I. DISPOSICIONS GENERALS

CAP DE L'ESTAT

12257 *Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació.*

I

L'evolució de les tecnologies de la informació i de la comunicació, especialment amb el desenvolupament d'Internet, ha fet que les xarxes i els sistemes d'informació tinguin actualment un paper crucial en la nostra societat, i la seva fiabilitat i seguretat són aspectes essencials per a la pràctica normal de les activitats econòmiques i socials.

Per això, els incidents que, en el moment que afecten les xarxes i els sistemes d'informació, alteren aquestes activitats representen una amenaça greu, atès que tant si són fortuïts com si provenen d'accions deliberades poden generar pèrdues financeres, menyscabar la confiança de la població i, en definitiva, causar danys greus a l'economia i a la societat, amb la possibilitat d'afectar la mateixa seguretat nacional en la pitjor hipòtesi.

El caràcter transversal i interconnectat de les tecnologies de la informació i de la comunicació, que també caracteritza les seves amenaces i riscos, limita l'eficàcia de les mesures que s'utilitzen per contrarestar-los quan es prenen de manera aïllada. Aquest caràcter transversal també fa que es corri el risc de perdre efectivitat si els requisits en matèria de seguretat de la informació es defineixen de manera independent per a cadascun dels àmbits sectorials afectats.

Per tant, és oportú establir mecanismes que, amb una perspectiva integral, permetin millorar la protecció davant de les amenaces que afecten les xarxes i els sistemes d'informació, i facilitar la coordinació de les actuacions dutes a terme en aquesta matèria tant en l'àmbit nacional com amb els països del nostre entorn, en particular, dins de la Unió Europea.

II

Amb aquest propòsit es dicta aquest Reial decret llei, que transposa a l'ordenament jurídic espanyol la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i els sistemes d'informació en la Unió. El Reial decret llei es basa igualment en les normes, en els instruments de resposta a incidents i en els òrgans de coordinació estatal existents en aquesta matèria, la qual cosa, juntament amb les raons que assenyala l'apartat I, justifica que el seu contingut transcendeixi el de la mateixa Directiva.

El Reial decret llei s'aplica a les entitats que prestin serveis essencials per a la comunitat i depenguin de les xarxes i els sistemes d'informació per dur a terme la seva activitat. El seu àmbit d'aplicació s'estén a sectors que no estan expressament inclosos en la Directiva, per donar-li a aquest Reial decret llei un enfocament global, encara que se'n preserva la legislació específica. Addicionalment, en el cas de les activitats d'explotació de les xarxes i de prestació de serveis de comunicacions electròniques i els recursos associats, així com dels serveis electrònics de confiança, expressament exclosos de la Directiva esmentada, el Reial decret llei s'aplica únicament pel que fa als operadors crítics.

El Reial decret llei s'aplica, així mateix, als proveïdors de determinats serveis digitals. La Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, els sotmet a un règim d'harmonització màxima, equivalent a un reglament, atès que es considera que la seva regulació a escala nacional no seria efectiva per tenir un caràcter intrínsecament transnacional. La funció de les autoritats nacionals es limita, per tant, a supervisar la seva aplicació per part dels proveïdors establerts al seu país, i coordinar-se amb les autoritats corresponents d'altres països de la Unió Europea.

Seguint la Directiva esmentada, el Reial decret llei identifica els sectors en què és necessari garantir la protecció de les xarxes i els sistemes d'informació, i estableix procediments per identificar els serveis essencials oferts en aquests sectors, així com els principals operadors que presten els serveis, que són, en definitiva, els destinataris d'aquest Reial decret llei.

Els operadors de serveis essencials i els proveïdors de serveis digitals han d'adoptar mesures adequades per gestionar els riscos que es plantegin per a la seguretat de les xarxes i els sistemes d'informació que utilitzin, encara que la seva gestió estigui externalitzada. Les obligacions de seguretat que assumeixin han de ser proporcionades al nivell de risc que afrontin i han d'estar basades en una avaluació prèvia d'aquests. Les normes de desplegament d'aquest Reial decret llei poden concretar les obligacions de seguretat exigibles als operadors de serveis essencials, incloses si s'escau les inspeccions que cal dur a terme o la participació en activitats i exercicis de gestió de crisi.

El Reial decret llei requereix així mateix que els operadors de serveis essencials i els proveïdors de serveis digitals notifiquin els incidents que pateixin en les xarxes i els serveis d'informació que utilitzen per a la prestació dels serveis essencials i digitals, i tinguin efectes pertorbadors significatius en aquests, alhora que preveu la notificació dels successos o les incidències que puguin afectar els serveis essencials, però que encara no hagin tingut un efecte advers real sobre aquells, i perfila els procediments de notificació.

La notificació d'incidents forma part de la cultura de gestió de riscos que la Directiva i el Reial decret llei fomenten. Per això, el Reial decret llei protegeix l'entitat notificadora i el personal que informi sobre incidents succeïts; es reserva la informació confidencial de la seva divulgació al públic o a altres autoritats diferents de la notificada i es permet la notificació d'incidents quan no sigui obligada la seva comunicació.

El Reial decret llei recalca la necessitat de tenir en compte els estàndards europeus i internacionals, així com les recomanacions que emanin del grup de cooperació i de la xarxa de CSIRT (Computer Security Incident Response Team) establerts en l'àmbit comunitari per la Directiva, amb vista a aplicar les millors pràctiques apreses en aquests fòrums i contribuir a l'impuls del mercat interior i a la participació de les nostres empreses en aquest.

Amb la finalitat d'augmentar la seva eficàcia i, alhora, reduir les càrregues administratives i econòmiques que aquestes obligacions suposen per a les entitats afectades, aquest Reial decret llei tracta de garantir la seva coherència amb les que es deriven de l'aplicació d'altres normatives en matèria de seguretat de la informació, tant de caràcter horitzontal com sectorial, i la coordinació en la seva aplicació amb les autoritats responsables en cada cas.

Respecte a les normes horitzontals, destaquen els vincles establerts amb les lleis 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques, i 36/2015, de 28 de setembre, de seguretat nacional, i amb el Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, com a normativa especial en matèria de seguretat dels sistemes d'informació del sector públic.

Així, s'aproxima l'àmbit d'aplicació d'aquest Reial decret llei al de la Llei 8/2011, de 28 d'abril, afegint als sectors que preveu la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, els sectors estratègics addicionals que estableix aquesta Llei; es basa en aquesta per definir el concepte de «servei essencial», i s'atribueix als seus òrgans col·legiats la determinació dels serveis essencials i dels operadors de serveis essencials subjectes a aquest Reial decret llei. Tenint en compte la Llei 36/2015, de 28 de setembre, s'atribueix al Consell de Seguretat Nacional la funció d'actuar com a punt de contacte amb altres països de la Unió Europea i un paper coordinador de la política de ciberseguretat a través de l'Estratègia de ciberseguretat nacional.

III

L'Estratègia de ciberseguretat nacional que Espanya té des de l'any 2013 estableix les prioritats, els objectius i les mesures adequades per assolir i mantenir un elevat nivell de seguretat de les xarxes i els sistemes d'informació. L'Estratègia ha de seguir desplegant el

marc institucional de la ciberseguretat que aquest Reial decret llei esbossa, compost per les autoritats públiques competents i els CSIRT de referència, d'una banda, i la cooperació publicoprivada, de l'altra.

Les autoritats competents han d'exercir les funcions de vigilància derivades d'aquest Reial decret llei i han d'aplicar el règim sancionador quan sigui procedent. Així mateix, han de promoure el desplegament de les obligacions que el Reial decret llei imposa, amb la consulta al sector i a les autoritats que exerceixin competències per raó de la matèria quan es refereixin a sectors específics, per evitar l'existència d'obligacions duplicades, innecessàries o excessivament oneroses.

Els CSIRT són els equips de resposta a incidents que analitzen riscos i supervisen incidents a escala nacional, difonen alertes sobre aquests i aporten solucions per mitigar-ne els efectes. El terme CSIRT és el que s'empra de manera comuna a Europa en lloc del terme protegit CERT (Computer Emergency Response Team), registrat als EUA.

El Reial decret llei delimita l'àmbit funcional d'actuació dels CSIRT de referència que preveu. Els CSIRT són la porta d'entrada de les notificacions d'incidents, la qual cosa permet organitzar ràpidament la resposta a aquests, però el destinatari de les notificacions és l'autoritat competent respectiva, que ha de tenir en compte aquesta informació per a la supervisió dels operadors. En tot cas, l'operador és responsable de resoldre els incidents i reposar les xarxes i els sistemes d'informació afectats al seu funcionament ordinari.

Es preveu la utilització d'una plataforma comuna per a la notificació d'incidents, de manera que els operadors no hagin d'efectuar diverses notificacions en funció de l'autoritat a què s'hagin de dirigir. Aquesta plataforma es pot utilitzar també per a la notificació de vulneracions de la seguretat de dades personals segons el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE.

IV

Aquest Reial decret llei consta de set títols que contenen, en primer lloc, les definicions dels termes que s'empren al llarg del text, la salvaguarda de funcions estatals essencials, com la seguretat nacional i altres disposicions generals. A continuació, en el títol II es determinen la forma i els criteris d'identificació dels serveis essencials i dels operadors que els prestin als quals s'aplica el Reial decret llei. L'ordre en què s'ha de procedir a la seva identificació per primera vegada s'estableix a la disposició addicional primera del Reial decret llei. El títol III recull el marc estratègic i institucional de la seguretat de les xarxes i els sistemes d'informació que s'ha descrit anteriorment. Es dedica un precepte específic a la cooperació entre autoritats públiques, com a pilar d'un exercici adequat de les diferents competències concurrents sobre la matèria.

El títol IV s'ocupa de les obligacions de seguretat dels operadors, i s'hi preveu l'aplicació preferent de normes sectorials que imposin obligacions equivalents a les que preveu aquest Reial decret llei, sense perjudici de la coordinació exercida pel Consell de Seguretat Nacional i del deure de cooperació amb les autoritats competents en virtut d'aquest Reial decret llei.

En el títol V, el més extens, es regula la notificació d'incidents i es presta atenció als incidents amb impacte transfronterer i a la informació i coordinació amb altres estats de la Unió Europea per a la seva gestió. En el títol VI, es disposen les potestats d'inspecció i control de les autoritats competents i la cooperació amb les autoritats nacionals d'altres estats membres, i en el títol VII es tipifiquen les infraccions i les sancions d'aquest Reial decret llei. En aquest aspecte, el Reial decret llei es decanta per impulsar l'esmena de la infracció abans que el seu càstig, el qual, si és necessari dispensar-lo, ha de ser efectiu, proporcionat i dissuasiu, en la línia del que ordena la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016.

El Reial decret llei es tanca amb una part final que inclou les disposicions addicionals i finals necessàries per completar la regulació.

Aquesta disposició s'ha sotmès al procediment d'informació de normes reglamentàries tècniques i de reglaments relatius als serveis de la societat de la informació, que preveuen la Directiva (UE) 2015/1535 del Parlament Europeu i del Consell, de 9 de setembre de 2015, per la qual s'estableix un procediment d'informació en matèria de reglamentacions tècniques i de regles relatives als serveis de la societat de la informació, així com el Reial decret 1337/1999, de 31 de juliol, pel qual es regula la remissió d'informació en matèria de normes i reglamentacions tècniques i reglaments relatius als serveis de la societat de la informació. Així mateix, s'adequa als principis de bona regulació que estableix l'article 129 de la Llei 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, de conformitat amb els quals han d'actuar les administracions públiques en l'exercici de la iniciativa legislativa, com són els principis de necessitat, eficàcia, proporcionalitat, seguretat jurídica, transparència i eficiència.

Aquest Reial decret llei es dicta en virtut de les competències exclusives que atribueix a l'Estat en matèria de règim general de telecomunicacions i seguretat pública l'article 149.1.21a i 29a de la Constitució.

El reial decret llei constitueix un instrument constitucionalment lícit, sempre que el fi que justifica la legislació d'urgència sigui, tal com ha exigit reiteradament el nostre Tribunal Constitucional (sentències 6/1983, de 4 de febrer, F 5; 11/2002, de 17 de gener, F 4; 137/2003, de 3 de juliol, F 3, i 189/2005, de 7 juliol, F 3), subvenir a una situació concreta, dins dels objectius governamentals, que per raons difícils de preveure requereix una acció normativa immediata en un termini més breu que el que es requereix per la via normal o pel procediment d'urgència per a la tramitació parlamentària de les lleis.

D'altra banda, la utilització de l'instrument jurídic del reial decret llei, en aquest cas, a més queda justificada per la doctrina del Tribunal Constitucional, que, en la Sentència 1/2012, de 13 de gener, ha avalat la concurrència del pressupòsit habilitador de l'extraordinària i urgent necessitat de l'article 86.1 de la Constitució, quan es doni el retard en la transposició de directives.

En efecte, el termini de transposició de la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, ja ha vençut a 9 de maig de 2018. La finalització del termini de transposició d'aquesta Directiva ha motivat la iniciació per part de la Comissió Europea d'un procediment formal d'infracció núm. 2018/168.

En conseqüència, s'entén que en el conjunt i en cadascuna de les mesures que s'adopten mitjançant el reial decret llei projectat concorren, per la seva naturalesa i finalitat, les circumstàncies d'extraordinària i urgent necessitat que exigeix l'article 86 de la Constitució com a pressupòsits habilitadors per a l'aprovació d'un reial decret llei.

En virtut d'això, fent ús de l'autorització que conté l'article 86 de la Constitució espanyola, a proposta de la vicepresidenta del Govern i ministra de la Presidència, Relacions amb les Corts i Igualtat, del ministre de l'Interior i de la ministra d'Economia i Empresa i amb la deliberació prèvia del Consell de Ministres, en la reunió del dia 7 de setembre de 2018,

DISPOSO:

TÍTOL I

Disposicions generals

Article 1. *Objecte.*

1. Aquest Reial decret llei té per objecte regular la seguretat de les xarxes i els sistemes d'informació utilitzats per a la provisió dels serveis essencials i dels serveis digitals, i establir un sistema de notificació d'incidents.

2. Així mateix, estableix un marc institucional per a l'aplicació d'aquest Reial decret llei i la coordinació entre autoritats competents i amb els òrgans de cooperació rellevants en l'àmbit comunitari.

Article 2. *Àmbit d'aplicació.*

1. Aquest Reial decret llei s'aplica a la prestació:

a) Dels serveis essencials dependents de les xarxes i els sistemes d'informació compresos en els sectors estratègics que defineix l'annex de la Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques.

b) Dels serveis digitals, considerats segons determina l'article 3 e), que siguin mercats en línia, motors de cerca en línia i serveis d'informàtica en núvol.

2. Estan sotmesos a aquest Reial decret llei:

a) Els operadors de serveis essencials establerts a Espanya. S'entén que un operador de serveis essencials està establert a Espanya quan la seva residència o domicili social es trobin en territori espanyol, sempre que aquests coincideixin amb el lloc en què estigui efectivament centralitzada la gestió administrativa i la direcció dels seus negocis o activitats.

Així mateix, aquest Reial decret llei és aplicable als serveis essencials que els operadors residents o domiciliats a un altre Estat ofereixin a través d'un establiment permanent situat a Espanya.

b) Els proveïdors de serveis digitals que tinguin la seva seu social a Espanya i que constitueixi el seu establiment principal a la Unió Europea, així com els que, tot i no estar establerts a la Unió Europea, designin a Espanya el seu representant a la Unió per al compliment de la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i els sistemes d'informació en la Unió.

3. Aquest Reial decret llei no s'aplica:

a) Als operadors de xarxes i serveis de comunicacions electròniques i als prestadors de serveis electrònics de confiança que no es designin com a operadors crítics en virtut de la Llei 8/2011, de 28 d'abril.

b) Als proveïdors de serveis digitals quan es tracti de microempreses o petites empreses, d'acord amb les definicions que recull la Recomanació 2003/361/CE de la Comissió, de 6 de maig de 2003, sobre la definició de microempreses, petites i mitjanes empreses.

Article 3. *Definicions.*

Als efectes d'aquest Reial decret llei, s'entén per:

a) Xarxes i sistemes d'informació, qualsevol dels elements següents:

1r Les xarxes de comunicacions electròniques, tal com les defineix el número 31 de l'annex II de la Llei 9/2014, de 9 de maig, general de telecomunicacions;

2n Qualsevol dispositiu o grup de dispositius interconnectats o relacionats entre si, en què un o diversos d'aquests duguin a terme, mitjançant un programa, el tractament automàtic de dades digitals;

3r Les dades digitals emmagatzemades, tractades, recuperades o transmeses mitjançant els elements que preveuen els números 1r i 2n anteriors, incloses les necessàries per al funcionament, la utilització, la protecció i el manteniment dels elements esmentats.

b) Seguretat de les xarxes i els sistemes d'informació: la capacitat de les xarxes i els sistemes d'informació de resistir, amb un nivell determinat de fiabilitat, qualsevol acció que comprometi la disponibilitat, l'autenticitat, la integritat o la confidencialitat de les dades emmagatzemades, transmeses o tractades, o els serveis corresponents oferts per aquestes xarxes i sistemes d'informació o accessibles a través d'aquests.

c) Servei essencial: servei necessari per al manteniment de les funcions socials bàsiques, la salut, la seguretat, el benestar social i econòmic dels ciutadans, o el funcionament eficaç de les institucions de l'Estat i les administracions públiques, que depengui per a la seva provisió de xarxes i sistemes d'informació.

d) Operador de serveis essencials: entitat pública o privada que s'identifiqui considerant els factors establerts a l'article 6 d'aquest Reial decret llei, que presti aquests serveis en algun dels sectors estratègics que defineix l'annex de la Llei 8/2011, de 28 d'abril.

e) Servei digital: servei de la societat de la informació entès en el sentit que recull la lletra a) de l'annex de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic.

f) Proveïdor de serveis digitals: persona jurídica que presta un servei digital.

g) Risc: qualsevol circumstància o fet raonablement identificable que tingui un possible efecte advers en la seguretat de les xarxes i els sistemes d'informació. Es pot quantificar com la probabilitat de materialització d'una amenaça que produeixi un impacte en termes d'operativitat, d'integritat física de persones o material o d'imatge.

h) Incident: succés inesperat o no desitjat amb conseqüències en detriment de la seguretat de les xarxes i els sistemes d'informació.

i) Gestió d'incidents: procediments seguits per detectar, analitzar i limitar un incident i respondre davant d'aquest.

j) Representant: persona física o jurídica establerta a la Unió Europea que s'ha designat expressament per actuar pel compte d'un proveïdor de serveis digitals no establert a la Unió Europea, a la qual, en substitució del proveïdor de serveis digitals, es pugui dirigir una autoritat competent nacional o un CSIRT, en relació amb les obligacions que, en virtut d'aquest Reial decret llei, té el proveïdor de serveis digitals.

k) Norma tècnica: una norma en el sentit de l'article 2.1 del Reglament (UE) núm. 1025/2012 del Parlament Europeu i del Consell, de 25 d'octubre de 2012, sobre la normalització europea.

l) Especificació: una especificació tècnica en el sentit de l'article 2.4 del Reglament (UE) núm. 1025/2012 del Parlament Europeu i del Consell, de 25 d'octubre de 2012.

m) Punt d'intercanvi d'Internet («IXP», per les seves sigles en anglès d'«Internet eXchange Point»): una instal·lació de xarxa que permet interconnectar més de dos sistemes autònoms independents, principalment per facilitar l'intercanvi de trànsit d'Internet. Un IXP permet interconnectar sistemes autònoms sense requerir que el trànsit d'Internet que passa entre qualsevol parell de sistemes autònoms participants passi per un tercer sistema autònom, i sense modificar ni interferir de cap altra manera el trànsit.

n) Sistema de noms de domini («DNS», per les seves sigles en anglès de «Domain Name System»): sistema distribuït jeràrquicament que respon consultes proporcionant informació associada a noms de domini, en particular, la relativa als identificadors utilitzats per localitzar i encaminar equips a Internet.

o) Proveïdor de serveis de DNS: entitat que presta serveis de DNS a Internet.

p) Registre de noms de domini de primer nivell: entitat que administra i dirigeix el registre de noms de domini d'Internet en un domini específic de primer nivell.

q) Mercat en línia: servei digital que permet als consumidors i als empresaris, tal com defineixen respectivament els articles 3 i 4 del text refós de la Llei general per a la defensa dels consumidors i usuaris i altres lleis complementàries, aprovat mitjançant el Reial decret legislatiu 1/2007, de 16 de novembre, formalitzar entre si contractes de compravenda o de prestació de serveis en línia amb empresaris, ja sigui en un lloc web específic del servei de mercat en línia o bé en un lloc web d'un empresari que utilitzi serveis informàtics proporcionats a l'efecte pel proveïdor del servei de mercat en línia.

r) Motor de cerca en línia: servei digital que permet als usuaris fer cerques de, en principi, tots els llocs web o de llocs web en una llengua en concret, mitjançant una consulta sobre un tema en forma de paraula clau, frase o un altre tipus d'entrada, i que, com a resposta, mostra enllaços en què es pot trobar informació relacionada amb el contingut sol·licitat.

s) Servei d'informàtica en núvol: servei digital que fa possible l'accés a un conjunt modulable i elàstic de recursos d'informàtica que es poden compartir.

Article 4. *Directrius i orientacions comunitàries.*

En l'aplicació d'aquest Reial decret llei i en l'elaboració dels reglaments i les guies que preveu s'han de tenir en compte els actes d'execució de la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, així com totes les recomanacions i les directrius emanades del grup de cooperació que estableix l'article 11 d'aquesta Directiva, i la informació sobre bones pràctiques recopilades pel grup esmentat i la xarxa de CSIRT, regulat a l'article 12 d'aquella.

Article 5. *Salvaguarda de funcions estatals essencials.*

El que disposa aquest Reial decret llei s'entén sense perjudici de les accions empreses per salvaguardar la seguretat nacional i les funcions estatals essencials, incloses les dirigides a protegir la informació classificada o la revelació de la qual sigui contrària als interessos essencials de l'Estat, o les que tinguin com a propòsit el manteniment de l'ordre públic, la detecció, investigació i persecució dels delictes, i l'enjudiciament dels seus autors.

TÍTOL II

Serveis essencials i serveis digitals

Article 6. *Identificació de serveis essencials i d'operadors de serveis essencials.*

1. La identificació dels serveis essencials i dels operadors que els prestin l'han d'efectuar els òrgans i a través dels procediments que preveuen la Llei 8/2011, de 28 d'abril, i la seva normativa de desplegament.

La relació dels serveis essencials i dels operadors d'aquests serveis s'ha d'actualitzar, per a cada sector, amb una freqüència biennal, en conjunció amb la revisió dels plans estratègics sectorials que preveu la Llei 8/2011, de 28 d'abril.

S'identifica un operador com a operador de serveis essencials si un incident patit per l'operador pot arribar a tenir efectes pertorbadors significatius en la prestació del servei, per a la qual cosa s'han de tenir en compte, almenys, els factors següents:

a) En relació amb la importància del servei prestat:

1r La disponibilitat d'alternatives per mantenir un nivell suficient de prestació del servei essencial;

2n La valoració de l'impacte d'un incident en la provisió del servei, amb l'avaluació de l'extensió o les zones geogràfiques que puguin quedar afectades per l'incident; la dependència d'altres sectors estratègics respecte del servei essencial ofert per l'entitat i la repercussió, en termes de grau i durada, de l'incident en les activitats econòmiques i socials o en la seguretat pública.

b) En relació amb els clients de l'entitat avaluada:

1r El nombre d'usuaris que confien en els serveis que aquesta presta;

2n La seva quota de mercat.

Reglamentàriament es poden afegir factors específics del sector per determinar si un incident pot tenir efectes pertorbadors significatius.

2. En cas que es tracti d'un operador crític designat en compliment de la Llei 8/2011, de 28 d'abril, n'hi ha prou que es constati la seva dependència de les xarxes i els sistemes d'informació per a la provisió del servei essencial de què es tracti.

3. En la identificació dels serveis essencials i dels operadors de serveis essencials s'han de tenir en consideració, tant com sigui possible, les recomanacions pertinents que adopti el grup de cooperació.

4. Quan un operador de serveis essencials ofereixi serveis en altres estats membres de la Unió Europea, s'ha d'informar els punts de contacte únic d'aquests estats sobre la intenció d'identificar-lo com a operador de serveis essencials.

Article 7. *Comunicació d'activitat per part dels proveïdors de serveis digitals.*

Els proveïdors de serveis digitals que indica l'article 2 han de comunicar la seva activitat a l'autoritat competent en el termini de tres mesos des que la inicïn, al simple efecte del seu coneixement.

TÍTOL III

Marc estratègic i institucional

Article 8. *Marc estratègic de seguretat de les xarxes i els sistemes d'informació.*

L'Estratègia de ciberseguretat nacional, a l'empara de l'Estratègia de seguretat nacional i alineada amb aquesta, emmarca els objectius i les mesures per assolir i mantenir un elevat nivell de seguretat de les xarxes i els sistemes d'informació.

L'Estratègia de ciberseguretat nacional ha d'abordar, entre altres qüestions, les que estableix l'article 7 de la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016.

A aquest efecte, el Consell de Seguretat Nacional ha d'impulsar la revisió de l'Estratègia de ciberseguretat nacional, de conformitat amb el que disposa l'article 21.1.e) de la Llei 36/2015, de 28 de setembre, de seguretat nacional.

Article 9. *Autoritats competents.*

1. Són autoritats competents en matèria de seguretat de les xarxes i els sistemes d'informació les següents:

a) Per als operadors de serveis essencials:

1r En cas que aquests es designin, a més, com a operadors crítics de conformitat amb la Llei 8/2011, de 28 d'abril, i la seva normativa de desplegament, independentment del sector estratègic en què es faci aquesta designació: la Secretaria d'Estat de Seguretat, del Ministeri de l'Interior, a través del Centre Nacional de Protecció d'Infraestructures i Ciberseguretat (CNPIC).

2n En cas que no siguin operadors crítics: l'autoritat sectorial corresponent per raó de la matèria, segons es determini reglamentàriament.

b) Per als proveïdors de serveis digitals: la Secretaria d'Estat per a l'Avanç Digital, del Ministeri d'Economia i Empresa.

c) Per als operadors de serveis essencials i proveïdors de serveis digitals que tot i no ser operadors crítics estiguin compresos en l'àmbit d'aplicació de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic: el Ministeri de Defensa, a través del Centre Criptològic Nacional.

2. El Consell de Seguretat Nacional, a través del seu comitè especialitzat en matèria de ciberseguretat, ha d'establir els mecanismes necessaris per a la coordinació de les actuacions de les autoritats competents.

Article 10. *Funcions de les autoritats competents.*

Les autoritats competents exerceixen les funcions següents:

a) Supervisar el compliment per part dels operadors de serveis essencials i dels proveïdors de serveis digitals de les obligacions que es determinin, de conformitat amb el que estableix el títol VI.

b) Establir els canals de comunicació oportuns amb els operadors de serveis essencials i amb els proveïdors de serveis digitals que, si s'escau, s'han de desplegar reglamentàriament.

c) Coordinar-se amb els CSIRT de referència a través dels protocols d'actuació que, si s'escau, s'han de desplegar reglamentàriament.

d) Rebre les notificacions sobre incidents que es presentin en el marc d'aquest Reial decret llei, a través dels CSIRT de referència, de conformitat amb el que estableix el títol V.

e) Informar el punt de contacte únic sobre les notificacions d'incidents presentades en el marc d'aquest Reial decret llei, de conformitat amb el que estableix l'article 27.

f) Informar, si s'escau, el públic sobre determinats incidents, quan la difusió d'aquesta informació sigui necessària per evitar un incident o gestionar-ne un que ja s'hagi produït, de conformitat amb el que estableix l'article 26.

g) Cooperar, en l'àmbit d'aplicació d'aquest Reial decret llei, amb les autoritats competents en matèria de protecció de dades de caràcter personal, seguretat pública, seguretat ciutadana i seguretat nacional, així com amb les autoritats sectorials corresponents, de conformitat amb el que estableixen els articles 14 i 29.

h) Establir obligacions específiques per garantir la seguretat de les xarxes i els sistemes d'informació i sobre notificació d'incidents, i dictar instruccions tècniques i guies orientatives per detallar el contingut d'aquestes obligacions, de conformitat amb el que estableixen els articles 16 i 19.

i) Exercir la potestat sancionadora en els casos que preveu aquest Reial decret llei, de conformitat amb el que estableix el títol VII.

j) Promoure l'ús de normes i especificacions tècniques, d'acord amb el que estableix l'article 17.

k) Cooperar amb les autoritats competents d'altres estats membres de la Unió Europea en la identificació d'operadors de serveis essencials entre entitats que ofereixin aquests serveis en diversos estats membres.

l) Informar el punt de contacte únic sobre incidents que puguin afectar altres estats membres, en els termes que preveu l'article 25.

Article 11. *Equips de resposta a incidents de seguretat informàtica de referència.*

1. Són equips de resposta a incidents de seguretat informàtica (CSIRT) de referència en matèria de seguretat de les xarxes i els sistemes d'informació els següents:

a) Quant a les relacions amb els operadors de serveis essencials:

1r El CCN-CERT, del Centre Criptològic Nacional, al qual correspon la comunitat de referència constituïda per les entitats de l'àmbit subjectiu d'aplicació de la Llei 40/2015, d'1 d'octubre.

2n L'INCIBE-CERT, de l'Institut Nacional de Ciberseguretat d'Espanya, al qual correspon la comunitat de referència constituïda per les entitats no incloses en l'àmbit subjectiu d'aplicació de la Llei 40/2015, d'1 d'octubre.

L'INCIBE-CERT l'operen conjuntament l'INCIBE i el CNPIC en tot el que es refereixi a la gestió d'incidents que afectin els operadors crítics.

3r L'ESPDEF-CERT, del Ministeri de Defensa, que coopera amb el CCN-CERT i l'INCIBE-CERT en les situacions que aquests requereixin en suport dels operadors de serveis essencials i, necessàriament, en els operadors que tinguin incidència en la defensa nacional i que es determinin reglamentàriament.

b) Quant a les relacions amb els proveïdors de serveis digitals que no estiguin compresos en la comunitat de referència del CCN-CERT: l'INCIBE-CERT.

L'INCIBE-CERT és, així mateix, l'equip de resposta a incidents de referència per als ciutadans, les entitats de dret privat i altres entitats no incloses anteriorment en aquest apartat 1.

2. Els CSIRT de referència s'han de coordinar entre si i amb la resta de CSIRT nacionals i internacionals en la resposta als incidents i la gestió de riscos de seguretat que

els corresponguin. En els supòsits d'especial gravetat que es determinin reglamentàriament i que requereixin un nivell de coordinació superior al necessari en situacions ordinàries, el CCN-CERT ha d'exercir la coordinació nacional de la resposta tècnica dels CSIRT.

Quan les activitats que duguin a terme puguin afectar d'alguna manera un operador crític, els CSIRT de referència s'han de coordinar amb el Ministeri de l'Interior, a través de l'Oficina de Coordinació Cibernètica del Centre Nacional de Protecció d'Infraestructures i Ciberseguretat (CNPIC), de la manera que es determini reglamentàriament.

Article 12. *Requisits i funcions dels CSIRT de referència.*

1. Els CSIRT han de complir les condicions següents:

a) Han de garantir un elevat nivell de disponibilitat dels seus serveis de comunicacions i evitar les fallades ocasionals i han de disposar de diversos mitjans perquè se'ls pugui contactar i puguin contactar amb altres en tot moment. A més, els canals de comunicació han d'estar clarament especificats i han de ser ben coneguts dels grups d'usuaris i els socis col·laboradors.

b) Les seves instal·lacions i les dels sistemes d'informació de suport han d'estar situades a llocs segurs.

c) Han de garantir la continuïtat de les activitats. Per a això:

1r Han d'estar dotats d'un sistema adequat per gestionar i canalitzar les sol·licituds amb la finalitat de facilitar els traspassos.

2n Han de disposar de personal suficient per garantir la seva disponibilitat en tot moment.

3r Han de tenir accés a infraestructures de comunicació la continuïtat de les quals estigui assegurada. Amb aquesta finalitat, han de disposar de sistemes redundants i espais de treball de reserva.

d) Han de tenir la capacitat de participar, quan ho desitgin, en xarxes de cooperació internacional.

2. Els CSIRT exerceixen, com a mínim, les funcions següents:

a) Supervisar incidents a escala nacional.

b) Difondre alertes primerenques, alertes, avisos i informació sobre riscos i incidents entre els interessats.

c) Respondre a incidents.

d) Efectuar una anàlisi dinàmica de riscos i incidents i de coneixement de la situació.

e) Participar en la xarxa de CSIRT.

3. Els CSIRT han d'establir relacions de cooperació amb el sector privat. A fi de facilitar la cooperació, els CSIRT han de fomentar l'adopció i la utilització de pràctiques comunes o normalitzades de:

a) Procediments de gestió d'incidents i riscos.

b) Sistemes de classificació d'incidents, riscos i informació.

Article 13. *Punt de contacte únic.*

El Consell de Seguretat Nacional exerceix, a través del Departament de Seguretat Nacional, una funció d'enllaç per garantir la cooperació transfronterera de les autoritats competents designades de conformitat amb l'article 9 amb les autoritats competents d'altres estats membres de la Unió Europea, així com amb el grup de cooperació i la xarxa de CSIRT.

Article 14. *Cooperació amb altres autoritats amb competències en seguretat de la informació i amb les autoritats sectorials.*

1. Les autoritats competents, els CSIRT de referència i el punt de contacte únic han de consultar, quan sigui procedent, els òrgans amb competències en matèria de seguretat

nacional, seguretat pública, seguretat ciutadana i protecció de dades de caràcter personal i hi han de col·laborar en l'exercici de les seves respectives funcions.

2. Així mateix, han de consultar, quan sigui procedent, els òrgans amb competències per raó de la matèria en cadascun dels sectors inclosos en l'àmbit d'aplicació d'aquest Reial decret llei, i hi han de col·laborar en l'exercici de les seves funcions.

3. Quan els incidents notificats presentin caràcters de delicte, les autoritats competents i els CSIRT de referència n'han de donar compte, a través de l'Oficina de Coordinació Cibernètica del Ministeri de l'Interior, al Ministeri Fiscal als efectes corresponents, i li han de traslladar al mateix temps tota la informació que tinguin en relació amb això.

Article 15. *Confidencialitat de la informació sensible.*

Sense perjudici del que disposa l'article 5, les autoritats competents, els CSIRT de referència i el punt de contacte únic han de preservar, com correspongui d'acord amb el dret, la seguretat i els interessos comercials dels operadors de serveis essencials i els proveïdors de serveis digitals, així com la confidencialitat de la informació que obtenen d'aquests en l'exercici de les funcions que els encomana aquest Reial decret llei.

Quan això sigui necessari, l'intercanvi d'informació sensible s'ha de limitar a la que sigui pertinent i proporcionada per a la finalitat d'aquest intercanvi.

TÍTOL IV

Obligacions de seguretat

Article 16. *Obligacions de seguretat dels operadors de serveis essencials i dels proveïdors de serveis digitals.*

1. Els operadors de serveis essencials i els proveïdors de serveis digitals han d'adoptar mesures tècniques i d'organització, adequades i proporcionades, per gestionar els riscos que es plantegin per a la seguretat de les xarxes i els sistemes d'informació utilitzats en la prestació dels serveis subjectes a aquest Reial decret llei.

Sense perjudici del seu deure de notificar incidents de conformitat amb el títol V, han de prendre mesures adequades per prevenir i reduir al mínim l'impacte dels incidents que els afectin.

2. El desplegament reglamentari d'aquest Reial decret llei ha de preveure les mesures necessàries per al compliment del que preceptua l'apartat anterior per part dels operadors de serveis essencials.

3. Els operadors de serveis essencials han de designar i comunicar a l'autoritat competent, en el termini que s'estableixi reglamentàriament, la persona, la unitat o l'òrgan col·legiat responsable de la seguretat de la informació, com a punt de contacte i de coordinació tècnica amb aquella.

Les seves funcions específiques són les previstes reglamentàriament.

4. Les autoritats competents poden establir mitjançant una ordre ministerial obligacions específiques per garantir la seguretat de les xarxes i els sistemes d'informació que emprin els operadors de serveis essencials. Així mateix, poden dictar instruccions tècniques i guies orientatives per detallar el contingut d'aquestes ordres.

Quan elaborin les disposicions reglamentàries, les instruccions i les guies, han de tenir en compte les obligacions sectorials, les directrius rellevants que s'adoptin en el grup de cooperació i els requisits en matèria de seguretat de la informació, a les quals estigui sotmès l'operador en virtut d'altres normes, com la Llei 8/2011, de 28 d'abril, i l'Esquema Nacional de Seguretat, aprovat pel Reial decret 3/2010, de 8 de gener.

5. Les autoritats competents s'han de coordinar entre si i amb els diferents òrgans sectorials amb competències per raó de la matèria, pel que fa al contingut i a l'aplicació de les ordres, les instruccions tècniques i les guies orientatives que dictin en els seus respectius àmbits de competència, per tal d'evitar duplicitats en les obligacions exigibles i facilitar-ne el compliment als operadors de serveis essencials.

6. Els proveïdors de serveis digitals han de determinar les mesures de seguretat que apliquin, tenint en compte, com a mínim, els avenços tècnics i els aspectes següents:

a) La seguretat dels sistemes i les instal·lacions;
b) La gestió d'incidents;
c) La gestió de la continuïtat de les activitats;
d) La supervisió, les auditories i les proves;
e) El compliment de les normes internacionals.

Els proveïdors de serveis digitals han d'atendre igualment els actes d'execució pels quals la Comissió Europea detalli els aspectes esmentats.

Article 17. *Normes tècniques.*

Les autoritats competents han de promoure la utilització de regulacions, normes o especificacions tècniques en matèria de seguretat de les xarxes i els sistemes d'informació elaborades en el marc del Reglament (UE) 1025/2012 del Parlament Europeu i del Consell, de 25 d'octubre de 2012, sobre la normalització europea.

En absència d'aquestes normes o especificacions, han de promoure l'aplicació de les normes o les recomanacions internacionals aprovades pels organismes internacionals de normalització, i, si s'escau, de les normes i especificacions tècniques acceptades en l'àmbit europeu o internacional que siguin pertinents en aquesta matèria.

Article 18. *Sectors amb una normativa específica equivalent.*

Quan una normativa nacional o comunitària estableixi per a un sector obligacions de seguretat de les xarxes i els sistemes d'informació o de notificació d'incidents que tinguin efectes, almenys, equivalents als de les obligacions que preveu aquest Reial decret llei, prevalen aquells requisits i els mecanismes de supervisió corresponents.

Això no afecta el deure de cooperació entre autoritats competents, la coordinació que exerceix el Consell de Seguretat Nacional ni, en la mesura en què no sigui incompatible amb la legislació sectorial, l'aplicació del títol V sobre notificació d'incidents.

TÍTOL V

Notificació d'incidents

Article 19. *Obligació de notificar.*

1. Els operadors de serveis essencials han de notificar a l'autoritat competent, a través del CSIRT de referència, els incidents que puguin tenir efectes pertorbadors significatius en aquests serveis.

Les notificacions es poden referir també, segons es determini reglamentàriament, als successos o les incidències que puguin afectar les xarxes i els sistemes d'informació emprats per a la prestació dels serveis essencials, però que encara no hagin tingut un efecte advers real sobre aquells.

2. Així mateix, els proveïdors de serveis digitals han de notificar a l'autoritat competent, a través del CSIRT de referència, els incidents que tinguin efectes pertorbadors significatius en aquests serveis.

L'obligació de la notificació de l'incident únicament s'aplica quan el proveïdor de serveis digitals tingui accés a la informació necessària per valorar l'impacte d'un incident.

3. Les notificacions tant d'operadors de serveis essencials com de proveïdors de serveis digitals s'han de referir als incidents que afectin les xarxes i els sistemes d'informació emprats en la prestació dels serveis indicats, tant si es tracta de xarxes i serveis propis com si són de proveïdors externs, fins i tot si aquests són proveïdors de serveis digitals sotmesos a aquest Reial decret llei.

4. Les autoritats competents i els CSIRT de referència han d'utilitzar una plataforma comuna per facilitar i automatitzar els processos de notificació, comunicació i informació sobre incidents.

5. El desplegament reglamentari d'aquest Reial decret llei ha de preveure les mesures necessàries per al compliment del que preceptua aquest article per part dels operadors de serveis essencials. Les autoritats competents poden establir, mitjançant una ordre ministerial, obligacions específiques de notificació dels operadors de serveis essencials. Així mateix, poden dictar instruccions tècniques i guies orientatives per detallar el contingut d'aquestes ordres.

Quan s'elaborin les disposicions reglamentàries, les instruccions i les guies, s'han de tenir en compte les obligacions sectorials, les directrius rellevants que s'adoptin en el grup de cooperació i els requisits en matèria de notificació d'incidents a les quals estigui sotmès l'operador en virtut d'altres normes, com la Llei 8/2011, de 28 d'abril, i l'Esquema Nacional de Seguretat, aprovat pel Reial decret 3/2010, de 8 de gener.

6. L'obligació de notificació d'incidents que preveuen els apartats anteriors no obsta per al compliment dels deures legals de denúncia dels fets que tinguin caràcters de delicte davant les autoritats competents, d'acord amb el que disposen els articles 259 i següents de la Llei d'enjudiciament criminal i tenint en compte el que preveu l'article 14.3 d'aquest Reial decret llei.

Article 20. *Protecció del notificador.*

1. Les notificacions considerades en aquest títol no subjecten l'entitat que les efectuï a una responsabilitat superior.

2. Els empleats i el personal que, per qualsevol tipus de relació laboral o mercantil, participin en la prestació dels serveis essencials o digitals i que informin sobre incidents no poden patir conseqüències adverses en el seu lloc de treball o amb l'empresa, tret dels supòsits en què s'acrediti mala fe en la seva actuació.

S'entenen nul·les i sense efecte legal les decisions de l'ocupador preses en perjudici o en detriment dels drets laborals dels treballadors que hagin actuat de conformitat amb aquest apartat.

Article 21. *Factors per determinar la importància dels efectes d'un incident.*

1. Als efectes de les notificacions a què es refereix l'article 19.1, primer paràgraf, la importància d'un incident es determina tenint en compte, com a mínim, els factors següents:

a) El nombre d'usuaris afectats per la pertorbació del servei essencial.
b) La durada de l'incident.
c) L'extensió o les àrees geogràfiques afectades per l'incident.
d) El grau de pertorbació del funcionament del servei.
e) L'abast de l'impacte en activitats econòmiques i socials crucials.
f) La importància dels sistemes afectats o de la informació afectada per l'incident per a la prestació del servei essencial.
g) El dany a la reputació.

2. En les notificacions a què es refereix l'article 19.2, la importància d'un incident es determina de conformitat amb el que estableixin els actes d'execució que preveuen els apartats 8 i 9 de l'article 16 de la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016.

Article 22. *Notificació inicial, notificacions intermèdies i notificació final.*

1. Els operadors de serveis essencials han de fer una primera notificació dels incidents a què es refereix l'article 19.1 sense cap dilació indeguda.

La notificació ha d'incloure, entre altres dades, informació que permeti determinar qualsevol efecte transfronterer de l'incident.

2. Els operadors de serveis essencials han d'efectuar les notificacions intermèdies que siguin necessàries per actualitzar la informació incorporada a la notificació inicial i informar sobre l'evolució de l'incident, mentre aquest no estigui resolt.

3. Els operadors de serveis essencials han d'enviar una notificació final de l'incident un cop s'hagi resolt.

Un incident es considera resolt quan s'hagin restablert les xarxes i els sistemes d'informació afectats i el servei operi amb normalitat.

Article 23. *Flexibilitat en l'observança dels terminis per a la notificació.*

Els operadors de serveis essencials i els proveïdors de serveis digitals poden ometre, en les comunicacions que facin sobre els incidents que els afectin, la informació que encara no tinguin relativa a la seva repercussió sobre serveis essencials o altres serveis que depenguin d'ells per a la seva prestació, o qualsevol altra informació que no tinguin. Tan aviat com coneguin aquesta informació l'han de trametre a l'autoritat competent.

Si, un cop transcorregut un temps prudencial des de la notificació inicial de l'incident, l'operador de serveis essencials o el proveïdor de serveis digitals no ha pogut reunir la informació pertinent, ha d'enviar a l'autoritat competent, sense demora, un informe justificatiu de les actuacions dutes a terme per reunir la informació i dels motius pels quals no ha estat possible obtenir-la.

Article 24. *Incidents que afectin serveis digitals.*

Els operadors de serveis essencials i els proveïdors de serveis digitals sotmesos a aquest Reial decret llei, així com qualsevol altra part interessada, que tinguin notícia d'incidents que afectin de manera significativa serveis digitals oferts a Espanya per proveïdors establerts en altres estats membres de la Unió Europea, ho poden notificar a l'autoritat competent juntament amb la informació pertinent, a l'objecte de facilitar la cooperació amb l'Estat membre en què estigui establert el proveïdor esmentat.

De la mateixa manera, si tenen notícia que aquests proveïdors han incomplert els requisits de seguretat o de notificació d'incidents succeïts a Espanya que els són aplicables, ho poden notificar a l'autoritat competent juntament amb la informació pertinent.

Article 25. *Tramitació d'incidents amb impacte transfronterer.*

1. Quan les autoritats competents o els CSIRT de referència tinguin notícia d'incidents que poden afectar altres estats membres de la Unió Europea, n'han d'informar a través del punt de contacte únic els estats membres afectats, i precisar si l'incident pot tenir efectes pertorbadors significatius per als serveis essencials prestats en aquests estats.

2. Quan a través del punt de contacte es rebi informació sobre incidents notificats en altres països de la Unió Europea que puguin tenir efectes pertorbadors significatius per als serveis essencials prestats a Espanya, s'ha de trametre la informació rellevant a l'autoritat competent i al CSIRT de referència, perquè adoptin les mesures pertinents en l'exercici de les seves funcions respectives.

3. Les actuacions considerades als apartats anteriors s'entenen sense perjudici dels intercanvis d'informació que les autoritats competents o els CSIRT de referència puguin fer de manera directa amb els seus homòlegs d'altres estats membres de la Unió Europea en relació amb els incidents que puguin ser d'interès mutu.

Article 26. *Informació al públic.*

1. L'autoritat competent pot exigir als operadors de serveis essencials o als proveïdors de serveis digitals que informin el públic o tercers potencialment interessats sobre els incidents quan el seu coneixement sigui necessari per evitar nous incidents o gestionar-ne un que ja s'hagi produït, o quan la divulgació d'un incident redundi en benefici de l'interès públic.

2. L'autoritat competent també pot decidir informar de manera directa el públic o tercers sobre l'incident.

En aquests casos l'autoritat competent ha de consultar i s'ha de coordinar amb l'operador de serveis essencials o el proveïdor de serveis digitals abans d'informar el públic.

Article 27. *Informació anual al punt de contacte únic i al grup de cooperació.*

1. Les autoritats competents han de transmetre al punt de contacte únic un informe anual sobre el nombre i el tipus d'incidents comunicats, els seus efectes en els serveis prestats o en altres serveis i el seu caràcter nacional o transfronterer dins de la Unió Europea.

Les autoritats competents han d'elaborar l'informe seguint les instruccions que dicti el punt de contacte únic tenint en compte les indicacions del grup de cooperació respecte al format i el contingut de la informació que cal transmetre.

2. El punt de contacte únic ha de trametre al grup de cooperació abans del 9 d'agost de cada any un informe anual resumit sobre les notificacions rebudes, i l'ha de trametre ulteriorment a les autoritats competents i als CSIRT de referència, per al seu coneixement.

Article 28. *Obligació de resoldre els incidents, d'informació i de col·laboració mútua.*

1. Els operadors de serveis essencials i els proveïdors de serveis digitals tenen l'obligació de resoldre els incidents de seguretat que els afectin, i de sol·licitar ajuda especialitzada, inclosa la del CSIRT de referència, quan no puguin resoldre per si mateixos els incidents.

En aquests casos han d'atendre les indicacions que rebin del CSIRT de referència per resoldre l'incident, mitigar-ne els efectes i reposar els sistemes afectats.

2. Els operadors de serveis essencials i els proveïdors de serveis digitals han de subministrar al CSIRT de referència i a l'autoritat competent tota la informació que se'ls requereixi per a l'exercici de les funcions que els encomana aquest Reial decret llei.

En particular, es pot requerir informació addicional als operadors de serveis essencials i als proveïdors de serveis digitals per analitzar la naturalesa, les causes i els efectes dels incidents notificats, i per elaborar estadístiques i reunir les dades necessàries per elaborar els informes anuals considerats a l'article 27.

Quan les circumstàncies ho permetin, l'autoritat competent o el CSIRT de referència han de proporcionar als operadors de serveis essencials o als proveïdors de serveis digitals afectats per incidents la informació derivada del seu seguiment que els pugui ser rellevant, en particular, per resoldre l'incident.

Article 29. *Cooperació pel que fa als incidents que afectin dades personals.*

Les autoritats competents i els CSIRT de referència han de cooperar estretament amb l'Agència Espanyola de Protecció de Dades per fer front als incidents que donin lloc a violacions de dades personals.

Les autoritats competents i els CSIRT de referència han de comunicar sense dilació a l'Agència Espanyola de Protecció de Dades els incidents que puguin suposar una vulneració de dades personals i l'han de mantenir informada sobre l'evolució d'aquests incidents.

Article 30. *Autorització per a la cessió de dades personals.*

Si la notificació d'incidents o la seva gestió, anàlisi o resolució requereix comunicar dades personals, el seu tractament s'ha de restringir a les que siguin estrictament adequades, pertinents i limitades al que sigui necessari en relació amb la finalitat, de les indicades, que es persegueixi en cada cas.

La seva cessió per a aquests fins s'entén autoritzada en els casos següents:

a) Dels operadors de serveis essencials i els proveïdors de serveis digitals a les autoritats competents, a través dels CSIRT de referència.
b) Entre els CSIRT de referència i les autoritats competents, i viceversa.
c) Entre els CSIRT de referència, i entre aquests i els CSIRT designats en altres estats membres de la Unió Europea.
d) Entre els CSIRT de referència i altres CSIRT nacionals o internacionals.
e) Entre el punt de contacte únic i els punts de contacte únics d'altres estats membres de la Unió Europea.

Article 31. *Notificacions voluntàries.*

1. Els operadors de serveis essencials i els proveïdors de serveis digitals poden notificar els incidents per als quals no s'estableixi una obligació de notificació.

Així mateix, les entitats que prestin serveis essencials i no hagin estat identificades com a operadors de serveis essencials i que no siguin proveïdors de serveis digitals poden notificar els incidents que afectin els serveis.

Aquestes notificacions obliguen l'entitat que les efectuï a resoldre l'incident d'acord amb el que estableix l'article 28.

2. Les notificacions a què es refereix l'apartat anterior es regeixen pel que disposa aquest títol, i s'ha d'informar sobre aquestes el punt de contacte únic en l'informe anual que preveu l'article 27.1.

3. Les notificacions obligatòries gaudeixen de prioritat sobre les voluntàries a l'efecte de la seva gestió per part dels CSIRT i les autoritats competents.

TÍTOL VI

Supervisió

Article 32. *Supervisió dels operadors de serveis essencials.*

1. Les autoritats competents poden requerir els operadors de serveis essencials perquè els proporcionin tota la informació necessària per avaluar la seguretat de les xarxes i els sistemes d'informació, inclosa la documentació sobre polítiques de seguretat.

Els poden requerir informació sobre l'aplicació efectiva de la seva política de seguretat, així com auditar l'operador o exigir-li que sotmeti la seguretat de les seves xarxes i sistemes d'informació a una auditoria d'una entitat externa, solvent i independent.

2. A la vista de la informació obtinguda, l'autoritat competent pot requerir a l'operador que repari les deficiències detectades i indicar-li com ho ha de fer.

Article 33. *Supervisió dels proveïdors de serveis digitals.*

1. L'autoritat competent per a la supervisió dels serveis digitals només ha d'inspeccionar el compliment de les obligacions que deriven d'aquest Reial decret llei quan tingui notícia d'algun incompliment, incloses la petició raonada d'altres òrgans o una denúncia.

En aquest cas, l'autoritat competent pot requerir el proveïdor de serveis digitals perquè li proporcioni tota la informació necessària per avaluar la seguretat de les seves xarxes i sistemes d'informació, inclosa la documentació sobre polítiques de seguretat, i perquè repari les deficiències detectades.

2. Quan l'autoritat competent tingui notícia d'incidents que pertorbin de manera significativa serveis digitals oferts en altres estats membres per proveïdors establerts a Espanya, ha d'adoptar les mesures de supervisió pertinents.

A aquests efectes, ha de tenir especialment en compte la informació que facilitin les autoritats competents d'altres estats membres.

Article 34. *Cooperació transfronterera.*

1. La supervisió s'ha de dur a terme, quan sigui procedent, en cooperació amb les autoritats competents dels estats membres en què s'ubiquin les xarxes i els sistemes d'informació emprats per a la prestació del servei, o en què estigui establert l'operador de serveis essencials, el proveïdor de serveis digitals o el seu representant.

2. Les autoritats competents han de col·laborar amb les autoritats competents d'altres estats membres quan aquestes requereixin la seva cooperació en la supervisió i l'adopció de mesures per part d'operadors de serveis essencials i proveïdors de serveis digitals en relació amb les xarxes i els sistemes d'informació ubicats a Espanya, així com respecte als proveïdors de serveis digitals establerts a Espanya o que tinguin un representant a la Unió Europea amb residència o domicili social a Espanya.

TÍTOL VII

Règim sancionador

Article 35. *Responsables.*

Són responsables els operadors de serveis essencials i els proveïdors de serveis digitals compresos en l'àmbit d'aplicació d'aquest Reial decret llei.

Article 36. *Infraccions.*

1. Les infraccions dels preceptes d'aquest Reial decret llei es classifiquen en molt greus, greus i lleus.

2. Són infraccions molt greus:

a) La manca d'adopció de mesures per reparar les deficiències detectades, d'acord amb el que disposen els articles 32.2 o 33.1, quan aquestes l'hagin fet vulnerable a un incident amb efectes pertorbadors significatius en el servei i l'operador de serveis essencials o el proveïdor de serveis digitals no hagi atès els requeriments dictats per l'autoritat competent abans de la producció de l'incident.

b) L'incompliment reiterat de l'obligació de notificar incidents amb efectes pertorbadors significatius en el servei. Es considera que és reiterat a partir del segon incompliment.

c) No prendre les mesures necessàries per resoldre els incidents d'acord amb el que disposa l'article 28.1 quan aquests tinguin un efecte pertorbador significatiu en la prestació de serveis essencials o de serveis digitals a Espanya o a altres estats membres.

3. Són infraccions greus:

a) L'incompliment de les disposicions reglamentàries o de les instruccions tècniques de seguretat que dicti l'autoritat competent referides a les precaucions mínimes que els operadors de serveis essencials han d'adoptar per garantir la seguretat de les xarxes i els sistemes d'informació.

b) La manca d'adopció de mesures per reparar les deficiències detectades en resposta a un requeriment dictat d'acord amb els articles 32.2 o 33.1, quan aquest sigui el tercer requeriment desatès que es dicta en els cinc últims anys.

c) L'incompliment de l'obligació de notificar incidents amb efectes pertorbadors significatius en el servei.

d) La demostració d'una manca d'interès notòria en la resolució d'incidents amb efectes pertorbadors significatius notificats quan doni lloc a una degradació més gran del servei.

e) Proporcionar informació falsa o enganyosa al públic sobre els estàndards que compleix o les certificacions de seguretat que manté en vigor.

f) Posar obstacles a la pràctica d'auditories per part de l'autoritat competent.

4. Són infraccions lleus:

a) L'incompliment de les disposicions reglamentàries o de les instruccions tècniques de seguretat que dicti l'autoritat competent a l'empara d'aquest Reial decret llei, quan no suposi una infracció greu.
b) La manca d'adopció de mesures per corregir les deficiències detectades en resposta a un requeriment d'esmena dictat d'acord amb els articles 32.2 o 33.1.
c) No facilitar la informació que requereixin les autoritats competents sobre les seves polítiques de seguretat, o proporcionar una informació incompleta o tardana sense cap justificació.
d) No sotmetre's a una auditoria de seguretat segons el que ordeni l'autoritat competent.
e) No proporcionar al CSIRT de referència o a l'autoritat competent la informació que sol·licitin en virtut de l'article 28.2.
f) La manca de notificació dels successos o les incidències per als quals, encara que no hagin tingut un efecte advers real sobre els serveis, hi hagi l'obligació de notificació en virtut del paràgraf segon de l'article 19.2.
g) No completar la informació que ha de contenir la notificació d'incidents tenint en compte el que disposa l'article 23, o no trametre l'informe justificatiu sobre la impossibilitat d'obtenir la informació que preveu l'article esmentat.
h) No seguir les indicacions que rebi del CSIRT de referència per resoldre un incident, d'acord amb l'article 28.

Article 37. *Sancions.*

1. Per la comissió de les infraccions que recull l'article anterior, s'imposen les sancions següents:

a) Per la comissió d'infraccions molt greus, multa de 500.001 fins a 1.000.000 euros.
b) Per la comissió d'infraccions greus, multa de 100.001 fins a 500.000 euros.
c) Per la comissió d'infraccions lleus, amonestació o multa fins a 100.000 euros.

2. Les sancions fermes en la via administrativa per infraccions molt greus i greus es poden publicar, a càrrec del sancionat, al «Butlletí Oficial de l'Estat» i al lloc d'Internet de l'autoritat competent, segons els fets concurrents i de conformitat amb l'article següent.

Article 38. *Graduació de la quantia de les sancions.*

L'òrgan sancionador ha d'establir la sanció tenint en compte els criteris següents:

a) El grau de culpabilitat o l'existència d'intencionalitat.
b) La continuïtat o la persistència en la conducta infractora.
c) La naturalesa i la quantia dels perjudicis causats.
d) La reincidència, per la comissió en l'últim any de més d'una infracció de la mateixa naturalesa, quan així ho hagi declarat una resolució ferma en la via administrativa.
e) El nombre d'usuaris afectats.
f) El volum de facturació del responsable.
g) La utilització per part del responsable de programes d'una recompensa pel descobriment de vulnerabilitats a les seves xarxes i sistemes d'informació.
h) Les accions que hagi dut a terme el responsable per pal·liar els efectes o les conseqüències de la infracció.

Article 39. *Proporcionalitat de sancions.*

1. L'òrgan sancionador pot establir la quantia de la sanció aplicant l'escala relativa a la classe d'infraccions que precedeixi immediatament en gravetat a aquella en què s'integra la considerada en el cas de què es tracti, en els supòsits següents:

a) Quan s'apreciï una qualificada disminució de la culpabilitat de l'imputat com a conseqüència de la concurrència significativa d'uns quants dels criteris que enuncia l'article 38.

b) Quan l'entitat infractora hagi regularitzat la situació irregular de manera diligent.
c) Quan l'infractor hagi reconegut espontàniament la seva culpabilitat.

2. Els òrgans amb competència sancionadora, atesa la naturalesa dels fets i la concurrència significativa dels criteris que estableix l'apartat anterior, poden no acordar l'inici del procediment sancionador i, en lloc d'això, advertir el subjecte responsable a fi que, en el termini que l'òrgan sancionador determini, acrediti l'adopció de les mesures correctores que, en cada cas, siguin pertinents, sempre que concorrin els pressupòsits següents:

a) Que els fets siguin constitutius d'una infracció lleu o greu de conformitat amb el que disposa aquest Reial decret llei.
b) Que l'òrgan competent no hagi sancionat o advertit l'infractor en els dos anys previs com a conseqüència de la comissió d'infraccions previstes en aquest Reial decret llei.

Si l'advertència no s'atén en el termini que l'òrgan sancionador determini, és procedent obrir el procediment sancionador corresponent per l'incompliment.
3. No poden ser objecte d'advertència les infraccions lleus que descriu l'article 36.4 c), d) i e) i la infracció greu que preveu l'article 36.3 e).

Article 40. *Infraccions de les administracions públiques.*

1. Quan les infraccions a què es refereix l'article 36 les cometin òrgans o entitats de les administracions públiques, l'òrgan sancionador ha de dictar una resolució en què estableixi les mesures que escau adoptar perquè cessin o es corregeixin els efectes de la infracció. Aquesta resolució s'ha de notificar a l'òrgan o l'entitat infractora i als afectats, si n'hi ha.
A més de tot això, l'òrgan sancionador pot proposar també la iniciació d'actuacions disciplinàries, si són procedents.
2. S'han de comunicar a l'òrgan sancionador les resolucions que es dictin en relació amb les mesures i les actuacions a què es refereix l'apartat anterior.

Article 41. *Competència sancionadora.*

1. La imposició de sancions correspon, en el cas d'infraccions molt greus, al ministre competent en virtut del que disposa l'article 9, i en el cas d'infraccions greus i lleus a l'òrgan de l'autoritat competent que es determini mitjançant el reglament de desplegament d'aquest Reial decret llei.
2. La potestat sancionadora s'ha d'exercir d'acord amb els principis i el procediment que preveuen les lleis 39/2015, d'1 d'octubre, del procediment administratiu comú de les administracions públiques, i 40/2015, d'1 d'octubre, de règim jurídic del sector públic.
3. L'exercici de la potestat sancionadora s'ha de subjectar al procediment aplicable, amb caràcter general, a l'actuació de les administracions públiques. No obstant això, el termini màxim de durada del procediment és d'un any i el termini d'al·legacions no ha de tenir una durada inferior a un mes.

Article 42. *Concurrència d'infraccions.*

1. No és procedent la imposició de sancions segons el que preveu aquest Reial decret llei quan els fets constitutius d'infracció ho siguin també d'una altra tipificada en la normativa sectorial a què estigui subjecte el prestador del servei i hi hagi identitat del bé jurídic protegit.
2. Quan, com a conseqüència d'una actuació sancionadora, es tingui coneixement de fets que poden ser constitutius d'infraccions tipificades en altres lleis, se n'ha de donar compte als òrgans o organismes competents per a la seva supervisió i sanció.

Disposició addicional primera. *Relació inicial de serveis essencials i operadors de serveis essencials.*

La Comissió Nacional per a la Protecció de les Infraestructures Crítiques ha d'aprovar una primera llista de serveis essencials dins dels sectors inclosos en l'àmbit d'aplicació d'aquest Reial decret llei i ha d'identificar els operadors que els prestin que s'han de subjectar a aquest Reial decret llei en l'ordre següent:

a) Abans del 9 de novembre de 2018: els serveis essencials i els operadors corresponents als sectors estratègics energia, transport, salut, sistema financer, aigua, i infraestructures digitals.

b) Abans del 9 de novembre de 2019: els serveis essencials i els operadors corresponents a la resta dels sectors estratègics que recull l'annex de la Llei 8/2011, de 28 d'abril.

Disposició addicional segona. *Comunicacions electròniques i serveis de confiança.*

L'aplicació d'aquest Reial decret llei als operadors de xarxes i serveis de comunicacions electròniques i de serveis electrònics de confiança que siguin designats com a operadors crítics en virtut de la Llei 8/2011, de 28 d'abril, no obsta a l'aplicació de la seva normativa específica en matèria de seguretat.

El Ministeri d'Economia i Empresa, com a òrgan competent per a l'aplicació de la normativa esmentada, i el Ministeri de l'Interior han d'actuar de manera coordinada en l'establiment d'obligacions que recaiguin sobre els operadors crítics. Així mateix, han de mantenir un intercanvi fluid d'informació sobre incidents que els afectin.

Disposició addicional tercera. *Notificació de violacions de seguretat de les dades personals a través de la plataforma comuna que preveu aquest Reial decret llei.*

La plataforma comuna per a la notificació d'incidents que preveu aquest Reial decret llei es pot emprar per a la notificació de vulneracions de la seguretat de dades personals segons el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de dades personals i a la lliure circulació d'aquestes dades i pel qual es deroga la Directiva 95/46/CE, en els termes que acordin l'Agència Espanyola de Protecció de Dades i els òrgans que gestionin aquesta plataforma.

Disposició addicional quarta. *Proveïdors de serveis digitals ja existents.*

Els proveïdors de serveis digitals que ja prestin serveis han de comunicar la seva activitat a la Secretaria d'Estat per a l'Avanç Digital del Ministeri d'Economia i Empresa, en el termini de tres mesos des de l'entrada en vigor d'aquest Reial decret llei.

Disposició final primera. *Títol competencial.*

Aquest Reial decret llei es dicta en virtut de les competències exclusives que atribueix a l'Estat en matèria de règim general de telecomunicacions i seguretat pública l'article 149.1.21a i 29a de la Constitució.

Disposició final segona. *Incorporació del dret de la Unió Europea.*

Aquest Reial decret llei incorpora a l'ordenament jurídic intern la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, relativa a les mesures destinades a garantir un elevat nivell comú de seguretat de les xarxes i els sistemes d'informació en la Unió.

Disposició final tercera. *Habilitació per al desplegament reglamentari.*

S'habilita el Govern per desplegar reglamentàriament el que preveu aquest Reial decret llei sense perjudici de la competència dels ministres per fixar les obligacions específiques mitjançant una ordre ministerial en els supòsits que preveu l'articulat d'aquesta norma.

Disposició final quarta. *Entrada en vigor.*

Aquest Reial decret llei entra en vigor l'endemà de la publicació en el «Butlletí Oficial de l'Estat».

Madrid, 7 de setembre de 2018.

FELIPE R.

El president del Govern,
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN