Euskal Autonomia Erkidegoko Administrazio Publikoaren

Informazioaren Segurtasuna

Kudeatzeko Sistema

Informazioaren Segurtasun eta Pribatutasun Politika

Honek onartua *Aprobado por*	Segurtasun eta pribatutasun Korporatiboko Batzordea	***Erreferentzia*** *Referencia*	Informazioaren segurtasun eta pribatutasun politika
Data *Fecha*	2023-01-25	***Jasotzaileak*** *Distribución*	Langile guztiak

Dokumentu honen jabea Eusko Jaurlaritza da eta, bere edukia, barnekoa. Eusko Jaurlaritzako langileen artean besterik ezin da zabaldu, ezin zaio zabalkunde publikorik eman eta ezin da erabili sortu zenerako helburuetatik at dauden bestelako helburuekin. Hirugarren batzuei ematen bazaie, emateko baldintzak betez besterik ezin izango da erabili. Eusko Jaurlaritzari ezin izango zaio leporatu dokumentu honen argitalpenean egiten den akatsik edo hutsegiterik.

Este documento es propiedad de Eusko Jaurlaritza – Gobierno Vasco y su contenido es interno. Su difusión debe limitarse al personal de Eusko Jaurlaritza – Gobierno Vasco, no debiendo ser difundido públicamente ni utilizado para otros propósitos que los que han originado su creación. En el caso de ser facilitado a terceros su utilización deberá limitarse exclusivamente a las condiciones bajo las cuales ha sido facilitado. Eusko Jaurlaritza – Gobierno Vasco no podrá ser considerado responsable de eventuales errores u omisiones en la edición del documento.

SEGURTASUN-SAILKAPENA / CLASIFICACIÓN DE SEGURIDAD									
Erabilgarritasuna Disponibilidad	TXIKIA	Osotasuna Integridad	TXIKIA	Konfidentzialtasuna Confidencialidad	TXIKIA	Benetakotasuna Autenticidad	TXIKIA	Trazabilitatea Trazabilidad	TXIKIA

Bertsioen kontrola

Bertsioa	Data	Aldaketa aurreko bertsioarekin alderatuta	Nork egina	Nork berrikusia	Nork onartua
v.1	2020/11/17	Hasierako bertsioa	Segurtasuneko bulego teknikoa	Segurtasun Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboko Batzordea
v.2	2023/xx/xx	Arau-aldaketak, sistemen arduradunarekin lotutako argibideak eta 3.7 atalean gidalerroak sartzea.	Segurtasuneko bulego teknikoa	Segurtasun Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboko Batzordea

Edukia

1. Sarrera

Segurtasun-eskema nazionalak (ENS) bere 11. artikuluan eta II. eranskineko org.1 neurrian dioenez, «***informazioaren segurtasun-politika formalki xedatu behar da***»; ezarrita dagoenez, politika hori goi mailako organo eskudunaren titularrak onetsi behar du, eta honako hau jaso behar da:

- Erakundearen helburuak edo egitekoa
- Jarduerak egiteko legezko eta arauzko esparrua
- Segurtasun-rol edo -eginkizunak. Horietako bakoitzerako karguaren betebehar eta erantzukizunak definituko dira, baita karguak izendatzeko eta berritzeko prozedura ere
- Segurtasun eta pribatutasuna kudeatu eta koordinatzeko batzordeen egitura. Halakoen erantzukizun-esparrua, kideak eta erakundeko beste elementu batzuekiko harremana zehaztu behar dira
- Sistemaren segurtasuneko agiriak egituratzeko, kudeatzeko eta eskuratzeko gidalerroak

UNE-ISO/IEC 27001 arauak, 5.2 zenbakian, segurtasun-politika bat eskura egon behar dela azaltzen du.

Informazioaren segurtasun-politika horrek erantzukizunak identifikatu behar ditu, baita IKT informazioaren eta komunikazioaren teknologien bidez kudeatutako informazio-zerbitzuak eta aktiboak behar bezala babesteko printzipioak eta gidalerroak ezarri ere.

Informazioaren segurtasun eta pribatutasun-politika da EAEko Administrazio Orokorrak eta haren erakunde autonomoek euren helburuak betetzeko erabiltzen duten tresna, informazioaren eta komunikazioaren sistemak modu seguruan erabilita. **Segurtasuna**ren barruan, segurtasuna prozesu integral gisa hartuta, informazioaren eta komunikazioen sistemekin zerikusia duten giza elementuak zein elementu materialak eta antolaketako elementuak sartzen dira. Segurtasuna ez da produktu gisa hartu behar, baizik eta **egokitzeko eta hobetzeko etengabeko prozesu** gisa. Prozesu hori, hain zuzen ere, kontrolatu, kudeatu eta monitorizatu egin behar da, Eusko Jaurlaritzan segurtasunaren kultura ezarriz.

1.1 *Segurtasun et pribatutasunari buruzko araudia garatzea*

Informazioaren segurtasunari buruzko araudia nahitaez bete beharrezkoa da, eta mailaz maila garatuko da, aplikazio-eremuaren eta zehaztasun teknikoko mailaren arabera; hala, arau bakoitzaren oinarria goragoko maila duten arauak izango dira. Garapen-maila horiek honako hauek dira:

#	Maila	Azalpena
1	Informazioaren segurtasun **politika**	Agiri honek osatzen du, eta nahitaez bete beharrekoa da.
2	Segurtasun-**arauak**: informazioaren segurtasunaren arloko jarraibideak, ekintza-planak eta jarduketa estrategikoak	Modu egokian nahiz inguruabarren bat prozedura esplizituren batean jasota ez dagoenean nola jardun behar den adierazteko erabiliko diren agiriak. Segurtasun-politika garatzen duten eta aipatu politikaren aplikazioa hizpide duten arauak dira. Arau bakoitzak honako hau bete beharko du: a) Lortu nahi diren helburuak ardatz hartu, horiek lortzeko modua baino lehen. Zalantzak daudenean, arauek erabaki zuzena hartzen laguntzen dute. b) Erabilera zuzentzat jotzen dena deskribatu, baita erabilera okertzat jotzen dena ere. c) Kasuan kasuko arloan garatu diren segurtasun-prozedurak lokalizatzeko modua adierazi. d) Laburra, arrazoitua eta deskribatzailea izan, eta interpretazio zuzena egiteko harreman-puntuak definitu. e) Ohiz kanpoko eta aurreikusi gabeko egoeretan nola jokatu behar den azaldu. f) Langileen erantzukizuna azaltzea, araua bete edo urratzeari dagokionez: eskubideak, betebeharrak eta diziplinazko neurriak, indarrean dagoen legeriaren arabera.
3	**Segurtasun eta pribatutasun-prozedurak**	Kontuan hartu behar diren izaera teknikoko edo prozedura-izaerako gidalerroen arabera, jarduera jakin bat nola egin modu esplizituan eta urratsez urrats azaltzen duten agiriak. Honako hau zehaztu beharko du prozedura bakoitzak: a) Zer baldintzatan aplikatu behar den b) Nork gauzatu behar duten c) Une bakoitzean zer egin behar den, hala badagokio, egindako jardueraren erregistroa barne hartuz d) Emaitzak nola neurtzen eta ebaluatzen diren e) Nola jorratzen diren prozeduretan jaso daitezkeen hobekuntzak eta gabeziak
4	Beste agiri batzuk	Aipatu agiriez gain, segurtasun eta pribatutasun-agiriek beste agiri gehigarri batzuk izan ditzakete; esaterako: gomendioak, jardunbide egokiak, txostenak, erregistroak eta nabaritasun elektronikoak.

2. Segurtasun eta pribatutasun-printzipioak

EAEko Administrazio Orokorraren eta haren erakunde autonomoen informazioaren segurtasun eta pribatutasun-politika, orokorrean, honako printzipioen arabera garatuko da:

#	Printzipioa	Azalpena
1	**Segurtasun integrala**	Sistemarekin zerikusia duten giza elementu eta antolaketa-elementu guztiek eta elementu tekniko eta material guztiek (aldian aldiko jarduketaren bat edo egoeraren araberako tratamenduren bat baztertuta) osatutako prozesu integral gisa ulertuko da segurtasuna. Prozesuan parte hartzen duten pertsonen kontzientziazioari eta horien hierarkia-arduradunei arretarik handiena jarriko zaie, ezjakintasuna, antolamendurik eta koordinaziorik eza eta jarraibide desegokiak segurtasunerako eta pribatutasunerako arrisku izan ez daitezen. Informazioaren segurtasun eta pribatutasun-errekerimenduei aktiboen bizi-ziklo osoan zehar emango zaie erantzuna, plangintzatik hasita kendu arte.
2	**Arriskuaren kudeaketa**	Informazioaren segurtasun eta pribatutasuna kudeatzea arriskuak aztertzean, segurtasun-neurri egokiak, eraginkorrak eta proportzionatuak ezartzean eta etengabeko zuzenketa eta hobekuntza barne hartzean datza; hala, erakundea segurtasun-gorabeheren aurrean gero eta prebentiboagoa izango da, erreaktiboa baino, eta ingurunea kontrolatuta egongo da. Arriskuak maila onargarrietara arte minimizatu behar dira eta segurtasun-neurrien eta informazioaren izaeraren arteko oreka bilatu behar da. Arriskuen azterketa eta kudeaketa segurtasun eta pribatutasun-prozesuaren funtsezko partea izango da eta une oro eguneratuta egon beharko da.
3	**Eskuragarritasuna, jarraitutasuna eta kontserbazioa**	Aktiboak eskuragarri egon daitezen ahalegindu behar da, horiek eskuratzeko baimendutako pertsonek eskatzen dituztenean. Horretarako, zerbitzuak etenik gabe emango direla eta jazo daitezkeen gertakizunen aurrean berehala lehengoratuko direla bermatuko da, zerbitzuak eta lotutako informazioa lehengoratzeko jarraitutasun-neurrien bidez. Halaber, datuak eta informazioak euskarri elektronikoan kontserbatzea bermatuko da. Era berean, sistemak eskuragarri mantenduko ditu zerbitzuak informazio digitalaren bizi-ziklo osoan; horretarako, ondare digitala iraunarazteko oinarri izango diren kontzeptu eta prozedurak erabiliko dira.
4	**Osotasuna**	Lan egiteko baliatzen den informazioa osoa eta zehatza dela bermatu beharko da eta informazio horren edukia eta tarteko prozesuena zehatzak izan behar direla azpimarratuko da.
5	**Konfidentzialtasuna**	Aktiboak horiek lortzeko berariazko baimena dutenek bakarrik eskura ditzaketela bermatu beharko da.
6	**Benetakotasuna**	Informazioa mintzaide egokiarekin trukatzen dela eta zerbitzuak behar bezala egiaztatzen direla bermatu beharko da.

#	Printzipioa	Azalpena
7	**Trazabilitatea**	Informazioaren eta hori eskatzen duten zerbitzuen inguruan egindako eragiketen jarraipena bermatu beharko da.
8	**Prebentzioa, erreakzioa eta lehengoratzea**	Segurtasun eta pribatutasunari lotutako iruzurrak, ez-betetzeak edo gorabeherak saihesteko lanerako plan eta ildoak garatuko dira berariaz. Sistemaren segurtasunak prebentzioaren, antzematearen eta zuzenketaren alderdiak jorratu behar ditu, horren gaineko mehatxuak gauza ez daitezen eta esku arteko informazioari edo ematen diren zerbitzuei larriki eragin ez diezaien. Prebentziorako neurriek sistemaren kalterako diren mehatxuak gauzatzeko arriskua ezabatu behar dute edo behintzat murriztu, besteak beste disuasioa eta esposizioaren murrizketa kontuan hartuta. Detekzio-neurriak erreakzio-neurriei erantsiko zaizkie, segurtasun-gorabeherak garaiz konpontzeko. Lehengoratzeko neurriek informazioa eta zerbitzuak berreskuratzeko aukera emango dute, segurtasun edo pribatutasun-gorabehera batek ohiko bideak desgaitzen dituen egoerei aurre egiteko.
9	**Mailaketa**	Sistemek babeserako estrategia bat eduki behar dute defentsa-lerroetan. Estrategia hori hainbat segurtasun-geruzak osatu behar du, eta geruza horiek modu jakin batean antolatuta egon behar dute. Hala, geruzetako batek huts eginez gero: a) Denbora irabazi ahal da eragotzi ezin izan diren gorabeheren aurrean erreakzio egokia izateko b) Sistema osorik arriskuan jartzeko aukera murriztu ahal da c) Azkenean sistemaren gaineko eragina murriztu ahal da Antolaketa-, fisika- eta logika-izaerako neurriek osatu behar dituzte defentsa-lerroak.
10	**Etengabeko hobekuntza eta aldizkako berrebaluazioa**	Behin eta berriz berrikusiko da erakundeak arriskuen eta ingurune teknologikoaren etengabeko bilakaerari egokitzeko ahalmena handitzeko ezarri dituen segurtasun eta pribatutasun-kontrolen eraginkortasuna. Segurtasun-neurriak aldian-aldian berrebaluatu eta eguneratuko dira, neurri horien eraginkortasuna arriskuen eta babeserako sistemen etengabeko bilakaerara egokitzeko; are gehiago, beharrezkoa bada, segurtasuna bera birplanteatuko da.
11	**Proportzionaltasuna kostuari dagokionez**	Aktiboen segurtasun-arriskuak arinduko dituzten neurrien ezarpena horretarako aurreikusitako aurrekontu-esparruaren barruan egin beharko da eta segurtasun-neurrien, informazioaren izaeraren eta aurreikusitako aurrekontuaren arteko oreka bilatu beharko da.
12	**Kontzientziazioa eta prestakuntza**	Erabiltzaileentzako informazioaren segurtasun eta pribatutasunaren arloko prestakuntza-, sentsibilizazio- eta kontzientziazio-programak artikulatuko dira, politika korporatiboetan behar bezala oinarrituta eta jarraipen- eta eguneratze-prozesu egokiarekin.

#	Printzipioa	Azalpena
13	**Eginkizun bereizia**	Segurtasuna eginkizun bereizitzat jotzeko legezko eskakizunari jarraikiz, informazio-sistemen segurtasuna, administrazioan, zerbitzuak ematearen gaineko erantzukizunetik desberdinduko da. Segurtasun eta pribatutasun-politikak arduradun bakoitzaren eskumenak eta gatazkak koordinatu eta ebazteko mekanismoak zehaztuko ditu.
14	**Arauak betetzea**	Informazio-sistema guztiak, baita lotutako edozein prozesu ere, informazio-segurtasun eta pribatutasunari eragiten dion legearen araberako aplikazio arauemaile eta sektorialera egokituko dira; bereziki, intimitatearekin eta izaera pertsonaleko datuen babesarekin eta sistemen, datuen, komunikazioen eta zerbitzu elektronikoen segurtasunarekin zerikusia duen hori, teknologiaren bidez herritarrei eta administrazio publikoei eskubideak baliatzeko eta betebeharrak betetzeko aukera ematen diena.

3. Gidalerroak

EAEko Administrazio Orokorraren eta haren erakunde autonomoen informazioaren segurtasun eta pribatutasun-politika hurrengo ataletan garatzen da.

3.1 *Eusko Jaurlaritzaren helburua*

Eusko Jaurlaritzaren egitekoa da **Administrazio berritzailea eta irekia** sortzea, gizarteari **kalitatezko** zerbitzuak, efizienteak, **eraginkorrak eta seguruak** emango dizkiona, ingurunearekin elkarlanean eta herritarren **parte-hartze aktiboa** aintzat hartuta; hau da, **pertsonak** izango dira **aldaketaren protagonista**. Hori guztia, gainera, **gobernantza-balio** berriak oinarri hartuta egingo da, hots, irekia izatea, emaitzetara bideratutako orientazioa, gardentasuna eta berrikuntza.

Helburu hori lortzeko, bere jardueraren oinarria Informazio Sistemak (IS) dira. Sistema horiek prestutasunez administratu behar dira, segurtasun-neurri egokiak hartuta, eskuragarritasun, benetakotasun, osotasun, konfidentzialtasun eta trazabilitate bermeak arriskuan jar ditzaketen ezbeharrezko edo nahita egindako kalteetatik babesteko.

Egiteko hori betetzearekin modu estuan lotuta, garrantzitsua da honako hau azpimarratzea: informazioaren eta komunikazioaren teknologien —aurrerantzean, IKTen— azpiegiturak lehenetsi egin behar ditu jokamolde irekiak, funtzionaltasuna, konektagarritasuna eta erabiltzailearentzako zerbitzua xede dituena, helburu estrategiko eta instituzionalak lortzeko lehentasunezko eginkizunekin.

Alde horretan, IKTak maila estrategiko handiko tresna dira, ahalmena dutelako Administrazio Orokorraren eta haren erakunde autonomoen modernizazioa bultzatzeko, eta gai direlako Euskadiren garapen sozial eta ekonomikoa pizteko eta garapen horri eusteko. Beraz, ezinbestekoa da IKT sistemak prestutasunez administratzea, baita neurri egokiak hartzea ere sistema horiek azkar eboluzionatzen duten mehatxuen aurka babesteko, mehatu horiek eragina izan ahal baitute lehenago aipatu diren berme edo dimentsio horietan.

3.2 *Araudia*

Euskal Autonomia Erkidegoko Administrazio Orokorraren eta haren erakunde autonomoen jardueren araudi-esparrua, informazioaren segurtasun eta pribatutasun-politikaren esparru horretan, honako arau hauek osatzen dute:

#	Araua	Eguna	Azalpena	Xedea
1	**15/1999 Legea**	Abenduaren 13a	Datu pertsonalak babesteari buruzkoa 3/20185 Legeak indargabetu du,22,23 eta 24 artikuluak izan ezik.	Segurtasun-neurrien eta babestu beharreko informazioaren arteko proportzionaltasuna ezartzeko irizpideak ekartzen ditu
2	**1720/2007 ED**	Abenduaren 21a	DBLO garatzeko erregelamendua onartzen duena	Datu Pertsonalak Babesteko 15/1999 Lege Organikoaren edukia garatu eta osatzen du.
3	**34/2002 Legea**	Uztailaren 11a	Informazioaren gizartearen eta merkataritza elektronikoaren zerbitzuei buruzkoa	Informazioaren gizarteko zerbitzuen alderdi juridiko jakin batzuk arautzen ditu; adibidez, merkataritza elektronikoa, online kontratazioa, informazioa eta publizitatea eta bitartekaritza-zerbitzuak
4	**59/2003 Legea**	Abenduaren 19a	Sinadura Elektronikoari buruzkoa. 39/2015 Legeak aldatua.	Sinadura elektronikoa arautzen du (Internet bidezko komunikazioei segurtasuna eranstearen beharrizanetik sortzen da sinadura hori), baita sinadura horren eraginkortasun juridikoa eta egiaztapen zerbitzuak emateko jarduera ere; 910/2014 Erregelamenduak (eIDAS deritzona) dioenari egokitu beharko zaio.
5	**11/2007 Legea**	Ekainaren 22a	Herritarrek Zerbitzu Publikoetan Sarbide Elektronikoa izateari buruzkoa. 39/2015 Legeak indargabetu du.	Administrazio Elektronikoaren oinarriak arautzen ditu; horretarako, zerbitzu publikoak bitarteko elektronikoekin emateko jarduera eraentzen duten printzipio orokorrak ezartzen ditu, bitarteko elektronikoak konfiantzaz erabil daitezen egoera sortzen du, ezarri beharreko neurriak hartuz oinarrizko eskubide guztiak babesteko eta, bereziki, intimitateari eta norbere datuen babesari loturikoak, segurtasuna alor guztietan bermatuz: sistemak, datuak, komunikazioak eta zerbitzu elektronikoak

#	Araua	Eguna	Azalpena	Xedea
6	**25/2007 Legea**	Urriaren 18a	Komunikazio elektronikoei eta komunikazioen sare publikoei buruzko datuak kontserbatzeari buruzkoa	Sarbide publikoko komunikazio elektronikoen edo komunikazio-sare publikoen zerbitzuak emateari dagokionez sortutako edo tratatutako datuak nola kontserbatu behar diren azaltzen du (2006/24/EE Zuzentarauaren transposizioa)
7	**37/2007 Legea**	Azaroaren 16a	sektore publikoaren informazioa berrerabiltzeari buruzkoa	Berrerabilera arautzen duten arauen gutxieneko multzo bat ezartzen du, eta estatu kideetako sektore publikoko erakundeek kontserbatutako agirien berrerabilera errazteko tresna praktikoak ere bai (sektore publikoaren informazioa kontserbatu eta berrerabiltzeari buruzko 2003/98/EE Zuzentarauaren transposizioa).
8	**232/2007 Dekretua**	Abenduaren 18a	administrazio-prozeduretan bitarteko elektroniko, informatiko eta telematikoen erabilera arautzen duena	Herritarrei bermatzen die legeetan aintzatetsitako eskubideak baliatzea, eta Administrazio Publikoko organo eta langileei aukera ematen die antolamendu juridikoak ezartzen dizkieten betebeharrak betetzeko.
9	**56/2007 Legea**	Abenduaren 28a	Informazioaren Gizartea Bultzatzeko Neurriei buruzkoa	Informazioaren Gizartea garatzeko eta Europarekin eta Komunitate eta Hiri Autonomoen artean bateratzeko 2006-2010 Avanza Plana eratu zuten neurrietarako esparrua ezartzen du. Plan hori Gobernuak 2005eko azaroan onartu zuen, eta horren ostean Avanza 2 Plana (2011-2015) atera zuen.
10	**1671/2009 ED**	Azaroaren 6a	11/2007 Legea zati batean garatzen duena. 39 eta 40/2015 Legeek zati batean indargabetu zuten.	11/2007 Legea zati batean garatzea datuen transmisioari, egoitza elektronikoei eta sarbide puntu nagusiari, identifikazioari eta autentifikazioari, komunikazio eta jakinarazpenei eta agiri elektronikoei eta kopiei dagokienez.
11	**3/2010 ED**	Urtarrilaren 8a	Administrazio Elektronikoaren esparruan Segurtasun Eskema Nazionala arautzen duena	Bitarteko elektronikoen erabileran beharrezkoak diren konfiantzazko baldintzak ezartzen ditu. Horretarako, segurtasunaren arloan bete beharreko oinarrizko printzipioak eta gutxieneko eskakizunak ezartzen ditu, eta aplikatu beharreko segurtasun-neurri batzuk ere bai.

#	Araua	Eguna	Azalpena	Xedea
12	**4/2010 ED**	Urtarrilaren 8a	Administrazio Elektronikoaren esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.	Administrazio Publikoaren sistema informatikoetako informazioaren segurtasun, normalizazio (estandarizazio) eta kontserbaziorako irizpideak zehazten ditu, datuen, informazioen eta zerbitzuen elkarreragintasuna ziurtatzeko antolaketaren, semantikaren eta teknikaren arloetan.
13	**Agindua**	Otsailaren 26a	EAEko Administrazio Orokorraren eta haren erakunde autonomoen informazioaren segurtasuna mantentzeko Segurtasun Eskuliburua onartzen duena	Informazioaren segurtasuna mantentzen du tramitazio telematikoari euskarria ematen dioten aplikazio informatikoen ingurunean (Administrazio Elektronikoa).
14	**21/2012 Dekretua**	Otsailaren 21a	Administrazio elektronikoari buruzkoa	Herritarren eta Administrazioaren arteko harremanak seguruak eta arinak izan daitezen eta berme juridiko osoak izan ditzaten beharrezkoak diren baliabide elektronikoak arautzen ditu.
15	**9/2014 Lege Orokorra**	Maiatzaren 9a	Telekomunikazioei buruzkoa	Telekomunikazioak arautzen ditu, barnean hartuta sareen ustiapena eta komunikazio elektronikoen zerbitzugintza eta lotutako baliabideak.
16	**910/2014 (EE) Erregelamendua (eIDAS)**	Uztailaren 9a	Europako Parlamentuarena eta Kontseiluarena	Elkarreragintasuna zaintzen du identifikazio elektronikoari eta transakzio elektronikoetarako konfiantzazko zerbitzuei buruz, barneko merkatuan (1999/93/EE indargabetzen du).
17	**39/2015 Legea**	Urriaren 1a	Administrazio Publikoen Administrazio Prozedura Erkidearena	Honako hauek arautzen ditu: administrazio-egintzak baliozko eta eraginkor izateko betekizunak; administrazio publiko guztiek erkide duten administrazio-prozedura, barnean harturik zehapen-prozedura eta administrazio publikoen erantzukizuna erreklamatzeko prozedura; eta zer printzipiori jarraitu behar zaion legegintza-ekimena eta erregelamendu-ahala baliatzean; halaber, Segurtasun Eskema Nazionala betetzeko betebeharra ezartzen da.

#	Araua	Eguna	Azalpena	Xedea
18	**40/2015 Legea**	Urriaren 1a	Sektore Publikoaren Araubide Juridikoarena	Honako hauek ezartzen eta arautzen ditu: Administrazio Publikoen araubide juridikoaren oinarriak, Administrazio Publikoen erantzukizun-sistemaren eta zehatzeko ahalmenaren printzipioak, bai eta Estatuko Administrazio Orokorraren eta haren sektore publiko instituzionalaren antolaketa eta funtzionamendua, haien jarduerak garatzeko, jarduera horietan Segurtasun Eskea Nazionalaren aplikazioa ezarrita.
19	**951/2015 ED**	Urriaren 23a	SENa aldatzen duena	SENa eguneratzen du. Horretarako, une bakoitzean Administrazioan erabiltzen diren sistema teknologikoen erantzuna segurtasunaren arloan hobetuko duten mekanismoak hartzen ditu, bereziki zibermehatxuei dagokienez, eta konfiantzazko zerbitzuak nahiz transakzio elektronikoetarako babesa indartzen ditu.
20	**2016/679 Erregelamendua (EB)**	Apirilaren 27a	Datuak babesteko Erregelamendu Orokorra	Datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituena, eta 95/46/EE Zuzentaraua (Datuak babesteko Erregelamendu Orokorra) indargabetzen duena
21	**Ebazpena**	2016 urriaren 7a	Herri Administrazioen Estatu Idazkaritzarena, Segurtasunaren Estatuko Txostenaren Segurtasunerako Jarraibide Teknikoa onartzen duena	datuak biltzeko eta komunikatzeko baldintzak ezartzen ditu, Segurtasun Eskema Nazionalaren aplikazio-eremuko sistemen informazioaren segurtasunaren aldagai nagusiak ezagutzeko aukera ematen duena, eta administrazio publikoetako zibersegurtasunaren egoeraren profil orokorra egiten du.
22	**Ebazpena**	2016ko urriaren 13a	Herri Administrazioen Estatu Idazkaritzarena, Segurtasunerako Jarraibide Teknikoa onartzen duena, Segurtasun Eskema Nazionalaren arabera.	Segurtasun Eskema Nazionalarekin bat etortzeari publizitatea emateko prozedurak ezartzen ditu, eta baita erakunde zirgatzaileei eska dakizkieken betekizunak ere.

#	Araua	Eguna	Azalpena	Xedea
23	**Ebazpena**	2018ko martxoaren 27a	Funtzio Publikoaren Estatu Idazkaritzarena, Informazio Sistemen Segurtasunaren Auditoretzako Segurtasun Jarraibide Teknikoa onartzen duena	Administrazio Elektronikoaren eremuan Segurtasun Eskema Nazionala arautzen duen urtarrilaren 8ko 3/2010 Errege Dekretuaren 34. artikuluan aurreikusitako auditoria arruntak edo apartekoak egiteko baldintzak ezartzen ditu.
24	**Ebazpena**	2018ko apirilaren 13a	Funtzio Publikoko Estatu Idazkaritzarena, segurtasun-gorabeherak jakinarazteko segurtasun-jarraibide teknikoa onartzen duena	Lege horren aplikazio-eremuko sektore publikoko erakundeen informazio-sistemetan segurtasun-intzidenteak jakinaraztea eta kudeatzea arautzen du, gorabehera horiek inpaktu nabarmena dutenean erabiltzen duten edo ematen dituzten zerbitzuen informazioaren segurtasunean, sistemaren kategoriari dagokionez eta organismo edo erakunde bakoitzak bere ingurune berezietara egokitzeko ezartzen dituen eskakizun gehigarriak alde batera utzita.
25	**3/2018 Legea**	Abenduaren 5a	Datu pertsonalen babesa eta eskubide digitalen bermea	a) Espainiako ordenamendu juridikoa egokitzen du Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamendura, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkora, eta haren xedapenak osatzen ditu. b) Herritarren eskubide digitalak bermatzen ditu, Konstituzioaren 18.4 artikuluan ezarritako aginduari jarraiki.
26	**4/2019 ED-Legea**	Urriaren 31a	Administrazio digitalaren, sektore publikoaren kontratazioaren eta telekomunikazioen arloan segurtasun publikoko arrazoiengatik presako neurriak hartzeko dena.	Arau-esparru bat arautzen du, honako gai hauei buruzko premiazko neurriak biltzen dituena: nortasun-agiri nazionala; herri-administrazioetan identifikazio elektronikoa; administrazio horien esku dauden datuak; kontratazio publikoa; eta telekomunikazioen sektorea.

#	Araua	Eguna	Azalpena	Xedea
27	**6/2020 Legea**	Azaroaren 11	konfiantzazko zerbitzu elektronikoen alderdi jakin batzuk arautzen dituena	Konfiantzazko zerbitzu elektronikoen alderdi jakin batzuk arautzen ditu, Europako Parlamentuaren eta Kontseiluaren 2014ko uztailaren 23ko 910/2014 (EB) Erregelamenduaren osagarri gisa. Erregelamendu hori barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantzazko zerbitzuei buruzkoa da, eta 1999/93/EE Zuzentaraua indargabetzen du.
28	**311/2022 ED-Legea**	Maiatzaren 3a	Segurtasun Eskema Nazionala arautzen duena	Bitarteko elektronikoen erabileran behar diren konfiantza-baldintzak sortzen ditu, eta, horretarako, kudeatutako informazioa eta haren aplikazio-eremuko erakundeek emandako zerbitzuak behar bezala babesteko beharrezkoak diren oinarrizko printzipioak eta betekizunak ezartzen ditu, beti ere beren eskumenak gauzatzean kudeatzen dituzten bitarteko elektronikoen bidez erabiltzen diren datuak, informazioa eta zerbitzuak eskuratu, konfidentzialtasuna, osotasuna, trazabilitatea, benetakotasuna, eskuragarritasuna eta kontserbazioa ziurtatzeko.

3.3 *Segurtasunaren antolaketa*

Segurtasunaren antolamendua honako hauetan oinarritzen da: **«Eusko Jaurlaritzaren administrazio elektronikorako antolaketa-egitura eta segurtasun-rolen esleipena onartzen dituen Akordioa»**, Gobernu Kontseiluarena, 2015eko ekainaren 30ekoa, eta **«Euskal Autonomia Erkidegoko administrazio publikoak tratatutako datu pertsonalak babesteko antolaketa-egitura eta rolen esleipena onartzen dituen Akordioa»** (2018ko ekainaren 19koa).

Aplikazio-eremuak Euskal Autonomia Erkidegoko Administrazio Publikoari eta Administrazio Elektronikoaren oinarri diren IKT azpiegiturak ustiatzeko ardura duen erakundeari eragiten die. Eragile horiek jarraian deskribatzen diren **segurtasun- eta pribatutasun-rolak** artikulatu behar dituzte, eta ezarritako segurtasun- eta pribatutasun-batzordeetan parte hartu behar dute.

Informazioaren segurtasun- eta pribatutasun-politika hori bat dator Euskal Autonomia Erkidegoko Administrazio Publikoaren eremuan dauden datu pertsonalak babesteko segurtasun-dokumentuekin. Hau da, definitutako rolen eta erantzukizunen artikulazioak bateragarria izan behar du, eta integratuta egon behar du, ahal den neurrian, 2016/679 (EB) Erregelamenduarekin eta abenduaren 5eko 3/2018 Legearekin.

GureSeK (*Gure Segurtasun Kudeaketa*) esaten zaio Euskal Autonomia Erkidegoko Administrazio Publikoak herritarrei ematen dizkien zerbitzu elektronikoen segurtasuna eta pribatutasuna kudeatzeaz arduratzen den informazioaren segurtasuna eta pribatutasuna kudeatzeko prozesuari.

Euskal Autonomia Erkidegoko Administrazio Publikoko langile guztiek bete beharreko betebehar batzuk ezartzen dira zerbitzu elektroniko horiek ematen parte hartzerakoan, zuzenean edo zeharka, *«3.8. Erabiltzaileen betebehar orokorrak»* atalean adierazten den bezala.

Halaber, informazioaren segurtasunaren eta pribatutasunaren ikuspegitik bete beharreko jarraibide batzuk ezartzen dira, Euskal Autonomia Erkidegoko Administrazio Publikoak zerbitzu elektronikoak ematearekin lotutako produktuak erosteko edo zerbitzuak kontratatzerakoan.

3.4 *Segurtasun eta pribatutasun-rolak*

Eginkizun-rolak honako hauek dira:

#	Rola	Titularra	Eginkizunak
1	Informazioaren arduradunak	Dagokion Saileko Zerbitzu Zuzendaritzaren edo Erakunde Autonomo bakoitzari dagokion gobernuko kide bakarreko organoaren titularra	Beren sailean edo erakunde autonomoan erabiltzen diren aplikazioen informazioa behar bezala babesteko informazioaren segurtasun eta pribatutasuneko eskakizunak ezartzeko ahalmena dute, baita zaindu beharreko interesak nahiz bete beharreko premiak zehazteko ahalmena ere. Dagokien saileko edo erakunde autonomoko aplikazioek maneiatzen duten informazioaren erabileraren erantzuleak dira, eta informazio hori babesteko ardura dute. Horregatik, aplikazio horiek behar ez bezala erabiltzeagatik edo zabarkeriaz jokatzeagatik informazioaren segurtasunari kalte egiten bazaio, haiek izango dira erantzuleak. Segurtasun Korporatiboko Batzordean parte hartzen dute eta euren zuzendaritzako edo erakunde autonomoko kideen artean Segurtasun Batzorde Teknikoan parte hartu behar duen pertsona izendatzen dute.
2	Zerbitzu komunen arduradunak	Zerbitzu komun baten eskumena duen zuzendaritzaren titularra: • Administrazio elektronikoa • Funtzio publikoa eta langileen kudeaketa • Araudi eta ekonomia kontroleko bulegoa • Lurralde plangintza eta hirigintza • Artxibo eta dokumentazio sistema • Instalazioen segurtasuna	Ahalmena dute aplikazio horiek eta plataforma teknologiko horiek ematen dituzten zerbitzuak behar bezala babesteko beharrezkoak diren segurtasun-betekizunak ezartzeko, eta aplikatu beharreko interes eta beharrizanak zehazteko. Zerbitzu komuna erabiltzeko moduaren erantzuleak dira, eta informazio hori babesteko ardura dute. Horregatik, zerbitzu horiek behar ez bezala erabiltzeagatik edo zabarkeriaz jokatzeagatik segurtasun-gorabehera bat sortzen bada, haiek izango dira erantzuleak. Segurtasun Korporatiboko Batzordean parte hartzen dute eta euren zuzendaritzako kideen artean Segurtasun Batzorde Teknikoan parte hartu behar duen pertsona izendatzen dute.

#	Rola	Titularra	Eginkizunak
3	Segurtasunaren arduraduna	Informazioaren eta komunikazioaren teknologietan eskumena duen Zuzendaritzako titularra	Ahalmena dute Administrazio Elektronikoaren euskarri diren informazio-sistemen segurtasun-betekizunak ezartzeko, eta alde horretan, aplikatu beharreko segurtasun-neurriak behar bezala zehazten dituzte. Eusko Jaurlaritzako sail eta erakunde autonomo guztietan informazioaren segurtasunaren arloko prestakuntza eta kontzientziazioa sustatzeko ardura dauka. Alde horretan, Eusko Jaurlaritzako sail eta erakunde autonomoetan informazioaren segurtasunaren arloko prestakuntza-programa Herri Arduralaritzaren Euskal Erakundeak (IVAP) emango du, eta erakunde autonomo horren zeharkako prestakuntza-programaren barruan egongo da. Administrazio Elektronikoaren euskarri diren informazio-sistemak babesteko ardura dauka. Beraz, segurtasun horri eragiten dioten akats edo zabarkerien erantzulea izango da. Segurtasun-neurri teknikoak aplikatzeko, «enkargu orokorra» egingo zaio Eusko Jaurlaritzaren Informatika Elkarteari [aurrerantzean EJIE] Segurtasun eta Pribatutasun Korporatiboko Batzordean parte hartzen du eta bere zuzendaritzako kideen artean Segurtasun Batzorde Teknikoan parte hartu behar duen pertsona izendatzen du.

#	Rola	Titularra	Eginkizunak
4	Sistemen ustiapenaren arduraduna	Eusko Jaurlaritzaren Informatika Elkarteko (EJIE) zuzendari nagusia. Sozietate hori, informatikan eta telekomunikazioetan eskuduna den zuzendaritzaren enkarguz, Eusko Jaurlaritzaren Administrazio Sare Korporatiboa osatzen duten sistema informatikoak hedatzeaz eta mantentzeaz arduratuko da, eta baita sistema horien segurtasunaz ere.	EJIEren azken ardura, bere estatutuen arabera, Administrazio Elektronikoaren eta haren segurtasunaren euskarri diren sistema informatikoak instalatzea, ekoizpenean jartzea eta mantentzea izango da, eta horien funtzionamenduan gertatzen diren akats guztien azken erantzulea izango da. Erantzukizun horiekin bat etorrita, informazioaren eta komunikazioaren teknologietan eskumena duen Zuzendaritzak ahalmena izango du EJIEk sistema informatiko horien eta sistemen segurtasunaren inguruan aplikatu beharreko arkitektura, ezaugarri teknologikoak eta kudeaketa-eredua definitzeko. Horren helburua da sistema horiek bete ditzatela euren gainean erantzukizunak dauzkaten Eusko Jaurlaritzako sail eta erakunde autonomoek ezarritako eginkizun nahiz segurtasun arloko baldintzak. EJIEko zuzendari nagusiak Segurtasun eta Pribatutasun Korporatiboko Batzordean parte hartu beharko du, eta EJIEko segurtasuneko arduradunak Segurtasun Batzorde Teknikoan. EJIEk aplikatu egin beharko ditu informazioaren eta komunikazioaren teknologietan eskumena duen Zuzendaritzak bere ahalmen ekonomikoarekin bat etorrita definitutako segurtasun-neurri teknikoak, Segurtasun eta Pribatutasun Korporatiboko Batzordean ezartzen denaren arabera. EJIEk Segurtasun eta Pribatutasun Korporatiboko Batzordeari proposatu beharko dio Administrazio Elektronikoko zerbitzuei buruz aurretiazko balorazioa egin dezala bere ahalmen ekonomikoarekin bat etorrita, batzorde horrek egokitzat jotzen dituen aldaketak ezarri ahal izan ditzan.

3.5 *Segurtasun eta pribatutasun- koordinatzeko batzordeen egitura*

Segurtasuna koordinatzeko, honako kide anitzeko erakunde hauek sortzen dira:

#	Erakundea	Titularrak	Eginkizunak
1	Segurtasun eta pribatutasun Korporatiboko Batzordea	1. Segurtasunaren eta sistemen arduraduna, Batzordeko buru izango dena 2. Zerbitzu komunen arduradunak 3. Informazioaren eta pribatutasun-neurrien arduradunak 4. Sistemen ustiapenaren arduraduna 5. Datuak Babesteko ordezkaria	Segurtasun eta pribatutasunaren arloan Administrazio Elektronikoaren eraginpean dauden guztien interesak zuzendu eta koordinatzea: 1) Administrazio Elektronikoaren eraginpean dauden guztien artean (sailak, erakunde autonomoak eta EJIE) segurtasuna dela-eta sor daitezkeen gatazkak ebaztea 2) Ezarritako betekizunen, haiei lotutako segurtasun-neurrien eta kostuaren arabera aplikatu beharreko segurtasun-mailak berrikusi, zuzendu eta onestea 3) Administrazio Elektronikoan segurtasunaren garapena bultzatzeko une bakoitzean aproposenak diren lan-organoak sortzea Gutxienez urtean behin egingo du bilera, baita buruak beharrezkotzat jotzen duen aldi guztietan ere.
2	Datuak Babesteko Batzordea	1. Datuak Babesteko ordezkaria 2. Sailetako, erakunde autonomoetako edo zuzenbide pribatuko erakunde publikoetako datuak babesteko erreferenteak diren pertsonak	1) Datuak babesteko ordezkariarekin koordinatzea datuak babesteko politiketan eta horien aplikazioan. 2) Datuak babesteko ordezkariaren jarraibideak jakinaraztea, erreferentziako pertsonek beren jarduerak modu koordinatuan, eraginkorrean eta efizientean egin ahal izan ditzaten. 3) Datuak Babesteko Batzordeko gainerako kideen aurrean azaltzea sail, erakunde autonomo edo zuzenbide pribatuko erakunde publiko bakoitzeko tratamenduaren arduradunek planteatutako gaiak, doktrina bateratzeko, datuak babesteko ordezkariak eskatzen duenean. 4) Datuen babesaren arloan sortu diren informazio garrantzitsuak aztertzea. 5) Kontrol-erakundeek eta beste administrazio publiko batzuek datu pertsonalen babesari dagokionez egindako azken aurrerapenak eta/edo interpretazioak aztertzea

#	Erakundea	Titularrak	Eginkizunak
3	Segurtasun Batzorde Teknikoa	1. Informazioaren eta komunikazioaren teknologien arloan eskumena duen Zuzendaritzako pertsona 2. Administrazio Elektronikoan eskumena duen Zuzendaritzako pertsona 3. Dokumentuen Kudeaketan eskumena duen Zuzendaritzako pertsona 4. Ondarearen Segurtasunean eskumena duen Zuzendaritzako pertsona 5. Eusko Jaurlaritzako sail eta erakunde autonomoetako informatika-arloko eta/edo segurtasuneko arduradun guztiak 6. EJIEko segurtasun-arduraduna	Administrazio Elektronikoaren segurtasuna koordinatzea zerikusia duten organoen artean: • EJIEk eta Eusko Jaurlaritzako sailek eta erakunde autonomoek Administrazio Elektronikoaren segurtasunaren arloan dauzkaten beharrizanak artatzea. • Segurtasun eta Pribatutasun Korporatiboko Batzordeari aldiro segurtasunaren egoeraren berri ematea. • Eusko Jaurlaritzaren segurtasuna kudeatzeko prozesuaren etengabeko hobekuntza sustatzea. • Eusko Jaurlaritzan segurtasunaren eboluziorako estrategia prestatzea. • Administrazio Elektronikoan parte hartzen duten edo horrekin zerikusia duten guztien ahaleginak koordinatzea informazioaren segurtasunaren arloan, eta ahalegin horiek sendoak eta bateratuak izan daitezela eta definitutako estrategiarekin lerrokatuta egon daitezela saiatzea. • Eusko Jaurlaritzak definitutako segurtasun-politika eta segurtasun-araudiak aldiro berrikustea eta egunera daitezela bultzatzea. • Administrazio Elektronikoaren administratzaile, operatzaile eta erabiltzaileek prestakuntzaren eta kualifikazioaren arloetan bete behar dituzten baldintzak definitzea, segurtasunaren ikuspuntutik. • Administrazio Elektronikoaren segurtasun-arriskuen azterketa eta kudeaketa zuzentzea. • Segurtasun-gorabeherak kudeatzeko prozesuen jarduna monitorizatzea eta horiei buruz egin litezkeen ekintzak gomendatzea. • Eusko Jaurlaritzaren segurtasun-auditoretzen programa egin dadila bultzatzea. • Segurtasun arloko jardueren artean lehentasunak ezartzea, baliabideak mugatuak direnean. • Bere kideen bitartez, teknikaz harago definitzen diren segurtasun-neurriak aplikatzea. • IKT proiektuetan hasierako zehaztapenetik ekoizpenerako eta eragiketarako jarri arte informazioaren segurtasuna kontuan har dadila zaintzea. • Arduradunen artean eta/edo sail edo erakunde autonomoen artean segurtasun arloan ager daitezkeen gatazkak tratatzea, eta kasu batean erabakitzeko aginte nahikorik ez badu, kasu hori Segurtasun eta Pribatutasun Korporatiboko Batzordeari igortzea. Burua segurtasunaren arduraduna izango da, edo zuzendaritzako kide bat, zuzendaritzak berak izendatua, eta urtean birritan egingo du bilera.

3.6 *Arriskuen kudeaketa*

Arriskuen kudeaketa segurtasun-prozesuko funtsezko atal bat da eta etengabe egin behar da informazio-sistemen gainean, inguruak kontrolatuta mantentzeko eta arriskuak maila onargarrietara txikiagotzeko. Nahitaezkoa izango da urtarrilaren 8ko 3/2010 Errege Dekretuak –Administrazio Elektronikoaren esparruko Segurtasunerako Eskema Nazionala arautzen duenak– ezarritako esparruaren barruko informazio-sistemetarako, eta gainerako kasuetan aukerakoa izan daiteke.

Informazioaren eta zerbitzuen arduradunak informazioaren eta zerbitzuen inguruko arriskuez arduratzen dira, hurrenez hurren, eta jarraipena eta kontrola bermatuko dutenak izango dira, zeregin horiek eskuordetzeko aukeraren kaltetan izan gabe. Horretarako, prozesuan segurtasunaren arduradunaren eta sistemen esplotazioaren arduradunaren partaidetza eta aholkularitza eduki ahal izango dute.

Arriskuen azterketa egiteko, administrazio publikoaren esparruan argitaratutako gomendioak eta, bereziki, Kriptologia Zentro Nazionalak egindako gidak hartuko dira kontuan. Arriskuen ebaluazio hori aldiro egingo da informazio-sistemetarako, Kriptologia Zentro Nazionalak egindako gomendioak aintzat hartuz.

Eusko Jaurlaritzak konpromisoa dauka eta informatikako arduradunek, aldiz, betebeharra, arriskuak aztertzekoa eta ondorioak jorratzekoa. Politika honi lotutako sistema guztiek arriskuen azterketa egin beharko dute, eta, horretarako, aktiboek jasan ditzaketen mehatxuak eta arriskuak ebaluatuko dituzte. Aipatu azterketa errepikatu egingo da:

- Aldiro, bi urtez behin behintzat
- Erabilitako informazioa edo emandako zerbitzuak nabarmen aldatzen direnean
- Segurtasunari lotutako gorabehera larriren bat jazotzen denean eta kalteberatasun larriak ekartzen dituenean

3.7 *Beste segurtasun baldintzak batzuk*

SENen Errege Dekretuaren 11. artikulua betez, segurtasun eta pribatutasun-politika hau garatzeko, aurreko kapituluetan adierazitako betekizunez gain, honako gutxieneko betekizun hauek aplikatuko dira:

• Profesionaltasuna.

EAEko Administrazio Publikoko sistemen segurtasuna langile kualifikatuek zainduko, berrikusiko eta ikuskatuko dute beti, beren bizi-zikloaren fase guztietan (instalazioan, mantentze-lanetan, gorabeheren kudeaketan eta eraistean) jardun eta ikasiko dute.

Gainera, langile guztiek beharrezko prestakuntza jasoko dute Administrazioaren sistemei eta zerbitzuei aplika dakizkiekeen informazio-teknologien segurtasuna bermatzeko.

• Sarbideak baimentzea eta kontrolatzea.

Informazio-sistemetarako sarbidea kontrolatua izango da, eta erabiltzaileei, prozesuei, gailuei eta beste informazio-sistema batzuei mugatuko zaie, behar bezala baimenduta eta sarbide mugatuarekin.

• Instalazioak babestea.

EAEko Administrazio Publikoaren instalazioetan sarbideak kontrolatzeko puntuak egongo dira.

• Segurtasun-produktuak erostea eta segurtasun-zerbitzuak kontratatzea

EAEko Administrazio Publikoak erabiliko dituen informazioaren eta komunikazioen teknologien segurtasun-produktuak eskuratzeko, sistemaren kategoria eta segurtasun-maila zehatzaren arabera eta erosketa horietarako garatutako gidari jarraituz erabiliko dira.

• Lehenetsitako segurtasuna.

Sistemak lehenetsitako segurtasuna bermatzeko moduan diseinatu eta konfiguratuko dira.

• Sistemaren osotasuna eta eguneratzea.

Edozein elementu fisiko edo logiko instalatzeko, sisteman instalatu aurreko baimen formala beharko da.

Uneoro jakingo da sistemen segurtasun-egoera, fabrikatzaileen zehaztapenei, urrakortasunei eta eragiten dieten eguneratzeei dagokienez, eta arretaz erreakzionatuko da arriskua kudeatzeko, horien segurtasun-egoera ikusita.

• Biltegiratutako eta iragaitzazko informazioa babestea.

Sistemaren segurtasunaren egituran eta antolamenduan, arreta berezia jarriko zaio ingurune ez-seguruetan zehar biltegiratutako edo iragaitzazko informazioari. Euskarri ez-elektronikoan dagoen informazio guztia babestuta egongo da.

- Prebentzioa elkarrekin konektatutako beste informazio-sistema batzuen aurrean

Sare publikoetara konektatuz gero, perimetroa babestuko da, eta sistema sareen bidez beste sistema batzuekin konektatzearen ondoriozko arriskuak aztertuko dira.

• Jarduera-erregistroa

3/2010 Errege Dekretua betetzeko helburu esklusiboarekin, eragindakoen ohorerako, norberaren eta familiaren intimitaterako eta norberaren irudirako eskubidea erabat bermatuta, eta datu pertsonalak, funtzio publikoari buruzkoak eta aplikatzekoak diren gainerako xedapenak betez, erabiltzaileen jarduerak erregistratuko dira, bidegabeko edo baimenik gabeko jarduerak monitorizatzeko, aztertzeko, ikertzeko eta dokumentatzeko behar den informazioa atxikiz, eta jarduten duen pertsona une bakoitzean identifikatzeko aukera emanez.

• Segurtasun-gorabeherak

Segurtasun-intzidenteak kudeatzeko berariazko prozedurak ezarriko dira.

• Jardueraren jarraitutasuna.

Sistemek segurtasun-kopiak izango dituzte, eta beharrezko mekanismoak ezarriko dituzte eragiketen jarraitutasuna bermatzeko, ohiko lan-bitartekoak galduz gero.

• Segurtasun-prozesua etengabe hobetzea.

EAEko Administrazio Publikoak etengabe eguneratzen eta hobetzen ditu bere sistemak.

3.8 *Segurtasun eta pribatutasun-politika berrikusteko prozesua*

Eusko Jaurlaritzak definitutako segurtasun eta pribatutasun-politika eta segurtasun eta pribatutasun-araudia berrikusi behar dira, eta egunera daitezela bultzatu behar da.

Segurtasun eta Pribatutasun Korporatiboko Batzordeak informazioaren segurtasun eta pribatutasun politika berrikusiko du, aldiro edo horretara behartzen duen aldaketa esanguratsu bat dagoenean. Berrikusteko proposamena, bidezkoa bada, onetsi egingo da, eta hedatu egingo da, ukitutako alde guztiek jakin dezaten.

3.9 *Erabiltzaileen betebehar orokorrak*

Informazio-sistemak eskura ditzaketen langile guztien betebeharra da informazioaren segurtasun eta pribatutasun politika eta hortik eratorrita ezartzen den segurtasun eta pribatutasun-araudia ezagutzea eta betetzea. Xede horrekin, informazioaren segurtasun-politika Administrazio Elektronikoaren esparruaren barruan dauden informazio-sistemen erabiltzaile guztiei jakinaraziko zaie modu egoki, eskuragarri eta ulergarrian. Segurtasun eta pribatutasun-politika urratzen bada, zehapenak ezarri ahalko dira, diziplina-araudiaren arabera.

Halaber, azpikontratatutako kanpoko enpresetako langileek, Eusko Jaurlaritzaren zerbitzuetako bati lotutako agiriak edo informazioa eskuratu ahal badituzte, informazioaren segurtasun eta pribatutasun-politika hori ezagutu eta bete behar dute.

Informazioaren eta komunikazioaren teknologietako sistemak erabiltzen dituzten langile guztiek prestakuntza jasoko dute sistema horiek modu seguruan erabiltzeko. Politika hori benetan bete dadila bermatuko duten kontrol-prozedurak ezarri beharko dira. Prozedura horiek sailek eta erakunde autonomoek egingo dituzte.

3.10 *Kontzientziazioa eta prestakuntza*

Segurtasun eta Pribatutasun Korporatiboko Batzordeak sustatu behar du informazioaren segurtasun eta pribatutasunaren arloko prestakuntza eta kontzientziazioa, Administrazio Orokorraren eta haren erakunde autonomoen esparruan.

Jarduera espezifikoak egingo dira, langile guztiei informazioaren segurtasun eta pribatutasunaren gaineko prestakuntza emateko eta langileok horri buruz kontzientziatzeko, bai eta informazioaren segurtasun eta pribatutasun-politika eta politika horren araubidezko garapena hedatzeko. Jarduera horiek bereziki langile berrientzat izango dira. Xede horrekin, prestakuntza-planetan informazioaren segurtasun eta pribatutasunari buruzko jarduera espezifikoak sartuko dira.

Eusko Jaurlaritzako sail eta erakunde autonomoetan informazioaren segurtasun eta pribatutasunaren arloko prestakuntza-programa Herri Arduralaritzaren Euskal Erakundeak (IVAP) emango du, eta erakunde autonomo horren zeharkako prestakuntza-programaren barruan egongo da.

3.11 *Hirugarren aldeak*

Eusko Jaurlaritzak hirugarrenen zerbitzuak edo informazioa erabiltzen dituenean, hirugarren horiei informazioaren segurtasun eta pribatutasun-politika honen berri emango die. Segurtasun Batzorde Teknikoak oharretarako eta koordinaziorako kanalak ezarriko ditu, eta segurtasun-gorabeheretan erreakziorako jardun-prozedurak ezarriko ditu.

Eusko Jaurlaritzak beste erakunde batzuei zerbitzuak ematen badizkie, informazioaren segurtasun- eta pribatutasun-politika honen eta zerbitzu edo informazio horiei dagozkien jarraibide eta prozeduren berri emango die.

Eusko Jaurlaritzak, hirugarrenei informazioa lagatzen dienean edo beste erakunde batzuei zerbitzugintzaren bat enkargatzen dienean, informazioaren segurtasun eta pribatutasun politika horren berri emango die, baita zerbitzu horiei edo informazio horri dagozkien Jarraibide eta Prozeduren berri ere. Hirugarren alde hori aipatu den araudian ezarritako betebeharrei lotuta geratuko da, eta araudi hori betetzeko bere prozedura propioak garatu ahalko ditu. Gorabeherez ohartarazteko eta gorabeherak konpontzeko prozedura espezifikoak ezarriko dira. Halaber, hirugarrenen langileak segurtasun eta pribatutasun arloan behar bezala kontzientziatuta egon daitezela eskatuko da, behintzat politika honetan ezarrita dagoenaren pareko maila batean.

4. Eranskina: terminoen eta laburduren glosarioa

Jarraian, dokumentuan erabili diren termino batzuk definituko dira, dokumentua errazago ulertu ahal izateko.

#	Terminoa	Definizioa
1	Aktiboa	Erakundearentzat balioa duen osagaia, funtzionaltasuna edo baliabidea: informazioa, datuak, zerbitzuak, aplikazioak, ekipoak, komunikazioak, baliabide administratiboak, fisikoak eta giza baliabideak.
2	Mehatxua	Informazio-sistema bati edo erakunde bati kalteak eragin diezazkiokeen gertakari baten kausa potentziala [UNE 71504:2008]. Mehatxuak beti daude presente, baina horiek saihesten edo gauzatzearen ondorioak arintzen saia daiteke.
3	Arriskuen analisia	Informazio-sistema batek jasaten dituen mehatxuak, kalteberatasunak, arriskuak eta inpaktuak aztertzeko prozesua, lehendik dauden segurtasun-neurriak kontuan hartuta. Segurtasun-neurrien hobekuntzak identifikatzeko abiapuntu gisa balio du, bai eraginkortasunari dagokionez, bai kostuei dagokienez.
4	Benetakotasun	Propietate edo ezaugarri bat da: erakunde batek esaten du izakia dela, edo datuen jatorria bermatzen du [SEN]
5	Konfidentzialtasuna	Informazioa baimendu gabeko gizabanakoen, erakundeen edo prozesuen eskura ez jartzearen edo horien berri ez ematearen ezaugarria [SEN]
6	Arau multzoa	Politika baten helburuak lortzeko modua zehatzago garatzen duten arauen multzoa.
7	Datu pertsonala	Identifikatutako edo identifika daitezkeen pertsona fisikoei buruzko edozein informazio.
8	Erabilgarritasuna	Aktiboen propietatea edo ezaugarria, hau da, baimendutako erakundeek edo prozesuek horiek eskuratzeko aukera izatea [SEN]
9	SEN	Segurtasun Eskema Nazionala
10	Jarraitutasunaren kudeaketa	Erakunde batek egiten dituen jarduerak, negozio-prozesu kritiko guztiak erabiltzaileentzat, bezeroentzat, hornitzaileentzat eta erabili behar dituzten beste erakunde batzuentzat eskuragarri egongo direla ziurtatzeko.
11	Gorabeherak kudeatzea	Zerbitzuaren ohiko funtzionamendu-maila berreskuratzera eta erakundean segurtasun-akats baten eragin negatiboa ahalik eta gehien murriztera bideratutako prozesuak, zerbitzuaren kalitatea eta erabilgarritasuna manten daitezen.
12	Arriskuen kudeaketa	Arriskuei dagokienez erakunde bat zuzentzeko eta kontrolatzeko jarduera koordinatuak [SEN]

#	Terminoa	Definizioa
13	Segurtasun-intzidentea	Ustekabeko edo nahi gabeko gertaera, informazio-sistemaren segurtasunean ondorio negatiboak dituena [SEN]
14	Osotasuna	Informazioaren aktiboa baimenik gabe ez dela aldatu dioen ezaugarria [SEN]
15	Segurtasun-neurriak	Informazio-sistemekin erlazionatuta egon daitezkeen arriskuetatik babesteko xedapenen multzoa, segurtasun-helburuak ziurtatzeko. Prebentzio-, disuasio-, babes-, detekzio- eta erreakzio-neurriak izan daitezke, edo berreskuratze-neurriak [SEN]
16	MSPLATEA	PLATEA Segurtasun Eskuliburua
17	PLATEA	Eusko Jaurlaritzaren Administrazio Elektronikorako plataforma.
18	Segurtasun- eta pribatutasun-politika	Goi-mailako dokumentua, erakunde baten segurtasun- eta pribatutasun-arloko helburuak zehazten dituena eta zuzendaritzak helburu horiek lortzeko duen konpromisoa islatzen duena.
19	Prozesua	Produktu edo zerbitzu bat ekoizteko egiten diren jardueren multzo antolatua; hasiera eta helburua mugatuta ditu, baliabideak inplikatzen ditu eta emaitza bat ematen du [SEN]
20	Arriskua	Mehatxu bat aktibo baten edo gehiagoren gainean gauzatzearen esposizio-maila zenbatestea, erakundeari kalte edo galerak eraginez [SEN]
21	Hondar-arriskua	Arriskuak tratatzeko planean babes jakin batzuk ezarri ondoren sisteman geratzen den arriskua.
22	Informazioaren segurtasuna	Informazioa eta informazio-sistemak babestea baimenik gabeko sarbide, erabilera, hedapen, eraldaketa, aldaketa edo suntsipenetik.
23	Informazio-sistema	Baliabideen multzo antolatua, informazioa bildu, biltegiratu, prozesatu edo tratatu, mantendu, erabili, partekatu, banatu, eskura jarri, aurkeztu edo transmititu ahal izateko [SEN]
24	Euskarria	Informazioa biltegiratzeko erabiltzen den edozein motatako ingurune fisikoa (papera, USB, DVD, disko eramangarriak, etab.).
25	Trazabilitatea	Erakunde baten jarduketak erakunde horri bakarrik egotzi ahal zaizkiola adierazten duen ezaugarria [SEN]
26	Ahultasuna	Aktibo baten ahultasuna, mehatxu batek aprobetxa dezakeena [SEN]