	aplica	+ R1	+ R1
mp.eq.2	Bloqueo de puesto de trabajo	A	n.a.	aplica	+ R1
mp.eq.3	Protección de dispositivos portátiles	Todas	aplica	+ R1	+ 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	Todas	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	Todas	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	aplica	aplica	aplica
mp.si.2	Criptografía	C I	n.a.	aplica	+ R1
mp.si.3	Custodia	Todas	aplica	aplica	aplica
mp.si.4	Transporte	Todas	aplica	aplica	aplica
mp.si.5	Borrado y destrucción	C	aplica	aplica	aplica
mp.sw	Protección de las aplicaciones informáticas				
mp.sw.1	Desarrollo de aplicaciones	Todas	n.a.	+ R1 + R2 + R3 + R4	+ R1 + R2 + R3 + R4
mp.sw.2	Aceptación y puesta en servicio	Todas	aplica	+ R1	+ R1
mp.info	Protección de la información				
mp.info.1	Datos personales	Todas	aplica	+ R1 + R2	+ R1 + R2
mp.info.2	Calificación de la información	C	n.a.	aplica	aplica
mp.info.4	Firma electrónica	I A	aplica	+ R1 + R2 + R3	+ R1 + R2 + R3 + R4



mp.info.5	Sellos de tiempo	T	n.a.	n.a.	aplica
mp.info.6	Limpieza de documentos	C	aplica	aplica	aplica
mp.info.9	Copias de seguridad	D	aplica	aplica	+ R1
mp.s	Protección de los servicios				
mp.s.1	Protección del correo electrónico	Todas	aplica	aplica	aplica
mp.s.2	Protección de servicios y aplicaciones web	Todas	+ [R1 o R2]	+ [R1 o R2]	+ R2 + R3
mp.s.3	Protección de la navegación web	Todas	aplica	aplica	+ R1
mp.s.8	Protección frente a denegación de servicio	D	n.a.	aplica	+ R1

En las tablas del presente Anexo se han empleado las siguientes convenciones:

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

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

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

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 indicar que se puede elegir entre aplicar un refuerzo u otro, se indicará entre corchetes [Rm o Rn].

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 bien, requieren un esfuerzo en seguridad superior al de categoría MEDIA.

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 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) Por último, se indica el conjunto de requisitos y refuerzos exigidos en función de los niveles de seguridad o de la categoría 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.



### 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 11 del presente 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, los miembros 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 avanzada, 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
	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.

##### 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 semi-formal

Se deberá realizar un análisis de riesgos semi-formal, 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.
- [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 seguridad con mejora continua

[op.pl.2.r2.1] Sistema de gestión de 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.

### **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
	no aplica	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 del presente 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 18.

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 suministren dicho servicio deben 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 18.

### **Refuerzo R1 – Protección de emisiones electromagnéticas**

- [op.pl.5.r1.1] La información deberá ser protegida frente a las amenazas TEMPEST de



acuerdo a la Normativa en vigor.

### 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 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, de 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 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) nº 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE:
- a) 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) nº 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) nº 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) nº 910/2014).

#### Refuerzo R1 – Identificación avanzada

- [op.acc.1.r1.1] El administrador de sistema/seguridad podrá identificar al usuario, así como su puesto y función en el sistema.
- [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 personal de administración de seguridad.

#### 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
	no aplica	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.
- [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]

Los mecanismos de autenticación se adecuarán al nivel de seguridad del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación:

- "algo que se sabe": contraseñas o claves concertadas.
- "algo que se tiene": componentes lógicos (tales como certificados software o aplicaciones móviles) o dispositivos físicos (en expresión inglesa, *tokens*).
- "algo que se es": elementos biométricos, basados en características físicas del usuario (un rasgo o propiedad biométrica como la fisonomía facial, la huella digital, el patrón de iris, etc.).

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

Se podrán definir diferentes mecanismos de autenticación en caso de haber más de un punto de acceso al sistema, en función del nivel de exposición de cada uno. Como puntos de acceso al sistema se entenderán aquellos elementos que solicitan las credenciales para su validación.

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

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

dimensiones	C I T A		
nivel	bajo	medio	alto
	+[R1oR2oR3]	+[R1oR2oR3]	+[R2oR3]+R4

#### 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] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
- [op.acc.5.3] El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida.
- [op.acc.5.4] Las credenciales se cambiarán con una periodicidad marcada por la política de la organización.
- [op.acc.5.5] Las credenciales se retirarán y serán inhabilitadas cuando se detecte su pérdida o falta de control exclusivo por parte del usuario.



- [op.acc.5.6] Las credenciales se retirarán y serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentican termina su relación con el sistema.
- [op.acc.5.7] La información suministrada en los accesos debe ser la mínima imprescindible.
- [op.acc.5.8] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, requiriendo una intervención específica para reactivar la cuenta, que se describirá en la documentación.

#### **Refuerzo R1 – Contraseñas**

- [op.acc.5.r1.1] Se empleará un mecanismo de autenticación de, al menos, un factor.
- [op.acc.5.r1.2] Si se emplean contraseñas o similares, se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación (ver guías CCN-STIC).

#### **Refuerzo R2 – Certificados**

- [op.acc.5.r2.1] Se emplearán certificados como mecanismo de autenticación.
- [op.acc.5.r2.2] Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo: presencial o telemático, usando certificado electrónico.

#### **Refuerzo R3 – Certificados en dispositivo físico**

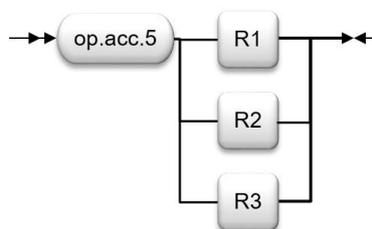
[op.acc.5.r3.1] Se emplearán certificados como mecanismo de autenticación, en soporte físico (tarjeta o similar) usando algoritmos, parámetros y dispositivos autorizados por el CCN.

#### **Refuerzo R4 – Suspensión por no utilización**

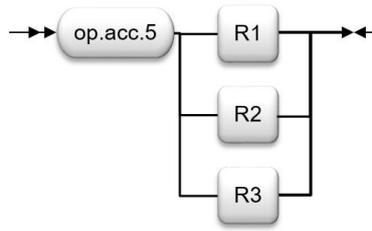
[op.acc.5.r4.1] Las credenciales se suspenderán tras un periodo definido de no utilización.

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

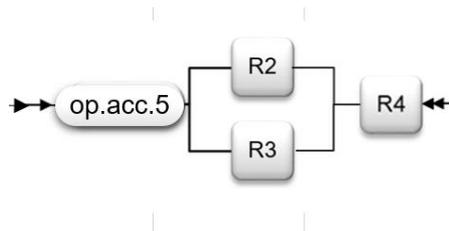
- Nivel BAJO: op.acc.5 + [R1 o R2 o R3]



- Nivel MEDIO: op.acc.5 + [R1 o R2 o R3]



- Nivel ALTO:  $op.acc.5 + [R2 \text{ o } R3] + R4$



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

Referente a personal del organismo, propio o contratado, estable o circunstancial, que se caracteriza por tener acceso a información de los administrados.

dimensiones	C I T A		
nivel	bajo	medio	alto
	+[R1oR2oR3]	+[R2oR3]+R4	+R3+R4+R5

#### Requisitos

- [op.acc.6.1] Las credenciales estarán bajo el control exclusivo del usuario y se activarán una vez estén bajo su control efectivo.
- [op.acc.6.2] El usuario reconocerá que las ha recibido y que conoce y acepta las obligaciones que implica su tenencia, en particular, el deber de custodia diligente, protección de su confidencialidad y notificación inmediata en caso de pérdida.
- [op.acc.6.3] Las credenciales se cambiarán con una periodicidad marcada por la política de la organización.
- [op.acc.6.4] Las credenciales se retirarán y serán inhabilitadas cuando se detecte su pérdida o falta de control exclusivo por parte del usuario.
- [op.acc.6.5] Las credenciales se retirarán y serán inhabilitadas cuando la entidad (persona, equipo o proceso) que autentica termina su relación con el sistema.
- [op.acc.6.6] Se prevendrán ataques que puedan revelar información del sistema sin llegar a acceder al mismo. La información suministrada en los accesos debe ser la imprescindible
- [op.acc.6.7] El número de intentos permitidos será limitado, bloqueando la oportunidad de acceso una vez superado tal número, requiriendo la intervención de los administradores de seguridad para reactivar la cuenta.



- [op.acc.6.8] El sistema informará al usuario de sus obligaciones inmediatamente después de obtener el acceso.

### **Refuerzo R1 – Contraseñas**

- [op.acc.6.r1.1] Se empleará un mecanismo de autenticación de, al menos, un factor.
- [op.acc.6.r1.2] Si se emplean contraseñas o similares, se impondrán normas de complejidad mínima y robustez frente a ataques de adivinación. Estos parámetros de complejidad y robustez se concretarán en las Guías CCN-STIC que sean de aplicación.

### **Refuerzo R2- Doble factor para acceso desde zonas no controladas**

Se denomina zona controlada aquella que no es de acceso público, sino que para llegar al equipo desde el que se accede el usuario se ha autenticado de alguna forma (control de acceso a las instalaciones) diferente al mecanismo de autenticación lógica frente al sistema.

[op.acc.6.r2.1] Para el acceso desde zonas no controladas se requerirá un doble factor de autenticación.

### **Refuerzo R3 – Doble factor para todos los accesos**

[op.acc.6.r3.1] Para el acceso se requerirá un doble factor de autenticación.

### **Refuerzo R4 – Registro**

- [op.acc.6.r4.1] Se registrarán los accesos con éxito y los fallidos.
- [op.acc.6.r4.2] Se informará al usuario del último acceso efectuado con su identidad.

### **Refuerzo R5 – Limitación de la ventana de acceso**

[op.acc.6.r5.1] 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 R6 – Seguridad de las credenciales de autenticación**

[op.acc.6.r6.1] Las credenciales de acceso deberán ser cambiadas cada vez que haya algún indicio de que hayan sido comprometidas o reveladas a personal no autorizado.

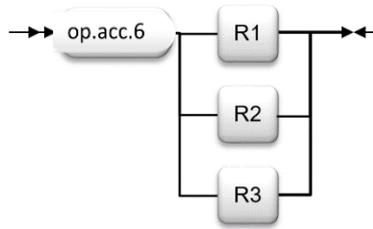
### **Refuerzo R7 – Acceso remoto de administración**

- [op.acc.6.r7.1] Se deberán aplicar los requisitos de seguridad que resulten de aplicación de la ITS de Interconexión de sistemas de información.
- [op.acc.6.r7.2] El acceso remoto para labores de administración deberá considerar los siguientes aspectos:
  - a) Ser autorizado por la autoridad correspondiente.
  - b) El tráfico de administración remoto deberá ser cifrado.
  - c) Si la utilización no se produce de manera constante, la administración remota deberá encontrarse inhabilitada y habilitarse únicamente cuando sea necesario.
  - d) Deberán recogerse registros de auditoría de este tipo de conexiones.

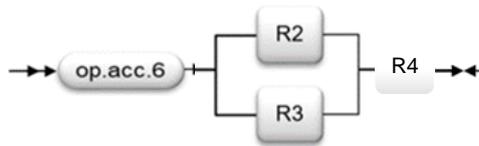
**Aplicación de la medida (por confidencialidad, integridad, trazabilidad y autenticidad)**



- Nivel BAJO: op.acc.6+[R1 o R2 o R3]



- Nivel MEDIO: op.acc.6 + [R2 o R3] + R4



- Nivel ALTO: op.acc.6 + R3+ R4+ R5

### 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 todos los activos en una red teniendo visibilidad completa de los dispositivos de usuario y de red.

#### 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.

#### 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	+ R1	+ R1

##### 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:
  - 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 tiene que realizar acciones conscientes.
  - c) El uso natural, en los casos que el usuario no ha consultado el manual, será un uso seguro.

#### Refuerzo R1- Configuración de seguridad de máquinas virtuales

[op.exp.2.r1.1] Las máquinas virtuales estarán configuradas y gestionadas de un modo seguro. La gestión del parchado, 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 + R1
- Categoría ALTA: op.exp.2 + R1

#### 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 "seguridad por defecto" ([op.exp.2]).
- [op.exp.3.3] El sistema se adapte a las nuevas necesidades, previamente autorizadas ([op.acc.4]).
- [op.exp.3.4] El sistema reaccione a vulnerabilidades notificadas ([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 asegurarse 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.

#### **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 el estado de seguridad de la configuración de los dispositivos de red de forma periódica y, en el caso de que resulte deficiente, poder corregirlo.

#### **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 aplicación o no de la actualización.
- [op.exp.4.3] El mantenimiento solamente 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 equipo que no esté en producción, que la nueva instalación funciona correctamente y no disminuye la eficacia de las funciones necesarias para el trabajo diario.

##### 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 la 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.

##### 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



	no aplica	aplica	+ R1
--	-----------	--------	------

## Requisitos

Se mantendrá un control continuo de 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 asignándoseles un número de referencia que permita su seguimiento, de forma equivalente a como se registran 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 gestionarlos 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 análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen una situación de riesgo de nivel ALTO serán aprobados explícitamente, de forma previa a su implantación, por el Responsable de 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 estructura de 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	+R1+R2+R3

## Requisitos



- [op.exp.6.1] Se dispondrá de mecanismos de prevención y reacción frente a código dañino, incluyendo el correspondiente mantenimiento de acuerdo a las recomendaciones del fabricante.
- [op.exp.6.2] Se instalará software de protección frente a código dañino en todos los equipos: puestos usuario, servidores y elementos perimetrales.
- [op.exp.6.3] Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.
- [op.exp.6.4] Las bases de datos de detección de código dañino se actualizarán permanentemente.
- [op.exp.6.5] El software de detección de código dañino instalado en los puestos de usuario deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

### **Refuerzo R1 – Escaneo periódico**

[op.exp.6.r1.1] Todo el sistema se escaneará regularmente para detectar código dañino.

### **Refuerzo R2 – Revisión preventiva del sistema**

[op.exp.6.r2.1] Las funciones críticas se analizarán al arrancar el sistema en prevención de modificaciones no autorizadas.

### **Refuerzo R3 - Lista blanca**

[op.exp.6.r3.1] Solamente se podrán ejecutar aplicaciones previamente autorizadas. Se implementará una lista blanca para impedir la ejecución de aplicaciones no autorizadas.

### **Refuerzo R4 – Capacidad de respuesta en caso de incidente**

[op.exp.6.r4.1] Se emplearán herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR – Endpoint Defense and Response).

### **Refuerzo R5 – Configuración de la herramienta de detección de código dañino**

[op.exp.6.r5.1] El software de detección de código dañino permitirá realizar configuraciones avanzadas y revisar el sistema al arrancar y cada vez que se conecte un dispositivo extraíble.

[op.exp.6.r1.2] El software de detección de código dañino instalado en servidores y elementos perimetrales deberá estar configurado de forma adecuada e implementará protección en tiempo real de acuerdo a las recomendaciones del fabricante.

### **Aplicación de la medida**

- Categoría BÁSICA: op.exp.6
- Categoría MEDIA: op.exp.6+ R1
- Categoría ALTA: op.exp.6+ R1 + R2 + R3



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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1+R2	+ R1+R2

##### Requisitos

- [op.exp.7.1] Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema que incluya el informe de eventos de seguridad y debilidades, detallando los criterios de clasificación y el escalado de la notificación.
- [op.exp.7.2] La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el presente real decreto.

##### Refuerzo R1 – Notificación

[op.exp.7.r1.1] Se dispondrá de soluciones de ventanilla única para la notificación de incidentes al CCN-CERT, que permita la distribución de notificaciones a las diferentes entidades de manera federada, utilizando para ello dependencias administrativas jerárquicas.

##### Refuerzo R2 –Detección y Respuesta

El proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema ([op.exp.7.1]) deberá incluir:

- [op.exp.7.r2.1] Implantación de medidas urgentes, incluyendo la detención de servicios, el aislamiento del sistema afectado, la recogida de evidencias y protección de los registros, según convenga al caso.
- [op.exp.7.r2.2] Asignación de recursos para investigar las causas, analizar las consecuencias y resolver el incidente.
- [op.exp.7.r2.3] Informar a los responsables de la información y servicios afectados del incidente y de las actuaciones llevadas a cabo para su resolución.
- [op.exp.7.r2.4] Medidas para:
  - a) Prevenir que se repita el incidente.
  - b) Incluir en los procedimientos de usuario la identificación y forma de tratar el incidente.
  - c) Actualizar, extender, mejorar u optimizar los procedimientos de resolución de incidentes.

##### Refuerzo R3 – Reconfiguración dinámica

La reconfiguración dinámica del sistema busca detener, desviar o limitar ataques, acotando los daños.



- [op.exp.7.r3.1] La reconfiguración dinámica incluye, por ejemplo, cambios en las reglas de los enrutadores (*routers*), listas de control de acceso, parámetros del sistema de detección / prevención de intrusiones y reglas en los cortafuegos y puertas de enlace, aislamiento de elementos críticos y aislamiento de las copias de seguridad.
- [op.exp.7.r3.2] El organismo adaptará los procedimientos de reconfiguración dinámica reaccionando a los anuncios recibidos del CCN-CERT relativos a ciberamenazas sofisticadas y campañas de ataques.

#### Refuerzo R4 – Prevención y Respuesta Automática

[op.exp.7.r4.1] Se dispondrá de herramientas que automaticen el proceso de prevención y respuesta mediante la detección e identificación de anomalías, segmentación dinámica de la red para reducir la superficie de ataque, el aislamiento de dispositivos críticos, etc.

#### Aplicación de la medida

- Categoría BÁSICA: op.exp.7
- Categoría MEDIA: op.exp.7+ R1 + R2
- Categoría ALTA: op.exp.7+ R1 + R2 + R3

#### 4.3.8. Registro de la actividad [op.exp.8]

dimensiones	T		
nivel	bajo	medio	alto
	aplica	+R1+R2+R3+R4	+R1+R2+R3+R4+R5

#### Requisitos

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

- [op.exp.8.1] Se generará un registro de auditoría, que incluirá al menos el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito) según la política de seguridad y los procedimientos asociados a la misma.
- [op.exp.8.2] Se activarán los registros de actividad en los servidores.

#### Refuerzo R1 – Revisión de los registros

[op.exp.8.r1.1] Se revisarán informalmente, de forma periódica, los registros de actividad buscando patrones anormales.

#### Refuerzo R2 – Sincronización del reloj del sistema

[op.exp.8.r2.1] El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

#### Refuerzo R3 – Retención de registros



[op.exp.8.r3.1] En la documentación de seguridad del sistema se deberán indicar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de ser eliminados.

#### **Refuerzo R4 – Control de acceso**

[op.exp.8.r4.1] Los registros de actividad y, en su caso, las copias de seguridad solamente podrán alterarse o eliminarse por personal debidamente autorizado.

#### **Refuerzo R5 – Revisión automática y correlación de eventos**

- [op.exp.8.r5.1] El sistema deberá implementar herramientas para analizar y revisar la actividad del sistema y la información de auditoría en búsqueda de comprometimientos de la seguridad posibles o reales.
- [op.exp.8.r5.2] Se dispondrá de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

#### **Aplicación de la medida (por trazabilidad)**

- Nivel BAJO: op.exp.8
- Nivel MEDIO: op.exp.8 + R1 + R2 + R3 + R4
- Nivel ALTO: op.exp.8 + R1 + R2 + R3 + R4 + R5

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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

#### **Requisitos**

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

- [op.exp.9.1] Se registrarán los reportes iniciales, intermedios y finales, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.
- [op.exp.9.2] Se registrará aquella evidencia que pueda dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones disciplinarias sobre el personal interno, sobre proveedores externos o en la persecución de delitos. En la determinación de la composición y detalle de estas evidencias, se recurrirá a asesoramiento legal especializado.
- [op.exp.9.3] Como consecuencia del análisis de los incidentes, se revisará la determinación de los eventos auditables.

#### **Aplicación de la medida**

- Categoría BÁSICA: op.exp.9
- Categoría MEDIA: op.exp.9
- Categoría ALTA: op.exp.9



#### 4.3.10. Protección de claves criptográficas [op.exp.11].

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	+ R1

##### Requisitos

- [op.exp.11.1] Las claves criptográficas se protegerán durante todo su ciclo de vida: (1) generación, (2) transporte al punto de explotación, (3) custodia durante la explotación, (4) archivo posterior a su retirada de explotación activa y (5) destrucción final.
- [op.exp.11.2] Los medios de generación estarán aislados de los medios de explotación.
- [op.exp.11.3] Las claves retiradas de operación que deban ser archivadas, lo serán en medios aislados de los de explotación.

##### Refuerzo R1 – Algoritmos autorizados

[op.exp.11.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

##### Refuerzo R2 – Protección avanzada de claves criptográficas

[op.exp.11.r2.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

##### Aplicación de la medida

- Categoría BÁSICA: op.exp.11
- Categoría MEDIA: op.exp.11 + R1
- Categoría ALTA: op.exp.11 + R1

#### 4.4. Recursos externos [op.ext]

Cuando la organización utilice recursos externos (servicios, productos, instalaciones o personal), mantendrá la plena responsabilidad de los riesgos para la información tratada o los servicios prestados, debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

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

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	aplica

##### Requisitos

[op.ext.1.1] Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio que incluirá las características del servicio prestado, lo que debe entenderse como “servicio mínimo admisible”, así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

##### Aplicación de la medida

- Categoría BÁSICA: no aplica



- Categoría MEDIA: op.ext.1
- Categoría ALTA: op.ext.1

#### 4.4.2. Gestión diaria [op.ext.2]

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	aplica

#### Requisitos

Se establecerá lo siguiente:

- [op.ext.2.1] Un sistema rutinario para medir el cumplimiento de las obligaciones de servicio, incluyendo el procedimiento para neutralizar cualquier desviación fuera del margen de tolerancia acordado ([op.ext.1]).
- [op.ext.2.2] El mecanismo y los procedimientos de coordinación para llevar a cabo las tareas de mantenimiento de los sistemas comprendidos en el acuerdo, que contemplarán los supuestos de incidentes y desastres (ver [op.exp.7]).

#### Aplicación de la medida

- Categoría BÁSICA: no aplica
- Categoría MEDIA: op.ext.2
- Categoría ALTA: op.ext.2

#### 4.4.3. Protección de la cadena de suministro [op.ext.3]

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	no aplica	aplica

#### Requisitos

- [op.ext.3.1] Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro.
- [op.ext.3.2] Se estimará el riesgo sobre el sistema por causa del impacto estimado en el punto anterior.
- [op.ext.3.3] Se tomarán medidas de contención de los impactos estimados en los puntos anteriores.

#### Refuerzo R1 – Plan de contingencia

- [op.ext.3.r1.1] El plan de continuidad de la organización tiene en cuenta la dependencia de proveedores externos críticos.
- [op.ext.3.r1.2] Se realizan pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

#### Refuerzo R2 – Sistema de gestión de la seguridad.

[op.ext.3.r2.1] Se implementará un sistema de protección de los procesos y flujos de



información en las relaciones en línea (*online*) entre los distintos integrantes de la cadena de suministro.

#### Aplicación de la medida

- Categoría BÁSICA: no aplica
- Categoría MEDIA: no aplica
- Categoría ALTA: op.ext.3

#### 4.4.4. Interconexión de sistemas [op.ext.4]

Se denomina interconexión al establecimiento de enlaces con otros sistemas de información para el intercambio de información y servicios.

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	+ R1

#### Requisitos

- [op.ext.4.1] Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.
- [op.ext.4.2] Para cada interconexión se documentará explícitamente: las características de la interfaz, los requisitos de seguridad y protección de datos y la naturaleza de la información intercambiada.

#### Refuerzo R1 – Coordinación de actividades

[op.ext.4.r1.1] Cuando se interconecten sistemas en los que la identificación, autenticación y autorización tengan lugar en diferentes dominios de seguridad, bajo distintas responsabilidades, las medidas de seguridad locales se acompañarán de los correspondientes mecanismos y procedimientos de coordinación para la atribución y ejercicio efectivos de las responsabilidades de cada sistema.

#### Aplicación de la medida

- Categoría BÁSICA: no aplica
- Categoría MEDIA: op.ext.4
- Categoría ALTA: op.ext.4 + R1

#### 4.5. Servicios en la nube [op.nub]

##### 4.5.1. Protección de servicios en la nube [op.nub.1]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	+R1+R2

#### Requisitos

- [op.nub.1.1] Los sistemas que suministran un servicio en la nube a organismos del sector público deberán cumplir con el conjunto de medidas de seguridad en función del modelo de servicio en la nube que presten: Software como Servicio (*Software as a*



Service SaaS), Plataforma como Servicio (*Platform as a Service* PaaS) e Infraestructura como Servicio (*Infrastructure as a Service* IaaS) definidas en las guías CCN-STIC que sean de aplicación.

- [op.nub.1.2] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán cumplir con las medidas desarrolladas en una guía CCN-STIC que incluirá, entre otros, requisitos relativos a:
  - a) Auditoría de pruebas de penetración (*pentesting*).
  - b) Transparencia.
  - c) Cifrado y gestión de claves.
  - d) Jurisdicción de los datos.

#### Refuerzo R1- Servicios certificados

- [op.nub.1.r1.1] Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.
- [op.nub.1.r1.2] Si el servicio en la nube es un servicio de seguridad deberá cumplir con los requisitos establecidos en [op.pl.5].

#### Refuerzo R2 – Guías de Configuración de Seguridad Específicas

[op.nub.1.r2.1] La configuración de seguridad de los sistemas que proporcionan estos servicios deberá realizarse según la correspondiente Guía CCN-STIC de Configuración de Seguridad Específica.

#### Aplicación de la medida

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

### 4.6. Continuidad del servicio [op.cont]

#### 4.6.1. Análisis de impacto [op.cont.1]

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	aplica

#### Requisitos

[op.cont.1.1] Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

#### Aplicación de la medida (por disponibilidad)

- Nivel BAJO: no aplica



- Nivel MEDIO: op.cont.1
- Nivel ALTO: op.cont.1

#### 4.6.2. Plan de continuidad [op.cont.2]

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

#### Requisitos

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

- [op.cont.2.1] Se identificarán funciones, responsabilidades y actividades a realizar.
- [op.cont.2.2] Existirá una previsión para coordinar la entrada en servicio de los medios alternativos de forma que se garantice poder seguir prestando los servicios esenciales de la organización.
- [op.cont.2.3] Todos los medios alternativos estarán planificados y materializados en acuerdos o contratos con los proveedores correspondientes.
- [op.cont.2.4] Las personas afectadas por el plan recibirán formación específica relativa a su papel en dicho plan.
- [op.cont.2.5] El plan de continuidad será parte integral y armónica de los planes de continuidad de la organización en otras materias ajenas a la seguridad.

#### Refuerzo R1 – Plan de emergencia y contingencia

[op.cont.2.r1.1] Cuando se determine la necesidad de continuidad de los sistemas, deberá existir un plan de emergencia y contingencia en consonancia. En función del Análisis de Impacto, se determinarán los aspectos a cubrir.

#### Refuerzo R2 – Comprobación de integridad

[op.cont.2.r2.1] Ante una caída o discontinuidad del sistema, se deberá comprobar la integridad del Sistema operativo, firmware y ficheros de configuración.

#### Aplicación de la medida (por disponibilidad)

- Nivel BAJO: no aplica
- Nivel MEDIO: no aplica
- Nivel ALTO: op.cont.2

#### 4.6.3. Pruebas periódicas [op.cont.3]

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

#### Requisitos



[op.cont.3.1] Se realizarán pruebas periódicas para localizar y, en su caso, corregir los errores o deficiencias que puedan existir en el plan de continuidad.

#### **Aplicación de la medida (por disponibilidad)**

- Nivel BAJO: no aplica
- Nivel MEDIO: no aplica
- Nivel ALTO: op.cont.3

#### **4.6.4. Medios alternativos [op.cont.4]**

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

#### **Requisitos**

- [op.cont.4.1] Estará prevista la disponibilidad de medios alternativos para poder seguir prestando servicio cuando los medios habituales no estén disponibles. En concreto se cubrirán los siguientes elementos del sistema:
  - a) Servicios contratados a terceros
  - b) Instalaciones alternativas
  - c) Personal alternativo
  - d) Equipamiento informático alternativo
  - e) Medios de comunicación alternativos
- [op.cont.4.2] Se establecerá un tiempo máximo para que los medios alternativos entren en funcionamiento.
- [op.cont.4.3] Los medios alternativos estarán sometidos a las mismas garantías de seguridad que los originales.

#### **Refuerzo R1 – Automatización de la transición a medios alternativos**

[op.cont.4.r1.1] El sistema dispondrá de elementos hardware o software que permitan la transferencia de los servicios automáticamente a los medios alternativos.

#### **Aplicación de la medida (por disponibilidad)**

- Nivel BAJO: no aplica
- Nivel MEDIO: no aplica
- Nivel ALTO: op.cont.4

#### **4.7. Monitorización del sistema [op.mon]**

El sistema estará sujeto a medidas de monitorización de su actividad y ejecutará acciones predeterminadas en función de las situaciones de compromiso de seguridad que figuren en el análisis de riesgos. Esto puede incluir la generación de alarmas en tiempo real, la finalización del proceso que está ocasionando la alarma, la inhabilitación de



determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

#### 4.7.1. Detección de intrusión [op.mon.1]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	+R1+R2

##### Requisitos

[op.mon.1.1] Se dispondrá de herramientas de detección o prevención de intrusiones.

##### Refuerzo R1 – Detección basada en reglas

[op.mon.1.r1.1] El sistema dispondrá de herramientas de detección o prevención de intrusiones basadas en reglas.

##### Refuerzo R2 – Procedimientos de respuesta

[op.mon.1.r2.1] Existirán procedimientos de respuesta a las alertas generadas por el sistema de detección o prevención de intrusiones.

##### Refuerzo R3 – Acciones predeterminadas

[op.mon.1.r3.1] El sistema ejecutará automáticamente acciones predeterminadas de respuesta a las alertas generadas. Esto puede incluir la finalización del proceso que está ocasionando la alerta, la inhabilitación de determinados servicios, la desconexión de usuarios y el bloqueo de cuentas.

##### Aplicación de la medida

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

#### 4.7.2. Sistema de métricas [op.mon.2]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1+R2	+ R1+R2

##### Requisitos

[op.mon.2.1] Atendiendo a la categoría de seguridad del sistema, se recopilarán los datos necesarios para conocer el grado de implantación de las medidas de seguridad que resulten aplicables y, en su caso, para proveer el informe anual requerido por el artículo 32.

##### Refuerzo R1 – Efectividad del sistema de gestión de incidentes

[op.mon.2.r1.1] Se recopilarán los datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes, de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC.



## Refuerzo R2 – Eficiencia del sistema de gestión de la seguridad

[op.mon.2.r2.1] Se recopilarán los datos precisos para conocer la eficiencia del sistema de seguridad, en relación con los recursos consumidos, en términos de horas y presupuesto.

### Aplicación de la medida

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

### 4.7.3. Vigilancia [op.mon.3]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1+R2	+ R1+R2+R3+R4+R5+R6

### Requisitos

[op.mon.3.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad.

### Refuerzo R1 – Correlación de eventos

[op.mon.3.r1.1] Se dispondrá de un sistema automático de recolección de eventos de seguridad que permita la correlación de los mismos.

### Refuerzo R2 – Análisis dinámico

[op.mon.3.r2.1] Se dispondrá de soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración.

### Refuerzo R3 – Ciberamenazas avanzadas

- [op.mon.3.r3.1] Se dispondrá de sistemas para detección de amenazas avanzadas y comportamiento anómalos.
- [op.mon.3.r3.2] Se dispondrá de sistemas para la detección de amenazas persistentes avanzadas (*Advanced Persistent Threat* APT) mediante la detección de anomalías significativas en el tráfico de la red.

### Refuerzo R4 – Observatorios digitales

[op.mon.3.r4.1] Se dispondrá de observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías, que pudieran representar indicadores de amenaza, en contenidos digitales.

### Refuerzo R5– Minería de datos

Se aplicarán medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos:

- [op.mon.3.r5.1] Limitación de las consultas, monitorizando volumen y frecuencia.



- [op.mon.3.r5.2] Alerta a los administradores de seguridad de comportamientos sospechosos en tiempo real.

### Refuerzo R6 – Inspecciones de seguridad

Se realizarán las siguientes inspecciones periódicamente y tras incidentes que hayan desvelado vulnerabilidades del sistema nuevas o subestimadas:

- [op.mon.3.r6.1] Verificación de configuración.
- [op.mon.3.r6.2] Análisis de vulnerabilidades.
- [op.mon.6.r6.3] Pruebas de penetración.

### Refuerzo R7 – Interconexiones

[op.mon.3.r7.1] En las interconexiones que lo requieran, se aplicarán controles en los flujos de intercambio de información a través del uso de metadatos.

### Aplicación de la medida

- Categoría BÁSICA: op.mon.3
- Categoría MEDIA: op.mon.3 + R1 + R2
- Categoría ALTA: op.mon.3 + R1 + R2 + R3 + R4 + R5 + R6

## 5. Medidas de protección [mp]

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

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

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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

### Requisitos

- [mp.if.1.1] El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas específicas para su función.
- [mp.if.1.2] Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

### Aplicación de la medida

- Categoría BÁSICA: mp.if.1
- Categoría MEDIA: mp.if.1
- Categoría ALTA: mp.if.1

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

dimensiones	Todas
-------------	-------



categoria	básica	media	alta
	aplica	aplica	aplica

## Requisitos

[mp.if.2.1] El procedimiento de control de acceso identificará a las personas que accedan a los locales donde hay equipamiento esencial que forme parte del sistema de información del CPD, registrando las correspondientes entradas y salidas.

### Aplicación de la medida

- Categoría BÁSICA: mp.if.2
- Categoría MEDIA: mp.if.2
- Categoría ALTA: mp.if.2

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

dimensiones	Todas		
categoria	básica	media	alta
	aplica	aplica	aplica

## Requisitos

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

- [mp.if.3.1] Las condiciones de temperatura y humedad.
- [mp.if.3.2] La protección frente a las amenazas identificadas en el análisis de riesgos.
- [mp.if.3.3] La protección del cableado frente a incidentes fortuitos o deliberados.

### Aplicación de la medida

- Categoría BÁSICA: mp.if.3
- Categoría MEDIA: mp.if.3
- Categoría ALTA: mp.if.3

### 5.1.4. Energía eléctrica [mp.if.4]

dimensiones	D		
nivel	bajo	medio	alto
	aplica	+ R1	+ R1

## Requisitos

[mp.if.4.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de tomas de energía eléctrica, de modo que se garantice el suministro y el correcto funcionamiento de las luces de emergencia.

### Refuerzo R1 – Suministro eléctrico de emergencia

[mp.if.4.r1.1] En caso de fallo del suministro principal, el abastecimiento eléctrico deberá



estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información.

#### Aplicación de la medida (por disponibilidad)

- Nivel BÁSICO: mp.if.4
- Nivel MEDIO: mp.if.4 + R1
- Nivel ALTO: mp.if.4 + R1

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

dimensiones	D		
nivel	bajo	medio	alto
	aplica	aplica	aplica

#### Requisitos

[mp.if.5.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incendios atendiendo, al menos, a la normativa industrial de aplicación.

#### Aplicación de la medida (por disponibilidad)

- Nivel BÁSICO: mp.if.5
- Nivel MEDIO: mp.if.5
- Nivel ALTO: mp.if.5

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

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	aplica

#### Requisitos

[mp.if.6.1] Los locales donde se ubiquen los sistemas de información y sus componentes esenciales se protegerán frente a incidentes causados por el agua.

#### Aplicación de la medida (por disponibilidad)

- Categoría BÁSICA: no aplica
- Categoría MEDIA: mp.if.6
- Categoría ALTA: mp.if.6

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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

#### Requisitos

[mp.if.7.1] Se llevará un registro pormenorizado de cualquier entrada y salida de



equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

### Aplicación de la medida

- Categoría BÁSICA: mp.if.7
- Categoría MEDIA: mp.if.7
- Categoría ALTA: mp.if.7

## 5.2. Gestión del personal [mp.per]

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

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	aplica	aplica

### Requisitos

- [mp.per.1.1] Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos.
- [mp.per.1.2] Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo, en particular, en términos de confidencialidad. Dichos requisitos se tendrán en cuenta en la selección de la persona que vaya a ocupar el puesto, incluyendo la verificación de sus antecedentes laborales, formación y otras referencias, de conformidad con el ordenamiento jurídico y el respeto a los derechos fundamentales.

### Refuerzo R1 – Habilitación Personal de Seguridad

[mp.per.1.r1.1] Los administradores de seguridad/sistema tendrán una Habilitación Personal de Seguridad (HPS) otorgada por la autoridad competente, como consecuencia de los resultados del análisis de riesgos previo o como requisito de seguridad de un sistema específico.

### Aplicación de la medida

- Categoría BÁSICA: no aplica
- Categoría MEDIA: mp.per.1
- Categoría ALTA: mp.per.1

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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	+ R1

### Requisitos



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

- [mp.per.2.1] Las medidas disciplinarias a que haya lugar.
- [mp.per.2.2] Tanto el periodo durante el cual se desempeña el puesto, como las obligaciones en caso de término de la asignación, o traslado a otro puesto de trabajo.
- [mp.per.2.3] El deber de confidencialidad respecto de los datos a los que tenga acceso, tanto durante el periodo que esté adscrito al puesto de trabajo, como posteriormente a su terminación.
- [mp.per.2.4] En caso de personal contratado a través de un tercero:
  - [mp.per.2.4.1] Se establecerán los deberes y obligaciones de cada parte y del personal contratado.
  - [mp.per.2.4.2] Se establecerá el procedimiento de resolución de incidentes relacionados con el incumplimiento de las obligaciones.

### Refuerzo R1 – Confirmación expresa

[mp.per.2.r1.1] Se ha de obtener la confirmación expresa por parte de los usuarios de conocer las instrucciones de seguridad necesarias y obligatorias, así como los procedimientos necesarios para llevarlas a cabo de manera adecuada.

### Aplicación de la medida

- Categoría BÁSICA: mp.per.2
- Categoría MEDIA: mp.per.2 + R1
- Categoría ALTA: mp.per.2 + R1

### 5.2.3. Concienciación [mp.per.3]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

### Requisitos

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:

- [mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
- [mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- [mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

### Aplicación de la medida



- Categoría BÁSICA: mp.per.3
- Categoría MEDIA: mp.per.3
- Categoría ALTA: mp.per.3

#### 5.2.4. Formación [mp.per.4]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

#### Requisitos

[mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:

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

Además, se evaluará la eficacia de las acciones formativas llevadas a cabo.

#### Aplicación de la medida

- Categoría BÁSICA: mp.per.4
- Categoría MEDIA: mp.per.4
- Categoría ALTA: mp.per.4

#### 5.3. Protección de los equipos [mp.eq]

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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	+ R1

#### Requisitos

[mp.eq.1.1] Los puestos de trabajo permanecerán despejados, sin que exista material distinto del necesario en cada momento.

#### Refuerzo R1 – Almacenamiento del material

[mp.eq.1.r1.1] Una vez usado, y siempre que sea factible, el material se almacenará en lugar cerrado.

#### Aplicación de la medida

- Categoría BÁSICA: mp.eq.1



- Categoría MEDIA: mp.eq.1 + R1
- Categoría ALTA: mp.eq.1 + R1

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

dimensiones	A		
nivel	bajo	medio	alto
	no aplica	aplica	+ R1

#### Requisitos

[mp.eq.2.1] El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso.

#### Refuerzo R1 – Cierre de sesiones

[mp.eq.2.r1.1] Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

Una Guía CCN-STIC concretará la implementación de la configuración de seguridad adaptada a la categorización del sistema o perfil de cumplimiento asociado.

#### Aplicación de la medida (por autenticidad)

- Nivel BÁSICO: no aplica
- Nivel MEDIO: mp.eq.2
- Nivel ALTO: mp.eq.2 + R1

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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	+R1+R2

#### Requisitos

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

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

- [mp.eq.3.1] Se llevará un inventario de equipos portátiles junto con una identificación de la persona responsable del mismo y un control regular de que está positivamente bajo su control.
- [mp.eq.3.2] Se establecerá un procedimiento operativo de seguridad para informar al servicio de gestión de incidentes de pérdidas o sustracciones.
- [mp.eq.3.3] Cuando un equipo portátil se conecte remotamente a través de redes que



no están bajo el estricto control de la organización, el ámbito de operación del servidor limitará la información y los servicios accesibles a los mínimos imprescindibles, requiriendo autorización previa de los responsables de la información y los servicios afectados. Este punto es de aplicación a conexiones a través de internet y otras redes que no sean de confianza.

- [mp.eq.3.4] Se evitará, en la medida de lo posible, que el equipo contenga claves de acceso remoto a la organización, que no sean imprescindibles. Se considerarán claves de acceso remoto aquellas que sean capaces de habilitar un acceso a otros equipos de la organización, u otras de naturaleza análoga.

### Refuerzo R1 – Entornos protegidos

[mp.eq.3.r1.1] El uso de equipos portátiles fuera de las instalaciones de la organización se restringirá a entornos protegidos, donde el acceso sea controlado, a salvo de hurtos y miradas indiscretas.

### Refuerzo R2 – Cifrado del disco

[mp.eq.3.r2.1] Se protegerá el portátil mediante cifrado del disco duro cuando el nivel de confidencialidad de la información almacenada en el mismo sea de nivel ALTO.

### Aplicación de la medida

- Categoría BÁSICA: mp.eq.3
- Categoría MEDIA: mp.eq.3
- Categoría ALTA: mp.eq.3 + R1 + R2

### 5.3.4. Otros dispositivos conectados a la red [mp.eq.4]

dimensiones	C		
nivel	bajo	medio	alto
	aplica	+ R1	+ R1

Esta medida afecta a todo tipo de dispositivos conectados a la red y que puedan tener el algún momento acceso a la información. Equipos tales como:

- a) dispositivos multifunción: impresoras, escáneres, etc.
- b) dispositivos multimedia: proyectores, altavoces inteligentes,...
- c) dispositivos internet de las cosas, en inglés *Internet of Things* (IoT).
- d) dispositivos de invitados y los personales de los propios empleados, en inglés *Bring Your Own Device* (BYOD).
- e) otros

### Requisitos

- [mp.eq.4.1] Los dispositivos presentes en el sistema deberán contar con una configuración de seguridad adecuada de manera que se garantice el control del flujo definido de entrada y salida de la información.



- [mp.eq.4.2] Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad necesaria para eliminar información de soportes de información (ver [mp.si.5]).

#### Refuerzo R1 – Productos certificados

[mp.eq.4.r1.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

#### Refuerzo R2 – Control de dispositivos conectados a la red

[mp.eq.4.r2.1] Se dispondrá de soluciones que permitan visualizar los dispositivos presentes en la red, controlar su conexión/desconexión a la misma y verificar su configuración de seguridad.

#### Aplicación de la medida (por confidencialidad)

- Nivel BAJO: mp.eq.4
- Nivel MEDIO: mp.eq.4 + R1
- Nivel ALTO: mp.eq.4+ R1

### 5.4. Protección de las comunicaciones [mp.com]

#### 5.4.1. Perímetro seguro [mp.com.1]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

#### Requisitos

- [mp.com.1.1] Se dispondrá un sistema de protección perimetral que separe la red interna del exterior. Todo el tráfico deberá atravesar dicho sistema.
- [mp.com.1.2] Todos los flujos de información a través del perímetro deben estar autorizados previamente.

La Instrucción Técnica de Seguridad de Interconexión de Sistemas de Información determinará los requisitos establecidos en el perímetro que han de cumplir todos los componentes del sistema en función de la categoría.

#### Aplicación de la medida

- Categoría BÁSICA: mp.com.1
- Categoría MEDIA: mp.com.1
- Categoría ALTA: mp.com.1

#### 5.4.2. Protección de la confidencialidad [mp.com.2]

dimensiones	C		
nivel	bajo	medio	alto
	aplica	+ R1	+R1+R2+R3



## Requisitos

[mp.com.2.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discorra por redes fuera del propio dominio de seguridad.

### Refuerzo R1 – Algoritmos y parámetros autorizados

[mp.com.2.r1.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

### Refuerzo R2 – Dispositivos hardware

[mp.com.2.r2.1] Se emplearán, dispositivos hardware en el establecimiento y utilización de la red privada virtual.

### Refuerzo R3 – Productos certificados

[mp.com.2.r3.1] Se usarán productos o servicios que cumplan lo establecido en [op.pl.5].

### Refuerzo R4 – Cifradores

[mp.com.2.r4.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

### Aplicación de la medida (por confidencialidad)

- Nivel BAJO: mp.com.2
- Nivel MEDIO: mp.com.2 + R1
- Nivel ALTO: mp.com.2 + R1 + R2+ R3

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

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+ R1 + R2	+ R1 + R2 + R3 + R4

## Requisitos

- [mp.com.3.1] En comunicaciones con puntos exteriores al dominio propio de seguridad, se asegurará la autenticidad del otro extremo del canal de comunicación antes de intercambiar información (ver [op.acc.5]).
- [mp.com.3.2] Se prevendrán ataques activos garantizando que al ser detectados se activarán los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:
  - a) La alteración de la información en tránsito.
  - b) La inyección de información espuria.
  - c) El secuestro de la sesión por una tercera parte.
- [mp.com.3.3] Se aceptará cualquier mecanismo de identificación y autenticación de los previstos en el ordenamiento jurídico en normativa de aplicación.

### Refuerzo R1 – Redes privadas virtuales



[mp.com.3.r1.1] Se emplearán redes privadas virtuales cifradas cuando la comunicación discorra por redes fuera del propio dominio de seguridad.

### Refuerzo R2 – Algoritmos y parámetros autorizados

[mp.com.2.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN.

### Refuerzo R3 – Dispositivos hardware

[mp.com.3.r3.1] Se recomienda emplear dispositivos hardware en el establecimiento y utilización de la red privada virtual.

### Refuerzo R4 – Productos certificados

[mp.com.3.r4.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

### Refuerzo R5 – Cifradores

[mp.com.3.r5.1] Se emplearán cifradores que cumplan con los requisitos establecidos en la guía CCN-STIC que sea de aplicación.

### Aplicación de la medida (por integridad y autenticidad)

- Nivel BAJO: mp.com.3
- Nivel MEDIO: mp.com.3 + R1 + R2
- Nivel ALTO: mp.com.3 + R1 + R2 + R3 + R4

### 5.4.4. Separación de flujos de información en la red [mp.com.4]

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	+[R1oR2oR3]	+[R2oR3]+R4

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

Cuando la transmisión de información por la red se restringe a ciertos segmentos, se acota el acceso a la información y los incidentes de seguridad quedan encapsulados en su segmento.

### Requisitos

Los flujos de información se separarán en segmentos de forma que:

- [mp.com.4.1] El tráfico por la red se segregará para que cada equipo solamente tenga acceso a la información que necesita.
- [mp.com.4.2] Si se emplean comunicaciones inalámbricas, será en un segmento separado.

### Refuerzo R1 – Segmentación lógica básica

- [mp.com.4.r1.1] Los segmentos de red se implementarán por medio de redes de área local virtuales (Virtual Local Area Network VLAN).



- [mp.com.4.r1.2] La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:
  - Usuarios
  - Servicios
  - Administración

### Refuerzo R2 – Segmentación lógica avanzada

[mp.com.4.r2.1] Los segmentos de red se implementarán por medio de redes privadas virtuales (*Virtual Private Network VPN*).

### Refuerzo R3 – Segmentación física

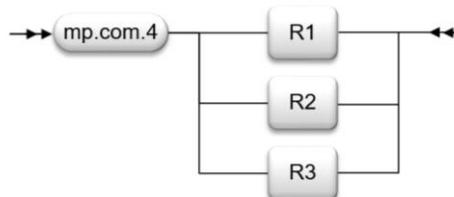
[mp.com.4.r3.1] Los segmentos de red se implementarán con medios físicos separados.

### Refuerzo R4 – Puntos de interconexión

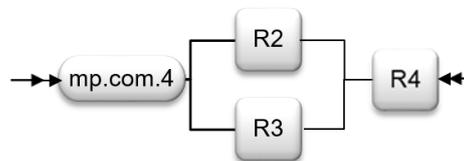
- [mp.com.4.r4.1] Control de entrada de los usuarios que llegan a cada segmento y control de entrada y salida de la información disponible en cada segmento.
- [mp.com.4.r4.2] El punto de interconexión estará particularmente asegurado, mantenido y monitorizado (como en [mp.com.1]).

### Aplicación de la medida

- Categoría BÁSICA: no aplica
- Categoría MEDIA: mp.com.4+ [R1o R2 o R3]



- Categoría ALTA: mp.com.4+[R2 o R3] + R4



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

### 5.5.1. Marcado de soportes [mp.si.1]

dimensiones	C		
nivel	bajo	medio	alto
	aplica	aplica	aplica

### Requisitos

[mp.si.1.1] Los soportes de información (papel impreso, documentos electrónicos,



contenidos multimedia - vídeos, cursos, presentaciones - etc.) que contengan información que según [mp.info.2] deba protegerse con medidas de seguridad específicas, llevarán las marcas o metadatos correspondientes que indiquen el nivel de seguridad de la información contenida de mayor calificación.

#### **Refuerzo R1– Marca de agua digital (por trazabilidad)**

- [mp.si.1.r1.1] La política de seguridad de la organización definirá marcas de agua para asegurar el uso adecuado de la información que se maneja.
- [mp.si.1.r1.2] Los soportes de información digital (documentos electrónicos, material multimedia...) podrán incluir una marca de agua según la política de seguridad.
- [mp.si.1.r1.3] Los equipos o dispositivos a través de los que se accede a aplicaciones, escritorios remotos o virtuales, datos... presentarán una marca de agua en pantalla según la política de seguridad.

#### **Aplicación de la medida (por confidencialidad)**

- Nivel BAJO: mp.si.1
- Nivel MEDIO: mp.si.1
- Nivel ALTO: mp.si.1

#### **5.5.2. Criptografía [mp.si.2]**

dimensiones	C I		
nivel	bajo	medio	alto
	no aplica	aplica	+ R1

Esta medida se aplica, en particular, a todos los dispositivos removibles cuando salen de un área controlada. Se entenderán por dispositivos removibles, los CD, DVD, discos extraíbles, *pendrives*, memorias USB, u otros de naturaleza análoga.

#### **Requisitos**

- [mp.si.2.1] Se usarán mecanismos criptográficos que garanticen la confidencialidad y la integridad de la información contenida.
- [mp.si.2.2] Se emplearán algoritmos y parámetros autorizados por el CCN.

#### **Refuerzo R1– Productos certificados**

[mp.si.2.r1.1] Se emplearán productos certificados conforme a lo establecido en [op.pl.5].

#### **Aplicación de la medida (por confidencialidad e integridad)**

- Nivel BAJO: no aplica
- Nivel MEDIO: mp.si.2



- Nivel ALTO: mp.si.2+ R1

### 5.5.3. Custodia [mp.si.3]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

#### Requisitos

- [mp.si.3.1] Se aplicará la debida diligencia y control a los soportes de información que permanecen bajo la responsabilidad de la organización, garantizando el control de acceso con medidas físicas ([mp.if.1] y [mp.if.7]) o lógicas ([mp.si.2]).
- [mp.si.3.2] Se respetarán las exigencias de mantenimiento del fabricante, en especial, en lo referente a temperatura, humedad y otros agentes medioambientales.

#### Aplicación de la medida

- Categoría BÁSICA: mp.si.3
- Categoría MEDIA: mp.si.3
- Categoría ALTA: mp.si.3

### 5.5.4. Transporte [mp.si.4]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

El responsable del sistema garantizará que los dispositivos permanecen bajo control y que satisfacen sus requisitos de seguridad mientras están siendo desplazados de un lugar a otro, fuera de las zonas controladas por la organización.

#### Requisitos

- [mp.si.4.1] Se dispondrá de un registro de entrada/salida que identifique al transportista que entrega/recibe el soporte.
- [mp.si.4.2] Se dispondrá de un procedimiento rutinario que coteje las salidas con las llegadas y levante las alarmas pertinentes cuando se detecte algún incidente.
- [mp.si.4.3] Se utilizarán los medios de protección criptográfica ([mp.si.2]) correspondientes al mayor nivel de seguridad de la información contenida.
- [mp.si.4.4] se gestionarán las claves según [op.exp.11].

#### Aplicación de la medida



- Categoría BÁSICA: mp.si.4
- Categoría MEDIA: mp.si.4
- Categoría ALTA: mp.si.4

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

dimensiones	C		
nivel	bajo	medio	alto
	aplica	aplica	aplica

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

#### Requisitos

[mp.si.5.1] Los soportes que vayan a ser reutilizados para otra información o liberados a otra organización serán objeto de un borrado seguro de su contenido empleando productos certificados conforme a lo establecido en [op.pl.5]. Cuando la naturaleza del soporte no permita un borrado seguro el soporte no podrá ser reutilizado en ningún otro sistema.

#### Refuerzo R1 – Destrucción de soportes

[mp.si.5.r1.1] Una vez finalizado el ciclo de vida del soporte de información deberá ser destruido de forma segura conforme a los criterios establecidos por el CCN.

#### Aplicación de la medida (por confidencialidad)

- Nivel BAJO: mp.si.5
- Nivel MEDIO: mp.si.5
- Nivel ALTO: mp.si.5

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

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

dimensiones	Todas		
categoría	básica	media	alta
	no aplica	+R1+R2+R3+R4	+R1+R2+R3+R4

#### Requisitos

[mp.sw.1.1] El desarrollo de aplicaciones se realizará sobre un sistema diferente y separado del de producción, no debiendo existir herramientas o datos de desarrollo en el entorno de producción, ni datos de producción en el de desarrollo.

#### Refuerzo R1 – Mínimo privilegio



[mp.sw.1.r1.1] Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

### Refuerzo R2 – Metodología de desarrollo seguro

[mp.sw.1.r2.1] Se aplicará una metodología de desarrollo seguro reconocida que:

- Tendrá en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida.
- Incluirá normas de programación segura: control de asignación y liberación de memoria, desbordamiento de memoria (*overflow*).
- Tratará específicamente los datos usados en pruebas.
- Permitirá la inspección del código fuente.

### Refuerzo R3 – Seguridad desde el diseño

[mp.sw.1.r3.1] Los siguientes elementos serán parte integral del diseño del sistema:

- Los mecanismos de identificación y autenticación.
- Los mecanismos de protección de la información tratada.
- La generación y tratamiento de pistas de auditoría.

### Refuerzo R4 – Datos de pruebas

[mp.sw.1.r4.1] Las pruebas previas a la implantación o modificación de los sistemas de información, preferentemente, no se realizarán con datos reales; en caso de que fuese necesario recurrir a datos reales, se garantizará el nivel de seguridad correspondiente.

### Aplicación de la medida

- Categoría BÁSICA: no aplica
- Categoría MEDIA: mp.sw.1 + R1 + R2 + R3 + R4
- Categoría ALTA: mp.sw.1 + R1 + R2 + R3 + R4

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

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1	+ R1

### Requisitos

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

[mp.sw.2.1] Se comprobará que:

- Se cumplen los criterios de aceptación en materia de seguridad.
- No se deteriora la seguridad de otros componentes del servicio.

### Refuerzo R1- Pruebas



[mp.sw.2.r1.1] Las pruebas se realizarán en un entorno aislado (pre-producción).

### Refuerzo R2 – Inspección de código fuente

[mp.sw.2.r2.1] Se realizará una auditoría de código fuente.

### Aplicación de la medida

- Categoría BÁSICA: mp.sw.2
- Categoría MEDIA: mp.sw.2 + R1
- Categoría ALTA: mp.sw.2 + R1

## 5.7. Protección de la información [mp.info]

### 5.7.1. Datos personales [mp.info.1]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	+ R1+R2	+ R1+R2

### Requisitos

[mp.info.1.1] Cuando el sistema trate datos personales, se estará a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016; la Ley Orgánica 3/2018, de 5 de diciembre, en especial su disposición adicional primera, así como el resto de normativa de aplicación, sin perjuicio de los requisitos establecidos en el presente real decreto.

### Refuerzo R1 – Anonimización y seudonimización de datos personales

[mp.info.1.r1.1] Se aplicarán medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado al riesgo, de forma que la persona física no sea identificable, ni directa ni indirectamente, salvo que esté justificado por los fines del tratamiento correspondiente. Estas medidas se aplicarán a los datos almacenados, transmitidos y compartidos.

### Refuerzo R2 – Tratamiento con fines estadísticos

[mp.info.1.r2.1] Se emplearán medidas que garanticen que los datos personales recolectados con fines estadísticos se destruirán lo antes posible, conservándose únicamente los necesarios para dichos fines y respetando el principio de minimización de los datos personales.

### Aplicación de la medida

- Categoría BÁSICA: mp.info.1
- Categoría MEDIA: mp.info.1 + R1 + R2
- Categoría ALTA: mp.info.1 + R1 + R2



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

dimensiones	C		
nivel	bajo	medio	alto
	no aplica	aplica	aplica

#### Requisitos

- [mp.info.2.1] Para calificar la información se estará a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas. El valor a emplear en el caso de información de materias no clasificadas sería USO OFICIAL para información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.
- [mp.info.2.2] La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema.
- [mp.info.2.3] La política de seguridad recogerá, directa o indirectamente, los criterios que, en cada organización, determinarán el nivel de seguridad requerido, dentro del marco establecido en el artículo 41 y los criterios generales prescritos en el Anexo I.
- [mp.info.2.4] El responsable de cada información seguirá los criterios determinados en el apartado anterior para asignar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal.
- [mp.info.2.5] El responsable de cada información en cada momento tendrá en exclusiva la potestad de modificar el nivel de seguridad requerido, de acuerdo a los apartados anteriores.

#### Aplicación de la medida (por confidencialidad)

- Nivel BAJO: no aplica
- Nivel MEDIO: mp.info.2
- Nivel ALTO: mp.info.2

### 5.7.3. Firma electrónica [mp.info.4]

dimensiones	I A		
nivel	bajo	medio	alto
	aplica	+R1+R2+R3	+ R1+R2+R3+R4

#### Requisitos

[mp.info.4.1] Se empleará cualquier tipo de firma electrónica de los previstos en el vigente ordenamiento jurídico, entre ellos, los sistemas de código seguro de verificación vinculados a la Administración Pública, órgano, organismo público o entidad de derecho público, en los términos y condiciones establecidos en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.



### Refuerzo R1 – Certificados cualificados

[mp.info.4.r1.1] Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.

### Refuerzo R2 – Algoritmos y parámetros autorizados

[mp.info.4.r2.1] Se emplearán algoritmos y parámetros autorizados por el CCN o por un esquema nacional o europeo.

El CCN determinará los algoritmos criptográficos que hayan sido autorizados nominalmente para su uso en el Esquema Nacional de Seguridad conforme a la Instrucción Técnica de Seguridad Criptología de empleo en el ENS.

### Refuerzo R3 – Verificación y validación de firma

[mp.info.4.r3.1] Cuando proceda, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquella soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, incluyendo certificados o datos de verificación y validación.

### Refuerzo R4 – Firma electrónica cualificada

[mp.info.4.r4.1] Se usará firma electrónica cualificada, empleando productos certificados conforme a lo establecido en [op.pl.5].

### Aplicación de la medida (por integridad y autenticidad)

- Nivel BAJO: mp.info.4
- Nivel MEDIO: mp.info.4 + R1 + R2 + R3
- Nivel ALTO: mp.info.4 + R1 + R2 + R3+ R4

### 5.7.4. Sellos de tiempo [mp.info.5]

dimensiones	T		
nivel	bajo	medio	alto
	no aplica	no aplica	aplica

### Requisitos

La utilización de sellos de tiempo exigirá adoptar las siguientes cautelas:

- [mp.info.5.1] Los sellos de tiempo se aplicarán a aquella información que sea susceptible de ser utilizada como evidencia electrónica en el futuro.
- [mp.info.5.2] Los datos pertinentes para la verificación posterior de la fecha serán tratados con la misma seguridad que la información fechada a efectos de disponibilidad, integridad y confidencialidad.



- [mp.info.5.3] Se renovarán regularmente los sellos de tiempo hasta que la información protegida ya no sea requerida por el proceso administrativo al que da soporte, en su caso.
- [mp.info.5.4] Se emplearán "sellos cualificados de tiempo electrónicos" atendiendo a lo dispuesto en el Reglamento (UE) nº 910/2014 y normativa de desarrollo.

#### Refuerzo R1 – Productos certificados

- [mp.info.5.r1.1.] Se utilizarán productos certificados (según [op.pl.5]).
- [mp.info.5.r1.2] Se asignará una fecha y hora a un documento electrónico, conforme a lo establecido en la ITS Criptología de empleo en el ENS.

#### Aplicación de la medida (por trazabilidad)

- Nivel BAJO: no aplica
- Nivel MEDIO: no aplica
- Nivel ALTO: mp.info.5

#### 5.7.5. Limpieza de documentos [mp.info.6]

dimensiones	C		
nivel	bajo	medio	alto
	aplica	aplica	aplica

#### Requisitos

[mp.info.6.1] En el proceso de limpieza de documentos, se retirará de estos toda la información adicional contenida en campos ocultos, metadatos, comentarios o revisiones anteriores, salvo cuando dicha información sea pertinente para el receptor del documento.

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

#### Aplicación de la medida (por confidencialidad)

- Nivel BAJO: mp.info.6
- Nivel MEDIO: mp.info.6
- Nivel ALTO: mp.info.6

#### 5.7.6. Copias de seguridad [mp.info.9]

dimensiones	D		
nivel	bajo	medio	alto
	aplica	aplica	+ R1



## Requisitos

- [mp.info.9.1] Se realizarán copias de seguridad que permitan recuperar datos perdidos, accidental o intencionadamente. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa relativa a copias de seguridad.
- [mp.info.9.2] Los procedimientos de respaldo establecidos indicarán:
  - a) Frecuencia de las copias.
  - b) Requisitos de almacenamiento en el propio lugar.
  - c) Requisitos de almacenamiento en otros lugares.
  - d) Controles para el acceso autorizado a las copias de respaldo.

## Refuerzo R1 – Pruebas de recuperación

[mp.info.9.r1.1] Los procedimientos de copia de seguridad y restauración deben probarse regularmente; la frecuencia dependerá de la criticidad de los datos y del impacto que cause la falta de disponibilidad.

## Refuerzo R2 – Protección de las copias de seguridad

[mp.info.9.r2.1] Al menos una de las copias de seguridad se almacenará de forma separada en lugar diferente, de tal manera que un incidente no pueda afectar tanto al repositorio original como a la copia simultáneamente.

## Aplicación de la medida (por disponibilidad)

- Nivel BAJO: mp.info.9
- Nivel MEDIO: mp.info.9
- Nivel ALTO: mp.info.9 + R1

## 5.8. Protección de los servicios [mp.s]

### 5.8.1. Protección del correo electrónico [mp.s.1]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	aplica

## Requisitos

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

- [mp.s.1.1] La información distribuida por medio de correo electrónico, se protegerá, tanto en el cuerpo de los mensajes, como en los anexos.
- [mp.s.1.2] Se protegerá la información de encaminamiento de mensajes y



establecimiento de conexiones.

- Se protegerá a la organización frente a problemas que se materializan por medio del correo electrónico, en concreto:
- [mp.s.1.3] Correo no solicitado, en su expresión inglesa «spam».
- [mp.s.1.4] Código dañino, constituidos por virus, gusanos, troyanos, espías, u otros de naturaleza análoga.
- [mp.s.1.5] Código móvil de tipo micro aplicación, en su expresión inglesa «applet».
- Se establecerán normas de uso del correo electrónico para el personal (Ver [org.2]). Estas normas de uso contendrán:
- [mp.s.1.6] Limitaciones al uso como soporte de comunicaciones privadas.
- [mp.s.1.7] Actividades de concienciación y formación relativas al uso del correo electrónico.

#### Aplicación de la medida

- Categoría BÁSICA: mp.s.1
- Categoría MEDIA: mp.s.1
- Categoría ALTA: mp.s.1

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

dimensiones	Todas		
categoría	básica	media	alta
	+[R1oR2]	+[R1oR2]	+R2+R3

#### Requisitos

Los sistemas que prestan servicios *web* deberán ser protegidos frente a las siguientes amenazas:

- [mp.s.2.1] Cuando la información requiera control de acceso, se garantizará la imposibilidad de acceder a la información obviando la autenticación, en particular tomando medidas en los siguientes aspectos:
  - a) Se evitará que el servidor ofrezca acceso a los documentos por vías alternativas al protocolo determinado.
  - b) Se prevendrán ataques de manipulación del localizador uniforme de recursos (*Uniform Resource Locator* URL).
  - c) Se prevendrán ataques de manipulación de fragmentos de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como *cookies*.



- d) Se prevendrán ataques de inyección de código.
- [mp.s.2.2] Se prevendrán intentos de escalado de privilegios.
- [mp.s.2.3] Se prevendrán ataques *de cross site scripting*.

### Refuerzo R1 – Auditorías de seguridad

- [mp.s.2.r1.1] Se realizarán auditorías continuas de seguridad de “caja negra” sobre las aplicaciones web durante la fase de desarrollo y antes de la fase de producción.
- [mp.s.2.r1.2] La frecuencia de estas auditorías de seguridad quedará definida en el procedimiento de auditoría.

### Refuerzo R2 – Auditorías de seguridad avanzada

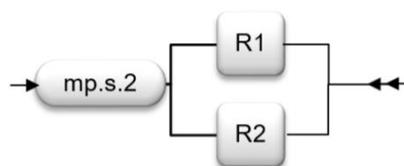
- [mp.s.2.r2.1] Se realizarán auditorías de seguridad de “caja blanca” sobre las aplicaciones web durante la fase de desarrollo.
- [mp.s.2.r2.2] Se emplearán metodologías definidas y herramientas automáticas de detección de vulnerabilidades en la realización de las auditorías de seguridad sobre las aplicaciones web.
- [mp.s.2.r2.3] Una vez finalizada una auditoría de seguridad, se analizarán los resultados y se solventarán las vulnerabilidades encontradas mediante los procedimientos definidos [op.exp.5].

### Refuerzo R3 – Protección de las cachés

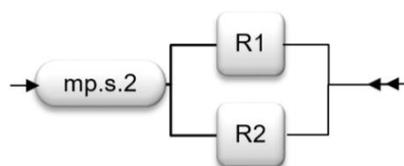
[mp.s.2.r3.1] Se prevendrán ataques de manipulación de programas o dispositivos que realizan una acción en representación de otros, conocidos en terminología inglesa como “proxies” y, sistemas especiales de almacenamiento de alta velocidad, conocidos en terminología inglesa como “caches”.

### Aplicación de la medida

- Categoría BÁSICA: mp.s.2 + [R1 o R2]



- Categoría MEDIA: mp.s.2 + [R1 o R2]





- Categoría ALTA: mp.s.2 + R2 + R3

### 5.8.3. Protección de la navegación web [mp.s.3]

dimensiones	Todas		
categoría	básica	media	alta
	aplica	aplica	+ R1

#### Requisitos

El acceso de los usuarios internos a navegar por internet se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

- [mp.s.3.1] Se establecerá una normativa de uso destacando el uso que se autoriza y las limitaciones de uso personal. En particular se concretará el uso permitido de conexiones cifradas.
- [mp.s.3.2] Se llevarán a cabo regularmente actividades de concienciación sobre higiene en la navegación web, fomentando el uso seguro y alertando de usos incorrectos.
- [mp.s.3.3] Se formará al personal encargado de la administración del sistema en monitorización del servicio y respuesta a incidentes.
- [mp.s.3.4] Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
- [mp.s.3.5] Se protegerá a la organización en general y al puesto de trabajo en particular frente a problemas que se materializan vía navegación web
- [mp.s.3.6] Se protegerá contra la actuación de programas dañinos: páginas activas, descargas de código ejecutable, previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
- [mp.s.3.6] Se establecerá una política ejecutiva de control de cookies, en particular para evitar la contaminación entre uso personal y uso organizativo.

#### Refuerzo R1 - Monitorización

- [mp.s.3.r1.1] Se registrará el uso de la navegación web, estableciendo los elementos que se registran, el periodo de retención de estos registros y el uso que el organismo prevé hacer de ellos.
- [mp.s.3.r1.2] Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido, indicando qué se analiza, qué se registra, durante cuánto tiempo se retienen los registros y qué uso prevé hacer el organismo de estas inspecciones. Sin perjuicio que se puedan autorizar accesos cifrados singulares a destinos de confianza.



- [mp.s.3.r1.3] Se establecerá una lista negra de destinos vetados.

### Refuerzo R2 – Destinos autorizados

[mp.s.3.r2.1] Se establecerá una lista blanca de destinos accesibles. Todo acceso fuera de los lugares en la lista blanca estará vetado, salvo autorización singular expresa.

### Aplicación de la medida

- Categoría BÁSICA: mp.s.3
- Categoría MEDIA: mp.s.3
- Categoría ALTA: mp.s.3 + R1

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

dimensiones	D		
nivel	bajo	medio	alto
	no aplica	aplica	+ R1

### Requisitos

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (*Denial of Service DoS, Distributed Denial of Service DDoS*). Para ello:

- [mp.s.8.1] Se planificará y dotará al sistema de capacidad suficiente para atender a la carga prevista con holgura.
- [mp.s.8.2] Se desplegarán tecnologías para prevenir los ataques conocidos.

### Refuerzo R1 – Detección y reacción

- [mp.s.8.r1.1] Se establecerá un sistema de detección y tratamiento de ataques de denegación deservicio (DoS y DDoS).
- [mp.s.8.r1.2] Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el proveedor de comunicaciones.

### Refuerzo R2 – Ataques propios

[mp.s.8.r2.1] Se detectará y se evitará el lanzamiento de ataques desde las propias instalaciones perjudicando a terceros.

### Aplicación de la medida (por disponibilidad)

- Nivel BAJO: no aplica
- Nivel MEDIO: mp.s.8
- Nivel ALTO: mp.s.8 + R1

## 7. Valoración de la implantación de las medidas de seguridad

Es habitual el empleo de niveles de madurez para caracterizar la implementación de un



proceso. El modelo de madurez de capacidad (*Capability Maturity Model, CMM*) permite describir las características que hacen un proceso efectivo, midiendo el grado o nivel de profesionalización de la actividad.

Un proceso es una colección de actividades o tareas relacionadas y estructuradas que, en una secuencia específica, proporciona un servicio para la organización.

Para la valoración de la implantación de las medidas de seguridad, éstas se analizarán como procesos y se estimará su nivel de madurez usando el modelo de madurez de capacidad (CMM).

Se identifican cinco "niveles de madurez", de modo que una organización que tenga institucionalizadas todas las prácticas incluidas en un nivel y sus inferiores, se considera que ha alcanzado ese nivel de madurez:

a) **L0 – Inexistente**

No existe un proceso que soporte el servicio requerido.

b) **L1 - Inicial. Ad hoc**

Las organizaciones en este nivel no disponen de un ambiente estable para la prestación del servicio requerido. Aunque se utilicen técnicas correctas de ingeniería, los esfuerzos se ven minados por falta de planificación. El éxito de los proyectos se basa la mayoría de las veces en el esfuerzo personal, aunque a menudo se producen fracasos y casi siempre retrasos y sobrecostos. El resultado es impredecible. A menudo las soluciones se implementan de forma reactiva a los incidentes.

Los procedimientos de trabajo, cuando existen, son informales, incompletos y no se aplican de forma sistemática.

c) **L2 – Reproducible, pero intuitivo.**

En este nivel las organizaciones disponen de unas prácticas institucionalizadas de gestión, existen unas métricas básicas y un razonable seguimiento de la calidad.

Existen procedimientos de trabajo, pero no están suficientemente documentados o no cubren todos los aspectos requeridos.

d) **L3 – Proceso definido.**

Además de una buena gestión, a este nivel las organizaciones disponen de normativa y procedimientos detallados y documentados de coordinación entre grupos, formación del personal, técnicas de ingeniería, etc.

e) **L4 – Gestionado y medible**

Se caracteriza porque las organizaciones disponen de un conjunto de métricas de efectividad y eficiencia, que se usan de modo sistemático para la toma de decisiones y la gestión de riesgos. El servicio resultante es de alta calidad.



f) **L5 - Optimizado.**

La organización completa está volcada en la mejora continua de los procesos. Se hace uso intensivo de las métricas y se gestiona el proceso de innovación.

Para cada medida de seguridad que sea de aplicación al sistema de información se exigirá un determinado nivel de madurez. Los niveles mínimos de madurez requeridos por el ENS en función de la categoría del sistema son:

<b>Categoría del sistema</b>	<b>Nivel mínimo de madurez requerido</b>
BÁSICA	L2 – Reproducible, pero intuitivo (50%)
MEDIA	L3 – Proceso definido (80%)
ALTA	L4 – Gestionado y medible (90%)

## **8. Desarrollo y complemento de las medidas de seguridad**

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

## **9. Interpretación**

La interpretación del presente Anexo se realizará según el sentido propio de sus palabras, en relación con el contexto, antecedentes históricos y legislativos, entre los que figura lo dispuesto en las instrucciones técnicas y a las guías CCN-STIC que sean de aplicación a la implementación y a diversos escenarios de aplicación tales como sedes electrónicas, servicios de validación de certificados electrónicos, servicios de fechado electrónico y validación de documentos fechados, atendiendo el espíritu y finalidad de aquellas.



## ANEXO III

### Auditoría de la seguridad

#### 1. Objeto de la auditoría.

1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos:

- a) Que la política de seguridad define los roles y funciones de los responsables de la información, los servicios, los activos y la seguridad del sistema de información.
- b) Que existen procedimientos para resolución de conflictos entre dichos responsables.
- c) Que se han designado personas para dichos roles a la luz del principio de "separación de funciones".
- d) Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.
- e) Que se cumplen las recomendaciones de protección descritas en el anexo II, sobre Medidas de Seguridad, en función de las condiciones de aplicación en cada caso.
- f) Que existe un sistema de gestión de la seguridad de la información, documentado y con un proceso regular de aprobación por la dirección.

1.2 La auditoría se basará en la existencia de evidencias que permitan sustentar objetivamente el cumplimiento de los puntos mencionados:

- a) Documentación de los procedimientos.
- b) Registro de incidentes.
- c) Examen del personal afectado: conocimiento y praxis de las medidas que le afectan.
- d) Productos certificados. Se considerará evidencia suficiente el empleo de productos que satisfagan lo establecido en el artículo 18 «Adquisición de productos y contratación de servicios de seguridad».

1.3. Se dispondrá de un programa o plan de auditorías documentado. Las actividades de auditoría que impliquen comprobaciones en los sistemas operativos deberán ser planificadas y acordadas previamente.

#### 2. Niveles de auditoría.

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

##### 2.1 Auditoría a sistemas de categoría BÁSICA.

- a) Los sistemas de información de categoría BÁSICA, o inferior, no necesitarán realizar una auditoría. Bastará una autoevaluación realizada por el mismo personal que administra el sistema de información, o en quien éste delegue.

El resultado de la autoevaluación debe estar documentado, indicando si cada medida de seguridad está implantada y sujeta a revisión regular y las evidencias que sustentan la valoración anterior.

- b) Los informes de autoevaluación serán analizados por el responsable de seguridad



competente, que elevará las conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

## 2.2 Auditoría a sistemas de categoría MEDIA O ALTA.

a) El informe de auditoría dictaminará sobre el grado de cumplimiento del presente real decreto, identificará sus deficiencias y sugerirá las posibles medidas correctoras o complementarias que sean necesarias, así como las recomendaciones que se consideren oportunas. Deberá, igualmente, incluir los criterios metodológicos de auditoría utilizados, el alcance y el objetivo de la auditoría, y los datos, hechos y observaciones en que se basen las conclusiones formuladas.

b) Los informes de auditoría serán analizados por el responsable de seguridad competente, que presentará sus conclusiones al responsable del sistema para que adopte las medidas correctoras adecuadas.

## 3. Interpretación.

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



## ANEXO IV

### Glosario

- Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.
- Análisis de riesgos. Estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en el organismo (en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.
- Área controlada. Zona o área en la que una organización considera cumplidas las medidas de seguridad físicas y procedimentales requeridas para la protección de la información y los sistemas de información ubicados en ella.
- Arquitectura de seguridad. Conjunto de elementos físicos y lógicos que forman parte de la arquitectura del sistema y cuyo objetivo es la protección de los activos dentro del sistema y en las interconexiones con otros sistemas.
- Auditoría de la seguridad. Revisión y examen independientes de los registros y actividades del sistema para verificar la idoneidad de dichos controles, asegurar que se cumplen la política de seguridad y los procedimientos operativos establecidos, detectar las infracciones de la seguridad y recomendar modificaciones apropiadas de los controles, de la política y de los procedimientos.
- Autenticidad. Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Cadena de suministro. Conjunto relacionado de recursos y procesos que comienza con la provisión de materias primas y se extiende a través de la entrega de productos o servicios al usuario final a través de los modos de transporte. Incluye a los proveedores (primer, segundo y tercer nivel), los almacenes de materia prima (directa o indirecta), las líneas de producción, los almacenes de productos terminados y los canales de distribución (mayoristas y minoristas), hasta llegar al cliente final.
- Categoría de un sistema. Es un nivel, dentro de la escala Básica-Media-Alta, con el que se adjetiva un sistema a fin de seleccionar las medidas de seguridad necesarias para el mismo. La categoría del sistema recoge la visión holística del conjunto de activos como un todo armónico, orientado a la prestación de unos servicios.
- Confidencialidad. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- Ciberseguridad. La protección de las redes y sistemas de información, sus usuarios y otras personas frente a las ciberamenazas.
- Distintivo de Declaración/Certificado de Conformidad. Documento electrónico, en formato PDF-A, firmado electrónicamente por la entidad bajo cuya responsabilidad se



encuentre el sistema de información en cuestión, incluyendo un enlace a la Declaración de Conformidad, que permanecerá accesible a través de la sede electrónica o página web de la entidad pública o privada, respectivamente, de que se trate.

- Dominio de seguridad: Colección de activos uniformemente protegidos, típicamente bajo una única autoridad. Los dominios de seguridad se utilizan para diferenciar entre zonas en el sistema de información. Por ejemplo:
  - instalaciones centrales, sucursales, comerciales trabajando con portátiles.
  - servidor central (host), frontal Unix y equipos administrativos.
  - seguridad física, seguridad lógica.
- Disponibilidad. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- Evento de seguridad. Ocurrencia identificada de un sistema, servicio o estado de red que indica un posible incumplimiento de la política de seguridad de la información o falla de los controles o una situación desconocida que puede ser relevante para la seguridad.
- Firma electrónica. Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
- Firma electrónica cualificada. Aquella que se realiza con un certificado de firma electrónica cualificado.
- Gestión de incidentes. Plan de acción para atender a los incidentes que se den. Además de resolverlos debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.
- Gestión de riesgos. Actividades coordinadas para dirigir y controlar a una organización con respecto a los riesgos.
- Incidente de seguridad. Un evento o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de la información.
- Integridad. Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- Medidas de seguridad. Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.
- Mínimo privilegio. Principio que determina que el diseño de la arquitectura de seguridad de un sistema garantiza el uso de los servicios y permisos mínimos necesarios para su correcto funcionamiento.



- Perfil de cumplimiento específico. Conjunto de medidas de seguridad, comprendidas o no en el Anexo II del presente real decreto, que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.
- Observatorio Digital. Un observatorio digital, en su propósito de conocer realidades de la información que se transmite a través de medios digitales, es un conjunto de capacidades para la toma de decisiones dedicado a la detección y seguimiento de anomalías en el origen, definición o diseminación de contenidos digitales, las cuales pudieran representar indicadores de amenaza.
- Política de firma electrónica. Conjunto de normas de seguridad, de organización, técnicas y legales para determinar cómo se generan, verifican y gestionan firmas electrónicas, incluyendo las características exigibles a los certificados de firma.
- Política de seguridad. Conjunto de directrices plasmadas en un documento, que rigen la forma en que una organización gestiona y protege la información y los servicios que consideran críticos.
- Principios básicos de seguridad. Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.
- Producto TIC. Elemento o grupo de elementos de las redes o los sistemas de información.
- Proceso. Conjunto organizado de actividades que se llevan a cabo para producir a un producto o servicio; tiene un principio y fin delimitado, implica recursos y da lugar a un resultado.
- Proceso TIC. Conjunto de actividades llevadas a cabo para la concepción, elaboración, suministro y mantenimiento de un producto o servicio de TIC.
- Proceso de seguridad. Método que se sigue para alcanzar los objetivos de seguridad de la organización. El proceso se diseña para identificar, medir, gestionar y mantener bajo control los riesgos a que se enfrenta el sistema en materia de seguridad.
- Requisitos mínimos de seguridad. Exigencias mínimas necesarias para asegurar la información y los servicios.
- TEMPEST. Término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por equipos eléctricos y electrónicos que, detectadas y analizadas, puedan llevar a la obtención de información) y a las medidas aplicadas a la protección contra dichas emanaciones.
- USO OFICIAL. Designa información con algún tipo de restricción en su manejo por su sensibilidad y confidencialidad.