I. DISPOSICIÓNS XERAIS

MINISTERIO DA PRESIDENCIA, RELACIÓNS COAS CORTES E MEMORIA DEMOCRÁTICA

1192 *Real decreto 43/2021, do 26 de xaneiro, polo que se desenvolve o Real decreto lei 12/2018, do 7 de setembro, de seguridade das redes e sistemas de información.*

No ámbito europeo, co obxectivo de dar unha resposta efectiva aos problemas de seguridade das redes e sistemas de información, aprobouse a Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, relativa ás medidas destinadas a garantir un elevado nivel común de seguridade das redes e sistemas de información na Unión, coñecida como Directiva NIS (*Security of Network and Information Systems*). Esta norma parte dun enfoque global da seguridade das redes e sistemas de información na Unión Europea e integra requisitos mínimos comúns en materia de desenvolvemento de capacidades e planificación, intercambio de información, cooperación e requisitos comúns de seguridade para os operadores de servizos esenciais e os provedores de servizos dixitais.

A transposición da citada Directiva NIS ao ordenamento xurídico español levouse a cabo mediante o Real decreto lei 12/2018, do 7 de setembro, de seguridade das redes e sistemas de información. Esta norma legal regula a seguridade das redes e sistemas de información utilizados para a provisión dos servizos esenciais e dos servizos dixitais establecendo mecanismos que, cunha perspectiva integral, permiten mellorar a protección fronte ás ameazas que afectan as redes e os sistemas de información, e fixando un marco institucional de cooperación que facilita a coordinación das actuacións realizadas nesta materia tanto a nivel nacional como cos países da nosa contorna, en particular dentro da Unión Europea.

O Real decreto lei 12/2018, do 7 de setembro, habilita o Goberno, na súa disposición derradeira terceira, para o seu desenvolvemento regulamentario. Con esa cobertura legal, e en cumprimento do citado mandato e do previsto nos seus artigos 9.1.a), 11.1.a), 11.2, 16.2, 16.3, 19.1 e 19.5, este real decreto ten por finalidade desenvolver o Real decreto lei 12/2018, do 7 de setembro, no relativo ao marco estratéxico e institucional de seguridade das redes e sistemas de información, ao cumprimento das obrigacións de seguridade dos operadores de servizos esenciais e dos provedores de servizos dixitais e á xestión de incidentes de seguridade.

O real decreto, no seu artigo 3, pormenoriza a designación de autoridades competentes en materia de seguridade das redes e sistemas de información prevista no artigo 9.1.a) 2.º do Real decreto lei 12/2018, do 7 de setembro. É oportuno mencionar, en relación coa seguridade no sector da alimentación, a participación da Axencia Española de Seguridade Alimentaria e Nutrición, dependente do Ministerio de Consumo. Adicionalmente, e de conformidade co artigo 11 do Real decreto lei 12/2018, do 7 de setembro, o real decreto desenvolve os supostos de cooperación e coordinación entre os equipos de resposta a incidentes de seguridade informática (CSIRT) de referencia, e destes coas autoridades competentes, que se instrumentan a través da Plataforma nacional de notificación e seguimento de ciberincidentes (artigo 4).

Con relación á figura do punto de contacto único (artigo 5) que consagra a Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, desenvólvense as súas funcións de enlace para garantir a cooperación transfronteiriza coas autoridades competentes doutros Estados membros da Unión Europea, así como co grupo de cooperación e coa rede de CSIRT.

Por outra banda, o artigo 6 deste real decreto desenvolve as previsións do artigo 16.2 do Real decreto lei 12/2018, do 7 de setembro, sobre as medidas necesarias para o

cumprimento das obrigacións de seguridade por parte dos operadores de servizos esenciais, que se deberán concretar nunha declaración de aplicabilidade de medidas de seguridade subscrita polo responsable de seguridade da información do operador, cuxas funcións tamén se desenvolven no artigo 7 deste real decreto. O prazo para a designación do responsable da seguridade establécese en cumprimento da habilitación recollida no artigo 16.3 do Real decreto lei 12/2018, do 7 de setembro.

Polo que se refire á notificación de incidentes, o real decreto, nos seus artigos 8 e 9, desenvolve as obrigacións de notificación por parte dos operadores de servizos esenciais dos incidentes que poidan ter efectos perturbadores significativos nos ditos servizos, así como dos incidentes que poidan afectar as redes e sistemas de información empregados para a prestación dos servizos esenciais mesmo cando non tivesen un efecto adverso real sobre aqueles, por referencia aos niveis de impacto e perigosidade, segundo sexa o caso, previstos na Instrución nacional de notificación e xestión de ciberincidentes que se contén no anexo.

O procedemento de notificación de incidentes articúlase a través da Plataforma nacional de notificación e seguimento de ciberincidentes (artigos 10 e 11), co fin de permitir o intercambio de información entre os operadores de servizos esenciais e provedores de servizos dixitais, as autoridades competentes e os CSIRT de referencia, garantindo a confidencialidade, integridade e dispoñibilidade da información (artigos 12 a 14).

Por último, en materia de supervisión de requisitos de seguridade, o real decreto desenvolve no seu artigo 15 a obrigación de colaboración dos operadores de servizos esenciais e dos provedores de servizos dixitais coas autoridades competentes, que poderán requirir, así mesmo, a colaboración dos CSIRT de referencia para o exercicio da súa función de supervisión.

Nas disposicións adicionais deste real decreto recóllese, entre outras materias, o réxime xurídico aplicable ao Banco de España tendo en conta a súa especial configuración xurídica como entidade de dereito público con personalidade xurídica propia e plena capacidade pública e privada que, no desenvolvemento da súa actividade e para o cumprimento dos seus fins, actúa con autonomía respecto á Administración xeral do Estado, e como parte integrante do Sistema europeo de bancos centrais (SEBC) e do Mecanismo único de supervisión (MUS). Esta especial configuración xurídica supón que o marco de seguridade das redes e sistemas de información resulte de aplicación na medida en que non interfira coa natureza, funcións e independencia do Banco de España.

Este real decreto adecúase aos principios de boa regulación establecidos no artigo 129 da Lei 39/2015, do 1 de outubro, do procedemento administrativo común das administracións públicas. Responde, en primeiro lugar, aos principios de necesidade e eficacia, en canto que a norma é necesaria para levar a cabo o desenvolvemento regulamentario do Real decreto lei 12/2018, do 7 de setembro, que traspón a Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016 e, en concreto, para establecer o marco estratéxico e institucional de seguridade das redes e sistemas de información, as obrigacións de seguridade e a xestión de incidentes, e é o instrumento máis idóneo para a consecución deste obxectivo. En segundo termo, a norma cumpre co principio de proporcionalidade, ao non existiren outras medidas menos gravosas para os operadores de servizos esenciais e provedores de servizos dixitais destinadas a cumprir a obrigación de adoptar medidas técnicas e de organización para xestionar os riscos para a seguridade das súas redes e dos seus sistemas de información, así como de notificar os incidentes que teñan efectos perturbadores significativos nos servizos que prestan. Así mesmo, este real decreto cumpre co principio de seguridade xurídica, pois o proxecto resulta conforme coa directiva europea de que deriva, así como coa Lei 8/2011, do 28 de abril, pola que se establecen medidas para a protección das infraestruturas críticas e a súa normativa de desenvolvemento, coa Lei 36/2015, do 28 de setembro, de seguridade nacional, e coa normativa comunitaria e nacional en materia de protección de datos. Cumpriuse igualmente co principio de transparencia, ao ter sometido o proxecto de real decreto ao trámite de audiencia e definírense claramente os obxectivos da iniciativa normativa e a súa xustificación. Por último, este real decreto resulta conforme

co principio de eficiencia, dado que non se establecen cargas adicionais ás recollidas no real decreto lei que desenvolve.

Na elaboración deste real decreto solicitouse informe de todos os departamentos ministeriais, así como da Axencia Española de Protección de Datos, da Comisión Nacional dos Mercados e da Competencia, da Comisión Nacional do Mercado de Valores, do Consello de Seguridade Nuclear e do Banco de España. Adicionalmente, solicitóuselles informe a todas as comunidades autónomas e déuselles audiencia ás organizacións representativas dos sectores afectados.

Na súa virtude, por proposta conxunta da vicepresidenta terceira do Goberno e ministra de Asuntos Económicos e Transformación Dixital, da ministra de Defensa, do ministro do Interior e da vicepresidenta primeira do Goberno e ministra da Presidencia, Relacións coas Cortes e Memoria Democrática, coa aprobación previa da ministra de Política Territorial e Función Pública, de acordo co Consello de Estado, e logo de deliberación do Consello de Ministros na súa reunión do día 26 de xaneiro de 2021,

DISPOÑO:

CAPÍTULO I

Disposicións xerais

Artigo 1. *Obxecto.*

Este real decreto ten por obxecto desenvolver o Real decreto lei 12/2018, do 7 de setembro, de seguridade das redes e sistemas de información, no relativo ao marco estratéxico e institucional de seguridade das redes e sistemas de información, á supervisión do cumprimento das obrigacións de seguridade dos operadores de servizos esenciais e dos provedores de servizos dixitais, e á xestión de incidentes de seguridade.

Artigo 2. *Ámbito de aplicación.*

1. De conformidade co artigo 2 do Real decreto lei 12/2018, do 7 de setembro, este real decreto aplicarase á prestación:

a) Dos servizos esenciais dependentes das redes e sistemas de información comprendidos nos sectores estratéxicos definidos no anexo da Lei 8/2011, do 28 de abril, pola que se establecen medidas para a protección das infraestruturas críticas.

b) Dos servizos dixitais que sexan mercados en liña, motores de busca en liña e servizos de computación en nube.

2. Estarán sometidos a este real decreto:

a) Os operadores de servizos esenciais establecidos en España. Entenderase que un operador de servizos esenciais está establecido en España cando a súa residencia ou domicilio social se encontren en territorio español, sempre que estes coincidan co lugar en que estea efectivamente centralizada a xestión administrativa e a dirección dos seus negocios ou actividades.

Así mesmo, este real decreto será de aplicación aos servizos esenciais que os operadores residentes ou domiciliados noutro Estado ofrezan a través dun establecemento permanente situado en España.

De conformidade co previsto no número 1 do artigo 6 do Real decreto lei 12/2018, a identificación dos servizos esenciais e dos operadores que os presten será efectuada polos órganos e procedementos previstos pola Lei 8/2011, do 28 de abril, pola que se establecen medidas para a protección das infraestruturas críticas, e a súa normativa de desenvolvemento, en particular o Real decreto 704/2011, do 20 de maio, polo que se aproba o Regulamento de protección das infraestruturas críticas.

b) Os provedores de servizos dixitais que teñan a súa sede social en España e que constitúa o seu establecemento principal na Unión Europea, así como os que, non estando

establecidos na Unión Europea, designen en España o seu representante na Unión para o cumprimento da Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, relativa ás medidas destinadas a garantir un elevado nivel común de seguridade das redes e sistemas de información na Unión.

3. Este real decreto non se aplicará:

a) Aos operadores de redes e servizos de comunicacións electrónicas e aos prestadores de servizos electrónicos de confianza que non sexan designados como operadores críticos en virtude da Lei 8/2011, do 28 de abril.

b) Aos provedores de servizos dixitais cando se trate de microempresas ou pequenas empresas, de acordo coas definicións recollidas na Recomendación 2003/361/CE da Comisión, do 6 de maio de 2003, sobre a definición de microempresas, pequenas e medianas empresas.

4. De conformidade co artigo 18 do Real decreto lei 12/2018, do 7 de setembro, cando unha normativa nacional ou comunitaria estableza para un sector obrigacións de seguridade das redes e sistemas de información ou de notificación de incidentes que teñan efectos, polo menos, equivalentes aos das obrigacións previstas no Real decreto lei 12/2018, do 7 de setembro, prevalecerán aqueles requisitos e os mecanismos de supervisión correspondentes.

CAPÍTULO II

Marco estratéxico e institucional

Artigo 3. *Autoridades competentes.*

As autoridades competentes en materia de seguridade das redes e sistemas de información serán, con carácter xeral, as establecidas no artigo 9.1 do Real decreto lei 12/2018, do 7 de setembro. En particular, son autoridades competentes para os operadores de servizos esenciais que non sexan operadores críticos de acordo coa Lei 8/2011, do 28 de abril, e que non estean incluídos no ámbito de aplicación da Lei 40/2015, do 1 de outubro, de réxime xurídico do sector público, as seguintes:

a) Respecto ao sector do transporte: o Ministerio de Transportes, Mobilidade e Axenda Urbana, a través da Secretaría de Estado de Transportes, Mobilidade e Axenda Urbana.

b) Respecto ao sector da enerxía: o Ministerio para a Transición Ecolóxica e o Reto Demográfico, a través da Secretaría de Estado de Enerxía.

c) Respecto ao sector das tecnoloxías da información e as telecomunicacións: o Ministerio de Asuntos Económicos e Transformación Dixital, a través da Secretaría de Estado de Dixitalización e Intelixencia Artificial e da Secretaría de Estado de Telecomunicacións e Infraestruturas Dixitais.

d) Respecto ao sector do sistema financeiro:

1.º O Ministerio de Asuntos Económicos e Transformación Dixital, a través da Secretaría de Estado de Economía e Apoio á Empresa, no ámbito dos seguros e fondos de pensións.

2.º O Banco de España, para as entidades de crédito.

3.º A Comisión Nacional do Mercado de Valores, para as entidades que prestan servizos de investimento e as sociedades xestoras de institucións de investimento colectivo.

e) Respecto ao sector do espazo: o Ministerio de Defensa, a través da Secretaría de Estado de Defensa.

f) Respecto ao sector da industria química: o Ministerio de Interior, a través da Secretaría de Estado de Seguridade.

g) Respecto ao sector das instalacións de investigación: o Ministerio de Ciencia e Innovación, a través da Secretaría Xeral de Investigación.

h) Respecto ao sector da saúde: o Ministerio de Sanidade, a través da Secretaría de Estado de Sanidade.

i) Respecto ao sector da auga: o Ministerio para a Transición Ecolóxica e o Reto Demográfico, a través da Secretaría de Estado de Medio Ambiente.

j) Respecto ao sector da alimentación:

1.º O Ministerio de Agricultura, Pesca e Alimentación, a través da Secretaría Xeral de Agricultura e Alimentación.

2.º O Ministerio de Sanidade, a través da Secretaría de Estado de Sanidade.

3.º O Ministerio de Industria, Comercio e Turismo, a través da Secretaría de Estado de Comercio.

4.º O Ministerio de Consumo, a través da Axencia Española de Seguridade Alimentaria e Nutrición (AESAN).

k) Respecto ao sector da industria nuclear:

1.º O Ministerio para a Transición Ecolóxica e o Reto Demográfico, a través da Secretaría de Estado de Enerxía.

2.º O Consello de Seguridade Nuclear.

Artigo 4. *Cooperación e coordinación dos CSIRT de referencia.*

1. A cooperación entre os CSIRT de referencia, e entre estes e as autoridades competentes, instrumentarase a través da Plataforma nacional de notificación e seguimento de ciberincidentes regulada no artigo 11.

2. Para efectos da cooperación prevista no artigo 11.1.a) 3.º do Real decreto lei 12/2018, do 7 de setembro, entenderase que son operadores con incidencia na Defensa nacional aqueles provedores de servizos esenciais básicos para o funcionamento do Ministerio de Defensa ou para a operatividade das Forzas Armadas que estableza, por proposta do Ministerio de Defensa, a Comisión Nacional para a Protección das Infraestruturas Críticas.

A designación como operador con incidencia na Defensa nacional levarase a cabo de conformidade co previsto no Regulamento de protección das infraestruturas críticas, aprobado polo Real decreto 704/2011, do 20 de maio. Así mesmo, os CSIRT de referencia serán informados da identidade dos operadores de servizos esenciais da súa comunidade que sexan designados operadores con incidencia na Defensa nacional.

O Ministerio de Defensa comunicaralle oportunamente á Comisión Nacional para a Protección das Infraestruturas Críticas as actualizacións derivadas de cambios de operadores na provisión destes servizos, que activarán as correspondentes notificacións de alta ou baixa como operadores con incidencia na Defensa nacional tanto aos propios operadores como aos seus CSIRT de referencia.

Cando un operador con incidencia na Defensa nacional sufra un incidente, deberá analizar se, polo seu alcance, este pode ter impacto no funcionamento do Ministerio de Defensa ou na operatividade das Forzas Armadas. No caso de que así for, porao de inmediato en coñecemento do seu CSIRT de referencia, quen informará o ESPDEF-CERT do Mando conxunto do ciberespazo a través das canles establecidas. Nestes casos, o ESPDEF-CERT do Mando conxunto do ciberespazo deberá ser oportunamente informado da evolución da xestión do incidente.

3. Os supostos de especial gravidade a que se refire o artigo 11.2, parágrafo primeiro, do Real decreto lei 12/2018, do 7 de setembro, en que o CCN-CERT exercerá a coordinación nacional da resposta técnica dos CSIRT, serán todos aqueles que, atendendo á natureza das notificacións inicial ou sucesivas do incidente recibidas polo CSIRT de referencia, posúan un impacto ou nivel de perigosidade moi alto ou crítico de acordo co establecido no anexo, e exixan un nivel de coordinación técnica cos outros CSIRT de referencia superior ao necesario en situacións ordinarias.

O Consello Nacional de Ciberseguridade será inmediatamente informado e poderá desactivar a coordinación prevista neste artigo, que unicamente se poderá producir cando cesase a situación prevista no parágrafo anterior e que non afectará o proceso de notificación de incidentes regulado nos artigos 11, 19.1 e 19.2 do Real decreto lei 12/2018, do 7 de setembro.

4. O CCN-CERT, no caso previsto no punto anterior, e a Oficina de Coordinación de Ciberseguridade do Ministerio do Interior (OCC), nos supostos previstos no artigo 11.2, parágrafo segundo, do Real decreto lei 12/2018, do 7 de setembro, requiriranlle ao CSIRT de referencia, tras a primeira notificación do incidente, polo menos a seguinte información:

a) Confirmación de que son correctos os datos asignados ao incidente, en particular verificando, se existe esta información, a validez:

1.º Da clasificación do incidente.
2.º Da perigosidade do incidente.
3.º Do impacto do incidente.

b) Plan de acción do CSIRT para abordar a resolución técnica do incidente, se procede.

c) Calquera información que permita determinar o posible impacto transfronteirizo do incidente.

Sempre que sexa posible, empregarase a Plataforma nacional de notificación e seguimento de ciberincidentes para as comunicacións consideradas neste punto.

Artigo 5. *Punto de contacto único.*

1. Na súa función de enlace para garantir a cooperación transfronteiriza das autoridades competentes designadas conforme o artigo 9 do Real decreto lei 12/2018, do 7 de setembro, coas autoridades competentes doutros Estados membros da Unión Europea, así como co grupo de cooperación recollido no artigo 11 da Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, e a rede de CSIRT, o Consello de Seguridade Nacional, a través do Departamento de Seguridade Nacional:

a) Comunicará á Comisión Europea a lista dos operadores de servizos esenciais nacionais establecidos para cada sector e subsector a que se refire o artigo 6 do Real decreto lei 12/2018, do 7 de setembro, e informará os puntos de contacto único doutros Estados sobre a intención de identificación dun operador de servizos esenciais doutro Estado membro que ofreza servizos en España.

b) Transmitirá aos puntos de contacto doutros Estados membros da Unión Europea afectados a información sobre incidentes con impacto transfronteirizo que lle transmitan as autoridades competentes ou o CSIRT de referencia, segundo o establecido no artigo 25 do Real decreto lei 12/2018, do 7 de setembro.

c) Remitirá aos CSIRT de referencia e ás autoridades competentes nacionais a correspondente información sobre incidentes que poidan ter efectos perturbadores nos servizos esenciais que reciba dos puntos de contacto dos correspondentes Estados membros, para que adopten as medidas oportunas no exercicio das súas funcións respectivas.

d) Ditará as instrucións pertinentes ás autoridades competentes para que elaboren, anualmente, o informe a que se refire o artigo 27.1 do Real decreto lei 12/2018, do 7 de setembro, sobre o tipo e número de incidentes comunicados, os seus efectos nos servizos prestados ou noutros servizos e o seu carácter nacional ou transfronteirizo dentro da Unión Europea, tendo en conta as indicacións do grupo de cooperación respecto ao formato e contido da información que se vai transmitir.

e) Obterá das autoridades competentes o informe anual a que se refire a letra anterior, e elaborará un informe anual resumido sobre as notificacións recibidas, que

remitirá ao grupo de cooperación antes do 15 de febreiro de cada ano e, posteriormente, ás autoridades competentes e aos CSIRT de referencia, para o seu coñecemento.

2. Adicionalmente ás funcións de enlace previstas no punto anterior, e de conformidade co previsto no artigo 9.2 do Real decreto lei 12/2018, do 7 de setembro, o Consello de Seguridade Nacional, a través do seu comité especializado en materia de ciberseguridade, garantirá a coordinación das actuacións das autoridades competentes mediante:

a) O fomento da coherencia entre os requisitos de seguridade específicos que, de ser o caso, adopten as autoridades competentes, conforme o previsto no artigo 6.6 deste real decreto.
b) O fomento da coherencia entre as obrigacións específicas que, de ser o caso, establezan as autoridades competentes, conforme o previsto no artigo 8.3 deste real decreto.
c) O impulso da coordinación das disposicións e actuacións das autoridades competentes e as actuacións dos CSIRT de referencia coas disposicións e actuacións en materia de seguridade da información das autoridades de protección de datos e de seguridade pública.

3. Do mesmo modo, o Consello de Seguridade Nacional exercerá as funcións de coordinación previstas no número 2 anterior nos supostos recollidos no artigo 18 do Real decreto lei 12/2018, do 7 de setembro.

CAPÍTULO III

Requisitos de seguridade

Artigo 6. *Medidas para o cumprimento das obrigacións de seguridade.*

1. Os operadores de servizos esenciais e os provedores de servizos dixitais deberán adoptar as medidas técnicas e de organización adecuadas e proporcionadas para xestionar os riscos que afecten a seguridade das redes e sistemas de información utilizados para a prestación dos seus servizos, tanto se se trata de redes e sistemas propios como de provedores externos.
2. No caso dos operadores de servizos esenciais, deberán aprobar unhas políticas de seguridade das redes e sistemas de información atendendo aos principios de seguridade integral, xestión de riscos, prevención, resposta e recuperación, liñas de defensa, reavaliación periódica e segregación de tarefas.
As ditas políticas considerarán, como mínimo, os seguintes aspectos:

a) Análise e xestión de riscos.
b) Xestión de riscos de terceiros ou provedores.
c) Catálogo de medidas de seguridade, organizativas, tecnolóxicas e físicas.
d) Xestión do persoal e profesionalidade.
e) Adquisición de produtos ou servizos de seguridade.
f) Detección e xestión de incidentes.
g) Plans de recuperación e aseguramento da continuidade das operacións.
h) Mellora continua.
i) Interconexión de sistemas.
j) Rexistro da actividade dos usuarios.

3. As medidas de seguridade que adopten os operadores de servizos esenciais deberán ter en conta, en particular, a dependencia das redes e sistemas de información e a continuidade de servizos ou subministracións contratados polo operador, así como as interaccións que presenten con redes e sistemas de información de terceiros.
4. A relación de medidas adoptadas formalizarase nun documento denominado Declaración de aplicabilidade de medidas de seguridade, que será subscrito polo

responsable de seguridade da información designado conforme o previsto no artigo seguinte e que se incluirá na política de seguridade que aprobe a dirección da organización. O dito documento, que se deberá remitir á autoridade competente respectiva no prazo de seis meses desde a designación do operador como operador de servizos esenciais, deberase revisar, polo menos, cada tres anos. Tanto a Declaración de aplicabilidade de medidas de seguridade inicial como as súas sucesivas revisións serán supervisadas pola autoridade competente respectiva, segundo se prevé no artigo 14 deste real decreto.

5. As medidas a que se refiren os puntos anteriores tomarán como referencia as recollidas no anexo II do Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema nacional de seguridade no ámbito da Administración electrónica, na medida en que sexan aplicables, e basearanse, cando sexa posible, noutros esquemas nacionais de seguridade existentes.

Sen prexuízo do anterior, poderanse ter en conta outros estándares recoñecidos internacionalmente.

6. As medidas adoptadas poderán ser complementadas con outras atendendo a necesidades específicas, entre elas a posibilidade de exixir un documento de aplicabilidade dos sistemas afectados por esta normativa, naqueles operadores con contornos de sistemas de información especialmente complexos. En particular, complementaranse coas que, de ser o caso, establezan con carácter específico as autoridades competentes, de conformidade co previsto no artigo 16.4 e no artigo 32.2 do Real decreto lei 12/2018, do 7 de setembro.

7. Na elaboración das políticas de seguridade das redes e sistemas de información teranse en conta os riscos que derivan do tratamento dos datos persoais, de acordo co artigo 24 do Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE (en diante, Regulamento xeral de protección de datos). En caso de que a análise de xestión de riscos, de acordo co Regulamento xeral de protección de datos, exixa implantar medidas adicionais ás previstas no Real decreto 3/2010, do 8 de xaneiro, adoptaranse as medidas de acordo co artigo 24.1 do Regulamento xeral de protección de datos.

Artigo 7. *Responsable da seguridade da información.*

1. Os operadores de servizos esenciais designarán unha persoa, unidade ou órgano colexiado, responsable da seguridade da información, que exercerá as funcións de punto de contacto e coordinación técnica coa autoridade competente e co CSIRT de referencia que lle corresponda, de conformidade co previsto no punto terceiro. No suposto de que o responsable de seguridade da información sexa unha unidade ou órgano colexiado, deberase designar unha persoa física representante, así como un substituto deste que asumirá as súas funcións en casos de ausencia, vacante ou enfermidade. O prazo para levar a cabo a dita designación será de tres meses desde a súa designación como operador de servizos esenciais.

2. Os operadores de servizos esenciais comunicaranlle á autoridade competente respectiva a designación do responsable da seguridade da información dentro do prazo establecido no punto anterior, así como os nomeamentos e cesamentos que afecten a designación do responsable da seguridade da información no prazo dun mes desde que aqueles se produzan.

3. O responsable da seguridade da información actuará como punto de contacto coa autoridade competente en materia de supervisión dos requisitos de seguridade das redes e sistemas de información, e como punto de contacto especializado para a coordinación da xestión dos incidentes co CSIRT de referencia. Desenvolveranse baixo a súa responsabilidade, entre outras, as seguintes funcións:

a) Elaborar e propor para que aprobe a organización, de conformidade co establecido no artigo 6.2 deste real decreto, as políticas de seguridade, que incluirán as medidas técnicas e organizativas, adecuadas e proporcionadas, para xestionar os riscos que

xurdan para a seguridade das redes e sistemas de información utilizados e para previr e reducir ao mínimo os efectos dos ciberincidentes que afecten a organización e os servizos, de conformidade co disposto no artigo 6.

b) Supervisar e desenvolver a aplicación das políticas de seguridade, normativas e procedementos derivados da organización, supervisar a súa efectividade e levar a cabo controis periódicos de seguridade.

c) Elaborar o documento de Declaración de aplicabilidade de medidas de seguridade considerado no artigo 6.3, parágrafo segundo, deste real decreto.

d) Actuar como capacitador de boas prácticas en seguridade das redes e sistemas de información, tanto en aspectos físicos como lóxicos.

e) Remitirlle á autoridade competente, a través do CSIRT de referencia e sen dilación indebida, as notificacións de incidentes que teñan efectos perturbadores na prestación dos servizos a que se refire o artigo 19.1 do Real decreto lei 12/2018, do 7 de setembro.

f) Recibir, interpretar e supervisar a aplicación das instrucións e guías emanadas da autoridade competente, tanto para a operativa habitual como para a emenda das deficiencias observadas.

g) Recompilar, preparar e subministrar información ou documentación á autoridade competente ou ao CSIRT de referencia, por solicitude deles ou por propia iniciativa.

O responsable da seguridade da información, para desenvolver estas funcións, poderase apoiar en servizos prestados por terceiros.

4. Os operadores de servizos esenciais garantirán que o responsable da seguridade da información cumpra cos seguintes requisitos:

a) Contar con persoal con coñecementos especializados e experiencia en materia de ciberseguridade, desde os puntos de vista organizativo, técnico e xurídico, adecuados ao desempeño das funcións indicadas no punto anterior.

b) Contar cos recursos necesarios para o desenvolvemento das ditas funcións.

c) Ter unha posición na organización que facilite o desenvolvemento das súas funcións, participando de forma adecuada e en tempo oportuno en todas as cuestións relativas á seguridade e mantendo unha comunicación real e efectiva coa alta dirección.

d) Manter a debida independencia respecto dos responsables das redes e dos sistemas de información.

5. Sempre que concorran os requisitos de coñecemento, experiencia, independencia e, de ser o caso, titulación, as funcións e responsabilidades encomendadas ao responsable da seguridade da información poderanse compatibilizar coas sinaladas para o responsable de seguridade e enlace e o responsable de seguridade do Esquema nacional de seguridade, de conformidade co disposto na normativa aplicable a estas figuras.

CAPÍTULO IV

Xestión de incidentes de seguridade

Artigo 8. *Xestión de incidentes de seguridade.*

1. Os operadores de servizos esenciais e os provedores de servizos dixitais deberán xestionar e resolver os incidentes de seguridade que afecten as redes e os sistemas de información utilizados para a prestación dos seus servizos. No caso de redes e sistemas que non sexan propios, os operadores deberán tomar as medidas necesarias para garantir que as ditas accións as leven a cabo os provedores externos.

Esta obrigación alcanza tanto os incidentes detectados polo propio operador ou provedor como os que lles sinalen o CSIRT de referencia ou a autoridade competente, cando teñan coñecemento dalgunha circunstancia que faga sospeitar da existencia dun incidente.

2. Sen prexuízo do previsto no artigo 28.1 do Real decreto lei 12/2018, do 7 de setembro, os operadores de servizos esenciais e os provedores de servizos dixitais

poderán solicitar voluntariamente axuda especializada do CSIRT de referencia para a xestión dos incidentes e, en tales casos, deberán atender ás indicacións que reciban deste para resolver o incidente, mitigar os seus efectos e repor os sistemas afectados.

3. Na resolución dos incidentes, os operadores de servizos esenciais aplicarán os aspectos pertinentes da política de xestión da seguridade das redes e sistemas de información a que se refire o artigo 6, así como as obrigacións específicas que, de ser o caso, establezan as autoridades competentes.

Artigo 9. *Obrigacións de notificación de incidentes dos operadores de servizos esenciais.*

1. Os operadores de servizos esenciais notificaranlle á autoridade competente respectiva, a través do CSIRT de referencia, os incidentes que poidan ter efectos perturbadores significativos nos ditos servizos. Para tal efecto, consideraranse os incidentes cun nivel de impacto crítico, moi alto ou alto, segundo o detalle que se especifica no número 4 da Instrución nacional de notificación e xestión de ciberincidentes, que se contén no anexo deste real decreto.

Así mesmo, notificarán os sucesos ou incidencias que, polo seu nivel de perigosidade, poidan afectar as redes e os sistemas de información empregados para a prestación dos servizos esenciais, mesmo cando non tivesen aínda un efecto adverso real sobre aqueles. Para estes efectos, consideraranse os incidentes cun nivel de perigosidade crítico, moi alto ou alto, segundo o detalle que se especifica no número 3 da citada instrución.

2. Sen prexuízo do anterior, as autoridades competentes poderán establecer, de conformidade co artigo 19.5 do Real decreto lei 12/2018, do 7 de setembro, obrigacións específicas de notificación que recollan niveis diferentes aos previstos na Instrución nacional de notificación e xestión de ciberincidentes, así como factores e limiares sectoriais específicos, aplicables aos operadores sometidos á súa supervisión.

3. A notificación dun ciberincidente conforme este real decreto non exclúe nin substitúe a notificación que dos mesmos feitos se deba realizar a outros organismos conforme a súa normativa específica.

En particular, as obrigacións de notificación previstas nos puntos anteriores son independentes das que se deban realizar á Axencia Española de Protección de Datos conforme o previsto no artigo 33 do Regulamento xeral de protección de datos, sen prexuízo da cooperación entre autoridades prevista no artigo 29 do Real decreto lei 12/2018, e a posibilidade de acceso por parte da citada axencia á Plataforma común de notificación de incidentes prevista na súa disposición adicional terceira.

Para estes efectos, as notificacións previstas nos números 1 e 2 deste artigo incluirán a información que, para os casos de violación da seguridade dos datos persoais, se conteña nos formularios aprobados pola Axencia Española de Protección de Datos.

Artigo 10. *Procedementos de notificación de incidentes.*

1. Os CSIRT de referencia garantirán un intercambio fluído de información coas autoridades competentes que correspondan, asegurando o adecuado seguimento durante a xestión dos incidentes, así como o acceso á información empregada nas distintas fases que compoñen a xestión de incidentes.

2. Os operadores de servizos esenciais realizarán as notificacións a través do responsable da seguridade da información designado.

No caso de que un operador de servizos esenciais reúna os criterios previstos no artigo 6.2 do Real decreto lei 12/2018, do 7 de setembro, sobre seguridade das redes e sistemas de información, o responsable da seguridade da información coordinarase, para estes efectos, co responsable de seguridade e enlace previsto no artigo 16 da Lei 8/2011, do 28 de abril, pola que se establecen medidas para a protección das infraestruturas críticas.

3. Os operadores de servizos esenciais deberán realizar unha primeira notificación tan pronto como dispoñan de información para determinar que se dan as circunstancias para a notificación, atendendo aos factores e limiares correspondentes.

Efectuaranse as notificacións intermedias que sexan precisas para actualizar ou completar a información incorporada á notificación inicial e informar sobre a evolución do incidente, mentres este non estea resolto, e realizarase unha notificación final do incidente tras a súa resolución, informando do detalle da evolución do suceso, da valoración da probabilidade da súa repetición e das medidas correctoras que eventualmente teña previsto adoptar o operador. Os limiares temporais exixidos para as ditas notificacións serán os recollidos no anexo deste real decreto.

4. As notificacións incluirán, en canto estea dispoñible, a información que permita determinar calquera efecto transfronteirizo do incidente.

5. O establecido nos puntos anteriores será de aplicación aos provedores de servizos dixitais mentres non se regule de modo diferente nos actos de execución previstos no artigo 16.9 da Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, relativa ás medidas destinadas a garantir un elevado nivel común de seguridade das redes e sistemas de información na Unión.

6. O CSIRT de referencia, en colaboración coa autoridade competente, valorará con prontitude a dita información con vistas a determinar se o incidente pode ter efectos perturbadores significativos para os servizos esenciais prestados noutros Estados membros da Unión Europea e, en tal caso, informará os Estados membros afectados a través do punto de contacto único.

Así mesmo, a autoridade competente valorará, conxuntamente co correspondente CSIRT de referencia, a información sobre incidentes con posibles impactos transfronteirizos que reciba doutros Estados membros, e indicarállelo e transmitiralles a información relevante aos operadores de servizos esenciais que se poidan ver afectados.

Artigo 11. *Plataforma nacional de notificación e seguimento de ciberincidentes.*

1. O CCN-CERT, en colaboración co INCIBE-CERT e o ESPDEF-CERT do Mando conxunto do ciberespazo, porá á disposición de todos os axentes involucrados a Plataforma nacional de notificación e seguimento de ciberincidentes a que se refire o artigo 19.4 do Real decreto lei 12/2018, do 7 de setembro.

2. A plataforma permitirá o intercambio de información e o seguimento de incidentes entre os operadores de servizos esenciais ou provedores de servizos dixitais, as autoridades competentes e os CSIRT de referencia de maneira segura e confiable, sen prexuízo dos requisitos específicos aplicables en materia de protección de datos de carácter persoal.

3. Esta plataforma deberá garantir, así mesmo, a dispoñibilidade, autenticidade, integridade e confidencialidade da información, e poderá empregarse tamén para dar cumprimento á exixencia de notificación derivada de regulacións sectoriais, de acordo co artigo 19.5 do Real decreto lei 12/2018, do 7 de setembro.

4. A plataforma disporá, así mesmo, de diversas canles de comunicación para o seu uso por parte das autoridades competentes e dos CSIRT de referencia. A plataforma garantirá o acceso das autoridades competentes a toda a información relativa á notificación e ao estado de situación dos incidentes do seu ámbito de competencia que lles permita efectuar en todo momento o necesario seguimento e control do seu estado de situación. Igualmente, as autoridades competentes terán acceso, a través da plataforma, a datos estatísticos, en particular aos necesarios para xerar os informes a que fai mención o artigo 5.

5. Así mesmo, a plataforma implementará o procedemento de notificación e xestión de incidentes, que estará dispoñible durante todas as horas do día e todos os días do ano, e disporá, como mínimo, das seguintes capacidades:

a) Capacidade de xestión de ciberincidentes, con incorporación de taxonomía, criticidade e notificacións a terceiros, segundo o establecido no anexo.

b) Capacidade de intercambio de información sobre ciberameazas.
c) Capacidade de análise de mostras.
d) Capacidade de rexistro e notificación de vulnerabilidades.
e) Capacidade de comunicacións seguras entre os axentes involucrados en diferentes formatos e plataformas.
f) Capacidade de intercambio masivo de datos.
g) Xeración de estatísticas e informes agregados.

Artigo 12. *Información sobre incidentes.*

1. Cando as circunstancias o permitan, os CSIRT de referencia proporcionaranlles aos operadores de servizos esenciais e aos provedores de servizos dixitais notificantes a información pertinente con respecto ao seguimento da notificación dun incidente, en particular aquela que poida facilitar a xestión eficaz do incidente.
2. Así mesmo, as autoridades competentes e os CSIRT de referencia proporcionaranlles aos operadores de servizos esenciais e aos provedores de servizos dixitais que se poidan ver afectados polos ditos incidentes a información que poida ser relevante para previren e, de ser o caso, resolveren o incidente.
3. Ao proporcionaren a información a que se refiren os puntos anteriores, as autoridades competentes e os CSIRT de referencia velarán polos intereses comerciais dos operadores de servizos esenciais e provedores de servizos dixitais, preservando a confidencialidade da información que obteñan destes, de conformidade co establecido no artigo 15 do Real decreto lei 12/2018, do 7 de setembro.

Artigo 13. *Actuacións ante incidentes con carácter presuntamente delituoso.*

En cumprimento do disposto no artigo 262 da Lei de axuizamento criminal, a OCC comunicaralles o antes posible ao Ministerio Fiscal e, de ser o caso, ás unidades orgánicas de policía xudicial competentes aqueles incidentes de seguridade que lle sexan notificados e que revistan carácter presuntamente delituoso, e trasladará ao mesmo tempo a información que posúa en relación con iso. Para o dito fin poderá requirir dos operadores afectados ou dos CSIRT de referencia canta información relacionada co incidente se considere necesaria.

Artigo 14. *Consulta con outras autoridades.*

1. As consultas con outras autoridades con competencia en materia de seguridade pública e seguridade cidadá, previstas no artigo 14.1 do Real decreto lei 12/2018, do 7 de setembro, realizaranse a través da OCC.
2. As consultas relativas ao resto de materias previstas no citado artigo 14 realizaranse directamente ás autoridades competentes correspondentes.

CAPÍTULO V

Supervisión

Artigo 15. *Supervisión do cumprimento de obrigacións de seguridade e de notificación de incidentes*.

1. As autoridades competentes supervisarán, no seu ámbito de actuación, o cumprimento das obrigacións de seguridade e de notificación de incidentes que lles sexan de aplicación aos operadores de servizos esenciais e aos provedores de servizos dixitais, de conformidade co Real decreto lei 12/2018, do 7 de setembro, e con este real decreto.
2. Os operadores de servizos esenciais e os provedores de servizos dixitais colaborarán coa autoridade competente na dita supervisión, facilitando as actuacións de inspección, proporcionando toda a información que se lles requira para tal efecto e

aplicando as instrucións ditadas, de ser o caso, para a emenda das deficiencias observadas.

3. O cumprimento das obrigacións de seguridade nas redes e sistemas de información poderá ser acreditado mediante a certificación nun esquema de seguridade que, logo de consulta ao CSIRT de referencia, sexa recoñecido pola autoridade competente.

4. As autoridades competentes poderán realizar as actuacións inspectoras que sexan precisas para o exercicio da súa función de control. En particular, as actuacións de inspección das autoridades competentes, que poderán ser apoiadas polos CSIRT de referencia, terán por obxecto:

a) Controlar o cumprimento das normas e instrucións técnicas que, de ser o caso, resulten aplicables aos operadores suxeitos á súa supervisión.

b) Verificar o cumprimento das funcións do responsable de seguridade da información designado polos operadores de servizos esenciais, segundo o previsto no artigo 7.3 deste real decreto.

c) Realizar as comprobacións, inspeccións, probas e revisións necesarias para verificar o cumprimento das medidas de seguridade previstas no artigo 6, en particular a política de seguridade dos operadores de servizos esenciais e a Declaración de aplicabilidade de medidas de seguridade.

De conformidade co previsto no artigo 32.1 do Real decreto lei 12/2018, do 7 de setembro, cando o volume ou complexidade das actuacións de inspección que se deban desenvolver así o aconselle, as autoridades competentes poderán requirir o operador de servizos esenciais para que remita un informe de auditoría, elaborado por unha entidade externa, solvente e independente, sobre a seguridade das súas redes e sistemas de información.

5. Os CSIRT de referencia colaborarán coas autoridades competentes, cando estas llelo requiran, no exercicio das funcións a que se refire o punto anterior. En particular, facilitarán asesoramento técnico sobre a idoneidade das medidas de seguridade adoptadas polos operadores de servizos esenciais e polos provedores de servizos dixitais en virtude do artigo 6 deste real decreto.

Así mesmo, cando se trate de operadores con incidencia na Defensa nacional a que se refire o artigo 4.2 deste real decreto, o ESPDEF-CERT do Mando conxunto do ciberespazo poderá colaborar na supervisión coa autoridade competente.

6. No caso dos provedores de servizos dixitais, a supervisión levarase a cabo de maneira coordinada coas autoridades competentes correspondentes dos Estados membros da Unión Europea onde os ditos provedores presten servizos ou teñan o seu establecemento principal na Unión.

Disposición adicional primeira. *Designación do responsable da seguridade da información polos operadores de servizos esenciais designados.*

Os operadores de servizos esenciais designados conforme o previsto na disposición adicional primeira do Real decreto lei 12/2018, do 7 de setembro, deberanlle comunicar á autoridade competente respectiva a identidade do responsable da seguridade da información no prazo de tres meses desde a entrada en vigor deste real decreto.

Disposición adicional segunda. *Orientacións para a xestión de incidentes e cumprimento das obrigacións de notificación.*

O Consello de Seguridade Nacional, por proposta do seu comité especializado en materia de ciberseguridade, e articuladas as súas funcións como punto de contacto único a través do Departamento de Seguridade Nacional, poderá aprobar orientacións en relación coa Instrución nacional de notificación e xestión de incidentes recollida no anexo, así como para a actualización da Guía nacional de notificación e xestión de ciberincidentes, que inclúan directrices e recomendacións para o cumprimento das obrigacións de

notificación previstas neste real decreto, así como no Real decreto lei 12/2018, do 7 de setembro, co obxecto de mellorar a coordinación e optimizar os recursos dedicados á xestión dos incidentes que afecten a seguridade das redes e sistemas de información.

Disposición adicional terceira. *Réxime específico do Banco de España.*

As disposicións deste real decreto entenderanse sen prexuízo das competencias e funcións atribuídas ao Banco de España, ao Banco Central Europeo e ao Sistema europeo de bancos centrais, de conformidade co Tratado de funcionamento da Unión Europea, cos estatutos do Sistema europeo de bancos centrais e do Banco Central Europeo, co Regulamento (UE) n.º 1024/2013 do Consello, do 15 de outubro de 2013, que lle encomenda ao Banco Central Europeo tarefas específicas respecto de políticas relacionadas coa supervisión prudencial das entidades de crédito, e coa Lei 13/1994, do 1 de xuño, de autonomía do Banco de España.

No non previsto na súa normativa específica, e en canto sexa compatible coa súa natureza, funcións e independencia, será de aplicación ao Banco de España o previsto neste real decreto.

Disposición adicional cuarta. *Suposto de dependencia de provedores externos.*

En referencia ao artigo 19.3 do Real decreto lei 12/2018, do 7 de setembro, cando os operadores de servizos esenciais ou provedores de servizos dixitais dependan de provedores externos aos cales lles sexa de aplicación a disposición adicional novena da Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico, o equipo de resposta ante emerxencias informáticas (CERT) competente do provedor externo corresponderase:

a) Co CCN-CERT, do Centro Criptolóxico Nacional, cando o provedor estea incluído no ámbito subxectivo de aplicación da Lei 40/2015, do 1 de outubro.

b) Co INCIBE-CERT, do Instituto Nacional de Ciberseguridade de España, no resto dos casos.

Disposición adicional quinta. *Tratamentos de datos de carácter persoal.*

Os tratamentos de datos de carácter persoal das persoas físicas realizaranse con estrita suxeición ao disposto no Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento dos seus datos persoais e á súa libre circulación, na Lei orgánica 3/2018, do 5 de decembro, de protección de datos persoais e garantía dos dereitos dixitais, e, de ser o caso, na normativa sobre protección de datos persoais especial ou específica que resulte de aplicación.

Disposición adicional sexta. *Información sobre incidentes no sistema financeiro.*

Os CSIRT de referencia informarán o titular da Secretaría de Estado de Economía e Apoio á Empresa, a través da Secretaría Xeral do Tesouro e Financiamento Internacional, dos incidentes que poidan ter efectos perturbadores significativos nos servizos esenciais do sistema financeiro. Para estes efectos, entenderase que teñen efectos perturbadores significativos cando o seu limiar ou nivel de impacto sexa crítico, moi alto ou alto, segundo o sinalado no anexo deste real decreto.

Disposición transitoria única. *Desempeño transitorio de funcións no sector enerxético.*

A Secretaría de Estado de Seguridade do Ministerio do Interior, a través da Oficina de Coordinación de Ciberseguridade (OCC), desempeñará temporalmente as funcións atribuídas por este real decreto ao departamento ministerial con competencias en materia de enerxía, ata que este dispoña dos recursos humanos necesarios coa formación

adecuada para exercer estas competencias de forma efectiva, segundo o previsto no artigo 3 e, en todo caso, nun prazo máximo de 12 meses.

Disposición derradeira primeira. *Título competencial.*

Este real decreto dítase ao abeiro do previsto no artigo 149.1.21.ª e 29.ª da Constitución, que lle atribúe ao Estado competencia exclusiva en materia de réxime xeral de telecomunicacións e seguridade pública, respectivamente.

Disposición derradeira segunda. *Habilitación para o desenvolvemento normativo e aplicación.*

Facúltanse os titulares dos ministerios de Asuntos Económicos e Transformación Dixital, do Interior e de Defensa, así como os titulares dos ministerios e organismos relacionados no artigo 3, para ditaren conxunta ou separadamente, segundo as materias de que se trate e no ámbito das súas respectivas competencias, as disposicións que exixan o desenvolvemento e a aplicación deste real decreto.

Disposición derradeira terceira. *Entrada en vigor.*

Este real decreto entrará en vigor o día seguinte ao da súa publicación no «Boletín Oficial del Estado».

Dado en Madrid o 26 de xaneiro de 2021.

FELIPE R.

A vicepresidenta primeira do Goberno e ministra da Presidencia,
Relacións coas Cortes e Memoria Democrática,
CARMEN CALVO POYATO

ANEXO

Instrución nacional de notificación e xestión de ciberincidentes

1. *Obrigatoriedade de notificación*

Os incidentes asociaranse a un dos niveis de perigosidade e impacto establecidos nesta instrución, tendo en conta a obrigatoriedade de notificación de todos aqueles que se categoricen cun nivel CRÍTICO, MOI ALTO ou ALTO para todos aqueles suxeitos obrigados aos que lles sexa aplicable esta «Instrución nacional de notificación e xestión de ciberincidentes». Nese caso, os suxeitos obrigados deberán comunicar, en tempo e forma, os incidentes que rexistren nas súas redes e sistemas de información e que estean obrigados a notificar por superaren os limiares de impacto ou perigosidade establecidos nesta instrución.

Para a notificación dos incidentes de ciberseguridade utilizarase como criterio de referencia o nivel de perigosidade que se asigne a un incidente, sen prexuízo de que ao longo do seu desenvolvemento, da súa mitigación ou resolución, se categorice cun determinado nivel de impacto que faga aconsellable a comunicación do incidente á autoridade competente ou CSIRT de referencia.

En todo caso, cando un determinado suceso se poida asociar a máis dun tipo de incidente debido ás súas características potenciais, este asociarase a aquel que teña un nivel de perigosidade superior de acordo cos criterios expostos nesta instrución.

2. *Clasificación/taxonomía dos ciberincidentes*

A seguinte clasificación/taxonomía dos ciberincidentes está aliñada coa taxonomía aprobada pola Axencia da Unión Europea para a Ciberseguridade (ENISA).

Esta clasificación/taxonomía dos ciberincidentes empregarase para a asignación dunha clasificación específica a un incidente rexistrado nas redes e sistemas de información cando se realice a comunicación á autoridade competente ou CSIRT de referencia.

Táboa 1. Clasificación/taxonomía dos ciberincidentes

Clasificación	Tipo de incidente	Descrición e exemplos prácticos
Contido abusivo.	*Spam.*	Correo electrónico masivo non solicitado. O receptor do contido non outorgou autorización válida para recibir unha mensaxe colectiva.
	Delitos de odio, contra a liberdade ou a honra.	Contido difamatorio ou discriminatorio. Ex.: ciberacoso, racismo, ameazas a unha persoa ou dirixidas contra colectivos.
	Pornografía infantil, contido sexual ou violento inadecuado.	Material que represente de maneira visual contido relacionado con pornografía infantil, apoloxía da violencia, etc.
Contido daniño.	Sistema infectado.	Sistema infectado con *malware*. Ex.: sistema, computadora ou teléfono móbil infectado cun *rootkit*.
	Servidor C&C (mando e control).	Conexión con servidor de mando e control (C&C) mediante *malware* ou sistemas infectados.
	Distribución de *malware*.	Recurso usado para distribución de *malware*. Ex.: recurso dunha organización empregado para distribuír *malware*.
	Configuración de *malware*.	Recurso que aloxe ficheiros de configuración de *malware* Ex.: ataque de *webinjects* para troiano.
Obtención de información.	Escaneamento de redes (*scanning*).	Envío de peticións a un sistema para descubrir posibles debilidades. Inclúense tamén procesos de comprobación ou *testeo* para recompilar información de aloxamentos, servizos e contas. Ex.: peticións DNS, ICMP, SMTP, escaneamento de portos.
	Análise de paquetes (*sniffing*).	Observación e gravación do tráfico de redes.
	Enxeñaría social.	Recompilación de información persoal sen o uso da tecnoloxía. Ex.: mentiras, trucos, subornos, ameazas.
Intento de intrusión.	Explotación de vulnerabilidades coñecidas.	Intento de compromiso dun sistema ou de interrupción dun servizo mediante a explotación de vulnerabilidades cun identificador estandarizado (véxase CVE). Ex.: desbordamento de *buffer*, portas traseiras, *cross site scripting* (XSS).
	Intento de acceso con vulneración de credenciais.	Múltiples intentos de vulnerar credenciais. Ex.: intentos de ruptura de contrasinais, ataque por forza bruta.
	Ataque descoñecido.	Ataque empregando *exploit* descoñecido.
Intrusión.	Compromiso de conta con privilexios.	Compromiso dun sistema en que o atacante adquiriu privilexios.
	Compromiso de conta sen privilexios.	Compromiso dun sistema empregando contas sen privilexios.
	Compromiso de aplicacións.	Compromiso dunha aplicación mediante a explotación de vulnerabilidades de software. Ex.: inxección SQL.
	Roubo.	Intrusión física. Ex.: acceso non autorizado a centro de procesamento de datos.

Clasificación	Tipo de incidente	Descrición e exemplos prácticos
Dispoñibilidade.	DoS (denegación de servizo).	Ataque de denegación de servizo. Ex.: envío de peticións a unha aplicación *web* que provoca a interrupción ou ralentización na prestación do servizo.
	DDoS (denegación distribuída de servizo).	Ataque de denegación distribuída de servizo. Ex.: inundación de paquetes SYN, ataques de reflexión e amplificación utilizando servizos baseados en UDP.
	Mala configuración.	Configuración incorrecta do software que provoca problemas de dispoñibilidade no servizo. Ex.: servidor DNS co KSK da zona raíz de DNSSEC obsoleto.
	Sabotaxe.	Sabotaxe física. Ex.: cortes de cablaxe de equipamentos ou incendios provocados.
	Interrupcións.	Interrupcións por causas alleas. Ex.: desastre natural.
Compromiso da información.	Acceso non autorizado a información.	Acceso non autorizado a información. Ex.: roubo de credenciais de acceso mediante interceptación de tráfico ou mediante o acceso a documentos físicos.
	Modificación non autorizada de información.	Modificación non autorizada de información. Ex.: modificación por un atacante empregando credenciais subtraídas dun sistema ou aplicación ou encriptaxe de datos mediante *ransomware*.
	Perda de datos.	Perda de información Ex.: perda por fallo de disco duro ou roubo físico.
Fraude.	Uso non autorizado de recursos.	Uso de recursos para propósitos inadecuados, incluídas accións con ánimo de lucro. Ex.: uso de correo electrónico para participar en estafas piramidais.
	Dereitos de autor.	Ofrecemento ou instalación de software carente de licenza ou doutro material protexido por dereitos de autor. Ex.: Warez.
	Suplantación.	Tipo de ataque en que unha entidade suplanta outra para obter beneficios ilexítimos.
	Phishing.	Suplantación doutra entidade coa finalidade de convencer o usuario para que revele as súas credenciais privadas.
Vulnerabilidade.	Criptografía débil.	Servizos accesibles publicamente que poidan presentar criptografía débil. Ex.: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS.	Servizos accesibles publicamente que poidan ser empregados para a reflexión ou amplificación de ataques DDoS. Ex.: DNS *open-resolvers* ou servidores NTP con monitorización *monlist*.
	Servizos con acceso potencial non desexado.	Ex.: Telnet, RDP ou VNC.
	Revelación de información.	Acceso público a servizos en que potencialmente se poida relevar información sensible. Ex.: SNMP ou Redis.
	Sistema vulnerable.	Sistema vulnerable. Ex.: mala configuración de *proxy* en cliente (WPAD), versións desfasadas de sistema.
Outros.	Outros.	Todo aquel incidente que non teña cabida en ningunha categoría anterior.
	APT.	Ataques dirixidos contra organizacións concretas, sustentados en mecanismos moi sofisticados de ocultación, anonimato e persistencia. Esta ameaza habitualmente emprega técnicas de enxeñaría social para conseguir os seus obxectivos xunto co uso de procedementos de ataque coñecidos ou xenuínos.

3. *Nivel de perigosidade do ciberincidente*

O indicador de perigosidade determina a potencial ameaza que suporía a materialización dun incidente nos sistemas de información ou comunicación do ente afectado, así como para os servizos prestados ou a continuidade de negocio en caso de habela. Este indicador fundaméntase nas características intrínsecas á tipoloxía de ameaza e o seu comportamento.

Os incidentes asociaranse a algún dos seguintes niveis de perigosidade: CRÍTICO, MOI ALTO, ALTO, MEDIO, BAIXO.

Nivel crítico:

– APT.

Nivel moi alto:

– Distribución de *malware*.
– Configuración de *malware*.
– Roubo.
– Sabotaxe.
– Interrupcións.

Nivel alto:

– Pornografía infantil, contido sexual ou violento inadecuado.
– Sistema infectado.
– Servidor C&C (mando e control).
– Compromiso de aplicacións.
– Compromiso de contas con privilexios.
– Ataque descoñecido.
– DoS (denegación de servizo).
– DDoS (denegación distribuída de servizo).
– Acceso non autorizado a información.
– Modificación non autorizada de información.
– Perda de datos.
– *Phishing.*

Nivel medio:

– Discurso de odio.
– Enxeñaría social.
– Explotación de vulnerabilidades coñecidas.
– Intento de acceso con vulneración de credenciais.
– Compromiso de contas sen privilexios.
– Desconfiguración.
– Uso non autorizado de recursos.
– Dereitos de autor.
– Suplantación.
– Criptografía débil.
– Amplificador DDoS.
– Servizos con acceso potencial non desexado.
– Revelación de información.
– Sistema vulnerable.

Nivel baixo:

– *Spam.*
– Escaneamento de redes (*scanning*).
– Análise de paquetes (*sniffing*).
– Outros.

4. *Nivel de impacto do ciberincidente*

O indicador de impacto dun ciberincidente determinarase avaliando as consecuencias que tal ciberincidente tivo nas funcións e actividades da organización afectada, nos seus activos ou nos individuos afectados. De acordo con iso, téñense en conta aspectos como

as consecuencias potenciais ou materializadas que provoca unha determinada ameaza nun sistema de información e/ou comunicación, así como na propia entidade afectada (organismos públicos ou privados, e particulares).

Os criterios empregados para a determinación do nivel de impacto asociado a un ciberincidente atenden aos seguintes parámetros:

– Impacto na seguridade nacional ou na seguridade cidadá.
– Efectos na prestación dun servizo esencial ou nunha infraestrutura crítica.
– Tipoloxía da información ou sistemas afectados.
– Grao de afectación ás instalacións da organización.
– Posible interrupción na prestación do servizo normal da organización.
– Tempo e custos propios e alleos ata a recuperación do normal funcionamento das instalacións.
– Perdas económicas.
– Extensión xeográfica afectada.
– Danos reputacionais asociados.

Os incidentes asociaranse a algún dos seguintes niveis de impacto: CRÍTICO, MOI ALTO, ALTO, MEDIO, BAIXO, SEN IMPACTO.

Nivel crítico:

– Afecta apreciablemente a seguridade nacional.
– Afecta a seguridade cidadá, con potencial perigo para a vida das persoas.
– Afecta unha infraestrutura crítica.
– Afecta sistemas clasificados SECRETO.
– Afecta máis do 90 % dos sistemas da organización.
– Interrupción na prestación do servizo superior a 24 horas e superior ao 50 % dos usuarios.
– O ciberincidente precisa para resolverse máis de 100 xornadas-persoa.
– Impacto económico superior ao 0,1 % do produto interior bruto (PIB) actual.
– Extensión xeográfica supranacional.
– Danos reputacionais moi elevados e cobertura continua en medios de comunicación internacionais.

Nivel moi alto:

– Afecta a seguridade cidadá con potencial perigo para bens materiais.
– Afecta apreciablemente actividades oficiais ou misións no estranxeiro.
– Afecta un servizo esencial.
– Afecta sistemas clasificados RESERVADO.
– Afecta máis do 75 % dos sistemas da organización.
– Interrupción na prestación do servizo superior a 8 horas e superior ao 35 % dos usuarios.
– O ciberincidente precisa para resolverse entre 30 e 100 xornadas-persoa.
– Impacto económico entre o 0,07 % e o 0,1 % do PIB actual.
– Extensión xeográfica superior a 4 comunidades autónomas (CC.AA.) ou un territorio de interese singular (TIS, considéranse como tal as cidades de Ceuta e Melilla e cada unha das illas que forman os arquipélagos das illas Baleares e das illas Canarias).
– Danos reputacionais á imaxe do país (marca España).
– Danos reputacionais elevados e cobertura continua en medios de comunicación nacionais.

Nivel alto:

– Afecta máis do 50 % dos sistemas da organización.
– Interrupción na prestación do servizo superior a 1 hora e superior ao 10 % de usuarios.

– O ciberincidente precisa para resolverse entre 5 e 30 xornadas-persoa.
– Impacto económico entre o 0,03 % e o 0,07 % do PIB actual.
– Extensión xeográfica superior a 3 comunidades autónomas.
– Danos reputacionais de difícil reparación, con eco mediático (ampla cobertura nos medios de comunicación) e que afecten a reputación de terceiros.

Nivel medio:

– Afecta máis do 20 % dos sistemas da organización.
– Interrupción na presentación do servizo superior ao 5 % de usuarios.
– O ciberincidente precisa para resolverse entre 1 e 5 xornadas-persoa.
– Impacto económico entre o 0,001 % e o 0,03 % do PIB actual.
– Extensión xeográfica superior a 2 comunidades autónomas.
– Danos reputacionais apreciables, con eco mediático (ampla cobertura nos medios de comunicación).

Nivel baixo:

– Afecta os sistemas da organización.
– Interrupción da prestación dun servizo.
– O ciberincidente precisa para resolverse menos de 1 xornada-persoa.
– Impacto económico entre o 0,0001 % e o 0,001 % do PIB actual.
– Extensión xeográfica superior a unha comunidade autónoma.
– Danos reputacionais puntuais, sen eco mediático.

Sen impacto:

– Non hai ningún impacto apreciable.

5. *Información que cómpre notificar á autoridade competente en caso de incidente*

O suxeito obrigado comunicará, na notificación inicial, todos aqueles campos acerca dos cales teña coñecemento nese momento de acordo coa seguinte táboa. Posteriormente será preceptivo cubrir todos os campos da táboa na notificación final do incidente.

Táboa 2. Información que cómpre notificar á autoridade competente en caso de incidente

Que notificar	Descrición
Asunto.	Frase que describa de forma xeral o incidente. Este campo herdarano todas as notificacións asociadas ao incidente.
OSE/PSD.	Denominación do operador de servizos esenciais ou provedor de servizos dixitais que notifica.
Sector estratéxico.	Enerxía, transporte, financeiro, etc.
Data e hora do incidente.	Indíquese coa maior precisión posible cando ocorreu o ciberincidente.
Data e hora de detección do incidente.	Indíquese coa maior precisión posible cando se detectou o ciberincidente.
Descrición.	Descríbase con detalle o sucedido.
Recursos tecnolóxicos afectados.	Indíquese a información técnica sobre o número e tipo de activos afectados polo ciberincidente, incluídos enderezos IP, sistemas operativos, aplicacións, versións…
Orixe do incidente.	Indíquese a causa do incidente, se se coñece. Apertura dun ficheiro sospeitoso, conexión dun dispositivo USB, acceso a unha páxina web maliciosa, etc.
Taxonomía (clasificación).	Posible clasificación e tipo de ciberincidente en función da taxonomía descrita.
Nivel de perigosidade.	Especifíquese o nivel de perigosidade asignado á ameaza.

Que notificar	Descrición
Nivel de impacto.	Especifíquese o nivel de impacto asignado ao incidente.
Impacto transfronteirizo.	Indíquese se o incidente ten impacto transfronteirizo nalgún Estado membro da Unión Europea.
Plan de acción e contramedidas.	Actuacións realizadas ata o momento en relación co ciberincidente. Indíquese o plan de acción seguido xunto coas contramedidas implantadas.
Afectación.	Indíquese se o afectado é unha empresa ou un particular, e as afectacións segundo o nivel de impacto asignado.
Medios necesarios para a resolución (J-P).	Capacidade empregada na resolución do incidente en xornadas-persoa.
Impacto económico estimado (se se coñece).	Custos asociados ao incidente, tanto de carácter directo como indirecto.
Extensión xeográfica (se se coñece).	Local, autonómico, nacional, supranacional, etc.
Danos reputacionais (se se coñecen).	Afectación á imaxe corporativa do operador.
Adxuntos.	Indíquese a relación de documentos adxuntos que se achegan para axudar a coñecer a causa do problema ou a súa resolución (capturas de pantalla, ficheiros de rexistro de información, correos electrónicos, etc.).
Regulación afectada.	ENS / RXPD / NIS / PIC / Outros.
Requírese actuación de FFCCSE.	Si / Non.

6. *Ventá temporal de reporte*

Todos aqueles suxeitos obrigados que se vexan afectados por un incidente de obrigada notificación á autoridade competente, a través do CSIRT de referencia, remitirán, en tempo e forma, aquelas notificacións inicial, intermedia e final requiridas de acordo coa seguinte ventá temporal de reporte.

– A notificación inicial é unha comunicación consistente en pór en coñecemento e alertar da existencia dun incidente.
– A notificación intermedia é unha comunicación mediante a cal se actualizarán os datos dispoñibles nese momento relativos ao incidente comunicado.
– A notificación final é unha comunicación final mediante a cal se amplían e confirman os datos definitivos relativos ao incidente comunicado.

Malia o anterior, achegaranse todas aquelas notificacións adicionais intermedias ou posteriores que se consideren necesarias.

Táboa 3. Ventá temporal de reporte

Nivel de perigosidade ou impacto	Notificación inicial	Notificación intermedia	Notificación final
CRÍTICO.	Inmediata.	24/48 horas.	20 días.
MOI ALTO.	Inmediata.	72 horas.	40 días.
ALTO.	Inmediata.	–	–
MEDIO.	–	–	–
BAIXO.	–	–	–

Os tempos reflectidos na táboa 3 para a «notificación intermedia» e a «notificación final» teñen como referencia o momento de remisión da «notificación inicial». A «notificación inicial» ten como referencia de tempo o momento en que se ten coñecemento do incidente.

7. *Definicións e conceptos*

A descrición das condutas aquí incluídas ten carácter técnico e enténdese polos meros efectos da notificación e xestión de ciberincidentes. Como tal, é independente tanto da cualificación dos feitos como da aplicación por parte da autoridade xudicial dos tipos penais establecidos na Lei orgánica 10/1995, do 23 de novembro, do Código penal.

Contido abusivo:

– Correo masivo non solicitado (*spam*): correo electrónico non solicitado que se envía a un gran número de usuarios, ou ben unha alta taxa de correos electrónicos enviados a un mesmo usuario nun curto espazo de tempo.

– Acoso: referido a acoso virtual ou ciberacoso, trátase do uso de medios de comunicación dixitais para acosar unha persoa, ou grupo de persoas, mediante ataques persoais, divulgación de información privada ou íntima, ou falsa.

– Extorsión: obrigar unha persoa ou mercantil, mediante o emprego de violencia ou intimidación, a realizar ou omitir actos coa intención de lle producir un prexuízo, ou ben con ánimo de lucro da que o provoca.

– Mensaxes ofensivas: comunicacións non esperadas ou desexadas, así como accións ou expresións que lesionan a dignidade doutra persoa, menoscabando a súa fama ou atentando contra a súa propia estimación.

– Delito: calquera acción tipificada como delito de acordo co establecido na Lei orgánica 10/1995, do 23 de novembro, do Código penal.

– Pederastia: calquera comportamento relacionado cos descritos no título VIII da Lei orgánica 10/1995, do 23 de novembro, do Código penal, relativos á captación ou utilización de menores de idade ou persoas con discapacidade necesitadas de especial protección en actos que atenten contra a súa indemnidade ou liberdade sexual.

– Racismo: calquera infracción penal, incluídas infraccións contra as persoas ou as propiedades, onde a vítima, o local ou o obxectivo da infracción se elixa pola súa, real ou percibida, conexión, simpatía, filiación, apoio ou pertenza a un grupo social, raza, relixión ou condición sexual.

– Apoloxía da violencia: exposición, ante unha concorrencia de persoas ou por calquera medio de difusión, de ideas ou doutrinas que enxalcen o crime ou enaltezan o seu autor.

Contido daniño:

– *Malware* (código daniño): palabra que deriva dos termos *malicious* e *software*. Calquera peza de *software* que leve a cabo accións como extracción de datos ou outro tipo de alteración dun sistema pode categorizarse como *malware*. Así pois, *malware* é un termo que engloba varios tipos de programas daniños.

– Virus: tipo de *malware* cuxo principal obxectivo é modificar ou alterar o comportamento dun sistema informático sen o permiso ou consentimento do usuario. Propágase mediante a execución no sistema de software, arquivos ou documentos con carga daniña, adquirindo a capacidade de replicarse dun sistema a outro. Os métodos máis comúns de infección danse a través de dispositivos extraíbles, descargas da internet e arquivos adxuntos en correos electrónicos. Non obstante, tamén se pode facer a través de *scripts*, documentos e vulnerabilidades XSS presentes na *web*. É destacable que un virus require a acción humana para a súa propagación a diferenza doutro *malware*; véxase Verme.

– Verme: programa malicioso que ten como característica principal o seu alto grao de dispersabilidade. O seu fin é replicarse a novos sistemas para infectalos e seguir replicándose a outros equipamentos informáticos aproveitándose de todo tipo de medios como o correo electrónico, IRC, FTP, correo electrónico, P2P e outros protocolos específicos ou amplamente utilizados.

– Troiano: tipo de *malware* que se enmascara como *software* lexítimo coa finalidade de convencer a vítima para que instale a peza no seu sistema. Unha vez instalado, o *software* daniño ten a capacidade de desenvolver actividade prexudicial en segundo plano.

Un troiano non depende dunha acción humana e non ten a capacidade de replicarse; non obstante, pode ter gran capacidade daniña nun sistema a modo de troianos ou explotando vulnerabilidades de *software*.

– Programa espía (*spyware*): tipo de *malware* que espía as actividades dun usuario sen o seu coñecemento ou consentimento. Estas actividades poden incluír *keyloggers*, monitorizacións, recolección de datos, así como roubo de datos. Os *spyware* pódense difundir como un troiano ou mediante explotación de *software*.

– *Rootkit*: conxunto de *software* daniño que permite o acceso privilexiado a áreas dunha máquina, mentres que ao mesmo tempo se oculta a súa presenza mediante a corrupción do sistema operativo ou outras aplicacións. Cómpre salientar que por máquina se entende todo o espectro de sistemas IT, desde *smartphones* ata ICS. O propósito dun *rootkit*, por tanto, é enmascarar eficazmente *payloads* e permitir a súa existencia no sistema.

– *Dialer*: tipoloxía de *malware* que se instala nunha máquina e, de forma automática e sen consentimento do usuario, realiza marcacións telefónicas a números de tarificación especial. Estas accións comportan custos económicos na vítima ao repercutir o importe da comunicación.

– *Ransomware*: englóbase baixo esta epígrafe aquel *malware* que infecta unha máquina, de modo que o usuario é incapaz de acceder aos datos almacenados no sistema. Normalmente, a vítima recibe posteriormente algún tipo de comunicación en que se coacciona para que se pague unha recompensa que permita acceder ao sistema e aos arquivos bloqueados.

– *Bot* daniño: unha *botnet* é o nome que se emprega para designar un conxunto de máquinas controladas remotamente con finalidade xeralmente maliciosa. Un *bot* é unha peza de *software* maliciosa que recibe ordes dun atacante principal que controla remotamente a máquina. Os servidores C&C habilitan o atacante para controlar os *bots* e que executen as ordes ditadas remotamente.

– RAT: do inglés *Remote Access Tool*, trátase dunha funcionalidade específica de control remoto dun sistema de información, que incorporan determinadas familias ou mostras de *software* daniño (*malware*).

– C&C: do inglés *Command and Control*, refírese a paneis de mando e control (tamén referenciados como C2), polo cal atacantes cibernéticos controlan determinados equipamentos *zombie* infectados con mostras da mesma familia de *software* daniño. O panel de comando e control actúa como punto de referencia, control e xestión dos equipamentos infectados.

– Conexión sospeitosa: todo intercambio de información no nivel de rede local ou pública, cuxa orixe ou destino non estean plenamente identificados, así como a lexitimidade destes.

Obtención de información:

– Escaneamento de portos (*scanning*): análise local ou remota, mediante *software*, do estado dos portos dunha máquina conectada a unha rede. A finalidade desta acción é a de obter información relativa á identificación dos servizos activos e as posibles vulnerabilidades que poidan existir na rede.

– Escaneamento de rede (*scanning*): análise local ou remota, mediante *software*, do estado dunha rede. A finalidade desta acción é a de obter información relativa á identificación dos servizos activos e as posibles vulnerabilidades que poidan existir na rede.

– Escaneamento de tecnoloxías: análise local ou remota, mediante *software*, das tecnoloxías presentes ou dispoñibles nunha rede determinada ou nun sistema de información concreto, mediante a cal se obteñen as referencias do *hardware/software* presente, así como a súa versión, e potenciais vulnerabilidades.

– Transferencia de zona DNS (AXFR IXFR): transacción dos servidores DNS utilizada para a replicación das bases de datos entre un servidor primario e os secundarios. Estas transaccións poden ser completas (AXFR) ou incrementais (IXFR).

– Análise de paquetes (*sniffing*): análise mediante *software* do tráfico dunha rede coa finalidade de capturar información. O tráfico que viaxe non cifrado poderá ser capturado e lido por un atacante.

– Enxeñaría social: técnicas que buscan a revelación de información sensible dun obxectivo, xeralmente mediante o uso de métodos persuasivos e con ausencia de vontade ou coñecemento da vítima.

– *Phishing*: estafa cometida a través de medios telemáticos mediante a cal o estafador intenta conseguir, de usuarios lexítimos, información confidencial (contrasinais, datos bancarios, etc.) de forma fraudulenta empregando métodos de enxeñaría social.

– *Spear Phishing*: variante do *phishing* mediante a cal o atacante focaliza a súa actuación sobre un obxectivo concreto.

Intrusións:

– Explotación: calquera práctica mediante a cal un atacante cibernético vulnera un sistema de información e/ou comunicación con fins ilícitos ou para os cales non está debidamente autorizado.

– Inxección SQL: tipo de explotación consistente na introdución de cadeas mal formadas de SQL ou cadeas que o receptor non espera ou controla debidamente, as cales provocan resultados non esperados na aplicación ou programa obxectivo, e pola cal o atacante produce efectos inesperados e para os cales non está autorizado no sistema obxectivo.

– *Cross Site Scripting* XSS (directo ou indirecto): ataque que trata de explotar unha vulnerabilidade presente en aplicacións web, pola cal un atacante inxecta sentenzas mal formadas ou cadeas que o receptor non espera ou controla debidamente.

– *Cross Site Request Forgery* (CSFR): falsificación de petición en sitios cruzados. É un tipo de *exploit* daniño dun sitio *web* en que comandos non autorizados son transmitidos por un usuario no cal o sitio web confía. Esta vulnerabilidade é coñecida tamén por outros nomes como XSRF, ligazón hostil, ataque dun clic, cabalgamento de sesión e ataque automático. Ao contrario que nos ataques XSS, os cales explotan a confianza que un usuario ten nun sitio en particular, o *Cross Site Request Forgery* explota a confianza que un sitio ten nun usuario en particular.

– *Defacement*: tipoloxía de ataque a sitios web en que se implementa un cambio na aparencia visual da páxina. Para iso adoitan empregarse técnicas como inxeccións SQL ou algún tipo de vulnerabilidade existente na páxina ou no servidor.

– Inclusión de ficheiros (RFI e LFI): vulnerabilidade que lle permite a un atacante mostrar ou executar arquivos remotos aloxados noutros servidores a causa dunha mala programación da páxina que contén funcións de inclusión de arquivos. A inclusión local de arquivos (LFI) é similar á vulnerabilidade de inclusión de arquivos remotos, excepto que, en lugar de incluír arquivos remotos, só se poden incluír arquivos locais, é dicir, arquivos no servidor actual para a súa execución.

– Evasión de sistemas de control: proceso polo cal unha mostra de software daniño, ou un conxunto de accións orquestradas por un atacante cibernético, conseguen vulnerar ou esquivar os sistemas ou as políticas de seguridade establecidas por un determinado sistema de información e comunicación.

– *Pharming*: ataque informático que aproveita vulnerabilidades dos servidores DNS (*Domain Name System*). Ao tratar de acceder o usuario ao sitio *web*, o navegador redirixirá automaticamente o usuario a un enderezo IP onde se aloxa unha *web* maliciosa que suplanta a auténtica e na cal o atacante poderá obter información sensible do usuario.

– Ataque por forza bruta: proceso polo cal un atacante trata de vulnerar un sistema de validación por credenciais de acceso, contrasinal ou similar, mediante o emprego de todas as combinacións posibles, co fin de acceder a sistemas de información e/ou comunicación para os cales non ten privilexios ou autorización.

– Ataque por dicionario: proceso polo cal un atacante trata de vulnerar un sistema de validación por credenciais de acceso, contrasinal ou similar, mediante o emprego dun dicionario previamente xerado con determinadas combinacións de caracteres, co fin de

acceder a sistemas de información e/ou comunicación para os cales non ten privilexios ou autorización.

– Roubo de credenciais de acceso: acceso ou subtracción non autorizada a credenciais de acceso a sistemas de información e/ou comunicación.

Dispoñibilidade:

– DoS (*Denial of Service*) ou ataque de denegación de servizo: conxunto de técnicas que teñen por obxectivo deixar un servidor inoperativo. Mediante este tipo de ataques búscase sobrecargar un servidor e desta forma impedir que os usuarios lexítimos poidan utilizar os servizos prestados por el. O ataque consiste en saturar con peticións de servizo o servidor, ata que este non pode atendelas, provocando o seu colapso.

– DDoS (*Distributed Denial of Service*) ou denegación distribuída de servizo: variante de DoS en que a remisión de peticións se leva a cabo de forma coordinada desde varios puntos cara a un mesmo destino. Para iso, empréganse redes de *bots*, xeralmente sen o coñecemento dos usuarios.

– Mala configuración: fallo de configuración no *software* que está directamente asociado cunha perda de dispoñibilidade dun servizo.

– Sabotaxe/terrorismo/vandalismo: ataques implementados co obxectivo de provocar a interrupción ou degradación da prestación dun servizo provocando danos relevantes na continuidade do servizo dunha institución ou danos reputacionais relevantes cometidos con propósitos ideolóxicos, políticos ou relixiosos.

– Disrupción sen intención daniña: accións que poden provocar a interrupción ou degradación da prestación dun servizo provocando danos relevantes na continuidade do servizo dunha institución ou danos reputacións relevantes.

– Inundación SYN ou UDP: procedementos usados para a realización de ataque DoS ou DDoS consistente en iniciar unha gran cantidade de sesións impedindo que o servidor atenda as peticións licitas.

– DNS *Open-Resolver*: servidor DNS capaz resolver consultas DNS recursivas procedentes de calquera orixe da internet. Este tipo de servidores adoita ser empregado por usuarios malintencionados para a realización de ataques DDoS.

Compromiso da información:

– Acceso non autorizado á información ou ciberespionaxe: proceso polo cal un usuario non autorizado accede a consultar contido para o cal non está autorizado.

– Modificación non autorizada de información: proceso polo cal un usuario non autorizado accede a modificar contido para o cal non está autorizado.

– Borrado non autorizado de información: proceso polo cal un usuario non autorizado accede a borrar contido para o cal non está autorizado.

– Exfiltración de información: proceso polo cal un usuario difunde información en canles ou fontes nas cales non está previsto ou autorizado que se comparta esa información.

– Acceso non autorizado a sistemas: proceso polo cal un usuario accede sen vulnerar ningún servizo, sistema ou rede, a sistemas de información e/ou comunicación para os cales non está debidamente autorizado, ou non ten autorización tácita ou manifesta.

– Ataque POODLE / ataque FREAK: proceso polo cal se consegue que un servidor faga uso dun protocolo de comunicacións non seguro, que orixinalmente non estaba previsto, co obxectivo de poder exfiltrar información.

Fraude:

– Uso non autorizado de recursos: emprego de tecnoloxías e/ou servizos por usuarios que non están debidamente autorizados pola dirección ou negociado competente.

– Suplantación de identidade: actividade maliciosa en que un atacante se fai pasar por outra persoa para cometer algún tipo de fraude ou acoso.

– Dereitos de propiedade intelectual: a propiedade intelectual é o conxunto de dereitos que corresponden aos autores e a outros titulares (artistas, produtores, organismos de radiodifusión…) respecto das obras e prestacións froito da súa creación.
– Outras fraudes: engano económico coa intención de conseguir un beneficio, e co cal alguén resulta prexudicado.

Vulnerabilidades:

– Tecnoloxía vulnerable: coñecemento, por parte dos administradores de tecnoloxías, servizos ou redes, de vulnerabilidades presentes nestas.
– Política de seguridade precaria: política de seguridade da organización deficiente, mediante a cal existe a posibilidade de que durante un espazo de tempo determinado atacantes cibernéticos realizasen accesos non autorizados a sistemas de información, sen que se poida determinar fidedignamente esta cuestión.

Outros:

– Ciberterrorismo: delitos informáticos previstos nos artigos 197 bis e ter e 264 a 264 *quater* da Lei orgánica 10/1995, do 23 de novembro, do Código penal, cando os ditos delitos se cometan coas finalidades previstas no artigo 573.1 do mesmo texto. Estas finalidades son:

• Subverter a orde constitucional, ou suprimir ou desestabilizar gravemente o funcionamento das institucións políticas ou das estruturas económicas ou sociais do Estado, ou obrigar os poderes públicos a realizar un acto ou a absterse de facelo.
• Alterar gravemente a paz pública.
• Desestabilizar gravemente o funcionamento dunha organización internacional.
• Provocar un estado de terror na poboación ou nunha parte dela.

– Danos informáticos PIC: delitos informáticos previstos nos artigos 264.2 3.º e 4.º da Lei orgánica 10/1995, do 23 de novembro, do Código penal, relacionados co borrado, danado, alteración, supresión ou inaccesibilidade de datos, programas informáticos ou documentos electrónicos dunha infraestrutura crítica, así como condutas graves relacionadas cos termos anteriores que afecten a prestación dun servizo esencial.
– APT (*Advanced Persistent Threat* ou ameaza persistente avanzada)/AVT (*Advanced Volatility Threat*): ataques dirixidos contra organizacións concretas, sustentados en mecanismos moi sofisticados de ocultación, anonimato e persistencia. Esta ameaza habitualmente emprega técnicas de enxeñaría social para conseguir os seus obxectivos, xunto co uso de procedementos de ataque coñecidos ou xenuínos.
– Dominios DGA: procedemento para xerar de forma dinámica dominios onde se aloxarán os servidores de comando e control, técnica usada en redes *botnet* para dificultar a súa detención.
– Criptografía: técnica que consiste en cifrar unha mensaxe, coñecida como texto en claro, e convertela nunha mensaxe cifrada ou criptograma, que resulta ilexible para todo aquel que non coñeza a clave mediante a cal foi cifrada.
– Proxy: ordenador, xeralmente un servidor, intermedio usado nas comunicacións entre outros dous equipamentos, normalmente usado de maneira transparente para o usuario.

Xeral:

– Ciberseguridade: a capacidade das redes e dos sistemas de información de resistir, cun nivel determinado de fiabilidade, toda acción que comprometa a dispoñibilidade, autenticidade, integridade ou confidencialidade dos datos almacenados, transmitidos ou tratados, ou os servizos correspondentes ofrecidos por tales redes e sistemas de información ou accesibles a través deles.
– Ciberespazo: espazo virtual que engloba todos os sistemas TIC. O ciberespazo apóiase na dispoñibilidade da internet como rede de redes, enriquecida con outras redes de transporte de datos.

– Redes e sistemas de información: enténdese por este concepto un dos tres seguintes puntos:

• As redes de comunicacións electrónicas, tal e como veñen definidas no número 31 do anexo II da Lei 9/2014, do 9 de maio, xeral de telecomunicacións.

• Todo dispositivo ou grupo de dispositivos interconectados ou relacionados entre si en que un ou varios deles realizan, mediante un programa, o tratamento automático de datos dixitais.

• Os datos dixitais almacenados, tratados, recuperados ou transmitidos mediante elementos recollidos anteriormente para o seu funcionamento, utilización, protección e mantemento.

– Seguridade en redes e sistemas de información: a capacidade das redes e dos sistemas de información de resistir, cun nivel determinado de fiabilidade, toda acción que comprometa a dispoñibilidade, autenticidade, integridade ou confidencialidade dos datos almacenados, transmitidos ou tratados, ou os servizos correspondentes ofrecidos por tales redes e sistemas de información ou accesibles a través deles.

– Operador de servizos esenciais: entidade pública ou privada que se identifique considerando os factores establecidos no artigo 6 do Real decreto lei 12/2018, do 7 de setembro, que preste os ditos servizos nalgún dos sectores estratéxicos definidos no anexo da Lei 8/2011, do 28 de abril.

– Servizo dixital: servizo da sociedade da información entendido no sentido recollido na letra a) do anexo da Lei 34/2002, do 11 de xullo, de servizos da sociedade da información e de comercio electrónico.

– Provedor de servizos dixitais: persoa xurídica que presta un servizo dixital.

– Ciberincidente: todo feito que teña efectos adversos reais na seguridade das redes e dos sistemas de información.

– Xestión de ciberincidentes: todos os procedementos seguidos para detectar, analizar e limitar un incidente e responder ante este.

– Ciberameaza: ameaza aos sistemas e servizos presentes no ciberespazo ou alcanzables a través deste.

– Taxonomía: clasificación ou ordenación en grupos de obxectos ou suxeitos que posúen unhas características comúns.

– RXPD: Regulamento xeral de protección de datos, Regulamento (UE) 2016/679 do Parlamento Europeo e do Consello, do 27 de abril de 2016, relativo á protección das persoas físicas no que respecta ao tratamento de datos persoais e á libre circulación destes datos e polo que se derroga a Directiva 95/46/CE.

– OpenPGP: estándar baseado no programa PGP, do inglés *Pretty Good Privacy*, cuxa finalidade é protexer a información mediante o uso de criptografía de clave pública, así como facilitar a autenticación de documentos grazas a sinaturas dixitais.

– *Webinject*: ferramenta gratuíta e de código aberto deseñada principalmente para automatizar a proba das aplicacións e dos servizos *web*.

– Telnet: protocolo de rede que permite acceder a outra máquina para manexala remotamente como se estivésemos sentados diante dela.

– RDP (*Remote Desktop Protocol*): protocolo propietario que permite a comunicación na execución dunha aplicación entre un terminal e un servidor.

– VNC (*Virtual Network Computing*): programa de software libre baseado nunha estrutura cliente-servidor que permite observar remotamente as accións do ordenador servidor a través dun ordenador cliente.

– SNMP (*Simple Network Management Protocol*): protocolo de rede utilizado para o intercambio de mensaxes para a administración de dispositivos en rede.

– Redis: motor de base de datos en memoria, baseado no almacenamento en táboas de *hashes*.

– ICMP (*Internet Control Message Protocol*): protocolo de control de mensaxes da internet.

– Copia de seguridade limpa: punto de restauración dun sistema da cal se ten a seguridade de que non está comprometida.