REAL DECRETO XX/20XX POR EL QUE SE DESARROLLA EL REAL DECRETO-LEY 12/2018, DE 7 DE SEPTIEMBRE, DE SEGURIDAD DE LAS REDES Y SISTEMAS DE INFORMACIÓN

El Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, que transpone 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, habilita al Gobierno, en su disposición final tercera, para desarrollar reglamentariamente lo previsto en el mencionado Real Decreto-ley.

En cumplimiento de este mandato, con la finalidad de desarrollar y concretar los aspectos contemplados en el citado Real Decreto-ley, se aprueba el presente real decreto, que se estructura en cinco capítulos e incluye cuatro disposiciones adicionales, cuatro disposiciones finales y un anexo.

Con el citado objeto, este real decreto culmina la designación de autoridades competentes en materia de seguridad de las redes y sistemas de información prevista en el Real Decreto-ley 12/2018, identificando las correspondientes a los operadores de servicios esenciales que no tienen la consideración de operadores críticos ni se encuentran comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, atendiendo a los sectores estratégicos identificados en la Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

En segundo lugar, el real decreto desarrolla los supuestos de cooperación y coordinación entre los CSIRT de referencia, que se instrumentan a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes. En particular, se desarrollan las previsiones del Real Decreto-ley en aquellas situaciones en que se vean afectados operadores con incidencia en la Defensa Nacional, así como las actuaciones de coordinación previstas para los supuestos de especial gravedad que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, y la coordinación requerida cuando las actividades que desarrollen los CSIRT de referencia puedan afectar de algún modo a un operador crítico.

Con relación a la figura del punto de contacto único que consagra la Directiva (UE) 2016/1148, 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. Estas funciones del Consejo de Seguridad Nacional como punto de contacto único son adicionales a las funciones de coordinación de las actuaciones de las autoridades competentes atribuidas por el Real Decreto-ley.

Por otra parte, el real decreto desarrolla las previsiones del Real Decreto-ley 12/2018 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 este real decreto.

Por lo que se refiere a la notificación de incidentes, el real decreto 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 aquéllos, por referencia a los niveles de impacto y peligrosidad, según sea el caso, previstos en la Instrucción Nacional de Notificación y de Gestión de Incidentes 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, 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.

Por ultimo, en materia de supervisión de requisitos de seguridad, el real decreto desarrolla 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 supervision.

Esta disposición 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, conforme a los cuales deben actuar las Administraciones públicas en el ejercicio de la iniciativa legislativa, como son los principios de necesidad, eficacia, proporcionalidad, seguridad jurídica, transparencia y eficiencia.

Este real decreto se dicta en virtud de las competencias exclusivas atribuidas al Estado en materia de régimen general de telecomunicaciones y seguridad pública, por el artículo 149.1.21.ª y 29.ª de la Constitución.

En la elaboración de este real decreto, que ha sido fruto de un intenso diálogo y colaboración entre los distintos Departamentos Ministeriales y organismos afectados, se ha dado audiencia a las organizaciones representativas de los sectores afectados.

En su virtud, a propuesta conjunta de la Ministra de Economía y Empresa, el Ministro del Interior y la Ministra de Defensa, 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 reunion del día….

DISPONGO:

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto y ámbito de aplicación.*

1. El presente 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 particular, tiene por objeto:

a) establecer las autoridades competentes en materia de seguridad de las redes y sistemas de información de los operadores de servicios esenciales que no tienen la consideración de operadores críticos ni se encuentran comprendidos en el ámbito de aplicación de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

b) instrumentar la cooperación y coordinación de los CSIRT de referencia a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes, prevista en el artículo 11 de este real decreto.

c) señalar las funciones del punto de contacto único.

d) establecer las medidas necesarias para el cumplimiento de las obligaciones de seguridad de los operadores de servicios esenciales y de los proveedores de servicios digitales.

e) señalar las funciones del responsable de seguridad de la información de los operadores de servicios esenciales.

f) aprobar la Instrucción Nacional de Notificación y Gestión de Incidentes.

2. El ámbito de aplicación del presente real decreto es el previsto en el artículo 2 del Real Decreto-ley 12/2018, de 7 de septiembre.

Artículo 2. *Definiciones.*

1. A los efectos de este real decreto, se entenderán por autoridades competentes las autoridades previstas en el artículo 9 del Real Decreto-ley 12/2018, de 7 de septiembre, y el artículo 3 de este real decreto.

2. Al resto de los conceptos utilizados en este real decreto le serán de aplicación las definiciones previstas en el Real Decreto-ley 12/2018, de 7 de septiembre.

CAPÍTULO II

Marco estratégico e institucional

Artículo 3. *Autoridades competentes.*

1. Son autoridades competentes de los operadores de servicios esenciales que no sean operadores críticos a que se refiere el artículo 9.1.a) 2ª del Real Decreto-ley 12/2018, de 7 de septiembre:

a) Respecto al sector del transporte: el Ministerio de Fomento, a través de la Secretaría de Estado de Infraestructuras, Transporte y Vivienda.

b) Respecto al sector de la energía: el Ministerio para la Transición Ecológica, 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 Economía y Empresa, a través de la Secretaría de Estado para el Avance Digital.

d) Respecto al sector del sistema financiero:

   i. El Ministerio de Economía y Empresa, a través de la Secretaría de Estado de Economía y Apoyo a la Empresa, para las entidades aseguradoras.
   ii. El Banco de España, para los bancos y entidades de crédito.
   iii. La Comisión Nacional del Mercado de Valores, para las entidades que operan en los mercados de valores.

e) Respecto al sector del espacio: el Ministerio de Defensa, a través de la Secretaría General de Política 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, Innovación y Universidades, a través de la Secretaría de Estado de Universidades, Investigación, Desarrollo e Innovación.

h) Respecto al sector de la salud: el Ministerio de Sanidad, Consumo y Bienestar Social, a través de la Secretaría General de Sanidad y Consumo.

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

j) Respecto al sector de la alimentación:

   i. El Ministerio de Agricultura, Pesca y Alimentación, a través de la Secretaría General de Agricultura y Alimentación.
   ii. El Ministerio de Sanidad, Consumo y Bienestar Social, a través de la Secretaría General de Sanidad y Consumo.
   iii. El Ministerio de Industria, Comercio y Turismo, a través de la Secretaría de Estado de Comercio.

k) Respecto al sector de la industria nuclear:
   i. El Ministerio para la Transición Ecológica, a través de la Secretaría de Estado de Energía.
   ii. El Consejo de Seguridad Nuclear.

2. Sin perjuicio de lo establecido en el Capítulo IV en relación con la gestión de incidentes de ciberseguridad, las autoridades competentes podrán establecer, mediante orden ministerial, canales de comunicación oportunos con los operadores de servicios esenciales y con los proveedores de servicios digitales para la supervisión de requisitos que les sean aplicables en materia de seguridad y de notificación de incidentes.

Dichas órdenes ministeriales podrán, asimismo, contemplar protocolos de actuación para la coordinación con los CSIRT de referencia.

Artículo 4. *Cooperación y coordinación de los CSIRT de referencia.*

1. La cooperación entre los CSIRT de referencia se instrumentará a través de la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

2. A efectos de la cooperación prevista en el artículo 11.1.a.3º del Real Decreto-ley 12/2018, 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 operadores con incidencia en la Defensa Nacional será comunicada por la Comisión Nacional para la Protección de las Infraestructuras Críticas a los operadores de conformidad con lo previsto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. Siempre que sea posible, la notificación será simultánea a su designación. 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.

3. Los supuestos de especial gravedad a los que se refiere el primer párrafo del artículo 11.2 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, que podrá actuar a través de su Comisión Permanente, será inmediatamente informado y podrá desactivar la coordinación prevista en este artículo, que no afectará al proceso de notificación de incidentes de 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 Cibernética en los supuestos previstos en el segundo párrafo del artículo 11.2 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:
   i. La clasificación del incidente
   ii. La peligrosidad del incidente
   iii. El impacto del incidente
b) Confirmación de que el operador afectado ha cumplido, en su caso, con los plazos determinados por la ventana temporal de reporte para los operadores críticos, según lo establecido en el anexo.
c) Plan de acción del CSIRT para abordar la resolución técnica del incidente, si procede.

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

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

En estos casos, el ESPDEF-CERT deberá ser oportunamente informado de la evolución de la gestión del incidente.

Artículo 5. *Punto de contacto único.*

1. De acuerdo con el artículo 13 del Real Decreto-ley 12/2018, de 7 de septiembre, 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 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.

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, un informe 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 el punto anterior, y elaborará un informe anual resumido sobre las notificaciones recibidas, que remitirá al grupo de cooperación antes del 9 de agosto 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, 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 6.4.

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.

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 necesarias 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 servicios propios como si lo son de proveedores externos.

2. En el caso de los operadores de servicios esenciales, deberán aprobar una política 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.

Dicha política considerará, como mínimo, los siguientes aspectos:

a. Análisis y gestión de riesgos.

b. Catálogo de medidas de seguridad, organizativas, tecnológicas y físicas.

c. Gestión del personal y profesionalidad.

d. Adquisición de productos o servicios de seguridad.

e. Detección y gestión de incidentes.

f. Planes de recuperación y aseguramiento de la continuidad de las operaciones.

g. Mejora continua.

h. Interconexión de sistemas.

i. Registro de la actividad de los usuarios

3. Las medidas de seguridad que se adopten 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.

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 del sistema de información del operador.

4. Las medidas adoptadas podrán ser complementadas con otras, atendiendo a necesidades específicas. En particular, se complementarán con las que, en su caso, establezcan con carácter específico las autoridades competentes de conformidad con lo previsto en el apartado 4 del artículo 16 y el apartado 2 del artículo 32 del Real Decreto-ley 12/2018.

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 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.

Artículo 7. *Responsable de seguridad de la información.*

1. De conformidad con lo previsto en el apartado 3 del artículo 16 del Real Decreto-ley 12/2018, los operadores de servicios esenciales deberán designar un responsable de seguridad de la información que ejercerá las funciones de punto de contacto y coordinación técnica con la autoridad competente que le corresponda de conformidad con lo previsto en este real decreto.

2. Los operadores de servicios esenciales designarán y comunicarán a la autoridad competente respectiva la designación del Responsable de la Seguridad de la Información en el plazo de tres meses desde su designación como operador de servicios esenciales, así como los nombramientos y ceses que afecten a la designación del responsable de la seguridad de la información en el plazo de 30 días 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 las siguientes funciones:

a) Elaborar y proponer para aprobación por la organización 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 del presente real decreto.

b) Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.

c) Elaborar el documento de Declaración de Aplicabilidad de medidas de seguridad considerado en el artículo 6.

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

e) Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los 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.

f) Recibir, interpretar y aplicar 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.

h) Cualesquiera otras funciones que se determinen reglamentariamente

El Responsable de la Seguridad de la Información, para desarrollar estas funciones, se podrá apoyar en servicios prestados por terceros.

4. El Responsable de la Seguridad de la Información deberá cumplir 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, en particular la comunicación real y efectiva con alta dirección.

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

5. Siempre que concurran los requisitos de conocimiento, experiencia, e 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, Delegado de Protección de Datos o el Responsable de Seguridad del Esquema Nacional de Seguridad, de conformidad con lo dispuesto en la regulación de aplicación 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, tanto si se trata de redes y servicios propios como si lo son de 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 apartado primero del artículo 28 del Real Decreto-ley 12/2018, los operadores de servicios esenciales y los proveedores de servicios digitales podrán solicitar ayuda especializada del CSIRT de referencia para la gestión de los incidentes, debiendo en tales casos atender a las indicaciones que reciban de éste 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.

4. Asimismo, deberán considerar los incidentes que puedan afectar tanto a las redes y sistemas de información propios del operador como de proveedores externos que puedan interaccionar con aquellos, incluso si éstos son proveedores de servicios digitales sometidos a este real decreto.

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 la sección I.A de la Instrucción Nacional de Notificación y de Gestión de Incidentes, 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 aquéllos. A estos efectos, se considerarán los incidentes con un nivel de peligrosidad crítico, muy alto o alto, según el detalle que se especifica en la sección I.B 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, obligaciones específicas de notificación que contemplen niveles diferentes a los previstos en la Instrucción Nacional de Notificación y de Gestión de Incidentes, así como factores y umbrales sectoriales específicos, aplicables a los operadores sometidos a su supervisión.

Artículo 10. *Procedimientos de notificación de incidentes.*

1. Los operadores de servicios esenciales y los proveedores de servicios digitales dirigirán las notificaciones de incidentes a la autoridad competente, a través del CSIRT de referencia, empleando los canales contemplados en la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

Los CSIRT de referencia garantizarán un intercambio fluido de información con las autoridades competentes que correspondan, asegurando el adecuado seguimiento en la gestión de los incidentes 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 Seguridad de la Información se coordinará a estos efectos con el Responsable de Seguridad y Enlace previsto en el artículo 17 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 éste no esté resuelto, y se realizarán una notificación final del incidente tras su resolución, informando del detalle de la evolución del suceso la valoración de la probabilidad de repetición del suceso, y las medidas correctoras que eventualmente tiene previsto adoptar el operador.

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

5. 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.

La autoridad competente valorará asimismo conjuntamente, con los 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.

6. Lo establecido en los apartados anteriores será de aplicación a los proveedores de servicios digitales en tanto que no se adopte el acto de ejecución previsto 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.

Artículo 11. *Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.*

1. El CCN-CERT en colaboración con el INCIBE-CERT y el ESPDEF-CERT pondrá a disposición de todos los actores involucrados la plataforma Nacional de Notificación y Seguimiento de Ciberincidentes.

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 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 confidencialidad, integridad y disponibilidad 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.

4. La plataforma dispondrá asimismo de diversos canales de comunicación para su uso por parte de las autoridades competentes y los CSIRT de referencia.

5. Asimismo, la plataforma implementará el procedimiento de notificación y gestión de incidentes que estará disponible en modalidad 24x7, y dispondrá como mínimo de las siguientes capacidades:

a) Capacidad de gestión de ciberincidentes con incorporación de taxonomía, criticidad, inclusión de autoridades subordinadas, notificaciones a terceros y métricas de eficiencia en su resolución, 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. *Actuaciones ante incidentes con carácter presuntamente delictivo.*

1. En el caso de que los incidentes de ciberseguridad revistan caracteres de delito, la Oficina de Coordinación Cibernética del CNPIC comunicará al Ministerio Fiscal y a la Policía Judicial, a la mayor brevedad posible y en cumplimiento de lo dispuesto en el art 262 de la Ley de Enjuiciamiento Criminal, aquellos incidentes de seguridad que les sean notificados y que revistan caracteres de delito, trasladando al tiempo la información que posean 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.

2. Las consultas que se prevén en el artículo 14.1 del Real Decreto-ley 12/2018 en materia de seguridad pública y seguridad ciudadana, se realizarán a través de la Oficina de Coordinación Cibernética.

Artículo 13. *Información sobre incidentes.*

1. Cuando las circunstancias lo permitan, los CSIRT de referencia proporcionarán a los operadores de servicios esenciales y a los prestadores 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, en las condiciones establecidas en el artículo 15 del Real Decreto-ley 12/2018, de 7 de septiembre.

CAPÍTULO V

Supervisión

Artículo 14. *Supervisión de los requisitos de seguridad.*

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 y el presente real decreto.

Los operadores de servicios esenciales y los proveedores de servicios digitales colaborarán con la autoridad competente en dicha supervisión, facilitando las inspecciones, proporcionándoles 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.

2. Los CSIRT de referencia colaborarán con las autoridades competentes, cuando éstas 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 prestadores de servicios digitales en virtud del artículo 6 de este real decreto.

Cuando se trate de operadores con incidencia en la Defensa Nacional a que se refiere el artículo 4.2 de este real decreto, la supervisión por la autoridad competente se desarrollará en colaboración el ESPDEF-CERT.

3. 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. *Referencias a las autoridades competentes.*

Las referencias a los Ministerios, órganos y entidades previstos en el artículo 3 de este real decreto se entenderán realizadas a aquellos que en un futuro les pudieran sustituir o asumir sus competencias.

Disposición adicional segunda. *Identificación de servicios esenciales y de operadores de servicios esenciales.*

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 al efecto en el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

Disposición adicional tercera. *Designación del responsable de 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 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 cuarta. *Orientaciones para la gestión de incidentes y cumplimiento de las obligaciones de notificación.*

El Consejo de Seguridad Nacional podrá adoptar, bajo la coordinación del Departamento de Seguridad Nacional, orientaciones en relación con la Instrucción Nacional de Notificación y Gestión de Incidentes contenida en el anexo, que incluyan directrices y recomendaciones para el cumplimiento de las obligaciones de notificación previstas en este real decreto, así como de las previstas en otras disposiciones para sectores específicos, 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 final primera. *Habilitación para el desarrollo normativo.*

Se faculta a los titulares de los Ministerios de Economía y Empresa, Interior y Defensa, así como a los titulares de los Ministerios 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 segunda. *Habilitación para la modificación del anexo.*

Se faculta al Consejo de Seguridad Nacional para la modificación del anexo, mediante acuerdo publicado por orden del Ministerio de la Presidencia.

Disposición final tercera. *Título competencial.*

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

Disposición final cuarta. *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 XX de XX de 2019.

ANEXO

INSTRUCCIÓN NACIONAL DE NOTIFICACIÓN Y DE GESTIÓN DE INCIDENTES

I. Detalle de los umbrales de impacto y peligrosidad para la notificación de incidentes por parte de los operadores de servicios esenciales con notificación obligatoria asociada

A. Umbrales o niveles de impacto

1. 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 ciber-incidente precisa para resolverse más de 30 Jornadas-Persona.
- Impacto económico superior al 0,1% del P.I.B. actual.
- Extensión geográfica supranacional.
- Daños reputacionales muy elevados y cobertura contínua en medios de comunicación internacionales.

2. 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 ciber-incidente precisa para resolverse entre 10 y 30 Jornadas-Persona.
- Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual.
- Extensión geográfica superior a 4 CC.AA. o 1 T.I.S.
- Daños reputacionales a la imagen del país (marca España).
- Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.

3. 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 ciber-incidente precisa para resolverse entre 5 y 10 Jornadas–Persona.
- Impacto económico entre el 0,03% y el 0,07% del P.I.B. 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.

B. Umbrales o niveles de peligrosidad

1. Nivel Crítico:

- APT
- Ciberterrorismo
- Daños informáticos PIC

2. Nivel Muy Alto:

- Distribución de malware
- Configuración de malware
- Ataque desconocido
- Robo
- Sabotaje
- Interrupciones

3. Nivel Alto:

- Pornografía infantil, contenido sexual o violento inadecuado
- Sistema infectado
- Servidor C&C (Mando y Control)
- Malware dominio DGA
- Compromiso de aplicaciones
- DoS (Denegación de servicio)
- DDoS (Denegación de servicio distribuida)
- Acceso no autorizado a información
- Modificación no autorizada de información
- Pérdida de datos
- Phishing

C. Definiciones y conceptos

- **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.
- **Ciberterrorismo**: Delitos informáticos previstos en los art. 197 bis y ter y 264 a 264 quater de la Ley Orgánica 10/1995 de 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 art 264.2 3º y 4º de la Ley Orgánica 10/1995 de 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.
- **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.
- **Servidor 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.
- **Malware 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.
- **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 éste 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.
- **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.

II. Información a notificar en caso de incidente

La entidad afectada por el ciberincidente aportará en su comunicación la siguiente información minima:

Información	Descripción
Asunto	Frase que describe de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
Descripción	Describir con detalle lo sucedido.
Afectado	Indicar si el afectado es una empresa o un particular
Fecha y hora del incidente (Indicando	Indicar con la mayor precisión posible

la zona horaria en formato UTC)	cuándo ha ocurrido el ciberincidente.
Fecha y hora de detección del incidente	Indicar con la mayor precisión posible cuándo se ha detectado el ciberincidente.
Taxonomía del incidente	Posible clasificación del ciberincidente en función de la taxonomía descrita a continuación. Se especificará: clasificación y tipo de incidente.
Recursos 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.
Contramedidas	Actuaciones realizadas para resolver el ciberincidente hasta el momento de la notificación a la autoridad competente o CSIRT de referencia.
Impacto	Impacto estimado en la entidad, en función del nivel de afectación del ciberincidente.
Adjuntos	Incluir documentos adjuntos que puedan aportar información que ayude 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

III. Taxonomía

La siguiente taxonomía 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 al CSIRT de referencia.

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.
	Delito de odio	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...

Código 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.
	Malware dominio DGA	Nombre de dominio generado mediante DGA (Algoritmo de Generación de Dominio), empleado por malware para contactar con un servidor de Mando y Control (C&C).
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.
	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.
Vulnerable	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.
	Ciberterrorismo	Uso de redes o sistemas de información con fines de carácter terrorista.
	Daños informáticos PIC	Borrado, dañado, alteración, supresión o inaccesibilidad de datos, programas informáticos o documentos electrónicos de una Infraestructura Crítica. Conductas graves relacionadas con los términos anteriores que afecten a la prestación de un Servicio Esencial.