

I - ARABAKO BATZAR NAGUSIAK ETA ARABAKO LURRALDE HISTORIKOAREN FORU ADMINISTRAZIOA

Arabako Foru Aldundia

ENPLEGU, MERKATARITZA, TURISMO ETA FORU ADMINISTRAZIOAREN SAILA

27/2026 Foru Dekretua, uztailaren 28koa, Foru Gobernu Kontseiluarena. Onestea Arabako Foru Aldundiaren datu pertsonalak babesteari eta informazioaren segurtasunari buruzko politika

Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamenduak, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoak eta 95/46/EE Zuzentaraua indargabetzen duenak (aurrerantzean, DBEO), 24. artikuluan ezartzen duenez, datu pertsonalen tratamenduaren arduradunaren betebeharrak orokorrean esparruan, tratamenduaren izaera, eremua, testuingurua eta helburuak kontuan hartuta, bai eta pertsona fisikoaren eskubide eta askatasunetarako hainbat mailatako probabilitate eta larritasuneko arriskuak ere, tratamenduaren arduradunak neurri tekniko eta antolamendu neurri egokiak aplikatuko ditu, tratamendua aipatutako erregelamenduekin bat datorrela bermatzeko eta egiaztatu ahal izateko. Hala berean, ezartzen du neurri horiek berrikusi eta eguneratu egingo direla beharrezkoa denean, eta, tratamendu jardueri dagokienez neurrizkoak direnean, neurri horien artean jasoko dela tratamenduaren arduradunak datuak babesteko politika egokiak aplikatzeko beharra.

Ildo berean, Datu Pertsonalak Babesteari eta Eskubide Digitalak Bermatzeari buruzko abenduaren 5eko 3/2018 Lege Organikoaren (aurrerantzean, DPBEBLO) 28. artikulua betebeharrak orokor gisa ezartzen ditu, bai tratamenduaren arduradunarentzat, bai eragilearentzat, eta DBEOren 24. eta 25. artikuluetan ezarritakoa aintzat hartuta, aurrekoek zehaztutako aplikatu beharreko neurri tekniko eta antolamendu neurri egokiak, tratamendua DBEOrekin, DPBEBLOrekin, haren garapen arauarekin eta aplikatzeko den sektoreko legeriarekin bat datorrela bermatzeko eta egiaztatzeko.

Beste alde batetik, Administrazio Publikoen Administrazio Prozedura Erkidearen urriaren 1eko 39/2015 Legearen 13. artikulua, pertsonen administrazio publikoekiko harremanetan dituzten eskubideei buruzkoak, berariaz jasotzen du datu pertsonalak babesteko eskubidea, eta, bereziki, administrazio publikoen fitxategi, sistema eta aplikazioetan agertzen diren datuen segurtasun eta konfidentzialtasunerako eskubidea.

Gainera, Sektore Publikoaren Araubide Juridikoaren urriaren 1eko 40/2015 Legearen 3.2 artikulua xedatzen duenez, administrazio publikoak harremanetan jarriko dira elkarren artean eta haiei atxikitako edo haien mendeko organoekin, organismo publikoekin eta entitateekin bitarteko elektronikoak erabiliz, betiere administrazio bakoitzak erabakitako sistemen eta itenbideen elkarrengarritasuna eta segurtasuna ziurtatuta, datu pertsonalen babesa bermatuko dute eta interesdunei zerbitzuak batera ematea lehenetsiko dute. Horren haritik, lege horren 156. artikulua xedatzen du Segurtasun Eskema Nazionalaren xedea dela sektore publikoan bitarteko elektronikoak erabiltzeko segurtasun politika ezartzea, eta tratatutako informazioaren segurtasuna behar bezala bermatzen duten oinarriko printzipioek eta gutxieneko baldintzek osatzen dutela.

Administrazio elektronikoaren esparruan, Segurtasun Eskema Nazionala (aurrerantzean, SEN) arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuak xedatzen duenez, administrazio publikoek segurtasun neurriak aplikatu behar dituzte, bai eta zerbitzuen prestazio mailen etengabeko jarraipena egin, antzemandako kalteberatasunak jarraitu eta aztertu, eta gertakariei erantzun eraginkorra prestatu ere, emandako zerbitzuen jarraitutasuna bermatzeko. Esparru horretan, informazioaren segurtasun politika da SENen ezarritako segurtasun tresnak eta prozedurak definitzea, kudeatzea, administratzea eta inplementatzea helburu duten erreferentziatzeko esparrua.

Bi arlo horien arteko lotura hertsia kontuan hartuta, hau da, datu pertsonalen babesa eta informazioaren segurtasunaren kudeaketa, eta eremu bakoitzeko politikak ezartzeko betebeharra, komenigarritzat jotzen da datuak babesteko eta informazioaren segurtasuna bermatzeko politika bateratua lantzea. Horrenbestez, datuak babesteko eta informazioaren segurtasuna bermatzeko politika da Arabako Foru Aldundiaren datu pertsonalen tratamendu jardueren eta informazio sistemen testuinguruan datuen babesa eta informazioaren segurtasuna kudeatzeko erreferentziatzeko esparrua definitzen duen oinarritzko dokumentua.

Foru dekretu hau bat dator 39/2015 Legearen 129. artikuluan jasotako eta Arabako Foru Aldundiaren xedapen orokorrak egiteko prozedura onartzen duen otsailaren 28ko 6/2023 Foru Dekretuaren 3. artikuluan jasotzen diren erregulazio onaren printzipioekin. Bereziki, beharraren, eraginkortasunaren, proportzionaltasunaren, segurtasun juridikoaren, gardentasunaren eta efizientziaren printzipioekin.

Hala, azaldutako aurrekarietan behar bezala justifikatu da datuak babesteko eta informazioaren segurtasuna bermatzeko politika berria onartzeko beharra, eta, gainera, hori lortzeko tresna egokiena da, bai eta araugintza jarduera proportzionatua ere, lortu nahi den helburua lortzeko ezinbestekoa den gutxienez mugatzen baita. Era berean, segurtasun juridikoaren printzipioa bermatzen da, eta berariaz indargabetzen dira Arabako Foru Aldundiaren datuen babesaren arloko aurreko segurtasunaren eta segurtasun egituraren politika onartzen zuten akordioak. Gardentasun printzipioari dagokionez, esan behar da ez dela urratu; izan ere, antolamenduzko edukia denez, alde aurreko kontsulta publikoaren eta entzunaldiaren eta jendaurreko informazioaren izapideak alde batera utz daitezke, eta, nolana ere, ALHAOn argitaratu egingo da manua onetsi eta berehala. Efizientzia printzipioari doakionez, proposatzen den erregulazioak ez dakar administrazio kargarik, ezta herritarrentzat alferrikakoa den kargarik ere. Azkenik, bakuntasun eta ulergarritasun printzipioei dagokionez, proposatutako testua modu egituratuan idatzi da, hizkuntza argia eta ulergarria erabiliz.

Ondorioz, Enplegu, Merkataritza, Turismo eta Foru Administrazioaren foru diputatuaren eta Berdintasun, Euskara eta Gobernantzako foru diputatuaren proposamenez, Foru Gobernuaren Kontseiluak gaur egindako bilkuran eztabaidatu ondotik, honako hau

XEDATZEN DUT

1. artikulua. Xedea eta aplikazio eremua

1. Foru Dekretu honen xedea da Arabako Foru Aldundiaren datuak babesteko eta informazioaren segurtasuna bermatzeko politika onestea. Politika hori dugu datu pertsonalen tratamenduari aplikatu beharreko araudia betetzen dela bermatzeko neurri tekniko eta antolaketa neurri egokien multzoa, bai eta Arabako Foru Aldundiaren eremuan kudeatzen den informazioa behar bezala babestea ahalbidetzen duten oinarritzko printzipioak eta gutxienezko baldintzak ere.

2. Politika hori Arabako Foru Aldundiaren ardurapeko informazio sistema guztiei eta datu pertsonalak tratatzeko jarduera guztiei aplikatuko zaie.

3. Arabako Foru Aldundiaren egitura organikoa osatzen duten unitate guztiek nahitaez bete beharko dute politika hori. Arabako gainerako foru sektore publikoa datuak babesteko eta informazioaren segurtasuna bermatzeko politika honi atxiki ahalko zaio, atxikitzeko protokoloa formalizatuz (l. eranskina).

4. Datu pertsonalak babesteak eta informazioaren segurtasuna babesteak Arabako Foru Aldundiko langile guztiei eragiten eta behartzen ditu, bai eta Aldundian zerbitzuak ematen dituzten edo harreman juridiko egokia duten hirugarren pertsonak ere.

5. DBEOren eta SENen aplikazio materialaren eremuan, politika honek Arabako Foru Aldundiak bere eskumenak erabiliz kudeatzen duen edozein bitartekoren bidez tratatutako informazioari eragingo dio, euskarria edozein dela ere.

2. artikulua. Arau esparrua

1. Politika hau honako legeria honetan eta arau aplikagarrietan oinarritzen da:

— Europako Parlamentuaren eta Kontseiluaren 2022/2555 (EB) Zuzentaraua, 2022ko abenduaren 14koa, Batasun osoan zibersegurtasun maila komun handia bermatzeko neurriei buruzkoa.

— Europako Parlamentuaren eta Kontseiluaren 2016/679 (EB) Arautegia, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa (DBEO).

— Europako Parlamentuaren eta Kontseiluaren 910/2014 (EB) Erregelamendua, 2014ko uztailaren 23koa, barne merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantzazko zerbitzuei buruzkoa eta 1999/93/EE Zuzentaraua indargabetzen duena.

— 3/2018 Lege Organikoa, abenduaren 5koa, datu pertsonalak babesteko eta eskubide digitalak bermatzeko (DPBEDBLO).

— 7/2021 Lege Organikoa, maiatzaren 26koa, arau hauste penalak prebenitzeko, detektatzeko, ikertzeko eta epaitzeko eta zehapen penalak betearazteko tratatzen diren datu pertsonalak babesteari buruzkoa.

— 16/2023 Legea, abenduaren 21koa, Datuak babesteko euskal agintaritzarena.

— 39/2015 Legea, urriaren 1koa, Administrazio Publikoen Administrazio Prozedura Erki-dearena.

— 40/2015 Legea, urriaren 1koa, Sektore Publikoaren Araubide Juridikoarena.

— 9/2017 Legea, azaroaren 8koa, Sektore Publikoko Kontratuena, Europako Parlamentuaren eta Kontseiluaren 2014ko otsailaren 26ko 2014/23/EB eta 2014/24/EB zuzentzarauen transposizioa egiten duena Espainiako ordenamendu juridikora.

— 34/2002 Legea, uztailaren 11koa, informazioaren gizarteko zerbitzuei eta merkataritza elektronikoari buruzkoa.

— 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasunaren Eskema Nazionala (SEN) arautzen duena.

— 4/2010 Errege Dekretua, urtarrilaren 8koa, administrazio elektronikoaren elkarrengarritasunerako eskema nazionala arautzen duena.

— 203/2021 Errege Dekretua, martxoaren 30koa, sektore publikoan baliabide elektronikoak erabiliz jarduteko arautegia onartzen duena.

— 1/2017 Foru Araua, otsailaren 8koa, Arabako Lurralde Historikoko sektore publikoaren gardentasunarena, herritarren parte-hartzearena eta gobernu onarena.

— 91/2023 Dekretua, ekainaren 20koa, herritarrei arreta integrala eta kanal anitzekoa emateari eta zerbitzu publikoak bitarteko elektronikoaren bidez eskuratzeari buruzkoa.

— Segurtasuna kudeatzeko nazioarteko estandarrak (ISO/IEC 27001:2022, 27002:2022, 31000:2010, 22301:2020, NIST SP 800-53).

— Aplikatu beharreko gainerako arauak.

2. Arau esparru hau osatzen duten arauak erregistro batean jasotzen dira ondorio horietarako, eta erregistro hori eguneratuta egongo da.

3. artikulua. Datuak babesteko eta informazioaren segurtasuna bermatzeko printzipioak

Arabako Foru Aldundiak honako printzipio hauen arabera tratatuko ditu informazioa eta datu pertsonalak:

1. Zilegitasuna, leialtasuna eta gardentasuna: datu pertsonalak modu zilegian, leialean eta gardenean tratatuko dira interesdunarekin. Helburua mugatzea: datu pertsonalak helburu jakin, esplizitu eta legitimoak betetzeko tratatuko dira, eta ez dira geroago tratatuko helburu horiekin bateraezina den moduan.

2. Datu pertsonalak hasieran jaso ez diren helburuetarako tratatzeko baimena eman behar da soil-soilik hasierako bilketaren helburuekin bateragarria denean eta datuak babesteko araudian ezarritako baldintzak eta betekizunak betetzen direnean.

3. Datuak minimizatzea: datu pertsonalak aproposak, egokiak eta mugatuak izango dira, tratatzen diren helburuei dagokienez.

4. Zehaztasuna: datu pertsonalak zehatzak izango dira, eta, beharrezkoa bada, eguneratuak. Zentzuzko neurri guztiak hartuko dira datu pertsonalak, tratatzen diren helburuei dagokienez okerrak direnean, berehala ezabatu edo zuzentzeko.

5. Datuak gordetzeko epea mugatzea: datu pertsonalak gorde egingo dira, interesdunak identifikatu ahal izateko moduan, tratamendua justifikatu zuten helburuetarako behar den denboran baino ez.

6. Osotasuna eta konfidentzialtasuna: datu pertsonalak datuen segurtasuna bermatzeko moduan tratatuko dira, baimenik gabeko edo legez kontrako tratamenduaren aurkako babesa eta ustekabeko galeraren, suntsiketaren edo kaltearen aurkako babesa aintzat hartuta, neurri tekniko edo antolaketa neurri egokiak aplikatuz.

7. Datuen tratamenduan esku hartzen dutenek sekretua gordetzeko eginbeharra izango dute, bai eta datuon tratamendua justifikatu zuen harremana amaitu ondoren ere.

8. Erantzukizun proaktiboa: Arabako Foru Aldundia arduratuko da artikulua honetan aipatutako printzipioak betetzeaz, eta antolaketa neurriak, operatiboak eta teknikoak hartuko ditu, betetze hori frogatzeko moduan egon dadin.

9. Eragindako pertsonen eskubideak kontuan hartzea: neurriak hartuko dira erakundean, hala bidezkoa denean, eragindako pertsonen datu pertsonalak eskuratzeko, datuak zuzentzeko, ezabatzeko, datuen aurka egiteko, tratamendua mugatzeko eta datu horien eramangarritasuna bermatzeko eskubideak egoki egikaritzea izan dezaten.

10. Irismen estrategikoa: datuen babesak eta informazioaren segurtasunak zuzendaritza maila guztien konpromisoa eta laguntza izan behar dute, Arabako Foru Aldundiaren gainerako ekimen estrategikoekin koordinatuta eta integratuta egon ahal izateko, osotasun koherente eta eraginkorra osatzeko xedez.

11. Erantzukizun bereizia: Arabako Foru Aldundiaren ardurapeko informazio sistemetan, erantzukizun bereziaren printzipioa beteko da, erantzukizunak eta rola mugatzeko:

a. Tratamenduaren arduraduna: tratamenduaren helburuak eta bitartekoak zehazten dituen pertsona.

b. Tratamenduaren eragilea: datu pertsonalak tratatzen dituen pertsona, tratamenduaren arduradunaren kontura, aurrekoaren eskakizunei jarraikiz.

c. Datuak babesteko ordezkaria: datuen tratamenduaren arduradunari DBEO betetzeko bete-beharren berri ematen dion pertsona.

d. Informazioaren arduraduna: tratatzen den informazioaren segurtasun betekizunak zehazten dituen pertsona.

e. Zerbitzuaren arduraduna: informazioan oinarrituta, emandako zerbitzuen betekizun funtzionalak eta segurtasunekoak zehazten dituen pertsona.

f. Informazioaren segurtasunaren arduraduna: segurtasun baldintzak betetzeko erabakiak hartzen dituen pertsona.

g. Sistemaren arduraduna: zerbitzuak emateko erabiltzen diren informazio sistemen eskakizun ez-funtzionalen eta diseinu, eraikuntza, eragiketa eta euskarriari loturiko betekizunen erantzukizuna duen pertsona.

12. Segurtasun integrala: segurtasuna prozesu integrala da, eta informazio sistemei lotutako elementu tekniko, giza elementu, elementu material, juridiko eta antolamenduzko guztiek osatzen dute. Politika honen aplikazioan, printzipio hau gailenduko da, edozein unean uneko jarduera edo egoeraren arabera tratamendu baxter utzita. Informazioaren segurtasunaren eta datu pertsonalen babesaren arloan indarrean dagoen araudia betetzeko beharrezkoak diren neurri teknikoak, antolakuntzakoak eta prozedurazkoak hartuko dira.

13. Arriskuen arabera segurtasunaren kudeaketa: interesdunen eskubideak eta askatasunak babesten dituen segurtasun prozesua, bai eta Arabako Foru Aldundiaren aktiboak ere, arriskua maila onargarrietaraino minimizatu ahal izateko kudeaketan oinarrituko dira, funtzionaltasunaren, datuen izaeraren, tratamenduen eta aplikatu beharreko kontrol neurrien arteko orekari eutsiz.

14. Arriskuen analisia eta kudeaketa: arriskuen analisia eta kudeaketa segurtasun prozesuaren funtsezko zatia izango da, eta etengabeko jarduera eguneratua izango da. Arriskuen kudeaketak ingurune kontrolatua izateko modua emango du, arriskuak maila onargarrietan minimizatuz. Maila horiek murrizteko, segurtasun neurriak behar bezala aplikatuko dira, tratatu beharreko informazioaren, eman beharreko zerbitzuen eta izan ditzaketen arriskuen izaeraren arabera.

15. Proportzionaltasuna: Arabako Foru Aldundiak babes, detekzio eta lehengoratzeko neurriak ezarriko ditu, balizko arriskuekiko eta informazioaren, datu pertsonalen tratamenduen eta eragindako zerbitzuen kritikotasun eta balioarekiko proportzionalak.

16. Datuen babesa eta segurtasuna diseinutik abiatuta eta lehenespenez: Arabako Foru Aldundiak datuen babesaren printzipioa sustatu eta lehenetsiko du diseinutik bertatik abiatuta, datuen babesa eta informazioaren segurtasuna lehenespenez aintzat hartu dadin datu pertsonalen tratamendu eta informazio sistema guztien diseinutik bertatik.

17. Egiaztatze-prozesua: Arabako Foru Aldundiak tratamenduen segurtasuna bermatzeko neurri teknikoak eta antolakuntzakoak eraginkortasuna egiaztatze, ebaluatze eta baloratzeko arauzko prozesua ezarriko du.

18. Informazio aktiboen segurtasuna: informazio aktiboetarako eta datu pertsonaletarako sarbidea duten pertsonak beren betebeharrak eta erantzukizunak berri izan dezaten beharrezkoak diren neurri teknikoak eta antolakuntzakoak ezarriko dira, eta, horrela, aktibo horiek behar bezala erabiltzearen ziozko arriskua murriztuko da.

19. Segurtasun fisikoa: informazio aktiboak eremu seguruetan kokatuko dira, beren kritikotasun mailari egokitutako sarbide kontrol fisikoen bidez babestuta. Eremu horietan dauden informazio sistemak eta aktiboak behar bezala babestuta egongo dira mehatxu fisikoen edo ingurumen-mehatxuen aurrean.

20. Komunikazioen kudeaketaren segurtasuna: informazioaren eta komunikazioen teknologien segurtasuna, eragiketa eta eguneratzea behar bezala kudeatzeko beharrezkoak diren prozedurak ezarriko dira. Komunikazio sareen bidez transmititzen den informazioa behar bezala babestu beharko da, haren sentikortasun eta kritikotasun maila kontuan hartuta, informazioaren segurtasuna bermatzen duten tresnak erabiliz.

21. Sarbideen kontrola: erabiltzaileek, prozesuek eta bestelako informazio sistemek duten informazio aktiboetarako sarbidea mugatuko da, aktibo bakoitzaren kritikotasunarekin bat datozen identifikazio, autentifikazio eta baimen mekanismoak ezarriz. Gainera, sistemaren erabilera erregistratuta geratuko da, sarbidearen trazabilitatea ziurtatzeko eta haren erabilera egokia ikuskatzeko, erakundearen jardueraren arabera.

22. Sistemaren informazioa atzitzen duen pertsona bakoitzak modu bakarrean identifikatuta egon behar du, zuzentzeko edo, hala badagokio, erantzukizunak eskatzeko; horrela, une oro jakin ahalko da sarbide eskubideak nork jasotzen dituen, eskubide horiek zer motatakoak diren eta jarduera jakin bat nork egin duen.

23. Segurtasun gertakariak kudeatzea: segurtasun gertakariak behar bezala identifikatzeko, erregistratzeko, ebazteko eta jakinarazteko tresna egokiak ezarriko dira, datuen babesari eta informazioaren segurtasunari buruzko araudian aurreikusitako baldintzetan.

24. Jarraitutasunaren kudeaketa: informazio sistemen erabilgarritasuna ziurtatzeko eta negozio prozesuen jarraitutasunari heltzeko tresna egokiak ezarriko dira, Arabako Foru Aldundiaren zerbitzu mailako premien arabera.

25. Informazio sistemak eskuratzea, garatzea eta mantentzea: informazio sistemen bizi zikloaren fase guztietako informazioaren segurtasun alderdiak hartuko dira kontuan, lehenetsitako segurtasuna bermatuz.

26. Betetzea: informazioaren segurtasunaren eta datu pertsonalen babesaren arloan indarrean dagoen legezko araudia betetzeko beharrezkoak diren neurri teknikoak, antolakuntzakoak eta prozedurazkoak hartuko dira.

4. artikulua. Datu pertsonalak babesteko eta informazioaren segurtasuna bermatzeko politika korporatiboa

Arabako Foru Aldundiaren datu pertsonalak babesteko eta informazioaren segurtasuna bermatzeko politika korporatiboa osorik onartu eta argitaratzen da foru dekretu honen II. eranskin gisa.

5. artikulua. Antolamendu egitura

Datuak babesteko eta informazioaren segurtasuna bermatzeko politikaren esparruan, informazioaren segurtasuna kudeatzeko antolamendu egitura foru dekretu honen III. eranskinean ageri diren ardura eta eginkizunen bidez garatzen da.

6. artikulua. Tratamendu jardueren erregistroa

1. Arabako Foru Aldundiak eguneratuta edukiko du bere ardurapeko datu pertsonalen tratamendu jardueren erregistroa, eta DBEOren 30. artikuluan aipatzen den informazio guztia jasoko du erregistro horretan. Saitetako zuzendaritzek, beren eskumenak erabiliz egiten dituzten datu pertsonalen tratamenduaren arduradunak diren aldetik, erregistro hori dokumentatzeko eginbeharra dute.

2. Tratamendu jardueren erregistroa etengabe eguneratuko da, eta inbentarioa www.araba.eus web orri korporatiboan kontsultatu ahal izango da.

7. artikulua. Arriskuen analisia, datuen babesaren gaineko eraginaren ebaluazioa eta informazioaren segurtasun arriskuen kudeaketa

1. Informazioak datu pertsonalak dituenean, arriskuen analisia egingo da aldiari behin, arriskuak identifikatu eta kudeatzeko, eta arriskuak minimizatzeko, onargarritzat jo daitezkeen mailetaraino. Ebaluazio horrek aintzat hartuko du pertsona fisikoek datu pertsonalen tratamendu jardueri dagokienez dituzten eskubide eta askatasunen arriskuen azterketa, bai eta tratamendu jarduera horietarako euskarri diren informazio sistemen ere. Era berean, egindako azterketatik ondorioztatzen bada tratamenduak pertsonen eskubide eta askatasunentzat arrisku handia ekar lezakeela, datu pertsonalak babesteko eraginaren ebaluazioa egingo da, DBEOren 35. artikuluan xedatutakoari jarraikiz.

2. Informazioaren segurtasun arriskuak etengabe kudeatu behar dira informazio sisteman, arriskueta eta aldizkako berrebaluazioan oinarritutako segurtasuna kudeatzeko printzipioei jarraituz.

8. artikulua. Datuak tratatzeko mandatuak

Tratamenduaren arduradunen eta tratamenduaren eragileen arteko harreman juridikoa ezartzen duten egintza juridikoak dira. Mandatuek alderdi hauek jaso behar dituzte: tratamenduaren xedea, iraupena, izaera eta helburua, datu pertsonalen motak eta pertsona interesdunen kategoria, bi alderdien betebeharrak eta eskubideak, bai eta DBEOren 28. artikuluan adierazitako gainerako alderdiak ere. Tratamendu mandatuak beharrezko jarraibideak ezarriko dituzte Arabako Foru Aldundiaren kontura datu pertsonalak tratatzen dituzten erakundeek honako baldintza hauek bete ditzaten:

- Datu pertsonalak agindutako zerbitzua emateko erabiltzea, eta berariaz baimendutako helburuekin bat ez datozen helburuetarako ez bideratzea.
- Datu pertsonalak ez jakinaraztea legitimatzeko oinarri juridikorik ez duten hirugarren pertsona edo erakundeei, DBEOren 6. artikulua dioenarekin bat etorritz.
- Datu pertsonalen konfidentzialtasuna eta osotasuna bermatzea, segurtasun neurriak ezarriz.

9. artikulua. Informazioaren gardentasuna

Gardentasun eginbeharra betetzeko, Arabako Foru Aldundiak, tratamenduaren arduradun gisa jarduten duenean, neurri egokiak hartuko ditu datuen titular diren pertsona fisikoei DBEOren 13. eta 14. artikuluetan adierazitako informazio guztia emateko. Informazio hori modu labur, garden, ulergarri eta eskuragarrian emango da, hizkuntza argia eta ulertteraza erabiliz.

10. artikulua. Eskubideak erabiltzea

1. DBEOren 15. artikulutik 22.era bitartekoak betez, Arabako Foru Aldundiak honako eskubide hauen egikaritzea bermatuko du: datuak eskuratzeko, zuzentzeko, ezabatzeko, datuen aurka egiteko, tratamendua mugatzeko, banakako erabaki automatizatuen xede ez izateko eta, hala badagokio, eramangarritasunerako eskubideak.

2. Hau da Arabako Foru Aldundian eskubide pertsonalak baliatzeko jarraitu beharreko prozedura:

a) Datu pertsonalen babesaren arloko eskubideak egikaritzeko eskaerak gaitutako eskabide ereduaren bidez aurkeztu ahal izango dira, honela:

- Era telematikoan: Arabako Foru Aldundiaren egoitza elektronikoan.
- Aurrez aurre: Arabako Foru Aldundiaren Erregistro Orokorren bulegoetan.

b) Tratamenduaren arduradunak atzerapenik gabe erantzun dio eskaerari, eta, edonola ere, gehienez ere, hilabeteko epean, DBEOren 12.3 artikulua dioenari jarraikiz. Epe hori, gehienez ere, bi hilabetez luzatu ahal da, eskaeren konplexutasuna eta kopurua kontuan hartuta. Horren berri emango zaio eragindako pertsonari, arrazoiak azalduta.

c) Datu pertsonalen babesaren arloko eskubideak egikaritzeko eskaera ezetsiz gero, eragindako pertsonak eskubidearen babesa eskatu ahal izango diote DBEAri, eta, horretarako, erreklamazioa aurkeztu ahal izango diote Arabako Foru Aldundiko datuak babesteko ordezkariari, DBLOren 37. Artikulua dioenarekin bat etorritz.

11. artikulua. Datu pertsonalak gordetzeko epea mugatzea

Datu pertsonalak, oro har, jasotzen diren jarduerari edo zerbitzuari dagokion prozedura izapidetzeko behar den denboran gordeko dira, eta, gainera, geroko preskripzio edo iraungitze epean, tratamenduaren beraren ziozko balizko erantzukizunei amaiera emateko helburuz.

12. artikulua. Datuen babesa eta segurtasuna diseinutik abiatuta eta lehenetsita

Arabako Foru Aldundiak neurri tekniko eta antolakuntzako neurri egokiak ezarriko ditu, datu pertsonalen tratamenduak, besterik adierazi ezean, tratamenduaren helburu espezifiko bakoitzeko beharrezkoak diren datu pertsonalak bakarrik tratatzeko moduan egingo direla ziurtatzeko. Zehazki, neurri horiek jasotako datu pertsonalen kopuruari, tratamenduaren hedadurari, kontserbazio epeari eta irisgarritasunari aplikatuko zaizkie.

Segurtasun neurriak lehenetsiko dira, informazioaren segurtasuna beti aintzat har dadin datu pertsonalak tratatzen dituzten sistema guztietan. Segurtasun neurri horiei dagokienez, arriskuari egokitutako segurtasun maila bermatzeko neurri tekniko eta antolakuntzako neurri egokiak aukeratuko dira, besteak beste, pseudonimizazioa, zifratzea eta datu pertsonalen anonimizazioa, DBEOren 32. artikulua ezartzen duen bezala.

13. artikulua. Datu pertsonalen segurtasun arrakalak eta segurtasun gertakariak jakinaraztea

Arabako Foru Aldundiak behar diren neurriak hartuko ditu kontrol-agintaritzari jakinarazteko eta, hala badagokio, eraginpeko pertsonen jakinarazteko gerta daitezkeen datu pertsonalen segurtasun-arrakalak, horretarako ezarritako prozeduraren bidez.

14. artikulua. Berrikuspena eta auditoretza

Arabako Foru Aldundiak, aldian-aldian eta lege ezarritako epeetan, auditoria bat egingo du, tratamenduen eta informazio sistemen segurtasuna bermatzeko neurri tekniko eta antolakuntzako eraginkortasuna egiaztatu, ebaluatu eta baloratzeko.

Nolanahi ere, auditoria espezifiko eta ezohiko bat egingo du informazio sisteman funtsezko aldaketak egiten diren guztietan, ezarritako segurtasun neurriak betetzean eragina izan dezaketenak.

15. artikulua. Langileen betebeharrak

Arabako Foru Aldundiko langileek laguntza emango dute datuak babesteko eta informazioaren segurtasunerako politika ezartzeko jardueretan.

Langile horiek politika honetan eta politika garatzen duten arau eta prozeduretan aurreikusitakoa ezagutzeko eta betetzeko betebeharra dute.

16. artikulua. Kontzientziazioa eta prestakuntza

Arabako Foru Aldundiak prestakuntza planen garapena sustatuko du. Plan horiek erakundearen langileentzat antolatuko dira, datu pertsonalen babesari eta informazioaren segurtasunari buruzko kontzientziazio saioak jaso ditzaten aldian-aldian. Bereziki, arreta bereziz jorratuko dira honako eremu eta helburu hauek:

a) Prestakuntza eta kontzientziazioa ematea Arabako Foru Aldundiko langile berriei, aldizka eta etengabe.

b) Sistemen erabilera, eragiketan edo administrazioan erantzukizuna duten pertsonen sistemak segurtasunez erabiltzeko prestakuntza jasotzea, beren lana eraginkortasunez eta efizientziaz egiteko prestakuntza behar duten neurrian.

c) Datu pertsonalak babesteari eta informazioaren segurtasunari buruzko prestakuntza, lanpostuaren beharengatik ezaupide zehatzak eskuratu behar dituzten talde espezifikoetako langileen artean emateko diseinatu eta onartzen dena, lehentasunezkoa izatea eta, hala bada, gorkio, nahitaezkoa izatea, prestakuntza premia horiek betetzeko lanpostuko eginkizunak betetzean eta lanpostuari dagozkion erantzukizunak behar bezala hartzean.

Xedapen gehigarri bakarra

Informazioaren Segurtasunaren dokumentuen corpusa, gehienez ere, sei hilabeteko epean ezarriko da politika honetan, indarrean sartzan denetik zenbatzen hasita.

Xedapen indargabetzaile bakarra

Indargabetuta geratzen dira foru dekretu honetan ezarritakoaren aurka dauden maila bereko edo apalagoko xedapen guztiak, eta, bereziki, Arabako Foru Aldundiaren segurtasun politika eta segurtasun dokumentua onartzen dituen Kontseiluaren maiatzaren 20ko 310/2008 Erabakia eta Foru Gobernuaren Kontseiluaren azaroaren 27ko 646/2018 Erabakia, Datu Pertsonalak Babesteko abenduaren 13ko 15/1999 Lege Organikoak (DBLO) eragindako aldundi horren fitxategien segurtasunerako egitura funtzionala onartu zuen maiatzaren 22ko 480/2007 Erabakiaren aldatzea onartzen duena, Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamendura egokitzeko.

Azken xedapenetatik lehenengoa. Arautegiak prestatzea

Enplegu, Merkataritza, Turismo eta Foru Administrazioaren Saileko titularrari ahalmena ematen zaio foru dekretu hau gauzatu eta garatzeko behar diren xedapenak eman ditzan. Era berean, Enplegu, Merkataritza, Turismo eta Foru Administrazioaren Saileko titularrari bera-riazko ahalmena ematen zaio foru dekretu honen eranskinetan ageri den Informazioaren Segurtasunari eta Segurtasunaren Antolaketari buruzko politika korporatiboaren zehaztapenak aldatzeko, eguneratzeko eta bilakaera teknologikoaren ildoan egokitzeko.

Zerbitzu Orokorretako zuzendariari ahalmena ematen zaio homogeneousotasuna eta kalitatea bermatzeko beharrezkoak diren zirkularrak eta jarraibideak eman ditzan.

Azken xedapenetako bigarrena. Indarrean jartzea

Foru dekretu hau ALHAOn argitaratu eta hurrengo egunean sartuko da indarrean.

Vitoria-Gasteiz, 2026ko uztailaren 28a

Diputatu nagusia

RAMIRO GONZÁLEZ VICENTE

Lehenengo diputatu nagusiordea eta Enplegu, Merkataritza, Turismo eta Foru Administrazioaren Saileko foru diputatua

CRISTINA GONZÁLEZ CALVAR

Berdintasun, Euskara eta Gobernantza Saileko foru diputatua

IÑAKI GURTUBAI ARTETXE

Zerbitzu Orokorren zuzendaria

IKER MIRANDA SERRANO

Gobernantza zuzendaria

MIREN ZABALA BASTERRECHEA

 Arabako Foru Aldundia Diputación Foral de Álava	AFAREN DATU PERTSONALAK BABESTEARI ETA INFORMAZIOAREN SEGURTASUNARI BURUZKO POLITIKA		Estrategia Digitaleko eta Informatikako Zerbitzua
	Bertsioa	Data	

**I. ERANSKINA. ARABAKO FORU ALDUNDIAREN DATU PERTSONALAK
BABESTEKO ETA INFORMAZIOAREN SEGURTASUNA BERMATZEKO
POLITIKARI ATXIKITZEKO PROTOKOLOA**

(Izena eta kargua), (erakunde autonomoa, sozietate publikoa edo partzuergoa) ordezkatzuz....., honako hau,

ADIERAZTEN DU:

..... (erakunde autonomoa, sozietate publikoa edo partzuergoa) (e)k,..... (e) ko.....
aren(e)(a)n, erabaki duela Arabako Foru Aldundiaren datu pertsonalak babesteko eta informazioaren segurtasunerako politikari atxikitze eskatzea.

Hori dela eta, honako hau.

ERABAKITZEN DU:

Lehenengoa. (Erakunde autonomoa, sozietate publikoa edo partzuergoa) Arabako Foru Aldundiaren datu pertsonalak babesteko eta informazioaren segurtasuna bermatzeko politikari atxiki dakion onestea, datuak babesteko eta informazioaren segurtasuna bermatzeko politikaren esparruan informazioaren segurtasuna kudeatzeko antolaketa egiturari izan ezik (aipatutako foru dekretuaren III. eranskina).

Atxikipen hori Arabako Foru Aldundiak unean-unean indarrean duen datu pertsonalak babesteko eta informazioaren segurtasuna bermatzeko politikari egin zaiola ulertuko da.

Bigarrena. Arabako Foru Aldundiaren datu pertsonalak babesteko eta informazioaren segurtasuna bermatzeko politika onesten duen foru dekretuan ezarritako betebeharrak bere gain hartzea, eta dekretu horretan aurreikusitako jarduerak egitea, behar bezala kudeatzeko.

Hirugarrena. Arabako Foru Aldundiaren datu pertsonalak babesteko eta informazioaren segurtasuna bermatzeko politikaren barne koordinazioa inplementatu, kudeatu eta gauzatuko duten pertsonak izendatzea. Pertsona horiek solaskide jardungo dute AFaren aurrean.



(Erakunde autonomo, sozietate publiko edo partzuergoaren solaskideen izen-abizenak)

-
-
-
-
-
-

Izen zerrenda horretako aldaketak ahalik eta lasterren jakinarazi beharko zaizkio AFAko Zerbitzu Orokorretako Zuzendaritzari.

(Lekua eta data)

Izena eta abizenak

Izena eta abizenak

(Sinadura)

AFAko Zerbitzu Orokorretako zuzendaria

(Sinadura)

Erakunde autonomo, sozietate publiko edo
partzuergoaren ordezkariaren kargua



Arabako Foru Aldundia
Diputación Foral de Álava

**DCSGPOSEG - ARABAKO FORU ALDUNDIAREN DATU PERTSONALAK
BABESTEKO ETA INFORMAZIOAREN SEGURTASUNA
BERMATZEKO POLITIKA**

Dokumentuaren sailkapena: Publikoa

AFAre Datu Pertsonalak Babesteari eta Informazioaren Segurtasunari buruzko Politika



Kontrol orria:

Agiria:	
Egilea:	
Bertsioa:	Bertsioaren data:
Nork berrikusia:	Berrikusi den data:
Onetsita:	Onarpen data:

Aldaketen kontrola:

Bertsioa	Data	Egilea	Azalpena



Arabako Foru Aldundia
Diputación Foral de Álava

1. Zioen azalpena.....	1
2. Xedea eta aplikazio eremua.....	1
2.1. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren asmoa.....	1
2.2. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren aplikazio eremua.....	1
2.3. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren aplikazio esparrua.....	2
2.4. Berrikuspena eta indarraldia	2
3. Ezarpenaren erreferentziak	2
4. Segurtasun printzipioak	2
5. Helburuak	5
6. Antolaketa.....	6
7. Datu pertsonalen babesa eta informazioaren segurtasunari buruzko dokumentu corpusaren garapena.....	7
8. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa eguneratzea eta berrikustea.....	7
9. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa ez betetzea	8
10. Onestea eta indarrean hastea.....	8

AFaren Datu Pertsonalak Babesteari eta Informazioaren Segurtasunari buruzko Politika



Arabako Foru Aldundia
Diputación Foral de Álava

1. Zioen azalpena

Administrazio publikoen eremuan, haiekin bitarteko elektronikoen bidez komunikatzeko eskubideak eta administrazio horiek behartuta dauden Informazioaren Gizartea garatzen laguntzeak badakar helburu horiek lortzea sustatzen duten ekintzak bultzatzea.

Horregatik, administrazio publikoek bitarteko elektronikoen erabileran konfiantza izateko beharrezko baldintzak sortu behar dituzte. Horretarako, informazio sistemen, datuen osotasunaren (datu pertsonaletan bereziki), komunikazioen eta zerbitzu elektronikoen segurtasuna bermatzeko beharrezko neurriak ezarri behar dituzte, eta herritarrei, enpresei eta beste administrazio publiko batzuei eskubideak baliatzeko eta betebeharrak bitarteko horien bidez betetzeko aukera eman behar diete.

Gainera, administrazio publikoak bereziki arriskuen mende daude, beren izaera eta misioagatik; hori dela eta, administrazioaren eginkizunak eraginkortasunez garatzeko, neurri ugari hartu behar dituzte, honako hauek lehentasunez babesteko:

- Informazioaren tratamendua eta hedapena ahalbidetzen duten teknologiak eta sistema informatikoak, bai eta zerbitzuaren kudeaketa arina eta eraginkorra ere.
- Eragiketaren jarraitutasuna, eskatutako zerbitzua hartzaileei une egokian ematea ahalbidetuz.

2. Xedea eta aplikazio eremua

2.1. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren asmoa

Arabako Foru Aldundian (aurrerantzean, AFA) informazioaren eta sistemen segurtasunaren oinarritzko printzipioak lor daitezen sustatzea eta bultzatzea.

Informazio sistemak babesteko antolakuntzako neurriak, neurri teknikoak, fisikoak eta legezkoak ezartzeko jarraibideak ematea.

Egungo legeria betetzen dela bermatzea, informazioaren segurtasunaren testuinguruan aplikagarria izanik, eta informazioaren konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna eta trazabilitatea une oro zaintzea.

2.2. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren aplikazio eremua

Politika hau nahitaez aplikatu behar zaio Arabako Foru Aldundiari (AFA). Era berean, Arabako gainerako foru sektore publikoa Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboari atxiki ahal izango zaio, atxikitzeko hitzarmena formalizatuz.



2.3. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren aplikazio esparrua

Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboak AFAn oro har aplikatzekoak diren Informazioaren Segurtasunari buruzko gidalerroak ezartzen ditu, horiek eska daitezkeen gutxienez hartuta, eta Arabako Foru Aldundiaren ingurune partikularretan Segurtasun Politika osagarriak sortzeko ahalmena ematen du, betiere horiek izaera murriztaileagoa badute maila korporatiboan ezarritakoa baino. Horregatik, politika hau erreferentziazko esparrua da, eta esparru partikular horien barruan ezartzen diren informazioaren segurtasuna bermatzeko politikak esparru horri lotuta lerrokatu beharko dira.

2.4. Berrikuspena eta indarraldia

Politika hau indarrean egongo da formalki eguneratzen den arte, eta haren edukiari eragiten dioten aldaketa garrantzitsuak gertatzen diren bakoitzean berrikusiko da.

3. Ezarpenaren erreferentziak

Arabako Foru Aldundiaren (AFA) Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa Segurtasun Eskema Nazionalan (aurrerantzean, SEN) ezarritako jarraibide eta printzipioetan oinarritzen da. Era berean, kontuan hartu dira, eta etorkizunean ere hala izaten jarraitu beharko dute, aplikatzekoak diren araudiak eta estandarrak, politika hori horien ondoriozko arau, erregelamendu eta jardunbide egokien betekizunetara egokitzeko.

Informazioaren segurtasunaren eta pribatutasunaren arloan aplikatzekoa den legeria identifikatzeko, berrikusteko eta eguneratzeko, «Dokumentazioa identifikatzea eta aplikatzekoa den erreferentziazko legeria» izeneko prozedura erabiliko da.

Era berean, foru sektore publikoa osatzen duten erakundeei dagokienez, bakoitzari dagokio aplikagarri zaien araudia identifikatzea, mantentzea eta eguneratzea, eta hori behar bezala dokumentatu beharko da «Dokumentazioa identifikatzea eta aplikatzekoa den erreferentziazko legeria» dokumentuan.

4. Segurtasun printzipioak

Gobernu Kontseilua, Arabako Foru Aldundiaren Gobernu, Antolaketa eta Araubide Juridikoari buruzko martxoaren 15eko 10/2023 Foru Arauaren arabera, Foru Aldundiaren kide anitzeko organoa da, eta diputatu nagusiaren zuzendaritzari men eginik, politika orokorra ezartzen du, foru administrazioa artezten du eta legeek eta foru arauak esleitzen dizkioten gainerako eskumenak gauzatzen ditu, eta, horretarako, gobernu ekintza, araugintza ekimena, erregelamenduak egiteko ahala eta eginkizun betearazlea gauzatzen ditu.

Segurtasun eta Pribatutasun Batzorde Korporatiboak egin eta zehaztuko du Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa, eta Gobernu Kontseiluak onartu beharko du.

Kide anitzeko organo artezlea den aldetik, segurtasun eredu bat ezartzeaz arduratuko da, gutxienez honako segurtasun printzipio hauek errespetatuko dituen:



- a) Informazio sistemen segurtasuna prozesu oso baten emaitza izango da, eta tratamenduan esku hartzen duten giza elementu, elementu tekniko, material eta antolakuntza elementu guztiak aintzat hartuko dira.
- b) Informazio sistemak garatu eta ezartzen dituen erakunde bakoitzak arriskuak aztertu eta kudeatuko ditu, arriskuarekiko esposizio maila monitorizatuz, eta arrisku hori desagerrarazteko, murrizteko edo transferitzeko neurriak ezarriko ditu. Ezartzen diren segurtasun neurriek eguneratuta egon beharko dute, eta informazioaren tratamenduari lotutako aplikazioen eta zerbitzuen bizi zikloaren fase guztietara egokitu beharko dute, oreka bat ezarri datuen izaeraren, egindako tratamenduen, azaldutako arriskuen eta aplikatutako neurrien artean. Horretarako, segurtasun arduradunaren edo datuak babesteko ordezkariaren aholkularitza eskatu ahal izango du.
- c) Informazio sistemekin lotura duten pertsona guztiei prestakuntza eta informazioa emango zaie segurtasunaren arloan dituzten eginbehar eta betebeharrak buruz, eta ezarritako prozedurak betetzen direla egiaztatuko da.
- d) Informazio sistemen segurtasuna pertsona kualifikatuek, adituek eta prestatuek zaindu, berrikusi eta ikuskatuko dute, beren bizi zikloaren aldi edo fase guztietan (instalazioan, mantentze lanetan, gorabeheren kudeaketan eta desegitean).
- e) Informazio sistemarako sarbideak kontrolatu eta mugatu egingo dira behar bezala baimendutako erabiltzaile, prozesu, gailu eta bestelako informazio sistemetara, eta irizpide murriztaileak aplikatuko dira sarbide horiek gaitzeko orduan. Informazio sistemak segurtasuna bermatzeko moduan diseinatu eta konfiguratu dira, erakundeak bere helburuak lortzeko behar duen gutxieneko funtzionaltasuna eskainiz.
- f) Informazio sistemak eremu babestuetan instalatu dira, sarbide fisikoa kontrolatzeko prozedurez hornituta.
- g) Elementu fisiko edo logiko orok sisteman instalatu aurreko baimen formala beharko du. Une oro jakin beharko da haien segurtasun egoera. Horretarako, kontuan hartuko dira fabrikatzaileen zehaztapenak, haiei eragiten dieten kalteberatasunak eta horiek arintzen edo ezabatzen dituzten eguneratzeak, eta dagokion arriskua kudeatzeko arretaz erantzungo da.
- h) Arabako Foru Aldundian, Adimen Artifizialean (IA) oinarritutako sistemak modu seguruan, arduratsuan eta informazioaren konfidentzialtasun, osotasun, eskuragarritasun, benetakotasun eta trazabilitate printzipioekin bat etorri erabili beharko dira. IAK eskaintako irtenbideak ezartzeko eta erabiltzeko, arriskuen azterketa espezifikoak eta dokumentatua egin beharko da. Hala, azterketa horretan, teknologiarik datuak erabiltzeko arriskuak eta erakundeak beste sistema eta prozesu batzuekin duten elkarrekin eratorritakoak jaso beharko dira. Informazioaren segurtasunean eta datu pertsonalen babesean izan dezakeen eragina ebaluatuko da, datuen babesaren eta eskubide digitalen arloan indarrean dagoen araudia betetzen dela ziurtatuz. Arrisku handiko adimen artifizialeko sistemak badira, oinarritzko eskubideei buruzko eraginaren ebaluazioa egin beharko da, Europako Parlamentuaren eta Kontseiluaren 2024ko ekainaren 13ko 2024/1689 (EB) Erregelamenduaren 27. Artikuluak dioenari jarraikiz (2024ko ekainaren 13ko Erregelamendua, adimen artifizialaren arloko arau bateratuak ezartzen dituena). Gainera, identifikatutako arriskuak arintzeko kontrolak eta babesak ezarriko dira, alborapenak



kudeatzeko neurriak, prozesu automatizatuaren gardentasuna, emaitzen giza ikuskapena eta erabaki automatizatuaren trazabilitatea ere kontuan hartuta. Arabako Foru Aldundiko segurtasun arduradunak onartu beharko du ingurumen ebaluazioko sistemen garapen, eskuratze edo hedapen oro, eta aldizkako berrikuspenei lotuko zaizkie, Arabako Foru Aldundiak ezarritako segurtasun printzipio eta eskakizunetara egokitzen dela bermatzeko.

- i) Informazio sistemaren segurtasunaren egiturak eta antolaketak arreta berezia eskainiko dio ingurune ez-seguruetan biltegiratzen den edo horietatik igarotzen den informazioari, hau da, biltegitratutako datuen kategoriari edo horien fluxuari, bai eta ingurune gabezi ere.
- j) AFaren perimetro logikoak baimendu gabeko pertsonen sarbidetik kontrolatu eta babestuko dira, bereziki sare publikoetarako konexioetan. Informazio sistemak sareen bidez beste sistema batzuekin konektatzearen ziozko arriskuak aztertuko dira, eta horien lotura puntua kontrolatuko da.
- k) Sistemen erabilera erregistratu ahal izango da, eta behar ez diren edo baimendu gabeko jarduerak monitorizatzeko, aztertzeko, ikertzeko eta dokumentatzeko beharrezkoa den informazioa atzitu ahal izango da. Era berean, horiek gauzatu izanaren ebidentziak behar dituzten kudeaketa prozesuek esandako prozesuak badirela frogatzeko beharrezkoak diren datuak erregistratuko dituzte, baita egileenak ere.
- l) Informazio sistemek kode kaltegarrien aurkako prebentzio, hautespen eta erantzun neurriak izango dituzte (sisteman atzealdeko ateak, segurtasun arrakalak, informazioaren eta datuen lapurreta eta fitxategi eta sistema informatikoetan izan daitezkeen beste kalte batzuk sortzea ahalbidetzen duten kalteberatasunak sortzeko diseinatuta daude), eta arreta berezia jarriko dute datuak tratatzeko ekipoen instalazioan. Horrez gain, berreskuratzeko neurri egokiak ere jasoko dira.
- m) Segurtasun gertakariak edo gorabeherak edo segurtasun arrakalak detektatzeko, horiek kudeatu beharko dira, erregistratu eta ebatzi ondoren sistemen segurtasuna etengabe hobetzeko prozesuak gaitu ahal izateko.
- n) Informazio sistemek segurtasun-kopiak izango dituzte. Gainera, ohiko lan baliabideak galduz gero, eragiketen jarraitutasuna bermatzeko beharrezko tresnak izango dituzte.
- o) Informazio sistemek informazioaren originaltasuna, zilegitasuna eta sendotasuna zaindu beharko dituzte, bai eta informazioaren egiazkotasuna eta egiletza ere. Era berean, datuen edo aplikazioen gainean egindako ekintzak erregistratu eta identifikatu beharko dituzte.
- p) Auditoretzek baliozkotuko dute segurtasun politiken aplikazio eraginkorra, kasuan-kasuan aplikatu beharreko legeriaren betetze maila, eta tratamendu jardueretan identifikatutako arriskuen aurrean segurtasun neurrien egokitzapena.
- q) Zerbitzuak kanpora ateratzeko prozedura ezarriko da, espero den segurtasun zerbitzuaren maila argi eta garbi arautzeko, eta tratamenduaren mandatu kontratua sinatu beharko da, datu pertsonalen tratamendua dakarrenean.
- r) Bizi zikloan garatzen edo eskuratzen diren software irtenbideen segurtasuna kudeatzeko, onartutako metodologiak hartuko dira oinarri.



- s) Informazio sistemiei buruzko kontratazio prozesuek aintzat hartu beharko dute enpresa kontratatzaileek informazioaren segurtasunean homologatuta edo ziurtatuta egon beharko dutela.
- t) Aktiboen (informazio sistemen) kudeaketa segurua ezartzeko, aktiboen sailkapena arautuko da, negozio prozesuetarako duten garrantziaren eta arriskuaren arabera, horiek erabiltzean bete behar diren eskakizunak ezarriko dira, eta horien arduradunak identifikatuko dira. Babes maila eta aplikatu beharreko neurriak sailkapen horren emaitzan oinarrituko dira.
- u) Giza baliabideen kudeaketak kontuan hartuko ditu segurtasun betekizunak hautaketa prozeduretan, kontratazio prozesuetan, berrantolaketa eta kontratazioa amaitzean.
- v) Informazioaren segurtasunari buruzko prestakuntza eta kontzientziakuntza funtsezko osagaiak izango dira sistemen babes eraginkorra bermatzeko. Segurtasunari buruzko prestakuntza programak ezarriko dira, arlo bakoitzaren beharretara egokituak, bai eta langile guztientzat antolatutako kontzientziakuntza kanpainak ere, segurtasun politikak ulertzen eta betetzen direla ziurtatzeko bitarteko eraginkorrenak erabiliz.
- w) Informazio sistemek zibererasoen aurrean jarduteko protokolo espezifikoak izango dute. Protokolo horretan, gainera, Kriptologia Zentro Nazionalari (CCN-CERT) jakinarazteko baldintzak jasoko dira. Izan ere, zentro horrek Estatuko esparru publikoan koordinatzen ditu segurtasun gertakariei erantzuteko gaitasunak.
- x) Kriptografia funtsezko osagai gisa erabiliko da informazioaren konfidentzialtasuna, osotasuna eta benetakotasuna bermatzeko, hala beharrezkoa den kasuetan. Kontrol kriptografikoak ezarriko dira, indarrean dagoen legediaren arabera eta segurtasun jardunbide onenekin bat etorrira.
- y) Datu pertsonalak ahalik eta zorrotzen tratatuko dira, datuen babesaren arloan indarrean dagoen araudiarekin bat etorriz. Segurtasun neurri egokiak ezarriko dira datu pertsonalen pribatasuna eta babesa bermatzeko, eta datu horien tratamendua bidezko helburuetara mugatzen dela ziurtatuko da.

Ezarritako segurtasun prozesu osoa etengabe eguneratu eta hobetuko da. Helburu horretarako, kudeaketa egokia egingo da, denboran zehar erakundearen aktiboak babesteko kontrolak eta neurriak ezarriko direla bermatzeko, eta kontrol eta neurri horiek berrikusi eta hobetzeko xedez, sortzen diren mehatxuei, erregulazio aldaketei edo segurtasun helburuen aldaketei behar bezala eta modu proaktiboan erantzuteko.

5. Helburuak

Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboan ezarritako printzipioen implementazioak AFaren helburuak betetzea ahalbidetuko du, eta, horrela, informazioaren segurtasun osoa bermatuko da alderdi guztietan:

- a) Konfidentzialtasunari, osotasunari, eskuragarritasunari, benetakotasunari eta trazabilitateari dagokienez segurtasun maila ezin hobeei oratzeko, AFaren eta herritarren premiekin bat datozenak eta horiekiko koherenteak.



- b) Indarrean dagoen lege esparrua betetzen dela bermatzea.
- c) Zibersegurtasunaren kultura sustatzea AFAko langileen artean.
- d) Informazioaren segurtasuna eta pribatutasuna kudeatzeko sistemari eustea, AFaren aktiboei, zerbitzuei eta prozesuei lotutako arriskuak identifikatu, aztertu eta tratatzeko.
- e) Segurtasun maila egokia emango duten neurri teknikoak eta antolakuntzako neurriak ezartzea, informazio hori lantzen duten sistemei eta prozesuei dagokienez.
- f) Informazio zerbitzuen eta sistemen jarraitutasuna ahalbidetzeko kontingentzia tresnak ezartzea, aldi onargarri batean horiek berreskuratzea ahalbidetuz.

6. Antolaketa

AFAk antolaketa egitura jakina izango du Datu Pertsonalen Segurtasuna eta Babesa kudeatzeko eta koordinatzeko, eta politika korporatibo honi darizkion erantzukizunak identifikatuko ditu, definizioari, ezarpenari, eragiketari, kudeaketari, jarraipenari eta komunikazioari dagokienez. Informazioaren Segurtasuna eta Pribatutasuna antolatzeko arduradunek eginkizun hauek izango dituzte:

- a) Segurtasun gertakariei eraginkortasunez erantzuteko beharrezko tresnak ezartzea.
Segurtasun prozesuak ezarritako segurtasun rolen arabera gauzatzea.
- b) Antolamendu kontrolak eta kontrol tekniko espezifikak definitzea, ezartzea, kudeatzea eta gainbegiratzea, hirugarrenek eskuataratutako aktiboen segurtasunari eusteko, eta informazioa prozesatzeko erantzukizuna beste erakunde bati eskuordetu zaion kasuetan.
- c) Agintari eskudunekin, zerbitzuak hornitzen dituzten enprekin eta informazio sistemen segurtasuna sustatzen duten erakunde publiko edo pribatuekin batera, segurtasunaren arloan lankidetzan aritzeko tresna egokiak ezartzea.

Antolakundea erakunde bakoitzaren egitura funtzionalera egokituko da, pertsona anitzeko eta pertsona bakarreko rolak hartuko ditu kontuan, eta horien maila funtzionala kontuan hartuko du (estrategikoa, taktikoa, operatiboa eta kontrolekoa), bai negozio-inguruneetarako (segurtasun-zerbitzuaren bezeroak), bai laguntza-inguruneetarako (segurtasun-zerbitzuaren hornitzaileak diren enpresak), eta honako printzipio hauen arabera ezarriko da:

- a) Segurtasun antolakundea ezarriko da AFaren eremu osorako, eta gutxieneko izaera izango du, eta ahalmena emango da AFaren ingurune zehatzetan segurtasun antolakunde osagarriak sortzeko, izaera orokorraz ezarritakoaren osagarri, betiere erakunde horiek antolakuntza eredu globalaren gutxieneko izaera errespetatzen eta gainditzen badute.
- b) Antolamendu globalaren ereduari txertatuko ditu gaur egun ezarrita dauden antolakuntza ekimenak, eta AFaren ingurune zehatzetan hartutako ekimen partikularren arteko koordinazioa erraztuko du, antolamendu eredu globalarekin bat eta horretan txertaturik.



- c) SEN aplikatzeari lotutako lanposturen bat kentzea edo aldatzea dakarren barne organigramaren edozein aldaketak nahitaez jaso beharko du eginkizun horiek zer lanposturi atxikita geratuko diren.
- d) Antolakunde horrek erantzukizunak dituen eremu tekniko edo antolakuntzakoetara egokitu ahal izango da.
- e) Politika honi atxikitako rolak eta erantzukizunak AFaren antolaketa egituraren atal izango dira, eta Aldundiko administrazio organo bakoitzera eta Foru Sektore Publikora egokitu beharko dira. Rol bakoitzaren eginkizunen, funtzioen eta erantzukizunen xehetasunak Datuen Segurtasun eta Babesaren Antolakundea izeneko agirian daude deskribatuta.

7. Datu pertsonalen babesa eta informazioaren segurtasunari buruzko dokumentu corpusaren garapena

Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko dokumentu edo agiri korpusaren egitura politika honen hasierako definizioaren bidez antolatzen eta ardazten da, eta bertatik **arau** batzuk (politika honen alderdi zehatz bati edo batzuei dagokienez lortu beharreko helburuak zehaztuko dituztenak), **prozedurak** (eguneroko jardunean segurtasun prozesu guztiak jasateko zeregin xehatuak, sekuentzialak eta espezifikoak bilduko dituztenak), **metodologiak**, **jarraibideak**, **jardunbide egokiak** eta abar sortuko dira. Horietan zehaztuko dira informazio sistema babesteko hartu beharreko neurriak, erakundearen osagaien funtzioak eta erantzukizunak eta horien funtzionamendu egokia kontrolatzeko mekanismoak.

Dokumentu corpusaren osagaiak Informazioaren Segurtasun eta Pribatutasunaren Antolakundeko kideek idatzi, berrikusi eta onartuko dituzte, baldin eta osagai horien izaera estrategiko, taktiko edo operatiboari badagozkio; horretarako, haien bizi zikloa arautzen duen prozedura ezarriko da.

8. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa eguneratzea eta berrikustea

Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren iraunkortasuna eta osotasuna politika horrek bete behar duen funtsezko baldintzetako bat izanik, dokumentu corpora garatzea ahalbidetzen duen jardura esparru egonkorra izan dadin, politika hori eguneratu egin beharko da, haren eraginkortasuna eta egokitasuna gal ez dadin.

Horregatik, Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa bi urtean behin berrikusiko da, baldin eta aldaketa esanguratsurik ez badago (legeria berria, mehatxu edo arrisku berriak, informazio sistemei eragiten dieten aldaketa estrategikoak...), edo segurtasuna berrikusteko prozesuetatik ateratako ondorioetatik berehala berrikusi, aldatu eta hobetu behar ez bada.

Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboaren indarraldiko egonkortasun gomendioak (jarraibide korporatiboetan ezarrita dago) ez dio dokumentu corpusari eragiten; izan ere, beharrezkoa den maiztasunez berrikusi eta eguneratu behar da, azpiegituraren aldaketa teknikoetara eta negozioaren eskakizunetara egokitzeko. Dokumentu corpuseko atalen bat Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatibo honekin bat ez badator, politika horrek lehentasuna izango du.



Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa ALHAOn argitaratuko da, bai eta aplikagarria den administrazio organoen, sozietateen eta erakundeen Intraneten ere.

9. Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa ez betetzea

Segurtasun eta Pribatutasun Batzorde Korporatiboak gainbegiratu ahalko du AFaren informaziorako sarbidea duten edo beren lanbide jardueran informazio hori tratatzen duten langileek Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboan edo haren barne-araudian araututako eginbeharrak betetzen ote dituzten.

Betetzen ez bada, informazioa babestu eta jagoteko prebentzio eta zuzenketa neurriak aurreikusita daude, hargatik eragotzi gabe Arabako Foru Aldundiko goi kargudunen jardunean aplikatu beharreko zehapen araubidea (uztailaren 11ko 10/2018 Foru Arauaren VI. kapitulua), bai eta funtzionarioen jarduerari dagokionez ere (11/2022 Legea, abenduaren 1ekoa, Euskal Enplegu Publikoari buruzkoa). XII. titulua).

10. Onestea eta indarrean hastera

Datu Pertsonalak Babesteko eta Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa ALHAOn argitaratu eta hurrengo egunean aplikatuko da, bertsio berri batek aldatzen duen arte.



Arabako Foru Aldundia
Diputación Foral de Álava

DOSORGSG – DATUEN BABES ETA SEGURTASUN ANTOLAKUNDEA

Dokumentuaren sailkapena: Publikoa

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa



Kontrol orria:

Agiria:	
Egilea:	
Bertsioa:	Bertsioaren data:
Nork berrikusia:	Berrikusi den data:
Onetsita:	Onarpen data:

Aldaketen kontrola:

Bertsioa	Data	Egilea	Azalpena

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa



1. Sarrera	1
1.1. Helburuak	1
1.2. Irismena	1
2. Segurtasun rolak	1
2.1. Segurtasun rolen ikuspegi orokorra	1
2.2. Segurtasun rolen deskribapena	2
2.2.1. Segurtasun eta Pribatutasun Batzorde Korporatiboa (SPBK)	2
2.2.1.1. Segurtasun eta Pribatutasun Batzorde Korporatiboaren eginkizun orokorrak	2
2.2.1.2. Segurtasun eta Pribatutasun Batzorde Korporatiboko kideak	4
2.2.2. Krisi Batzordea (KB)	5
2.2.2.1. Krisi Batzordearen eginkizun orokorrak	5
2.2.2.2. Krisi Batzordeko kideak	5
2.2.3. Segurtasunaren Aholku Batzorde Teknikoa (SAB)	6
2.2.3.1. Segurtasunaren Aholku Batzorde Teknikoaren eginkizun orokorrak	6
2.2.3.2. Segurtasunaren Aholku Batzorde Teknikoko kideak	7
2.2.4. Segurtasun arduraduna (SegArd)	7
2.2.4.1. Segurtasun arduradunaren eginkizun orokorrak	8
2.2.5. Datu Pertsonalen Tratamenduaren arduraduna (DPTTrArd)	9
2.2.5.1. Datu Pertsonalen Tratamenduaren arduradunaren eginkizun orokorrak	9
2.2.6. Informazioaren arduraduna (InfArd)	10
2.2.6.1. Informazioaren arduradunaren eginkizun orokorrak	10
2.2.7. Zerbitzuaren arduraduna (ZerArd)	11
2.2.7.1. Zerbitzuaren arduradunaren eginkizun orokorrak	11
2.2.8. Zerbitzu Erkideen arduraduna (ZerErArd)	11
2.2.8.1. Zerbitzu Erkideen arduradunaren eginkizun orokorrak	11
2.2.9. Datuak Babesteko ordezkaria (DBOrd)	12

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa



2.3. Datuak Babesteko ordezkariaren eginkizun orokorrak	12
2.4. Segurtasunaren eta Datuen Babesaren erreferenteak (SegErr).....	13
2.4.1.1. Segurtasunaren eta Datuen Babesaren erreferentearen eginkizun orokorrak	13
2.4.2. Sistemaren arduraduna (SisArd)	14
2.4.2.1. Sistemaren arduradunaren eginkizun orokorrak	15
2.4.3. Segurtasun Fisikoaren arduraduna (SegFArd)	15
2.4.3.1. Segurtasun Fisikoaren arduradunaren eginkizun orokorrak	15
2.4.4. Erabiltzaileak (Erab)	16
2.4.4.1. Erabiltzaileen eginkizun orokorrak.....	17
2.5. Gatazkak koordinatzeko eta konpontzeko bideak	17
1. eranskina: Segurtasunaren eta Datuen Babesaren rolak esleitzea – Izendapenak	18
2. eranskina: Segurtasunaren eta Datuen Babesaren rolak esleitzea – AOKI kodeak.....	20
3. eranskina: Segurtasun rolak esleitzea – AOKI batzordeak	22

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa



Arabako Foru Aldundia
Diputación Foral de Álava

1. Sarrera

1.1. Helburuak

Arabako Foru Aldundiaren (aurrerantzean, AFA) antolakuntza egitura ezartzea, bere jardueren gobernua, eragiketa, ikuskapena eta kontrol eraginkorra bermatzeko. Jarduera horrek aintzat hartzen du Informazioaren Segurtasunari lotutako rolen eta erantzukizunen definizio zehatza, baita datuen babesa ere, horien garapena, implementazioa, kudeaketa eta mantentzea ere kontuan hartuta, AFaren aktiboak babesteko ikuspegi oso eta proaktiboa ziurtatzeko.

Dokumentu honetan definitutako egitura eta rola AFaren Informazioaren Segurtasunerako Politika Korporatiboan ezarritako printzipioak erabat garatzeko eta horiekin bat etortzeko diseinatu daude, Informazioaren Segurtasunarekin engaiatutako erakunde kultura sustatuz.

1.2. Irismena

Arestian deskribatu den segurtasunaren antolakuntza eredua AFA osoari eta haren erabiltzaileei aplikatzen zaie, barrukoei zein kanpokoei. Informazioaren segurtasuna babestea eta datuak babestea erantzukizun partekatua da, eta ez dagokie soilik karguagatik edo eginkizunengatik informazio sistemen segurtasuna garatzeko eta kudeatzeko erantzukizun espezifikoak esleituta dituztenei.

2. Segurtasun rola

2.1. Segurtasun rolen ikuspegi orokorra

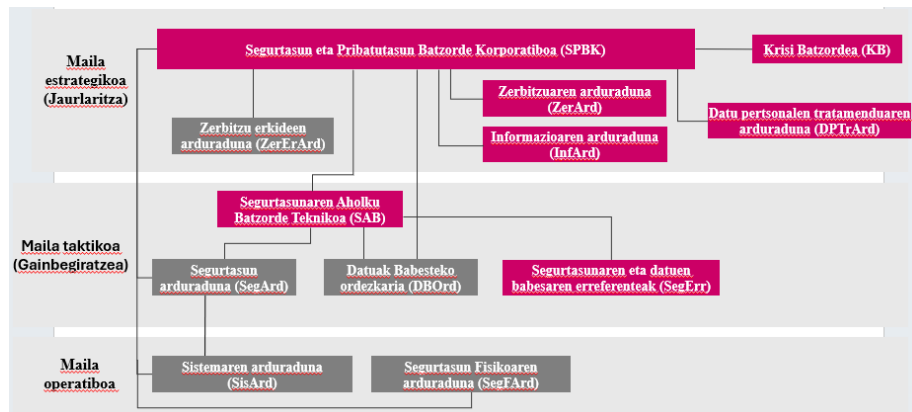
Informazioaren Segurtasunaren testuinguruan, funtsezkoa da rolen egitura argia eta eraginkorra ezartzea AFaren informazioa eta sistemak babesteko. Atal honek segurtasun rolen ikuspegi orokorrak dihardu, eta AFaren barruan dituzten erantzukizunak eta funtzioak nabarmentzen ditu. Rol bakoitza segurtasun-maila espezifiko bati lotuta dago, eta ziurtatzen du babes neurriak AFaren barruan funtzio bakoitzari lotutako beharrian eta arriskuekiko egokiak eta proportzionalak direla. Aurrekoaz gain, kontuan hartu behar da DBEOren araudia, datu pertsonalen kudeaketari eta babesari buruzko nahitaez bete beharreko arauak ezartzen dituenak, eta, aldi berean, bermatzen du AFaren segurtasun jardunbideek Europako legezko estandarrak betetzen dituztela eta parte hartzen duten norbanakoen babesa bermatzen dela. Ikuspegi hori bat dator NIS2 zuzentarauarekin; hain zuzen ere, zibersegurtasunaren arloko rola eta erantzukizunak argi definitzea eskatzen du manu horrek, arriskuak eraginkortasunez kudeatzeko.

AFaren segurtasuna antolatzeko eredu honetan, hiru geruza bereizi definitu dira, Datuen Babesa eta Informazio Sistemak berariaz helburu dituztenak: Gobernua, Gainbegiratzeko eta Eragiketa. Gobernu geruzak politika eta jarraibide estrategikoak ezartzen ditu; gainbegiratzeko geruzak segurtasun politikak eta jarraibideak etengabe monitorizatzen direla eta betetzen direla ziurtatzen du; azkenik, eragiketa geruzak beharrezko segurtasun neurriak ezartzen ditu.

Grafikoki, segurtasun rolen mapa erantsi da, eta horrek jaso egiten ditu informazioaren segurtasunaren kudeaketan parte hartzen duten rola modu egituratuan, aldeztu aurretik definitutako geruzen arabera antolatuta:

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

1/24



Pertsona anitzeko rolak kutxa gorrietan irudikatu dira, eta pertsona bakarreko rolak, berriz, gris koloreko kutxetan. Bereizketa hori funtsezkoa da segurtasun rolak AFaren antolakuntza egituraren behar bezala barruratzin direla ziurtatzeko, zuzendaritza bakoitzean. Pertsona anitzeko rolen esleipena kideak zehaztuz egingo da; pertsona bakarreko rolak, berriz, antolakuntza egituraren barruan hierarkia maila egokien arabera izendatuko dira.

2.2. Segurtasun rolen deskribapena

Hurrengo ataletan, aurretik identifikatutako rolen deskribapena jasotzen da. Rol horiek bat datoz Informazioaren Segurtasuna Bermatzeko Politika Korporatiboan horri buruz ezartzen diren jarraibideekin.

2.2.1. Segurtasun eta Pribatasun Batzorde Korporatiboa (SPBK)

Segurtasun eta Pribatasun Batzorde Korporatiboak (SPBK) berebiziko garrantzia du AFaren aktiboen babesean. Segurtasun ekimenak koordinatzeaz eta gainbegiratzeaz arduratzen da, helburu korporatiboekin bat datozela eta araudi aplikagarriak betetzen dituztela ziurtatuz. Batzordea, **gutxienez, urtean** behin bilduko da.

2.2.1.1. Segurtasun eta Pribatasun Batzorde Korporatiboaren eginkizun orokorrak

Segurtasun eta Pribatasun Batzorde Korporatiboaren (SPBK) eginkizunak honako hauek izango dira:

- AFAk informazioaren segurtasunaren arloan dituen helburuak zehaztea, eta helburu horiek negozio eskakizunekin, prozesu garrantzitsuenekin eta eragiten dieten araudiekin lotuta daudela ziurtatzea.
- Informazioaren Segurtasuna Bermatzeko Politika Korporatiboa onartzea.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

2/24



- Segurtasun arduradunak proposatutako segurtasun estrategia eta hobekuntza planak onartzea, eta AFaren helburu orokorrekin bat datozela ziurtatzea.
- Informazioaren segurtasunaren arloan AFaren barruan ezartzen diren betebeharrak eta eginkizunak onartzea, eta AFAko arduradunen edo arloen artean suertatzen diren erantzukizun gatazkak ebaztea.
- Arrisku korporatiboaren atalasea onartzea, eta erakundean identifikatutako arriskuen onarpenari eta tratamenduari buruzko erabakiak hartzeko prozedura gidatzen duen arriskuarekiko tolerantzia esparrua ezartzea.
- AFaren Informazioaren Segurtasunaren egoeraren berri izatea aldian-aldian, arrisku garrantzitsuak, gorabehera esanguratsuak eta arauen betetze maila aintzat hartuta.
- Informazioaren segurtasuna kudeatzeko sistemaren etengabeko hobekuntza sustatzea, plan espezifikoak onartuz, erresilientziari eta jarraitutasun operatiboari buruzkoak barne, NIS2 arauaren arabera.
- Informazioaren segurtasunaren arloan baliatzen diren finantza baliabide, baliabide teknologiko eta giza baliabideen esleipen eta kudeaketa eraginkorra gainbegiratzea eta koordinatzea, esleitutako aurrekontua behar estrategiko eta operatiboekin bat datorrela ziurtatuz, eta baliabideak mugatuak direnean, segurtasun arloko jardueri lehenetsia emanda, segurtasun neurriak behar bezala ezarri, horiei eutsi eta etengabe hobetzen direla bermatzeko.
- Segurtasun arloko jardueri lehenetsia ematea, baliabideak mugatuak direnean.
- Informazioaren segurtasuneko gertakarien kudeaketa gainbegiratzea, gorabehera garrantzitsuei buruzko informazioa jasotzea eta, hala badagokio, erabaki estrategikoak hartzea eta baliabideak lehenetsia.
- Segurtasunaren eragina duten erakundearen ekimen guztietan segurtasun printzipioa errespetatzen dela zaintzea, zerbitzu horizontalak eta irtenbide komunak sustatzea, bikoiztasunak murrizteko, SENen eremuko sistemen funtzionamendu homogeneoa bermatzeko eta aplikatzekoak diren gainerako araudiak betetzen direla errazteko.
- Arabako Foru Aldundian, prestakuntza, kontzientiazio eta segurtasun kulturako planak bultzatzea eta onartzea.

Batzordea, **gutxienez, urtean** behin bilduko da, aurreko ekitaldian egindako informazioaren segurtasunaren kudeaketa onartzeko eta hurrengo ekitaldirako ildo estrategikoak eta lehenetsiak ezartzeko.

Era berean, aparteko bilera egin ahal izango du gorabehera garrantzitsuen edo salbuespenezko egoeren aurrean, baldin eta, beren eragin edo garrantziagatik, erabaki estrategikoak hartzea edo baliabideak lehenetsia beharrezkoa bada, buruaren iritziz edo Segurtasun arduradunak proposatuta.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

3/24



Segurtasun eta Pribatutasun Batzorde Korporatiboko burua AFAko Zerbitzu Orokorretako zuzendaria izango da, edo hark eskuordetzen duena.

AFAko Segurtasun arduradunak batzordeko idazkari jardungo du, eta honako eginkizun hauek izango ditu:

- Segurtasun eta Pribatutasun Batzorde Korporatiboaren (SPBK) bileretarako deialdia egitea, buruak aginduta.
- Aztertu beharreko gaiak prestatzea eta arduradunei beharrezko informazioa biltzea.
- Bileren aktak egitea.
- Bileren akta bertaratuei bidaltzea, sinatu dezaten.
- Aktak jagotea, erakundearen dokumentuak kontserbatzeko irizpideen arabera.

2.2.1.2. Segurtasun eta Pribatutasun Batzorde Korporatiboko kideak

Segurtasun eta Pribatutasun Batzorde Korporatiboa osatuko dute tratatutako informazioaren segurtasunaren edo emandako zerbitzuen erantzukizunean, definizioan edo ezarpenean parte hartzen duten pertsona guztiek:

- Gobernu Kontseilua.
- Zerbitzu Orokorretako zuzendaria, batzordeburua izango dena.
- AFAko Segurtasun Arduraduna (SegArd), idazkari jardungo duena.
- Arabako Kalkulu Guneako IKT Segurtasun Arduraduna (IKTSegArd-AKG).
- Zerbitzu Erkideen arduraduna (ZerArd).
- Segurtasun Fisikoaren arduraduna (SFArd).
- Sistemaren arduraduna (SisArd).

Honako hauek hartuko dute parte, aholkulari gisa:

- Datuak Babesteko ordezkaria (DBO), DBEOn xedatutakoaren arabera.

Era berean:

- Gonbidatu gisa parte hartu ahaliko dute jorratu beharreko gaien arabera beharrezkotzat jotzen direnek.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

4/24



2.2.2. Krisi Batzordea (KB)

Krisi Batzordea (KB) **eskatu ahala** deituko da, protokoloak aktibatzeke, premiazko erabakiak hartzeko eta krisi protokoloak formalki aktibatzeke berehala esku hartzea eskatzen duten gorabeherak edo egoerak agertzen direnean.

2.2.2.1. Krisi Batzordearen eginkizun orokorrak

Krisi Batzordearen (KB) eginkizunak honako hauek izango dira:

- Kontingentzia eta jarraitutasun protokoloak aktibatzea, AFAren ohiko funtzionamenduari eragiten dioten salbuespenezko egoerei aurre egiteko.
- Ezohiko neurri operatiboak onartzea, krisiaren larritasunari eta inpaktuari erantzun eraginkorra eta proportzionala emateko.
- Beharrezkoa denean, erakunde eta agintari eskudunei bidalitako jakinarazpenak koordinatzea, aplikatzeko den araudiaren arabera (SEN, NIS2 eta DBEO).
- Krisitik eratorritako inpaktua berreskuratzeko eta arintzeko ekintzak gainbegiratzeko, funtsezko zerbitzuak azkar leheneratzea ziurtatuz eta galerak minimizatuz.
- Krisi Batzordearen aktibazioa eta desaktibazioa ebaluatzea eta erabakitzea, egoeraren bilakaeraren arabera.
- Segurtasun eta Pribatutasun Batzorde Korporatiboa eta beste organo erabakitzaile batzuk krisiaren bilakaerari, identifikatutako arriskuei eta hartutako neurriei buruz informatuta edukitzea.
- Parte hartzen duten arloen arteko koordinazioa bermatzea, sailen arteko komunikazioa eta lankidetzaz erraztuz.
- Krisiaren ondoko berrikuspina sustatzea, ikasitakoak identifikatzeko eta kontingentzia eta erresilientzia planak hobetzeko.

Salbuespenezko egoeren kudeaketari lotuta Krisi Batzordeari esleitzen zaizkion beste eginkizun batzuk Segurtasun eta Pribatutasun Batzorde Korporatiboak onartu beharko ditu.

Krisi Batzordeko burua Segurtasun arduraduna izango da, edo hark eskuordetzen duena.

2.2.2.2. Krisi Batzordeko kideak

Krisi Batzordea osatuko dute gertakari kritikoei erantzuteko neurriak koordinatzean, gauzatzean eta gainbegiratzean funtsezko rolak betetzen dituzten pertsonak, besteak beste:

- AFAko eta Arabako Kalkulu Guneko Zerbitzu Orokorrerako Zuzendaritzako diputatu arduraduna.



- Arabako Kalkulu Guneko zuzendari kudeatzailea.
- Arabako Foru Aldundiko Segurtasun arduraduna.
- Arabako Kalkulu Guneko IKT Segurtasun arduraduna.
- Sistemaren arduraduna (SisArd).
- Arabako Kalkulu Guneko Azpiegituren Arloko arduraduna.
- AFAko Aholkularitza Juridikoko Zerbitzuaren Burutzaren ardura daukan zuzendaritza.
- Kabinete eta Komunikazio Zuzendaritza.
- Datuak Babesteko ordezkaria (DBO), gertakariak datu pertsonalei eragiten dienean.

2.2.3. Segurtasunaren Aholku Batzorde Teknikoa (SAB)

Segurtasunaren Aholku Batzorde Teknikoa (SAB) Arabako Foru Aldundian informazioaren segurtasuna ezarri, jarraitu eta hobetzeko beharrezkoak diren neurri teknikoak eta antolakuntzakoak aztertu, prestatu eta proposatzeaz arduratzen den organo teknikoa da. Segurtasunaren gobernu ereduan definitutako rol eta organoekin koordinatuta betetzen ditu eginkizunak batzorde horrek, eta aplikagarria den araudia betetzen dela eta proposatutako neurriak Segurtasun eta Pribatutasun Batzorde Korporatiboak ezarritako helburu korporatiboekin era egokian bat datozela bermatzen du.

Batzordea **sei hilean behin** bilduko da.

2.2.3.1. Segurtasunaren Aholku Batzorde Teknikoaren eginkizun orokorrak

Hauexek dira Segurtasunaren Aholku Batzorde Teknikoaren (SAB) eginkizunak:

- Zehaztutako neurri eta kontrolen aplikazioa teknikoki koordinatzea.
- Segurtasunaren bilakaerari buruzko proposamen teknikoak eta zirriborroak egitea, teknologia, arau eta arrisku aldatetara egokituta.
- Informazio sistemen kategoria proposatzea.
- Aplikagarritasun adierazpenaren zirriborro teknikoa egitea.
- Gertakariei, auditoretzei, kontrolei eta auditoretza planei, prestakuntzari eta jarraitutasunari buruzko txosten teknikoak prestatzea, Segurtasun arduradunari helarazteko.
- Arriskuen analisia eta kudeaketa teknikoki gauzatzea eta koordinatzea, bai eta BIA direlakoak eta negozioaren jarraitutasun planak ere.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

6/24



- Segurtasunari lotutako gatazka teknikoak kudeatzea eta Segurtasun arduradunari helaraztea, eta, hala badagokio, Segurtasun eta Pribatutasun Batzorde Korporatiboari (SPBK).
- Irizpide eta gomendio teknikoak ematea, datu pertsonalen segurtasunaren eta babesaren arloko lege eta arau betekizunak behar bezala ezartzen laguntzeko.
- Segurtasunari eragin diezaioketen teknologia eta arrisku berriak ebaluatzea, eta horiek behar bezala kudeatzeko beharrezko neurriak proposatzea.
- Datu pertsonalak babesteko araudiaren ziozko neurriak ezartzeko laguntza teknikoa ematea, Datuak Babesteko ordezkariarekin eta tratamenduaren arduradunekin koordinatuta.

Segurtasunaren Aholku Batzorde Teknikoari esleitzen zaizkion beste eginkizun tekniko batzuk Segurtasun eta Pribatutasun Batzorde Korporatiboak onartu beharko ditu, bereziki maila teknikoko segurtasunaren kudeaketarekin zerikusia dutenak.

Segurtasunaren Aholku Batzorde Teknikoaren burua Segurtasun arduraduna izango da, edo hark eskuordetzen duena.

2.2.3.2. Segurtasunaren Aholku Batzorde Teknikoko kideak

Segurtasunaren Aholku Batzorde Teknikoa erakundearen barruan informazioaren segurtasunaren kudeaketa teknikoan eta koordinazioan funtsezko rolak betetzen dituzten pertsonen osatuko dute, besteak beste:

- Segurtasun arduraduna.
- Segurtasun erreferenteak (SegErr).
- Arabako Kalkulu Guneko IKT Segurtasun arduraduna.
- Arabako Kalkulu Guneko teknikariak, landu beharreko gaien arabera.

Honako hauek hartuko dute parte, aholkulari gisa:

- Datuak Babesteko ordezkaria (DBO), landutako gaiak datu pertsonalen babesarekiko lotura dutenean.
- Kanpoko aholkulariak. Eskatu ahala parte hartu ahalko dute, erakundearen behar espezifikoan edo aztertu beharreko gaien arabera.

2.2.4. Segurtasun arduraduna (SegArd)

Segurtasun arduradunak (SegArd) AFaren informazioaren eta zerbitzuen segurtasunaren betekizunak betetzeko beharrezkoak diren erabakiak zehazteko ardura du, segurtasun sistemaren koherentzia, egokitasuna eta eraginkortasuna ziurtatuz.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

7/24



Horretarako, neurri teknikoen eta antolakuntzako ezarpena eta betearazpena gainbegiratu behar ditu, eta lotura gisa jarduten du gobernu organoen, arduradun funtzionalen eta talde teknikoen artean, araudi aplikagarriaren arabera ezarritako baldintzak betetzen direla bermatzeko.

2.2.4.1. Segurtasun arduradunaren eginkizun orokorrak

Segurtasun arduradunaren eginkizunak honako hauek izango dira:

- AFaren Informazioaren Segurtasunaren eta zerbitzuen baldintzak betetzen direla bermatzeko beharrezko erabakiak zehaztea eta gainbegiratzea, segurtasun sistemaren koherentzia, egokitasuna eta eraginkortasuna ziurtatuz.
- Segurtasun eta Pribatasun Batzorde Korporatiboaren (SPBK) deialdia egitea eta haren funtzionamendua koordinatzea, laguntzeko organo tekniko gisa jardunez eta Informazioaren Segurtasunaren arloko politikak, araudiak, planak eta txostenak aurkeztuz, berrikusteko edo onartzeko xedez.
- SPBKri proposatzea Informazioaren Segurtasunaren Politika Korporatiboa, segurtasun araudia eta Segurtasuna Hobetzeko Plana, baliabidez hornitzeko proposamena ere aintzat hartuta.
- SPBKrekiko lotura eta komunikazio kanal gisa jardutea, segurtasun gorabehera garrantzitsuei, arrisku esanguratsuei eta informazioaren segurtasunaren arloko jarraibide estrategikoei dagokienez.
- Eskumena duten organo teknikoek landutako Segurtasunaren Eskema Nazionalaren aplikagarritasun adierazpena onartzea.
- Organo tekniko eskudunek egindako informazioaren segurtasunaren arloko arau esparrua baliozkotzea —politikak, arauak, prozedurak, jarraibideak eta gidak—, Segurtasun Eskema Nazionalera, NIS2 Zuzentaraura eta aplikatzekoa den indarreko gainerako araudira egokitzen dela ziurtatuz.
- Informazio sistemen arriskuen analisiak koordinatzea eta gainbegiratzea, eta sistemen kategoria baliozkotzea, informazioaren arduradunek (InfArd) eta zerbitzuen arduradunek (ZerArd) egindako balorazioetan oinarrituta.
- Kasuan kasuko arduradunek onartutako hondar arriskuak berrikustea eta baliozkotzea, eta erakundeak onartutako arrisku korporatiboaren atalera egokitzen direla egiaztatzea.
- AFaren arrisku maila globalari buruzko txosten bateratuak organo eskudunari helaraztea.
- Datuak Babesteko Erregelamendu Orokorreko printzipioak eta betebeharrak eta adimen artifizialean oinarritutako sistemei aplikatu dakizkiekeen arau betekizunak

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

8/24



neurri teknikoaren eta antolakuntzakoaren diseinuan eta ezarpenean txertatzen direla zaintzea, Datuak Babesteko ordezkariarekin eta arduradunekin koordinatuta.

- Informazioaren segurtasunaren, datu pertsonalen babesaren eta sortzen ari diren teknologiei aplikatu dakiekeen araudiaren arloko legeria nazionalaren eta nazioartekoaren etengabeko jarraipena egitea, adimen artifizialean oinarritutako sistemak ere aintzat hartuta, eta AFAn behar bezala interpretatzea, aplikatzea eta betetzen dela sustatzea.
- Adimen artifizialean oinarritutako sistemen erabilerari lotutako segurtasun arriskuak aztertzea eta baliozkotzea, hedatu aurretik eta ondotik.
- Sistemen segurtasunaren egoera gainbegiratzea, arduradun teknikoek eta zerbitzu hornitzaileek emandako txostenak eta ebidentziak oinarri hartuta.
- Segurtasunaren jarraipena egiteko irizpideak eta adierazleak zehaztea eta metriken txostenak baliozkotzea.
- Kanpora ateratako zerbitzuen hornitzaileek segurtasun arloko betebeharrak betetzen dituztela gainbegiratzea.
- Informazioaren Segurtasunaren arloko gertakariak koordinatzea, eta informazioa Krisi Batzordeari edo, hala badagokio, SPBKri helaraztea.
- Negozioaren jarraitutasunaren eta hondamendien aurreko berreskuratzearen arloan dagozkion eginkizunak betetzea, onartutako jarraitutasun-; esparruarekin bat etorriz.
- AFAn harremanetarako gune gisa jardutea Informazioaren Segurtasunaren arloko agintari eskudunen, erakundeen eta kanpoko eragileen aurrean.

2.2.5. Datu Pertsonalen Tratamenduaren arduraduna (DPTrArd)

Datu pertsonalen tratamenduaren arduradunak dagozkien tratamenduak egiteko ardura duten zuzendaritzetako titularrak izango dira, Datuak Babesteko Erregelamendu Orokorrean eta aplikatzekoa den araudian xedatutakoarekin bat etorriz.

2.2.5.1. Datu Pertsonalen Tratamenduaren arduradunaren eginkizun orokorrak

Tratamenduaren arduradunaren eginkizunak honako hauek izango dira:

- Bere ardurapean dauden datuen tratamenduetan egokiak diren segurtasun neurri teknikoak eta antolakuntzakoak zehaztea eta aplikatzea.
- Arriskuen analisiak eta datuen babesaren arloko eraginaren ebaluazioak egitea bultzatu eta ziurtatzea, hala dagokionean, datuak babesteko ordezkariarekin eta organo tekniko eskudunekin koordinatuta.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

9/24



- Datu pertsonalen segurtasun arrakalak kontrol agintaritzaren eskudunari eta, hala badagokio, interesdunei jakinaraziko zaizkiela bermatzea, lege ezarritako epeen barruan. Horretarako, Datuak Babesteko ordezkararen aholkularitza eta Segurtasun arduradunaren koordinazioa izango ditu.
- Datu pertsonalen babesaren arloan eskubideak baliatzeko eskaerak ebatzea (DBEOren 15. artikulutik 22. artikulura), unitate arduradunaren laguntzarekin eta Datuak Babesteko ordezkararen aholkularitzarekin.
- Datu pertsonalak babesteko arloan indarrean dagoen araudiak esleitzen dizkion gainerako eginkizunak betetzea.

2.2.6. Informazioaren arduraduna (InfArd)

Informazioaren arduradunaren zeregina zuzendaritza bakoitzak izendatutako pertsona batek hartuko du bere gain, eta hari dagokio informazioa bere eskumen eremuaren barruan erabiltzeko, babesteko eta egokitze azken erantzukizuna.

Informazioaren arduradunaren erantzukizunak zerbitzuko arduradunaren erantzukizunekin bateratu daitezke (2.2.7 atalean deskribatutako ZerArd).

Informazioaren arduradunak Segurtasun erreferenteen eta dagozkien unitate teknikoekin laguntzarekin beteko ditu bere eginkizunak.

2.2.6.1. Informazioaren arduradunaren eginkizun orokorrak

Informazioaren arduradunaren eginkizunak honako hauek izango dira:

- Bere ardurapeko informazioaren segurtasun baldintzak ezartzea, datuen konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna, trazabilitatea eta babesa bermatzeko beharrezkoak diren babes mailak ezartzen direla ziurtatuz, AFaren politika eta arauetan ezarritako printzipio eta betekizunekin bat etorriz, bai eta Segurtasunaren Eskema Nazionalarekin eta aplikatzekoa den araudiarekin bat etorriz ere.
- Informazioari lotutako arriskuak aztertze eta kategorizatzeko prozesuetan gogotik parte hartzea, eta organo arduradunekin lankidetzan aritzea kalteberatasunak eta mehatxuak identifikatu, ebaluatu eta sailkatzeko, babes neurri egokiak zehazte aldera, indarrean dagoen araudiaren eta politiken arabera.
- Bere erantzukizuneko informazioaren kudeaketatik eratorritako hondar arriskuak bere gain hartzea eta onartzea, betiere arrisku horiek erakundeak onartutako arrisku atalase korporatiboen barruan badaude.
- Informazioari eragiten dioten segurtasun gertakarien inpaktua behar bezala eta zehatz-mehatz jakinaraztea.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

10/24



2.2.7. Zerbitzuaren arduraduna (ZerArd)

Zerbitzuaren arduradunaren (ZerArd) zeregina zuzendaritza bakoitzak izendatutako pertsona batek hartuko du bere gain, eta pertsona horri egokituko zaio zerbitzuak bere eskumen eremuan emateari, erabilgarritasunari eta egokitzeari buruzko azken erantzukizuna.

Zerbitzuaren arduradunaren erantzukizunak zerbitzuko arduradunaren erantzukizunekin bateratu daitezke (2.2.6 atalean deskribatutako InfArd).

2.2.7.1. Zerbitzuaren arduradunaren eginkizun orokorrak

Zerbitzuaren arduradunaren eginkizunak honako hauek izango dira:

- Bere ardurapeko zerbitzuen segurtasun eta erabilgarritasun-baldintzak definitzea, eta horiek behar bezala ematen direla bermatzeko beharrezko mailak ezartzea, AFaren politika eta arauekin eta Segurtasunaren Eskema Nazionalarekin bat etorriz.
- Zerbitzu kritikoak identifikatzea eta zehaztea, erakundearen jardueran duten eraginaren ikuspegitik, eta arriskuak eta jarraitutasuna aztertzeo prozesuei informazio hori ematea.
- Zerbitzuei lotutako arriskuen analisietan, Negozioaren gaineko Eraginaren Azterketetan (BIA) eta Negozioaren Jarraitutasun Planean parte hartzea, eta organo tekniko eskudunekin lankidetzan aritzea mehatxuak, kalteberatasunak eta inpaktuak identifikatzeko.
- Bere ardurapeko zerbitzuei lotutako hondar arriskuak bere gain hartzea eta onartzea, betiere onartutako arrisku atalase korporatiboen barruan badaude.
- Zerbitzuei eragiten dieten segurtasun gertakarien eragina behar bezala jakinaraztea, eta ardura duten organoek horiek kudeatzea erraztea.

2.2.8. Zerbitzu Erkideen arduraduna (ZerErArd)

Zerbitzu Erkideen arduradunaren (ZerErArd) zeregina horretarako izendatutako pertsonak hartuko du bere gain, eta hari egokituko zaio AFAn izaera erkide eta partekatutako zerbitzuei aplikatu beharreko segurtasun baldintzak koordinatzeko eta definitzeko ardura, ikuspegi homogeneoa, koherentea eta efizientea bermatzeko.

Zerbitzu Erkideen arduradunak segurtasun arduradunarekin, eragindako zerbitzuen arduradunekin eta organo tekniko eskudunekin koordinatuta beteko ditu bere eginkizunak.

2.2.8.1. Zerbitzu Erkideen arduradunaren eginkizun orokorrak

Hauexek izango dira Zerbitzu Erkideen arduradunaren eginkizunak:

- Zerbitzu arduradunen arteko koordinazioa bermatzea, zerbitzu erkide eta partekatuei aplikatutako segurtasun neurrien koherentzia, estandarizazioa eta egokitzapena ziurtatzeko.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

11/24



- Zerbitzu erkideen segurtasun behar estrategikoak eta operatiboak ebaluatzea, haien bilakaera teknologikoa, arau aldaketak eta erakundearen jardueraren ondoriozko betekizunak kontuan hartuta.
- Azpiegitura partekatuen eta zerbitzu erkideen segurtasunari lotutako gobernantza eta kontrol ereduak definitzen parte hartzea.
- Zerbitzu erkideetan parte hartzen duten hornitzaileek eta hirugarrenek segurtasun baldintzak betetzen dituztela koordinatzea eta gainbegiratzea, kontratu akordioetan eta aplikatu beharreko araudian ezarritakoarekin bat etorritik, Segurtasun arduradunarekin koordinatuta.
- Zerbitzu erkideen segurtasunaren etengabeko hobekuntza bultzatzea, arriskua murriztea eta babes gaitasunak optimizatzea helburu duten planak, proiektuak eta jarduerak proposatuz.
- Erakundeko organo eta arloekin lankidetzan aritzea, zerbitzu erkideen segurtasuna Segurtasun eta Pribatutasun Batzorde Korporatiboak zehaztutako Informazioaren Segurtasunaren estrategia orokorrarekin bat datorrela ziurtatzeko.

2.2.9. Datuak Babesteko ordezkaria (DBOrd)

Datuak Babesteko ordezkaria AFAn datu pertsonalen babesari buruzko araudia betetzen den informatzeko, aholkatzeko eta gainbegiratzeko izendatzen den pertsona da, Datuak Babesteko Erregelamendu Orokorrean xedatutakoarekin bat etorritik.

Datuak Babesteko ordezkariak independentzia osoz beteko ditu bere eginkizunak, bere zereginak betetzeko jarraibiderik jaso gabe, eta aholkularitza eta gainbegiratze organo gisa jardungo du, tratamenduen kudeaketan erantzukizun operatiborik hartu gabe.

2.3. Datuak Babesteko ordezkariaren eginkizun orokorrak

Datuak Babesteko ordezkariaren eginkizunak honako hauek izango dira:

- Tratamenduaren arduradunari eta eragileari, bai eta tratamendu eragiketetan parte hartzen duten langileei ere, informazioa eta aholkuak ematea, Datuak Babesteko Erregelamendu Orokorrean eta datu pertsonalak babesteko aplikatu beharreko gainerako araudiaren arabera dagozkien betebeharrei buruz.
- Datuak Babesteko Erregelamendu Orokorrean, datu pertsonalak babesteko AFaren barne politiketan eta erantzukizunen esleipen egokian xedatutakoa betetzen dela gainbegiratzea, kontzientziario eta prestakuntza ekintzak ere aintzat hartuta.
- Tratamenduaren arduradunari aholkuak ematea, datuen babesari buruzko eragin ebaluazioak egiteko eskatzen zaionean, eta horiek behar bezala aplikatzen direla gainbegiratzea.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

12/24



- Tratamenduaren arduradunari aholku ematea datu pertsonalen segurtasun arrakalen kudeaketan, kontrol agintaritzari eta, hala badagokio, interesdunei jakinarazita, Datuak Babesteko Erregelamendu Orokorrean ezarritako epeen eta baldintzen arabera.
- Kontrol agintaritzarekin lankidetzan aritzea eta haren harremanetarako gune gisa jardutea tratamenduari buruzko gaitan, aurretiazko kontsulta eta bidezko beste jarduketa batzuk barne.
- Datu pertsonalen babesarekin zerikusia duten gaiak lantzen dituzten batzorde, lantalde eta bestelako gobernantza organoetan aholkulari gisa parte hartzea, araudia betetzen dela bermatzeko irizpide espezializatuak emanez.
- Datu pertsonalen babesaren arloan indarrean dagoen araudiaren jarraipena egitea, estatuan zein nazioartean, eta AFaren jardueran eragin dezaketen aldaketa garrantzitsuen berri ematea.
- Datu pertsonalak babestearen arloko barne politikak landu, berrikusi eta eguneratzeari buruz aholkatzea eta gainbegiratzea, eta aplikatzekoa den araudiarekin bat datozela egiaztatzea.

2.4. Segurtasunaren eta Datuen Babesaren erreferenteak (SegErr)

Segurtasun erreferentearen zeregina zerbitziburuek edo haiek eskuordetzen dituzten pertsonak beteko dute, eta laguntza operatiboko eta loturako puntu gisa jardungo dute informazioaren segurtasunaren eta datuen babesaren arloan, bere antolamendu eremuaren barruan.

Erreferentearen funtzioa ezarritako neurriak behar bezala aplikatzen laguntzea da, korporazioko arduradunekin lotura gisa jardunez arriskuak aztertzeko jardueretan, negozioaren gaineko eraginaren azterketan (BIA), jarraitutasun planetan, auditoretzetan eta hobekuntza planetan, bai eta tratamenduaren arduradunari datu pertsonalak babesteko araudia betetzen laguntzean ere. Illo horretan, honako hauetan parte hartuko dute: arriskuen identifikazioan eta kudeaketan, inpaktu ebaluazioak egitean, hala dagokionean, segurtasun arrakalak kudeatzean eta neurri teknikoak eta antolakuntzakoak behar bezala ezartzean.

Antolamendu ereduari esker, pertsona berak hainbat rol har ditzake bere gain, eta, horretarako, arduradunen arteko etengabeko koordinazioa behar da, bai eta bitarteko eta baliabide teknikoaren hornidura egokia ere, ezarritako betebeharrak benetan beteko direla bermatzeko.

2.4.1.1. Segurtasunaren eta Datuen Babesaren erreferentearen eginkizun orokorrak:

Segurtasunaren eta Datuen Babesaren erreferentearen eginkizunak honako hauek izango dira:

- Bere eremuan, segurtasun auditoretzak egiten laguntzea eta erraztea, bai eta auditoria horien ondoriozko hobekuntza planen jarraipen operatiboa egitea ere.



- Bere sailaren edo erakundearen eta Segurtasun arduradun korporatiboen (InfArd eta ZerArd) arteko solaskidetza eginkizunak betetzea, komunikazio eraginkorra eta arina erraztuz.
- Bere eremuan, informazioaren segurtasunaren arloko neurri teknikoak eta antolakuntzakoak behar bezala aplikatu eta zabaltzen lagundu, koordinatu eta bultzatzea.
- Bere eremuan, informazioaren segurtasunaren prozesuetan, negozioaren gaineko eraginaren azterketan (BIA), negozioaren jarraitutasun planak (BCP) eta hondamendien aurreko berreskuratze planak (DRP) egiten eta horien jarraipena egiten parte hartzea, eta zerbitzuari buruzko informazioa eta ezagutza ematea.
- Bere sailari edo erakundeari buruzko informazioaren segurtasunaren arloan eskatutako informazioa, ebidentziak eta dokumentazioa prestatzea eta ematea.
- Aldizka eta sistematikoki informatzea informazioaren segurtasunaren egoerari buruz, identifikatutako arriskuei buruz eta bere eremuan hautemandako gorabeheriei buruz arduradun korporatiboei (InfArd eta ZerArd).
- Bere eremuari eragiten dioten segurtasun gertakarien kudeaketa operatiboa babestea, beharrezko informazioa emanez eta kasuan kasuko arduradunekin koordinatuz.
- Informazioaren segurtasunaren eta datu pertsonalen babesaren arloko arau betekizunak praktikan aplikatzen laguntzea, tratamenduaren arduradunei eta datuak babesteko ordezkariei laguntza operatiboa emanez.
- Hobekuntza operatiboak proposatzea informazioaren segurtasunaren eta datu pertsonalen babesaren arloan, bere eremuko zerbitzuen eta prozesuen benetako funtzionamenduaren ezagutzan oinarrituta.
- Bere eremuko datu pertsonalen tratamenduak identifikatzen laguntzea, bai eta arriskuen kudeaketa egiten ere, arriskuen analisiak eta inpaktuaren ebaluazioak egitea barne, hala dagokionean (IEDB).
- Datu pertsonalen segurtasun arrakalak detektatzen eta kudeatzen laguntzea, eta, horretarako, datuen babesaren arloko neurri teknikoak eta antolamendukoak aplikatzea erraztea.
- Datuak babesteko harremanetarako gune operatibo gisa jardutea bere eremuaren barruan, dagozkion arduradunekin koordinatuta.

2.4.2. Sistemaren arduraduna (SisArd)

Sistemaren arduraduna (SisArd) informazio sistemen eragiketaz, administrazioaz eta mantentzeaz arduratzen da, segurtasun arduradunak zehaztutako neurri teknikoekin eta antolakuntzako neurriekin eta segurtasunaren gobernu ereduaren ezarritako jarraibideekin bat etorriz.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

14/24



Sistemaren arduradunak sistemaren bizi ziklo osoan betetzen ditu bere eginkizunak, eta funtzionamendua segurtatzen du, erakundeak zehaztutako segurtasun, erabilgarritasun eta jarraitutasun betekizunen arabera.

2.4.2.1. Sistemaren arduradunaren eginkizun orokorrak

Sistemaren arduradunaren eginkizunak honako hauek izango dira:

- Informazio sistemak beren bizi ziklo osoan jardutea eta mantentzea, organo eskudunek ezarritako segurtasuneko neurri teknikoak eta antolakuntzakoak aplikatuz.
- Sistemak barne eta kanpo mehatxuetatik babesteko beharrezkoak diren segurtasun babesak implementatzea eta mantentzea, aldian-aldian behar bezala funtzionatzen dutela egiaztatuz.
- Beharrezkoak diren eguneratzeak, zuzenketak eta hobekuntza teknikoak gauzatzea, segurtasun adabakien aplikazio egokia eta sistemen konfigurazio egokia ziurtatuta.
- Segurtasun auditoretzetatik, ebaluazio txostenetatik eta onartutako hobekuntza planetatik eratorritako neurri zuzentzaileak aplikatzea.
- Informazioaren segurtasuneko gertakariak detektatzen, aztertzen eta konpontzen laguntzea, eragindako sistemei eusteko, arintzeko eta berreskuratze euskarri teknikoak emanez.
- Negozioaren jarraitutasun eta berreskuratze prozedurak gauzatzea hondamendien aurrean (BCP/DRP), bere ardurapeko sistemetan aplikatzekoak direnak, onartutako planen arabera.
- Informazio tekniko, ebidentziak eta datu garrantzitsuak ematea sistemen segurtasun egoeraren jarraipena egiteko, auditoriak, arriskuen analisiak eta gertakariak kudeatzeko.

2.4.3. Segurtasun Fisikoaren arduraduna (SegFArd)

Segurtasun Fisikoaren arduraduna (SegFArd) arduratuko da AFaren instalazioak eta aktibo fisikoak babesteko baldintzak definitzeaz, ezartzeaz eta kudeatzeaz, bere eskumen eremuaren barruan, segurtasun arduradunak ezarritako jarraibideen arabera.

Segurtasun fisikoko neurriek sistemak eta zerbitzuak osorik babesten lagunduko dutela bermatuko du, erresilientzia operatiboa eta jardueraren jarraitutasuna babestuz.

2.4.3.1. Segurtasun Fisikoaren arduradunaren eginkizun orokorrak

Segurtasun Fisikoaren arduradunaren eginkizunak honako hauek izango dira:



- Bere eskumen eremuko instalazioei, bulegoei eta aktibo fisikoei aplikatu beharreko segurtasun fisikoaren baldintzak definitzea, segurtasun arduradunak ezarritako jarraibide eta irizpideekin eta aplikatu beharreko araudiarekin bat etorriz.
- Segurtasun arduradunarekin lankidetzan aritzea, segurtasun fisikoaren eta segurtasun logikoko politiken eta neurrien arteko koherentzia eta integrazioan laguntzeko.
- Segurtasun fisikoaren neurriei eta pertsonen sarbide kontrolari dagokienez, sistemak, instalazioak eta kokalekuak kudeatzea eta gainbegiratzea, bereziki sarbide mugatuko eremuak.
- Arlo eskudunekin koordinatuta, hainbat arlotan sartzeko baimena duten pertsonen zerrenda kudeatzea eta egiaztatzea, bai eta sarreren eta irteeren erregistroekiko koherentzia ere.
- Arriskuen analisietan laguntzea, ingurune fisikoei lotutako mehatxuei, kalteberatasunei eta inpaktuei buruzko informazioa emanez.
- Datu zentroen ekipamenduan egiten diren jarduketak gainbegiratzea (instalazioa, aldaketa, erretiratzea), baita sarreren eta irteeren kontrola eta erregistroa ere.
- Segurtasun fisikoaren aldizkako ikuskapenak egitea eta dagozkion auditoretzetan laguntzea, gabeziak edo arriskuak atzematen direnean hobekuntzak proposatuz.
- Segurtasun fisikoaren arloan langileak eta bisitariak prestatzeko eta kontzientziatzeko ekintzak bultzatu eta kudeatzea, sartzeko, ebakutzeko eta gorabeheren aurrean jarduteko protokoloak barne.
- Segurtasun fisikoaren gertakarien kudeaketan eta erantzunean parte hartzea, eta organo arduradunekin lankidetzan aritzea, inpaktuak arintzeko eta jarraitutasun operatiboa errazteko.
- Segurtasun fisikoaren prozedurak eta protokoloak eguneratuta edukitzea, eta aplikatzekoak diren barneko eta kanpoko araudiarekin bat datoze la ziurtatzea.
- Segurtasun fisikoarekin lotutako simulazio ariketak planifikatzen eta egiten laguntzea.
- Bere eskumen eremuan, hornitzaileei eta kanpo zerbitzuei lotutako segurtasun fisikoaren alderdiak koordinatzea eta gainbegiratzea.

2.4.4. Erabiltzaileak (Erab)

Arabako Foru Aldundiaren informazio sistematarako sarbide baimendua duten pertsona guztiak izango dira, barnekoak edo kanpokoak, erakundearekin duten harreman mota edozein dela ere.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

16/24



Erabiltzaileak arduratuko dira AFaren politiketan eta arauetan ezarritako informazioaren segurtasun neurriak betetzeaz, bai eta aplikatu beharreko gainerako legeetan eta araudian ezarritakoak betetzeaz ere.

Beren eginkizunak betetzean, informazio sistemak modu seguru eta arduratsuan erabili beharko dituzte, kudeatutako informazioa babesten lagunduz eta haren konfidentziasuna, osotasuna, erabilgarritasuna, benetakotasuna eta trazabilitatea zainduz.

2.4.4.1. Erabiltzaileen eginkizun orokorrak

Erabiltzaileen eginkizun orokorrak hauexek dira:

- Informazioaren Segurtasunaren Politika Korporatiboan zehaztutako segurtasun printzipioak ezagutzea eta betetzea, bai eta Informazio Sistemak Erabiltzeko Araudian eta aplikagarri diren gainerako politika, araudi eta legeetan ezarritako betebeharrak ere.
- Aplikatzekoak zaizkien prozedurak ezagutzea eta betetzea, beren eginkizunak eta betebeharrak betetzeko erabiltzen dituzten sistemen eta informazioaren babesa bermatzeko.
- Arabako Foru Aldundiak informazioaren segurtasunaren arloan antolatutako prestakuntza eta kontzientzia-ekintzetan parte hartzea.
- Informazioaren segurtasuna arriskuan jar dezakeen edozein susmo, erabilera oker edo segurtasun gorabeheraren berri berehala ematea.
- Segurtasun arduradunarekin eta segurtasun arloko erreferenteekin lankidetzan aritzea, ezarritako prozeduren arabera, babes neurriak ezartzeko eta indartzeko.
- Sarbide kredentzialen konfidentziasunari eta segurtasunari eustea, horiek arduraz erabiliz eta kudeatzeko metodo seguruak erabiliz.

2.5. Gatazkak koordinatzeko eta konpontzeko bideak

Organigrama honetan definitutako rolei esleitutako eginkizunak betetzearen inguruko lotutako desadostasunak, gainjartzeak edo eztabaidak sortzen diren egoeretan —bai informazioaren segurtasunaren arloan, bai datu pertsonalen babesaren arloan—, gatazka hori aztertzeke eta ebazteko erantzukizuna Segurtasun eta Pribatutasun Batzorde Korporatiboari (SPBK) dagokio.

Era berean, segurtasun jarduera, prozesu eta neurrien koordinazio egokia bermatzeko, Segurtasun eta Pribatutasun Batzorde Korporatiboak hartutako jarraibide eta erabakiei jarraikiz jardungo da. Batzorde horrek orientabide estrategikoko eta lerrotze orokorreko eginkizunak beteko ditu, eta Segurtasuneko arduradunari dagokio beharrezkoak diren jarduketan koordinazio operatiboa eta teknikoa egitea.



1. eranskina: Segurtasunaren eta Datuen Babesaren rolak esleitzea – Izendapenak

Segurtasun rolak profil hauen arabera esleitu dira:

- **Segurtasun eta Pribatutasun Batzorde Korporatiboko kideak Gobernu Kontseiluak izendatzen ditu.**
- **Segurtasun arduraduna (SegArd)** indarreko egiturari buruzko dekretuan ezarritakoaren arabera izendatuko da, eta Arabako Foru Aldundiaren egitura zentralizatuaren barruan, rol horretarako zehaztutako eginkizunak, eskumenak eta eskuduntzak bere gain hartuko dituen pertsona izango da.
- **Segurtasun Fisikoaren arduraduna (SegFArd)** Segurtasun eta Pribatutasun Batzorde Korporatiboak proposatuta izendatzen da, eta Arabako Foru Aldundiaren egitura zentralizatuaren barruan rol horretarako ezarritako funtzioak, eskumenak eta eskuduntzak betetzen dituen pertsona izango da.
- **Informazioaren arduradunaren (InfArd)** zeregina dagokion informazioa kudeatzeko ardura duten zuzendaritzetako titularrek hartuko dute beren gain.
- **Datu pertsonalen tratamenduaren arduradunak (TrArd)** dagozkien tratamenduak egiteko ardura duten zuzendaritzetako titularrak izango dira, Datuak Babesteko Erregelamendu Orokorrean eta aplikatzekoa den araudian xedatutakoarekin bat etorritik.
- **Zerbitzuaren arduradunaren (ZerArd)** zeregina dagokion informazioa kudeatzeko ardura duten zuzendaritzetako titularrek hartuko dute beren gain.
- **Sistemaren arduradunaren (SisArd)** zeregina Segurtasun eta Pribatutasun Batzorde Korporatiboak proposatuta izendatzen da, eta Arabako Foru Aldundiaren egitura zentralizatuaren barruan rol horretarako ezarritako funtzioak, eskumenak eta eskuduntzak betetzen dituen pertsona izango da.
- **Zerbitzu Erkideen arduraduna (ZerErArd)** Segurtasun eta Pribatutasun Batzorde Korporatiboak proposatuta izendatzen da, eta Arabako Foru Aldundiaren egitura zentralizatuaren barruan rol horretarako ezarritako funtzioak, eskumenak eta eskuduntzak betetzen dituen pertsona izango da.
- **Segurtasunaren eta Datuen Babesaren Erreferentearen (SegErr)** zeregina zerbitzu bakoitzeko buruek edo horretarako berariaz izendatutako pertsonak hartuko dute beren gain, baldin eta, dagokion sailaren burutzaren eremuan, rol horretarako ezarritako eginkizunak, eskumenak eta eskuduntzak betetzen badituzte.
- **Datuak Babesteko ordezkaria (DBOrd)** erakundeak berak izendatuko du, Datuak Babesteko Erregelamendu Orokorrean eta aplikatzekoa den araudian xedatutakoaren arabera.

Segurtasun eta Pribatutasun Batzorde Korporatiboko kide bakoitzak boto bat izango du arduradunak izendatzeko, pertsona horrek rol ugari betetzen dituela ere.

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

18/24



Zuzendaritzan aldaketak daudenean, kideen eginkizunetan eragina izan dezaketenean edo izendatutako rolari doakion lanpostua hutsik geratzen denean berrikusiko dira rolak.

Era berean, izendatutako arduradunak ordeztu ahal izango dira, baldin eta beren eginkizunetan eraginkortasunik eza eragin dezaketen absentsia luzeak gertatzen direnean edo, iraupen laburrekoak izanik ere, horrek sistemari eragiten diotenean.



2. eranskina: Segurtasunaren eta Datuen Babesaren rolak esleitzea – AOKI kodeak

Ardura	SegArd	SegFArd	InfArd	DPTTrArd	ZerArd	ZerErArd	SisArd	SegErr.	DBO	UB
Segurtasun Antolakunde Korporatiboa	K	K	I	I	I	I	I	I	I	I
Informazioaren Segurtasunaren Politika Korporatiboa	ARR	I	K	K	K	K	K	I	I	I
Segurtasuna kudeatzeko helburuak eta planak	ARR	K	K	K	K	K	K	I		I
Informazioak beharrezkoak dituen segurtasun mailak	ARR		A	A	I	I	K	I		
Zerbitzuak beharrezkoak dituen segurtasun mailak	ARR		I	I	A	A	K	I		
Sistemaren kategoria zehaztea	O / A		I	I	I	I	I	I		
Arriskuen analisia	ARR	K	I	I	I	I	K	K		
Aplikagarritasun adierazpena	O / A	I	I	I	I	I	K	I		
Baliabideak ematea	K	K	K	K	I	I	I			
Segurtasun konfigurazioa	A		I	I	I	I	ARR	I		
Hondar arriskua onartzea	ARR	K	K	K	K	K	K	I		
Segurtasun araudia	O / A	K	K	K	K	K	K	I		I
Segurtasun prozedurak	O / A	I	I	I	I	I	A	I		I
Interes taldeekiko barremanak	O / A		I	I	I	I	I			
Segurtasun neurriak ezartzea	K	I	I	I	I	I	ARR	I		I

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

20/24



Ardura	SegArd	SegFArd	InfArd	DPTArArd	ZerArd	ZerErArd	SisArd	SegErr.	DBO	UB
Segurtasun neurriak gainbegiratzea	O / A	K	K	K	K	K	K	I		
Sistemaren segurtasun egoera	O / A		I	I	I	I	I	I		
Segurtasun zerbitzuaren gaineko akordioa	A	I	K	K	ARR	ARR	I	I		
DBEOren kudeaketa	K		I	ARR				I	K	I
Segurtasuna hobetzeko planak	O / A	I	I	I	I	I	K		I	
Kontzientiazio eta prestakuntza planak	O / A	I	I	I	I	I	K			I
Gorabeheren kudeaketa	O / A		I	I	I	I	K	I	I	I
Datu pertsonalen segurtasun arrakalak kudeatzea	K		I	ARR				K	K	
Negozioaren jarraitutasun planak	K	I	I	I	O / A	O / A	K	I	K	I
Zerbitzua kautelaz etetea	A		I	I	K	K	ARR			I
Segurtasuna bizi zikloan	K		I	I	I	I	O / A			I

A: Arduraduna / O: Oneslea / K: Kontsultatua / I: Informatua

SegArd: Segurtasun arduraduna / **SegFArd:** Segurtasun Fisikoaren arduraduna / **InfArd:** Informazioaren arduraduna / **DPTArArd:** Datu Pertsonalen Tratamenduaren arduraduna / **ZerArd:** Zerbitzuaren arduraduna / **ZerErArd:** Zerbitzu Erkideen arduraduna / **SisArd:** Sistemaren arduraduna / **SegErr:** Segurtasunaren eta Datuen Babesaren arloko erreferenteak / **DBOOrd:** Datuak Babestekoordetzakaria / **Erab:** Erabiltzaileak



3. eranskina: Segurtasun rolak esleitzea – AOKI batzordeak

Ardura	SPBK	SAB
Segurtasun Antolakunde Korporatiboa	O / A	I
Informazioaren Segurtasunaren Politika Korporatiboa	A	I
Segurtasuna kudeatzeko helburuak eta planak	A	I
Informazioak beharrezkoak dituen segurtasun mailak	I	I
Zerbitzuak beharrezkoak dituen segurtasun mailak	I	I
Sistemaren kategoria zehaztea		
Arriskuen analisia	A	I
Aplikagarritasun adierazpena		I
Baliabideak ematea	O / A	I
Segurtasun konfigurazioa		
Hondar arriskua onartzea	A	I
Segurtasun araudia	I	I
Segurtasun prozedurak	I	I
Interes taldeekiko harremanak	I	I
Segurtasun neurriak ezartzea		I
Segurtasun neurriak gainbegiratzea	I	I

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

22/24



Ardura	SPBK	SAB
Sistemaren segurtasun egoera	I	I
Segurtasun zerbitzuaren gaineko akordioa	K	I
DBEOren kudeaketa	I	I
Segurtasuna hobetzeko planak	I	I
Kontzientziazio eta prestakuntza planak	K	I
Gorabeheren kudeaketa	I	I
Negozioaren jarraitutasun planak	K	I
Zerbitzua kautelaz etetea	I	I
Segurtasuna bizi zikloan		

A: Arduraduna / O: Oneslea / K: Kontsultatua / I: Informatua
SPBK: Segurtasun eta Pribatutasun Batzorde Korporatiboa / SAB: Segurtasuneko Aholku Batzorde Teknikoa

Datuen segurtasuna eta babesa antolatzea
Dokumentuaren sailkapena: Publikoa

23/24