I. DISPOSICIÓNS XERAIS

XEFATURA DO ESTADO

12257 *Real decreto lei 12/2018, do 7 de setembro, de seguridade das redes e sistemas de información.*

I

A evolución das tecnoloxías da información e da comunicación, especialmente co desenvolvemento da internet, fixo que as redes e sistemas de información desempeñen actualmente un papel crucial na nosa sociedade, polo que a súa fiabilidade e seguridade son aspectos esenciais para o desenvolvemento normal das actividades económicas e sociais.

Por iso, os incidentes que afectan as redes e sistemas de información e alteran as ditas actividades representan unha grave ameaza, pois, tanto se son fortuítos como se proveñen de accións deliberadas, poden xerar perdas financeiras, menoscabar a confianza da poboación e, en definitiva, causar graves danos á economía e á sociedade, coa posibilidade de afectar a propia seguridade nacional na peor das hipóteses.

O carácter transversal e interconectado das tecnoloxías da información e da comunicación, que tamén caracteriza as súas ameazas e riscos, limita a eficacia das medidas que se empregan para contrarrestalos cando se toman de modo illado. Este carácter transversal tamén fai que se corra o risco de perder efectividade se os requisitos en materia de seguridade da información se definen de forma independente para cada un dos ámbitos sectoriais afectados.

Por tanto, é oportuno establecer mecanismos que, cunha perspectiva integral, permitan mellorar a protección fronte ás ameazas que afectan as redes e sistemas de información e facilitan a coordinación das actuacións realizadas nesta materia tanto a nivel nacional como con países da nosa contorna, en particular, dentro da Unión Europea.

II

Con este propósito dítase este real decreto lei, que traspón ao ordenamento xurídico español 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. O real decreto lei apóiase igualmente nas normas, nos instrumentos de resposta a incidentes e nos órganos de coordinación estatal existentes nesta materia, o que, xunto ás razóns sinaladas no punto I, xustifica que o seu contido transcenda o da propia directiva.

O real decreto lei aplicarase ás entidades que presten servizos esenciais para a comunidade e dependan das redes e sistemas de información para o desenvolvemento da súa actividade. O seu ámbito de aplicación esténdese a sectores que non están expresamente incluídos na directiva, para darlle a este real decreto lei un enfoque global, aínda que se preserva a súa lexislación específica. Adicionalmente, no caso das actividades de explotación das redes e de prestación de servizos de comunicacións electrónicas e dos recursos asociados, así como dos servizos electrónicos de confianza, expresamente excluídos da dita directiva, o real decreto lei aplicarase unicamente no que respecta aos operadores críticos.

O real decreto lei aplicarase, así mesmo, aos provedores de determinados servizos dixitais. A Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, sométeos a un réxime de harmonización máxima, equivalente a un regulamento, pois considérase que a súa regulación a escala nacional non sería efectiva por teren un carácter intrinsecamente transnacional. A función das autoridades nacionais limítase, por

tanto, a que os provedores establecidos no seu país supervisen a súa aplicación e se coordinen coas autoridades correspondentes doutros países da Unión Europea.

Seguindo a citada directiva, o real decreto lei identifica os sectores nos cales é necesario garantir a protección das redes e sistemas de información, e establece procedementos para identificar os servizos esenciais ofrecidos nos ditos sectores, así como os principais operadores que prestan os ditos servizos, que son, en definitiva, os destinatarios deste real decreto lei.

Os operadores de servizos esenciais e os provedores de servizos dixitais deberán adoptar medidas adecuadas para xestionar os riscos que se presenten para a seguridade das redes e sistemas de información que utilicen, aínda que a súa xestión estea externalizada. As obrigas de seguridade que asuman deberán ser proporcionadas ao nivel de risco que afronten e estar baseadas nunha avaliación previa destes. As normas de desenvolvemento deste real decreto lei poderán concretar as obrigas de seguridade exixibles aos operadores de servizos esenciais, incluídas, se é o caso, as inspeccións que cumpra realizar ou a participación en actividades e exercicios de xestión de crise.

O real decreto lei require, así mesmo, que os operadores de servizos esenciais e os provedores de servizos dixitais notifiquen os incidentes que sufran nas redes e servizos de información que empregan para a prestación dos servizos esenciais e dixitais e teñan efectos perturbadores significativos neles, ao tempo que prevé a notificación dos sucesos ou incidencias que poidan afectar os servizos esenciais pero que aínda non tivesen un efecto adverso real sobre aqueles, e perfila os procedementos de notificación.

A notificación de incidentes forma parte da cultura de xestión de riscos que a directiva e o real decreto lei fomentan. Por iso, o real decreto lei protexe a entidade notificante e o persoal que informe sobre incidentes ocorridos; reserva para si a información confidencial da súa divulgación ao público ou a outras autoridades distintas da notificada e permítese a notificación de incidentes cando non sexa obrigada a súa comunicación.

O real decreto lei recalca a necesidade de ter en conta os estándares europeos e internacionais, así como as recomendacións que emanen do grupo de cooperación e da rede de CSIRT (*Computer Security Incident Response Team)* establecidos no ámbito comunitario pola directiva, con vistas a aplicar as mellores prácticas aprendidas nestes foros e contribuír ao impulso do mercado interior e á participación da nosas empresas nel.

Co fin de aumentar a súa eficacia e, ao tempo, reducir as cargas administrativas e económicas que estas obrigas supoñen para as entidades afectadas, este real decreto lei trata de garantir a súa coherencia coas que derivan da aplicación doutras normativas en materia de seguridade da información, tanto de carácter horizontal como sectorial, e a coordinación na súa aplicación coas autoridades responsables en cada caso.

Respecto das normas horizontais, destacan os vínculos establecidos coas leis 8/2011, do 28 de abril, pola que se establecen medidas para a protección das infraestruturas críticas, e 36/2015, do 28 de setembro, de seguridade nacional, e co Real decreto 3/2010, do 8 de xaneiro, polo que se regula o Esquema nacional de seguridade no ámbito da Administración electrónica, como normativa especial en materia de seguridade dos sistemas de información do sector público.

Así, aproxímase o ámbito de aplicación deste real decreto lei ao da Lei 8/2011, do 28 de abril, engadindo aos sectores previstos pola Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, os sectores estratéxicos adicionais recollidos nesa lei; apóiase nela para definir o concepto de «servizo esencial» e atribúese aos seus órganos colexiados a determinación dos servizos esenciais e dos operadores de servizos esenciais suxeitos ao presente real decreto lei. Tendo en conta a Lei 36/2015, do 28 de setembro, atribúese ao Consello de Seguridade Nacional a función de actuar como punto de contacto con outros países da Unión Europea e un papel coordinador da política de ciberseguridade a través da Estratexia de ciberseguridade nacional.

III

A Estratexia de ciberseguridade nacional con que España conta desde o ano 2013 senta as prioridades, obxectivos e medidas adecuadas para alcanzar e manter un elevado

nivel de seguridade das redes e sistemas de información. A dita estratexia seguirá desenvolvendo o marco institucional da ciberseguridade que este real decreto lei bosquexa, composto polas autoridades públicas competentes e os CSIRT de referencia, por unha parte, e a cooperación público-privada, por outra.

As autoridades competentes exercerán as funcións de vixilancia derivadas deste real decreto lei e aplicarán o réxime sancionador cando proceda. Así mesmo, promoverán o desenvolvemento das obrigas que o real decreto lei impón, en consulta co sector e coas autoridades que exerzan competencias por razón da materia cando se refiran a sectores específicos, para evitar a existencia de obrigas duplicadas, innecesarias ou excesivamente onerosas.

Os CSIRT son os equipos de resposta a incidentes que analizan riscos e supervisan incidentes a escala nacional, difunden alertas sobre eles e achegan solucións para mitigar os seus efectos. O termo CSIRT é o usado comunmente en Europa en lugar do termo protexido CERT (*Computer Emergency Response Team),* rexistrado en EE.UU.

O real decreto lei delimita o ámbito funcional de actuación dos CSIRT de referencia previstos nela. Os ditos CSIRT son a porta de entrada das notificacións de incidentes, o que permitirá organizar rapidamente a resposta a eles, pero o destinatario das notificacións é a autoridade competente respectiva, que terá en conta esta información para a supervisión dos operadores. En todo caso, o operador é responsable de resolver os incidentes e repoñer as redes e sistemas de información afectados ao seu funcionamento ordinario.

Prevese a utilización dunha plataforma común para a notificación de incidentes, de tal maneira que os operadores non deban efectuar varias notificacións en función da autoridade a que se deban dirixir. Esta plataforma poderá ser empregada tamén para a notificación de vulneracións da seguridade de datos persoais segundo o 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.

IV

Este real decreto lei consta de sete títulos que conteñen, en primeiro lugar, as definicións dos termos que se usan ao longo do texto, a salvagarda de funcións estatais esenciais, como a seguridade nacional, e outras disposicións xerais. A continuación, no título II determínanse a forma e criterios de identificación dos servizos esenciais e dos operadores que os presten aos cales se aplicará o real decreto lei. A orde en que se procederá á súa identificación por primeira vez establécese na disposición adicional primeira do real decreto lei. O título III recolle o marco estratéxico e institucional da seguridade das redes e sistemas de información que se describiu anteriormente. Dedícase un precepto específico á cooperación entre autoridades públicas, como alicerce dun exercicio adecuado das diferentes competencias concorrentes sobre a materia.

O título IV ocúpase das obrigas de seguridade dos operadores e nel prevese a aplicación preferente de normas sectoriais que impoñan obrigas equivalentes ás previstas neste real decreto lei, sen prexuízo da coordinación exercida polo Consello de Seguridade Nacional e do deber de cooperación coas autoridades competentes en virtude deste real decreto lei.

No título V, o máis extenso, regúlase a notificación de incidentes e préstase atención aos incidentes con impacto transfronteirizo e á información e coordinación con outros Estados da Unión Europea para a súa xestión. No título VI, dispóñense as potestades de inspección e control das autoridades competentes e a cooperación coas autoridades nacionais doutros Estados membros e, no título VII, tipifícanse as infraccións e sancións deste real decreto lei. Neste aspecto, o real decreto lei decántase por impulsar a emenda da infracción antes que o castigo, o cal, se é necesario dispensalo, será efectivo, proporcionado e disuasorio, en liña co ordenado pola Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016.

O real decreto lei féchase cunha parte final que inclúe as disposicións adicionais e derradeiras necesarias para completar a regulación.

Esta disposición foi sometida ao procedemento de información de normas regulamentarias técnicas e de regulamentos relativos aos servizos da sociedade da información, previsto na Directiva (UE) 2015/1535 do Parlamento Europeo e do Consello, do 9 de setembro de 2015, pola que se establece un procedemento de información en materia de regulamentacións técnicas e de regras relativas aos servizos da sociedade da información, así como no Real decreto 1337/1999, do 31 de xullo, polo que se regula a remisión de información en materia de normas e regulamentacións técnicas e regulamentos relativos aos servizos da sociedade da información. Así mesmo, 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, conforme os cales deben actuar as administracións públicas no exercicio da iniciativa lexislativa, como son os principios de necesidade, eficacia, proporcionalidade, seguridade xurídica, transparencia e eficiencia.

Este real decreto lei dítase en virtude das competencias exclusivas atribuídas ao Estado en materia de réxime xeral de telecomunicacións e seguridade pública polo artigo 149.1.21.ª e 29.ª da Constitución.

O real decreto lei constitúe un instrumento constitucionalmente lícito, sempre que o fin que xustifica a lexislación de urxencia, sexa, tal como reiteradamente exixiu o noso Tribunal Constitucional (sentenzas 6/1983, do 4 de febreiro, F. 5; 11/2002, do 17 de xaneiro, F. 4, 137/2003, do 3 de xullo, F. 3 e 189/2005, do 7 xullo, F.3), acorrer a unha situación concreta, dentro dos obxectivos gobernamentais que, por razóns difíciles de prever, require unha acción normativa inmediata nun prazo máis breve que o requirido pola vía normal ou polo procedemento de urxencia para a tramitación parlamentaria das leis.

Por outro lado, a utilización do instrumento xurídico do real decreto lei no presente caso, ademais, queda xustificada pola doutrina do Tribunal Constitucional, que, na súa Sentenza 1/2012, do 13 de xaneiro, avalou a concorrencia do presuposto habilitante da extraordinaria e urxente necesidade do artigo 86.1 da Constitución cando concorra o atraso na transposición de directivas.

En efecto, o prazo de transposición da mencionada Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, encóntrase xa vencido o 9 de maio de 2018. A finalización do prazo de transposición desta directiva motivou a iniciación por parte da Comisión Europea dun procedemento formal de infracción n.º 2018/168.

En consecuencia, enténdese que, no conxunto e en cada unha das medidas que se adoptan mediante o real decreto lei proxectado, concorren, pola súa natureza e finalidade, as circunstancias de extraordinaria e urxente necesidade que exixe o artigo 86 da Constitución como presupostos habilitantes para a aprobación dun real decreto lei.

Na súa virtude, facendo uso da autorización contida no artigo 86 da Constitución española, por proposta da vicepresidenta do Goberno e ministra da Presidencia, Relacións coas Cortes e Igualdade, do ministro do Interior e da ministra de Economía e Empresa e logo de deliberación do Consello de Ministros, na súa reunión do día 7 de setembro de 2018,

DISPOÑO:

TÍTULO I

Disposicións xerais

Artigo 1. *Obxecto.*

1. O presente real decreto lei ten por obxecto regular a seguridade das redes e sistemas de información utilizados para a provisión dos servizos esenciais e dos servizos dixitais e establecer un sistema de notificación de incidentes.

2. Así mesmo, establece un marco institucional para a aplicación deste real decreto lei e a coordinación entre autoridades competentes e cos órganos de cooperación relevantes no ámbito comunitario.

Artigo 2. *Ámbito de aplicación.*

1. Este real decreto lei 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, considerados conforme se determina no artigo 3 e), que sexan mercados en liña, motores de busca en liña e servizos de computación na nube.

2. Estarán sometidos a este real decreto lei:

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 lei será de aplicación aos servizos esenciais que os operadores residentes ou domiciliados noutro Estado ofrezan a través dun establecemento permanente situado en España.

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 lei 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.

Artigo 3. *Definicións.*

Para os efectos deste real decreto lei, entenderanse por:

a) Redes e sistemas de información, calquera dos elementos seguintes:

1.º 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;

2.º Todo dispositivo ou grupo de dispositivos interconectados ou relacionados entre si no que un ou varios deles realicen, mediante un programa, o tratamento automático de datos dixitais;

3.º Os datos dixitais almacenados, tratados, recuperados ou transmitidos mediante os elementos recollidos nos números 1.º e 2.º anteriores, incluídos os necesarios para o funcionamento, utilización, protección e mantemento dos ditos elementos.

b) Seguridade das redes e sistemas de información: a capacidade das redes e 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.

c) Servizo esencial: servizo necesario para o mantemento das funcións sociais básicas, a saúde, a seguridade, o benestar social e económico dos cidadáns, ou o eficaz funcionamento das institucións do Estado e das administracións públicas, que dependa para a súa provisión de redes e sistemas de información.

d) Operador de servizos esenciais: entidade pública ou privada que se identifique considerando os factores establecidos no artigo 6 deste real decreto lei e que preste os ditos servizos nalgún dos sectores estratéxicos definidos no anexo da Lei 8/2011, do 28 de abril.

e) 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.

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

g) Risco: toda circunstancia ou feito razoablemente identificable que teña un posible efecto adverso na seguridade das redes e sistemas de información. Pódese cuantificar como a probabilidade de materialización dunha ameaza que produza un impacto en termos de operatividade, de integridade física de persoas ou material ou de imaxe.

h) Incidente: suceso inesperado ou non desexado con consecuencias en detrimento da seguridade das redes e sistemas de información.

i) Xestión de incidentes: procedementos seguidos para detectar, analizar e limitar un incidente e responder ante este.

j) Representante: persoa física ou xurídica establecida na Unión Europea que foi designada expresamente para actuar por conta dun provedor de servizos dixitais non establecido na Unión Europea, a que, en substitución do provedor de servizos dixitais, se poida dirixir unha autoridade competente nacional ou un CSIRT, en relación coas obrigas que, en virtude deste real decreto lei, ten o provedor de servizos dixitais.

k) Norma técnica: unha norma no sentido do artigo 2.1 do Regulamento (UE) n.º 1025/2012 do Parlamento Europeo e do Consello, do 25 de outubro de 2012, sobre a normalización europea.

l) Especificación: unha especificación técnica no sentido do artigo 2.4 do Regulamento (UE) n.º 1025/2012 do Parlamento Europeo e do Consello, do 25 de outubro de 2012.

m) Punto de intercambio da internet («IXP», polas súas siglas en inglés de «Internet eXchange Point»): unha instalación de rede que permite interconectar máis de dous sistemas autónomos independentes, principalmente para facilitar o intercambio de tráfico da internet. Un IXP permite interconectar sistemas autónomos sen requirir que o tráfico da internet que pasa entre calquera par de sistemas autónomos participantes pase por un terceiro sistema autónomo, e sen modificar nin interferir doutra forma no dito tráfico.

n) Sistema de nomes de dominio («DNS», polas súas siglas en inglés de «Domain Name System»): sistema distribuído xerarquicamente que responde a consultas proporcionando información asociada a nomes de dominio, en particular, a relativa aos identificadores utilizados para localizar e direccionar equipamentos na internet.

o) Provedor de servizos de DNS: entidade que presta servizos de DNS na internet.

p) Rexistro de nomes de dominio de primeiro nivel: entidade que administra e dirixe o Rexistro de nomes de dominio da internet nun dominio específico de primeiro nivel.

q) Mercado en liña: servizo dixital que permite aos consumidores e aos empresarios, tal e como se definen respectivamente nos artigos 3 e 4 do texto refundido da Lei xeral para a defensa dos consumidores e usuarios e outras leis complementarias, aprobado mediante o Real decreto lexislativo 1/2007, do 16 de novembro, celebrar entre si contratos de compravenda ou de prestación de servizos en liña con empresarios, xa sexa nun sitio web específico do servizo de mercado en liña ou nun sitio web dun empresario que utilice servizos informáticos proporcionados para o efecto polo provedor do servizo de mercado en liña.

r) Motor de busca en liña: servizo dixital que permite aos usuarios facer buscas de, en principio, todos os sitios web ou de sitios web nunha lingua en concreto, mediante unha consulta sobre un tema en forma de palabra clave, frase ou outro tipo de entrada, e que, en resposta, mostra ligazóns nas cales se pode encontrar información relacionada co contido solicitado.

s) Servizo de computación na nube: servizo dixital que fai posible o acceso a un conxunto modulable e elástico de recursos de computación que se poden compartir.

Artigo 4. *Directrices e orientacións comunitarias.*

Na aplicación deste real decreto lei e na elaboración dos regulamentos e guías previstos nel teranse en conta os actos de execución da Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016, así como todas as recomendacións e directrices emanadas do grupo de cooperación establecido polo artigo 11 da citada directiva, e a información sobre boas prácticas compiladas polo dito grupo e a rede de CSIRT, regulado no artigo 12 daquela.

Artigo 5. *Salvagarda de funcións estatais esenciais.*

O disposto neste real decreto lei entenderase sen prexuízo das accións emprendidas para salvagardar a seguridade nacional e as funcións estatais esenciais nas cales se inclúen as dirixidas a protexer a información clasificada ou cuxa revelación for contraria aos intereses esenciais do Estado, ou as que teñan como propósito o mantemento da orde pública, a detección, investigación e persecución dos delitos, e o axuizamento dos seus autores.

TÍTULO II

Servizos esenciais e servizos dixitais

Artigo 6. *Identificación de servizos esenciais e de operadores de servizos esenciais.*

1. A identificación dos servizos esenciais e dos operadores que os presten efectuarana os órganos e polos procedementos previstos na Lei 8/2011, do 28 de abril, e na súa normativa de desenvolvemento.

A relación dos servizos esenciais e dos operadores dos ditos servizos actualizarase, para cada sector, cunha frecuencia bienal, en conxunción coa revisión dos plans estratéxicos sectoriais previstos na Lei 8/2011, do 28 de abril.

Identificarase un operador como operador de servizos esenciais se un incidente sufrido polo operador pode chegar a ter efectos perturbadores significativos na prestación do servizo, para o que se terán en conta, cando menos, os seguintes factores:

a) En relación coa importancia do servizo prestado:

1.º A dispoñibilidade de alternativas para manter un nivel suficiente de prestación do servizo esencial;

2.º A valoración do impacto dun incidente na provisión do servizo, avaliando a extensión ou zonas xeográficas que se poderían ver afectadas polo incidente; a dependencia doutros sectores estratéxicos respecto do servizo esencial ofrecido pola entidade e a repercusión, en termos de grao e duración, do incidente nas actividades económicas e sociais ou na seguridade pública.

b) En relación cos clientes da entidade avaliada:

1.º O número de usuarios que confían nos servizos prestados por ela;

2.º A súa cota de mercado.

Regulamentariamente poderán engadirse factores específicos do sector para determinar se un incidente podería ter efectos perturbadores significativos.

2. No caso de tratarse dun operador crítico designado en cumprimento da Lei 8/2011, do 28 de abril, bastará con que se constate a súa dependencia das redes e sistemas de información para a provisión do servizo esencial de que se trate.

3. Na identificación dos servizos esenciais e dos operadores de servizos esenciais teranse en consideración, na maior medida posible, as recomendacións pertinentes que adopte o grupo de cooperación.

4. Cando un operador de servizos esenciais ofreza servizos e outros Estados membros da Unión Europea, informaranse os puntos de contacto único dos ditos Estados sobre a intención de identificalo como operador de servizos esenciais.

Artigo 7. *Comunicación de actividade polos provedores de servizos dixitais.*

Os provedores de servizos dixitais sinalados no artigo 2 deberán comunicar a súa actividade á autoridade competente no prazo de tres meses desde que a inicien, para os meros efectos do seu coñecemento.

TÍTULO III

Marco estratéxico e institucional

Artigo 8. *Marco estratéxico de seguridade das redes e sistemas de información.*

A Estratexia de ciberseguridade nacional, ao abeiro e aliñada coa Estratexia de seguridade nacional, enmarca os obxectivos e as medidas para alcanzar e manter un elevado nivel de seguridade das redes e sistemas de información.

A Estratexia de ciberseguridade nacional abordará, entre outras cuestións, as establecidas no artigo 7 da Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016.

Para tal efecto, o Consello de Seguridade Nacional impulsará a revisión da Estratexia de ciberseguridade nacional, de conformidade co disposto no artigo 21.1 e) da Lei 36/2015, do 28 de setembro, de seguridade nacional.

Artigo 9. *Autoridades competentes.*

1. Son autoridades competentes en materia de seguridade das redes e sistemas de información as seguintes:

a) Para os operadores de servizos esenciais:

1.º No caso de que estes sexan, ademais, designados como operadores críticos conforme a Lei 8/2011, do 28 de abril, e a súa normativa de desenvolvemento, con independencia do sector estratéxico en que se realice tal designación: a Secretaría de Estado de Seguridade, do Ministerio do Interior, a través do Centro Nacional de Protección de Infraestruturas e Ciberseguridade (CNPIC).

2.º No caso de que non sexan operadores críticos: a autoridade sectorial correspondente por razón da materia, segundo se determine regulamentariamente.

b) Para os provedores de servizos dixitais: a Secretaría de Estado para o Avance Dixital, do Ministerio de Economía e Empresa.

c) Para os operadores de servizos esenciais e provedores de servizos dixitais que. non sendo operadores críticos. se encontren comprendidos no ámbito de aplicación da Lei 40/2015, do 1 de outubro, de réxime xurídico do sector público: o Ministerio de Defensa, a través do Centro Criptolóxico Nacional.

2. O Consello de Seguridade Nacional, a través do seu comité especializado en materia de ciberseguridade, establecerá os mecanismos necesarios para a coordinación das actuacións das autoridades competentes.

Artigo 10. *Funcións das autoridades competentes.*

As autoridades competentes exercerán as seguintes funcións:

a) Supervisar o cumprimento por parte dos operadores de servizos esenciais e dos provedores de servizos dixitais das obrigas que se determinen, conforme o establecido no título VI.

b) Establecer canles de comunicación oportunas cos operadores de servizos esenciais e cos provedores de servizos dixitais que, se é o caso, serán desenvolvidos regulamentariamente.

c) Coordinarse cos CSIRT de referencia a través dos protocolos de actuación que, se é o caso, se desenvolverán regulamentariamente.

d) Recibir as notificacións sobre incidentes que sexan presentadas no marco deste real decreto lei, a través dos CSIRT de referencia, conforme o establecido no título V.

e) Informar o punto de contacto único sobre as notificacións de incidentes presentadas no marco deste real decreto lei, conforme o establecido no artigo 27.

f) Informar, se é o caso, o público sobre determinados incidentes, cando a difusión da dita información sexa necesaria para evitar un incidente ou xestionar un que xa se producise, conforme o establecido no artigo 26.

g) Cooperar, no ámbito de aplicación deste real decreto lei, coas autoridades competentes en materia de protección de datos de carácter persoal, seguridade pública, seguridade cidadá e seguridade nacional, así como coas autoridades sectoriais correspondentes, conforme o establecido nos artigos 14 e 29.

h) Establecer obrigas específicas para garantir a seguridade das redes e sistemas de información e sobre notificación de incidentes, e ditar instrucións técnicas e guías orientativas para detallar o contido das ditas obrigas, conforme o establecido nos artigos 16 e 19.

i) Exercer a potestade sancionadora nos casos previstos no presente real decreto lei, conforme o establecido no título VII.

j) Promover o uso de normas e especificacións técnicas, de acordo co establecido no artigo 17.

k) Cooperar coas autoridades competentes doutros Estados membros da Unión Europea na identificación de operadores de servizos esenciais entre entidades que ofrezan os ditos servizos en varios Estados membros.

l) Informar o punto de contacto único sobre incidentes que poidan afectar outros Estados membros, nos termos previstos no artigo 25.

Artigo 11. *Equipos de resposta a incidentes de seguridade informática de referencia.*

1. Son equipos de resposta a incidentes de seguridade informática (CSIRT) de referencia en materia de seguridade das redes e sistemas de información, os seguintes:

a) No concernente ás relacións cos operadores de servizos esenciais:

1.º O CCN-CERT, do Centro Criptolóxico Nacional, a que corresponde a comunidade de referencia constituída polas entidades do ámbito subxectivo de aplicación da Lei 40/2015, do 1 de outubro.

2.º O INCIBE-CERT, do Instituto Nacional de Ciberseguridade de España, a que corresponde a comunidade de referencia constituída por aquelas entidades non incluídas no ámbito subxectivo de aplicación da Lei 40/2015, do 1 de outubro.

O INCIBE-CERT será operado conxuntamente polo INCIBE e o CNPIC en todo o que se refira á xestión de incidentes que afecten os operadores críticos.

3.º O ESPDEF-CERT, do Ministerio de Defensa, que cooperará co CCN-CERT e co INCIBE-CERT naquelas situacións que estes requiran en apoio dos operadores de servizos esenciais e, necesariamente, naqueles operadores que teñan incidencia na defensa nacional e que regulamentariamente se determinen.

b) No concernente ás relacións cos provedores de servizos dixitais que non estivesen comprendidos na comunidade de referencia do CCN-CERT: o INCIBE-CERT.

O INCIBE-CERT será, así mesmo, equipo de resposta a incidentes de referencia para os cidadáns, entidades de dereito privado e outras entidades non incluídas anteriormente neste punto 1.

2. Os CSIRT de referencia coordinaranse entre si e co resto de CSIRT nacionais e internacionais na resposta aos incidentes e xestión de riscos de seguridade que lles correspondan. Nos supostos de especial gravidade que regulamentariamente se determinen e que requiran un nivel de coordinación superior ao necesario en situacións ordinarias, o CCN-CERT exercerá a coordinación nacional da resposta técnica dos CSIRT.

Cando as actividades que desenvolvan poidan afectar dalgunha maneira un operador crítico, os CSIRT de referencia coordinaranse co Ministerio do Interior, a través da Oficina de Coordinación Cibernética do Centro Nacional de Protección de Infraestruturas e Ciberseguridade (CNPIC), da forma que regulamentariamente se determine.

Artigo 12. *Requisitos e funcións dos CSIRT de referencia.*

1. Os CSIRT deberán reunir as seguintes condicións:

a) Garantirán un elevado nivel de dispoñibilidade dos seus servizos de comunicacións evitando os fallos ocasionais e contarán con varios medios para que se poida contactar con eles e poidan contactar outros en todo momento. Ademais, as canles de comunicación estarán claramente especificadas e serán ben coñecidas dos grupos de usuarios e dos socios colaboradores.

b) As súas instalacións e as dos sistemas de información de apoio estarán situadas en lugares seguros.

c) Garantirán a continuidade das actividades. Para iso:

1.º Estarán dotadas dun sistema adecuado para xestionar e canalizar as solicitudes co fin de facilitar os traspasos.

2.º Contarán con persoal suficiente para garantir a súa dispoñibilidade en todo momento.

3.º Terán acceso a infraestruturas de comunicación cuxa continuidade estea asegurada. Para tal fin, disporán de sistemas redundantes e espazos de traballo de reserva.

d) Deberán ter a capacidade de participar, cando o desexen, en redes de cooperación internacional.

2. Os CSIRT desempeñarán, como mínimo, as seguintes funcións:

a) Supervisar incidentes a escala nacional.

b) Difundir alertas temperás, alertas, avisos e información sobre riscos e incidentes entre os interesados.

c) Responder a incidentes.

d) Efectuar unha análise dinámica de riscos e incidentes e de coñecemento da situación.

e) Participar na rede de CSIRT.

3. Os CSIRT establecerán relacións de cooperación co sector privado. Co fin de facilitar a cooperación, os CSIRT fomentarán a adopción e utilización de prácticas comúns ou normalizadas de:

a) Procedementos de xestión de incidentes e riscos.
b) Sistemas de clasificación de incidentes, riscos e información.

Artigo 13. *Punto de contacto único.*

O Consello de Seguridade Nacional exercerá, a través do Departamento de Seguridade Nacional, unha función de enlace para garantir a cooperación transfronteiriza das autoridades competentes designadas conforme o artigo 9 coas autoridades competentes doutros Estados membros da Unión Europea, así como co grupo de cooperación e a rede de CSIRT.

Artigo 14. *Cooperación con outras autoridades con competencias en seguridade da información e coas autoridades sectoriais.*

1. As autoridades competentes, os CSIRT de referencia e o punto de contacto único consultarán, cando proceda, cos órganos con competencias en materia de seguridade nacional, seguridade pública, seguridade cidadá e protección de datos de carácter persoal e colaborarán con elas no exercicio das súas respectivas funcións.
2. Consultarán, así mesmo, cando proceda, cos órganos con competencias por razón da materia en cada un dos sectores incluídos no ámbito de aplicación deste real decreto lei, e colaborarán con eles no exercicio das súas funcións.
3. Cando os incidentes notificados presenten caracteres de delito, as autoridades competentes e os CSIRT de referencia darán conta diso, a través da Oficina de Coordinación Cibernética do Ministerio do Interior, ao Ministerio Fiscal, para os efectos oportunos, trasladándolle ao tempo canta información posúan en relación con iso.

Artigo 15. *Confidencialidade da información sensible.*

Sen prexuízo do disposto no artigo 5, as autoridades competentes, os CSIRT de referencia e o punto de contacto único preservarán como corresponda en dereito a seguridade e os intereses comerciais dos operadores de servizos esenciais e provedores de servizos dixitais, así como a confidencialidade da información que soliciten destes no exercicio das funcións que lles encomenda o presente real decreto lei.

Cando iso sexa necesario, o intercambio de información sensible limitarase a aquela que sexa pertinente e proporcionada para a finalidade do dito intercambio.

TÍTULO IV

Obrigas de seguridade

Artigo 16. *Obrigas de seguridade dos operadores de servizos esenciais e dos provedores de servizos dixitais.*

1. Os operadores de servizos esenciais e os provedores de servizos dixitais deberán adoptar medidas técnicas e de organización, adecuadas e proporcionadas, para xestionar os riscos que se presenten para a seguridade das redes e sistemas de información utilizados na prestación dos servizos suxeitos a este real decreto lei.

Sen prexuízo do seu deber de notificar incidentes conforme o título V, deberán tomar medidas adecuadas para previr e reducir ao mínimo o impacto dos incidentes que os afecten.

2. O desenvolvemento regulamentario deste real decreto lei preverá as medidas necesarias para o cumprimento do preceptuado no punto anterior por parte dos operadores de servizos esenciais.
3. Os operadores de servizos esenciais designarán e comunicarán á autoridade competente, no prazo que regulamentariamente se estableza, a persoa, unidade ou órgano colexiado responsable da seguridade da información, como punto de contacto e de coordinación técnica con aquela.

As súas funcións específicas serán as previstas regulamentariamente.

4. As autoridades competentes poderán establecer mediante orde ministerial obrigas específicas para garantir a seguridade das redes e sistemas de información empregados polos operadores de servizos esenciais. Así mesmo, poderán ditar instrucións técnicas e guías orientativas para detallar o contido das ditas ordes.

Ao elaborar as disposicións regulamentarias, instrucións e guías, terán en conta as obrigas sectoriais, as directrices relevantes que se adopten no grupo de cooperación e os requisitos en materia de seguridade da información a que estiver sometido o operador en virtude doutras normas, como a Lei 8/2011, do 28 de abril, e o Esquema nacional de seguridade, aprobado polo Real decreto 3/2010, do 8 de xaneiro.

5. As autoridades competentes deberán coordinarse entre si e cos diferentes órganos sectoriais con competencias por razón da materia no relativo ao contido e á aplicación das ordes, instrucións técnicas e guías orientativas que diten nos seus respectivos ámbitos de competencia, con obxecto de evitar duplicidades nas obrigas exixibles e facilitar o seu cumprimento aos operadores de servizos esenciais.

6. Os provedores de servizos dixitais determinarán as medidas de seguridade que aplicarán, tendo en conta, como mínimo, os avances técnicos e os seguintes aspectos:

a) A seguridade dos sistemas e instalacións;
b) A xestión de incidentes;
c) A xestión da continuidade das actividades;
d) A supervisión, auditorías e probas;
e) O cumprimento das normas internacionais.

Os provedores de servizos dixitais atenderán igualmente os actos de execución polos cales a Comisión Europea detalle os aspectos citados.

Artigo 17. *Normas técnicas.*

As autoridades competentes promoverán a utilización de regulacións, normas ou especificacións técnicas en materia de seguridade das redes e sistemas de información elaboradas no marco do Regulamento (UE) 1025/2012 do Parlamento Europeo e do Consello, do 25 de outubro de 2012, sobre a normalización europea.

En ausencia das ditas normas ou especificacións, promoverán a aplicación das normas ou recomendacións internacionais aprobadas polos organismos internacionais de normalización, e, se é o caso, das normas e especificacións técnicas aceptadas a nivel europeo ou internacional que sexan pertinentes nesta materia.

Artigo 18. *Sectores con normativa específica equivalente.*

Cando unha normativa nacional ou comunitaria estableza para un sector obrigas de seguridade das redes e sistemas de información ou de notificación de incidentes que teñan efectos, cando menos, equivalentes aos das obrigas previstas neste real decreto lei, prevalecerán aqueles requisitos e os mecanismos de supervisión correspondentes.

Iso non afectará o deber de cooperación entre autoridades competentes, a coordinación exercida polo Consello de Seguridade Nacional nin, na medida en que non sexa incompatible coa lexislación sectorial, a aplicación do título V sobre notificación de incidentes.

TÍTULO V

Notificación de incidentes

Artigo 19. *Obrigación de notificar.*

1. Os operadores de servizos esenciais notificarán á autoridade competente, a través dos CSIRT de referencia, os incidentes que poidan ter efectos perturbadores significativos nos ditos servizos.

As notificacións poderán referirse tamén, conforme se determine regulamentariamente, aos sucesos ou incidencias que poidan afectar as redes e sistemas de información empregados para a prestación dos servizos esenciais pero que aínda non tivesen un efecto adverso real sobre aqueles.

2. Así mesmo, os provedores de servizos dixitais notificarán á autoridade competente, a través dos CSIRT de referencia, os incidentes que teñan efectos perturbadores significativos nos ditos servizos.

A obrigación da notificación do incidente únicamente se aplicará cando o provedor de servizos dixitais teña acceso á información necesaria para valorar o impacto dun incidente.

3. As notificacións tanto de operadores de servizos esenciais como de provedores de servizos dixitais referiranse aos incidentes que afecten as redes e sistemas de información empregados na prestación dos servizos indicados tanto se se trata de redes e servizos propios como se o son de provedores externos, incluso se estes son provedores de servizos dixitais sometidos a este real decreto lei.

4. As autoridades competentes e os CSIRT de referencia utilizarán unha plataforma común para facilitar e automatizar os procesos de notificación, comunicación e información sobre incidentes.

5. O desenvolvemento regulamentario deste real decreto lei preverá as medidas necesarias para o cumprimento do preceptuado neste artigo por parte dos operadores de servizos esenciais. As autoridades competentes poderán establecer, mediante orde ministerial, obrigas específicas de notificación para operadores de servizos esenciais. Así mesmo, poderán ditar instrucións técnicas e guías orientativas para detallar o contido das ditas ordes.

Ao elaborar as disposicións regulamentarias, instrucións e guías, teranse en conta as obrigas sectoriais, as directrices relevantes que se adopten no grupo de cooperación e os requisitos en materia de notificación de incidentes a que estiver sometido o operador en virtude doutras normas, como a Lei 8/2011, do 28 de abril, e o Esquema nacional de seguridade, aprobado polo Real decreto 3/2010, do 8 de xaneiro.

6. A obrigación de notificación de incidentes prevista nos puntos anteriores non obsta o cumprimento dos deberes legais de denuncia daqueles feitos que revistan caracteres de delito ante as autoridades competentes, de acordo co disposto nos artigos 259 e seguintes da Lei de axuizamento criminal, e tendo en conta o previsto no artigo 14.3 deste real decreto lei.

Artigo 20. *Protección do notificante.*

1. As notificacións consideradas neste título non suxeitarán a entidade que as efectúe a unha maior responsabilidade.

2. Os empregados e o persoal que, por calquera tipo de relación laboral ou mercantil, participen na prestación dos servizos esenciais ou dixitais, e informen sobre incidentes non poderán sufrir consecuencias adversas no seu posto de traballo ou coa empresa, salvo nos supostos en que se acredite má fe na súa actuación.

Entenderanse nulas e sen efecto legal as decisións do empregador tomadas en prexuízo ou detrimento dos dereitos laborais dos traballadores que actuasen conforme este punto.

Artigo 21. *Factores para determinar a importancia dos efectos dun incidente.*

1. Para os efectos das notificacións a que se refire o artigo 19.1, primeiro parágrafo, a importancia dun incidente determinarase tendo en conta, como mínimo, os seguintes factores:

a) O número de usuarios afectados pola perturbación do servizo esencial.
b) A duración do incidente.
c) A extensión ou áreas xeográficas afectadas polo incidente.
d) O grao de perturbación do funcionamento do servizo.
e) O alcance do impacto en actividades económicas e sociais cruciais.
f) A importancia dos sistemas afectados ou da información afectada polo incidente para a prestación do servizo esencial.
g) O dano á reputación.

2. Nas notificacións a que se refire o artigo 19.2, a importancia dun incidente determinarase conforme o que establezan os actos de execución previstos nos puntos 8 e 9 do artigo 16 da Directiva (UE) 2016/1148 do Parlamento Europeo e do Consello, do 6 de xullo de 2016.

Artigo 22. *Notificación inicial, notificacións intermedias e notificación final.*

1. Os operadores de servizos esenciais deberán realizar unha primeira notificación dos incidentes a que se refire o artigo 19.1 sen dilación indebida.

A notificación incluirá, entre outros datos, información que permita determinar calquera efecto transfronteirizo do incidente.

2. Os operadores de servizos esenciais efectuarán as notificacións intermedias que sexan precisas para actualizar a información incorporada á notificación inicial e informar sobre a evolución do incidente, mentres este non estea resolto.

3. Os operadores de servizos esenciais enviarán unha notificación final do incidente tras a súa resolución.

Un incidente considerarase resolto cando se restablecesen as redes e sistemas de información afectados e o servizo opere con normalidade.

Artigo 23. *Flexibilidade na observancia dos prazos para a notificación.*

Os operadores de servizos esenciais e os provedores de servizos dixitais poderán omitir, nas comunicacións que realicen sobre os incidentes que os afecten, a información da que aínda non dispoñan relativa á súa repercusión sobre servizos esenciais ou outros servizos que dependan deles para a súa prestación, ou outra información da que non dispoñan. Tan pronto como coñezan a dita información, deberán remitila á autoridade competente.

Se, transcorrido un tempo prudencial desde a notificación inicial do incidente, o operador de servizos esenciais ou o provedor de servizos dixitais non puider reunir a información pertinente, enviará á autoridade competente, sen demora, un informe xustificativo das actuacións realizadas para reunir a información e dos motivos polos que non foi posible obtela.

Artigo 24. *Incidentes que afecten servizos dixitais.*

Os operadores de servizos esenciais e os provedores de servizos dixitais sometidos a este real decreto lei, así como calquera outra parte interesada, que teñan noticia de incidentes que afecten, de modo significativo, servizos dixitais ofrecidos en España por provedores establecidos noutros Estados membros da Unión Europea, poderán notificarllo á autoridade competente achegando a información pertinente, co obxecto de facilitar a cooperación co Estado membro no que estiver establecido o citado provedor.

Do mesmo modo, se teñen noticia de que os ditos provedores incumpriron os requisitos de seguridade ou de notificación de incidentes ocorridos en España que lles son aplicables, poderán notificalo á autoridade competente achegando a información pertinente.

Artigo 25. *Tramitación de incidentes con impacto transfronteirizo.*

1. Cando as autoridades competentes ou os CSIRT de referencia teñan noticia de incidentes que poden afectar outros Estados membros da Unión Europea, informarán, a través do punto de contacto único, os Estados membros afectados, precisando se o incidente pode ter efectos perturbadores significativos para os servizos esenciais prestados nos ditos Estados.

2. Cando, a través do dito punto de contacto se reciba información sobre incidentes notificados noutros países da Unión Europea que poidan ter efectos perturbadores significativos para os servizos esenciais prestados en España, remitirase a información relevante á autoridade competente e ao CSIRT de referencia, para que adopten as medidas pertinentes no exercicio das súas funcións respectivas.

3. As actuacións consideradas nos puntos anteriores enténdense sen prexuízo dos intercambios de información que as autoridades competentes ou os CSIRT de referencia poidan realizar, de modo directo, cos seus homólogos doutros Estados membros da Unión Europea en relación con aqueles incidentes que poidan resultar de interese mutuo.

Artigo 26. *Información ao público.*

1. A autoridade competente poderá exixir aos operadores de servizos esenciais ou aos provedores de servizos dixitais que informen o público ou terceiros potencialmente interesados sobre os incidentes cando o seu coñecemento sexa necesario para evitar novos incidentes ou xestionar un que xa se tivese producido, ou cando a divulgación dun incidente redunde en beneficio do interese público.

2. A autoridade competente tamén poderá decidir informar, de modo directo, o público ou terceiros sobre o incidente.

Nestes casos a autoridade competente consultará e coordinarase co operador de servizos esenciais ou co provedor de servizos dixitais antes de informar o público.

Artigo 27. *Información anual ao punto de contacto único e ao grupo de cooperación.*

1. As autoridades competentes transmitirán ao punto de contacto único un informe anual sobre o número e tipo de incidentes comunicados, os seus efectos nos servizos prestados ou noutros servizos e o seu carácter nacional ou transfronteirizo dentro da Unión Europea.

As autoridades competentes elaborarán o informe seguindo as instrucións que dite o punto de contacto único e terán en conta as indicacións do grupo de cooperación respecto ao formato e contido da información que se vaia transmitir.

2. O punto de contacto único remitirá ao grupo de cooperación, antes do 9 de agosto de cada ano, un informe anual resumido sobre as notificacións recibidas, e remitirao ulteriormente ás autoridades competentes e aos CSIRT de referencia, para o seu coñecemento.

Artigo 28. *Obrigación de resolver os incidentes, de información e de colaboración mutua.*

1. Os operadores de servizos esenciais e os provedores de servizos dixitais teñen a obrigación de resolver os incidentes de seguridade que os afecten e de solicitar axuda especializada, incluída a do CSIRT de referencia, cando non poidan resolver por si mesmos os incidentes.

En tales casos deberán atender as indicacións que reciban do CSIRT de referencia para resolver o incidente, mitigar os seus efectos e repoñer os sistemas afectados.

2. Os operadores de servizos esenciais e os provedores de servizos dixitais deben subministrar ao CSIRT de referencia e á autoridade competente toda a información que

lles for requirida para o desempeño das funcións que lles encomenda o presente real decreto lei.

En particular, poderá requirirse información adicional aos operadores de servizos esenciais e aos provedores de servizos dixitais para analizar a natureza, causas e efectos dos incidentes notificados, e para elaborar estatísticas e reunir os datos necesarios para elaborar os informes anuais considerados no artigo 27.

Cando as circunstancias o permitan, a autoridade competente ou o CSIRT de referencia proporcionarán aos operadores de servizos esenciais ou aos provedores de servizos dixitais afectados por incidentes a información derivada do seu seguimento que poida ser relevante para eles, en particular, para resolver o incidente.

Artigo 29. *Cooperación no relativo aos incidentes que afecten datos persoais.*

As autoridades competentes e os CSIRT de referencia cooperarán estreitamente coa Axencia Española de Protección de Datos para facer fronte aos incidentes que dean lugar a violacións de datos persoais.

As autoridades competentes e os CSIRT de referencia comunicarán sen dilación á Axencia Española de Protección de Datos os incidentes que poidan supor unha vulneración de datos persoais e manterana informada sobre a evolución de tales incidentes.

Artigo 30. *Autorización para a cesión de datos persoais.*

Se a notificación de incidentes ou a súa xestión, análise ou resolución requirise comunicar datos persoais, o seu tratamento restrinxirase aos que sexan estritamente adecuados, pertinentes e limitados ao necesario en relación coa finalidade, das indicadas, que se persiga en cada caso.

A súa cesión para estes fins entenderase autorizada nos seguintes casos:

a) Dos operadores de servizos esenciais e dos provedores de servizos dixitais ás autoridades competentes, a través dos CSIRT de referencia.

b) Entre os CSIRT de referencia e as autoridades competentes, e viceversa.

c) Entre os CSIRT de referencia, e entre estes e os CSIRT designados noutros Estados membros da Unión Europea.

d) Entre os CSIRT de referencia e outros CSIRT nacionais ou internacionais.

e) Entre o punto de contacto único e os puntos de contacto únicos doutros Estados membros da Unión Europea.

Artigo 31. *Notificacións voluntarias.*

1. Os operadores de servizos esenciais e os provedores de servizos dixitais poderán notificar os incidentes para os que non se estableza unha obrigación de notificación.

Así mesmo, as entidades que presten servizos esenciais e non fosen identificadas como operadores de servizos esenciais e que non sexan provedores de servizos dixitais poderán notificar os incidentes que afecten os ditos servizos.

Estas notificacións obrigan a entidade que as efectúe a resolver o incidente de acordo co establecido no artigo 28.

2. As notificacións a que se refire o punto anterior rexeranse polo disposto neste título e informarase sobre elas ao punto de contacto único no informe anual previsto no artigo 27.1.

3. As notificacións obrigatorias gozarán de prioridade sobre as voluntarias para os efectos da súa xestión polos CSIRT e polas autoridades competentes.

TÍTULO VI

Supervisión

Artigo 32. *Supervisión dos operadores de servizos esenciais.*

1. As autoridades competentes poderán requirir os operadores de servizos esenciais para que lles proporcionen toda a información necesaria para avaliar a seguridade das redes e sistemas de información, incluída a documentación sobre políticas de seguridade.

Poderán requirirlles información sobre a aplicación efectiva da súa política de seguridade, así como auditar ou exixir ao operador que someta a seguridade das súas redes e sistemas de información a unha auditoría por unha entidade externa, solvente e independente.

2. Á vista da información solicitada, a autoridade competente poderá requirir ao operador que emende as deficiencias detectadas e indicarlle como debe facelo.

Artigo 33. *Supervisión dos provedores de servizos dixitais.*

1. A autoridade competente para a supervisión dos servizos dixitais soamente inspeccionará o cumprimento das obrigas derivadas deste real decreto lei cando teña noticia dalgún incumprimento, incluíndo por petición razoada doutros órganos ou denuncia.

En tal caso, a autoridade competente poderá requirir o provedor de servizos dixitais para que lle proporcione toda a información necesaria para avaliar a seguridade das súas redes e sistemas de información, incluída a documentación sobre políticas de seguridade, e para que emende as deficiencias detectadas.

2. Cando a autoridade competente teña noticia de incidentes que perturben, de modo significativo, servizos dixitais ofrecidos noutros Estados membros por provedores establecidos en España, adoptará as medidas de supervisión pertinentes.

Para estes efectos, terá especialmente en conta a información facilitada polas autoridades competentes doutros Estados membros.

Artigo 34. *Cooperación transfronteiriza.*

1. A supervisión levarase a cabo, cando proceda, en cooperación coas autoridades competentes dos Estados membros nos cales se sitúen as redes e sistemas de información empregados para a prestación do servizo, ou en que estea establecido o operador de servizos esenciais, o provedor de servizos dixitais ou o seu representante.

2. As autoridades competentes colaborarán coas autoridades competentes doutros Estados membros cando estas requiran a súa cooperación na supervisión e adopción de medidas por operadores de servizos esenciais e provedores de servizos dixitais en relación coas redes e sistemas de información situados en España, así como respecto aos provedores de servizos dixitais establecidos en España ou cuxo representante na Unión Europea teña a súa residencia ou domicilio social en España.

TÍTULO VII

Réxime sancionador

Artigo 35. *Responsables.*

Serán responsables os operadores de servizos esenciais e os provedores de servizos dixitais comprendidos no ámbito de aplicación deste real decreto lei.

Artigo 36. *Infraccións.*

1. As infraccións dos preceptos deste real decreto lei clasifícanse en moi graves, graves e leves.

2. Son infraccións moi graves:

a) A falta de adopción de medidas para emendar as deficiencias detectadas, de acordo co disposto nos artigos 32.2 ou 33.1, cando estas o fixesen vulnerable a un incidente con efectos perturbadores significativos no servizo e o operador de servizos esenciais ou o provedor de servizos dixitais non atendese os requirimentos ditados pola autoridade competente con anterioridade á produción do incidente.

b) O incumprimento reiterado da obrigación de notificar incidentes con efectos perturbadores significativos no servizo. Considerarase que é reiterado a partir do segundo incumprimento.

c) Non tomar as medidas necesarias para resolver os incidentes de acordo co disposto no artigo 28.1 cando estes teñan un efecto perturbador significativo na prestación de servizos esenciais ou de servizos dixitais en España ou noutros Estados membros.

3. Son infraccións graves:

a) O incumprimento das disposicións regulamentarias ou das instrucións técnicas de seguridade ditadas pola autoridade competente referidas ás precaucións mínimas que os operadores de servizos esenciais deben adoptar para garantir a seguridade das redes e sistemas de información.

b) A falta de adopción de medidas para emendar as deficiencias detectadas en resposta a un requirimento ditado de acordo cos artigos 32.2 ou 33.1, cando ese sexa o terceiro requirimento desatendido que se dita nos cinco últimos anos.

c) O incumprimento da obrigación de notificar incidentes con efectos perturbadores significativos no servizo.

d) A demostración dunha notoria falta de interese na resolución de incidentes con efectos perturbadores significativos notificados cando dea lugar a unha maior degradación do servizo.

e) Proporcionar información falsa ou enganosa ao público sobre os estándares que cumpre ou as certificacións de seguridade que mantén en vigor.

f) Poñer obstáculos á realización de auditorías pola autoridade competente.

4. Son infraccións leves:

a) O incumprimento das disposicións regulamentarias ou das instrucións técnicas de seguridade ditadas pola autoridade competente ao abeiro deste real decreto lei, cando non supoña unha infracción grave.

b) A falta de adopción de medidas para corrixir as deficiencias detectadas en resposta a un requirimento de emenda ditado de acordo cos artigos 32.2 ou 33.1.

c) Non facilitar a información que sexa requirida polas autoridades competentes sobre os seus políticas de seguridade, ou proporcionar información incompleta ou tardía sen xustificación.

d) Non someterse a unha auditoría de seguridade segundo o ordenado pola autoridade competente.

e) Non proporcionar ao CSIRT de referencia ou á autoridade competente a información que soliciten en virtude do artigo 28.2.

f) A falta de notificación dos sucesos ou incidencias para os que, aínda que non tivesen un efecto adverso real sobre os servizos, exista obrigación de notificación en virtude do parágrafo segundo do artigo 19.2.

g) Non completar a información que debe reunir a notificación de incidentes tendo en conta o disposto no artigo 23, ou non remitir o informe xustificativo sobre a imposibilidade de reunir a información prevista no dito artigo.

h) Non seguir as indicacións que reciba do CSIRT de referencia para resolver un incidente, de acordo co artigo 28.

Artigo 37. *Sancións.*

1. Pola comisión das infraccións recollidas no artigo anterior, imporanse as seguintes sancións:

a) Pola comisión de infraccións moi graves, multa de 500.001 ata 1.000.000 euros.
b) Pola comisión de infraccións graves, multa de 100.001 ata 500.000 euros.
c) Pola comisión de infraccións leves, amoestación ou multa ata 100.000 euros.

2. As sancións firmes en vía administrativa por infraccións moi graves e graves poderán ser publicadas, á custa do sancionado, no «Boletín Oficial del Estado» e no sitio da internet da autoridade competente, en atención aos feitos concorrentes e de conformidade co artigo seguinte.

Artigo 38. *Graduación da contía das sancións.*

O órgano sancionador establecerá a sanción tendo en conta os seguintes criterios:

a) O grao de culpabilidade ou a existencia de intencionalidade.
b) A continuidade ou persistencia na conduta infractora.
c) A natureza e contía dos prexuízos causados.
d) A reincidencia, pola comisión no último ano de máis dunha infracción da mesma natureza, cando así fose declarado por resolución firme en vía administrativa.
e) O número de usuarios afectados.
f) O volume de facturación do responsable.
g) A utilización polo responsable de programas de recompensa polo descubrimento de vulnerabilidades nas súas redes e sistemas de información.
h) As accións realizadas polo responsable para paliar os efectos ou consecuencias da infracción.

Artigo 39. *Proporcionalidade de sancións.*

1. O órgano sancionador poderá establecer a contía da sanción aplicando a escala relativa á clase de infraccións que preceda inmediatamente en gravidade aquela en que se integra a considerada no caso de que se trate, nos seguintes supostos:

a) Cando se aprecie unha cualificada diminución da culpabilidade do imputado como consecuencia da concorrencia significativa de varios dos criterios enunciados no artigo 38.
b) Cando a entidade infractora regularizase a situación irregular de forma dilixente.
c) Cando o infractor recoñecese espontaneamente a súa culpabilidade.

2. Os órganos con competencia sancionadora, atendida a natureza dos feitos e a concorrencia significativa dos criterios establecidos no punto anterior, poderán non acordar o inicio do procedemento sancionador e, no seu lugar, apercibir o suxeito responsable co fin de que, no prazo que o órgano sancionador determine, acredite a adopción das medidas correctoras que en cada caso resulten pertinentes, sempre que concorran os seguintes presupostos:

a) Que os feitos fosen constitutivos de infracción leve ou grave conforme o disposto neste real decreto lei.
b) Que o órgano competente non sancionase ou apercibise o infractor nos dous anos previos como consecuencia da comisión de infraccións previstas neste real decreto lei.

Se o apercibimento non for atendido no prazo que o órgano sancionador determinase, procederá a apertura do correspondente procedemento sancionador polo dito incumprimento.

3. Non poderán ser obxecto de apercibimento as infraccións leves descritas no artigo 36.4 c), d) e e) e a infracción grave prevista no artigo 36.3 e).

Artigo 40. *Infraccións das administracións públicas.*

1. Cando as infraccións a que se refire o artigo 36 fosen cometidas por órganos ou entidades das administracións públicas, o órgano sancionador ditará unha resolución mediante a cal se establecen as medidas que procede adoptar para que cesen ou se corrixan os efectos da infracción. Esta resolución notificarase ao órgano ou entidade infractora e aos afectados, se os houber.

Ademais do anterior, o órgano sancionador poderá propoñer tamén a iniciación de actuacións disciplinarias, se procederen.

2. Deberanse comunicar ao órgano sancionador as resolucións que recaian en relación coas medidas e actuacións a que se refire o punto anterior.

Artigo 41. *Competencia sancionadora.*

1. A imposición de sancións corresponderá, no caso de infraccións moi graves, ao ministro competente en virtude do disposto no artigo 9, e no caso de infraccións graves e leves, ao órgano da autoridade competente que se determine mediante o regulamento de desenvolvemento deste real decreto lei.

2. A potestade sancionadora exercerase de acordo cos principios e o procedemento previstos nas leis 39/2015, do 1 de outubro, do procedemento administrativo común das administracións públicas, e 40/2015, do 1 de outubro, de réxime xurídico do sector público.

3. O exercicio da potestade sancionadora suxeitarase ao procedemento aplicable con carácter xeral á actuación das administracións públicas. Non obstante, o prazo máximo de duración do procedemento será dun ano e o prazo de alegacións non terá unha duración inferior a un mes.

Artigo 42. *Concorrencia de infraccións.*

1. Non procederá a imposición de sancións segundo o previsto neste real decreto lei cando os feitos constitutivos de infracción o sexan tamén doutra tipificada na normativa sectorial á que estea suxeito o prestador do servizo e exista identidade do ben xurídico protexido.

2. Cando, como consecuencia dunha actuación sancionadora, se teña coñecemento de feitos que poidan ser constitutivos de infraccións tipificadas noutras leis, daranse conta destes aos órganos ou organismos competentes para a súa supervisión e sanción.

Disposición adicional primeira. *Relación inicial de servizos esenciais e operadores de servizos esenciais.*

A Comisión Nacional para a Protección das Infraestruturas Críticas aprobará unha primeira lista de servizos esenciais dentro dos sectores incluídos no ámbito de aplicación deste real decreto lei e identificará os operadores que os presten e que deban suxeitarse a este real decreto lei na seguinte orde:

a) Antes do 9 de novembro de 2018: os servizos esenciais e os operadores correspondentes aos sectores estratéxicos de enerxía, transporte, saúde, sistema financeiro, auga e infraestruturas dixitais.

b) Antes do 9 de novembro de 2019: os servizos esenciais e os operadores correspondentes ao resto dos sectores estratéxicos recollidos no anexo da Lei 8/2011, do 28 de abril.

Disposición adicional segunda. *Comunicacións electrónicas e servizos de confianza.*

A aplicación deste real decreto lei aos operadores de redes e servizos de comunicacións electrónicas e de servizos electrónicos de confianza que sexan designados como operadores críticos en virtude da Lei 8/2011, do 28 de abril, non obstará para a aplicación da súa normativa específica en materia de seguridade.

O Ministerio de Economía e Empresa, como órgano competente para a aplicación da dita normativa, e o Ministerio do Interior actuarán de maneira coordinada no establecemento de obrigas que recaian sobre os operadores críticos. Así mesmo, manterán un intercambio fluído de información sobre incidentes que os afecten.

Disposición adicional terceira. *Notificación de violacións de seguridade dos datos persoais a través da plataforma común prevista neste real decreto lei.*

A plataforma común para a notificación de incidentes prevista neste real decreto lei poderá ser empregada para a notificación de vulneracións da seguridade de datos persoais segundo o 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, nos termos que acorden a Axencia Española de Protección de Datos e os órganos que xestionen a dita plataforma.

Disposición adicional cuarta. *Provedores de servizos dixitais xa existentes.*

Os provedores de servizos dixitais que xa viñesen prestando servizos deberán comunicar a súa actividade á Secretaría de Estado para o Avance Dixital do Ministerio de Economía e Empresa, no prazo de tres meses desde a entrada en vigor deste real decreto lei.

Disposición derradeira primeira. *Título competencial.*

Este real decreto lei dítase en virtude das competencias exclusivas atribuídas ao Estado en materia de réxime xeral de telecomunicacións e seguridade pública polo artigo 149.1.21.ª e 29.ª da Constitución.

Disposición derradeira segunda. *Incorporación do dereito da Unión Europea.*

Este real decreto lei incorpora ao ordenamento xurídico interno 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.

Disposición derradeira terceira. *Habilitación para o desenvolvemento regulamentario.*

Habilítase o Goberno para desenvolver regulamentariamente o previsto neste real decreto lei, sen prexuízo da competencia dos ministros para fixar as obrigas específicas mediante orde ministerial nos supostos previstos no articulado desta norma.

Disposición derradeira cuarta. *Entrada en vigor.*

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

Dado en Madrid o 7 de setembro de 2018.

FELIPE R.

O presidente do Goberno,
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN