I. XEDAPEN OROKORRAK

ESTATUKO BURUZAGITZA

12257 *12/2018 Errege Lege Dekretua, irailaren 7koa, Informazio Sare eta Sistemen Segurtasunarena.*

I

Informazioaren eta komunikazioaren teknologien ondorioz eta, bereziki, Interneten garapenaren ondorioz, informazio-sareek eta -sistemek funtsezko eginkizuna betetzen dute gure gizartean; hortaz, ezinbestekoa da fidagarriak eta seguruak izan daitezen, jarduera ekonomikoak eta sozialak normal aurrera egin ahal izateko.

Ildo horretatik, informazio-sareetan edo -sistemetan intzidenteak gertatzen baldin badira, jarduera ekonomiko eta sozialak ere nahastuko dira. Intzidenteak gertatzea, beraz, arrisku handia da, eta, ustekabean zein nahita gertatuta ere, honako ondorio hauek eragin ditzakete: diru-galerak izatea, herritarren konfiantzari kalte egitea eta, azken batean, ekonomian eta gizartean kalte larriak eragitea, bai eta nazioaren segurtasunean eragitea ere, hipotesi okerrenean.

Informazioaren eta komunikazioaren teknologien bereizgarria zeharkakoak eta interkonektatuak izatea da; baina teknologia horiek dituzten mehatxuak eta arriskuak ere halakoak dira. Horregatik, banaka aztertzen badira, txikiagoa izango da mehatxu eta arrisku horiei aurre egiteko neurrien eraginkortasuna. Informazio-segurtasunaren arloko eskakizunak sektore-eremu bakoitzarentzat era independentean zehazten badira, eraginkorrak ez izateko arriskua dago, aipatutako zeharkakotasuna dela eta.

Horrenbestez, komeni da ikuspegi integralaren araberako mekanismoak ezartzea. Mekanismook aukera eman behar dute informazio-sare eta -sistemek dituzten arriskuetatik hobeto babesteko eta nazioan edo gure inguruneko herrialdeen eremuan –bereziki, Europar Batasunean– egiten diren jarduketak koordinatzen laguntzeko.

II

Errege lege-dekretu hau xede hori betetzeko ematen da, hain zuzen ere. Beronen bidez, Espainiako ordenamendu juridikoan Europako Parlamentuaren eta Kontseiluaren 2016/1148 (EB) Zuzentarauaren transposizioa egiten da, 2016ko uztailaren 6koa da zuzentarau hori, Europar Batasuneko informazio-sare eta -sistema guztietan segurtasun handia eta berdina bermatzeko neurriei buruzkoa. Errege lege-dekretu honek oinarri hartzen ditu arlo horretako arauak, intzidenteei erantzuna emateko tresnak eta Estatuko koordinazio-tresnak. Horrek eta I. apartatuan emandako arrazoiek justifikatzen dute dekretu honen edukiaren irismenak zuzentarau horrena gainditzea.

Errege lege-dekretu hau komunitatean ezinbesteko zerbitzuak ematen dituzten erakundeei aplikatuko zaie, baldin eta, beren jarduera garatzeko, informazio-sare eta -sistemak behar badituzte. Zuzentarauan berariaz jasota ez dauden sektoreei ere aplikatuko zaie; hortaz, errege lege-dekretu honek ikuspegi globala dauka, baina lege espezifikoak ere errespetatzen dira. Baina, sareak ustiatzeko eta komunikazio elektronikoko zerbitzuak emateko jardueretan eta horiekin lotutako baliabideetan, bai eta konfiantzako zerbitzu elektronikoetan ere, zeinak zuzentarau horretatik berariaz baztertu baitziren, errege lege-dekretu hau operadore kritikoei baino ez zaie aplikatuko.

Errege lege-dekretu hau zerbitzu digital zehatz batzuk ematen dituzten hornitzaileei ere aplikatuko zaie; zehazki, harmonizazio handieneko araubide baten mende jartzen ditu Europako Parlamentuaren eta Kontseiluaren 2016/1148 (EB) Zuzentarauak, 2016ko uztailaren 6koak: erregelamendu baten baliokidea den araubide baten mende. Hala egin da, eremu nazionaleko arauketa eraginkorra izango ez litzatekeelakoan, zerbitzuok transnazionalak direlako. Nazioko agintarien zeregina, beraz, beren herrialdeetan

ezarritako hornitzaileek araubidea betetzen duten gainbegiratzea eta Europar Batasuneko beste herrialde batzuetako agintariekin koordinatzea baino ez da.

Zuzentarau horren arabera, errege dekretu-legeak zehazten du zer sektoretan bermatu behar den informazio-sareen eta -sistemen babesa. Horrez gain, prozedurak ezartzen ditu sektore horietako ezinbesteko zerbitzuak eta zerbitzuok ematen dituzten operadore nagusiak identifikatzeko. Izan ere, operadore nagusi horiek dira errege lege-dekretu honen hartzaile nagusiak.

Ezinbesteko zerbitzuak ematen dituzten operadoreek eta zerbitzu digitalak ematen dituzten hornitzaileek neurri egokiak hartu behar dituzte beren informazio-sareetan eta -sistemetan sortzen diren segurtasun-arriskuak kudeatzeko, nahiz eta kudeaketa azpikontratatuta egon. Hartzen duten arriskua eta aurretiazko ebaluazioaren emaitzak nolakoak diren, halakoak izan behar dute beren gain hartu behar dituzten segurtasun-betebeharrek. Errege lege-dekretu honetako garapen-arauetan zehazten dira ezinbesteko zerbitzuak ematen dituzten operadoreei eskatu ahal zaizkien segurtasun-betebeharrak eta, hala dagokionean, egin behar dituzten ikuskapenak, bai eta krisiak kudeatzeko jarduerak eta ariketak ere.

Errege lege-dekretu honek ezartzen du ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek beren informazio-sareetako eta -sistemetako intzidenteak jakinarazi behar dituztela intzidenteok zerbitzuotan perturbazio nabarmenak dakartzatenean. Halaber, ezinbesteko zerbitzuei eragin diezaieketen baina oraindik benetan kalte egin ez dieten gertaerak edo gorabeherak jakinarazteko aukera jasotzen du, eta jakinarazpenak egiteko prozedurak zehazten ditu.

Intzidenteak jakinaraztea arriskuak kudeatzeko kulturaren alderdi bat da, eta zuzentarauak eta errege lege-dekretu honek kultura hori sustatzen dute. Hori dela eta, jakinarazpena egiten duen erakundea eta gertaeren berri ematen duten langileak babesten ditu errege lege-dekretu honek; isilpeko informazioa babesten du, jendaurrean edo jakinarazpenaren hartzaileak ez diren agintarien artean ez zabaltzeko, eta baimena ematen du intzidenteak jakinarazteko betebeharrik ez dagoenean ere jakinarazteko.

Errege lege-dekretu honetan azpimarratzen da kontuan hartu behar direla Europar Batasuneko eta nazioarteko estandarrak, bai eta kooperazio-taldeak eta CSIRT (*Computer Security Incident Response Team*) sareak ematen dituzten gomendioak ere –zuzentarauak ezarri ditu estandar eta gomendio horiek Europar Batasunaren esparruan–. Horren xedea da foro horietan ikasitako jardunbide egokienak aplikatzea, barne-merkatua sustatzen laguntzea eta gure enpresek bertan parte har dezaten bultzatzea.

Betebeharren eraginkortasuna areagotzeko eta, aldi berean, betebeharrek erakundeei eragiten dizkieten administrazio- eta ekonomia-zamak arintzeko, errege lege-dekretu honetan, bermatu nahi izan da informazio-segurtasunaren arloko beste araudi batzuek –hala horizontalek nola sektorialek– dakartzaten betebeharrak eta errege lege-dekretu honetakoak koherenteak direla elkarrekin. Horrez gain, kasu bakoitzean erantzuleak diren agintariekiko koordinazioa bermatu nahi izan da.

Arau horizontalei dagokienez, ezarritako loturak kontuan hartzen baldin badira, honako hauek nabarmendu behar dira: apirilaren 28ko 8/2011 Legea, azpiegitura kritikoak babesteko neurriak ezartzen dituena; irailaren 28ko 36/2015 Legea, Segurtasun Nazionalari buruzkoa, eta urtarrilaren 8ko 3/2010 Errege Dekretua, Segurtasunerako Eskema Nazionala Administrazio Elektronikoaren eremuan arautzen duena (sektore publikoko informazio-sistemen segurtasun-arloari buruzko arautegi berezitzat hartuta).

Hori horrela, errege lege-dekretu honen aplikazio-eremua eta apirilaren 28ko 8/2011 Legearena antzekoak dira, eta Europako Parlamentuaren eta Kontseiluaren 2016ko uztailaren 6ko 2016/1148 (EB) Zuzentarauan ezarritako sektoreekin batera, lege horretan ezarritako sektore estrategikoak ere kontuan hartzen dira. Lege horretan oinarritzen da *ezinbesteko zerbitzu*aren definizioa; eta kide anitzeko organoei egozten zaie errege lege-dekretu honen mende dauden ezinbesteko zerbitzuak eta ezinbesteko zerbitzuen operadoreak zehaztea. Irailaren 28ko 36/2015 Legearekin bat etorrita, Segurtasun Nazionalerako Kontseiluari esleitzen zaio Europar Batasuneko beste herrialde batzuekin

harremanetan egoteko gunea izateko funtzioa, bai eta zibersegurtasunaren arloko politika Zibersegurtasun Nazionalaren Estrategiaren bitartez koordinatzekoa ere.

III

Espainian 2013az geroztik ezarrita dago Zibersegurtasun Nazionalaren Estrategia. Estrategia horretan lehentasunak, helburuak eta neurri egokiak ezartzen dira informazio-sareetan eta -sistemetan segurtasun handia lortzeko eta horri eusteko. Estrategia horrek are gehiago garatuko du errege lege-dekretu honetan zirriborratzen den esparru instituzionala. Esparru hori, batetik, agintari publiko eskudunek eta erreferentziako CSIRTek eta, bestetik, kooperazio publiko-pribatuek osatzen dute.

Errege lege-dekretu honen arabera bete behar diren zaintza-betebeharrak agintari eskudunek beteko dituzte, eta, beharrezkoa denean, zehapen-araubidea ere aplikatuko dute. Halaber, errege lege-dekretu honetan ezartzen diren betebeharren garapena ere sustatuko dute. Horretarako, kontsulta egingo diete sektoreari eta, sektore zehatz batzuk direnean, gaiaren araberako agintari eskudunei, betebehar bikoizturik, beharrezkoa ez denik edo kostu handiegikorik egon ez dadin.

CSIRT taldeak intzidenteei erantzuna emateko taldeak dira; arriskuak ebaluatzen dituzte eta intzidenteak gainbegiratzen dituzte nazio mailan; intzidenteen gaineko alertak zabaltzen dituzte, eta intzidenteen ondorioak murrizteko irtenbideak ematen dituzte. Europan, CSIRT terminoa da erabiliena, CERT termino babestuaren ordez (*Computer Emergency Response Team*). CERT terminoa Ameriketako Estatu Batuetan erregistratuta dago.

Errege lege-dekretu honetan, dagozkion erreferentziako CSIRT taldeen jardun-eremua mugatzen da. CSIRT taldeak intzidenteen gaineko jakinarazpenak jasotzeko sarrera-ateak dira; hartara, azkar antolatu ahal dute intzidenteei eman behar zaien erantzuna. Intzidenteen gaineko jakinarazpenen hartzaileak, ordea, arlo horretako agintari eskudunak dira; agintariok kontuan hartuko dute informazio hori, operadoreak ikuskatzeko. Edonola ere, operadorea erantzulea da intzidenteak konpontzeko eta eragindako informazio-sareen eta -sistemen ohiko funtzionamendua berreskuratzeko.

Intzidenteak jakinarazteko plataforma komun bat erabiltzea ezartzen da. Horrela, operadoreek ez dituzte banakako zenbait jakinarazpen egin beharko dagokien agintari eskudunaren arabera. Plataforma hori datu pertsonalen segurtasunaren urratze-kasuak jakinarazteko ere erabili ahalko da, Europako Parlamentuaren eta Kontseiluaren apirilaren 27ko 2016/679 (EB) Erregelamenduarekin bat etorrita, zeina datu pertsonalen tratamenduan eta datu horien zirkulazio librean pertsona fisikoak babesteari buruzkoa baita eta 95/46/EE Zuzentaraua indargabetzen baitu.

IV

Errege lege-dekretu hau zazpi titulutan egituratuta dago. Lehenik eta behin, testu osoan zehar erabiltzen diren terminoen definizioak jasota daude, eta funtsezko estatu-funtzioen babesa (besteak beste, segurtasun nazionalarena) eta beste xedapen orokor batzuk. Segidan, II. tituluan, ezinbesteko zerbitzuak eta zerbitzuok emango dituzten operadoreak identifikatzeko modua eta irizpideak zehaztu dira, errege lege-dekretu hau aplikatuko zaien horiek identifikatzekoak. Lehenengo aldiz identifikatzeko jarraitu behar zaion hurrenkera errege lege-dekretu honen lehen xedapen gehigarrian jasota dago. III. tituluan, informazio-sareen eta -sistemen segurtasunaren esparru estrategiko eta instituzionala jaso da, arestian azaldutakoa. Artikulu bat eskaini zaio propio agintari publikoen arteko lankidetzari, arlo horretako eskumenak egoki baliatzeko oinarritzat hartuta.

IV. titulua operadoreen segurtasun-betebeharrei buruzkoa da. Titulu horren arabera, arau sektorialak lehentasunez aplikatu ahal izango dira, errege lege-dekretu honetan ezarritako betebeharren baliokideak ezartzen badituzte, baina horrek ez ditu eragotziko Segurtasun Nazionalerako Kontseiluaren koordinazio-lana eta errege lege-dekretu honi jarraituz agintari eskudunekin lankidetzan jarduteko betebeharra.

V. titulua da titulu luzeena. Hor, intzidenteen jakinarazpena arautzen da, eta mugaz haraindiko inpaktua duten intzidenteei erreparatzen zaie, eta haiek kudeatzeko Europar Batasuneko beste estatu batzuekin partekatu behar den informazioari eta egin behar den koordinazio-lanari. VI. tituluan, agintari eskudunen ikuskaritza- eta kontrol-ahalak ezartzen dira, bai eta beste estatu kide batzuetako agintari nazionalekiko kooperazioa ere. VII. tituluan, errege lege-dekretu honetan ezarritako arau-hausteak eta zehapenak tipifikatuta daude. Horri dagokionez, errege lege-dekretuak, zehapena ezartzeari baino, lehentasun handiagoa ematen dio arau-haustea zuzentzeari. Zigorra ezarri behar izatekotan, disuasio-zigor eraginkorra eta neurritsua izango da, Europako Parlamentuaren eta Kontseiluaren 2016ko uztailaren 6ko 2016/1148 (EB) Zuzentarauan agindutakoarekin bat etorrita.

Errege lege-dekretuaren amaieran, xedapen gehigarriak eta azken xedapenak bildu dira, beharrezkoak baitira arauketa osatzeko.

Xedapen honek bete du informazio-gizartearen zerbitzuei buruzko erregelamendu-arau teknikoen eta erregelamenduen berri emateko prozedura. Prozedura hori Europako Parlamentuaren eta Kontseiluaren 2015/1535 (EB) Zuzentarauan ezarrita dago –2015/1535 (EB) Zuzentaraua, 2015eko irailaren 9koa, informazio-gizartearen zerbitzuei buruzko erregelamendu teknikoen eta arauen arloko informazioa emateko prozedura ezartzen duena–, bai eta 1337/1999 Errege Dekretuan ere –1337/1999 Errege Dekretua, uztailaren 31koa, informazio-gizartearen zerbitzuei buruzko arau eta erregelamendu teknikoen arloko informazioaren bidalketa arautzen duena–. Era berean, betetzen ditu urriaren 1eko 39/2015 Legeak –Administrazio Publikoen Administrazio Prozedura Erkidearenak– 129. artikuluan ezartzen dituen erregulazio onaren printzipioak. Administrazio publikoek, legegintzako ekimena baliatzen dutenean, honako printzipio hauek bete behar dituzte: premia, efikazia, proportzionaltasuna, segurtasun juridikoa, gardentasuna eta efizientzia.

Errege lege-dekretu hau telekomunikazioen eta segurtasun publikoaren araubide orokorraren arloan Estatuari Konstituzioaren 149. artikuluaren 1.21. eta 1.29. puntuen bidez esleitzen zaizkion ahalmen esklusiboak baliatuta ematen da.

Errege lege-dekretu hau legezko tresna da, Konstituzioaren araberakoa. Izan ere, Konstituzio Auzitegiak behin eta berriz eskatu bezala –otsailaren 4ko 6/1983 epaia, 5. oinarria; urtarrilaren 17ko 11/2002 epaia, 4. oinarria; uztailaren 3ko 137/2003 epaia, 3. oinarria, eta uztailaren 7ko 189/2005 epaia, 3. oinarria–, presako legegintza justifikatuta dago, baldin eta haren xedea egoera batean laguntza ematea bada eta hori Gobernuaren helburuetako bat bada eta aurreikusteko zailak diren arrazoi batzuk direla-eta berehala arautu behar bada, hau da, legeak Parlamentuan bide arruntetik edo presako prozeduraren bidez izapidetzeko behar dena baino epe laburragoan arautu behar bada.

Bestalde, kasu honetan, Konstituzio Auzitegiaren doktrinak justifikatzen du tresna juridiko hau –hau da, errege lege-dekretua– erabiltzea. Urtarrilaren 13ko 1/2012 epaian, zehazki, berresten du Konstituzioaren 86.1 artikuluan ezarritako aparteko eta presako beharrizanaren baldintza betetzat ematen duela zuzentarauen transposizioa atzeratzen denean.

Izatez, 2018ko maiatzaren 9an, jada iraungita dago Europako Parlamentuaren eta Kontseiluaren 2016ko uztailaren 6ko 2016/1148 (EB) Zuzentarauaren transposizio-epea. Zuzentarau horren transposizio-epea amaitu dela eta, Europako Batzordeak arau-hausteen prozedura formal bat abiarazi du (2018/168 zenbakikoa).

Horren ondorioz, errege lege-dekretu honetako neurri guztiek –oro har zein banan-banan hartuta–, haien izaera eta xedea ikusirik, bete egiten dute Konstituzioaren 86. artikuluak errege lege-dekretu bat onartu ahal izateko eskatzen duen aparteko eta presako beharrizanaren baldintza.

Horrenbestez, Espainiako Konstituzioaren 86. artikuluan jasotako baimena baliatuta, Gobernuko presidenteorde eta Presidentetzako, Gorteekiko Harremanetako eta Berdintasuneko ministroaren, Barne Arazoetako ministroaren eta Ekonomia eta Enpresako ministroaren proposamenari jarraikiz, Ministroen Kontseiluak 2018ko irailaren 7ko bileran eztabaidatu ondoren, honako hau

XEDATZEN DUT:

I. TITULUA

Xedapen orokorrak

1. artikulua. *Xedea.*

1. Honako hauek dira errege lege-dekretu honen xedeak: ezinbesteko zerbitzuak eta zerbitzu digitalak emateko erabiltzen diren informazio-sareen eta -sistemen segurtasuna arautzea eta intzidenteak jakinarazteko sistema bat ezartzea.
2. Halaber, esparru instituzional bat ezartzen da errege lege-dekretu hau aplikatzeko, agintari eskudunak koordinatzeko eta Europar Batasunaren esparruko lankidetza-organo nabarmenekiko koordinazio-lana egiteko.

2. artikulua. *Aplikazio-eremua.*

1. Zerbitzu hauei aplikatzen zaie errege lege-dekretu hau:

a) Informazio-sareen eta -sistemen mende dauden ezinbesteko zerbitzuak, apirilaren 28ko 8/2011 Legearen eranskinean zehaztuta dauden zerbitzu estrategikoetakoak (lege horrek azpiegitura kritikoak babesteko neurriak ezartzen ditu).
b) Honako zerbitzu digital hauek, 3 e) artikuluan zehaztuta dauden moduan: lineako merkatuak, lineako bilaketa-tresnak eta hodei-informatikako zerbitzuak.

2. Honako hauek daude errege lege-dekretu honen mende:

a) Espainian finkatuta dagoen ezinbesteko zerbitzuetako operadorea. Ezinbesteko zerbitzuetako operadore baten helbidea edo egoitza soziala Espainiako lurraldean badago, operadore hori Espainian finkatuta dagoela iritziko zaio, baldin eta bat bera badira helbide edo egoitza sozial hori eta kudeaketa administratiboa benetan egiten den eta negozioak edo jarduerak benetan zuzentzen diren tokia.
Era berean, operadore baten helbidea edo egoitza beste estatu batean baldin badago baina ezinbesteko zerbitzuak Espainian era iraunkorrean finkatutako establezimendu baten bitartez ematen baldin baditu operadore horrek, ezinbesteko zerbitzu horiei ere aplikatuko zaie errege lege-dekretu hau.
b) Honako baldintza hauek betetzen dituen zerbitzu digitalen hornitzailea: egoitza soziala Espainian izatea eta egoitza hori Europar Batasunean duen establezimendu nagusia izatea, edo Europar Batasunean ezarrita ez egon arren Europar Batasuneko ordezkaria Espainian izendatzea 2016/1148 (EB) Zuzentaraua betetze aldera (Europako Parlamentuaren eta Kontseiluaren 2016/1148 Zuzentaraua, 2016ko uztailaren 6koa, Europar Batasuneko informazio-sare eta sistema guztietan segurtasun handia eta berdina bermatzeko neurriei buruzkoa).

3. Honako hauek ez daude errege lege-dekretu honen mende:

a) Apirilaren 28ko 8/2011 Legean operadore kritiko gisa ezarrita ez dauden komunikazio elektronikoen sareen eta zerbitzuen operadoreak eta konfiantzako zerbitzu elektronikoen emaileak.
b) Zerbitzu digitalen hornitzaileak, Europako Batzordearen 2003/361/EB Gomendioan bildutako definizioekin bat etorrita mikroenpresak edo enpresa txikiak direnak (2003ko maiatzaren 6ko 2003/361/EB Gomendioa, mikroenpresei, enpresa txikiei eta enpresa ertainei buruzkoa).

3. artikulua *Definizioak.*

Honako definizio hauek ezartzen dira, errege lege-dekretu honen ondorioetarako:

a) Informazio-sare eta -sistema (honako elementu hauetako edozein):

1. Komunikazio elektronikoen sareak, Telekomunikazioen maiatzaren 9ko 9/2014 Lege Orokorraren II. eranskineko 31. apartatuan definitzen diren moduan.
2. Lotuta edo beren artean konektatuta dauden gailuak oro edo gailuen multzoa, baldin eta haietako batek edo batzuek programa baten bidez datu digitalak automatikoki tratatzen badituzte.
3. Aurreko 1. eta 2. zenbakietan aipatzen diren elementuen bidez biltegiratu, tratatu, berreskuratu edo igortzen diren datu digitalak, bai eta elementu horien funtzionamendurako, erabilerarako, babeserako edo mantentze-lanetarako behar direnak ere.

b) Informazio-sareen eta -sistemen segurtasun: informazio-sareen eta -sistemen gaitasuna, fidagarritasun-maila zehatzez aurre egitekoa datu biltegiratuen, igorrien edo tratatuen edo informazio-sare eta -sistema horiek ematen dituzten zerbitzuen edo haien bitartez eskuragarri dauden zerbitzuen erabilgarritasuna, benetakotasuna, osotasuna edo konfidentzialtasuna arriskuan jartzen dituen ekintza orori.

c) Ezinbesteko zerbitzu: oinarrizko gizarte-funtzioak, osasuna, segurtasuna, herritarren ongizatea eta ekonomia mantentzeko edo Estatuko eta administrazio publikoetako erakundeek modu eraginkorrean funtzionatzeko behar den zerbitzua, informazio-sareak eta -sistemak behar dituena emango bada.

d) Ezinbesteko zerbitzuen operadore: errege lege-dekretu honen 6. artikuluan ezarritako faktoreen arabera identifikatzen den erakunde publiko edo pribatua, zerbitzu horiek apirilaren 28ko 8/2011 Legearen eranskinean zehaztutako sektore estrategikoetako batean ematen dituena.

e) Zerbitzu digital: informazio-gizartearen zerbitzua, uztailaren 11ko 34/2002 Legearen eranskineko a) letran ezarritako zentzuan ulertua (34/2002 Legea, informazio-gizartearen eta merkataritza elektronikoaren zerbitzuei buruzkoa).

f) Zerbitzu digitalen hornitzaile: zerbitzu digital bat ematen duen pertsona juridikoa.

g) Arrisku: informazio-sareen eta -sistemen segurtasunean kalte eragin dezakeen inguruabar edo egitate oro, baldin eta era arrazoituan identifikatu ahal bada. Funtzionamenduan, pertsonen osotasun fisikoan edo materialean, irudian edo itxuran kalte egiteko mehatxu bat gauzatzeko probabilitate gisa kuantifikatu daiteke.

h) Intzidente: informazio-sareen eta -sistemen segurtasunari kalte egiten dion ezusteko edo nahi gabeko gertaera.

i) Intzidenteen kudeaketa: intzidenteak detektatzeko, aztertzeko, mugatzeko edo haiei erantzuteko erabiltzen diren prozedurak.

j) Ordezkari: Europar Batasunean ezarrita dagoen pertsona fisiko edo juridikoa, Europar Batasunean ezarrita ez dagoen zerbitzu digitalen hornitzaile batek espresuki izendatu duena, eta agintari eskudun nazionalek edo CSIRT taldeek, zerbitzu digitalen hornitzailearengana jo beharrean, berarengana jo ahal dutena, zerbitzu digitalen hornitzaile horrek errege lege-dekretu honen arabera bete behar dituen betebeharrei buruzko gaiak jorratzeko.

k) Arau tekniko: Europako Parlamentuaren eta Kontseiluaren 1025/2012 (EB) Erregelamenduaren 2.1 artikuluan ezarritakoaren araberako araua (2012ko urriaren 25eko 1025/2012 [EB] Erregelamendua, Europako normalizazioari buruzkoa).

l) Espezifikazio: espezifikazio teknikoa, Europako Parlamentuaren eta Kontseiluaren 1025/2012 (EB) Erregelamenduaren 2.4 artikuluan ezarritakoaren araberakoa (2012ko urriaren 25eko 1025/2012 [EB] Erregelamendua).

m) Interneteko truke-gune («IXP»; «*Internet eXchange Point*», ingelesezko izenaren arabera): sare-instalazio bat da, eta aukera ematen du bi sistema autonomo independente edo gehiago elkarrekin konektatzeko, batez ere Interneteko trafikoa arintzeko xedez; IXP baten bidez, sistema autonomoak elkarrekin konektatu ahal dira, eta ez da beharrezkoa bi

sistemaren arteko trafikoa hirugarren sistema autonomo batetik ere igarotzea, eta ez da aldatzen, ez eta oztopatzen ere, trafiko hori.

n) Domeinu-izenen sistema («DNS»; «*Domain Name System*», ingelesezko izenaren arabera): hierarkia baten arabera antolatuta dagoen sistema bat da, domeinu-izenei buruzko kontsultei erantzuten diena; batez ere, ordenagailuak edo gailuak Interneten kokatzeko eta helbideratzeko identifikatzaileei buruzko kontsultei erantzuten die.

o) DNS zerbitzuen hornitzaile: Interneten DNS zerbitzuak ematen dituen erakundea.

p) Lehen mailako domeinu-izenen erregistro: lehen mailako domeinu espezifiko batean Interneten domeinu-izenen erregistroa administratzen eta zuzentzen duen erakunde bat.

q) Lineako merkatu: zerbitzu digital bat da, kontsumitzaileei eta enpresaburuei aukera ematen diena salerosketa-kontratuak edo lineako zerbitzuak emateko kontratuak elkarrekin egin ditzaten, eta lineako merkatuaren zerbitzuaren webgune espezifiko batean gauzatu dezakete, edo lineako merkatuaren zerbitzuko hornitzaileak horretarako bereziki eman dituen informatika-zerbitzuak erabiltzen dituen enpresaburu baten webgunean; Kontsumitzaileak eta Erabiltzaileak defendatzeko Lege Orokorraren testu bateginak –azaroaren 16ko 1/2007 Legegintzako Errege Dekretuak onartzen duenak– hurrenez hurren 3. eta 4. artikuluetan ematen dituen definizioen arabera eta beste lege osagarri batzuetan jasotako definizioen arabera definitzen dira hemen kontsumitzaileak eta enpresaburuak.

r) Lineako bilaketa-tresna: zerbitzu digital bat da, erabiltzaileei aukera ematen diena, printzipioz, webgune guztietan edo hizkuntza zehatz bateko webguneetan bilaketak egiteko gai bati buruzko kontsultak eginez gako-hitz bat, gako-esaldi bat edo beste sarrera mota bat erabilita, eta eskatutako edukiei lotutako informazioa duten estekak erakusten dituena erantzunean.

s) Hodei-informatikako zerbitzu: zerbitzu digital horrek aukera ematen du partekatu daitezkeen baliabideak erabiltzeko; gainera, baliabide multzoa elastikoa da.

4. artikulua. *Europar Batasuneko gidalerroak eta orientabideak.*

Errege lege-dekretu hau aplikatzeko eta dekretuan ezarritako erregelamenduak eta gidak egiteko, honako hauek kontuan hartu beharko dira: 2016ko uztailaren 6ko Europako Parlamentuaren eta Kontseiluaren 2016/1148 (EB) Zuzentarauan ezarritako egikaritze-egintzak; zuzentarau horretako 11. artikuluan ezarritako kooperazio-taldeak eman dituen gomendio eta gidalerro guztiak, eta talde horrek eta CSIRT taldeen sareak bildu dituzten jardunbide egokien gaineko informazioa (CSIRT sarea zuzentarauaren 12. artikuluan araututa dago).

5. artikulua. *Funtsezko estatu-funtzioak babestea.*

Errege lege-dekretu honetan ezarritakoa ez da izango segurtasun nazionala eta ezinbesteko estatu-funtzioak babesteko hartzen diren neurrien kalterako. Besteak beste, honako neurri hauek sartzen dira hor: informazio sailkatua babesteko neurriak edo argitalpena Estatuaren interesen aurkakoa izateagatik argitaratu ezin den informazioa babestekoak; ordena publikoa zaintzeko ekintzak; delituak detektatzeko, ikertzeko eta haiei jazartzeko ekintzak, eta haien egileak epaitzekoak.

II. TITULUA

Ezinbesteko zerbitzuak eta zerbitzu digitalak

6. artikulua. *Ezinbesteko zerbitzuak eta ezinbesteko zerbitzuen operadoreak identifikatzea.*

1. Ezinbesteko zerbitzuak eta ezinbesteko zerbitzuen operadoreak apirilaren 28ko 8/2011 Legean ezarritako organoen eta prozeduren bidez identifikatuko dira, bai eta lege hori garatzeko araudietan ezarritakoen bidez ere.

Sektore bakoitzak ezinbesteko zerbitzuen eta ezinbesteko zerbitzuen operadoreen zerrenda eguneratuko du bi urtez behin, apirilaren 28ko 8/2011 Legean ezarritako sektore-plan estrategikoen berrikuspenarekin batera.

Operadore bat ezinbesteko zerbitzuen operadoretzat hartzeko, operadore horrek jasandako intzidente batek zerbitzua modu nabarmenean nahasteko modukoa izan behar du. Honako faktore hauek kontuan hartuko dira hori zehazteko:

a) Emandako zerbitzuaren garrantziari buruz:

1. Ematen den ezinbesteko zerbitzuak nahikoa izateari ez uzteko eskura dagoen aukera sorta.
2. Zerbitzu-hornikuntzan intzidente batek izan dezakeen eraginaren balorazioa –intzidenteak norainoko eragina duen edo zer eremu geografikotan duen ebaluatu beharko da–; entitateak ematen duen ezinbesteko zerbitzuarekiko beste sektore estrategiko batzuek duten mendekotasuna, eta intzidenteak jarduera ekonomiko eta sozialetan edo segurtasun publikoan dituen ondorioen tamaina eta iraupena.

b) Ebaluatu den entitatearen bezeroei buruz:

1. Entitateak ematen dituen zerbitzuen erabiltzaileen kopurua.
2. Merkatu-kuota.

Intzidente batek perturbazio nabarmenak eragin ditzakeen zehazte aldera, sektoreko faktore espezifikoak gehitu ahalko dira, erregelamendu bidez.

2. Apirilaren 28ko 8/2011 Legea betez izendatutako operadore kritikoei dagokienez, dena delako ezinbesteko zerbitzua emateko informazio-sareen eta -sistemen mende daudela egiaztatu baino ez dute egin behar horiek.
3. Ezinbesteko zerbitzuak eta ezinbesteko zerbitzuen operadoreak identifikatzeko, lankidetza-taldeak horri lotuta ematen dituen gomendioei ahalik eta gehien jarraitu beharko zaie.
4. Ezinbesteko zerbitzuen operadore batek Europar Batasuneko beste estatu batzuei zerbitzuak ematen dizkienean, operadore hori ezinbesteko zerbitzuen operadore gisa identifikatzeko asmoa jakinaraziko zaie estatu horietako harreman-gune bakarrei.

7. artikulua. *Zerbitzu digitalen hornitzaileen jarduera jakinaraztea.*

2. artikuluan aipatutako zerbitzu digitalen hornitzaileek beren jardueraren berri eman beharko diete agintari eskudunei, hiru hilabeteko epean, jarduerari ekiten diotenetik zenbatuta, jakinaren gainean egoteko besterik ez bada.

III. TITULUA

Esparru estrategikoa eta instituzionala

8. artikulua. *Informazio-sareen eta -sistemen segurtasunaren esparru estrategikoa.*

Zibersegurtasun Nazionalaren Estrategian, Segurtasun Nazionalaren Estrategiarekin bat etorrita eta haren babespean, helburuak eta neurriak ezartzen dira informazio-sareetan eta -sistemetan segurtasun handia lortzeko eta segurtasun horri eusteko.

Zibersegurtasun Nazionalaren Estrategiak, besteak beste, 2016/1148 (EB) Zuzentarauaren 7. artikuluan ezarritako gaiei heldu beharko die (2016/1148 [EB] Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko uztailaren 6koa).

Ondorio horietarako, Segurtasun Nazionalerako Kontseiluak Zibersegurtasun Nazionalaren Estrategia berrikustea bultzatuko du, 36/2015 Legearen 21.1 e) artikuluan ezarritakoarekin bat etorrita (36/2015 Legea, irailaren 28koa, Segurtasun Nazionalarena).

9. artikulua. *Agintari eskudunak.*

1. Honako hauek dira informazio-sareen eta -sistemen segurtasunaren arloko agintari eskudunak:

a) Ezinbesteko zerbitzuen operadoreentzat:

1. Apirilaren 28ko 8/2011 Legean eta haren garapen-araudietan ezarritakoarekin bat etorrita, operadore kritiko izendatuta dauden operadoreak direnean, zer sektore estrategikotan izendatuta dauden alde batera utzita: Barne Arazoetako Ministerioko Segurtasunerako Estatu Idazkaritza, Azpiegiturak Babesteko eta Zibersegurtasuneko Zentro Nazionalaren bitartez (CNPIC).
2. Operadore kritikoak ez direnean: gaiaren arabera eskuduna den agintari sektoriala, erregelamendu bidez ezarritakoari jarraikiz.

b) Zerbitzu digitalen hornitzaileentzat: Ekonomia eta Enpresako Ministerioko Aurrerapen Digitalerako Estatu Idazkaritza.
c) Operadore kritikoak ez izan arren 40/2015 Legearen aplikazio-eremuan dauden ezinbesteko zerbitzuen operadoreentzat eta zerbitzu digitalen hornitzaileentzat (40/2015 Legea, urriaren 1ekoa, Sektore Publikoaren Araubide Juridikoarena): Defentsa Ministerioa, Zentro Kriptologiko Nazionalaren bidez.

2. Segurtasun Nazionalerako Kontseiluak, zibersegurtasunaren arloko batzorde espezializatuaren bidez, agintari eskudunak koordinatzeko behar diren mekanismoak ezarriko ditu.

10. artikulua. *Agintari eskudunen eginkizunak*.

Honako eginkizun hauek beteko dituzte agintari eskudunek:

a) Ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek betebeharrak betetzen dituzten gainbegiratzea, VI. tituluan ezarritakoarekin bat etorrita.
b) Komunikazio-kanal egokiak ezartzea ezinbesteko zerbitzuen operadoreekin eta zerbitzu digitalen hornitzaileekin; hala dagokionean, erregelamendu bidez garatuko dira.
c) Erreferentziako CSIRT taldeekin jardun-protokoloen bidez koordinatzea; hala dagokionean, protokolook erregelamendu bidez garatuko dira.
d) Errege lege-dekretu honen esparruan CSIRT taldeen bidez aurkezten diren intzidenteen gaineko jakinarazpenak jasotzea, V. tituluan ezarritakoarekin bat etorrita.
e) Harreman-gune bakarrari errege lege-dekretu honen esparruan aurkezten diren intzidenteen gaineko jakinarazpenen berri ematea, 27. artikuluan ezarritakoarekin bat etorrita.
f) Herritarrei intzidente zehatz batzuen gaineko informazioa jakinaraztea, baldin eta informazio hori beharrezkoa bada intzidente bati aurrea hartzeko edo jada gertatu den intzidente bat kudeatzeko, 26. artikuluan ezarritakoarekin bat etorrita betiere.
g) Datu pertsonalen babesaren, segurtasun publikoaren, herritarren segurtasunaren eta segurtasun nazionalaren arloetako agintari eskudunekin elkarlanean jardutea errege lege-dekretu honen aplikazio-eremuan, bai eta dagokien agintari sektorialekin ere, 14. eta 29. artikuluetan ezarritakoarekin bat etorrita.
h) Betebehar espezifikoak ezartzea informazio-sareen eta -sistemen segurtasuna bermatzeko eta intzidenteak jakinarazteko, eta jarraibide teknikoak eta orientazio-gidak ematea, betebehar horien edukia zehazteko, 16. eta 19. artikuluetan ezarritakoarekin bat etorrita betiere.
i) Zehapen-ahala baliatzea errege lege-dekretu honetan aurreikusitako kasuetan, VII. tituluan ezarritakoarekin bat etorrita.
j) Arauen eta espezifikazio teknikoen erabilera sustatzea, 17. artikuluan ezarritakoarekin bat etorrita.

k) Europar Batasuneko beste estatu batzuetako agintari eskudunekin batera jardutea, ezinbesteko zerbitzuen operadoreak identifikatzeko ezinbesteko zerbitzuak zenbait estatu kidetan eskaintzen dituzten entitateen artean.

l) Harreman-gune bakarrari beste estatu kide batzuei eragin diezaieketen intzidenteen berri ematea, 25. artikuluan ezarritakoarekin bat etorrita.

11. artikulua. *Informatika-segurtasunaren arloko intzidenteei erantzuteko erreferentzia-taldeak.*

1. Informazio-sareen eta -sistemen segurtasunaren arloan, honako hauek dira segurtasunaren arloko intzidenteei erantzuna emateko erreferentzia-taldeak (CSIRT):

a) Ezinbesteko zerbitzuen operadoreekiko harremanen arloan:

1. Zentro Kriptologiko Nazionalaren CCN-CERTi dagokio urriaren 1eko 40/2015 Legearen aplikazio-eremu subjektiboko erakundeek osatzen duten erreferentzia-komunitatea.

2. Espainiako Zibersegurtasuneko Institutu Nazionalaren INCIBE-CERTi dagokio urriaren 1eko 40/2015 Legearen aplikazio-eremu subjektibokoak ez diren erakundeek osatzen duten erreferentzia-komunitatea.

INCIBEk eta CNPICk jardungo dute INCIBE-CERTen, batera, operadore kritikoei eragiten dieten intzidenteen kudeaketaren gaineko gai guztietan.

3. ESPDEF-CERT, Defentsa Ministeriokoa, zeinak CCN-CERTekin eta INCIBE-CERTekin lankidetzan jardungo baitu, baldin eta CCN-CERTek eta INCIBE-CERTek errefortzua behar badute ezinbesteko zerbitzuen operadoreei eta, bereziki, Defentsa Nazionalean eragina duten eta erregelamendu bidez zehazten diren operadoreei laguntzeko.

b) CCN-CERTeko erreferentzia-komunitatekoak ez diren zerbitzu digitalen hornitzaileekiko harremanen arloan: INCIBE-CERT.

INCIBE-CERT, halaber, herritarrentzat, zuzenbide pribatuko entitateentzat eta 1. atal honetan sartuta ez dauden beste entitate batzuentzat izango da erantzun-taldea erreferentzia-intzidenteak gertatzen direnean.

2. Erreferentziakoak diren CSIRT taldeak elkarrekin koordinatuko dira, eta gainerako CSIRT nazionalekin eta nazioartekoekin ere bai, haiei dagozkien segurtasun arloko intzidenteei erantzuna emateko eta segurtasun-arriskuak kudeatzeko. Biziki larriak diren kasuetan, erregelamendu bidez zehazten diren eta egoera arruntetan baino koordinazio handiagoa behar duten horietan, CCN-CERTek egingo du CSIRT taldeen erantzun teknikoaren koordinazio-lan nazionala.

Beren jarduerek operadore bati nolabait eragin ahal badiote, erreferentziako CSIRT taldeak Barne Arazoetako Ministerioarekin koordinatuko dira, Azpiegiturak babesteko eta Zibersegurtasuneko Zentro Nazionaleko (CNPIC) Koordinazio Zibernetikoko Bulegoaren bitartez, erregelamenduz zehazten den moduan.

12. artikulua. *Erreferentziako CSIRT taldeen eskakizunak eta eginkizunak.*

1. CSIRT taldeek honako baldintza hauek bete behar dituzte:

a) Komunikazio-zerbitzuen erabilgarritasuna handia dela bermatu behar dute, ustekabeko hutsegiterik gerta ez dadin; eta modu bat baino gehiago eduki behar dute une oro beraiekin harremanetan jartzeko, bai eta beraiek beste batzuekin harremanetan jartzeko ere. Gainera, komunikazio-kanalek argi zehaztuta egon behar dute, eta erabiltzaile-taldeek eta bazkide laguntzaileek ondo ezagutu beharko dituzte.

b) Haien instalazioek eta laguntzako informazio-sistemek leku seguruetan jarrita egon behar dute.

c) Jardueren jarraitutasuna bermatu behar dute. Horretarako:

1. Eskaerak kudeatzeko eta bideratzeko, sistema egokia edukiko dute, transferentziak egitea errazagoa izan dadin.
2. Une oro erabilgarri egoteko, behar diren beste langile eduki beharko dituzte.
3. Jarraitutasuna bermatua duten komunikazio-azpiegiturak erabiltzeko aukera izango dute. Horretarako, sistema erredundanteak eta lan egiteko erreserba-guneak eduki behar dituzte.

d) Nazioarteko lankidetza-sareetan parte hartzeko gaitasuna eduki beharko dute, horretan parte hartu nahi izanez gero.

2. Gutxienez honako eginkizun hauek beteko dituzte CSIRT taldeek:

a) Intzidenteak eremu nazionalean gainbegiratzea.
b) Arriskuei eta intzidenteei buruzko alerta goiztiarrak, alertak, abisuak eta informazioa hedatzea interesdunei.
c) Intzidenteei erantzuna ematea.
d) Arriskuen eta intzidenteen gaineko azterketa dinamikoa egitea, bai eta egoeraren gainekoa ere, hura ezagutzeko.
e) CSIRT taldeen sarean parte hartzea.

3. CSIRT taldeek lankidetza-harremanak ezarriko dituzte sektore pribatuarekin. Lankidetza errazagoa izan dadin, CSIRT taldeek jardunbide berak edo normalizatuak erabiltzea sustatu behar dute honako hauetan:

a) Intzidenteak eta arriskuak kudeatzeko prozedurak.
b) Intzidenteak, arriskuak eta informazioa sailkatzeko sistemak.

13. artikulua. *Harreman-gune bakarra.*

Segurtasun Nazionalerako Kontseiluak, Segurtasun Nazionaleko Sailaren bitartez, lotura-eginkizuna bete behar du 9. artikuluaren arabera izendatu diren agintari eskudunen eta Europar Batasuneko beste estatu batzuetako agintari eskudunen arteko mugaz haraindiko lankidetza bermatzeko, bai eta lankidetza-taldearekiko eta CSIRT taldearekiko lankidetza bermatzeko ere.

14. artikulua. *Informazio-segurtasunaren arloan eskumenak dituzten beste agintari batzuekin eta agintari sektorialekin lankidetzan jardutea.*

1. Agintari eskudunek, erreferentziako CSIRTek eta harreman-gune bakarrak, hala dagokionean, kontsulta egingo diete segurtasun nazionalaren, segurtasun publikoaren, herritarren segurtasunaren eta datu pertsonalen babesaren arloko eskumenak dituzten organoei, eta lankidetzan jardungo dute haiekin, beren eginkizunak betetzeko.
2. Hala dagokionean, gaiaren arabera, errege lege-dekretu honen aplikazio-eremuko sektore bakoitzean eskumenak dituzten organoei kontsulta egingo diete, eta lankidetzan jardungo dute haiekin, beren eginkizunak betetzeko.
3. Jakinarazten diren intzidenteak delitu izan daitezkeenean, agintari eskudunek eta erreferentziako CSIRTek Fiskaltzari emango diote horren berri, Barne Arazoetako Ministerioko Koordinazio Zibernetikoko Bulegoaren bitartez, dagozkion ondorioak sor ditzan. Horri buruz duten informazio guztia eman beharko diote.

15. artikulua. *Isilpeko informazioaren konfidentzialtasuna.*

5. artikuluan ezarritakoa alde batera utzi gabe, agintari eskudunek, erreferentziako CSIRTek eta harreman-gune bakarrak ezinbesteko zerbitzuen operadoreen eta zerbitzu digitalen hornitzaileen segurtasuna eta merkataritza-interesak zaindu behar dituzte, Zuzenbidean ezarritako moduan. Halaber, errege lege-dekretu honetan agintzen zaizkien

eginkizunak betetzean operadoreok eta hornitzaileok ematen dizkieten datuen konfidentzialtasuna zaindu behar dute.

Isilpeko informazioa elkarri eman behar diotenean, trukearen xedea betetzeko beharrezkoa dena baino ez diote emango elkarri, eta bere neurrian.

IV. TITULUA

Segurtasunaren arloko betebeharrak

16. artikulua. *Ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek segurtasunaren arloan bete behar dituzten betebeharrak.*

1. Ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek neurri tekniko eta antolaketa-neurri egokiak hartu behar dituzte, eta neurrian, errege lege-dekretu honen mendeko zerbitzuak emateko erabiltzen dituzten informazio-sare eta -sistemetako segurtasun-arriskuak kudeatzeko.

V. tituluan ezartzen den intzidenteak jakinarazteko betebeharra alde batera utzi gabe, neurri egokiak hartu behar dituzte berei eragiten dieten intzidenteei aurrea hartzeko eta eragina ahalik eta gehien murrizteko.

2. Errege lege-dekretu honen erregelamenduzko garapenean, behar diren neurriak bilduko dira ezinbesteko zerbitzuen operadoreek aurreko apartatuan agintzen dena bete dezaten.

3. Ezinbesteko zerbitzuen operadoreek informazioaren segurtasunaren arloko arduradun izendatuko dute pertsona bat, unitate bat edo kide anitzeko organo bat, agintari eskudunekiko harremanetarako eta haiekiko koordinazio-lan teknikoa egin dezan, eta erregelamendu bidez ezarritako epean jakinaraziko diete izendapen hori agintari eskudunei.

Haren eginkizun espezifikoak erregelamendu bidez ezarriko dira.

4. Agintari eskudunek, ministerio-agindu baten bitartez, betebehar espezifikoak ezarri ahalko dituzte ezinbesteko zerbitzuen operadoreek erabiltzen dituzten informazio-sareen eta -sistemen segurtasuna bermatzeko. Era berean, jarraibide teknikoak eta orientazio-gidak eman ahalko dituzte agindu horien edukia zehazteko.

Erregelamenduzko xedapenak, jarraibideak eta gidak egiten direnean, kontuan hartuko dira betebehar sektorialak, lankidetza-taldean erabakitzen diren gidalerro egokiak eta informazio-segurtasunaren arloko eskakizunak: beste manu batzuen arabera operadoreak bete behar dituztenak. Beste manu horiek, besteak beste, hauek izan daitezke: apirilaren 28ko 8/2011 Legea eta Segurtasun Eskema Nazionala, urtarrilaren 8ko 3/2010 Errege Dekretuak onartua.

5. Agintari eskudunek elkarrekin koordinatuta jardun behar dute, bai eta gaiaren arabera eskudunak diren organo sektorialekin ere, beren eskumenen eremuetan ematen dituzten aginduen, jarraibide teknikoen eta orientazio-giden edukiari eta aplikazioari dagokienez. Horren xedea bikoiztasunik ez gertatzea eta ezinbesteko zerbitzuen operadoreek aginduak, jarraibide teknikoak eta orientazio-gidak betetzen laguntzea da.

6. Zerbitzu digitalen hornitzaileek zehaztu behar dute zer segurtasun-neurri aplikatuko dituzten. Honako aurrerapen tekniko eta alderdi hauek kontuan hartuko dituzte, gutxienez:

a) Sistemen eta instalazioen segurtasuna.
b) Intzidenteen kudeaketa.
c) Jardueren jarraitutasunaren kudeaketa.
d) Gainbegiratzea, auditoriak egitea eta probak egitea.
e) Nazioarteko arauak betetzea.

Horrez gain, Europar Batasunak alderdi horiek egikaritze-egintzen bidez zehazten baditu, zerbitzu digitalen hornitzaileek egintza horiek ere bete behar dituzte.

17. artikulua. *Arau teknikoak.*

Agintari eskudunek 1025/2012 (EB) Erregelamenduaren esparruan informazio-sareen eta -sistemen segurtasunaren arloan ematen diren erregulazio, arau edota espezifikazio teknikoen erabilera sustatuko dute (1025/2012 [EB] Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2012ko urriaren 25ekoa, Europako Normalizazioari buruzkoa).

Arau edo espezifikazio horiek eman ez badira, normalizaziorako nazioarteko erakundeek onartu dituzten arauak edo gomendioak aplikatzea sustatuko dute, eta, hala dagokionean, Europan edo nazioartean gai honi buruz onartu diren arauak edota espezifikazio teknikoak.

18. artikulua. *Araudi espezifiko baliokidea duten sektoreak.*

Nazioko edo Europar Batasuneko araudi batek informazio-sareen eta -sistemen segurtasunaren arloko betebeharrak edo intzidenteak jakinarazteko betebeharrak ezartzen badizkio sektore bati, eta betebehar horien ondorioak eta errege lege-dekretu honetan ezarritako betebeharrenak parekoak badira behintzat, nazioko edo EBko eskakizunak eta gainbegiratze-mekanismoak izango dira jarraitu beharrekoak.

Horrek, ordea, ez die eragingo agintari eskudunen arteko lankidetza-betebeharrari, Segurtasun Nazionalerako Kontseiluaren koordinazioari, ez eta, legeria sektorialarekin bateraezina izan ezean, V. titulua (intzidenteak jakinarazteari buruzkoa) aplikatzeari ere.

V. TITULUA

Intzidenteak jakinaraztea

19. artikulua. *Intzidenteak jakinarazteko betebeharra.*

1. Ezinbesteko zerbitzuen operadoreek, erreferentziako CSIRTaren bidez, intzidenteak jakinaraziko dizkiete agintari eskudunei, baldin eta intzidenteok zerbitzu horiei perturbazio nabarmenak ekarri ahal badizkiete.

Erregelamenduz ezarritakoari jarraikiz, ezinbesteko zerbitzuak emateko erabiltzen diren informazio-sareei edo -sistemei eragin diezaieketen gertaeren edo gorabeheren gaineko jakinarazpenak ere egingo dira, nahiz eta gertaera edo gorabehera horiek oraindik ere ez duten perturbaziorik ekarri.

2. Zerbitzu digitalen hornitzaileek, erreferentziako CSIRTaren bidez, intzidenteak jakinaraziko dizkiete agintari eskudunei, baldin eta intzidenteok zerbitzu horiei perturbazio nabarmenak ekarri ahal badizkiete.

Zerbitzu digitalen hornitzaileak intzidente baten eragina baloratzeko behar den informazioa lortu ahal duenean baino ez du bete behar intzidentea jakinarazteko betebeharra.

3. Aipatutako zerbitzuak emateko erabilitako informazio-sareei eta -sistemei eragiten dieten intzidenteei buruzkoak izango dira ezinbesteko zerbitzuen operadoreen eta zerbitzu digitalen hornitzaileen jakinarazpenak, bai sare eta zerbitzu horiek berezko sareak eta zerbitzuak direnean, bai kanpoko hornitzaileenak direnean, bai eta hornitzaile horiek errege lege-dekretu honen mendeko zerbitzu digitalen hornitzaileak direnean ere.

4. Agintari eskudunek eta erreferentziako CSIRTek plataforma komun bat erabiliko dute, intzidenteak jakinarazteko, komunikatzeko eta haien gaineko informazioa emateko prozesuak arintzeko eta automatizatzeko.

5. Errege lege-dekretu honen erregelamenduzko garapenean, behar diren neurriak ezarri beharko dira ezinbesteko zerbitzuen operadoreek artikulu honetan ezarritakoa bete dezaten. Agintari eskudunek, ministerio-agindu baten bitartez, ezinbesteko zerbitzuen operadoreen jakinarazpen-betebehar espezifikoak ezarri ahalko dituzte. Era berean, jarraibide teknikoak eta orientazio-gidak eman ahalko dituzte, agindu horien edukia zehazteko.

Erregelamenduzko xedapenak, jarraibideak eta gidak egiten direnean, kontuan hartuko dira betebehar sektorialak, lankidetza-taldean erabakitzen diren gidalerro nabarmenenak eta intzidenteen jakinarazpenaren arloko eskakizunak, operadoreak beste manu batzuen arabera bete beharrekoak. Beste manu horiek hauek izan daitezke, besteak beste: apirilaren 28ko 8/2011 Legea, eta Segurtasun Eskema Nazionala, urtarrilaren 8ko 3/2010 Errege Dekretuaren bidez onartua.

6. Aurreko apartatuetan ezarritako jakinarazpen-betebeharra gorabehera, delitu izan daitezkeen egitateak agintari eskudunen aurrean salatu beharko dira, legezko betebeharrei jarraikiz, eta, betiere, Prozedura Kriminalaren Legearen 259. artikuluan eta hurrengoetan eta errege lege-dekretu honen 14.3 artikuluan ezarritakoarekin bat etorrita.

20. artikulua. *Jakinarazpena egiten duena babestea.*

1. Titulu honetan aipatzen diren jakinarazpenek ez diote erantzukizun handiagorik ezarriko erakunde jakinarazleari.

2. Edozein lan- edo merkataritza-harreman edukita ere, ezinbesteko zerbitzuak edo zerbitzu digitalak ematen dituzten enplegatuek eta langileek, intzidenteen gaineko informazioa ematen baldin badute, ezin izango dute ondorio kaltegarririk jaso beren lanpostuan edo enpresan, fede gaiztoan jardun direla egiaztatu ezean.

Langileek apartatu honetan ezarritakoari jarraikiz jardun arren enplegu-emaileak langile horien eskubideen kalterako erabakiak hartzen baldin baditu, erabakiok deusez izango dira, eta ez dute lege-ondoriorik edukiko.

21. artikulua. *Intzidente baten ondorioen garrantzia zehazteko faktoreak.*

1. 19.1 artikuluko lehen paragrafoan aipatzen diren jakinarazpenen ondorioetarako, intzidente baten garrantzia zehazte aldera, gutxienez honako faktore hauek kontuan hartuko dira:

a) Ezinbesteko zerbitzuaren perturbazioak zenbat erabiltzaileri eragin dion.
b) Intzidenteak zenbat iraun duen.
c) Intzidenteak noraino edo zer eremu geografikotan izan duen eragina.
d) Zerbitzuaren funtzionamendua zenbateraino nahasi duen.
e) Jarduera ekonomiko eta sozial erabakigarrietan zenbateraino eragin duen.
f) Intzidenteak eragin dien sistemek edo informazioak zenbaterainoko garrantzia duten ezinbesteko zerbitzua eman ahal izateko.
g) Ospeari zenbaterainoko kaltea egin dion.

2. 19.2 artikuluan aipatzen diren jakinarazpenak direnean, intzidente baten garrantzia zehazteko, 2016/1148 (EB) Zuzentarauaren 16. artikuluko 8. eta 9. apartatuetan ezarritako egikaritze-egintzetan ezarritakoari jarraituko zaio (2016/1148 [EB] Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2016ko uztailaren 6koa).

22. artikulua. *Hasierako jakinarazpena, tarteko jakinarazpenak eta amaierako jakinarazpenak.*

1. Ezinbesteko zerbitzuen operadoreek bidegabeko atzerapenik gabe egin beharko dute intzidenteen hasierako jakinarazpena, 19.1 artikuluan ezarritakoari jarraikiz.

Intzidenteak mugaz haraindi izan dezakeen edozein ondorio zehazteko bidea ematen duten datu guztiak bilduko dira jakinarazpenean, besteak beste.

2. Ezinbesteko zerbitzuen operadoreek tarteko jakinarazpenak egingo dituzte, baldin eta hasierako jakinarazpenean sartutako informazioa eguneratzeko eta intzidentearen bilakaerari buruz informatzeko beharrezko irizten badiete, intzidentea konpondu bitartean.

3. Ezinbesteko zerbitzuen operadoreek amaierako jakinarazpena bidaliko dute intzidentea konpondu eta gero.

Intzidenteak eragin dien informazio-sare eta -sistema guztiak berrezarrita daudenean eta zerbitzua normal dabilenean esan ahal izango da intzidentea konpondu dela.

23. artikulua. *Jakinarazpena egiteko epeak betetzeko malgutasuna.*

Ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek, eragin dieten intzidenteen gaineko komunikazioetan, aipatu gabe utzi ahalko dituzte intzidenteek ezinbesteko zerbitzuetan edo zerbitzu horien mende dauden beste batzuetan izandako ondorioei buruzko informazioa edo beste informazio batzuk, oraindik eskuragarri ez badituzte. Dena den, informazio hori, eskuratu bezain laster, agintari eskudunei bidali beharko diete.

Intzidentearen gaineko hasierako jakinarazpena egin zenetik behar baino denbora gehiago igaro baldin bada eta ezinbesteko zerbitzuen operadoreak edo zerbitzu digitalen hornitzaileak informazio egokia bildu ezin izan badu, txosten bat bidaliko die agintari eskudunei berandu gabe, informazio hori biltzeko zer neurri hartu dituen eta zergatik ezin izan duen bildu azaltzeko.

24. artikulua. *Zerbitzu digitalei eragiten dieten intzidenteak.*

Espainian ematen diren zerbitzu digitalei nabarmen eragin dien intzidente baten berri izaten baldin badute, eta zerbitzuok Europar Batasuneko beste estatu batean ezarrita dagoen beste hornitzaile batek ematen baditu, errege lege-dekretu honen mende dauden ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek, bai eta interesa duen edozein alderdik ere, jakinaren gainean jarri ahalko dituzte agintari eskudunak, dagokion informazioa emanda, beste hornitzaile hori ezarrita dagoen estatuarekiko lankidetza errazteko.

Era berean, operadoreak eta hornitzaileak jakitun badira hornitzaile horrek ez dituela bete segurtasun-eskakizunak edo Espainian gertatutako intzidenteak jakinarazteko dagozkion betekizunak, agintari eskudunari jakinarazi ahalko diote, dagokion informazioa emanda.

25. artikulua. *Mugaz haraindiko eragina duten intzidenteak izapidetzea.*

1. Agintari eskudunek edo erreferentziako CSIRTek, Europar Batasuneko beste estatu batzuei eragin ahal dieten intzidenteen berri baldin badute, harreman-gune bakarraren bidez emango diete horren berri estatu horiei, eta zehaztu egingo dute intzidenteak perturbazio nabarmenik ekarri ahal dien estatu horietan ematen diren ezinbesteko zerbitzuei.

2. Europar Batasuneko beste herrialde batzuetan jakinarazi diren intzidenteen berri jasotzen bada harreman-gune horren bidez, eta intzidenteok perturbazio nabarmenak ekarri ahal badizkie Espainian ematen diren ezinbesteko zerbitzuei, informazio garrantzitsua emango zaie agintari eskudunei eta erreferentziako CSIRTari, behar diren neurriak har ditzan nork bere alorrean.

3. Aurreko apartatuetan azaldu diren jarduketak gorabehera, agintari eskudunek edo erreferentziako CSIRTek informazioa trukatu ahalko dute zuzenean Europar Batasuneko beste estatu batzuetako homologoekin alderdi biei interesatzen zaizkien intzidenteei buruz.

26. artikulua. *Jendeari jakinaraztea*

1. Agintari eskudunek ezinbesteko zerbitzuen operadoreei edo zerbitzu digitalen hornitzaileei eskatu ahalko diete herritarrei edo interesa eduki dezaketen hirugarren pertsonei informazioa eman diezaieten, baldin eta informazio hori ezagutzea beharrezkoa bada intzidente gehiago ez gertatzeko edo jada gertatu direnak kudeatzeko, edo interes publikoaren onerako bada intzidentearen gaineko informazioa zabaltzea.

2. Agintari eskudunek erabaki ahalko dute herritarrei edo hirugarren pertsonei zuzenean ematea intzidentearen berri.

Hala denean, herritarrei informazioa zabaldu aurretik, agintari eskudunek kontsulta egingo diote ezinbesteko zerbitzuen operadoreari edo zerbitzu digitalen hornitzaileari, eta harekin koordinatuko dira.

27. artikulua. *Harreman-gune bakarrari eta lankidetza-taldeari urtero eman behar zaien informazioa.*

1. Agintari eskudunek urteko txosten bat bidaliko diote harreman-gune bakarrari, honako hauek azalduko dituena: zenbat intzidente jakinarazi dituzten, zer motatakoak izan diren, emandako zerbitzuetan edo beste zerbitzu batzuetan zer ondorio izan dituzten, eta estatu barrukoak izan diren edo mugaz haraindikoak izan diren, betiere Europar Batasunaren barrualdean.

Agintari eskudunek, txosten hori egiteko, harreman-gune bakarrak eman dituen jarraibideak beteko dituzte, eta igorri behar den informazioaren formatuari eta edukiari buruz lankidetza-taldeak eman dituen oharrak kontuan hartuko dituzte.

2. Harreman-gune bakarrak urte bakoitzeko abuztuaren 9a baino lehen txosten laburtu bat bidaliko dio lankidetza-taldeari, jasotako jakinarazpenei buruz. Gero, agintari eskudunei eta erreferentziako CSIRTei ere bidaliko die, informazio hori ezagut dezaten.

28. artikulua. *Intzidenteak konpontzeko, informazioa emateko eta lankidetzan jarduteko betebeharra*

1. Ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek konpondu egin behar dituzte berei eragiten dieten segurtasun-intzidenteak, eta beren kabuz ezin badituzte konpondu, laguntza espezializatua eskatu beharko dute, erreferentziako CSIRTaren laguntza ere barne.

Hala denean, erreferentziako CSIRTak egindako oharrei jarraitu beharko diete intzidentea konpontzeko, ondorioak murrizteko edo kaltetutako sistemak berrezartzeko.

2. Errege lege-dekretu honek agintzen dizkien eginkizunak betetzeko eskatzen zaien informazio guztia eman beharko diete ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek erreferentziako CSIRTari eta agintari eskudunei.

Zehazki, ezinbesteko zerbitzuen operadoreei eta zerbitzu digitalen hornitzaileei informazio osagarria eskatu ahalko diete jakinarazitako intzidenteen ezaugarriak, arrazoiak eta ondorioak aztertzeko, estatistikak egiteko eta 27. artikuluan ezarritako urteko txostenak egiteko behar diren datuak biltzeko.

Ahal denean, agintari eskudunek edo erreferentziako CSIRTak intzidenteen jarraipenaren ondorioz bildu duten informazioa emango diete intzidenteen eragina jasan duten ezinbesteko zerbitzuen operadoreei edota zerbitzu digitalen hornitzaileei, baldin eta haientzat garrantzitsua izan badaiteke bereziki intzidentea konpontzeko.

29. artikulua. *Datu pertsonalei eragiten dieten intzidenteetan lankidetzan jardutea*

Agintari eskudunek eta erreferentziako CSIRTek Datuak Babesteko Espainiako Bulegoarekin lankidetzan jardungo dute, hertsiki, datu pertsonalak urratzea dakarten intzidenteei aurre egiteko.

Agintari eskudunek eta erreferentziako CSIRTek Datuak Babesteko Espainiako Bulegoari berehala emango diote datu pertsonalak urratzea ekar dezaketen intzidenteen berri; halaber, intzidente horien bilakaera jakinarazi beharko diote.

30. artikulua. *Datu pertsonalak lagatzeko baimena.*

Intzidenteak jakinarazteko, kudeatzeko, aztertzeko edo konpontzeko datu pertsonalak eman behar badira, bidezkoak, egokiak eta beharrezkoak diren datuak baino gehiago ez dira tratatuko, adierazitako xedeetako zein lortu nahi den kontuan hartuta.

Honako kasu hauetan egongo da baimenduta datu pertsonalak xede horietarako lagatzea:

a) Ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek agintari eskudunei lagatzen dizkietenean erreferentziako CSIRTen bitartez.

b) Erreferentziako CSIRTek agintari eskudunei lagatzen dizkietenean, eta alderantziz.

c) Erreferentziako CSIRTen artean, eta horien eta Europar Batasuneko beste estatu batzuetan izendatutako CSIRTen artean.

d) Erreferentziako CSIRTen eta nazioko zein nazioarteko beste CSIRT batzuen artean.

e) Harreman-gune bakarraren eta Europar Batasuneko beste estatu batzuetako harreman-gune bakarren artean.

31. artikulua. *Borondatezko jakinarazpenak.*

1. Ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek intzidenteak jakinarazi ahalko dituzte, nahiz eta jakinarazteko betebeharrik ez egon.

Era berean, ezinbesteko zerbitzuak ematen dituzten erakundeek, nahiz eta ezinbesteko zerbitzuen operadore gisa edo zerbitzu digitalen hornitzaile gisa identifikatuta ez egon, zerbitzu horiei eragiten dieten intzidenteak jakinarazi ahalko dituzte.

Jakinarazpen hori egiten duen erakundea behartuta dago intzidentea konpontzera, 28. artikuluan ezarritakoarekin bat etorrita.

2. Aurreko apartatuan aipatzen diren jakinarazpenak titulu honek arautzen ditu, eta 27.1 artikuluan ezarritako urteko txostenean emango zaio jakinarazpen horien berri harreman-gune bakarrari.

3. CSIRTek eta agintari eskudunek, jakinarazpenak kudeatzen dituztenean, borondatezko jakinarazpenei baino lehentasun handiagoa emango diete nahitaezko jakinarazpenei.

VI. TITULUA

Gainbegiratzea

32. artikulua. *Ezinbesteko zerbitzuen operadoreak gainbegiratzea.*

1. Agintari eskudunek informazio-sareen eta -sistemen segurtasuna ebaluatzeko behar duten informazio guztia eskatu ahalko diete ezinbesteko zerbitzuen operadoreei, segurtasunaren arloko politiken gaineko dokumentazioa ere bai.

Segurtasunaren arloko politika benetan aplikatu izanari buruzko informazioa eskatu ahalko diete operadoreei, eta auditoria egin ahalko diete, edota haiek behartu kanpoko erakunde fidagarri eta independente batek informazio-sareen eta -sistemen segurtasuna ikuskatu dezan.

2. Bildutako informazioa kontuan hartuta, agintari eskudunek operadoreari eskatu ahalko diote aurkitutako hutsuneak zuzendu ditzan, bai eta nola zuzendu adierazi ere.

33. artikulua. *Zerbitzu digitalen hornitzaileak gainbegiratzea.*

1. Zerbitzu digitalak gainbegiratzeko agintari eskudunek ez-betetze baten berri dutenean gainbegiratuko dute errege lege-dekretu honen ondoriozko betebeharrak betetzen diren, eta eskaera arrazoitu bat edo salaketa bat jasotzen dutenean ere bai.

Halakoetan, informazio-sareak eta -sistemak ebaluatzeko behar duten informazio guztia eskatu ahalko diote agintari eskudunek zerbitzu digitalen hornitzaileari, bai eta segurtasunaren arloko politiken gaineko agiriak ere. Horrez gain, hutsuneak zuzentzeko eskatu ahalko diote.

2. Agintari eskudunak behar diren gainbegiratze-neurriak hartuko ditu, jakitun badira Espainian ezarritako hornitzaileek beste estatu kide batzuetan ematen dituzten zerbitzu digitalei perturbazio nabarmena eragiten dieten intzidenteak gertatu direla.

Horretarako, beste estatu kide batzuetako agintari eskudunek emandako informazioari erreparatuko diote bereziki.

34. artikulua. *Mugaz haraindiko lankidetza.*

1. Zerbitzua emateko erabiltzen diren informazio-sareak eta -sistemak, ezinbesteko zerbitzuen operadorea, zerbitzu digitalen hornitzailea edo beraren ordezkaria ezarrita dauden estatu kideetako agintari eskudunekin elkarlanean egingo da gainbegiratzeko jarduna, beharrezkoa denean.

2. Agintari eskudunek beste estatu kide batzuetako agintari eskudunekin elkarlanean jardungo dute, baldin eta lankidetza eskatzen badiete gainbegiratze-lana egiteko eta ezinbesteko zerbitzuen operadoreek eta zerbitzu digitalen hornitzaileek neurriak har ditzaten Espainian ezarrita dauden informazio-sareei eta -sistemei buruz, bai eta Espainian ezarrita dauden zerbitzu digitalen hornitzaileei dagokienez ere, edo Europar Batasunean duten eta bizilekua edo egoitza soziala Espainian duen ordezkari baten bitartez jarduten duten hornitzaileei dagokienez.

VII. TITULUA

Zehapen-araubidea

35. artikulua. *Erantzuleak.*

Errege lege-dekretu honen aplikazio-eremukoak diren ezinbesteko zerbitzuen operadoreak eta zerbitzu digitalen hornitzaileak erantzuleak izango dira.

36. artikulua. *Arau-hausteak.*

1. Errege lege-dekretu honetan ezarritako arau-hausteak oso astunak, astunak edota arinak izan daitezke.

2. Arau-hauste oso astunak:

a) Hutsuneak detektatu eta ezinbesteko zerbitzuen operadoreak edo zerbitzu digitalen hornitzaileak haiek zuzentzeko neurririk ez hartzea, 32.2 edo 33.1 artikuluetan ezarritakoarekin bat etorrita, baldin eta hutsuneok zerbitzuan perturbazio nabarmenak eragiteko arriskua ekarri badiete eta agintari eskudunek intzidentea gertatu aurretik eman zizkieten aginduak bete gabe utzi badituzte.

b) Zerbitzuari perturbazio nabarmenak ekartzen dizkioten intzidenteak jakinarazteko betebeharra behin eta berriro ez betetzea. Betebeharrari uko egiten dion bigarren alditik aurrera iritziko zaio behin eta berriro ari zaiola uko egiten.

c) 28.1 artikuluan ezarritakoarekin bat etorrita intzidenteak konpontzeko behar diren neurriak ez hartzea, baldin eta intzidenteok Espainian edo beste estatu kide batzuetan ezarritako ezinbesteko zerbitzuetan edo zerbitzu digitaletan perturbazio nabarmena eragiten badute.

3. Arau-hauste astunak:

a) Informazio-sareen eta -sistemen segurtasuna bermatzeko bete behar dituzten gutxieneko ardurei buruz agintari eskudunek ematen dituzten erregelamenduzko xedapenak edo segurtasunaren arloko jarraibide teknikoak ez betetzea ezinbesteko zerbitzuen operadoreek.

b) 32.2 edo 33.1 artikuluekin bat etorrita egin den errekerimendu bat jasotzea, detektatu diren hutsuneak zuzentzeko, eta neurririk ez hartzea, eta hura erantzunik eman ez zaion hirugarren errekerimendua izatea azken bost urteetan.

c) Zerbitzuari perturbazio nabarmenak dakarzkioten intzidenteak jakinarazteko betebeharra ez betetzea.

d) Jakinarazi diren eta perturbazio nabarmenak dakartzaten intzidenteak konpontzeko batere interesik ez adieraztea, baldin eta zerbitzua horren ondorioz gehiago degradatzen bada.

e) Betetzen dituen estandarrei edo indarrean dituen segurtasun-ziurtagiriei buruzko informazio faltsua edo engainagarria ematea.
f) Agintari eskudunen auditoretza oztopatzea.

4. Arau-hauste arinak dira:

a) Errege lege-dekretu honen babespean agintari eskudunak ematen dituen erregelamenduzko xedapenak edo segurtasunaren arloko jarraibide teknikoak ez betetzea, hori arau-hauste astuna ez denean.
b) 32.2 o 33.1 artikuluen araberako errekerimendu bat jaso arren, detektatu diren hutsuneak zuzentzeko neurririk ez hartzea.
c) Agintari eskudunek segurtasunaren arloko politikei buruz eskatzen dioten informazioa ez ematea, edo informazio osatu gabea ematea edo berandu ematea, justifikaziorik gabe.
d) Agintari eskudunek agindutakoaren araberako segurtasun-auditoria ez egitea.
e) Erreferentziako CSIRTari edo agintari eskudunei 28.2 artikuluari jarraituz eskatzen dioten informazioa ez ematea.
f) 19.2 artikuluaren bigarren paragrafoarekin bat etorrita jakinarazi behar diren gertakari edo gorabeherak ez jakinaraztea, horiek zerbitzuetan benetako eragin kaltegarririk ez izan arren.
g) Intzidenteak jakinarazteko eman behar den informazioa ez osatzea 23. artikuluaren arabera, edo informazio hori biltzeko ezintasuna azaltzeko txostena, artikulu horretan bertan ezarria, ez bidaltzea.
h) Intzidente bat konpontzeko erreferentziako CSIRTak egin dituen oharrei ez jarraitzea, 28. artikuluak agintzen duenaz bestera.

37. artikulua. *Zehapenak.*

1. Aurreko artikuluan azaldu diren arau-hausteengatik, honako zehapen hauek ezarriko dira:

a) Arau-hauste oso astunak direnean: 500.001 eta 1.000.000 euro bitarteko isuna.
b) Arau-hauste astunak direnean: 100.001 eta 500.000 euro bitarteko isuna.
b) Arau-hauste arinak direnean: kargu-hartzea edo 100.000 euro arteko isuna.

2. Arau-hauste astunengatik edo oso astunengatik administrazio-bidean irmo ezartzen diren zehapenak *Estatuko Aldizkari Ofizial*ean argitaratu ahalko dira, bai eta agintari eskudunaren webgunean ere, zehatuaren kontura, gertatu denari erreparatuta eta hurrengo artikuluarekin bat etorrita.

38. artikulua. *Zehapenen zenbatekoa mailakatzea.*

Honako irizpide hauek kontuan hartuko ditu zehapen-organoak, zehapena ezartzeko:

a) Erruduntasuna zenbaterainokoa den edo intentzionalitaterik egon den.
b) Araua hausteko joera jarraitua edota iraunkorra den.
c) Zer-nolako kalteak eta zenbatekoak sortu diren.
d) Berrerori den, azken urtean izaera bereko arau-hauste bat baino gehiago eginda eta ebazpen irmo batek hala deklaratuta administrazio-bidean.
e) Zenbat erabiltzaileri eragin dien.
f) Erantzulearen fakturazioa zenbatekoa den.
g) Erantzuleak sariak emateko programak erabiltzen dituen bere informazio-sareetan eta -sistemetan ahuleziak atzemateagatik.
h) Erantzuleak arau-haustearen ondorioak edo eragina arintzeko zer neurri hartu dituen.

39. artikulua. *Zehapenen proportzionaltasuna.*

1. Zehapen-organoak eskala baten arabera ezarri ahalko du zehapenaren zenbatekoa; dagokion kasuaren larritasuna kontuan hartu, eta larritasun horren aurre-aurretik dagoen arau-hauste motaren eskala aplikatu ahalko du honako kasu hauetan:

a) Inputatuaren erruduntasuna nabarmen jaitsi dela uste denean, 38. artikuluan adierazitako zenbait irizpide nabarmenki erabiltzearen ondorioz.
b) Erakunde arau-hausleak bere egoera irregularra modu arretatsuan erregularizatu duenean.
c) Arau-hausleak bat-batean bere erruduntasuna aitortzen duenean.

2. Zehapen-eskumena duten erakundeek, egitatearen izaera kontuan hartuta eta aurreko apartatuan ezarritako irizpide esanguratsurik baden aztertuta, zehapen-prozedura ez abiaraztea erabaki ahal izango dute, eta, horren ordez, subjektu erantzuleari ohartarazpena egitea, kasu bakoitzean dagozkion neurri zuzentzaileak hartu dituela froga dezan zehapen-organoak zehazten duen epean. Horretarako, honako aurrebaldintza hauek bete behar dira:

a) Egitateak arau-hauste arinak edo astunak izatea errege lege-dekretu honetan xedatutakoaren arabera.
b) Organo eskudunak arau-hausleari aurreko bi urteetan zehapenik jarri edo ohartarazpenik egin ez izana errege lege-dekretu honetako arau-hausteak egiteagatik.

Arau-hausleak ohartarazpena zehapen-organoak zehaztutako epean aintzat hartzen ez badu, dagokion zehapen-prozedura abiaraziko da, ez-betetze horrengatik.
3. 36.4 artikuluaren c), d) eta e) letretan azaltzen diren arau-hauste arinengatik eta 36.3 artikuluaren e) letran azaltzen den arau-hauste larriarengatik ezin izango da ohartarazpenik egin.

40. artikulua. *Administrazio publikoen arau-hausteak.*

1. 36. artikuluan aipatzen diren arau-hausteak administrazio publikoetako organoek edo erakundeek egiten dituztenean, zehapen-organoak ebazpen bat emango du, eta arau-haustearen ondorioak amaitzeko edo zuzentzeko hartu behar diren neurriak bertan ezarriko ditu. Ebazpen hori organo edo erakunde arau-hausleari jakinarazi beharko zaio, bai eta kaltetuei ere, halakorik dagoenean.
Horrekin guztiarekin batera, zehapen-organoak diziplina-jarduketei ekitea ere proposatu ahalko du, hala dagokionean.
2. Aurreko apartatuan aipatu diren neurrien eta jardunen inguruan emandako ebazpenak komunikatu beharko zaizkio zehapen-organoari.

41. artikulua. *Zehatzeko eskumena*

1. Arau-hauste oso astunak direnean, 9. artikuluan ezarritakoaren arabera eskuduna den ministroak ezarriko ditu zehapenak; arau-hauste astunak edo arinak direnean, errege lege-dekretu hau garatzeko erregelamenduaren bidez zehazten den agintari eskudunak ezarriko ditu zehapenak.
2. Zehatzeko ahala gauzatzeko, urriaren 1eko 39/2015 Legean eta urriaren 1eko 40/2015 Legean ezarritako printzipioak eta prozedurak beteko dira (39/2015 Legea, Administrazio Publikoen Administrazio Prozedura Erkidearena; 40/2015 Legea, Sektore Publikoaren Araubide Juridikoarena).
3. Zehatzeko ahala baliatzean, administrazio publikoen jardunari orokorrean aplikatzen zaion prozedura erabiliko da. Hala ere, prozedurak urtebete iraungo du gehienez ere; eta alegazioen epea ez da hilabetetik beherakoa izango.

42. artikulua. *Arau-hausteak batera gertatzea.*

1. Ezin izango da errege lege-dekretu honetan ezarritakoaren araberako zehapenik jarri, arau-haustetzat jotzen diren egitateak zerbitzuaren emaileak bete behar duen araudi sektorialean ere arau-haustetzat jotzen badira eta ondasun juridiko babestua bat bera bada.

2. Beste lege batzuetan tipifikatuta dauden arau-hausteak izan daitezkeen egitateen berri jakiten baldin bada zehapen-jarduera baten ondorioz, egitate horien berri emango zaie egitateok gainbegiratzeko eta zehatzeko eskumena duten organoei edo erakundeei.

Lehen xedapen gehigarria. *Ezinbesteko zerbitzuen eta ezinbesteko zerbitzuen operadoreen hasierako zerrenda.*

Azpiegitura Kritikoak Babesteko Batzorde Nazionalak ezinbesteko zerbitzuen hasierako zerrenda onartuko du errege lege-dekretu honen aplikazio-eremuko sektoreetan, eta zerbitzu horiek ematen dituzten eta errege lege-dekretu hau bete behar duten operadoreak identifikatuko ditu, honako hurrenkera honetan:

a) 2018ko azaroaren 9a baino lehen: energiaren, garraioen, osasunaren, finantza-sistemaren, uraren eta azpiegitura digitalen arloetako sektore estrategikoei dagozkien ezinbesteko zerbitzuak eta operadoreak.

b) 2019ko azaroaren 9a baino lehen: apirilaren 28ko 8/2011 Legearen eranskinean bilduta dauden gainerako sektore estrategikoei dagozkien ezinbesteko zerbitzuak eta operadoreak.

Bigarren xedapen gehigarria. *Komunikazio elektronikoak eta konfiantzako zerbitzuak.*

Apirilaren 28ko 8/2011 Legearen arabera operadore kritiko izendatzen diren sareen, komunikazio elektronikoen eta zerbitzu elektronikoen operadoreei errege lege-dekretu hau aplikatzea ez da eragozpena izango segurtasunaren arloan haiei dagokien araudi espezifikoa ere aplikatzeko.

Ekonomia eta Enpresa Ministerioak, araudi hori aplikatzeko organo eskuduna izanik, eta Barne Arazoetako Ministerioak koordinatuta jardungo dute, operadore kritikoek bete behar dituzten betebeharrak ezartzeko. Halaber, informazioa trukatuko dute, trabarik gabe, eragiten dieten intzidenteei buruz.

Hirugarren xedapen gehigarria. *Errege lege-dekretu honetan ezarritako plataforma komunaren bidez jakinaraztea datu pertsonalen segurtasuna urratutako kasuak.*

Errege lege-dekretu honetan ezartzen den intzidenteak jakinarazteko plataforma komuna datu pertsonalen segurtasuna urratutako kasuak jakinarazteko erabili ahalko da, Europako Parlamentuaren eta Kontseiluaren 2016/679 (EB) Erregelamenduarekin bat etorrita (2016/679 [EB] Erregelamendua, apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituena eta 95/46/EE Zuzentaraua indargabetzen duena), Datuak Babesteko Espainiako Agentziak eta plataforma hori kudeatzen duten organoek erabakitzen dituzten baldintzei jarraikiz.

Laugarren xedapen gehigarria. *Zerbitzu digitalen egungo hornitzaileak.*

Aurrez ere zerbitzu digitalak ematen zituzten hornitzaileek beren jardueraren berri eman beharko diote Ekonomia eta Enpresa Ministerioko Aurrerapen Digitalerako Estatu Idazkaritzari. Hori egiteko, hiru hilabete dituzte errege lege-dekretu hau indarrean sartzen denetik.

Azken xedapenetako lehenengoa. *Eskumen-titulua.*

Errege lege-dekretu hau ematen da telekomunikazioen eta segurtasun publikoaren araubide orokorraren arloan Estatuari Konstituzioaren 149. artikuluaren 1.21 eta 1.29 puntuen bidez esleitzen zaizkion eskumen esklusiboak baliatuta.

Azken xedapenetako bigarrena. *Europar Batasuneko zuzenbidea txertatzea.*

Errege lege-dekretu honen bidez, Espainiako Estatuaren ordenamendu juridikora egokitzen da Europako Parlamentuaren eta Kontseiluaren 2016/1148 (EB) Zuzentaraua, 2016ko uztailaren 6koa, Europar Batasuneko informazio-sare eta -sistema guztietan segurtasun handia eta berdina bermatzeko neurriei buruzkoa.

Azken xedapenetako hirugarrena. *Erregelamendua garatzeko baimena.*

Gobernuari baimena ematen zaio errege lege-dekretu honetan ezarritakoa gara dezan, alde batera utzi gabe ministroek betebehar espezifikoak ezartzeko eskumena dutela ministro-aginduen bidez, arau honen artikuluetan hala ezarritako kasuetan.

Azken xedapenetako laugarrena. *Indarrean jartzea.*

Errege lege-dekretu hau *Estatuko Aldizkari Ofizial*ean argitaratu eta hurrengo egunean jarriko da indarrean.

Madril, 2018ko irailaren 7a

FELIPE E.

Gobernuko presidentea,
PEDRO SÁNCHEZ PÉREZ-CASTEJÓN