TEXTO OFICIAL DEL BOE

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.

BOE-A-2021-1192
Última actualización en el BOE: 2025-12-20
Recopilado por Coposita el 2026-11-22

Cómo usar este PDF

- El índice dice en qué página empieza cada título y capítulo; pulsa una línea para ir allí. El panel lateral de tu lector tiene los mismos marcadores.
- Arriba, en cada página, ves en qué título y capítulo estás.
- Cada artículo va en su bloque, con la numeración destacada.
- El texto es el del BOE, sin alterar. Comprueba siempre la versión vigente en el BOE.

La citan: 1 programa de oposición de Coposita

Versión oficial: https://www.boe.es/buscar/act.php?id=BOE-A-2021-1192

Índice

CAPÍTULO I 4

Disposiciones generales 4

CAPÍTULO II · Marco estratégico e institucional 5

CAPÍTULO III · Requisitos de seguridad 8

CAPÍTULO IV · Gestión de incidentes de seguridad 10

CAPÍTULO V · Supervisión 12

Disposición adicional segunda. Orientaciones para la gestión de incidentes y cumplimiento de las obligaciones de notificación. 14

Disposición adicional tercera. Régimen específico del Banco de España. 14

Disposición adicional cuarta. Supuesto de dependencia de proveedores externos. 14

Disposición adicional quinta. Tratamientos de datos de carácter personal. 14

Disposición adicional sexta. Información sobre incidentes en el sistema financiero. 15

Disposición transitoria única. Desempeño transitorio de funciones en el sector energético. 15

Disposición final primera. Título competencial. 15

Disposición final segunda. Habilitación para el desarrollo normativo y aplicación. 15

Disposición final tercera. Entrada en vigor. 15

En el ámbito europeo, con el objetivo de dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información, se aprobó la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, conocida como la Directiva NIS (Security of Network and Information Systems). Esta norma parte de un enfoque global de la seguridad de las redes y sistemas de información en la Unión Europea, integrando requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.

La transposición de la citada Directiva NIS al ordenamiento jurídico español se llevó a cabo mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. Esta norma legal regula la seguridad de las redes y sistemas de información utilizados para la provisión de los servicios esenciales y los servicios digitales, estableciendo mecanismos que, con una perspectiva integral, permiten mejorar la protección frente a las amenazas que afectan a las redes y sistemas de información, y fijando un marco institucional de cooperación que facilita la coordinación de las actuaciones realizadas en esta materia tanto a nivel nacional como con los países de nuestro entorno, en particular, dentro de la Unión Europea.

El Real Decreto-ley 12/2018, de 7 de septiembre, habilita al Gobierno, en su disposición final tercera, para su desarrollo reglamentario. Con esa cobertura legal, y en cumplimiento del citado mandato y lo previsto en sus artículos 9.1 a), 11.1 a), 11.2, 16.2, 16.3, 19.1 y 19.5, este real decreto tiene por finalidad desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información al cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales y a la gestión de incidentes de seguridad.

El real decreto, en su artículo 3, pormenoriza la designación de autoridades competentes en materia de seguridad de las redes y sistemas de información prevista en el artículo 9.1.a) 2.º del Real Decreto-ley 12/2018, de 7 de septiembre. Es oportuno mencionar, en relación con la seguridad en el sector de la alimentación, la participación de la Agencia Española de Seguridad Alimentaria y Nutrición, dependiente del Ministerio de Consumo. Adicionalmente, y de conformidad con el artículo 11 del Real Decreto-ley 12/2018, de 7 de septiembre, el real decreto desarrolla los supuestos de cooperación y coordinación entre los equipos de respuesta a incidentes de seguridad informática (CSIRT) de referencia, y de estos con las autoridades competentes, que se instrumentan a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (artículo 4).

Con relación a la figura del punto de contacto único (artículo 5) que consagra la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, se desarrollan sus funciones de enlace para garantizar la cooperación transfronteriza con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación y la red de CSIRT.

Por otra parte, el artículo 6 de este real decreto desarrolla las previsiones del artículo 16.2 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre las medidas necesarias para el cumplimiento de las obligaciones de seguridad por parte de los operadores de servicios esenciales, que habrán de concretarse en una declaración de aplicabilidad de medidas de seguridad suscrita por el responsable de seguridad de la información del operador, cuyas funciones también se desarrollan en el artículo 7 de este real decreto. El plazo para la designación del responsable de la seguridad se establece en cumplimiento de la habilitación recogida en el artículo 16.3 del Real Decreto-ley 12/2018, de 7 de septiembre.

Por lo que se refiere a la notificación de incidentes, el real decreto, en sus artículos 8 y 9, desarrolla las obligaciones de notificación por parte de los operadores de servicios esenciales de los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, así como de los incidentes que puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales aun cuando no hayan tenido un efecto adverso real sobre aquellos, por referencia a los niveles de impacto y peligrosidad, según sea el caso, previstos en la Instrucción nacional de notificación y gestión de ciberincidentes que se contiene en el anexo.

El procedimiento de notificación de incidentes se articula a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes (artículos 10 y 11), a fin de permitir el intercambio de información entre los operadores de servicios esenciales y proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia, garantizando la confidencialidad, integridad y disponibilidad de la información (artículos 12 a 14).

Por último, en materia de supervisión de requisitos de seguridad, el real decreto desarrolla en su artículo 15 la obligación de colaboración de los operadores de servicios esenciales y los proveedores de servicios digitales con las autoridades competentes, que podrán requerir, asimismo, la colaboración de los CSIRT de referencia para el ejercicio de su función de supervisión.

En las disposiciones adicionales de este real decreto se recoge, entre otras materias, el régimen jurídico aplicable al Banco de España teniendo en cuenta su especial configuración jurídica como entidad de Derecho público con personalidad jurídica propia y plena capacidad pública y privada, que en el desarrollo de su actividad y para el cumplimiento de sus fines actúa con autonomía respecto a la Administración General del Estado, y como parte integrante del Sistema Europeo de Bancos Centrales (SEBC) y del Mecanismo Único de Supervisión (MUS). Esta especial configuración jurídica supone que el marco de seguridad de las redes y sistemas de información resulte de aplicación en la medida en que no interfiera con la naturaleza, funciones e independencia del Banco de España.

Este real decreto se adecúa a los principios de buena regulación establecidos en el artículo 129 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Responde, en primer lugar, a los principios de necesidad y eficacia, en tanto que la norma es necesaria para llevar a cabo el desarrollo reglamentario del Real Decreto-ley 12/2018, de 7 de septiembre, que transpone la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016 y, en concreto, para establecer el marco estratégico e institucional de seguridad de las redes y sistemas de información, las obligaciones de seguridad y la gestión de incidentes, siendo el instrumento más idóneo para la consecución de este objetivo. En segundo término, la norma cumple con el principio de proporcionalidad, al no existir otras medidas menos gravosas para los operadores de servicios esenciales y proveedores de servicios digitales destinadas a cumplir la obligación de adoptar medidas técnicas y de organización para gestionar los riesgos para la seguridad de sus redes y sistemas de información, así como de notificar los incidentes que tengan efectos perturbadores significativos en los servicios que prestan. Asimismo, este real decreto cumple con el principio de seguridad jurídica, resultando el proyecto conforme a la directiva europea de la que trae causa, así como con la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y su normativa de desarrollo, la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, y la normativa comunitaria y nacional en materia de protección de datos. Se ha cumplido igualmente con el principio de transparencia, al haber sometido el proyecto de real decreto al trámite de audiencia, definiéndose claramente los objetivos de la iniciativa normativa y su justificación. Por último, este real decreto resulta conforme con el principio de eficiencia, dado que no se establecen cargas adicionales a las contempladas en el real decreto-ley que desarrolla.

En la elaboración de este real decreto se ha solicitado informe de todos los departamentos ministeriales, así como de la Agencia Española de Protección de Datos, de la Comisión Nacional de los Mercados y de la Competencia, de la Comisión Nacional del Mercado de Valores, del Consejo de Seguridad Nuclear, y del Banco de España. Adicionalmente, se ha solicitado informe a todas las comunidades autónomas y se ha dado audiencia a las organizaciones representativas de los sectores afectados.

En su virtud, a propuesta conjunta de la Vicepresidenta Tercera del Gobierno y Ministra de Asuntos Económicos y Transformación Digital, de la Ministra de Defensa, del Ministro del Interior y de la Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes y Memoria Democrática, con la aprobación previa de la Ministra de Política Territorial y Función Pública, de acuerdo con el Consejo de Estado, y previa deliberación del Consejo de Ministros en su reunión del día 26 de enero de 2021,

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1 Objeto.

Este real decreto tiene por objeto desarrollar el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, en lo relativo al marco estratégico e institucional de seguridad de las redes y sistemas de información, la supervisión del cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales, y la gestión de incidentes de seguridad.

Artículo 2 Ámbito de aplicación.

1. De conformidad con el artículo 2 del Real Decreto-ley 12/2018, de 7 de septiembre, este real decreto se aplicará a la prestación de:

a) Los servicios esenciales dependientes de las redes y sistemas de información comprendidos en los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

b) Los servicios digitales que sean mercados en línea, motores de búsqueda en línea y servicios de computación en nube.

2. Estarán sometidos a este real decreto:

a) Los operadores de servicios esenciales establecidos en España. Se entenderá que un operador de servicios esenciales está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que estos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios o actividades.

Así mismo, este real decreto será de aplicación a los servicios esenciales que los operadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

De conformidad con lo previsto en el apartado 1 del artículo 6 del Real Decreto-ley 12/2018, la identificación de los servicios esenciales y de los operadores que los presten se efectuará por los órganos y procedimientos previstos por la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, y su normativa de desarrollo, en particular el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

b) Los proveedores de servicios digitales que tengan su sede social en España y que constituya su establecimiento principal en la Unión Europea, así como los que, no estando establecidos en la Unión Europea, designen en España a su representante en la Unión para el cumplimiento 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.

3. Este real decreto no se aplicará a:

a) Los operadores de redes y servicios de comunicaciones electrónicas y los prestadores de servicios electrónicos de confianza que no sean designados como operadores críticos en virtud de la Ley 8/2011, de 28 de abril.

b) Los proveedores de servicios digitales cuando se trate de microempresas o pequeñas empresas, de acuerdo con las definiciones recogidas en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas.

4. De conformidad con el artículo 18 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando una normativa nacional o comunitaria establezca para un sector obligaciones de seguridad de las redes y sistemas de información o de notificación de incidentes que tengan efectos, al menos, equivalentes a los de las obligaciones previstas en el Real Decreto-ley 12/2018, de 7 de septiembre, prevalecerán aquellos requisitos y los mecanismos de supervisión correspondientes.

CAPÍTULO II · Marco estratégico e institucional

Artículo 3 Autoridades competentes.

Las autoridades competentes en materia de seguridad de las redes y sistemas de información serán, con carácter general, las establecidas en el artículo 9.1 del Real Decreto-ley 12/2018, de 7 de septiembre. En particular, son autoridades competentes para los operadores de servicios esenciales que no sean operadores críticos de acuerdo con la Ley 8/2011, de 28 de abril, y que no estén incluidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, las siguientes:

a) Respecto al sector del transporte: el Ministerio de Transportes, Movilidad y Agenda Urbana, a través de la Secretaría de Estado de Transportes, Movilidad y Agenda Urbana.

b) Respecto al sector de la energía: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

c) Respecto al sector de las tecnologías de la información y las telecomunicaciones: el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales.

d) Respecto al sector del sistema financiero:

1.º El Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, en el ámbito de los seguros y fondos de pensiones.

2.º El Banco de España, para las entidades de crédito.

3.º La Comisión Nacional del Mercado de Valores, para las entidades que prestan servicios de inversión y las sociedades gestoras de instituciones de inversión colectiva.

e) Respecto al sector del espacio: el Ministerio de Defensa, a través de la Secretaría de Estado de Defensa.

f) Respecto al sector de la industria química: el Ministerio de Interior, a través de la Secretaría de Estado de Seguridad.

g) Respecto al sector de las instalaciones de investigación: el Ministerio de Ciencia e Innovación, a través de la Secretaría General de Investigación.

h) Respecto al sector de la salud: el Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

i) Respecto al sector del agua: el Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Medio Ambiente.

j) Respecto al sector de la alimentación:

1.º El Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación.

2.º El Ministerio de Sanidad, a través de la Secretaría de Estado de Sanidad.

3.º El Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio.

4.º El Ministerio de Consumo, a través de la Agencia Española de Seguridad Alimentaria y Nutrición (AESAN).

k) Respecto al sector de la industria nuclear:

1.º El Ministerio para la Transición Ecológica y el Reto Demográfico, a través de la Secretaría de Estado de Energía.

2.º El Consejo de Seguridad Nuclear.

Artículo 4 Cooperación y coordinación de los CSIRT de referencia.

1. La cooperación entre los CSIRT de referencia, y entre estos y las autoridades competentes, se instrumentará a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes regulada en el artículo 11.

2. A efectos de la cooperación prevista en el artículo 11.1.a) 3.º del Real Decreto-ley 12/2018, de 7 de septiembre, se entenderá que son operadores con incidencia en la Defensa Nacional aquellos proveedores de servicios esenciales básicos para el funcionamiento del Ministerio de Defensa o para la operatividad de las Fuerzas Armadas que se establezcan, a propuesta del Ministerio de Defensa, por la Comisión Nacional para la Protección de las Infraestructuras Críticas.

La designación como operador con incidencia en la Defensa Nacional se llevará a cabo de conformidad con lo previsto en el Reglamento de protección de las infraestructuras críticas, aprobado por el Real Decreto 704/2011, de 20 de mayo. Así mismo, los CSIRT de referencia serán informados de la identidad de los operadores de servicios esenciales de su comunidad que sean designados operadores con incidencia en la Defensa Nacional.

El Ministerio de Defensa comunicará oportunamente a la Comisión Nacional para la Protección de las Infraestructuras Críticas las actualizaciones derivadas de cambios de operadores en la provisión de estos servicios, que activarán las correspondientes notificaciones de alta o baja como operadores con incidencia en la Defensa Nacional tanto a los propios operadores como a sus CSIRT de referencia.

Cuando un operador con incidencia en la Defensa Nacional sufra un incidente deberá analizar si, por su alcance, este pudiera tener impacto en el funcionamiento del Ministerio de Defensa o en la operatividad de las Fuerzas Armadas. En el caso de que así fuera, lo pondrá de inmediato en conocimiento de su CSIRT de referencia, quien informará al ESPDEF-CERT del Mando Conjunto del Ciberespacio a través de los canales establecidos. En estos casos, el ESPDEF-CERT del Mando Conjunto del Ciberespacio deberá ser oportunamente informado de la evolución de la gestión del incidente.

3. Los supuestos de especial gravedad a los que se refiere el artículo 11.2 párrafo primero del Real Decreto-ley 12/2018, de 7 de septiembre, en los que el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT, serán todos aquellos que, atendiendo a la naturaleza de las notificaciones inicial o sucesivas del incidente recibidas por el CSIRT de referencia, posean un impacto o nivel de peligrosidad muy alta o crítica de acuerdo con lo establecido en el anexo, y exijan un nivel de coordinación técnica con los otros CSIRT de referencia superior al necesario en situaciones ordinarias.

El Consejo Nacional de Ciberseguridad será inmediatamente informado y podrá desactivar la coordinación prevista en este artículo, que únicamente podrá producirse cuando haya cesado la situación prevista en el párrafo anterior y que no afectará al proceso de notificación de incidentes regulados en los artículos 11, 19.1 y 19.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. El CCN-CERT, en el caso previsto en el apartado anterior, y la Oficina de Coordinación de Ciberseguridad del Ministerio del Interior (OCC), en los supuestos previstos en el artículo 11.2 párrafo segundo del Real Decreto-ley 12/2018, de 7 de septiembre, requerirán al CSIRT de referencia, tras la primera notificación del incidente, al menos la siguiente información:

a) Confirmación de que son correctos los datos asignados al incidente, en particular verificando, si existe esta información, la validez de:

1.º La clasificación del incidente.

2.º La peligrosidad del incidente.

3.º El impacto del incidente.

b) Plan de acción del CSIRT para abordar la resolución técnica del incidente, si procede.

c) Cualquier información que permita determinar el posible impacto transfronterizo del incidente.

Siempre que sea posible se empleará la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes para las comunicaciones consideradas en este apartado.

Artículo 5 Punto de contacto único.

1. En su función de enlace para garantizar la cooperación transfronteriza de las autoridades competentes designadas conforme al artículo 9 del Real Decreto-ley 12/2018, de 7 de septiembre, con las autoridades competentes de otros Estados miembros de la Unión Europea, así como con el grupo de cooperación contemplado en el artículo 11 de la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, y la red de CSIRT, el Consejo de Seguridad Nacional, a través del Departamento de Seguridad Nacional:

a) Comunicará a la Comisión Europea la lista de los operadores de servicios esenciales nacionales establecidos para cada sector y subsector a los que se refiere el artículo 6 del Real Decreto-ley 12/2018, de 7 de septiembre e informará a los puntos de contacto único de otros Estados sobre la intención de identificación de un operador de servicios esenciales de otro Estado miembro que ofrezca servicios en España.

b) Transmitirá a los puntos de contacto de otros Estados miembros de la Unión Europea afectados la información sobre incidentes con impacto transfronterizo que le transmitan las autoridades competentes o CSIRT de referencia, según lo establecido en el artículo 25 del Real Decreto-ley 12/2018, de 7 de septiembre.

c) Remitirá a los CSIRT de referencia y a las autoridades competentes nacionales la correspondiente información sobre incidentes que puedan tener efectos perturbadores en los servicios esenciales que reciba de los puntos de contacto de los correspondientes Estados miembros, para que adopten las medidas oportunas en el ejercicio de sus funciones respectivas.

d) Dictará las instrucciones pertinentes a las autoridades competentes para que elaboren, anualmente, el informe al que se refiere el artículo 27.1 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre el tipo y número de incidentes comunicados, sus efectos en los servicios prestados o en otros servicios y su carácter nacional o transfronterizo dentro de la Unión Europea, teniendo en cuenta las indicaciones del grupo de cooperación respecto al formato y contenido de la información a transmitir.

e) Recabará de las autoridades competentes el informe anual al que se refiere la letra anterior, y elaborará un informe anual resumido sobre las notificaciones recibidas, que remitirá al grupo de cooperación antes del 15 de febrero de cada año y, posteriormente, a las autoridades competentes y a los CSIRT de referencia, para su conocimiento.

2. Adicionalmente a las funciones de enlace previstas en el apartado anterior, y de conformidad con lo previsto en el artículo 9.2 del Real Decreto-ley 12/2018, de 7 de septiembre, el Consejo de Seguridad Nacional, a través de su comité especializado en materia de ciberseguridad, garantizará la coordinación de las actuaciones de las autoridades competentes mediante:

a) El fomento de la coherencia entre los requisitos de seguridad específicos que en su caso adopten las autoridades competentes, conforme a lo previsto en el artículo 6.6 de este real decreto.

b) El fomento de la coherencia entre las obligaciones específicas que en su caso establezcan las autoridades competentes, conforme a lo previsto en el artículo 8.3 de este real decreto.

c) El impulso de la coordinación de las disposiciones y actuaciones de las autoridades competentes y las actuaciones de los CSIRT de referencia con las disposiciones y actuaciones en materia de seguridad de la información de las autoridades de protección de datos y de seguridad pública.

3. Del mismo modo, el Consejo de Seguridad Nacional ejercerá las funciones de coordinación previstas en el apartado 2 anterior en los supuestos contemplados en el artículo 18 del Real Decreto-ley 12/2018, de 7 de septiembre.

CAPÍTULO III · Requisitos de seguridad

Artículo 6 Medidas para el cumplimiento de las obligaciones de seguridad.

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán adoptar las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que afecten a la seguridad de las redes y sistemas de información utilizados para la prestación de sus servicios, tanto si se trata de redes y sistemas propios, como de proveedores externos.

2. En el caso de los operadores de servicios esenciales, deberán aprobar unas políticas de seguridad de las redes y sistemas de información, atendiendo a los principios de seguridad integral, gestión de riesgos, prevención, respuesta y recuperación, líneas de defensa, reevaluación periódica y segregación de tareas.

Dichas políticas considerarán, como mínimo, los siguientes aspectos:

a) Análisis y gestión de riesgos.

b) Gestión de riesgos de terceros o proveedores.

c) Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.

d) Gestión del personal y profesionalidad.

e) Adquisición de productos o servicios de seguridad.

f) Detección y gestión de incidentes.

g) Planes de recuperación y aseguramiento de la continuidad de las operaciones.

h) Mejora continua.

i) Interconexión de sistemas.

j) Registro de la actividad de los usuarios.

3. Las medidas de seguridad que se adopten por los operadores de servicios esenciales deberán tener en cuenta, en particular, la dependencia de las redes y sistemas de información y la continuidad de servicios o suministros contratados por el operador, así como las interacciones que presenten con redes y sistemas de información de terceros.

4. La relación de medidas adoptadas se formalizará en un documento denominado Declaración de Aplicabilidad de medidas de seguridad, que será suscrito por el responsable de seguridad de la información designado conforme a lo previsto en el artículo siguiente y que se incluirá en la política de seguridad que apruebe la Dirección de la organización. Dicho documento, que deberá remitirse a la autoridad competente respectiva en el plazo de seis meses desde la designación del operador como operador de servicios esenciales, deberá revisarse, al menos, cada tres años. Tanto la Declaración de Aplicabilidad de medidas de seguridad inicial, como sus sucesivas revisiones serán objeto de supervisión por la autoridad competente respectiva, según se prevé en el artículo 14 de este real decreto.

5. Las medidas a las que se refieren los apartados anteriores tomarán como referencia las recogidas en el anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en la medida en que sean aplicables, y se basarán, cuando sea posible, en otros esquemas nacionales de seguridad existentes.

Sin perjuicio de lo anterior, podrán tenerse en cuenta otros estándares reconocidos internacionalmente.

6. Las medidas adoptadas podrán ser complementadas con otras, atendiendo a necesidades específicas, entre ellas, la posibilidad de exigir un documento de aplicabilidad de los sistemas afectados por esta normativa, en aquellos operadores con entornos de sistemas de información especialmente complejos. En particular, se complementarán con las que, en su caso, establezcan con carácter específico las autoridades competentes, de conformidad con lo previsto en el artículo 16.4 y el artículo 32.2 del Real Decreto-ley 12/2018, de 7 de septiembre.

7. En la elaboración de las políticas de seguridad de las redes y sistemas de información se tendrán en cuenta los riesgos que se derivan del tratamiento de los datos personales, de acuerdo con el artículo 24 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 (en adelante, Reglamento general de protección de datos). En caso de que el análisis de gestión de riesgos de acuerdo con el Reglamento general de protección de datos exija medidas adicionales a implantar respecto de las previstas en el

Real Decreto 3/2010, de 8 de enero, se adoptarán las medidas de acuerdo con el artículo 24.1 del Reglamento general de protección de datos.

Artículo 7 Responsable de la seguridad de la información.

1. Los operadores de servicios esenciales designarán una persona, unidad u órgano colegiado, responsable de la seguridad de la información que ejercerá las funciones de punto de contacto y coordinación técnica con la autoridad competente y CSIRT de referencia que le corresponda de conformidad con lo previsto en el apartado tercero. En el supuesto de que el responsable de seguridad de la información sea una unidad u órgano colegiado, se deberá designar una persona física representante, así como un sustituto de este que asumirá sus funciones en casos de ausencia, vacante o enfermedad. El plazo para llevar a cabo dicha designación será de tres meses desde su designación como operador de servicios esenciales.

2. Los operadores de servicios esenciales comunicarán a la autoridad competente respectiva la designación del responsable de la seguridad de la información dentro del plazo establecido en el apartado anterior, así como los nombramientos y ceses que afecten a la designación del responsable de la seguridad de la información en el plazo de un mes desde que aquellos se produzcan.

3. El responsable de la seguridad de la información actuará como punto de contacto con la autoridad competente en materia de supervisión de los requisitos de seguridad de las redes y sistemas de información, y como punto de contacto especializado para la coordinación de la gestión de los incidentes con el CSIRT de referencia. Se desarrollarán bajo su responsabilidad, entre otras, las siguientes funciones:

a) Elaborar y proponer para aprobación por la organización, de conformidad con lo establecido en el artículo 6.2 de este real decreto, las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios, de conformidad con lo dispuesto en el artículo 6.

b) Supervisar y desarrollar la aplicación de las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo controles periódicos de seguridad.

c) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad considerado en el artículo 6.3 párrafo segundo de este real decreto.

d) Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.

e) Remitir a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, las notificaciones de incidentes que tengan efectos perturbadores en la prestación de los servicios a los que se refiere el artículo 19.1 del Real Decreto-ley 12/2018, de 7 de septiembre.

f) Recibir, interpretar y supervisar la aplicación de las instrucciones y guías emanadas de la autoridad competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.

g) Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

El responsable de la seguridad de la información, para desarrollar estas funciones, se podrá apoyar en servicios prestados por terceros.

4. Los operadores de servicios esenciales garantizarán que el responsable de la seguridad de la información cumpla con los siguientes requisitos:

a) Contar con personal con conocimientos especializados y experiencia en materia de ciberseguridad, desde los puntos de vista organizativo, técnico y jurídico, adecuados al desempeño de las funciones indicadas en el apartado anterior.

b) Contar con los recursos necesarios para el desarrollo de dichas funciones.

c) Ostentar una posición en la organización que facilite el desarrollo de sus funciones, participando de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la seguridad, y manteniendo una comunicación real y efectiva con la alta dirección.

d) Mantener la debida independencia respecto de los responsables de las redes y los sistemas de información.

5. Siempre que concurran los requisitos de conocimiento, experiencia, independencia y, en su caso, titulación, las funciones y responsabilidades encomendadas al responsable de la seguridad de la información podrán compatibilizarse con las señaladas para el Responsable de Seguridad y Enlace y el Responsable de Seguridad del Esquema Nacional de Seguridad, de conformidad con lo dispuesto en la normativa aplicable a estas figuras.

CAPÍTULO IV · Gestión de incidentes de seguridad

Artículo 8 Gestión de incidentes de seguridad.

1. Los operadores de servicios esenciales y los proveedores de servicios digitales deberán gestionar y resolver los incidentes de seguridad que afecten a las redes y sistemas de información utilizados para la prestación de sus servicios. En el caso de redes y sistemas que no sean propios los operadores deberán tomar las medidas necesarias para garantizar que dichas acciones se lleven a cabo por los proveedores externos.

Esta obligación alcanza tanto a los incidentes detectados por el propio operador o proveedor como a los que les señalen el CSIRT de referencia o la autoridad competente, cuando tengan conocimiento de alguna circunstancia que haga sospechar de la existencia de un incidente.

2. Sin perjuicio de lo previsto en el artículo 28.1 del Real Decreto-ley 12/2018, de 7 de septiembre, los operadores de servicios esenciales y los proveedores de servicios digitales podrán solicitar voluntariamente ayuda especializada del CSIRT de referencia para la gestión de los incidentes, debiendo en tales casos atender a las indicaciones que reciban de este para resolver el incidente, mitigar sus efectos y reponer los sistemas afectados.

3. En la resolución de los incidentes, los operadores de servicios esenciales aplicarán los aspectos pertinentes de la política de gestión de la seguridad de las redes y sistemas de información a la que se refiere el artículo 6, así como las obligaciones específicas que en su caso establezcan las autoridades competentes.

Artículo 9 Obligaciones de notificación de incidentes de los operadores de servicios esenciales.

1. Los operadores de servicios esenciales notificarán a la autoridad competente respectiva, a través del CSIRT de referencia, los incidentes que puedan tener efectos perturbadores significativos en dichos servicios, considerándose a tal efecto los incidentes con un nivel de impacto crítico, muy alto o alto, según el detalle que se especifica en el apartado 4 de la Instrucción nacional de notificación y gestión de ciberincidentes, que se contiene en el anexo de este real decreto.

Asimismo, notificarán los sucesos o incidencias que, por su nivel de peligrosidad, puedan afectar a las redes y sistemas de información empleados para la prestación de los servicios esenciales, aun cuando no hayan tenido todavía un efecto adverso real sobre aquellos. A estos efectos, se considerarán los incidentes con un nivel de peligrosidad crítico, muy alto o alto, según el detalle que se especifica en el apartado 3 de la citada Instrucción.

2. Sin perjuicio de lo anterior, las autoridades competentes podrán establecer, de conformidad con el artículo 19.5 del Real Decreto-ley 12/2018, de 7 de septiembre, obligaciones específicas de notificación que contemplen niveles diferentes a los previstos en la Instrucción nacional de notificación y gestión de ciberincidentes, así como factores y umbrales sectoriales específicos, aplicables a los operadores sometidos a su supervisión.

3. La notificación de un ciberincidente conforme a este real decreto no excluye ni sustituye la notificación que de los mismos hechos deba realizarse a otros organismos conforme a su normativa específica.

En particular, las obligaciones de notificación previstas en los apartados anteriores son independientes de las que deban realizarse a la Agencia Española de Protección de Datos conforme a lo previsto en el artículo 33 del Reglamento general de protección de datos, sin perjuicio de la cooperación entre autoridades prevista en el artículo 29 del Real Decreto-ley 12/2018, y la posibilidad de acceso por parte de la citada agencia a la plataforma común de notificación de incidentes prevista en su disposición adicional tercera.

A estos efectos, las notificaciones previstas en los apartados 1 y 2 de este artículo incluirán la información que, para los casos de violación de la seguridad de los datos personales, se contenga en los formularios aprobados por la Agencia Española de Protección de Datos.

Artículo 10 Procedimientos de notificación de incidentes.

1. Los CSIRT de referencia garantizarán un intercambio fluido de información con las autoridades competentes que correspondan, asegurando el adecuado seguimiento durante la gestión de los incidentes, así como el acceso a la información empleada en las distintas fases que componen la gestión de incidentes.

2. Los operadores de servicios esenciales realizarán las notificaciones a través del responsable de la seguridad de la información designado.

En el caso de que un operador de servicios esenciales reúna los criterios previstos en el artículo 6.2 del Real Decreto-ley 12/2018, de 7 de septiembre, sobre seguridad de las redes y sistemas de información, el responsable de la seguridad de

la información se coordinará a estos efectos con el Responsable de Seguridad y Enlace previsto en el artículo 16 de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

3. Los operadores de servicios esenciales deberán realizar una primera notificación tan pronto como dispongan de información para determinar que se dan las circunstancias para la notificación, atendiendo a los factores y umbrales correspondientes.

Se efectuarán las notificaciones intermedias que sean precisas para actualizar o completar la información incorporada a la notificación inicial, e informar sobre la evolución del incidente, mientras este no esté resuelto, y se realizará una notificación final del incidente tras su resolución, informando del detalle de la evolución del suceso, la valoración de la probabilidad de su repetición, y las medidas correctoras que eventualmente tenga previsto adoptar el operador. Los umbrales temporales exigidos para dichas notificaciones serán los recogidos en el anexo de este real decreto.

4. Las notificaciones incluirán, en cuanto esté disponible, la información que permita determinar cualquier efecto transfronterizo del incidente.

5. Lo establecido en los apartados anteriores será de aplicación a los proveedores de servicios digitales en tanto que no se regule de modo diferente en los actos de ejecución previstos en el artículo 16.9 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.

6. El CSIRT de referencia, en colaboración con la autoridad competente, valorará con prontitud dicha información con vistas a determinar si el incidente puede tener efectos perturbadores significativos para los servicios esenciales prestados en otros Estados miembros de la Unión Europea, informando en tal caso a través del punto de contacto único a los Estados miembros afectados.

Asimismo, la autoridad competente valorará, conjuntamente con el correspondiente CSIRT de referencia, la información sobre incidentes con posibles impactos transfronterizos que reciba de otros Estados miembros, y se lo indicará y transmitirá la información relevante a los operadores de servicios esenciales que puedan verse afectados.

Artículo 11 Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

1. El CCN-CERT en colaboración con el INCIBE-CERT y el ESPDEF-CERT del Mando Conjunto del Ciberespacio pondrá a disposición de todos los actores involucrados la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes a la que se refiere el artículo 19.4 del Real Decreto-ley 12/2018, de 7 de septiembre.

2. La plataforma permitirá el intercambio de información y el seguimiento de incidentes entre los operadores de servicios esenciales o proveedores de servicios digitales, las autoridades competentes y los CSIRT de referencia de manera segura y confiable, sin perjuicio de los requisitos específicos que apliquen en materia de protección de datos de carácter personal.

3. Esta plataforma deberá garantizar asimismo la disponibilidad, autenticidad, integridad y confidencialidad de la información, así como podrá emplearse también para dar cumplimiento a la exigencia de notificación derivada de regulaciones sectoriales, de acuerdo con el artículo 19.5 del Real Decreto-ley 12/2018, de 7 de septiembre.

4. La plataforma dispondrá asimismo de diversos canales de comunicación para su uso por parte de las autoridades competentes y los CSIRT de referencia. La plataforma garantizará el acceso de las autoridades competentes a toda la información relativa a la notificación y estado de situación de los incidentes de su ámbito de competencia que les permita efectuar en todo momento el necesario seguimiento y control de su estado de situación. Igualmente, las autoridades competentes tendrán acceso a través de la plataforma a datos estadísticos, en particular a los necesarios para generar los informes a los que hace mención el artículo 5.

5. Asimismo, la plataforma implementará el procedimiento de notificación y gestión de incidentes, que estará disponible durante todas las horas del día y todos los días del año, y dispondrá como mínimo de las siguientes capacidades:

a) Capacidad de gestión de ciberincidentes, con incorporación de taxonomía, criticidad y notificaciones a terceros, según lo establecido en el anexo.

b) Capacidad de intercambio de información sobre ciberamenazas.

c) Capacidad de análisis de muestras.

d) Capacidad de registro y notificación de vulnerabilidades.

e) Capacidad de comunicaciones seguras entre los actores involucrados en diferentes formatos y plataformas.

f) Capacidad de intercambio masivo de datos.

g) Generación de estadísticas e informes agregados.

Artículo 12 Información sobre incidentes.

1. Cuando las circunstancias lo permitan, los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los proveedores de servicios digitales notificantes la información pertinente con respecto al seguimiento de la notificación de un incidente, en particular aquella que pueda facilitar la gestión eficaz del incidente.

2. Asimismo, las autoridades competentes y los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los proveedores de servicios digitales que pudieran verse afectados por dichos incidentes la información que pudiera serles relevante para prevenir y en su caso resolver el incidente.

3. Al proporcionar la información a la que se refieren los apartados anteriores, las autoridades competentes y los CSIRT de referencia velarán por los intereses comerciales de los operadores de servicios esenciales y proveedores de servicios digitales, preservando la confidencialidad de la información que recaben de estos, de conformidad con lo establecido en el artículo 15 del Real Decreto-ley 12/2018, de 7 de septiembre.

Artículo 13 Actuaciones ante incidentes con carácter presuntamente delictivo.

En cumplimiento de lo dispuesto en el artículo 262 de la Ley de Enjuiciamiento Criminal, la OCC comunicará a la mayor brevedad posible al Ministerio Fiscal y, en su caso, a las Unidades orgánicas de Policía Judicial competentes, aquellos incidentes de seguridad que le sean notificados y que revistan carácter presuntamente delictivo, trasladando al tiempo la información que posea en relación con ello. A dicho fin podrá requerir de los operadores afectados o de los CSIRT de referencia cuanta información relacionada con el incidente se estime necesaria.

Artículo 14 Consulta con otras autoridades.

1. Las consultas con otras autoridades con competencia en materia de seguridad pública y seguridad ciudadana, previstas en el artículo 14.1 del Real Decreto-ley 12/2018, de 7 de septiembre, se realizarán a través de la OCC.

2. Las consultas relativas al resto de materias previstas en el citado artículo 14 se realizarán directamente a las autoridades competentes correspondientes.

CAPÍTULO V · Supervisión

Artículo 15 Supervisión del cumplimiento de obligaciones de seguridad y de notificación de incidentes.

1. Las autoridades competentes supervisarán en su ámbito de actuación el cumplimiento de las obligaciones de seguridad y de notificación de incidentes que sean de aplicación a los operadores de servicios esenciales y a los proveedores de servicios digitales de conformidad con el Real Decreto-ley 12/2018, de 7 de septiembre, y este real decreto.

2. Los operadores de servicios esenciales y los proveedores de servicios digitales colaborarán con la autoridad competente en dicha supervisión, facilitando las actuaciones de inspección, proporcionando toda la información que a tal efecto se les requiera, y aplicando las instrucciones dictadas, en su caso, para la subsanación de las deficiencias observadas.

3. El cumplimiento de las obligaciones de seguridad en las redes y sistemas de información podrá ser acreditado mediante la certificación en un esquema de seguridad que, previa consulta al CSIRT de referencia, sea reconocido por la autoridad competente.

4. Las autoridades competentes podrán realizar las actuaciones inspectoras que sean precisas para el ejercicio de su función de control. En particular, las actuaciones de inspección de las autoridades competentes, que podrán ser apoyadas por los CSIRT de referencia, tendrán por objeto:

a) Controlar el cumplimiento de las normas e instrucciones técnicas que, en su caso, resulten aplicables a los operadores sujetos a su supervisión.

b) Verificar el cumplimiento de las funciones del responsable de seguridad de la información designado por los operadores de servicios esenciales, según lo previsto en el artículo 7.3 de este real decreto.

c) Realizar las comprobaciones, inspecciones, pruebas y revisiones necesarias para verificar el cumplimiento de las medidas de seguridad previstas en el artículo 6, en particular, la política de seguridad de los operadores de servicios esenciales y la Declaración de aplicabilidad de medidas de seguridad.

De conformidad con lo previsto en el artículo 32.1 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando el volumen o complejidad de las actuaciones de inspección que deban desarrollarse así lo aconseje, las autoridades competentes

podrán requerir al operador de servicios esenciales la remisión de un informe de auditoría, elaborado por una entidad externa, solvente e independiente, sobre la seguridad de sus redes y sistemas de información.

5. Los CSIRT de referencia colaborarán con las autoridades competentes, cuando estas se lo requieran, en el ejercicio de las funciones a las que se refiere el apartado anterior. En particular, facilitarán asesoramiento técnico sobre la idoneidad de las medidas de seguridad adoptadas por los operadores de servicios esenciales y los proveedores de servicios digitales en virtud del artículo 6 de este real decreto.

Asimismo, cuando se trate de operadores con incidencia en la Defensa Nacional a que se refiere el artículo 4.2 de este real decreto, el ESPDEF-CERT del Mando Conjunto del Ciberespacio podrá colaborar en la supervisión con la autoridad competente.

6. En el caso de los proveedores de servicios digitales la supervisión se llevará a cabo de manera coordinada con las autoridades competentes correspondientes de los Estados miembros de la Unión Europea donde dichos proveedores presten servicios o tengan su establecimiento principal en la Unión.

Disposición adicional primera. Designación del responsable de la seguridad de la información por los operadores de servicios esenciales designados.

Los operadores de servicios esenciales designados conforme a lo previsto en la disposición adicional primera del Real Decreto-ley 12/2018, de 7 de septiembre, deberán comunicar a la autoridad competente respectiva la identidad del responsable de la seguridad de la información en el plazo de tres meses desde la entrada en vigor de este real decreto.

Disposición adicional segunda. Orientaciones para la gestión de incidentes y cumplimiento de las obligaciones de notificación.

El Consejo de Seguridad Nacional, a propuesta de su comité especializado en materia de ciberseguridad, y articuladas sus funciones como punto de contacto único a través del Departamento de Seguridad Nacional, podrá aprobar orientaciones en relación con la Instrucción Nacional de Notificación y Gestión de Incidentes recogida en el anexo, así como para la actualización de la Guía Nacional de Notificación y Gestión de Ciberincidentes, que incluyan directrices y recomendaciones para el cumplimiento de las obligaciones de notificación previstas en este real decreto, así como en el Real Decreto-ley 12/2018, de 7 de septiembre, con objeto de mejorar la coordinación y optimizar los recursos dedicados a la gestión de los incidentes que afecten a la seguridad de las redes y sistemas de información.

Disposición adicional tercera. Régimen específico del Banco de España.

Las disposiciones del presente real decreto se entenderán sin perjuicio de las competencias y funciones atribuidas al Banco de España, al Banco Central Europeo y al Sistema Europeo de Bancos Centrales, de conformidad con el Tratado de Funcionamiento de la Unión Europea, los Estatutos del Sistema Europeo de Bancos Centrales y del Banco Central Europeo, Reglamento (UE) n.º 1024/2013 del Consejo, de 15 de octubre de 2013, que encomienda al Banco Central Europeo tareas específicas respecto de políticas relacionadas con la supervisión prudencial de las entidades de crédito, y la Ley 13/1994, de 1 de junio, de Autonomía del Banco de España.

En lo no previsto en su normativa específica, y en cuanto sea compatible con su naturaleza, funciones e independencia, será de aplicación al Banco de España lo previsto en este real decreto.

Disposición adicional cuarta. Supuesto de dependencia de proveedores externos.

En referencia al artículo 19.3 del Real Decreto-ley 12/2018, de 7 de septiembre, cuando los operadores de servicios esenciales o proveedores de servicios digitales dependan de proveedores externos a los que les sea de aplicación la disposición adicional novena de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, el Equipo de Respuesta ante Emergencias Informáticas (CERT) competente del proveedor externo se corresponderá con:

a) El CCN-CERT, del Centro Criptológico Nacional, cuando el proveedor esté incluido en el ámbito subjetivo de aplicación de la Ley 40/2015, de 1 de octubre.

b) El INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, en el resto de los casos.

Disposición adicional quinta. Tratamientos de datos de carácter personal.

Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a su libre circulación; en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y, en su caso, en la normativa sobre protección de datos personales especial o específica que resulte de aplicación.

Disposición adicional sexta. Información sobre incidentes en el sistema financiero.

Los CSIRT de referencia informarán al titular de la Secretaría de Estado de Economía y Apoyo a la Empresa, a través de la Secretaría General del Tesoro y Financiación Internacional, de los incidentes que puedan tener efectos perturbadores significativos en los servicios esenciales del sistema financiero. A estos efectos, se entenderá que tienen efectos perturbadores significativos cuando su umbral o nivel de impacto sea crítico, muy alto o alto, según lo señalado en el anexo de este real decreto.

Disposición transitoria única. Desempeño transitorio de funciones en el sector energético.

La Secretaría de Estado de Seguridad del Ministerio del Interior, a través de la Oficina de Coordinación de Ciberseguridad (OCC), desempeñará temporalmente las funciones atribuidas por este real decreto al departamento ministerial con competencias en materia de energía, hasta que este disponga de los recursos humanos necesarios con la formación adecuada para ejercer estas competencias de forma efectiva según lo previsto en el artículo 3 y, en todo caso, en un plazo máximo de 12 meses.

Disposición final primera. Título competencial.

Este real decreto se dicta al amparo de lo previsto en el artículo 149.1.21.ª y 29.ª de la Constitución, que atribuye al Estado competencia exclusiva en materia de régimen general de telecomunicaciones y seguridad pública, respectivamente.

Disposición final segunda. Habilitación para el desarrollo normativo y aplicación.

Se faculta a los titulares de los Ministerios de Asuntos Económicos y Transformación Digital, Interior y Defensa, así como a los titulares de los Ministerios y organismos relacionados en el artículo 3, para dictar conjunta o separadamente, según las materias de que se trate, y en el ámbito de sus respectivas competencias, las disposiciones que exijan el desarrollo y aplicación de este real decreto.

Disposición final tercera. Entrada en vigor.

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

Dado en Madrid, el 26 de enero de 2021.

FELIPE R.

La Vicepresidenta Primera del Gobierno y Ministra de la Presidencia, Relaciones con las Cortes y Memoria Democrática,

CARMEN CALVO POYATO

ANEXO

Instrucción nacional de notificación y gestión de ciberincidentes

1. Obligatoriedad de notificación

Los incidentes se asociarán a uno de los niveles de peligrosidad e impacto establecidos en esta instrucción, teniendo en cuenta la obligatoriedad de notificación de todos aquellos que se categoricen con un nivel CRÍTICO, MUY ALTO o ALTO para todos aquellos sujetos obligados a los que les sea aplicable esta «Instrucción nacional de notificación y gestión de ciberincidentes». En ese caso, los sujetos obligados deberán comunicar, en tiempo y forma, los incidentes que registren en sus redes y sistemas de información y que estén obligados a notificar por superar los umbrales de impacto o peligrosidad establecidos en esta instrucción.

Para la notificación de los incidentes de ciberseguridad se utilizará como criterio de referencia el nivel de peligrosidad que se asigne a un incidente, sin perjuicio de que a lo largo del desarrollo, mitigación o resolución del mismo, se categorice con un determinado nivel de impacto que haga aconsejable la comunicación del incidente a la autoridad competente o CSIRT de referencia.

En todo caso, cuando un determinado suceso pueda asociarse a más de un tipo de incidente debido a sus características potenciales, este se asociará a aquel que tenga un nivel de peligrosidad superior de acuerdo a los criterios expuestos en esta Instrucción.

2. Clasificación/taxonomía de los ciberincidentes

La siguiente Clasificación/Taxonomía de los ciberincidentes está alineada con la taxonomía aprobada por la Agencia de la Unión Europea para la Ciberseguridad (ENISA).

Esta Clasificación/Taxonomía de los ciberincidentes se empleará para la asignación de una clasificación específica a un incidente registrado en las redes y sistemas de información cuando se realice la comunicación a la autoridad competente o CSIRT de referencia.

Tabla 1. Clasificación/Taxonomía de los ciberincidentes

Clasificación

Tipo de incidente

Descripción y ejemplos prácticos

Contenido abusivo.

Spam.

Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.

Delitos de odio, contra la libertad o el honor.

Contenido difamatorio o discriminatorio.

Ej.: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.

Pornografía infantil, contenido sexual o violento inadecuado.

Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.

Contenido dañino.

Sistema infectado.

Sistema infectado con malware. Ej.: sistema, computadora o teléfono móvil infectado con un rootkit.

Servidor C&C (Mando y Control).

Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.

Distribución de malware.

Recurso usado para distribución de malware. Ej.: recurso de una organización empleado para distribuir malware.

Configuración de malware.

Recurso que aloje ficheros de configuración de malware Ej.: ataque de webinjects para troyano.

Obtención de información.

Escaneo de redes (scanning).

Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej.: peticiones DNS, ICMP, SMTP, escaneo de puertos.

Análisis de paquetes (sniffing).

Observación y grabación del tráfico de redes.

Ingeniería social.

Recopilación de información personal sin el uso de la tecnología. Ej.: mentiras, trucos, sobornos, amenazas.

Intento de intrusión.

Explotación de vulnerabilidades conocidas.

Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej.: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).

Intento de acceso con vulneración de credenciales.

Múltiples intentos de vulnerar credenciales. Ej.: intentos de ruptura de contraseñas, ataque por fuerza bruta.

Ataque desconocido.

Ataque empleando exploit desconocido.

Intrusión.

Compromiso de cuenta con privilegios.

Compromiso de un sistema en el que el atacante ha adquirido privilegios.

Compromiso de cuenta sin privilegios.

Compromiso de un sistema empleando cuentas sin privilegios.

Compromiso de aplicaciones.

Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej.: inyección SQL.

Robo.

Intrusión física. Ej.: acceso no autorizado a Centro de Proceso de Datos.

Disponibilidad.

DoS (Denegación de servicio).

Ataque de denegación de servicio. Ej.: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.

DDoS (Denegación distribuida de servicio).

Ataque de denegación distribuida de servicio. Ej.: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

Mala configuración.

Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej.: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.

Sabotaje.

Sabotaje físico. Ej.: cortes de cableados de equipos o incendios provocados.

Interrupciones.

Interrupciones por causas ajenas. Ej.: desastre natural.

Compromiso de la información.

Acceso no autorizado a información.

Acceso no autorizado a información. Ej.: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.

Modificación no autorizada de información.

Modificación no autorizada de información. Ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.

Pérdida de datos.

Pérdida de información Ej.: pérdida por fallo de disco duro o robo físico.

Fraude.

Uso no autorizado de recursos.

Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej.: uso de correo electrónico para participar en estafas piramidales.

Derechos de autor.

Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej.: Warez.

Suplantación.

Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

Phishing.

Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

Vulnerabilidad.

Criptografía débil.

Servicios accesibles públicamente que puedan presentar criptografía débil. Ej.: servidores web susceptibles de ataques POODLE/FREAK.

Amplificador DDoS.

Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej.: DNS open-resolvers o Servidores NTP con monitorización monlist.

Servicios con acceso potencial no deseado.

Ej.: Telnet, RDP o VNC.

Revelación de información.

Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej.: SNMP o Redis.

Sistema vulnerable.

Sistema vulnerable. Ej.: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

Otros.

Otros.

Todo aquel incidente que no tenga cabida en ninguna categoría anterior.

APT.

Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

3. Nivel de peligrosidad del ciberincidente

El indicador de peligrosidad determina la potencial amenaza que supondría la materialización de un incidente en los sistemas de información o comunicación del ente afectado, así como para los servicios prestados o la continuidad de negocio en caso de haberla. Este indicador se fundamenta en las características intrínsecas a la tipología de amenaza y su comportamiento.

Los incidentes se asociarán a alguno de los siguientes niveles de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO.

Nivel crítico:

– APT.

Nivel muy alto:

– Distribución de malware.

– Configuración de malware.

– Robo.

– Sabotaje.

– Interrupciones.

Nivel alto:

– Pornografía infantil, contenido sexual o violento inadecuado.

– Sistema infectado.

– Servidor C&C (Mando y Control).

– Compromiso de aplicaciones.

– Compromiso de cuentas con privilegios.

– Ataque desconocido.

– DoS (Denegación de servicio).

– DDoS (Denegación distribuida de servicio).

– Acceso no autorizado a información.

– Modificación no autorizada de información.

– Pérdida de datos.

– Phishing.

Nivel medio:

– Discurso de odio.

– Ingeniería social.

– Explotación de vulnerabilidades conocidas.

– Intento de acceso con vulneración de credenciales.

– Compromiso de cuentas sin privilegios.

– Desconfiguración.

– Uso no autorizado de recursos.

– Derechos de autor.

– Suplantación.

– Criptografía débil.

– Amplificador DDoS.

– Servicios con acceso potencial no deseado.

– Revelación de información.

– Sistema vulnerable.

Nivel bajo:

– Spam.

– Escaneo de redes (scanning).

– Análisis de paquetes (sniffing).

– Otros.

4. Nivel de impacto del ciberincidente

El indicador de impacto de un ciberincidente se determinará evaluando las consecuencias que tal ciberincidente ha tenido en las funciones y actividades de la organización afectada, en sus activos o en los individuos afectados. De acuerdo a ello, se tienen en cuenta aspectos como las consecuencias potenciales o materializadas que provoca una determinada amenaza en un sistema de información y/o comunicación, así como en la propia entidad afectada (organismos públicos o privados, y particulares).

Los criterios empleados para la determinación del nivel de impacto asociado a un ciberincidente atienden a los siguientes parámetros:

– Impacto en la Seguridad Nacional o en la seguridad ciudadana.

– Efectos en la prestación de un servicio esencial o en una infraestructura crítica.

– Tipología de la información o sistemas afectados.

– Grado de afectación a las instalaciones de la organización.

– Posible interrupción en la prestación del servicio normal de la organización.

– Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.

– Pérdidas económicas.

– Extensión geográfica afectada.

– Daños reputacionales asociados.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO, SIN IMPACTO.

Nivel crítico:

– Afecta apreciablemente a la Seguridad Nacional.

– Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.

– Afecta a una infraestructura crítica.

– Afecta a sistemas clasificados SECRETO.

– Afecta a más del 90 % de los sistemas de la organización.

– Interrupción en la prestación del servicio superior a 24 horas y superior al 50 % de los usuarios.

– El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.

– Impacto económico superior al 0,1 % del Producto Interior Bruto (PIB) actual.

– Extensión geográfica supranacional.

– Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.

Nivel muy alto:

– Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.

– Afecta apreciablemente a actividades oficiales o misiones en el extranjero.

– Afecta a un servicio esencial.

– Afecta a sistemas clasificados RESERVADO.

– Afecta a más del 75 % de los sistemas de la organización.

– Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios.

– El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.

– Impacto económico entre el 0,07 % y el 0,1 % del PIB actual.

– Extensión geográfica superior a 4 Comunidades Autónomas (CC.AA.) o un territorio de Interés Singular (TIS, se considera como tal a las ciudades de Ceuta y Melilla y a cada una de las islas que forman los archipiélagos de las islas Baleares y las islas Canarias).

– Daños reputacionales a la imagen del país (marca España).

– Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

Nivel alto:

– Afecta a más del 50 % de los sistemas de la organización.

– Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios.

– El ciberincidente precisa para resolverse entre 5 y 30 Jornadas-Persona.

– Impacto económico entre el 0,03 % y el 0,07 % del PIB actual.

– Extensión geográfica superior a 3 CC.AA.

– Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.

Nivel medio:

– Afecta a más del 20 % de los sistemas de la organización.

– Interrupción en la presentación del servicio superior al 5 % de usuarios.

– El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.

– Impacto económico entre el 0,001 % y el 0,03 % del PIB actual.

– Extensión geográfica superior a 2 CC.AA.

– Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).

Nivel bajo:

– Afecta a los sistemas de la organización.

– Interrupción de la prestación de un servicio.

– El ciberincidente precisa para resolverse menos de 1 Jornada-Persona.

– Impacto económico entre el 0,0001 % y el 0,001 % del PIB actual.

– Extensión geográfica superior a 1 CC.AA.

– Daños reputacionales puntuales, sin eco mediático.

Sin impacto:

– No hay ningún impacto apreciable.

5. Información a notificar a la autoridad competente en caso de incidente

El sujeto obligado comunicará, en la notificación inicial, todos aquellos campos acerca de los que tenga conocimiento en ese momento de acuerdo a la siguiente tabla, siendo posteriormente preceptiva la cumplimentación de todos los campos de la tabla en la notificación final del incidente.

Tabla 2. Información a notificar a la autoridad competente en caso de incidente

Qué notificar

Descripción

Asunto.

Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.

OSE/PSD.

Denominación del operador de servicios esenciales o proveedor de servicios digitales que notifica.

Sector estratégico.

Energía, transporte, financiero, etc.

Fecha y hora del incidente.

Indicar con la mayor precisión posible cuándo ha ocurrido el ciberincidente.

Fecha y hora de detección del incidente.

Indicar con la mayor precisión posible cuándo se ha detectado el ciberincidente.

Descripción.

Describir con detalle lo sucedido.

Recursos tecnológicos afectados.

Indicar la información técnica sobre el número y tipo de activos afectados por el ciberincidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones....

Origen del incidente.

Indicar la causa del incidente si se conoce. Apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etc.

Taxonomía (clasificación).

Posible clasificación y tipo de ciberincidente en función de la taxonomía descrita.

Nivel de peligrosidad.

Especificar el nivel de peligrosidad asignado a la amenaza.

Nivel de impacto.

Especificar el nivel de impacto asignado al incidente.

Impacto transfronterizo.

Indicar si el incidente tiene impacto transfronterizo en algún Estado miembro de la Unión Europea.

Plan de acción y contramedidas.

Actuaciones realizadas hasta el momento en relación al ciberincidente. Indicar el Plan de acción seguido junto con las contramedidas implantadas.

Afectación.

Indicar si el afectado es una empresa o un particular, y las afectaciones según el nivel de impacto asignado.

Medios necesarios para la resolución (J-P).

Capacidad empleada en la resolución del incidente en Jornadas-Persona.

Impacto económico estimado (Si se conoce).

Costes asociados al incidente, tanto de carácter directo como indirecto.

Extensión geográfica (Si se conoce).

Local, autonómico, nacional, supranacional, etc.

Daños reputacionales (Si se conocen).

Afectación a la imagen corporativa del operador.

Adjuntos.

Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.).

Regulación afectada.

ENS / RGPD / NIS / PIC / Otros.

Se requiere actuación de FFCCSE.

Si / No.

6. Ventana temporal de reporte

Todos aquellos sujetos obligados que se vean afectados por un incidente de obligada notificación a la autoridad competente, a través del CSIRT de referencia, remitirán, en tiempo y forma, aquellas notificaciones inicial, intermedia y final requeridas de acuerdo a la siguiente ventana temporal de reporte.

– La notificación inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.

– La notificación intermedia es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.

– La notificación final es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

No obstante lo anterior, se aportarán todas aquellas notificaciones adicionales intermedias o posteriores que se consideren necesarias.

Tabla 3. Ventana temporal de reporte

Nivel de peligrosidad o impacto

Notificación inicial

Notificación intermedia

Notificación final

CRÍTICO.

Inmediata.

24/48 horas.

20 días.

MUY ALTO.

Inmediata.

72 horas.

40 días.

ALTO.

Inmediata.

–

–

MEDIO.

–

–

–

BAJO.

–

–

–

Los tiempos reflejados en la tabla 3 para la «notificación intermedia» y la «notificación final» tienen como referencia el momento de remisión de la «notificación inicial». La «notificación inicial» tiene como referencia de tiempo el momento de tener conocimiento del incidente.

7. Definiciones y conceptos

La descripción de las conductas aquí incluidas tiene carácter técnico y se entiende a los meros efectos de la notificación y gestión de ciberincidentes. Como tal, es independiente tanto de la calificación de los hechos, como de la aplicación por

parte de la autoridad judicial de los tipos penales establecidos en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

Contenido abusivo:

– Correo masivo no solicitado (spam): correo electrónico no solicitado que se envía a un gran número de usuarios, o bien una alta tasa de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.

– Acoso: referido a acoso virtual o ciberacoso, se trata del uso de medios de comunicación digitales para acosar a una persona, o grupo de personas, mediante ataques personales, divulgación de información privada o íntima, o falsa.

– Extorsión: obligar a una persona o mercantil, mediante el empleo de violencia o intimidación, a realizar u omitir actos con la intención de producir un perjuicio a esta, o bien con ánimo de lucro de la que lo provoca.

– Mensajes ofensivos: comunicaciones no esperadas o deseadas, así como acciones o expresiones que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación.

– Delito: cualquier acción tipificada como delito de acuerdo a lo establecido en la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

– Pederastia: cualquier comportamiento relacionado con los descritos en el título VIII la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, relativos a la captación o utilización de menores de edad o personas con discapacidad necesitadas de especial protección en actos que atenten contra su indemnidad o libertad sexual.

– Racismo: cualquier infracción penal, incluyendo infracciones contra las personas o las propiedades, donde la víctima, el local o el objetivo de la infracción se elija por su real o percibida, conexión, simpatía, filiación, apoyo o pertenencia a un grupo social, raza, religión o condición sexual.

– Apología de la violencia: exposición, ante una concurrencia de personas o por cualquier medio de difusión, de ideas o doctrinas que ensalcen el crimen o enaltezcan a su autor.

Contenido dañino:

– Malware (código dañino): palabra que deriva de los términos malicious y software. Cualquier pieza de software que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como malware. Así pues malware es un término que engloba varios tipos de programas dañinos.

– Virus: tipo de malware cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina, adquiriendo la capacidad de replicarse de un sistema a otro. Los métodos más comunes de infección se dan a través de dispositivos extraíbles, descargas de Internet y archivos adjuntos en correos electrónicos. No obstante también puede hacerlo a través de scripts, documentos, y vulnerabilidades XSS presentes en la web. Es reseñable que un virus requiere la acción humana para su propagación a diferencia de otro malware, véase Gusano.

– Gusano: programa malicioso que tiene como característica principal su alto grado de dispersabilidad. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.

– Troyano: tipo de malware que se enmascara como software legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el software dañino tiene la capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no depende una acción humana y no tiene la capacidad de replicarse, no obstante puede tener gran capacidad dañina en un sistema a modo de troyanos o explotando vulnerabilidades de software.

– Programa espía (spyware): tipo de malware que espía las actividades de un usuario sin su conocimiento o consentimiento. Estas actividades pueden incluir keyloggers, monitorizaciones, recolección de datos así como robo de datos. Los spyware se pueden difundir como un troyano o mediante explotación de software.

– Rootkit: conjunto de software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. Denotar que por maquina se entiende todo el espectro de sistemas IT, desde smartphones hasta ICS. El propósito por tanto de un rootkit es enmascarar eficazmente payloads y permitir su existencia en el sistema.

– Dialer: tipología de malware que se instala en una máquina y, de forma automática y sin consentimiento del usuario, realiza marcaciones telefónicas a número de tarificación especial. Estas acciones conllevan costes económicos en la víctima al repercutir el importe de la comunicación.

– Ransomware: se engloba bajo este epígrafe a aquel malware que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. Normalmente la víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.

– Bot dañino: una botnet es el nombre que se emplea para designar a un conjunto de máquinas controladas remotamente con finalidad generalmente maliciosa. Un bot es una pieza de software maliciosa que recibe órdenes de un atacante principal que controla remotamente la máquina. Los servidores C&C habilitan al atacante para controlar los bots y que ejecuten las órdenes dictadas remotamente.

– RAT: del inglés Remote Access Tool, se trata de una funcionalidad específica de control remoto de un sistema de información, que incorporan determinadas familias o muestras de software dañino (malware).

– C&C: del inglés Command and Control, se refiere a paneles de mando y control (también referenciados como C2), por el cual atacantes cibernéticos controlan determinados equipos zombie infectados con muestras de la misma familia de software dañino. El panel de comando y control actúa como punto de referencia, control y gestión de los equipos infectados.

– Conexión sospechosa: todo intercambio de información a nivel de red local o pública, cuyo origen o destino no esté plenamente identificado, así como la legitimidad de los mismos.

Obtención de información:

– Escaneo de puertos (Scanning): análisis local o remoto mediante software, del estado de los puertos de una máquina conectada a una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

– Escaneo de red (Scanning): análisis local o remoto mediante software, del estado de una red. La finalidad de esta acción es la de obtener información relativa a la identificación de los servicios activos y las posibles vulnerabilidades que puedan existir en la red.

– Escaneo de tecnologías: análisis local o remoto mediante software, de las tecnologías presentes o disponibles en una red determinada o un sistema de información concreto, mediante el cual se obtienen las referencias del hardware/software presente, así como su versión, y potenciales vulnerabilidades.

– Transferencia de zona DNS (AXFR IXFR): transacción de los servidores DNS utilizada para la replicación de las bases de datos entre un servidor primario y los secundarios. Estas transacciones pueden ser completas (AXFR) o incrementales (IXFR).

– Análisis de paquetes (Sniffing): análisis mediante software del tráfico de una red con la finalidad de capturar información. El tráfico que viaje no cifrado podrá ser capturado y leído por un atacante.

– Ingeniería social: técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.

– Phishing: estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta empleando métodos de ingeniería social.

– Spear Phishing: variante del phishing mediante la que el atacante focaliza su actuación sobre un objetivo concreto.

Intrusiones:

– Explotación: cualquier práctica mediante la cual un atacante cibernético vulnera un sistema de información y/o comunicación, con fines ilícitos o para los cuales no está debidamente autorizado.

– Inyección SQL: tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.

– Cross Site Scripting XSS (Directo o Indirecto): ataque que trata de explotar una vulnerabilidad presente en aplicaciones web, por la cual un atacante inyecta sentencias mal formadas o cadenas que el receptor no espera o controla debidamente.

– Cross Site Request Forgery (CSFR): falsificación de petición en sitios cruzados. Es un tipo de exploit dañino de un sitio web en el que comandos no autorizados son transmitidos por un usuario en el cual el sitio web confía. Esta vulnerabilidad es conocida también por otros nombres como XSRF, enlace hostil, ataque de un clic, cabalgamiento de sesión, y ataque automático. Al contrario que en los ataques XSS, los cuales explotan la confianza que un usuario tiene en un sitio en particular, el Cross Site Request Forgery explota la confianza que un sitio tiene en un usuario en particular.

– Defacement: tipología de ataque a sitios web en el que se implementa un cambio en la apariencia visual de la página. Para ello suelen emplearse técnicas como inyecciones SQL o algún tipo de vulnerabilidad existente en la página o en el servidor.

– Inclusión de ficheros (RFI y LFI): vulnerabilidad que permite a un atacante mostrar o ejecutar archivos remotos alojados en otros servidores a causa de una mala programación de la página que contiene funciones de inclusión de archivos. La

inclusión local de archivos (LFI) es similar a la vulnerabilidad de Inclusión de archivos remotos, excepto que en lugar de incluir archivos remotos solo se pueden incluir archivos locales, es decir, archivos en el servidor actual para su ejecución.

– Evasión de sistemas de control: proceso por el cual una muestra de software dañino, o un conjunto de acciones orquestadas por un atacante cibernético, consiguen vulnerar o esquivar los sistemas o políticas de seguridad establecidas por un determinado sistema de información y comunicación.

– Pharming: ataque informático que aprovecha vulnerabilidades de los servidores DNS (Domain Name System). Al tratar de acceder el usuario al sitio web, el navegador redirigirá automáticamente al usuario a una dirección IP donde se aloja una web maliciosa que suplanta la auténtica, y en la que el atacante podrá obtener información sensible de los usuarios.

– Ataque por fuerza bruta: proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de todas las combinaciones posibles, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

– Ataque por diccionario: proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de un diccionario previamente generado con determinadas combinaciones de caracteres, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.

– Robo de credenciales de acceso: acceso o sustracción no autorizada a credenciales de acceso a sistemas de información y/o comunicación.

Disponibilidad:

– DoS (Denial of Service) o ataque de denegación de servicio: conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él. El ataque consiste en saturar con peticiones de servicio al servidor, hasta que este no puede atenderlas, provocando su colapso.

– DDoS (Distributed Denial of Service) o denegación distribuida de servicio: variante de DoS en el que la remisión de peticiones se lleva a cabo de forma coordinada desde varios puntos hacia un mismo destino. Para ello se emplean redes de bots, generalmente sin el conocimiento de los usuarios.

– Mala configuración: fallo de configuración en el software que está directamente asociado con una pérdida de disponibilidad de un servicio.

– Sabotaje/Terrorismo/Vandalismo: ataques implementados con el objetivo de provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputacionales relevantes cometidos con propósitos ideológicos, políticos o religiosos.

– Disrupción sin intención dañina: acciones que pueden provocar la interrupción o degradación de la prestación de un servicio, provocando daños relevantes en la continuidad del servicio de una institución o daños reputaciones relevantes.

– Inundación SYN o UDP: procedimientos usados para la realización de ataque DoS o DDoS consistente en iniciar una gran cantidad de sesiones impidiendo al servidor atender las peticiones licitas.

– DNS Open-Resolver: servidor DNS capaz resolver consultas DNS recursivas procedentes de cualquier origen de Internet. Este tipo de servidores suele emplearse por usuarios malintencionados para la realización de ataques DDoS.

Compromiso de la información:

– Acceso no autorizado a la información o ciberespionaje: proceso por el cual un usuario no autorizado accede a consultar contenido para el cual no está autorizado.

– Modificación no autorizada de información: proceso por el cual un usuario no autorizado accede a modificar contenido para el cual no está autorizado.

– Borrado no autorizado de información: proceso por el cual un usuario no autorizado accede a borrar contenido para el cual no está autorizado.

– Exfiltración de información: proceso por el cual un usuario difunde información en canales o fuentes en las cuales no está prevista o autorizada la compartición de esa información.

– Acceso no autorizado a sistemas: proceso por el cual un usuario accede sin vulnerar ningún servicio, sistema o red, a sistemas de información y/o comunicación para los cuales no está debidamente autorizado, o no tiene autorización tácita o manifiesta.

– Ataque POODLE / Ataque FREAK: proceso por el que se consigue que un servidor haga uso de un protocolo de comunicaciones no seguro, que originalmente no estaba previsto, con el objetivo de poder exfiltrar información.

Fraude:

– Uso no autorizado de recursos: empleo de tecnologías y/o servicios por usuarios que no están debidamente autorizados por la Dirección o negociado competente.

– Suplantación de identidad: actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso.

– Derechos de propiedad intelectual: la propiedad intelectual es el conjunto de derechos que corresponden a los autores y a otros titulares (artistas, productores, organismos de radiodifusión...) respecto de las obras y prestaciones fruto de su creación.

– Otros fraudes: engaño económico con la intención de conseguir un beneficio, y con el cual alguien resulta perjudicado.

Vulnerabilidades:

– Tecnología vulnerable: conocimiento por parte de los administradores de tecnologías, servicios o redes, de vulnerabilidades presentes en estas.

– Política de seguridad precaria: política de seguridad de la organización deficiente, mediante la cual existe la posibilidad de que durante un espacio de tiempo determinado, atacantes cibernéticos realizaron accesos no autorizados a sistemas de información, no pudiendo determinar fehacientemente este extremo.

Otros:

– Ciberterrorismo: delitos informáticos previstos en los artículo 197 bis y ter y 264 a 264 quater de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal cuando dichos delitos se cometan con las finalidades previstas en el artículo 573.1 del mismo texto. Estas finalidades son:

• Subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas o de las estructuras económicas o sociales del Estado, u obligar a los poderes públicos a realizar un acto o a abstenerse de hacerlo.

• Alterar gravemente la paz pública.

• Desestabilizar gravemente el funcionamiento de una organización internacional.

• Provocar un estado de terror en la población o en una parte de ella.

– Daños informáticos PIC: delitos informáticos previstos en los artículos 264.2 3.º y 4.º de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, relacionadas con el borrado, dañado, alteración, supresión, o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una Infraestructura Crítica. Así como conductas graves relacionadas con los términos anteriores que afecten a la prestación de un servicio esencial.

– APT (Advanced Persistent Threat o Amenaza Persistente Avanzada)/AVT (Advanced Volatility Threat): ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

– Dominios DGA: procedimiento para generar de forma dinámica dominios donde se alojarán los servidores de Comando y Control, técnica usada en redes Botnet para dificultar su detención.

– Criptografía: técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca la clave mediante la cual ha sido cifrado.

– Proxy: ordenador, generalmente un servidor, intermedio usado en las comunicaciones entre otros dos equipos, siendo normalmente usado de manera trasparente para el usuario.

General:

– Ciberseguridad: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Ciberespacio: espacio virtual que engloba todos los sistemas TIC. El ciberespacio se apoya en la disponibilidad de Internet como red de redes, enriquecida con otras redes de transporte de datos.

– Redes y sistemas de información: se entiende por este concepto uno de los tres siguientes puntos:

• Las redes de comunicaciones electrónicas, tal y como vienen definidas en el número 31 del anexo II de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

• Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales.

• Los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados anteriormente para su funcionamiento, utilización, protección y mantenimiento.

– Seguridad en redes y sistemas de información: la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

– Operador de servicios esenciales: entidad pública o privada que se identifique considerando los factores establecidos en el artículo 6 del Real Decreto-ley 12/2018, de 7 de septiembre, que preste dichos servicios en alguno de los sectores estratégicos definidos en el anexo de la Ley 8/2011, de 28 de abril.

– Servicio digital: servicio de la sociedad de la información entendido en el sentido recogido en la letra a) del anexo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

– Proveedor de servicios digitales: persona jurídica que presta un servicio digital.

– Ciberincidente: todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.

– Gestión de ciberincidentes: todos los procedimientos seguidos para detectar, analizar y limitar un incidente y responder ante este.

– Ciberamenaza: amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de este.

– Taxonomía: clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.

– RGPD: Reglamento General de Protección de Datos, 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.

– OpenPGP: estándar basado en el programa PGP, del inglés Pretty Good Privacy, cuya finalidad es proteger la información mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

– Webinject: herramienta gratuita y de código abierto diseñada principalmente para automatizar la prueba de las aplicaciones y servicios web.

– Telnet: protocolo de red que permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

– RDP (Remote Desktop Protocol): protocolo propietario que permite la comunicación en la ejecución de una aplicación entre un terminal y un servidor.

– VNC (Virtual Network Computing): programa de software libre basado en una estructura cliente-servidor que permite observar remotamente las acciones del ordenador servidor a través de un ordenador cliente.

– SNMP (Simple Network Management Protocol): protocolo de red utilizado para el intercambio de mensajes para la administración de dispositivos en red.

– Redis: motor de base de datos en memoria, basado en el almacenamiento en tablas de hashes.

– ICMP (Internet Control Message Protocol): protocolo de control de mensajes de Internet.

– Copia de seguridad limpia: punto de restauración de un sistema de la que se tiene la seguridad de no estar comprometida.