Euskal Autonomia Erkidegoko Administrazio Publikoaren Informazioaren Segurtasuna Kudeatzeko Sistema

Informazioaren segurtasun- eta pribatutasun-politika

Honek onartua *Nork onartua*	Segurtasun eta Pribatutasun Korporatiboaren Batzordea.	***Erreferentzia*** *Referencia*	Informazioaren segurtasun- eta pribatutasun-politika
Data *Data*	2023-15-11	***Jasotzaileak*** *Distribución*	Langile guztiak

SEGURTASUN-SAILKAPENA / CLASIFICACIÓN DE SEGURIDAD									
Erabilgarritasuna Eskuragarritasuna	TXIKIA	Osotasuna Osotasuna	TXIKIA	Konfidentzialtasuna Konfidentzialtasuna	TXIKIA	Benetakotasuna Benetakotasuna	TXIKIA	Trazabilitatea Trazabilitatea	TXIKIA

Bertsioen kontrola

Bertsioa	Data	Aurreko bertsioarekiko aldaketa	Nork egina	Nork berrikusia	Nork onartua
1. b	2020/11/17	Hasierako bertsioa	Segurtasuneko Bulego Teknikoa	Segurtasuneko Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboaren Batzordea
2. b	2023/01/25	Arau-aldaketak, sistemen arduradunarekin lotutako argibideak eta 3.7 atalean gidalerroak sartzea	Segurtasuneko Bulego Teknikoa	Segurtasuneko Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboaren Batzordea
3. b	2023/11/15	Arau-aldaketak, 311/2022 EDra egokitzea eta akatsak zuzentzea	Segurtasuneko Bulego Teknikoa	Segurtasuneko Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboaren Batzordea

Edukia

1. Sarrera.

Segurtasunaren Eskema Nazionalak (ENS) bere 12. artikuluan eta II. eranskineko org.1 neurrian dioenez, «***informazioaren segurtasun-politika formalki xedatu behar da***»; politika hori goi mailako organo eskudunaren titularrak onetsi behar duela ezartzen du, eta hau jaso behar duela:

- Erakundearen helburuak edo egitekoa.
- Jarduerak zein esparru arautzailearen arabera burutuko diren.
- Segurtasun-rol edo -eginkizunak. Horietako bakoitzari dagozkion betebehar eta erantzukizunak definituko dira, baita horiek izendatzeko eta berritzeko prozedura ere.
- Segurtasuna eta pribatutasuna kudeatu eta koordinatzeko batzordeen egitura eta osaera. Halakoen erantzukizun-esparrua, kide bakoitza eta erakundeko beste elementu batzuekiko harremana zehaztu behar dira.
- Sistemaren segurtasun-dokumentazioa egituratzeko, kudeatzeko eta eskuratzeko gidalerroak.
- Datu pertsonalen tratamenduaren ondoriozko arriskuak.

Informazioaren segurtasunaren arloan Euskal Autonomia Erkidegoko Administrazio Publikoarentzat (aurrerantzean EAEko Administrazio Publikoa) erreferentzia gisa, UNE-ISO/IEC 27001 Arauak ere, 5.2. atalean, segurtasun-politika bat eduki behar dela adierazten 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 Publikoak bere helburuak betetzeko erabiltzen duen tresna, informazioaren eta komunikazioaren sistemak modu seguruan erabilita. Segurtasunaren 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, Euskal Administrazio Publikoan segurtasunaren kultura ezarriz.

1.1 *Segurtasunari eta pribatutasunari buruzko araudia garatzea*

Informazioaren segurtasunari eta pribatutasunari buruzko araudia nahitaez bete behar da, eta mailaz maila garatuko da, aplikazio-eremuaren eta zehaztasun teknikoko mailaren arabera; hala, arau bakoitzak goragoko mailako arauak izango ditu oinarri. Hona hemen garapen-mailak:

#	Maila	Deskribapena
1	Informazioaren segurtasun- eta pribatutasun-**politika**.	Agiri honek osatzen du, eta nahitaez bete beharrekoa da.
2	Segurtasun- eta pribatutasun-**arauak**: informazioaren segurtasunaren eta pribatutasunaren arloko jarraibideak, ekintza-planak eta jarduketa estrategikoak.	Modu egokian nahiz inguruabarren bat prozedura espliziturен batean jasota ez dagoenean nola jardun behar den adierazteko erabiliko diren agiriak. Segurtasun- eta pribatutasun-politika garatzen duten eta politika horren aplikazioaz diharduten arauak dira. Arau bakoitzak honako hau bete beharko du: a) Lortu nahi diren helburuetan jarri arreta, helburuak lortzeko moduan baino gehiago. 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- eta pribatutasun-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 azaldu, 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; eta, hala dagokionean, egindako jardueraren erregistroa. d) Emaitzak nola neurtu eta nola ebaluatu behar diren. e) Nola jakinarazten 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 ebidentzia elektronikoak.

2. Segurtasun- eta pribatutasun-printzipioak

EAEko Administrazio Publikoaren informazioaren segurtasun- eta pribatutasun-politika, oro har, honako printzipioen arabera garatuko da:

#	Printzipioa	Deskribapena
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**	Honetan datza informazioaren segurtasunaren eta pribatutasunaren kudeaketa: arriskuak aztertzea, segurtasun-neurri egokiak, eraginkorrak eta neurrikoak ezartzea, eta etengabeko zuzenketa eta hobekuntza ere kontuan hartzea, erakundea gero eta prebentiboagoa izan dadin, erreaktiboa baino, segurtasun-gorabeheren aurrean, inguruneari kontrolpean eutsi ahal izateko. 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 mintzakide egokiekin trukatzen dela eta zerbitzuak behar bezala egiaztatzen direla bermatu beharko da.

#	Printzipioa	Deskribapena
7	**Trazabilitatea**	Informazioaren eta hori eskatzen duten zerbitzuen inguruan egindako eragiketen jarraipena bermatu beharko da.
8	**Prebentzioa, erreakzioa eta lehengoratzea**	Segurtasunari edo 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 segurtasunaren eta pribatutasunaren arloko prestakuntza-, sentsibilizazio- eta kontzientziazio-programak artikulatuko dira, politika korporatiboetan behar bezala oinarrituta eta jarraipen- eta eguneratze-prozesu egokiarekin.

#	Printzipioa	Deskribapena
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-segurtasunari 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 Publikoaren segurtasun- eta -pribatutasun-politika hurrengo ataletan garatzen da.

3.1 *EAEko Administrazio Publikoaren helburua.*

EAEko Administrazio Publikoaren egitekoa da **Administrazio berri 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 horretatik, IKTak maila estrategiko handiko tresna dira, ahalmena dutelako EAEko Administrazio publikoaren 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, mehatxu horiek eragina izan ahal baitute lehenago aipatu diren berme edo dimentsio horietan.

3.2 *Arau-esparrua*

EAEko Administrazio Publikoaren jardueren araudi-esparrua, informazioaren segurtasun- eta pribatutasun-politikaren esparru horretan, arau hauek osatzen dute:

#	Araua	Data	Deskribapena	Xedea
1	**15/1999 Legea**	Abenduaren 13koa	Datu pertsonalak babesteari buruzkoa 3/2018 Legeak indargabetua, 22., 23. eta 24. artikuluak izan ezik.	Segurtasun-neurrien eta babestu beharreko informazioaren arteko proportzionaltasuna ezartzeko irizpideak ematen ditu.
2	**1720/2007 ED**	Abenduaren 21ekoa	DPBL garatzeko Erregelamendua onartzen duena	Datu Pertsonalak Babesteko 15/1999 Lege Organikoaren edukia garatzen eta osatzen du.
3	**34/2002 Legea**	Uztailaren 11koa	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 19koa	Sinadura elektronikoari buruzkoa. 6/2020 Legeak indargabetua.	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 22koa	Herritarrek Zerbitzu Publikoetan Sarbide Elektronikoa izateari buruzkoa. 39/2015 Legeak indargabetua.	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	Data	Deskribapena	Xedea
6	**25/2007 Legea**	Urriaren 18koa	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 16koa	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 18koa	Administrazio-prozeduretan bitarteko elektroniko, informatiko eta telematikoen erabilera arautzen duena Administrazio Elektronikoari buruzko otsailaren 21eko 21/2012 Dekretuak indargabetua.	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 28koa	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 6koa	11/2007 Legea zati batean garatzen duena. 39 eta 40/2015 Legeek partzialki indargabetua.	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.

#	Araua	Data	Deskribapena	Xedea
11	**3/2010 ED**	Urtarrilaren 8koa	Administrazio Elektronikoaren esparruan Segurtasunaren Eskema Nazionala (ENS) arautzen duena. 311/2022 Errege Dekretuaren xedapen indargabetzaile bakarrak indargabetua.	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.
12	**4/2010 ED**	Urtarrilaren 8koa	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**	2010eko otsailaren 26koa	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 inguruanean (Administrazio Elektronikoa).

#	Araua	Data	Deskribapena	Xedea
14	**21/2012 Dekretua**	Otsailaren 21ekoa	Administrazio Elektronikoari buruzkoa. Herritarrei arreta integral eta multikanala emateko eta zerbitzu publikoak bitarteko elektronikoz irispidean izateko ekainaren 20ko 91/2023 Dekretuak indargabetua.	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 Legea**	Maiatzaren 9koa	Telekomunikazioei buruzkoa. Ekainaren 28ko 11/2022 Legearen xedapen indargabetzaile bakarraren a) atalaren bidez indargabetutako araua, hamaseigarren xedapen gehigarria eta zazpigarren, bederatzigarren eta hamabigarren xedapen iragankorrak izan ezik, 2022ko ekainaren 30etik aurrerako ondorioekin, hargatik eragotzi gabe xedapen iragankorretan xedatutakoa.	Telekomunikazioak arautzen ditu, barnean hartuta sareen ustiapena eta komunikazio elektronikoen zerbitzugintza eta lotutako baliabideak.
16	**910/2014 (EE) Erregelamendua (eIDAS)**	Uztailaren 9koa	Europako Parlamentuarena eta Kontseiluarena	Elkarreragintasuna zaintzen du identifikazio elektronikoari eta transakzio elektronikoetarako konfiantzazko zerbitzuei buruz, barneko merkatuan (1999/93/EE indargabetzen du).

#	Araua	Data	Deskribapena	Xedea
17	**39/2015 Legea**	Urriaren 1ekoa	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, Segurtasunaren Eskema Nazionala betetzeko betebeharra ezartzen da.
18	**40/2015 Legea**	Urriaren 1ekoa	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 23koa	ENS aldatzekoa **Indargabetua.**	ENS 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 27koa	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**	2016ko urriaren 7koa	Administrazio Publikoen Estatu Idazkaritzarena, Segurtasunaren Egoerari buruzko Txostenaren Segurtasun Jarraibide Teknikoa onartzen duena.	Datuak biltzeko eta komunikatzeko baldintzak ezartzen ditu, Segurtasunaren Eskema Nazionalaren aplikazio-eremuko sistemen informazioaren segurtasunaren aldagai nagusiak ezagutzeko aukera ematen duena, eta administrazio publikoetako zibersegurtasunaren egoeraren profil orokorra egiten du.

#	Araua	Data	Deskribapena	Xedea
22	**Ebazpena**	2016ko urriaren 13koa	Administrazio Publikoen Estatu Idazkaritzarena, Segurtasun Jarraibide Teknikoa onartzen duena, Segurtasunaren Eskema Nazionalarekin bat.	Segurtasunaren Eskema Nazionalarekin bat etortzeari publizitatea emateko prozedurak ezartzen ditu, bai eta erakunde ziurtatzaileei eska dakizkiekeen baldintzak ere.
23	**Ebazpena**	2018Ko martxoaren 27koa	Funtzio Publikoaren Estatu Idazkaritzarena, Informazio Sistemen Segurtasunaren Auditoretzako Segurtasun Jarraibide Teknikoa onartzen duena.	Administrazio Elektronikoaren esparruan Segurtasunaren Eskema Nazionala arautzen duen urtarrilaren 8ko 3/2010 Errege Dekretuak 34. artikuluan aurreikusitako ohiko edo ezohiko auditoretzak egiteko baldintzak ezartzen ditu.
24	**Ebazpena**	2018ko apirilaren 13koa	Administrazio Publikoen Estatu Idazkaritzarena, Segurtasun-intzidentziak Jakinarazteko Segurtasun Jarraibide Teknikoa onartzen duena.	Lege horren aplikazio-eremuko sektore publikoko erakundeen informazio-sistemetan segurtasun-intzidenteak jakinaraztea eta kudeatzea arautzen du, gorabehera horiek eragin nabarmena dutenean erabiltzen duten informazioaren edo ematen dituzten zerbitzuen 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 5ekoa	Datu Pertsonalen Babesa eta Eskubide Digitalen Bermea	a) Espainiako ordenamendu juridikoa Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamendura egokitzen du (pertsona fisikoen babesari buruzkoa, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez), eta haren xedapenak osatzen ditu. b) Herritarren eskubide digitalak bermatzen ditu, Konstituzioaren 18.4 artikuluan ezarritako aginduaren arabera.

#	Araua	Data	Deskribapena	Xedea
26	**14/2019 ELD**	Urriaren 31koa	Premiazko neurriak biltzen ditu segurtasun publikoko arrazoiengatik administrazio digitalaren, sektore publikoko kontratazioaren eta telekomunikazioen arloan.	Arau-esparru bat arautzen du, honako hauei buruzko premiazko neurriak biltzen dituena: nortasun-agiri nazionalak, identifikazio elektronikoa administrazio publikoen aurrean, administrazio horien esku dauden datuak, kontratazio publikoa eta telekomunikazioen sektorea.
27	**6/2020 Legea**	azaroaren 11koa	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/CE Zuzentaraua indargabetzen du.	

#	Araua	Data	Deskribapena	Xedea
28	**311/2022 ED**	Maiatzaren 3koa	Segurtasunaren Eskema Nazionala arautzen du.	Bitarteko elektronikoak erabiltzeko beharrezko konfiantza-baldintzak sortzen ditu, eta, horretarako, tratatutako informazioa eta bere aplikazio-eremuko erakundeek ematen dituzten zerbitzuak behar bezala babesteko oinarrizko printzipioak eta betekizunak ezartzen ditu, betiere beren eskumenak gauzatzean kudeatzen dituzten bitarteko elektronikoen bidez erabiltzen diren datuen, informazioaren eta zerbitzuen sarbidea, konfidentzialtasuna, osotasuna, trazabilitatea, benetakotasuna, eskuragarritasuna eta kontserbazioa ziurtatzeko.
29	**11/2022 Legea**	Ekainaren 28koa	Telekomunikazioei buruzkoa.	Modu integralean arautzen du telekomunikazioen araubidea, Konstituzioaren 149.1.21 artikuluko Estatuaren eskumen esklusiboaren babesean.
30	**91/2023 Dekretua.**	Ekainaren 20koa	Herritarrei arreta integral eta multikanala ematekoa eta zerbitzu publikoak bitarteko elektronikoz irispidean izatekoa.	Herritarrei arreta egokia emateko beharrezkoak diren tresna guztiak biltzen ditu, ikuspegi berri batekin eta baliabide elektronikoen bidez zerbitzu publikoetara iristeko aukerarekin; eta bitarteko horiek herritarrekiko beste interakzio-bide bat baino ez dira.

3.3 *Segurtasunaren antolaketa*

Segurtasunaren antolaketaren oinarriak hauek dira: Gobernu Kontseiluaren 2015eko ekainaren 30eko **«*Akordioa, Eusko Jaurlaritzaren administrazio elektronikorako antolamendu-egitura eta segurtasun-rolen esleipena onartzen dituena*»**, eta ***"Euskal Autonomia Erkidegoko Administrazio Publikoak tratatutako datu pertsonalen babeserako antolamendu-egitura eta rolen esleipena onartzen duen akordioa"***, 2018ko ekainaren 19koa.

Aplikazio-eremuan sartzen dira EAEko Administrazio Publikoa eta Administrazio Elektronikoaren euskarri diren IKT azpiegiturak ustiatzeko ardura duen erakundea. Eragile horiek jarraian azalduko diren **segurtasun- eta pribatutasun-rolak** egituratu behar dituzte, eta ezarrita dauden segurtasun batzordeetan parte hartu behar dute.

Informazioaren segurtasun eta pribatutasun politika hori EAEko Administrazio Publikoaren esparruan dauden datu pertsonalen babeserako segurtasun-agiriei buruzkoa da, eta koherentea da agiri horiekin. Hau da, definitutako rolak eta erantzukizunak (EB) 2016/679 Erregelamenduarekin eta abenduaren 5eko 3/2018 Legearekin bateragarriak eta integratuak izan behar dira, ahal den neurrian.

GureSeK (Gure Segurtasun Kudeaketa) izena ematen zaio EAEko Administrazio Publikoak herritarrei ematen dizkieten zerbitzu elektronikoen segurtasuna eta pribatutasuna kudeatzeaz arduratzen den segurtasunaren kudeaketarako prozesuari.

Langile guztiek –bai EAEko Administrazio Publikoko langileek, bai azpikontratatuek– aipatutako zerbitzu elektronikoak ematean –dela zuzenean, dela zeharka– bete beharreko hainbat betebehar ezartzen dira, «*3.9 - Erabiltzaileen betebehar orokorrak*» atalean adierazita dagoenez.

Halaber, EAEko Administrazio Publikoak zerbitzu elektronikoak ematearekin zerikusia duten produktuak eskuratzerakoan edo zerbitzuak kontratatzean informazioaren segurtasunaren eta pribatutasunaren ikuspuntutik bete beharreko gidalerro batzuk ezartzen dira.

3.4 *Segurtasun- eta pribatutasun-rolak*

Eginkizun-rolak hauek dira:

#	Rola	Titularra	Eginkizunak
1	Informazioaren arduradunak	Dagokion Saileko Zerbitzu Zuzendaritzaren edo erakunde autonomo edo zuzenbide pribatuko erakunde publiko bakoitzari dagokion gobernuko kide bakarreko organoaren titularra.	Beren sailean, erakunde autonomoan edo zuzenbide pribatuko erakunde publikoan erabiltzen diren aplikazioen informazioa behar bezala babesteko informazioaren segurtasuneko eta pribatutasuneko eskakizunak ezartzeko ahalmena dute, baita zaindu beharreko interesak nahiz bete beharreko premiak zehazteko ere. Dagokien saileko, erakunde autonomoko edo zuzenbide pribatuko erakunde publikoko 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 Korporatiboaren Batzordean parte hartzen dute eta euren zuzendaritzako, erakunde autonomoko edo zuzenbide pribatuko erakunde publikoko 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 • Kontrol Ekonomikoko eta Finantzetako 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 Korporatiboaren 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 zuzendaritzaren titularra	Ahalmena dute administrazio elektronikoaren euskarri diren informazio-sistemen segurtasun-betekizunak ezartzeko, eta alde horretan, aplikatu beharreko segurtasun-neurriak behar bezala zehazten dituzte. EAEko Administrazio Publikoan informazioaren segurtasunaren arloko prestakuntza eta kontzientziazioa sustatzeko ardura dauka. Alde horretatik, EAEko Administrazio Publikoan informazioaren segurtasunaren eta pribatutasunaren arloko prestakuntza-programa Administrazio Publikoaren Euskal Institutuak (IVAP) emango du, eta erakunde autonomo horren zeharkako prestakuntza-programaren barruan egongo da. Administrazio elektronikoaren euskarri diren informazio-sistemak babesteko ardura dauka. Beraz, segurtasun-gorabeheraren bat sortzen duten edo segurtasunari eragiten dioten akats edo zabarkeria guztien erantzulea izango da. Segurtasun-neurri teknikoak aplikatzeko, «enkargu orokorra» egingo zaio Eusko Jaurlaritzaren Informatika Elkarteari [aurrerantzean EJIE] Segurtasun eta Pribatutasun Korporatiboaren 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, 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 eskuduna den 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 EAEko Administrazio Publikoak ezarritako eginkizun nahiz segurtasun arloko baldintzak. EJIEko zuzendari nagusiak Segurtasun eta Pribatutasun Korporatiboaren Batzordean parte hartu beharko du, eta EJIEko segurtasuneko arduradunak Segurtasun Batzorde Teknikoan. EJIEk aplikatu egin beharko ditu informazioaren eta komunikazioen teknologietan eskuduna den zuzendaritzak bere ahalmen ekonomikoarekin bat etorrita definitutako segurtasun-neurri teknikoak, Segurtasun eta Pribatutasun Korporatiboaren Batzordean ezartzen denaren arabera. EJIEk Segurtasun eta Pribatutasun Korporatiboaren 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 *Segurtasuna eta pribatutasuna koordinatzeko organoen egitura*

Segurtasuna koordinatzeko, kide anitzeko erakunde hauek sortzen dira:

#	Erakundea	Titularrak	Eginkizunak
1	Segurtasun eta Pribatutasun Korporatiboaren Batzordea.	1. Segurtasunaren eta sistemen arduraduna, Batzordeko buru izango dena. 2. Zerbitzu komunen arduradunak. 3. Pribatutasun-neurrien eta informazioaren arduradunak. 4. Sistemen ustiapenaren arduraduna. 5. Datuak babesteko ordezkaria.	Segurtasunaren eta pribatutasunaren arloan Administrazio Elektronikoaren eraginpean dauden guztien interesak zuzendu eta koordinatzea: 1) Administrazio Elektronikoaren eraginpean dauden guztien artean (sailak, erakunde autonomoak, zuzenbide pribatuko erakundeak 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 erreferentzia diren pertsonak.	1) Datuak babesteko ordezkariarekin koordinazioan aritzea, datuak babesteko politiketan eta horien aplikazioan. 2) Datuak babesteko ordezkariaren jarraibideak jakinaraztea, dagokien pertsonek beren jarduerak eraginkortasunez koordinatuta egin ditzaten. 3) Datuak Babesteko Batzordeko gainerako kideen aurrean azaltzea sail, erakunde autonomo edo zuzenbide pribatuko ente publiko bakoitzeko tratamenduaren arduradunek planteatu dituzten gaiak, doktrina bateratze aldera, baldin eta datuak babesteko ordezkariak hala eskatzen badu. 4) Datuak babestearen gainean sortu diren informazio esanguratsuak aztertzea. 5) Kontrol-erakundeek eta beste administrazio publiko batzuek datu pertsonalak babestearekin lotuta egin dituzten interpretazioak edo/eta azken aurrerapenak aztertzea.

#	Erakundea	Titularrak	Eginkizunak
3	Segurtasuneko Batzorde Teknikoa	1. Informazioaren eta komunikazioaren teknologietan eskumena duen Zuzendaritzako kide bat. 2. Administrazio elektronikoan eskumena duen Zuzendaritzako kide bat. 3. Dokumentuen kudeaketan eskumena duen Zuzendaritzako kide bat. 4. Ondarearen segurtasunean eskumena duen Zuzendaritzako kide bat. 5. EAEko Administrazio Publikoko informatika-arloko edota segurtasuneko arduradun guztiak. 6. EJIEko segurtasun-arduraduna	Administrazio elektronikoaren segurtasuna koordinatzea inplikatutako organoen artean: • EJIEk eta EAEko Administrazio Publikoak administrazio elektronikoaren segurtasunaren arloan dauzkaten beharrizanak artatzea. • Segurtasun eta Pribatutasun Korporatiboaren Batzordeari aldiro segurtasunaren egoeraren berri ematea. • EAEko Administrazio Publikoaren segurtasuna kudeatzeko prozesuaren etengabeko hobekuntza sustatzea. • EAEko Administrazio Publikoaren 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 daitezen eta definitutako estrategiarekin lerrokatuta egon daitezen saiatzea. • Euskal Administrazio Publikoak 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. • EAEko Administrazio Publikoaren segurtasun-auditoretzen programa egin dadila bultzatzea. • Segurtasun arloko jardueren artean lehentasunak ezartzea, baliabideak mugatuak direnean. • Kide diren entitateen bitartez, maila teknikotik kanpo definitzen diren segurtasun-neurriak aplikatzea. • IKT proiektu guztietan, hasieran zehazten direnetik martxan jartzen diren arte, informazioaren segurtasuna kontuan hartzen dela zaintzea. • Arduradunen artean eta/edo sail, erakunde autonomo edo zuzenbide pribatuko erakunde publikoen artean segurtasun arloan ager daitezkeen gatazkak tratatzea, eta kasu batean erabakitzeko aginte nahikorik ez badu, kasu hori Segurtasun eta Pribatutasun Korporatiboaren Batzordeari igortzea. Burua segurtasunaren arduraduna izango da, edo zuzendaritzako kide bat, zuzendaritzak berak izendatua, eta urtean birritan egingo du bilera.

3.6 *Arriskuen analisia eta kudeaketa.*

Arriskuen kudeaketa segurtasun-prozesuko funtsezko atal bat da eta etengabe egin behar da informazio-sistemen eta datu pertsonalen tratamenduen gainean. Helburu nagusia inguruak kontrolatuta mantentzea da, tratamenduak pertsona fisikoen eskubide eta askatasunetan eragin ditzakeen arriskuak ebaluatzea eta hautemandako arriskuak maila onargarrietara murriztea. Nahitaezkoa izango da ENS arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuak ezarritako esparruaren barruko informazio-sistemetarako.

Informazioaren eta zerbitzuen arduradunak informazioaren eta zerbitzuen inguruko arriskuez arduratzen dira, hurrenez hurren, eta jarraipena eta kontrola bermatzen dituzte. Nolanahi ere, egiteko horiek eskuordetu ahal dituzte. Horretarako, prozesuan segurtasunaren arduradunaren eta sistemen ustiaketaren arduradunaren partaidetza eta aholkularitza eduki ahal izango dituzte.

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.

EAEko Administrazio Publikoak konpromisoa dauka eta informazioaren arduradunek, aldiz, betebeharra, arriskuak aztertzekoa eta ondorioak aintzat hartzeko. Politika honi lotutako sistema guztiek arriskuen analisia egin beharko dute, aktiboek jasan ditzaketen mehatxuak eta arriskuak ebaluatuz. Analisi hori errepikatu egingo da:

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

3.7 *Segurtasuneko beste betekizun batzuk*

ENSri buruzko Errege Dekretuaren 12. artikulua betez, segurtasun- eta pribatutasun-politika hau garatzeko, aurreko kapituluetan ikusitako betekizunez gain, gutxieneko hauek beteko dira:

- Segurtasun-prozesua antolatzea eta ezartzea

Informazio-sistemen segurtasunak EAEko Administrazio Publikoko kide guztiak konprometitzen ditu, eta dokumentu honetan pertsona bakoitzaren rolak eta erantzukizunak definitzen dira, beren rolen arabera.

Bestalde, aurreko paragrafoetan adierazi den bezala, **GureSeK** izena ematen zaio EAEko Administrazio Publikoak herritarrei ematen dizkieten zerbitzu elektronikoen segurtasuna eta pribatutasuna kudeatzeaz arduratzen den segurtasunaren kudeaketarako prozesuari.

- Langileen kudeaketa.

EAEko Administrazio Publikoko langile guztiei, barnekoei zein kanpokoei, beren eginbeharren, betebeharren eta erantzukizunen berri eman eta prestakuntza ematen zaie.

- Profesionaltasuna.

EAEko Administrazio Publikoko sistemen segurtasuna langile kualifikatuek zaindu, berrikusi eta ikuskatuko dute beti, eta horretan jardungo dute eta trebatuko dira sistemen bizi-zikloaren fase guztietan: instalazioan, mantentze-lanetan, gorabeheren kudeaketan eta eraispenean.

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

- Sartzeko baimenak ematea eta kontrolatzea

Informazio-sistemetarako sarbidea kontrolatu egingo da, eta erabiltzaileei, prozesuei, gailuei eta bestelako informazio-sistemei mugatuko zaie, behar bezala baimenduta eta sarbide mugatuarekin.

- Instalazioak babestea.

EAEko Administrazio Publikoaren instalazioetan sarbideak kontrolatzeko puntuak egongo dira.

- Segurtasun-produktuak eskuratzea eta segurtasun-zerbitzuak kontratatzea.

EAEko Administrazio Publikoak erabiliko dituen informazioaren eta komunikazioaren teknologien segurtasun-produktuak eskuratzeko, sistemaren kategoria eta zehaztutako segurtasun-maila hartuko dira kontuan eta erosketa horietarako garatutako gida jarraituko da.

- Gutxieneko pribilegioa.

Informazio-sistemak behar bezala jarduteko behar diren gutxieneko pribilegioak emanez diseinatzen eta konfiguratzen 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, ahuleziei eta eragiten dieten eguneratzeei dagokienez, eta arduraz erreakzionatuko da arriskua kudeatzeko, horien segurtasun-egoera ikusita.

- Informazioa babestea, gordeta dagoela zein transmisioetan.

Sistemaren segurtasunaren egituran eta antolaketan, arreta berezia jarriko zaio gordeta dagoen edo ingurune ez-seguruetan transmisioan dagoen 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

- Jardueraren erregistroa eta kode kaltegarriaren detekzioa

Eragindakoen ohorerako, norberaren eta familiaren intimitaterako eta norberaren irudirako eskubidea erabat bermatuta, eta datu pertsonalak babesteari buruzko araudiarekin, funtzio publikoaren araudiarekin eta aplikatzekoak diren gainerako xedapenekin bat etorriz, erabiltzaileen jarduerak erregistratu egingo dira, eta bidegabeko edo baimenik gabeko jarduerak monitorizatzeko, aztertzeko, ikertzeko eta dokumentatzeko beharrezkoa den informazioa gordeko da, jarduten duen pertsona une bakoitzean identifikatzeko aukera emanez.

- Segurtasun-gorabeherak.

Segurtasun-gorabeherak kudeatzeko prozedura espezifikoak ezarriko dira.

- Jardueraren jarraitutasuna.

Sistemetan segurtasun-kopiak egingo dira, eta mekanismo egokiak ezarriko dira ohiko lan-baliabideak galduz gero eragiketak egiten jarraitu ahal izango dela bermatzeko.

- Segurtasun-prozesua etengabe hobetzea.

EAEko Administrazio Publikoak etengabe eguneratzen eta hobetzen ditu bere sistemak.

3.8 *Segurtasun- eta pribatutasun-politika berrikusteko prozesua*

EAEko Administrazio Publikoak definitutako segurtasun- eta pribatutasun-politika eta segurtasun- eta pribatutasun-araudia berrikusi behar dira, eta egunera daitezen bultzatu.

Segurtasun eta Pribatutasun Korporatiboaren 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, eragindako 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- eta pribatutasun-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, EAEko Administrazio Publikoaren 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 betetzen dela bermatzeko kontrol-prozedurak ezarri beharko dira, eta sail, erakunde autonomo eta zuzenbide pribatuko erakunde publikoek egingo dituzte.

3.10 *Kontzientziazioa eta prestakuntza*

Korporazioaren Segurtasun eta Pribatutasun Batzordeak sustatu behar ditu informazioaren segurtasunaren eta pribatutasunaren arloan trebatzea eta kontzientzia hartzea, EAEko Administrazio Publikoaren eremuan.

Jarduera espezifikoak egingo dira, langile guztiei informazioaren segurtasunaren 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 segurtasunari eta pribatutasunari buruzko jarduera espezifikoak sartuko dira.

EAEko Administrazio Publikoan informazioaren segurtasunaren eta pribatutasunaren arloko prestakuntza-programa Administrazio Publikoaren Euskal Institutuak (IVAP) emango du, eta erakunde autonomo horren zeharkako prestakuntza-programaren barruan egongo da. Prestakuntza hori, halaber, datuak babesteko ordezkariaren eginkizuna izango da.

3.11 *Hirugarren alderdiak*

EAEko Administrazio Publikoak hirugarren alderdien zerbitzuak edo informazioa erabiltzen dituenean, hirugarren horiei informazioaren segurtasun- eta pribatutasun-politika honen berri emango die. Segurtasun eta Pribatutasun Batzorde Teknikoak oharretarako eta koordinaziorako kanalak ezarriko ditu, eta segurtasun- eta pribatutasun-gorabeheren aurrean erantzuteko jarduketa-prozedurak ezarriko ditu.

EAEko Administrazio Publikoak beste erakunde batzuei zerbitzuak ematen dizkienean, informazioaren segurtasun- eta pribatutasun-politika horren berri emango die, baita zerbitzu horiei edo informazio horri dagozkien Jarraibide eta Prozeduren berri ere.

EAEko Administrazio Publikoak hirugarren alderdiei 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, hirugarren alderdien 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 osagai, funtzio edo bitarteko bat da: esaterako, informazioa, datuak, zerbitzuak, aplikazioak, ekipamenduak, komunikazioak, administrazio-baliabideak, baliabide fisikoak edota giza baliabideak.
2	Mehatxua	Informazio-sistema bati edo erakunde bati kalte egin ahal dion gorabehera baten kausa [UNE 71504:2008]. Mehatxuak beti daude presente, baina saihestu daitezke edo ondorioak arindu, gauzatzen badira.
3	Arriskuen azterketa	Informazio-sistema batek izan ditzakeen mehatxuak, ahulguneak, arriskuak eta eraginak aztertzeko prozesua, kontuan hartuta jada ezarrita dauden segurtasun-neurriak. Abiapuntutzat hartzen da segurtasun-neurrien eraginkortasuna eta kostua hobetzeko alderdiak zehazteko.
4	Benetakotasuna	Entitate batek adierazitako identitatea egiazkoa dela edo datuen iturria bermatzen duela adierazten duen ezaugarria [ENS].
5	Konfidentzialtasuna	Informazioa baimendu gabeko pertsonen, erakundeen edo prozesuen eskura ez dela jartzen, ez jakinarazten adierazten duen ezaugarria [ENS].
6	Araudia	Politika baten helburuak lortzeko modua zehatzago garatzen duten arauen multzoa.
7	Datu pertsonalak	Identifikatutako edo identifika daitezkeen pertsona fisikoei buruzko edozein informazio.
8	Eskuragarritasuna	Entitate edo prozesu baimendunek behar dutenean aktiboetara irispidea dutela adierazten duen ezaugarria [ENS].
9	ENS	Segurtasunaren Eskema Nazionala.
10	Jarraitutasunaren kudeaketa	Negozio-prozesu kritiko guztiak erabiltzaileentzat, bezeroentzat, hornitzaileentzat eta prozesu horiek erabili behar dituzten beste erakunde batzuentzat eskuragarri egongo direla ziurtatzeko erakunde batek egiten dituen jarduerak.
11	Gorabeherak kudeatzea	Zerbitzuaren ohiko funtzionamendua lehengoratzea eta ahal den neurrian erakundearen segurtasun-akats baten ondoriozko eragin txarra murriztea xede duten prozesuak, zerbitzuaren kalitatea eta eskuragarritasuna mantentzeko helburuz.
12	Arriskuen kudeaketa	Erakunde bat arriskuen aurrean gidatzeko eta kontrolatzeko jarduera koordinatuak [ENS].

#	Terminoa	Definizioa
13	Segurtasun-intzidentea	Ezusteko edo nahi gabeko gertakaria, informazio-sistemaren segurtasunari kalte egiten diona [ENS].
14	Osotasuna	Informazioaren aktiboa baimenik gabe ez dela aldatu adierazten duen ezaugarria [ENS].
15	Segurtasun-neurriak	Informazio-sistemak izan ditzakeen arriskuetatik babesteko xedapenak, sistemaren segurtasun-helburuak ziurtatzeko hartuta. Hainbat neurri mota izan daitezke: prebentziozkoak, disuasiozkoak, babesgarriak, detekziozkoak eta erreakziozkoak edo berreskuratzekoak [ENS].
16	Segurtasun- eta pribatutasun-politika	Maila handiko dokumentua, erakunde batek segurtasun eta pribatutasun arloan dituen helburuak azaltzen dituena eta zuzendaritzak helburu horiek betetzeko duen konpromisoa agerrarazten duena.
17	Prozesua	Produktu edo zerbitzu bat sortzeko egiten diren jardueren multzo antolatua. Prozesuak hasiera eta amaiera jakin bat du, baliabideak erabili beharra eskatzen du, eta emaitza bat dakar beti [ENS].
18	Arriskua	Mehatxu batek erakundearen aktibo bati edo gehiagori ekar diezaiekeen kalteen probabilitatearen estimazioa [ENS].
19	Hondar-arriskua	Informazioaren segurtasunerako planean zehaztutako zaintzak ezarri ostean sisteman geratzen den arriskua.
20	Informazioaren segurtasuna	Informazioa eta informazio-sistemak babestea baimendu gabeko atzipen, erabilera, dibulgazio, aldaketa edo suntsipenaren aurka.
21	Informazio-sistema	Informazioa bildu ahal izateko, eta, orobat, biltegiratu, prozesatu edo tratatu, mantendu, erabili, partekatu, banatu, eskuragarri jarri, aurkeztu edo transmititu ahal izateko antolatutako baliabide-multzoa [ENS].
22	Euskarria	Informazioa biltegiratzeko erabilitako edozein motatako bitarteko fisikoa (papera, USBak, DVDak, disko eramangarriak eta abar).
23	Trazabilitatea	Entitate baten jardunak entitate horri baino ez dakizkiokeela egotzi adierazten duen ezaugarria [ENS].
24	Ahultasuna	Aktibo baten ahulgunea, mehatxu batek aprobetxatu ahal duena [ENS].