I. DISPOSICIONS GENERALS

MINISTERI DE LA PRESIDÈNCIA, RELACIONS AMB LES CORTS I MEMÒRIA DEMOCRÀTICA

1192 *Reial decret 43/2021, de 26 de gener, pel qual es desplega el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i els sistemes d'informació.*

En l'àmbit europeu, amb l'objectiu de donar una resposta efectiva als problemes de seguretat de les xarxes i els sistemes d'informació, es va aprovar 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, coneguda com la Directiva NIS (Security of Network and Information Systems). Aquesta norma parteix d'un enfocament global de la seguretat de les xarxes i els sistemes d'informació a la Unió Europea, i integra requisits mínims comuns en matèria de desenvolupament de capacitats i planificació, intercanvi d'informació, cooperació i requisits comuns de seguretat per als operadors de serveis essencials i els proveïdors de serveis digitals.

La transposició de la Directiva NIS a l'ordenament jurídic espanyol es va portar a terme mitjançant el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació. Aquesta norma legal regula la seguretat de les xarxes i els sistemes d'informació utilitzats per a la provisió dels serveis essencials i dels serveis digitals, estableix mecanismes que, amb una perspectiva integral, permeten millorar la protecció enfront de les amenaces que afecten les xarxes i els sistemes d'informació, i fixa un marc institucional de cooperació que facilita 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.

El Reial decret llei 12/2018, de 7 de setembre, habilita el Govern, en la seva disposició final tercera, per al seu desplegament reglamentari. Amb aquesta cobertura legal, i en compliment del manament esmentat i del que preveuen els seus articles 9.1 a), 11.1 a), 11.2, 16.2, 16.3, 19.1 i 19.5, aquest Reial decret té per finalitat desplegar el Reial decret llei 12/2018, de 7 de setembre, pel que fa al marc estratègic i institucional de seguretat de les xarxes i els sistemes d'informació, al compliment de les obligacions de seguretat dels operadors de serveis essencials i dels proveïdors de serveis digitals i a la gestió d'incidents de seguretat.

El Reial decret, en l'article 3, detalla la designació d'autoritats competents en matèria de seguretat de les xarxes i els sistemes d'informació que preveu l'article 9.1.a) 2n del Reial decret llei 12/2018, de 7 de setembre. És oportú esmentar, en relació amb la seguretat en el sector de l'alimentació, la participació de l'Agència Espanyola de Seguretat Alimentària i Nutrició, que depèn del Ministeri de Consum. Addicionalment, i de conformitat amb l'article 11 del Reial decret llei 12/2018, de 7 de setembre, el Reial decret desplega els supòsits de cooperació i coordinació entre els equips de resposta a incidents de seguretat informàtica (CSIRT) de referència, i d'aquests amb les autoritats competents, que s'instrumenten a través de la Plataforma Nacional de Notificació i Seguiment de Ciberincidents (article 4).

En relació amb la figura del punt de contacte únic (article 5) que consagra la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, es despleguen les seves funcions d'enllaç per garantir la cooperació transfronterera amb les autoritats competents d'altres estats membres de la Unió Europea, així com amb el grup de cooperació i la xarxa de CSIRT.

D'altra banda, l'article 6 d'aquest Reial decret desplega les previsions de l'article 16.2 del Reial decret llei 12/2018, de 7 de setembre, sobre les mesures necessàries perquè els

operadors de serveis essencials compleixin les obligacions de seguretat, que s'han de concretar en una declaració d'aplicabilitat de mesures de seguretat subscrita pel responsable de seguretat de la informació de l'operador, les funcions del qual també es despleguen a l'article 7 d'aquest Reial decret. El termini per designar el responsable de la seguretat s'estableix en compliment de l'habilitació que recull l'article 16.3 del Reial decret llei 12/2018, de 7 de setembre.

Pel que fa a la notificació d'incidents, el Reial decret, en els seus articles 8 i 9, desplega les obligacions de notificació per part dels operadors de serveis essencials dels incidents que puguin tenir efectes pertorbadors significatius en aquests serveis, així com dels incidents que puguin afectar les xarxes i els sistemes d'informació utilitzats per prestar els serveis essencials encara que no hagin tingut un efecte advers real sobre aquells, per referència als nivells d'impacte i perillositat, segons sigui el cas, que preveu la Instrucció nacional de notificació i gestió de ciberincidents que conté l'annex.

El procediment de notificació d'incidents s'articula a través de la Plataforma Nacional de Notificació i Seguiment de Ciberincidents (articles 10 i 11), a fi de permetre l'intercanvi d'informació entre els operadors de serveis essencials i proveïdors de serveis digitals, les autoritats competents i els CSIRT de referència, i garantir la confidencialitat, integritat i disponibilitat de la informació (articles 12 a 14).

Finalment, en matèria de supervisió de requisits de seguretat, el Reial decret desplega en el seu article 15 l'obligació de col·laboració dels operadors de serveis essencials i els proveïdors de serveis digitals amb les autoritats competents, que poden requerir, així mateix, la col·laboració dels CSIRT de referència per a l'exercici de la seva funció de supervisió.

Les disposicions addicionals d'aquest Reial decret recullen, entre altres matèries, el règim jurídic aplicable al Banc d'Espanya tenint en compte la seva configuració jurídica especial com a entitat de dret públic amb personalitat jurídica pròpia i plena capacitat pública i privada, que en l'exercici de la seva activitat i per al compliment dels seus fins actua amb autonomia respecte a l'Administració General de l'Estat, i com a part integrant del Sistema Europeu de Bancs Centrals (SEBC) i del Mecanisme Únic de Supervisió (MUS). Aquesta configuració jurídica especial suposa que el marc de seguretat de les xarxes i els sistemes d'informació sigui aplicable en la mesura que no interfereixi amb la naturalesa, les funcions i la independència del Banc d'Espanya.

Aquest Reial decret 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. Respon, en primer lloc, als principis de necessitat i eficàcia, ja que la norma és necessària per portar a terme el desplegament reglamentari del Reial decret llei 12/2018, de 7 de setembre, que transposa la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, i, en concret, per establir el marc estratègic i institucional de seguretat de les xarxes i els sistemes d'informació, les obligacions de seguretat i la gestió d'incidents, i és l'instrument més idoni per aconseguir aquest objectiu. En segon terme, la norma compleix el principi de proporcionalitat, ja que no hi ha altres mesures menys costoses per als operadors de serveis essencials i proveïdors de serveis digitals destinades a complir l'obligació d'adoptar mesures tècniques i d'organització per gestionar els riscos per a la seguretat de les seves xarxes i sistemes d'informació, així com de notificar els incidents que tinguin efectes pertorbadors significatius en els serveis que presten. Així mateix, aquest Reial decret compleix el principi de seguretat jurídica, i el projecte és conforme a la directiva europea de la qual deriva, així com la Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques, i la seva normativa de desplegament, la Llei 36/2015, de 28 de setembre, de seguretat nacional, i la normativa comunitària i nacional en matèria de protecció de dades. S'ha complert igualment el principi de transparència, ja que s'ha sotmès el projecte de reial decret al tràmit d'audiència, i s'han definit clarament els objectius de la iniciativa normativa i la seva justificació. Finalment, aquest Reial decret és conforme al principi d'eficiència, atès que no s'estableixen càrregues addicionals a les que preveu el Reial decret llei que desplega.

En l'elaboració d'aquest Reial decret s'ha sol·licitat un informe de tots els departaments ministerials, així com de l'Agència Espanyola de Protecció de Dades, de la Comissió Nacional dels Mercats i la Competència, de la Comissió Nacional del Mercat de Valors, del Consell de Seguretat Nuclear i del Banc d'Espanya. Addicionalment, s'ha sol·licitat un informe a totes les comunitats autònomes i s'ha donat audiència a les organitzacions representatives dels sectors afectats.

En virtut d'això, a proposta conjunta de la vicepresidenta tercera del Govern i ministra d'Afers Econòmics i Transformació Digital, de la ministra de Defensa, del ministre de l'Interior i de la vicepresidenta primera del Govern i ministra de la Presidència, Relacions amb les Corts i Memòria Democràtica, amb l'aprovació prèvia de la ministra de Política Territorial i Funció Pública, d'acord amb el Consell d'Estat, i amb la deliberació prèvia del Consell de Ministres a la reunió del dia 26 de gener de 2021,

DISPOSO:

CAPÍTOL I

Disposicions generals

Article 1. *Objecte.*

Aquest Reial decret té per objecte desplegar el Reial decret llei 12/2018, de 7 de setembre, de seguretat de les xarxes i sistemes d'informació, pel que fa al marc estratègic i institucional de seguretat de les xarxes i els sistemes d'informació, la supervisió del compliment de les obligacions de seguretat dels operadors de serveis essencials i dels proveïdors de serveis digitals, i la gestió d'incidents de seguretat.

Article 2. *Àmbit d'aplicació.*

1. De conformitat amb l'article 2 del Reial decret llei 12/2018, de 7 de setembre, aquest Reial decret 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 que siguin mercats en línia, motors de cerca en línia i serveis d'informàtica en núvol.

2. Estan sotmesos a aquest Reial decret:

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 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.

De conformitat amb el que preveu l'apartat 1 de l'article 6 del Reial decret llei 12/2018, la identificació dels serveis essencials i dels operadors que els prestin l'han d'efectuar els òrgans i els procediments que preveuen la Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques, i la seva normativa de desplegament, en particular el Reial decret 704/2011, de 20 de maig, pel qual s'aprova el Reglament de protecció de les infraestructures crítiques.

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 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.

4. De conformitat amb l'article 18 del Reial decret llei 12/2018, de 7 de setembre, 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 el Reial decret llei 12/2018, de 7 de setembre, prevalen aquells requisits i els mecanismes de supervisió corresponents.

CAPÍTOL II

Marc estratègic i institucional

Article 3. *Autoritats competents.*

Les autoritats competents en matèria de seguretat de les xarxes i els sistemes d'informació són, amb caràcter general, les que estableix l'article 9.1 del Reial decret llei 12/2018, de 7 de setembre. En particular, són autoritats competents per als operadors de serveis essencials que no siguin operadors crítics d'acord amb la Llei 8/2011, de 28 d'abril, i que no estiguin inclosos en l'àmbit d'aplicació de la Llei 40/2015, d'1 d'octubre, de règim jurídic del sector públic, les següents:

a) Respecte al sector del transport: el Ministeri de Transports, Mobilitat i Agenda Urbana, a través de la Secretaria d'Estat de Transports, Mobilitat i Agenda Urbana.
b) Respecte al sector de l'energia: el Ministeri per a la Transició Ecològica i el Repte Demogràfic, a través de la Secretaria d'Estat d'Energia.
c) Respecte al sector de les tecnologies de la informació i les telecomunicacions: el Ministeri d'Afers Econòmics i Transformació Digital, a través de la Secretaria d'Estat de Digitalització i Intel·ligència Artificial i la Secretaria d'Estat de Telecomunicacions i Infraestructures Digitals.
d) Respecte al sector del sistema financer:

1r El Ministeri d'Afers Econòmics i Transformació Digital, a través de la Secretaria d'Estat d'Economia i Suport a l'Empresa, en l'àmbit de les assegurances i els fons de pensions.
2n El Banc d'Espanya, per a les entitats de crèdit.
3r La Comissió Nacional del Mercat de Valors, per a les entitats que presten serveis d'inversió i les societats gestores d'institucions d'inversió col·lectiva.

e) Respecte al sector de l'espai: el Ministeri de Defensa, a través de la Secretaria d'Estat de Defensa.
f) Respecte al sector de la indústria química: el Ministeri de l'Interior, a través de la Secretaria d'Estat de Seguretat.
g) Respecte al sector de les instal·lacions de recerca: el Ministeri de Ciència i Innovació, a través de la Secretaria General de Recerca.
h) Respecte al sector de la salut: el Ministeri de Sanitat, a través de la Secretaria d'Estat de Sanitat.

i) Respecte al sector de l'aigua: el Ministeri per a la Transició Ecològica i el Repte Demogràfic, a través de la Secretaria d'Estat de Medi Ambient.

j) Respecte al sector de l'alimentació:

1r El Ministeri d'Agricultura, Pesca i Alimentació, a través de la Secretaria General d'Agricultura i Alimentació.

2n El Ministeri de Sanitat, a través de la Secretaria d'Estat de Sanitat.

3r El Ministeri d'Indústria, Comerç i Turisme, a través de la Secretaria d'Estat de Comerç.

4t El Ministeri de Consum, a través de l'Agència Espanyola de Seguretat Alimentària i Nutrició (AESAN).

k) Respecte al sector de la indústria nuclear:

1r El Ministeri per a la Transició Ecològica i el Repte Demogràfic, a través de la Secretaria d'Estat d'Energia.

2n El Consell de Seguretat Nuclear.

Article 4. *Cooperació i coordinació dels CSIRT de referència.*

1. La cooperació entre els CSIRT de referència, i entre aquests i les autoritats competents, s'instrumenta a través de la Plataforma Nacional de Notificació i Seguiment de Ciberincidents que regula l'article 11.

2. A l'efecte de la cooperació que preveu l'article 11.1.a) 3r del Reial decret llei 12/2018, de 7 de setembre, s'entén que són operadors amb incidència en la defensa nacional els proveïdors de serveis essencials bàsics per al funcionament del Ministeri de Defensa o per a l'operativitat de les Forces Armades que estableixi, a proposta del Ministeri de Defensa, la Comissió Nacional per a la Protecció de les Infraestructures Crítiques.

La designació com a operador amb incidència en la defensa nacional s'ha de portar a terme de conformitat amb el que preveu el Reglament de protecció de les infraestructures crítiques, aprovat pel Reial decret 704/2011, de 20 de maig. Així mateix, els CSIRT de referència han de ser informats de la identitat dels operadors de serveis essencials de la seva comunitat que siguin designats operadors amb incidència en la defensa nacional.

El Ministeri de Defensa ha de comunicar oportunament a la Comissió Nacional per a la Protecció de les Infraestructures Crítiques les actualitzacions derivades de canvis d'operadors en la provisió d'aquests serveis, que han d'activar les notificacions corresponents d'alta o baixa com a operadors amb incidència en la defensa nacional tant als mateixos operadors com als seus CSIRT de referència.

Quan un operador amb incidència en la defensa nacional pateixi un incident ha d'analitzar si, pel seu abast, aquest pot tenir impacte en el funcionament del Ministeri de Defensa o en l'operativitat de les Forces Armades. En cas que sigui així, ho ha de posar immediatament en coneixement del seu CSIRT de referència, qui n'ha d'informar l'ESPDEF-CERT del Comandament Conjunt del Ciberespai a través dels canals establerts. En aquests casos, l'ESPDEF-CERT del Comandament Conjunt del Ciberespai ha de ser informat oportunament de l'evolució de la gestió de l'incident.

3. Els supòsits d'especial gravetat als quals es refereix l'article 11.2 paràgraf primer del Reial decret llei 12/2018, de 7 de setembre, en què el CCN-CERT exerceix la coordinació nacional de la resposta tècnica dels CSIRT, són tots aquells que, atenent la naturalesa de les notificacions inicial o successives de l'incident rebudes pel CSIRT de referència, tinguin un impacte o nivell de perillositat molt alta o crítica d'acord amb el que estableix l'annex, i exigeixin un nivell de coordinació tècnica amb els altres CSIRT de referència superior al necessari en situacions ordinàries.

El Consell Nacional de Ciberseguretat ha de ser informat immediatament i pot desactivar la coordinació que preveu aquest article, que únicament es pot produir quan hagi cessat la situació que preveu el paràgraf anterior i que no ha d'afectar el procés de notificació d'incidents que regulen els articles 11, 19.1 i 19.2 del Reial decret llei 12/2018, de 7 de setembre.

4. El CCN-CERT, en el cas que preveu l'apartat anterior, i l'Oficina de Coordinació de Ciberseguretat del Ministeri de l'Interior (OCC), en els supòsits que preveu l'article 11.2 paràgraf segon del Reial decret llei 12/2018, de 7 de setembre, han de requerir al CSIRT de referència, després de la primera notificació de l'incident, almenys la informació següent:

a) Confirmació que són correctes les dades assignades a l'incident, en particular que verifiquin, si existeix aquesta informació, la validesa de:

1r La classificació de l'incident.
2n La perillositat de l'incident.
3r L'impacte de l'incident.

b) Pla d'acció del CSIRT per abordar la resolució tècnica de l'incident, si escau.
c) Qualsevol informació que permeti determinar el possible impacte transfronterer de l'incident.

Sempre que sigui possible s'ha d'utilitzar la Plataforma Nacional de Notificació i Seguiment de Ciberincidents per a les comunicacions considerades en aquest apartat.

Article 5. *Punt de contacte únic.*

1. En la seva funció d'enllaç per garantir la cooperació transfronterera de les autoritats competents designades segons l'article 9 del Reial decret llei 12/2018, de 7 de setembre, amb les autoritats competents d'altres estats membres de la Unió Europea, així com amb el grup de cooperació que preveu l'article 11 de la Directiva (UE) 2016/1148 del Parlament Europeu i del Consell, de 6 de juliol de 2016, i la xarxa de CSIRT, el Consell de Seguretat Nacional, a través del Departament de Seguretat Nacional:

a) Ha de comunicar a la Comissió Europea la llista dels operadors de serveis essencials nacionals establerts per a cada sector i subsector als quals es refereix l'article 6 del Reial decret llei 12/2018, de 7 de setembre, i ha d'informar els punts de contacte únic d'altres estats sobre la intenció d'identificació d'un operador de serveis essencials d'un altre Estat membre que ofereixi serveis a Espanya.
b) Ha de transmetre als punts de contacte d'altres estats membres de la Unió Europea afectats la informació sobre incidents amb un impacte transfronterer que li transmetin les autoritats competents o CSIRT de referència, segons el que estableix l'article 25 del Reial decret llei 12/2018, de 7 de setembre.
c) Ha de remetre als CSIRT de referència i a les autoritats competents nacionals la informació corresponent sobre incidents que puguin tenir efectes pertorbadors en els serveis essencials que rebi dels punts de contacte dels estats membres corresponents, perquè adoptin les mesures oportunes en l'exercici de les seves funcions respectives.
d) Ha de dictar les instruccions pertinents a les autoritats competents perquè elaborin, anualment, l'informe al qual es refereix l'article 27.1 del Reial decret llei 12/2018, de 7 de setembre, sobre el tipus i el nombre 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, tenint en compte les indicacions del grup de cooperació respecte al format i el contingut de la informació que s'ha de transmetre.
e) Ha de sol·licitar a les autoritats competents l'informe anual al qual es refereix la lletra anterior i ha d'elaborar un informe anual resumit sobre les notificacions rebudes, que ha de remetre al grup de cooperació abans del 15 de febrer de cada any i, posteriorment, a les autoritats competents i als CSIRT de referència, perquè en tinguin coneixement.

2. Addicionalment a les funcions d'enllaç que preveu l'apartat anterior, i de conformitat amb el que preveu l'article 9.2 del Reial decret llei 12/2018, de 7 de setembre, el Consell de Seguretat Nacional, a través del seu comitè especialitzat en matèria de ciberseguretat, ha de garantir la coordinació de les actuacions de les autoritats competents mitjançant:

a) El foment de la coherència entre els requisits de seguretat específics que si s'escau adoptin les autoritats competents, de conformitat amb el que preveu l'article 6.6 d'aquest Reial decret.
b) El foment de la coherència entre les obligacions específiques que si s'escau estableixin les autoritats competents, de conformitat amb el que preveu l'article 8.3 d'aquest Reial decret.
c) L'impuls de la coordinació de les disposicions i actuacions de les autoritats competents i les actuacions dels CSIRT de referència amb les disposicions i actuacions en matèria de seguretat de la informació de les autoritats de protecció de dades i de seguretat pública.

3. De la mateixa manera, el Consell de Seguretat Nacional ha d'exercir les funcions de coordinació que preveu l'apartat 2 anterior en els supòsits que estableix l'article 18 del Reial decret llei 12/2018, de 7 de setembre.

CAPÍTOL III

Requisits de seguretat

Article 6. *Mesures per al compliment de les obligacions de seguretat.*

1. Els operadors de serveis essencials i els proveïdors de serveis digitals han d'adoptar les mesures tècniques i d'organització adequades i proporcionades per gestionar els riscos que afectin la seguretat de les xarxes i els sistemes d'informació utilitzats per prestar els seus serveis, tant si es tracta de xarxes i sistemes propis com de proveïdors externs.
2. En el cas dels operadors de serveis essencials, han d'aprovar unes polítiques de seguretat de les xarxes i els sistemes d'informació, atenent els principis de seguretat integral, gestió de riscos, prevenció, resposta i recuperació, línies de defensa, reavaluació periòdica i segregació de tasques.
Aquestes polítiques han de considerar, com a mínim, els aspectes següents:

a) Anàlisi i gestió de riscos.
b) Gestió de riscos de tercers o proveïdors.
c) Catàleg de mesures de seguretat, organitzatives, tecnològiques i físiques.
d) Gestió del personal i professionalitat.
e) Adquisició de productes o serveis de seguretat.
f) Detecció i gestió d'incidents.
g) Plans de recuperació i assegurament de la continuïtat de les operacions.
h) Millora contínua.
i) Interconnexió de sistemes.
j) Registre de l'activitat dels usuaris.

3. Les mesures de seguretat que adoptin els operadors de serveis essencials han de tenir en compte, en particular, la dependència de les xarxes i els sistemes d'informació i la continuïtat de serveis o subministraments contractats per l'operador, així com les interaccions que presentin amb xarxes i sistemes d'informació de tercers.
4. La relació de mesures adoptades s'ha de formalitzar en un document denominat Declaració d'aplicabilitat de mesures de seguretat, que ha de subscriure el responsable de seguretat de la informació designat de conformitat amb el que preveu l'article següent i que s'ha d'incloure en la política de seguretat que aprovi la Direcció de l'organització. Aquest document, que s'ha de remetre a l'autoritat competent respectiva en el termini de sis

mesos des de la designació de l'operador com a operador de serveis essencials, s'ha de revisar, almenys, cada tres anys. Tant la Declaració d'aplicabilitat de mesures de seguretat inicial com les seves revisions successives han de ser supervisades per l'autoritat competent respectiva, segons el que preveu l'article 14 d'aquest Reial decret.

5. Les mesures a què es refereixen els apartats anteriors han d'agafar com a referència les que recull l'annex II del Reial decret 3/2010, de 8 de gener, pel qual es regula l'Esquema Nacional de Seguretat en l'àmbit de l'Administració electrònica, en la mesura que siguin aplicables, i s'han de basar, quan sigui possible, en altres esquemes nacionals de seguretat existents.

Sense perjudici d'això, es poden tenir en compte altres estàndards reconeguts internacionalment.

6. Les mesures adoptades es poden complementar amb d'altres, atenent necessitats específiques, entre les quals la possibilitat d'exigir un document d'aplicabilitat dels sistemes afectats per aquesta normativa, en aquells operadors amb entorns de sistemes d'informació especialment complexos. En particular, s'han de complementar amb les que, si s'escau, estableixin amb caràcter específic les autoritats competents, de conformitat amb el que preveuen l'article 16.4 i l'article 32.2 del Reial decret llei 12/2018, de 7 de setembre.

7. En l'elaboració de les polítiques de seguretat de les xarxes i els sistemes d'informació s'han de tenir en compte els riscos que es deriven del tractament de les dades personals, d'acord amb l'article 24 del 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 (d'ara endavant, Reglament general de protecció de dades). En cas que l'anàlisi de gestió de riscos d'acord amb el Reglament general de protecció de dades exigeixi implantar mesures addicionals respecte de les que preveu el Reial decret 3/2010, de 8 de gener, s'han d'adoptar les mesures d'acord amb l'article 24.1 del Reglament general de protecció de dades.

Article 7. *Responsable de la seguretat de la informació.*

1. Els operadors de serveis essencials han de designar una persona, unitat o òrgan col·legiat, responsable de la seguretat de la informació que ha d'exercir les funcions de punt de contacte i coordinació tècnica amb l'autoritat competent i CSIRT de referència que li correspongui de conformitat amb el que preveu l'apartat tercer. En el supòsit que el responsable de seguretat de la informació sigui una unitat o un òrgan col·legiat, s'ha de designar una persona física representant, així com un substitut d'aquesta que n'assumeixi les funcions en casos d'absència, vacant o malaltia. El termini per portar a terme aquesta designació és de tres mesos des de la seva designació com a operador de serveis essencials.

2. Els operadors de serveis essencials han de comunicar a l'autoritat competent respectiva la designació del responsable de la seguretat de la informació dins del termini que estableix l'apartat anterior, així com els nomenaments i cessaments que afectin la designació del responsable de la seguretat de la informació en el termini d'un mes des que aquells es produeixin.

3. El responsable de la seguretat de la informació ha d'actuar com a punt de contacte amb l'autoritat competent en matèria de supervisió dels requisits de seguretat de les xarxes i els sistemes d'informació, i com a punt de contacte especialitzat per a la coordinació de la gestió dels incidents amb el CSIRT de referència. S'han d'exercir sota la seva responsabilitat, entre d'altres, les funcions següents:

a) Elaborar i proposar perquè l'organització les aprovi, de conformitat amb el que estableix l'article 6.2 d'aquest Reial decret, les polítiques de seguretat, que han d'incloure les mesures tècniques i organitzatives, adequades i proporcionades, per gestionar els riscos que es plantegin per a la seguretat de les xarxes i els sistemes d'informació utilitzats i per prevenir i reduir al mínim els efectes dels ciberincidents que afectin l'organització i els serveis, de conformitat amb el que disposa l'article 6.

b) Supervisar i desenvolupar l'aplicació de les polítiques de seguretat, normatives i procediments derivats de l'organització, supervisar-ne l'efectivitat i portar a terme controls periòdics de seguretat.

c) Elaborar el document de Declaració d'aplicabilitat de mesures de seguretat considerat a l'article 6.3 paràgraf segon d'aquest Reial decret.

d) Actuar com a capacitador de bones pràctiques en seguretat de les xarxes i els sistemes d'informació, tant en aspectes físics com lògics.

e) Remetre a l'autoritat competent, a través del CSIRT de referència i sense dilació indeguda, les notificacions d'incidents que tinguin efectes pertorbadors en la prestació dels serveis als quals es refereix l'article 19.1 del Reial decret llei 12/2018, de 7 de setembre.

f) Rebre, interpretar i supervisar l'aplicació de les instruccions i guies emanades de l'autoritat competent, tant per a l'operativa habitual com per a l'esmena de les deficiències observades.

g) Recopilar, preparar i subministrar informació o documentació a l'autoritat competent o el CSIRT de referència, quan ho sol·licitin o per iniciativa pròpia.

El responsable de la seguretat de la informació, per exercir aquestes funcions, es pot recolzar en serveis prestats per tercers.

4. Els operadors de serveis essencials han de garantir que el responsable de la seguretat de la informació compleixi els requisits següents:

a) Disposar de personal amb coneixements especialitzats i experiència en matèria de ciberseguretat, des dels punts de vista organitzatiu, tècnic i jurídic, adequats a l'exercici de les funcions que indica l'apartat anterior.

b) Disposar dels recursos necessaris per a l'exercici de les funcions esmentades.

c) Tenir una posició en l'organització que faciliti l'exercici de les seves funcions, i participar de manera adequada i en temps oportú en totes les qüestions relatives a la seguretat i mantenir una comunicació real i efectiva amb l'alta direcció.

d) Mantenir la independència deguda respecte dels responsables de les xarxes i els sistemes d'informació.

5. Sempre que concorrin els requisits de coneixement, experiència, independència i, si s'escau, titulació, les funcions i responsabilitats encomanades al responsable de la seguretat de la informació es poden compatibilitzar amb les assenyalades per al responsable de Seguretat i Enllaç i el responsable de Seguretat de l'Esquema Nacional de Seguretat, de conformitat amb el que disposa la normativa aplicable a aquestes figures.

CAPÍTOL IV

Gestió d'incidents de seguretat

Article 8. *Gestió d'incidents de seguretat.*

1. Els operadors de serveis essencials i els proveïdors de serveis digitals han de gestionar i resoldre els incidents de seguretat que afectin les xarxes i els sistemes d'informació utilitzats per prestar els seus serveis. En el cas de xarxes i sistemes que no siguin propis, els operadors han de prendre les mesures necessàries per garantir que aquestes accions les portin a terme els proveïdors externs.

Aquesta obligació engloba tant els incidents detectats pel mateix operador o proveïdor com els que els assenyalin el CSIRT de referència o l'autoritat competent, quan tinguin coneixement d'alguna circumstància que faci sospitar de l'existència d'un incident.

2. Sense perjudici del que preveu l'article 28.1 del Reial decret llei 12/2018, de 7 de setembre, els operadors de serveis essencials i els proveïdors de serveis digitals poden sol·licitar voluntàriament ajuda especialitzada del CSIRT de referència per a la gestió dels incidents, i en aquests casos han d'atendre les indicacions que rebin d'aquest per resoldre l'incident, mitigar-ne els efectes i reposar els sistemes afectats.

3. En la resolució dels incidents, els operadors de serveis essencials han d'aplicar els aspectes pertinents de la política de gestió de la seguretat de les xarxes i els sistemes d'informació a la qual es refereix l'article 6, així com les obligacions específiques que si s'escau estableixin les autoritats competents.

Article 9. *Obligacions de notificació d'incidents dels operadors de serveis essencials.*

1. Els operadors de serveis essencials han de notificar a l'autoritat competent respectiva, a través del CSIRT de referència, els incidents que puguin tenir efectes pertorbadors significatius en els serveis esmentats, i a aquest efecte es consideren els incidents amb un nivell d'impacte crític, molt alt o alt, segons el detall que especifica l'apartat 4 de la Instrucció nacional de notificació i gestió de ciberincidents, que conté l'annex d'aquest Reial decret.

Així mateix, han de notificar els successos o incidències que, pel seu nivell de perillositat, puguin afectar les xarxes i els sistemes d'informació utilitzats per prestar els serveis essencials, encara que no hagin tingut encara un efecte advers real sobre aquells. A aquest efecte, s'han de considerar els incidents amb un nivell de perillositat crític, molt alt o alt, segons el detall que especifica l'apartat 3 de la Instrucció esmentada.

2. Sense perjudici d'això, les autoritats competents poden establir, de conformitat amb l'article 19.5 del Reial decret llei 12/2018, de 7 de setembre, obligacions específiques de notificació que prevegin nivells diferents dels que preveu la Instrucció nacional de notificació i gestió de ciberincidents, així com factors i llindars sectorials específics, aplicables als operadors sotmesos a la seva supervisió.

3. La notificació d'un ciberincident de conformitat amb aquest Reial decret no exclou ni substitueix la notificació que d'aquests fets s'hagi d'efectuar a altres organismes de conformitat amb la seva normativa específica.

En particular, les obligacions de notificació que preveuen els apartats anteriors són independents de les que s'hagin d'efectuar a l'Agència Espanyola de Protecció de Dades de conformitat amb el que preveu l'article 33 del Reglament general de protecció de dades, sense perjudici de la cooperació entre autoritats prevista a l'article 29 del Reial decret llei 12/2018 i la possibilitat que l'agència esmentada accedeixi a la plataforma comuna de notificació d'incidents que preveu la seva disposició addicional tercera.

A aquests efectes, les notificacions que preveuen els apartats 1 i 2 d'aquest article han d'incloure la informació que, per als casos de violació de la seguretat de les dades personals, continguin els formularis aprovats per l'Agència Espanyola de Protecció de Dades.

Article 10. *Procediments de notificació d'incidents.*

1. Els CSIRT de referència han de garantir un intercanvi fluid d'informació amb les autoritats competents que corresponguin, i assegurar el seguiment adequat durant la gestió dels incidents, així com l'accés a la informació utilitzada en les diferents fases que componen la gestió d'incidents.

2. Els operadors de serveis essencials han d'efectuar les notificacions a través del responsable de la seguretat de la informació designat.

En cas que un operador de serveis essencials reuneixi els criteris que preveu l'article 6.2 del Reial decret llei 12/2018, de 7 de setembre, sobre seguretat de les xarxes i els sistemes d'informació, el responsable de la seguretat de la informació s'ha de coordinar a aquests efectes amb el responsable de Seguretat i Enllaç que preveu l'article 16 de la Llei 8/2011, de 28 d'abril, per la qual s'estableixen mesures per a la protecció de les infraestructures crítiques.

3. Els operadors de serveis essencials han d'efectuar una primera notificació tan aviat com disposin d'informació per determinar que es donen les circumstàncies per a la notificació, atenent els factors i llindars corresponents.

S'han d'efectuar les notificacions intermèdies que siguin necessàries per actualitzar o completar la informació incorporada a la notificació inicial, i informar sobre l'evolució de

l'incident, mentre aquest no estigui resolt, i s'ha d'efectuar una notificació final de l'incident després que es resolgui, i informar del detall de l'evolució del succés, la valoració de la probabilitat de la seva repetició i les mesures correctores que eventualment tingui previst adoptar l'operador. Els llindars temporals exigits per a aquestes notificacions són els que recull l'annex d'aquest Reial decret.

4. Les notificacions han d'incloure, quan estigui disponible, la informació que permeti determinar qualsevol efecte transfronterer de l'incident.

5. El que estableixen els apartats anteriors és aplicable als proveïdors de serveis digitals mentre no es reguli d'una manera diferent en els actes d'execució que preveu l'article 16.9 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.

6. El CSIRT de referència, en col·laboració amb l'autoritat competent, ha de valorar amb promptitud aquesta informació amb vista a determinar si l'incident pot tenir efectes pertorbadors significatius per als serveis essencials prestats en altres estats membres de la Unió Europea, i informar en aquest cas a través del punt de contacte únic als estats membres afectats.

Així mateix, l'autoritat competent ha de valorar, conjuntament amb el CSIRT de referència corresponent, la informació sobre incidents amb possibles impactes transfronterers que rebi d'altres estats membres, i ha d'indicar i transmetre la informació rellevant als operadors de serveis essencials que es puguin veure afectats.

Article 11. *Plataforma Nacional de Notificació i Seguiment de Ciberincidents.*

1. El CCN-CERT, en col·laboració amb l'INCIBE-CERT i l'ESPDEF-CERT del Comandament Conjunt del Ciberespai, ha de posar a disposició de tots els actors involucrats la Plataforma Nacional de Notificació i Seguiment de Ciberincidents a què es refereix l'article 19.4 del Reial decret llei 12/2018, de 7 de setembre.

2. La plataforma ha de permetre l'intercanvi d'informació i el seguiment d'incidents entre els operadors de serveis essencials o proveïdors de serveis digitals, les autoritats competents i els CSIRT de referència de manera segura i de confiança, sense perjudici dels requisits específics que apliquin en matèria de protecció de dades de caràcter personal.

3. Aquesta plataforma ha de garantir així mateix la disponibilitat, autenticitat, integritat i confidencialitat de la informació, i també es pot utilitzar per complir l'exigència de notificació derivada de regulacions sectorials, d'acord amb l'article 19.5 del Reial decret llei 12/2018, de 7 de setembre.

4. La plataforma ha de disposar així mateix de diversos canals de comunicació perquè els puguin utilitzar les autoritats competents i els CSIRT de referència. La plataforma ha de garantir l'accés de les autoritats competents a tota la informació relativa a la notificació i estat de situació dels incidents del seu àmbit de competència que els permeti efectuar en tot moment el seguiment i control necessari del seu estat de situació. Igualment, les autoritats competents han de tenir accés a través de la plataforma a dades estadístiques, en particular a les necessàries per generar els informes als quals fa menció l'article 5.

5. Així mateix, la plataforma ha d'implementar el procediment de notificació i gestió d'incidents, que ha d'estar disponible durant totes les hores del dia i cada dia de l'any, i ha de disposar com a mínim de les capacitats següents:

a) Capacitat de gestió de ciberincidents, amb incorporació de taxonomia, criticitat i notificacions a tercers, segons el que estableix l'annex.

b) Capacitat d'intercanvi d'informació sobre ciberamenaces.

c) Capacitat d'anàlisi de mostres.

d) Capacitat de registre i notificació de vulnerabilitats.

e) Capacitat de comunicacions segures entre els actors involucrats en diferents formats i plataformes.

f) Capacitat d'intercanvi massiu de dades.
g) Generació d'estadístiques i informes agregats.

Article 12. *Informació sobre incidents.*

1. Quan les circumstàncies ho permetin, els CSIRT de referència han de proporcionar als operadors de serveis essencials i als proveïdors de serveis digitals notificadors la informació pertinent respecte al seguiment de la notificació d'un incident, en particular aquella que pugui facilitar la gestió eficaç de l'incident.
2. Així mateix, les autoritats competents i els CSIRT de referència han de proporcionar als operadors de serveis essencials i als proveïdors de serveis digitals que es puguin veure afectats pels incidents esmentats la informació que els pugui ser rellevant per prevenir i si s'escau resoldre l'incident.
3. Quan proporcionin la informació a la qual es refereixen els apartats anteriors, les autoritats competents i els CSIRT de referència han de vetllar pels interessos comercials dels operadors de serveis essencials i proveïdors de serveis digitals, i preservar la confidencialitat de la informació que obtenen d'aquests, de conformitat amb el que estableix l'article 15 del Reial decret llei 12/2018, de 7 de setembre.

Article 13. *Actuacions davant incidents amb caràcter presumptament delictiu.*

En compliment del que disposa l'article 262 de la Llei d'enjudiciament criminal, l'OCC ha de comunicar tan aviat com sigui possible al Ministeri Fiscal i, si s'escau, a les unitats orgàniques de policia judicial competents, aquells incidents de seguretat que li siguin notificats i que revesteixin caràcter presumptament delictiu, i traslladar al mateix temps la informació relacionada de què disposi. Amb aquesta finalitat pot requerir dels operadors afectats o dels CSIRT de referència tota la informació relacionada amb l'incident que consideri necessària.

Article 14. *Consulta amb altres autoritats.*

1. Les consultes amb altres autoritats amb competència en matèria de seguretat pública i seguretat ciutadana, que preveu l'article 14.1 del Reial decret llei 12/2018, de 7 de setembre, s'han d'efectuar a través de l'OCC.
2. Les consultes relatives a la resta de matèries que preveu l'article 14 esmentat s'han d'efectuar directament a les autoritats competents corresponents.

CAPÍTOL V

Supervisió

Article 15. *Supervisió del compliment d'obligacions de seguretat i de notificació d'incidents.*

1. Les autoritats competents han de supervisar en el seu àmbit d'actuació el compliment de les obligacions de seguretat i de notificació d'incidents que siguin aplicables als operadors de serveis essencials i als proveïdors de serveis digitals de conformitat amb el Reial decret llei 12/2018, de 7 de setembre, i aquest Reial decret.
2. Els operadors de serveis essencials i els proveïdors de serveis digitals han de col·laborar amb l'autoritat competent en la supervisió esmentada, i facilitar les actuacions d'inspecció, proporcionar tota la informació que a aquest efecte se'ls requereixi i aplicar les instruccions dictades, si s'escau, per esmenar les deficiències observades.
3. El compliment de les obligacions de seguretat en les xarxes i els sistemes d'informació es pot acreditar mitjançant la certificació en un esquema de seguretat que, amb la consulta prèvia al CSIRT de referència, sigui reconegut per l'autoritat competent.

4. Les autoritats competents poden dur a terme les actuacions inspectores que siguin necessàries per a l'exercici de la seva funció de control. En particular, les actuacions d'inspecció de les autoritats competents, que poden rebre suport per part dels CSIRT de referència, tenen per objecte:

a) Controlar el compliment de les normes i instruccions tècniques que, si s'escau, siguin aplicables als operadors subjectes a la seva supervisió.

b) Verificar el compliment de les funcions del responsable de seguretat de la informació designat pels operadors de serveis essencials, segons el que preveu l'article 7.3 d'aquest Reial decret.

c) Fer les comprovacions, inspeccions, proves i revisions necessàries per verificar el compliment de les mesures de seguretat que preveu l'article 6, en particular la política de seguretat dels operadors de serveis essencials i la Declaració d'aplicabilitat de mesures de seguretat.

De conformitat amb el que preveu l'article 32.1 del Reial decret llei 12/2018, de 7 de setembre, quan el volum o la complexitat de les actuacions d'inspecció que s'hagin de dur a terme ho aconselli, les autoritats competents poden requerir a l'operador de serveis essencials que remeti un informe d'auditoria, elaborat per una entitat externa, solvent i independent, sobre la seguretat de les seves xarxes i sistemes d'informació.

5. Els CSIRT de referència han de col·laborar amb les autoritats competents, quan aquestes els ho requereixin, en l'exercici de les funcions a les quals es refereix l'apartat anterior. En particular, han de facilitar assessorament tècnic sobre la idoneïtat de les mesures de seguretat adoptades pels operadors de serveis essencials i els proveïdors de serveis digitals en virtut de l'article 6 d'aquest Reial decret.

Així mateix, quan es tracti d'operadors amb incidència en la defensa nacional a què es refereix l'article 4.2 d'aquest Reial decret, l'ESPDEF-CERT del Comandament Conjunt del Ciberespai pot col·laborar en la supervisió amb l'autoritat competent.

6. En el cas dels proveïdors de serveis digitals la supervisió s'ha de portar a terme de manera coordinada amb les autoritats competents corresponents dels estats membres de la Unió Europea on els proveïdors esmentats prestin serveis o tinguin el seu establiment principal a la Unió.

Disposició addicional primera. *Designació del responsable de la seguretat de la informació per part dels operadors de serveis essencials designats.*

Els operadors de serveis essencials designats de conformitat amb el que preveu la disposició addicional primera del Reial decret llei 12/2018, de 7 de setembre, han de comunicar a l'autoritat competent respectiva la identitat del responsable de la seguretat de la informació en el termini de tres mesos des de l'entrada en vigor d'aquest Reial decret.

Disposició addicional segona. *Orientacions per a la gestió d'incidents i compliment de les obligacions de notificació.*

El Consell de Seguretat Nacional, a proposta del seu comitè especialitzat en matèria de ciberseguretat, i articulades les seves funcions com a punt de contacte únic a través del Departament de Seguretat Nacional, pot aprovar orientacions en relació amb la Instrucció nacional de notificació i gestió d'incidents que recull l'annex, així com per a l'actualització de la Guia nacional de notificació i gestió de ciberincidents, que incloguin directrius i recomanacions per al compliment de les obligacions de notificació que preveu aquest Reial decret, així com el Reial decret llei 12/2018, de 7 de setembre, per tal de millorar la coordinació i optimitzar els recursos dedicats a la gestió dels incidents que afectin la seguretat de les xarxes i els sistemes d'informació.

Disposició addicional tercera. *Règim específic del Banc d'Espanya.*

Les disposicions d'aquest Reial decret s'entenen sense perjudici de les competències i funcions atribuïdes al Banc d'Espanya, al Banc Central Europeu i al Sistema Europeu de Bancs Centrals, de conformitat amb el Tractat de funcionament de la Unió Europea, els estatuts del Sistema Europeu de Bancs Centrals i del Banc Central Europeu, el Reglament (UE) núm. 1024/2013 del Consell, de 15 d'octubre de 2013, que encomana al Banc Central Europeu tasques específiques respecte de polítiques relacionades amb la supervisió prudencial de les entitats de crèdit, i la Llei 13/1994, d'1 de juny, d'autonomia del Banc d'Espanya.

En allò que no preveu la seva normativa específica, i quan sigui compatible amb la seva naturalesa, funcions i independència, és aplicable al Banc d'Espanya el que preveu aquest Reial decret.

Disposició addicional quarta. *Supòsit de dependència de proveïdors externs.*

En referència a l'article 19.3 del Reial decret llei 12/2018, de 7 de setembre, quan els operadors de serveis essencials o proveïdors de serveis digitals depenguin de proveïdors externs als quals els és aplicable la disposició addicional novena de la Llei 34/2002, d'11 de juliol, de serveis de la societat de la informació i de comerç electrònic, l'Equip de Resposta davant Emergències Informàtiques (CERT) competent del proveïdor extern s'ha de correspondre amb:

a) El CCN-CERT, del Centre Criptològic Nacional, quan el proveïdor estigui inclòs en l'àmbit subjectiu d'aplicació de la Llei 40/2015, d'1 d'octubre.

b) L'INCIBE-CERT, de l'Institut Nacional de Ciberseguretat d'Espanya, en la resta dels casos.

Disposició addicional cinquena. *Tractaments de dades de caràcter personal.*

Els tractaments de dades de caràcter personal de les persones físiques s'han d'efectuar amb una subjecció estricta al que disposen el Reglament (UE) 2016/679 del Parlament Europeu i el Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les seves dades personals i a la lliure circulació d'aquestes dades; la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, i, si s'escau, la normativa sobre protecció de dades personals especial o específica que sigui aplicable.

Disposició addicional sisena. *Informació sobre incidents en el sistema financer.*

Els CSIRT de referència han d'informar el titular de la Secretaria d'Estat d'Economia i Suport a l'Empresa, a través de la Secretaria General del Tresor i Finançament Internacional, dels incidents que puguin tenir efectes pertorbadors significatius en els serveis essencials del sistema financer. A aquests efectes, s'entén que tenen efectes pertorbadors significatius quan el seu llindar o nivell d'impacte sigui crític, molt alt o alt, segons el que assenyala l'annex d'aquest Reial decret.

Disposició transitòria única. *Exercici transitori de funcions en el sector energètic.*

La Secretaria d'Estat de Seguretat del Ministeri de l'Interior, a través de l'Oficina de Coordinació de Ciberseguretat (OCC), ha d'exercir temporalment les funcions atribuïdes per aquest Reial decret al departament ministerial amb competències en matèria d'energia, fins que aquest disposi dels recursos humans necessaris amb la formació adequada per exercir aquestes competències de forma efectiva segons el que preveu l'article 3 i, en tot cas, en un termini màxim de 12 mesos.

Disposició final primera. *Títol competencial.*

Aquest Reial decret es dicta a l'empara del que preveu l'article 149.1.21a i 29a de la Constitució, que atribueix a l'Estat la competència exclusiva en matèria de règim general de telecomunicacions i seguretat pública, respectivament.

Disposició final segona. *Habilitació per al desplegament normatiu i aplicació.*

Es faculta els titulars dels ministeris d'Afers Econòmics i Transformació Digital, Interior i Defensa, així com els titulars dels ministeris i organismes relacionats a l'article 3, per dictar conjuntament o separadament, segons les matèries de què es tracti, i en l'àmbit de les seves competències respectives, les disposicions que exigeixin el desplegament i l'aplicació d'aquest Reial decret.

Disposició final tercera. *Entrada en vigor.*

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

Madrid, 26 de gener de 2021.

FELIPE R.

La vicepresidenta primera del Govern i ministra de la Presidència,
Relacions amb les Corts i Memòria Democràtica,
CARMEN CALVO POYATO

ANNEX

Instrucció nacional de notificació i gestió de ciberincidents

1. *Obligatorietat de notificació*

Els incidents s'han d'associar a un dels nivells de perillositat i impacte que estableix aquesta Instrucció, tenint en compte l'obligatorietat de notificació de tots aquells que es categoritzin amb un nivell CRÍTIC, MOLT ALT o ALT per a tots els subjectes obligats als quals els sigui aplicable aquesta «Instrucció nacional de notificació i gestió de ciberincidents». En aquest cas, els subjectes obligats han de comunicar, dins el termini establert i en la forma pertinent, els incidents que registrin en les seves xarxes i sistemes d'informació i que estiguin obligats a notificar per superar els llindars d'impacte o perillositat que estableix aquesta Instrucció.

Per notificar els incidents de ciberseguretat s'ha d'utilitzar com a criteri de referència el nivell de perillositat que s'assigni a un incident, sense perjudici que al llarg del desenvolupament, mitigació o resolució d'aquest es categoritzi amb un determinat nivell d'impacte que faci aconsellable la comunicació de l'incident a l'autoritat competent o CSIRT de referència.

En tot cas, quan un determinat succés es pugui associar a més d'un tipus d'incident a causa de les seves característiques potencials, aquest s'ha d'associar a aquell que tingui un nivell de perillositat superior d'acord amb els criteris que exposa aquesta Instrucció.

2. *Classificació/taxonomia dels ciberincidents*

La següent classificació/taxonomia dels ciberincidents està alineada amb la taxonomia aprovada per l'Agència de la Unió Europea per a la Ciberseguretat (ENISA).

Aquesta classificació/taxonomia dels ciberincidents s'ha d'utilitzar per assignar una classificació específica a un incident registrat en les xarxes i els sistemes d'informació quan s'efectuï la comunicació a l'autoritat competent o CSIRT de referència.

Taula 1. Classificació/taxonomia dels ciberincidents

Classificació	Tipus d'incident	Descripció i exemples pràctics
Contingut abusiu.	Correu brossa (*spam*).	Correu electrònic massiu no sol·licitat. El receptor del contingut no ha atorgat autorització vàlida per rebre un missatge col·lectiu.
	Delictes d'odi, contra la llibertat o l'honor.	Contingut difamatori o discriminatori. Ex.: ciberassetjament, racisme, amenaces a una persona o dirigides contra col·lectius.
	Pornografia infantil, contingut sexual o violent inadequat.	Material que representi de manera visual contingut relacionat amb pornografia infantil, apologia de la violència, etc.
Contingut perjudicial.	Sistema infectat.	Sistema infectat amb programari maliciós (*malware*). Ex.: sistema, ordinador o telèfon mòbil infectat amb un paquet d'intrusió (*rootkit*).
	Servidor C&C (comandament i control).	Connexió amb un servidor de comandament i control (C&C) mitjançant programari maliciós o sistemes infectats.
	Distribució de programari maliciós.	Recurs utilitzat per distribuir programari maliciós. Ex.: recurs d'una organització emprat per distribuir programari maliciós.
	Configuració de programari maliciós.	Recurs que allotgi fitxers de configuració de programari maliciós Ex.: atac de *webinjects* per a troià.

Classificació	Tipus d'incident	Descripció i exemples pràctics
Obtenció d'informació.	Escaneig de xarxes (*scanning*).	Enviament de peticions a un sistema per descobrir possibles debilitats. S'inclouen també processos de comprovació o testatge per recopilar informació d'allotjaments, serveis i comptes. Ex.: peticions DNS, ICMP, SMTP, escaneig de ports.
	Anàlisi de paquets (*sniffing*).	Observació i gravació del trànsit de xarxes.
	Enginyeria social.	Recopilació d'informació personal sense l'ús de la tecnologia. Ex.: mentides, trucs, suborns, amenaces.
Intent d'intrusió.	Explotació de vulnerabilitats conegudes.	Intent de compromís d'un sistema o d'interrupció d'un servei mitjançant l'explotació de vulnerabilitats amb un identificador estandarditzat (vegeu CVE). Ex.: desbordament de memòria intermèdia (*buffer*), portes del darrere, injecció indirecta de scripts (*cross site scripting*) (XSS).
	Intent d'accés amb vulneració de credencials.	Múltiples intents de vulneració de credencials. Ex.: intents de ruptura de contrasenyes, atac per força bruta.
	Atac desconegut.	Atac utilitzant un explotador (*exploit*) desconegut.
Intrusió.	Compromís de compte amb privilegis.	Compromís d'un sistema en què l'atacant ha adquirit privilegis.
	Compromís de compte sense privilegis.	Compromís d'un sistema utilitzant comptes sense privilegis.
	Compromís d'aplicacions.	Compromís d'una aplicació mitjançant l'explotació de vulnerabilitats de programari. Ex.: injecció SQL.
	Robatori.	Intrusió física. Ex.: accés no autoritzat a centre de processament de dades.
Disponibilitat.	DoS (denegació de servei).	Atac de denegació de servei. Ex.: enviament de peticions a una aplicació web que provoca la interrupció o alentiment en la prestació del servei.
	DDoS (denegació de servei distribuït).	Atac de denegació de servei distribuït. Ex.: inundació de paquets SYN, atacs de reflexió i amplificació utilitzant serveis basats en UDP.
	Mala configuració.	Configuració incorrecta del programari que provoca problemes de disponibilitat en el servei. Ex.: servidor DNS amb el KSK de la zona arrel de DNSSEC obsolet.
	Sabotatge.	Sabotatge físic. Ex.: talls de cablejats d'equips o incendis provocats.
	Interrupcions.	Interrupcions per causes alienes. Ex.: desastre natural.
Compromís de la informació.	Accés no autoritzat a informació.	Accés no autoritzat a informació. Ex.: robatori de credencials d'accés mitjançant intercepció de trànsit o mitjançant l'accés a documents físics.
	Modificació no autoritzada d'informació.	Modificació no autoritzada d'informació. Ex.: modificació per part d'un atacant que utilitza credencials sostretes d'un sistema o aplicació o encriptació de dades mitjançant programari de segrest (*ransomware*).
	Pèrdua de dades.	Pèrdua d'informació Ex.: pèrdua per fallada de disc dur o robatori físic.
Frau.	Ús no autoritzat de recursos.	Ús de recursos per a propòsits inadequats, incloses accions amb ànim de lucre. Ex.: ús de correu electrònic per participar en estafes piramidals.
	Drets d'autor.	Oferiment o instal·lació de programari que no té llicència o un altre material protegit per drets d'autor. Ex.: programari piratejat (*warez*).
	Suplantació.	Tipus d'atac en què una entitat en suplanta una altra per obtenir beneficis il·legítims.
	Pesca (*phishing*).	Suplantació d'una altra entitat amb la finalitat de convèncer l'usuari perquè reveli les seves credencials privades.

Classificació	Tipus d'incident	Descripció i exemples pràctics
Vulnerabilitat.	Criptografia feble.	Serveis accessibles públicament que puguin presentar criptografia feble. Ex.: servidors web susceptibles d'atacs POODLE/FREAK.
	Amplificador DDoS.	Serveis accessibles públicament que es puguin utilitzar per a la reflexió o amplificació d'atacs DDoS. Ex.: DNS *open-resolvers* o servidors NTP amb monitoratge *monlist*.
	Serveis amb accés potencial no desitjat.	Ex.: Telnet, RDP o VNC.
	Revelació d'informació.	Accés públic a serveis en els quals potencialment es pugui revelar informació sensible. Ex.: SNMP o Redis.
	Sistema vulnerable.	Sistema vulnerable. Ex.: mala configuració del servidor intermediari (*proxy*) en client (WPAD), versions desfasades de sistema.
Altres.	Altres.	Tot aquell incident que no tingui cabuda en cap de les categories anteriors.
	APT.	Atacs dirigits contra organitzacions concretes, sustentats en mecanismes molt sofisticats d'ocultació, anonimat i persistència. Aquesta amenaça habitualment utilitza tècniques d'enginyeria social per aconseguir els seus objectius juntament amb l'ús de procediments d'atac coneguts o genuïns.

3. *Nivell de perillositat del ciberincident*

L'indicador de perillositat determina l'amenaça potencial que suposaria la materialització d'un incident en els sistemes d'informació o comunicació de l'ens afectat, així com per als serveis prestats o la continuïtat de negoci en cas que n'hi hagi. Aquest indicador es fonamenta en les característiques intrínseques a la tipologia d'amenaça i el seu comportament.

Els incidents s'han d'associar a un dels nivells de perillositat següents: CRÍTIC, MOLT ALT, ALT, MITJÀ, BAIX.

Nivell crític:

– APT.

Nivell molt alt:

– Distribució de programari maliciós.
– Configuració de programari maliciós.
– Robatori.
– Sabotatge.
– Interrupcions.

Nivell alt:

– Pornografia infantil, contingut sexual o violent inadequat.
– Sistema infectat.
– Servidor C&C (comandament i control).
– Compromís d'aplicacions.
– Compromís de comptes amb privilegis.
– Atac desconegut.
– DoS (denegació de servei).
– DDoS (denegació de servei distribuït).
– Accés no autoritzat a informació.
– Modificació no autoritzada d'informació.
– Pèrdua de dades.
– Pesca.

Nivell mitjà:

– Discurs d'odi.
– Enginyeria social.
– Explotació de vulnerabilitats conegudes.
– Intent d'accés amb vulneració de credencials.
– Compromís de comptes sense privilegis.
– Desconfiguració.
– Ús no autoritzat de recursos.
– Drets d'autor.
– Suplantació.
– Criptografia feble.
– Amplificador DDoS.
– Serveis amb accés potencial no desitjat.
– Revelació d'informació.
– Sistema vulnerable.

Nivell baix:

– Correu brossa.
– Escaneig de xarxes (*scanning*).
– Anàlisi de paquets (*sniffing*).
– Altres.

4. *Nivell d'impacte del ciberincident*

L'indicador d'impacte d'un ciberincident es determina avaluant les conseqüències que aquest ciberincident ha tingut en les funcions i les activitats de l'organització afectada, en els seus actius o en els individus afectats. D'acord amb això, es tenen en compte aspectes com les conseqüències potencials o materialitzades que provoca una amenaça determinada en un sistema d'informació i/o comunicació, així com en la mateixa entitat afectada (organismes públics o privats, i particulars).

Els criteris emprats per determinar el nivell d'impacte associat a un ciberincident atenen els paràmetres següents:

– Impacte en la seguretat nacional o en la seguretat ciutadana.
– Efectes en la prestació d'un servei essencial o en una infraestructura crítica.
– Tipologia de la informació o sistemes afectats.
– Grau d'afectació a les instal·lacions de l'organització.
– Possible interrupció en la prestació del servei normal de l'organització.
– Temps i costos propis i aliens fins a la recuperació del funcionament normal de les instal·lacions.
– Pèrdues econòmiques.
– Extensió geogràfica afectada.
– Danys reputacionals associats.

Els incidents s'han d'associar a un dels nivells d'impacte següents: CRÍTIC, MOLT ALT, ALT, MITJÀ, BAIX, SENSE IMPACTE.

Nivell crític:

– Afecta apreciablement la seguretat nacional.
– Afecta la seguretat ciutadana, amb perill potencial per a la vida de les persones.
– Afecta una infraestructura crítica.
– Afecta sistemes classificats SECRET.
– Afecta més del 90% dels sistemes de l'organització.
– Interrupció en la prestació del servei superior a 24 hores i superior al 50% dels usuaris.

– El ciberincident requereix per resoldre's més de 100 jornades-persona.
– Impacte econòmic superior al 0,1% del producte interior brut (PIB) actual.
– Extensió geogràfica supranacional.
– Danys reputacionals molt elevats i cobertura contínua en mitjans de comunicació internacionals.

Nivell molt alt:

– Afecta la seguretat ciutadana amb perill potencial per a béns materials.
– Afecta apreciablement activitats oficials o missions a l'estranger.
– Afecta un servei essencial.
– Afecta sistemes classificats RESERVAT.
– Afecta més del 75% dels sistemes de l'organització.
– Interrupció en la prestació del servei superior a 8 hores i superior al 35% dels usuaris.
– El ciberincident requereix per resoldre's entre 30 i 100 jornades-persona.
– Impacte econòmic entre el 0,07% i el 0,1% del PIB actual.
– Extensió geogràfica superior a 4 comunitats autònomes o un territori d'interès singular (TIS, es consideren com a tal les ciutats de Ceuta i Melilla i cadascuna de les illes que formen els arxipèlags de les illes Balears i les illes Canàries).
– Danys reputacionals a la imatge del país (marca Espanya).
– Danys reputacionals elevats i cobertura contínua en mitjans de comunicació nacionals.

Nivell alt:

– Afecta més del 50% dels sistemes de l'organització.
– Interrupció en la prestació del servei superior a 1 hora i superior al 10% d'usuaris.
– El ciberincident requereix per resoldre's entre 5 i 30 jornades-persona.
– Impacte econòmic entre el 0,03% i el 0,07% del PIB actual.
– Extensió geogràfica superior a 3 comunitats autònomes.
– Danys reputacionals de difícil reparació, amb ressò mediàtic (àmplia cobertura en els mitjans de comunicació) i que afecta la reputació de tercers.

Nivell mitjà:

– Afecta més del 20% dels sistemes de l'organització.
– Interrupció en la presentació del servei superior al 5% d'usuaris.
– El ciberincident requereix per resoldre's entre 1 i 5 jornades-persona.
– Impacte econòmic entre el 0,001% i el 0,03% del PIB actual.
– Extensió geogràfica superior a 2 comunitats autònomes.
– Danys reputacionals apreciables, amb ressò mediàtic (àmplia cobertura en els mitjans de comunicació).

Nivell baix:

– Afecta els sistemes de l'organització.
– Interrupció de la prestació d'un servei.
– El ciberincident requereix per resoldre's menys d'1 jornada-persona.
– Impacte econòmic entre el 0,0001% i el 0,001% del PIB actual.
– Extensió geogràfica superior a 1 comunitat autònoma.
– Danys reputacionals puntuals, sense ressò mediàtic.

Sense impacte:

– No hi ha cap impacte apreciable.

5. *Informació que s'ha de notificar a l'autoritat competent en cas d'incident*

El subjecte obligat ha de comunicar, en la notificació inicial, tots els camps sobre els quals tingui coneixement en aquell moment d'acord amb la taula següent, i posteriorment és preceptiu emplenar tots els camps de la taula en la notificació final de l'incident.

Taula 2. *Informació que s'ha de notificar a l'autoritat competent en cas d'incident*

Què notificar	Descripció
Afer.	Frase que descrigui de manera general l'incident. Aquest camp l'han d'heretar totes les notificacions associades a l'incident.
OSE/PSD.	Denominació de l'operador de serveis essencials o proveïdor de serveis digitals que notifica.
Sector estratègic.	Energia, transport, financer, etc.
Data i hora de l'incident.	Indiqueu amb la precisió més alta possible quan ha ocorregut el ciberincident.
Data i hora de detecció de l'incident.	Indiqueu amb la precisió més alta possible quan s'ha detectat el ciberincident.
Descripció.	Descriviu amb detall el que ha succeït.
Recursos tecnològics afectats.	Indiqueu la informació tècnica sobre el nombre i tipus d'actius afectats pel ciberincident, incloses adreces IP, sistemes operatius, aplicacions, versions…
Origen de l'incident.	Indiqueu la causa de l'incident si es coneix. Obertura d'un fitxer sospitós, connexió d'un dispositiu USB, accés a una pàgina web maliciosa, etc.
Taxonomia (classificació).	Possible classificació i tipus de ciberincident en funció de la taxonomia descrita.
Nivell de perillositat.	Especifiqueu el nivell de perillositat assignat a l'amenaça.
Nivell d'impacte.	Especifiqueu el nivell d'impacte assignat a l'incident.
Impacte transfronterer.	Indiqueu si l'incident té impacte transfronterer en algun Estat membre de la Unió Europea.
Pla d'acció i contramesures.	Actuacions efectuades fins al moment en relació amb el ciberincident. Indiqueu el pla d'acció seguit juntament amb les contramesures implantades.
Afectació.	Indiqueu si l'afectat és una empresa o un particular, i les afectacions segons el nivell d'impacte assignat.
Mitjans necessaris per a la resolució (J-P).	Capacitat emprada en la resolució de l'incident en jornades-persona.
Impacte econòmic estimat (si es coneix).	Costos associats a l'incident, tant de caràcter directe com indirecte.
Extensió geogràfica (si es coneix).	Local, autonòmic, nacional, supranacional, etc.
Danys reputacionals (si es coneixen).	Afectació de la imatge corporativa de l'operador.
Adjunts.	Indiqueu la relació de documents adjunts que s'aporten per ajudar a conèixer la causa del problema o a la seva resolució (captures de pantalla, fitxers de registre d'informació, correus electrònics, etc.).
Regulació afectada.	ENS / RGPD / NIS / PIC / Altres.
Es requereix actuació de les forces i cossos de seguretat de l'Estat.	Sí / No.

6. *Finestra temporal de report*

Tots els subjectes obligats que es vegin afectats per un incident de notificació obligada a l'autoritat competent, a través del CSIRT de referència, han de remetre, dins el termini establert i en la forma pertinent, aquelles notificacions inicial, intermèdia i final requerides d'acord amb la finestra temporal de report següent.

– La notificació inicial és una comunicació consistent a posar en coneixement un incident i alertar-ne de l'existència.
– La notificació intermèdia és una comunicació mitjançant la qual s'actualitzen les dades disponibles en aquell moment relatives a l'incident comunicat.
– La notificació final és una comunicació final mitjançant la qual s'amplien i es confirmen les dades definitives relatives a l'incident comunicat.

No obstant això, s'han d'aportar totes les notificacions addicionals intermèdies o posteriors que es considerin necessàries.

Taula 3. Finestra temporal de report

Nivell de perillositat o impacte	Notificació inicial	Notificació intermèdia	Notificació final
CRÍTIC.	Immediata.	24/48 hores.	20 dies.
MOLT ALT.	Immediata.	72 hores.	40 dies.
ALT.	Immediata.	–	–
MITJÀ.	–	–	–
BAIX.	–	–	–

Els temps reflectits a la taula 3 per a la «notificació intermèdia» i la «notificació final» tenen com referència el moment de remissió de la «notificació inicial». La «notificació inicial» té com a referència de temps el moment de tenir coneixement de l'incident.

7. *Definicions i conceptes*

La descripció de les conductes aquí incloses té caràcter tècnic i s'entén als mers efectes de la notificació i gestió de ciberincidents. Com a tal, és independent tant de la qualificació dels fets com de l'aplicació per part de l'autoritat judicial dels tipus penals que estableix la Llei orgànica 10/1995, de 23 de novembre, del Codi penal.

Contingut abusiu:

– Correu massiu no sol·licitat (*spam*): correu electrònic no sol·licitat que s'envia a un gran nombre d'usuaris, o bé una taxa alta de correus electrònics enviats a un mateix usuari en un espai curt de temps.
– Assetjament: referit a assetjament virtual o ciberassetjament, es tracta de l'ús de mitjans de comunicació digitals per assetjar una persona, o grup de persones, mitjançant atacs personals, divulgació d'informació privada o íntima, o falsa.
– Extorsió: obligar una persona o mercantil, mitjançant l'ús de violència o intimidació, a fer o ometre actes amb la intenció de produir un perjudici a aquesta, o bé amb ànim de lucre de la que ho provoca.
– Missatges ofensius: comunicacions no esperades o desitjades, així com accions o expressions que lesionen la dignitat d'una altra persona, i que menyscaben la seva fama o atempten contra la seva autoestima.
– Delicte: qualsevol acció tipificada com a delicte d'acord amb el que estableix la Llei orgànica 10/1995, de 23 de novembre, del Codi penal.

– Pederàstia: qualsevol comportament relacionat amb els que descriu el títol VIII la Llei orgànica 10/1995, de 23 de novembre, del Codi penal, relatius a la captació o utilització de menors d'edat o persones amb discapacitat necessitades d'una protecció especial en actes que atemptin contra la seva indemnitat o llibertat sexual.

– Racisme: qualsevol infracció penal, incloses les infraccions contra les persones o les propietats, en què la víctima, el local o l'objectiu de la infracció es tria per la seva connexió, simpatia, filiació, suport o pertinença, real o percebuda, a un grup social, raça, religió o condició sexual.

– Apologia de la violència: exposició, davant una concurrència de persones o per qualsevol mitjà de difusió, d'idees o doctrines que exalcin el crim o n'enalteixin l'autor.

Contingut perjudicial:

– *Malware* (codi perjudicial): paraula que deriva dels termes *malicious* i *software*. Qualsevol peça de *software* que porti a terme accions com ara extracció de dades o un altre tipus d'alteració d'un sistema es pot categoritzar com a programari maliciós. Així doncs, programari maliciós és un terme que engloba diversos tipus de programes perjudicials.

– Virus: tipus de programari maliciós l'objectiu principal del qual és modificar o alterar el comportament d'un sistema informàtic sense el permís o consentiment de l'usuari. Es propaga mitjançant l'execució en el sistema de programari, arxius o documents amb una càrrega perjudicial, que adquireix la capacitat de replicar-se d'un sistema a un altre. Els mètodes més comuns d'infecció es donen a través de dispositius extraïbles, descàrregues d'Internet i arxius adjunts en correus electrònics. No obstant això, també ho pot fer a través de *scripts*, documents i vulnerabilitats XSS presents en el web. És ressenyable que un virus requereix l'acció humana per propagar-se a diferència d'altres programaris maliciosos, vegeu cuc.

– Cuc: programa maliciós que té com a característica principal un alt grau de dispersabilitat. La seva finalitat és replicar-se a nous sistemes per infectar-los i seguir replicant-se a altres equips informàtics, aprofitant-se de tot tipus de mitjans com el correu electrònic, IRC, FTP, P2P i altres protocols específics o utilitzats àmpliament.

– Troià: tipus de programari maliciós que s'emmascara com a programari legítim amb la finalitat de convèncer la víctima perquè instal·li la peça en el seu sistema. Una vegada instal·lat, el programari perjudicial té la capacitat de desenvolupar activitat perjudicial en segon pla. Un troià no depèn d'una acció humana i no té la capacitat de replicar-se, però pot tenir una gran capacitat perjudicial en un sistema com a troians o explotant vulnerabilitats de programari.

– Programari espia (*spyware*): tipus de programari maliciós que espia les activitats d'un usuari sense el seu coneixement o consentiment. Aquestes activitats poden incloure enregistradors de teclat (*keyloggers*), monitoratges i recol·lecció de dades, així com robatori de dades. Els *spyware* es poden difondre com un troià o mitjançant explotació de programari.

– Paquet d'intrusió: conjunt de programari perjudicial que permet l'accés privilegiat a àrees d'una màquina, mentre al mateix temps s'oculta la seva presència mitjançant la corrupció del sistema operatiu o altres aplicacions. Cal denotar que per maquina s'entén tot l'espectre de sistemes IT, des de *smartphones* fins a ICS. El propòsit d'un paquet d'intrusió, per tant, és emmascarar eficaçment càrregues útils (*payloads*) i permetre'n l'existència en el sistema.

– Marcador (*dialer*): tipologia de programari maliciós que s'instal·la en una màquina i, de manera automàtica i sense consentiment de l'usuari, efectua marcatges telefònics a números de tarifació especial. Aquestes accions comporten costos econòmics en la víctima en repercutir l'import de la comunicació.

– Programari de segrest: s'engloba sota aquest epígraf el programari maliciós que infecta una màquina de manera que l'usuari és incapaç d'accedir a les dades emmagatzemades en el sistema. Normalment la víctima rep posteriorment algun tipus de comunicació en la qual se'l coacciona perquè pagui una recompensa que permeti accedir al sistema i als arxius bloquejats.

– Bot perjudicial: xarxa de zombis (*botnet*) és el nom que s'utilitza per designar un conjunt de màquines controlades remotament amb finalitat generalment maliciosa. Un bot és una peça de programari maliciosa que rep ordres d'un atacant principal que controla remotament la màquina. Els servidors C&C habiliten l'atacant per controlar els bots per tal que executin les ordres dictades remotament.

– RAT: de l'anglès *Remote Access Tool*, es tracta d'una funcionalitat específica de control remot d'un sistema d'informació, que incorporen determinades famílies o mostres de programari maliciós.

– C&C: de l'anglès *Command and Control*, es refereix a quadres de comandament i control (també referenciats com a C2), pels quals atacants cibernètics controlen determinats equips zombis infectats amb mostres de la mateixa família de programari perjudicial. El quadre de comandament i control actua com a punt de referència, control i gestió dels equips infectats.

– Connexió sospitosa: tot intercanvi d'informació a escala de xarxa local o pública, l'origen o destinació de la qual no estigui plenament identificat, així com la seva legitimitat.

Obtenció d'informació:

– Escaneig de ports (*scanning*): anàlisi local o remot, mitjançant programari, de l'estat dels ports d'una màquina connectada a una xarxa. La finalitat d'aquesta acció és la d'obtenir informació relativa a la identificació dels serveis actius i les possibles vulnerabilitats que puguin existir en la xarxa.

– Escaneig de xarxa (*scanning*): anàlisi local o remota, mitjançant programari, de l'estat d'una xarxa. La finalitat d'aquesta acció és la d'obtenir informació relativa a la identificació dels serveis actius i les possibles vulnerabilitats que puguin existir en la xarxa.

– Escaneig de tecnologies: anàlisi local o remota, mitjançant programari, de les tecnologies presents o disponibles en una xarxa determinada o un sistema d'informació concret, mitjançant la qual s'obtenen les referències del maquinari/programari present, així com la seva versió, i potencials vulnerabilitats.

– Transferència de zona DNS (AXFR IXFR): transacció dels servidors DNS utilitzada per replicar les bases de dades entre un servidor primari i els secundaris. Aquestes transaccions poden ser completes (AXFR) o incrementals (IXFR).

– Anàlisi de paquets (*sniffing*): anàlisi mitjançant programari del trànsit d'una xarxa amb la finalitat de capturar informació. El trànsit que viatgi no xifrat pot ser capturat i llegit per un atacant.

– Enginyeria social: tècniques que cerquen la revelació d'informació sensible d'un objectiu, generalment mitjançant l'ús de mètodes persuasius i amb absència de voluntat o coneixement de la víctima.

– Pesca: estafa comesa a través de mitjans telemàtics mitjançant la qual l'estafador intenta aconseguir, d'usuaris legítims, informació confidencial (contrasenyes, dades bancàries, etc.) de manera fraudulenta utilitzant mètodes d'enginyeria social.

– Pesca dirigida (*spear phishing*): variant de la pesca mitjançant la qual l'atacant focalitza la seva actuació sobre un objectiu concret.

Intrusions:

– Explotació: qualsevol pràctica mitjançant la qual un atacant cibernètic vulnera un sistema d'informació i/o comunicació, amb fins il·lícits o per als quals no està degudament autoritzat.

– Injecció SQL: tipus d'explotació, consistent en la introducció de cadenes mal formades de SQL, o cadenes que el receptor no espera o controla degudament, les quals provoquen resultats no esperats en l'aplicació o programa objectiu, i per la qual l'atacant produeix efectes inesperats i per als quals no està autoritzat en el sistema objectiu.

– *Cross Site Scripting* XSS (directe o indirecte): atac que tracta d'explotar una vulnerabilitat present en aplicacions web, per la qual un atacant injecta sentències mal formades o cadenes que el receptor no espera o controla degudament.

– *Cross Site Request Forgery* (CSFR): falsificació de petició en llocs creuats. És un tipus d'explotador perjudicial d'un lloc web en què un usuari en el qual el lloc web confia transmet comandaments no autoritzats. Aquesta vulnerabilitat és coneguda també per altres noms, com ara XSRF, enllaç hostil, atac d'un clic, encavalcament de sessió, i atac automàtic. Al contrari que en els atacs XSS, els quals exploten la confiança que un usuari té en un lloc en particular, el *Cross Site Request Forgery* explota la confiança que un lloc té en un usuari en particular.

– Desfiguració (*defacement*): tipologia d'atac a llocs web en què s'implementa un canvi en l'aparença visual de la pàgina. Amb aquesta finalitat, se solen utilitzar tècniques com ara injeccions SQL o algun tipus de vulnerabilitat existent a la pàgina o al servidor.

– Inclusió de fitxers (RFI i LFI): vulnerabilitat que permet a un atacant mostrar o executar arxius remots allotjats en altres servidors a causa d'una mala programació de la pàgina que conté funcions d'inclusió d'arxius. La inclusió local d'arxius (LFI) és similar a la vulnerabilitat d'inclusió d'arxius remots, excepte que en lloc d'incloure arxius remots només es poden incloure arxius locals, és a dir arxius en el servidor actual per a la seva execució.

– Evasió de sistemes de control: procés pel qual una mostra de programari perjudicial, o un conjunt d'accions orquestrades per un atacant cibernètic, aconsegueixen vulnerar o esquivar els sistemes o les polítiques de seguretat establertes per un determinat sistema d'informació i comunicació.

– Descaminament (*pharming*): atac informàtic que aprofita vulnerabilitats dels servidors DNS (*Domain Name System*). Quan l'usuari tracta d'accedir al lloc web, el navegador redirigeix automàticament l'usuari a una adreça IP on s'allotja un web maliciós que suplanta l'autèntic i en el qual l'atacant pot obtenir informació sensible dels usuaris.

– Atac per força bruta: procés pel qual un atacant tracta de vulnerar un sistema de validació per credencials d'accés, contrasenya o similar mitjançant l'ús de totes les combinacions possibles, amb la finalitat d'accedir a sistemes d'informació i/o comunicació per als quals no té privilegis o autorització.

– Atac per diccionari: procés pel qual un atacant tracta de vulnerar un sistema de validació per credencials d'accés, contrasenya o similar mitjançant l'ús d'un diccionari prèviament generat amb determinades combinacions de caràcters, amb la finalitat d'accedir a sistemes d'informació i/o comunicació per als quals no té privilegis o autorització.

– Robatori de credencials d'accés: accés o sostracció no autoritzada de credencials d'accés a sistemes d'informació i/o comunicació.

Disponibilitat:

– DoS (*Denial of Service*) o atac de denegació de servei: conjunt de tècniques que tenen per objectiu deixar un servidor inoperatiu. Mitjançant aquest tipus d'atacs es pretén sobrecarregar un servidor i d'aquesta manera impedir que els usuaris legítims puguin utilitzar els serveis que presta. L'atac consisteix a saturar el servidor amb peticions de servei fins que aquest no les pot atendre, cosa que en provoca el col·lapse.

– DDoS (*Distributed Denial of Service*) o denegació de servei distribuït: variant de DoS en què la remissió de peticions es porta a terme de manera coordinada des de diversos punts cap a una mateixa destinació. Amb aquesta finalitat s'utilitzen xarxes de bots, generalment sense el coneixement dels usuaris.

– Mala configuració: fallada de configuració en el programari que està directament associada amb una pèrdua de disponibilitat d'un servei.

– Sabotatge/Terrorisme/Vandalisme: atacs implementats amb l'objectiu de provocar la interrupció o degradació de la prestació d'un servei, que provoquen danys rellevants en la continuïtat del servei d'una institució o danys reputacionals rellevants comesos amb propòsits ideològics, polítics o religiosos.

– Disrupció sense intenció perjudicial: accions que poden provocar la interrupció o degradació de la prestació d'un servei, que provoquen danys rellevants en la continuïtat del servei d'una institució o danys reputacionals rellevants.

– Inundació SYN o UDP: procediments utilitzats per cometre un atac DoS o DDoS que consisteix a iniciar una gran quantitat de sessions per impedir que el servidor atengui les peticions lícites.

– DNS *Open-Resolver*: servidor DNS capaç de resoldre consultes DNS recursives procedents de qualsevol origen d'Internet. Aquest tipus de servidors els solen utilitzar usuaris malintencionats per efectuar atacs DDoS.

Compromís de la informació:

– Accés no autoritzat a la informació o ciberespionatge: procés pel qual un usuari no autoritzat accedeix a consultar contingut per al qual no està autoritzat.

– Modificació no autoritzada d'informació: procés pel qual un usuari no autoritzat accedeix a modificar contingut per al qual no està autoritzat.

– Esborrament no autoritzat d'informació: procés pel qual un usuari no autoritzat accedeix a esborrar contingut per al qual no està autoritzat.

– Exfiltració d'informació: procés pel qual un usuari difon informació en canals o fonts en què no està previst o autoritzat compartir aquesta informació.

– Accés no autoritzat a sistemes: procés pel qual un usuari accedeix, sense vulnerar cap servei, sistema o xarxa, a sistemes d'informació i/o comunicació per als quals no està degudament autoritzat o no té autorització tàcita o manifesta.

– Atac POODLE / Atac FREAK: procés pel qual s'aconsegueix que un servidor faci ús d'un protocol de comunicacions no segur, que originalment no estava previst, amb l'objectiu de poder exfiltrar informació.

Frau:

– Ús no autoritzat de recursos: utilització de tecnologies i/o serveis per part d'usuaris que no estan degudament autoritzats per la direcció o negociat competent.

– Suplantació d'identitat: activitat maliciosa en la qual un atacant es fa passar per una altra persona per cometre algun tipus de frau o assetjament.

– Drets de propietat intel·lectual: la propietat intel·lectual és el conjunt de drets que corresponen als autors i a altres titulars (artistes, productors, organismes de radiodifusió…) respecte de les obres i prestacions fruit de la seva creació.

– Altres fraus: engany econòmic amb la intenció d'aconseguir un benefici, i amb el qual algú resulta perjudicat.

Vulnerabilitats:

– Tecnologia vulnerable: coneixement, per part dels administradors de tecnologies, serveis o xarxes, de vulnerabilitats presents en aquestes.

– Política de seguretat precària: política de seguretat de l'organització deficient, mitjançant la qual hi ha la possibilitat que, durant un espai de temps determinat, atacants cibernètics realitzessin accessos no autoritzats a sistemes d'informació, però aquest punt no es pot determinar fefaentment.

Altres:

– Ciberterrorisme: delictes informàtics que preveuen els article 197 bis i ter i 264 a 264 quater de la Llei orgànica 10/1995, de 23 de novembre, del Codi penal, quan aquests delictes es cometin amb les finalitats que preveu l'article 573.1 del mateix text. Aquestes finalitats són:

• Subvertir l'ordre constitucional, o suprimir o desestabilitzar greument el funcionament de les institucions polítiques o de les estructures econòmiques o socials de l'Estat, o obligar els poders públics a fer un acte o a abstenir-se de fer-lo.
• Alterar greument la pau pública.
• Desestabilitzar greument el funcionament d'una organització internacional.
• Provocar un estat de terror en la població o en una part d'aquesta.

– Danys informàtics PIC: delictes informàtics que preveuen els articles 264.2 3r i 4t de la Llei orgànica 10/1995, de 23 de novembre, del Codi penal, relacionats amb l'esborrament, dany, alteració, supressió o inaccessibilitat de dades, programes informàtics o documents electrònics d'una infraestructura crítica. Així com conductes greus relacionades amb els termes anteriors que afectin la prestació d'un servei essencial.
– APT (*Advanced Persistent Threat* o amenaça persistent avançada)/AVT (*Advanced Volatility Threat*): atacs dirigits contra organitzacions concretes, sustentats en mecanismes molt sofisticats d'ocultació, anonimat i persistència. Aquesta amenaça habitualment utilitza tècniques d'enginyeria social per aconseguir els seus objectius juntament amb l'ús de procediments d'atac coneguts o genuïns.
– Dominis DGA: procediment per generar de manera dinàmica dominis on s'han d'allotjar els servidors de comandament i control, tècnica utilitzada en xarxes de zombis per dificultar-ne la detenció.
– Criptografia: tècnica que consisteix a xifrar un missatge, conegut com a text net, per convertir-lo en un missatge xifrat o criptograma, que resulta il·legible per a tot aquell que no conegui la clau mitjançant la qual s'ha xifrat.
– Proxy: ordinador, generalment un servidor, intermediari utilitzat en les comunicacions entre dos equips més, i que normalment s'utilitza de manera transparent per a l'usuari.

General:

– Ciberseguretat: 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.
– Ciberespai: espai virtual que engloba tots els sistemes TIC. El ciberespai es recolza en la disponibilitat d'Internet com a xarxa de xarxes, enriquida amb altres xarxes de transport de dades.
– Xarxes i sistemes d'informació: s'entén per aquest concepte un dels tres punts següents:

• Les xarxes de comunicacions electròniques, tal com venen definides en el número 31 de l'annex II de la Llei 9/2014, de 9 de maig, general de telecomunicacions.
• Tot dispositiu o grup de dispositius interconnectats o relacionats entre si en què un o diversos d'aquests efectuen, mitjançant un programa, el tractament automàtic de dades digitals.
• Les dades digitals emmagatzemades, tractades, recuperades o transmeses mitjançant elements previstos anteriorment per al seu funcionament, utilització, protecció i manteniment.

– Seguretat en xarxes i 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.

– Operador de serveis essencials: entitat pública o privada que s'identifiqui considerant els factors que estableix l'article 6 del Reial decret llei 12/2018, de 7 de setembre, que presti els serveis esmentats en algun dels sectors estratègics que defineix l'annex de la Llei 8/2011, de 28 d'abril.

– 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.

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

– Ciberincident: tot fet que tingui efectes adversos reals en la seguretat de les xarxes i els sistemes d'informació.

– Gestió de ciberincidents: tots els procediments seguits per detectar, analitzar i limitar un incident i respondre davant d'aquest.

– Ciberamenaça: amenaça als sistemes i serveis presents en el ciberespai o assolibles a través d'aquest.

– Taxonomia: classificació o ordenació en grups d'objectes o subjectes que tenen unes característiques comunes.

– RGPD: Reglament general de protecció de dades, 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.

– OpenPGP: estàndard basat en el programa PGP, de l'anglès *Pretty Good Privacy*, la finalitat del qual és protegir la informació mitjançant l'ús de criptografia de clau pública, així com facilitar l'autenticació de documents gràcies a signatures digitals.

– *Webinject*: eina gratuïta i de codi obert dissenyada principalment per automatitzar la prova de les aplicacions i serveis web.

– Telnet: protocol de xarxa que permet accedir a una altra màquina per manejar-la remotament com si estiguéssim asseguts davant d'ella.

– RDP (*Remote Desktop Protocol*): protocol propietari que permet la comunicació en l'execució d'una aplicació entre un terminal i un servidor.

– VNC (*Virtual Network Computing*): programa de programari lliure basat en una estructura client-servidor que permet observar remotament les accions de l'ordinador servidor a través d'un ordinador client.

– SNMP (*Simple Network Management Protocol*): protocol de xarxa utilitzat per a l'intercanvi de missatges per a l'administració de dispositius en xarxa.

– Redis: motor de base de dades en memòria, basat en l'emmagatzematge en taules de *hashes*.

– ICMP (*Internet Control Message Protocol*): protocol de control de missatges d'Internet.

– Còpia de seguretat neta: punt de restauració d'un sistema de la qual es té la seguretat que no està compromesa.