Informazioaren Segurtasuna Kudeatzeko Sistema

Erabiltzaileen betebehar orokorrak

Honek onartua *Aprobado por*	Segurtasun eta Pribatutasun Korporatiboaren Batzordea	***Erreferentzia*** *Referencia*	Erabiltzaileen betebehar orokorrak
Data *Fecha*	2025-06-10	***Jasotzaileak*** *Distribución*	Langile guztiak

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

Bertsioen kontrola

Bertsioa	Data	Aurreko bertsioarekiko aldaketa	Nork egina	Nork berrikusia	Nork onartua
1.b	2018/11/29	Hasierako bertsioa	Segurtasuneko Bulego Teknikoa	Segurtasuneko Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboaren Batzordea
2.b	2021/11/17	Kanpoko segurtasunerako neurriak sartu dira (VPN erabilera). Euskarri ateragarrien kudeaketaren atala eguneratu da. Betebeharrak ez betetzearen ondorioak aipatzen dira.	Segurtasuneko Bulego Teknikoa	Segurtasuneko Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboaren Batzordea
3.b	2023/11/15	Formatu aldaketa, hutsen zuzenketa eta indargabetutako arauak eguneratu. Datu pertsonalen babesari eta Platea segurtasun-eskuliburuari buruzko aipamenak kendu.	Segurtasuneko Bulego Teknikoa	Segurtasuneko Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboaren Batzordea
4.b	2025/06/10	Titulu nagusia eguneratzea. IKTZ sailaren izena EDZ izatera aldatzea, antolaketa-egitura berria dela eta.	Segurtasuneko Bulego Teknikoa	Segurtasuneko Batzorde Teknikoa	Eusko Jaurlaritzako Segurtasun eta Pribatutasun Korporatiboaren Batzordea

EUSKO JAURLARITZA
GOBIERNO VASCO

GureSeK

Edukia

1. Sarrera

Datu pertsonalen babesaren arloan (DBEO) eta zerbitzu elektronikoen segurtasunaren arloan (ENS) aplikatzekoak diren legezko betebeharretatik datoz arau hauek. Euskal Autonomia Erkidegoko Administrazio Publikoaren (aurrerantzean, EAEko Administrazio Publikoa) segurtasun-erregulazioan daude jasota. GureSeKen garatzen da erregulazio hori, eta **«Informazioaren Segurtasun eta Pribatutasun Politika»** dokumentuan dago jasota.

1.1 *Dokumentuaren helburua*

Dokumentu honen helburua hauxe da: EAEko Administrazio Publikoko erabiltzaileek Administrazioko zerbitzu elektronikoei lotutako datu pertsonalak, informazioa edo dokumentazioa erabiltzerakoan bete behar dituzten betebehar orokorrak zehaztea.

Dokumentu honen bidez, langile guztiek informazioaren segurtasunaren eta datu pertsonalen pribatutasunaren arloan bete behar dituzten gidalerro orokorrak ezarri nahi dira.

Dokumentu hau EAEko Administrazio Publikoak emandako zerbitzuei buruz eta, bereziki, zerbitzu horiek bitarteko elektronikoen bidez emateari buruz dauden edozein datu pertsonali, dokumentu guztiei edo bestelako informazio guztiei (egituratuta egon zein ez) aplikatu behar zaie.

2. Ikuspegi orokorra

2.1 *Definizioa*

«Erabiltzaileen betebehar orokorrak» informazioaren segurtasunaren eta datu pertsonalen pribatutasunaren ikuspegitik bete beharreko jarraibideak ezartzen dituen dokumentua da, EAEko Administrazio Publikoak zerbitzuak ematearekin zerikusia duen dokumentazio, datu pertsonal edo informazio oro erabiltzerakoan bete beharrekoa.

2.2 *Irismena*

Dokumentu honetan jasota dauden erabiltzaileen betebehar orokorrak EAEko Administrazio Orokorreko langile guztiek bete behar dituzte datu pertsonalen tratamenduan zein administrazio elektronikoaren arloan, bai eta Administrazioaren zerbitzuetako bati lotutako dokumentuak edo informazioa eskura ditzaketen kanpoko enpresa azpikontratatuetako langile guztiek ere.

2.3 *Helburuak*

Hauek dira erabiltzaileen betebehar orokorren dokumentuaren helburuak:

- EAEko Administrazio Publikoaren zerbitzuak ematen edo datu pertsonalen tratamenduan nola edo hala parte hartzen duten pertsona guztien betebeharren bilduma izatea.
- EAEko Administrazio Publikoaren zerbitzuak emateari lotutako informazioa zein dokumentazioa eta datu pertsonalak tratatzean bete behar diren jokabide-arau orokorrak ezartzea.

2.4 *Aplikazio-eremua*

Erabiltzaileen betebehar orokor hauek EAEko Administrazio Publikoko langileek eta hark datu pertsonalen arloan edota administrazio elektronikoaren arloan azpikontratatzen dituen langile guztiek aplikatu beharko dituzte jarraian ageri diren egoeretan:

- Erabiltzailearen ekipamendu informatikoa erabiltzean.
- EAEko Administrazio Publikoak emandako bitarteko elektroniko mugikorrak erabiltzean.
- EAEko Administrazio Publikoak lanbide-jarduera egiteko emandako baliabide eta zerbitzuak eskuratzean.
- EAEko Administrazio Publikoaren dokumentuak erabiltzean, bai formatu elektronikoan, bai inprimatuta.

- EAEko Administrazio Publikoak ematen dituen zerbitzuei buruzko informazioa kudeatzean.
- EAEko Administrazio Publikoak datu pertsonalen tratamenduan.

2.5 *Salbuespenak*

Hemen biltzen diren betebehar guztiak bete behar dira, salbuespenik gabe. Betebeharren bat urratuz gero, Eusko Jaurlaritzako Korporazioaren Segurtasun eta Pribatutasun Batzordeak berariaz aztertuko du urraketa hori.

Araudi hau ez da aplikatu behar Segurtasun Publikoaren EAEko Zerbitzuak kontsumitu, tratatu edo sortu duen informazioan, baldin eta, informazio horren ezaugarriak direla eta, Europako Parlamentuaren eta Kontseiluaren 2016/679 (EB) Erregelamenduaren irispidetik at badago [2016/679 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituena]. Horrelakoetan, Europako Parlamentuaren eta Kontseiluaren 2016/680 (EB) Zuzentarauak arautuko du informazio hori [2016/680 (EB) Zuzentaraua, 2016ko apirilaren 27koa, Europako Parlamentuarena eta Kontseiluarena, pertsona fisikoak babestearen gainekoa, agintari eskudunek arau-hausteak edo zigor penalak prebenitu, ikertu, antzeman edo auzitaratzeko asmoz datu pertsonalak tratatzeari buruz eta datu horiek aske zirkulatzeari dagokienez; eta Kontseiluaren 2008/977/AI Esparru Erabakia indargabetzen duena].

3. Erabiltzaileen betebehar orokorrak

Erabiltzaileek dokumentu honen edukia ezagutu eta aintzat hartu beharko dute. Beraz, erabiltzaile guztiek dokumentuaren kopia bat eskuratu ahal izango dute, eta dokumentu honetan xedatuta dagoenaren arabera beteko dituzte agintzen zaizkien zereginak.

Informazioaren segurtasuna bermatzeko, erabiltzaileek jarraian ageri diren jokabidearauak bete beharko dituzte.

3.1 *Informazioa sailkatzea eta tratatzea*

#	Informazioa sailkatzea eta tratatzea
1	Erabiltzaile guztiek jakin beharko dute lanean erabiltzen duten informazioa eta dokumentazioa (hala balitz) zein segurtasun-mailatan dagoen sailkatuta, eta informazio mota horretarako ezarritako jarraibideen arabera erabili beharko dute.
2	Informazioaren sailkapena EAEko Administrazio Publikoko Informazioaren Sailkapenerako Politikan ezarritako gidalerroek zehaztuko dute.
3	Orokorrean, informazio baten segurtasun-maila ezarrita ez badago, edo bere segurtasunaren katalogazioa BALORATU GABE badago, informazio hori ez sailkatutzat joko da. Aldiz, informazio edo dokumentazio baten segurtasun-maila TXIKI, ERTAIN EDO HANDI gisa ezarri bada, informazio hori informazio sailkatutzat joko da, eta halakotzat joko da zerbitzu bati lotutako informazioa eta dokumentazioa ere, bere segurtasun-maila TXIKI, ERTAIN EDO HANDI gisa ezarri bada.

#	Informazioa sailkatzea eta tratatzea
4	Hauek dira sailkatutako informazio edo dokumentazioa maneiatzean zaindu behar diren jokabide-arauak: a. Dokumentazioa garatzeko, txantiloi ofizialak eta EAEko Administrazio Publikoan estandarizatutako formatuak erabili beharko dira beti. b. Erabilitako txantiloi eta formatuen metadatu eta eremu osagarriak nahitaez bete beharko dira, eta eremu bat betetzea egokia ez bada, eremu horiek beren-beregi ez aplikagarri gisa azalduko dira. c. Informazioa eta dokumentazioa kudeatzeko, ezarrita dauden prozedura eta protokoloei jarraitu beharko zaie, eta une oro bermatu beharko da lotutako administrazioprozedurak betetzea. d. Formalki onartutako dokumentazioa soilik argitaratu ahalko da ingurune irekietan (intranet, estranet edo Internet), eta bermatu beharko da aldaketa-fasean dagoen informazioaren eta dokumentazioaren kudeaketa ez dela administrazio-inguruneetatik irtengo, aldaketak onartu arte. e. Informazio edo dokumentazio bat ingurune irekietan (intranet, estranet edo Internet) argitaratu aurretik, **informazio horretan dokumentuen hartzaileentzat egokia ez den metadatu edo eremu ezkuturik ez dagoela ziurtatu beharko da**. Horretarako, dokumentuen garbiketarako ezarrita dauden tresnak erabili beharko dira. f. Onarpena eman ostean, ingurune irekietan dagoen informazioa eta dokumentazioa eguneratu beharko da. Une oro egokia den prestasunez jokatu beharko da presari eta ezarritako prozedurak betetzeari dagokienez. g. Informazio edo dokumentu jakin batek duen kopia kopurua ahalik eta txikiena izango da, eta kontuan hartu beharko da kopia horiek aldi baterakoak direla. h. Arreta berezia jarri beharko da publikoki sailkatutako informazioa ez dibulgatzeko (ponentzietan edo azalpen publikoetan, Internet bidez eta abar), salbu eta esanbidezko baimena badago. Halaber, kontu handiz jokatu beharko da mota horretako informazioa ingurune publikoetan edo EAEko Administrazio Publikoko bulegoetatik kanpo ez erabiltzeko, ez ahoz, ez formatu elektroniko edo inprimatuan. i. Kontu handiz jokatu beharko da informazio sailkatua eduki dezakeen dokumentazio inprimaturik ez galtzeko.
5	ERABILGARRITASUN ERTAIN edo HANDIko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, neurri hauek ere bete beharko dira: a. Ingurune irekietan argitaratutako informazioan edo dokumentazioan egin beharreko aldaketak ahalik eta txikienak izango dira. Ahal dela, ingurune horietara erabiltzaile gutxien sartzen diren epealdietan egingo dira aldaketok, eskuragarri dauden erabileraestatistikak kontuan hartuta. Informazioa eskura ez egoteari lotutako gorabehera guztiak ELZri jakinarazi beharko zaizkio, lehenbailehen ebatz ditzan, 3.13 atalean (Gorabeheren kudeaketa) ezarrita dagoenaren arabera.
6	OSOTASUN ERTAINeko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, neurri hauek ere bete beharko dira: a. Ingurune irekietan argitaratutako informazioan edo dokumentazioan egin beharreko aldaketak ahalik eta txikienak izango dira, eta onarpen fasean dagoen edukia bereziki egiaztatu beharko da. Informazio edo dokumentazio horren inguruan ezarritako aldaketak eta bertsioak kudeatzeko prozedurak zorrozki bete beharko dira.

#	Informazioa sailkatzea eta tratatzea
7	OSOTASUN HANDIko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez eta OSOTASUN ERTAINeko informaziorako espezifikoki ezarritakoez gain, neurri hau ere bete beharko da: Sinadura Elektronikoaren Politika aplikatu beharko da osotasun maila horrekin sailkatutako informazioa sinatzeko.
8	KONFIDENTZIALTASUNA BALORATU GABE duen informazio guztia informazio publikotzat jo beharko da. Halako informazioa tratatzeko, atal honen 5. eta 6. puntuetan egindako oharrak bete beharko dira, hurrenez hurren, erabilgarritasun eta osotasun betekizun bereziak dituen informazioari buruz. Informazio hori erabiltzeko, neurri horiez gain, hau bete beharko da: Informazio publiko gisa katalogatuta dagoen informazioa edo dokumentazioa soilik argitaratu ahalko da Interneten.
9	KONFIDENTZIALTASUN ERTAINeko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, beste neurri hauek ere bete beharko dira: a. Zorrozki bete beharko dira idazmahai garbiari buruz 3.4 atalean (Lanpostua) eta 3.5 atalean (Erabiltzailearen ekipamendu informatikoa) zehaztutako politikak, atal horien barruan espezifikoki ezarritako jarraibideekin. b. Informazioa konfidentzialtasun maila horrekin kokatzen edo tratatzen den ingurune bakoitzeko arduradunei ingurune horietan sartzeko eskariak jakinarazi beharko zaizkie. Hala, haiek baimenduko dituzte sarbide horiek, baita sarbideen aldaketak ere. c. Informazioa konfidentzialtasun maila horrekin kokatzen edo tratatzen den inguruneetara sartzeko baimenak aldizka berrikusi beharko dira, arduradunek sartzeko baimen horiek egiazta ditzaten. d. Ahal dela, konfidentzialtasun maila hori duen informazioa EAEko Administrazio Publikoaren bulegoetatik kanpo ahalik eta gutxien erabiliko da. Erabili behar izanez gero, ezarrita dauden segurtasun-neurriak areagotu beharko dira, batez ere, informazio horrek konfidentzialtasuna galtzeari dagokionez. Konfidentzialtasun maila hori duen informazio-kopia bat beharrezkoa ez bada, bereziki kontuan hartu beharko da kopia hori ezabatu behar dela; neurri horrek erabiltzaileen ekipamendu eta mahaietan biltegiratuta dauden kopiei eragiten die batez ere.

#	Informazioa sailkatzea eta tratatzea
10	KONFIDENTZIALTASUN HANDIko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez eta KONFIDENTZIALTASUN ERTAINeko informaziorako espezifikoki ezarritakoez gain, neurri hauek ere bete beharko dira: a. Konfidentzialtasun-maila hori duen informazio guztia zifratu egin beharko da, bai biltegiratzean, bai transmititzean. Horretarako, EAEko Administrazio Publikoak ingurune desberdinetan horretarako ezarritako zifratze-tresnak erabiliko dira: 1) Komunikazioetan VPN erabiltzea. 2) Ordenagailu eramangarrietan diskoa zifratzea. 3) Ordenagailu pertsonaletan, bitarteko erauzgarrietan (CDak, DVDak, USB memoriak eta abar) eta zerbitzarietan fitxategiak, karpetak eta unitateak zifratzeko tresnak. 4) Aplikazioek beraiek inplementatutako zifratzea, beharrezkoa bada. b. Konfidentzialtasun-maila hori duen informazioa partekatzen bada, ez da informazio horri buruz hitz egin beharko leku publikoetan edo eremu irekietan, ezta EAEko Administrazio Publikoaren bulegoetan ere. Elkarrizketa horiek behar bezala itxitako gela pribatuetan egin beharko dira, hirugarrenek ezer ere entzun ez dezaten. c. Konfidentzialtasun-maila hori duen informazio horrekin lan egitean, kontu handiz jokatu beharko da, behar ez duen inork ere informazio hori ikus ez dezan. Beraz, dokumentu guztiak –paperezkoak zein elektronikoak– estali edo babestu beharko dira, «disimulurik gabeko begiradak» saihesteko. d. Konfidentzialtasun-maila horretako informazioa duten dokumentuek behar bezala babestuta egon beharko dute. Espresuki baimenduta dauden erabiltzaileek soilik eskuratu ahalko dituzte halako dokumentuak. e. Paperean dagoen informazioa behar bezala gorde beharko da, leku egokietan. Leku horietara sartzeko, beharrezkoa izan beharko da behintzat giltza bat edukitzea edo pasahitz bat jakitea. Arreta handiz jokatu beharko da konfidentzialtasun-maila hori duen informazioaren kopiak egiterakoan. Ahalik eta kopia gutxien egin beharko dira, eta jatorrizkoei aplikatzen zaizkien babes-neurri berak aplikatu beharko zaizkie.
11	BENETAKOTASUN ERTAIN edo HANDIko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, neurri hau ere bete beharko da: Sinadura Elektronikoaren Politika aplikatu beharko da benetakotasun maila horrekin sailkatutako informazioa sinatzeko.
12	TRAZABILITATE ERTAINeko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, neurri hau ere bete beharko da: Informazio hori tratatzeko, edukien kudeaketarako, dokumentuen kudeaketarako edo bertsioen kudeaketarako plataformak edo antzekoak erabili beharko dira. Horien bidez, informazioak jasaten dituen aldaketak eta ondoz ondoren dituen egoerak automatikoki erregistratu ahalko dira.

#	Informazioa sailkatzea eta tratatzea
13	TRAZABILITATE HANDIko informazio sailkatua erabiltzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez eta TRAZABILITATE ERTAINeko informaziorako espezifikoki ezarritakoez gain, neurri hauek ere bete beharko dira: a. Informazio hori tratatzeko, edukien kudeaketarako, dokumentuen kudeaketarako edo bertsioen kudeaketarako plataformak edo antzekoak erabili beharko dira. Horien bidez, informazio horren inguruan erabiltzaileek egin duten jarduera automatikoki erregistratu ahalko da, eta informazioa eskuratzen den bakoitzean identifikatuko da zein erabiltzailek eskuratu duen, zein unetan, zer eskurapen mota egin den eta zein izan den eskurapen horren emaitza. Informazio hori tratatzeko DOKUSI plataforma erabili beharko da, administrazio-dokumentu elektronikoaren formarekin, eta plataforma horrek denbora-zigilu eta guztiko sinadura elektronikorako eskaintzen dituen funtzioak erabiliko dira.

3.2 *Datu pertsonalen tratamendua*

#	Datu pertsonalen tratamendua
1	Datu pertsonalen tratamendua legezkoa, leiala eta gardena izango da, interesdunari dagokionez. Horrez gain, honako printzipio hauek bete behar dira: zilegitasuna, fideltasuna eta gardentasuna.
2	Xedea mugatzeko printzipioa ere beteko da. Horrek eskatzen du datu pertsonalak xede zehatz, esplizitu eta bidezkoetarako biltzea, eta, bildu ondoren, ezin izango dira tratatu xede horiekin bateraezinak diren xedeetarako. Horren harira, interes publikoaren onurarako artxibatzea, zientzia-ikerketak egitea, ikerketa historikoak egitea edo estatistikak egitea ez dira inoiz bateraezinak izango hasierako xedeekin.
3	Datuak txikiagotzeko printzipioa beti hartuko da aintzat. Horrek eskatzen du datuak egokiak eta mugatuak izatea, zertarako tratatzen diren kontuan hartuta.
4	Zehaztasun-printzipioa beteko da. Horren arabera, datuak zehatzak eta, beharrezkoa bada, eguneratuak izango dira. Arrazoizko neurri guztiak hartuko dira tratamenduaren helburuen ikuspegitik zehaztugabeak diren datu pertsonalak berehala ezabatzeko ala zuzentzeko.
5	Datuak gordetzeko epea mugatzeko printzipioa bete behar da, eta interesdunak identifikatzeko datu pertsonalak ez dira gordeko datu pertsonalaren helburuak betetzeko behar den denboran baino denbora handiagoan. Horretatik salbuetsita daude interes publikoaren onurarako artxibatuta daudenak eta zientzia-, historia- edota estatistika-ikerketak egiteari buruzkoak; horiek epe luzeagoetan gorde ahalko dira, hargatik eragotzi gabe dokumentu honetan ezartzen diren teknika- eta antolaketa-neurri egokiak aplikatzea, interesdunaren eskubideak eta askatasuna babesteko.

#	Datu pertsonalen tratamendua
6	Datuen segurtasuna babesteko printzipioa beti bete beharko da. Horren arabera, datu pertsonalen tratamenduan bermatu behar dira baimenik gabeko edo legez kontrako tratamenduaren aurkako babesa, bai eta datuok ustekabean galdu, suntsitu edo kaltetzearen aurkako babesa ere bai. Horretarako, antolaketa- eta teknika-neurri egokiak erabili beharko dira, EAEko Administrazio Publikoak garatuta. Neurri horiek tratamendubaliabideak zehaztean eta tratamendua bera egitean aplikatu beharko dira. Horrela, modu lehenetsian bermatu beharko da tratamenduaren helburu espezifiko bakoitzerako behar diren datuak baino datu gehiago ez hartzea.
7	Datu pertsonalak tratatzeko jarduera guztiak behar bezala erregistratu behar dira Tratamenduen Erregistroan. Hortaz, Tratamenduen Erregistroa eguneratu beharko da, tratamendu berri bat gehitzen bada, tratamendua aldatzen bada, edo bertan behera uzten bada.
8	Tratamendu berri edo aldatu baten ezaugarriak, irispidea, testuingurua, xedea edo behar dituen teknologiak direla eta, tratamendu horrek pertsona fisikoen eskubideak eta askatasuna arrisku larrian jartzen baditu, beharrezkoa izango da tratamendu horrek datu pertsonalen babesean izan dezakeen inpaktua ebaluatzea, tratamendua egiten hasi aurretik.

3.3 *Identifikazioa eta autentifikazioa*

#	Identifikazioa eta autentifikazioa
1	Informazio-sistemak erabili ahal izateko, erabiltzaileak sarbide baimendua eduki behar du. Oro har, erabiltzailearen izena eta pasahitza erabiltzen dira.
	Pasahitzak JAKINAn «*Informatika eta Telekomunikazioak*» atalean dagoen SARguneren Pasahitzen Politika bete beharko du.
	Erabiltzaileak sinadura elektroniko aurreratua edo, informazioaren ezaugarrien arabera, bere burua identifikatzeko egokia den beste baliabide bat eduki beharko du, informazioaren arduradunak edo datu pertsonalen tratamenduaren arduradunak hori eskatzen badu. Horrelakorik erabiltzen duenean, aurreko zenbakian (2) ezarritako jarduketa-arauak aplikatu beharko dira, behar bezala egokituta.

3.4 *Baliabideen erabilera egokia*

EAEko Administrazio Publikoak ematen dituen baliabide materialak, informatikoak, komunikazio-baliabideak edo beste edozein motatako baliabideak, erabiltzaileak bere lana egitean bete behar dituen zereginak betetzeko soilik ematen dira Hala, EAEko Administrazio Publikoak kontrolsistemak ezarri ahalko ditu baliabide horiek babesten eta behar bezala erabiltzen direla ziurtatzeko. Dena den, langilearen duintasuna eta intimitaterako eskubidea zainduz baliatuko du ahalmen hori.

Hori dela eta, hauxe bete behar dute langileek:

#	Betebeharrak
1	Birusen kontrako programak eta programa horien eguneratzeak erabiltzea, eta beharrezko arreta jartzea, informazio-sistemak atzipen eta erabilera baimendu gabeetatik babesteko eta erabiltzen duten materialaren hondatzea edo bestelako kalteak ez gertatzeko.
2	Estrategia Digitalaren Zuzendaritzak, EJIEk edo behar bezalako baimena duen beste hornitzaile batek eman dituen software-bertsioak baino ez erabiltzea, eta erabilera-arauak beti betetzea. Ezin izango dute inolaz ere instalatu programen legez edo arauz kanpoko kopiarik; eta ezin dituzte inolaz ere ezabatu legez instalatu direnak.
3	Pertsonei buruzko identifikazio-datuak eta helbideak bulegotika-tresnetako (adibidez, Outlook) harremanetarako agendetan baino ez dira sartuko.

Xede hori betetzeko, hauek debekatuta daude:

#	Debekuak
1	Erabiltzaile bakoitzak lanpostuan berez dituen egitekoez bestelako jarduerak egiteko erabiltzea baliabideak.
2	Administrazioan eskumena duen erakundeak baimendu ez dituen jarduerak, ekipamenduak edo aplikazioak.
3	Administrazioa arriskuan jar dezaketen edukiak sartzea informazio-sistemetan edo sare korporatiboan. Edukiok lizunak, mehatxagarriak, immoralak edo iraingarriak izan daitezke, bai eta bestelakoak ere.
4	Programak, birusak, makroak, miniaplikazioak, ActiveX kontrolak, usnariak, crackinga eragiteko aplikazioak edo informatika-sistemetan aldaketak edo kalteak edo informaziolapurreta eragin ditzakeen edozein gailu logiko edo fisiko nahita sartzea.
5	Administrazioko baliabide telematikoak hondatzen, eraldatzen edo nola edo hala erabilezin bihurtzen saiatzea.
6	Informatika-sistemen jarduera-erregistroak (log) okertzen edo faltsutzen saiatzea.

3.5 *Lanpostua*

Erabiltzaile guztiek euren lanpostuetan idazmahai garbiari buruzko politika hau bete beharko dute:

#	Idazmahai garbiari buruzko politika
1	Lanpostuek garbi egon beharko dute. Mahai gainean egongo diren dokumentu bakarrak unean uneko jarduera egiteko beharrezkoak direnak izango dira.
2	Paperezko dokumentu guztiak nahiz informazio elektronikoko euskarri guztiak leku itxi batean gordeko dira, erabiltzen ari ez direnean.

3.6 *Erabiltzailearen ekipamendu informatikoa*

Erabiltzailearen ekipamenduak erabiltzen ari direnean, honako betebehar hauek bete beharko dira:

#	Betebeharrak
1	Eskura duten informazioaren konfidentzialtasuna, ahal denean, babestu behar dute, baimenik ez duen beste inori erakutsi gabe eta behar ez den bezala tratatu edo erabili gabe, informazioa edozein euskarritan bildurik dagoela ere.
2	Ekipamendu informatiko bakoitza erabiltzaile baimendu baten erantzukizunaren mende egongo da, eta hark ziurtatuko du ekipoak erakusten duen informazioa ikusgai ez izatea pertsona baimendu gabeen aurrean.
3	Horrek esan nahi du ekipamendu informatikoarekin konektaturik dauden pantailek nahiz inprimagailuek edo bestelako gailuek fisikoki egon beharko dutela konfidentzialtasun hori ziurtatzen duten tokietan.
4	Ekipamendu informatiko baten arduraduna ekipamendu horren kokaleku fisikotik aldi baterako urruntzen denean, informazio sailkatua ikustea eragotziko duen egoera batean utzi beharko du ekipamendu hori, adibidez, ekipamendua blokeatuz. Berriz ere lanari ekiteko, blokeoa desaktibatu behar du dagokion pasahitzaren bitartez. Lan-txanda bukatu duelako ekipamendutik aldendu behar badu, erabiltzaileak guztiz itxi beharko du sisteman hasitako saioa
5	Informazio sailkatua daukaten paper-formatuko ahalik eta txosten gutxien erabili, eta txosten horiek toki seguruan eta hirugarrenen irismenetik kanpo eduki behar dituzte.
6	Ordenagailu pertsonaletako disko lokaletan ezin dute gorde informazio sailkaturik, ezta bereziki datu pertsonalak dauzkan fitxategirik ere.
7	Informazioaren edo datu pertsonalen behin-behineko kopiek eta datu horien jatorrizko fitxategi nagusiek segurtasun-neurri berak eduki behar dituzte, betiere, baldin eta segurtasun-maila horri eutsi behar bazaio, hautatutako datuen tipologia kontuan hartuta eta datuen jatorria zein xedea ere kontuan hartuta. Kopiak zertarako egin ziren, xede horietarako jada beharrezkoak ez direnean, kopiak sortu zituen erabiltzaileak ezabatu beharko ditu.

#	Betebeharrak
8	Inprimagailurik egonez gero, irteera-erretiluan datu babestuak dauzkan agiririk inprimatuta ez dagoen ziurtatu behar du. Inprimagailuak informazioa eskuratzeko baimenik ez duten beste erabiltzaile batzuekin konpartitzen badira, ekipamendu bakoitzaren arduradunek dokumentuak jaso beharko dituzte inprimatu ahala, edo, ahal izanez gero, inprimaketa atxikia erabili (pasahitz batez babestua, ikus *«Funtzio anitzeko gailuak konfiguratu eta erabiltzeko jardunbide egokien gida»*).
9	Erabiltzailearen ekipamendu informatikoek konfigurazio finkoa izango dute beren aplikazioetan, sistema eragileetan eta abarretan. Informazioaren arduradunak, datu pertsonalen tratamenduaren arduradunak edo administratzaile baimenduek baino ezin dute aldatu konfigurazio hori.
10	Erabiltzaile guztiek euren ekipamendu informatikoetan instalatutako segurtasun-tresnak (suebakiak, antibirusak, antimalwareak, informazioa zifratzeko tresnak, VPN tresnak eta abar) behar bezala erabili beharko dituzte.
11	Debekatuta dago erabiltzailearen ekipamendu informatikoetan segurtasuna babesteko instalatu den edozein tresna, programa, baliabide edo software mota desgaitzea.
12	Ordenagailu eramangarrien erabiltzaileak ahal den neurrian saiatuko dira Eusko Jaurlaritzaren barneko baliabideetarako sarbide-gakorik ez jartzen ekipamendu horietan.
13	KONFIDENTZIALTASUN HANDIko informazioa ordenagailu eramangarri batean aldi baterako biltegiratuta badago, zifratuta gorde beharko da, xede horrekin ekipamenduan ezarrita dauden tresnak erabiliz.

3.7 *Segurtasuna kanpoan*

Erabiltzaile batek, EAEko Administrazio Publikoaren bulegoetatik kanpo dagoela, edozein informazio sailkatu erabiltzen edo atzitzen duenean, jokabide-arau hauek bete beharko ditu:

#	Jokabide-arauak
1	Informazioa atzitzean ahalik eta zuhurtzia handienaz jokatu beharko du. Beste pertsona batzuek informazio hori kasualitatez ikustea (paperezko dokumentuan bertan edo erabiltzailearen ekipamenduko pantailan irakurriz edo elkarrizketa entzunez) eragotzi beharko du.
2	Arreta bereziaz jokatu beharko da erabiltzailearen paperezko dokumentu, informazio-euskarri edo ekipamenduen galera edo lapurreta eragozteko, halakoetan informazio sailkatua badago edo galera edo lapurreta gertatuz gero halako informazioa atzitu ahal bada.
3	KONFIDENTZIALTASUN ERTAIN edo HANDIko informazioarekin lan eginez gero, arreta bereziaz bete beharko dira 3.1 ataleko 9. eta 10. puntuetan (**Informazioa sailkatzea eta tratatzea**) xede horretarako ezartzen diren gidalerroak.

#	Jokabide-arauak
4	Galera edo lapurreta gertatuz gero, edo informazio sailkatuaren konfidentzialtasuna nola edo hala urratu dela susmatuz gero, berehala ELZri edo informazioaren arduradunari (unean-unean egoki denari) abisua eman beharko zaio, segurtasun-gertakaria irekitzeko, 3.13 atalean (**Gorabeheren kudeaketa**) ezarrita dagoenaren arabera.
5	EAEko Administrazio Publikoaren instalazioetatik kanpo informazio-sistemetara sartu behar izanez gero, VPN sare baten bidez sartu beharko da, eta erabiltzaileari tokiko sarbideetarako dituen baimen berberak esleituko zaizkio. Urruneko sarbidea eskatzeko, saileko informatikariak egingo dio eskaera Erabiltzaileen Segurtasun Zerbitzuari, eta hark baliozkotuko ditu sarbide horiek. Aplikazio jakin baterako sarbidea behar izanez gero, Erabiltzaileen Segurtasun Zerbitzuak aplikazioaren arduradunari bidaliko dio eskaera.

3.8 *Sareko baliabideak*

Erabiltzaileen esku uzten diren datuak, aplikazioak eta gainerako baliabide informatikoak sortu diren eta ezarri diren zeregina gauzatzeko baino ez dira erabiliko. Oro har, erabiltzaileek dute horretarako erabiltzen direla ziurtatzeko ardura. Alde horretatik, informatika-sistemetan sartzeko aukera duten pertsonek segurtasun-neurri hauek bete beharko dituzte:

#	Segurtasun-neurria
1	Beharrezkoa den baimenik gabe, informatika-baliabideekin ez konektatu sare korporatiborako konexioa ahalbidetzen duen inolako komunikazio-tresnarik.
2	Estrategia Digitalaren Zuzendaritzak(EDZ), EJIEk edo eskumena duen beste erakunde batek (tratamenduaren arduraduna EJIE ez denean) zehaztu edo eman dituen baliabideez bestelako baliabiderik ez erabili sare korporatiboan sartzeko.
3	Ez saiatu norberaren edo beste batzuen informazio-sistemetako eremu murriztuetara sartzen, ez eta esleituta dituzten sarbideez bestelako sarbideak erabiltzen ere.
4	Ez saiatu prozesu telematikoetan esku hartzen duten gakoak, enkriptatze-sistemak, algoritmoak edo segurtasun-elementuak deszifratzen.
5	Ez edukitzea, garatzea edo exekutatzea beste erabiltzaile batzuen lanean interferentziak eragin dezakeen programarik, ez eta baliabide informatikoetan kalteak edo aldaketak eragin dezakeenik ere.

3.9 *Helbide elektronikoa*

Posta elektronikoa erabiltzeari dagokionez, printzipio hauek ezartzen dira:

#	Printzipioa
1	Posta elektronikoa beste lan-tresna bat izango da. Tresna hori erabiltzaileari ematen zaio, zertarako egin den, erabiltzaileak horretarako erabil dezan.
2	EAEko Administrazio Publikoaren posta elektronikoko sistema ezingo da erabili iruzurrezko mezurik, mezu lizunik, mehatxagarririk edo antzekorik bidaltzeko.
3	Erabiltzaileek ezingo dute publizitate-mezurik edo mezu piramidalik (erabiltzaile askori heltzen zaizkienak) sortu, bidali edo birbidali.
4	Posta elektronikoaren bidezko informazio-trukeari dagokionez, jarduera hauek ez daude baimendurik: a. Copyright bidez babestutako materiala igorri edo jasotzea Jabetza Intelektuala Babesteko Legea urratuz. b. Material pornografikoa, sexu esplizituzko mezuak edo txantxak, arrazakeriazko adierazpen baztertzaileak edo iraingarri edo legez kontrakotzat har daitekeen beste edozein adierazpen edo mezu igorri edo jasotzea. c. Baimendu gabeko hirugarrenei igortzea erakundearen materiala edo nolabait konfidentziala den materiala. d. Datu Pertsonalak babesteko Legea edo EAEko Administrazio Publikoaren jarraibideak urratzen dituzten fitxategiak igorri edo jasotzea. EAEko Administrazio Publikoaren jarduerari lotu gabeko datu eta informazio mota oro igortzea edo jasotzea.
5	Berariaz beteko dira informazioaren bidalketari buruz indarrean dauden legezko xedapenak; posta elektronikoaren erabilera, ahal den neurrian, datuak babestearen, trazabilitatearen, benetakotasunaren, konfidentzialtasunaren eta nahitaezko onarpenaren arloan baldintza bereziak ezartzen ez diren kasuetara mugatuko da. Bestela, lehentasuna emango zaie EAEko Administrazio Publikoak komunikazio eta jakinarazpen elektronikoak igortzeko ezarritako bide ofizialei.
6	Posta elektronikoa babesteko ezarritako segurtasuneko tresna guztiak erabili beharko dira: a. Sinadura elektronikoaren erabilera kanporako mezu elektronikoetan, haien benetakotasuna eta osotasuna bermatu nahi direnean b. Zifratuaren erabilera konfidentzialtasuna bermatu nahi den mezu elektronikoetan Antibirusa erabiltzea, mezu elektronikoek birusik ez daukatela egiaztatzeko.
7	Ez da onartuko posta elektroniko bidez KONFIDENTZIALTASUN HANDIko informaziorik bidaltzea, ezta kategoria bereziko datu pertsonalik ere, salbu eta komunikazio elektronikoa zifratuta badago, eta bidalketa berariaz onartu bada.
8	Hartzaile izateko sartutako helbide elektronikoak berariaz egiaztatuko dira, ahal den neurrian mezu elektronikoak okerreko helbideetara ez bidaltzeko.
9	Arreta berezia jarriko zaio Bcc (kopia ezkutua) eremuak erabiltzeari, erabiltzaile edo erakunde askori, banaketa-zerrendei edo EAEko Administrazio Publikotik kanpoko zenbait erakundetako hartzaileei bidalitako mezu guztien pertsona edo erakunde hartzaileak definitzeko.
10	Herritarrekiko eta beste erakunde batzuekiko elkarreraginerako posta-kontu generikoak erabili beharko dira. Kasu horietan, posta-kontu pertsonalizatuak ahalik eta gutxienetan erabili beharko dira, soilik ezinbestekoa den kasuetarako.

3.10 *Internet*

Interneterako sarbideari dagokionez, gidalerro hauek kontuan hartuko dira:

#	Gidalerroa
1	Internet lan-tresna bat da. Interneten egiten diren jarduera guztiek lotura izan beharko dute laneko eginbeharrekin. Erabiltzaileek ez dituzte bilatu edo bisitatu behar EAEko Administrazio Publikoaren eginbeharren edo eguneroko lanaren euskarri ez diren webguneak.
2	Sare korporatibotik Interneterako sarbidea mugatuta dago, sare horretan ezarritako kontrol-sistemen bidez. Konektatzeko bestelako bitartekoek aurrez baliozkotuta egon beharko dute, eta, kasu horietan ere, Interneten erabilerari buruz aipatutako zehaztapenak bete beharko dira.
3	Erabiltzaileek ezingo dute erabili EAEko Administrazio Publikoaren izena, sinboloa, logotipoa edo antzekorik Interneteko ezein elementutan (posta elektronikoan, web-orrietan eta abarretan), ez bada laneko jarduerei lotutako arrazoiengatik.
4	Internetera edo Internetetik datu-transferentziak egitea onartuko da, soilik EAEko Administrazio Publikoaren jarduerekin lotura badute. Debekatuta dago jarduera horiekin zerikusirik ez duten fitxategi-transferentziak egitea (adibidez, ordenagailuko jokoak, soinu-fitxategiak, multimedia-edukiak eta abar deskargatzea).
5	Erabiltzaileek ezin izango dute inola ere beren nortasuna isildu edo manipulatu, identifikatzaile anonimoak erabiltzea baimenduta dagoen kasuetan izan ezik.
6	Interneten erabilerari dagokionez, jarduera hauek ez daude baimendurik: a. Copyright bidez babestutako materiala igorri edo jasotzea Jabetza Intelektuala Babesteko Legea urratuz. b. Material pornografikoa, sexu esplizituzko mezuak edo txantxak, arrazakeriazko adierazpen baztertzaileak edo iraingarri edo legez kontrakotzat har daitekeen beste edozein adierazpen edo mezu igorri edo jasotzea. c. Baimendu gabeko hirugarrenei igortzea erakundearen materiala edo nolabait konfidentziala den materiala. d. Datu Pertsonalak babesteko Legea edo EAEko Administrazio Publikoaren jarraibideak urratzen dituzten fitxategiak igorri edo jasotzea. e. EAEko Administrazio Publikoaren jarduerari lotu gabeko datu eta informazio mota oro igortzea edo jasotzea. f. Interneteko zenbait jardueratan parte hartzea, hala nola berri-taldeetan, jolasetan edo EAEko Administrazio Publikoaren jarduerarekin lotura zuzenik ez duten beste batzuetan. EAEko Administrazio Publikoaren izen ona kalte dezaketen jarduerak egitea. Halakotzat jotzen dira EAEko Administrazio Publikoko langileek euren onura ekonomikorako edo hirugarrenen onura ekonomikorako egindako jarduerak, jarduera politikoak edo antzeko beste batzuk.
7	EAEko Administrazio Publikoko langileek gizarte-sareetan parte hartzen badute, Lehendakaritza Sailak argitaratutako «Eusko Jaurlaritzaren gizarte-sareetako erabileren eta estiloaren gida» izenburuko dokumentuan ezarritakoa bete beharko dute.

3.11 *Webgune korporatiboak*

Ingurune irekietatik (intranet, estranet eta Internet) erabili ahal den edozein webgune korporatibotan informazioa eta dokumentazioa argitaratzeari dagokionez, gidalerro hauek kontuan hartu beharko dira:

#	Gidalerroa
1	Webgunean argitaratutako informazioaren osotasuna babesteko neurriak hartuko dira, EAEko Administrazio Publikoaren izen ona kalte dezaketen baimenik gabeko aldaketak prebenitzeko.
2	Informazioa publiko objektiboaren esku jarri aurretik baimen formala emateko prozedura bat inplementatuko da.
3	Sarbide publikoko sistema guztietan hauxe hartu beharko da kontuan: a. Informazioa lortu, prozesatu eta emateko indarreko legeria bete behar da; bereziki, DPBEDBLO eta IGMEZL. b. Argitaratzen edo prozesatzen den informazioak zuzena izan behar du. c. Informazio konfidentziala argitaratu aurreko urratsetan babestu behar da. d. Argitalpen-sistemak ez du aukerarik eman behar ezbeharrez beste ingurune batzuetara sartzeko. e. Informazioa webgune publikoan argitaratzeko ardura duen pertsona identifikatu behar da. Argitaratutako informazioaren baliozkotasuna eta indarraldia bermatu behar dira.
4	Interneten informazio publikoa soilik argitaratu ahalko da, informazio horren KONFIDENTZIALTASUNA BALORATU GABE gisa sailkatu bada. Kasu horretan, EAEko Administrazio Publikoko langileek informazio hori jendaurrean jartzeko betebeharra izango dute.
5	Estraneteko ingurunean KONFIDENTZIALTASUN TXIKI edo ERTAINeko informazioa soilik argitaratu ahalko da, eta bigarren kasu horretan, baldin eta informazio eta dokumentazio hori atzitzeko baimena duten kanpoko pertsonek informazio eta dokumentazio hori eskuratu behar badute.
6	Intranet orokorreko ingurunean (*Jakina*) KONFIDENTZIALTASUN TXIKIko informazioa soilik argitaratu ahalko da. KONFIDENTZIALTASUN ERTAINeko informazioa eta dokumentazioa atzitzeko kontrola duten *Jakina* inguruneetan ere argitaratu ahalko da; sarbidea, betiere, informazio eta dokumentazio hori eskuratu behar duten pertsona-taldeek soilik izango dute.
7	KONFIDENTZIALTASUN HANDIko informazioa inola ere ez da argitaratuko ingurune ireki batean.

3.12 *Euskarrien kudeaketa*

Erabiltzaileek segurtasun-neurri hauek bete behar dituzte informazioaren euskarri ateragarrien kudeaketari dagokionez:

#	Segurtasun-neurria
1	Ez dira euskarri ateragarriak erabili behar EAEko Administrazio Publikoaren informazioarekin. Informazio hori partekatzeko, Office 365 tresna korporatiboak (OneDrive, Sharepoint) erabiltzea lehenetsiko da.
2	Espresuki debekatzen da GOI-MAILAKO informazioa, KONFIDENTZIALA, SENTIKORRA edo baliokidea garraiatzeko euskarri ateragarriak erabiltzea. Gainerako informaziokategorietarako, euskarria zifratuta egon behar da (kontsultatu Zifratze-gida).
3	Aparteko premien kasuan, sailetako, erakunde autonomoetako edo zuzenbide pribatuko erakunde publikoetako zerbitzu-zuzendaritzek aldi baterako erabilerako USBak hornitu ahal izango dituzte.
4	Informazioa duten euskarriak — eta, bereziki datu pertsonalak dituztenak— nahitaez itzuli behar dira, haiek aldi batean erabili beharra eragin duten lanak bukatu eta berehala.
5	Informazioa daukaten euskarriak, erabili behar ez direnean, leku seguruan eta giltzapean gorde behar dira, lanaldia amaitutakoan batez ere. Nolanahi ere, euskarri horiek toki seguruetan gorde behar dira, datu horiek erabiltzeko baimenik ez duten pertsonak leku horietan ez sartzeko.
6	Euskarriak erabiltzen eta biltegiratzen ari diren bitartean, euskarriok behar bezala kontserbatzeko beharrezkoak diren neurriak hartu beharko dira eta euskarriak fabrikatzen dituen enpresak mantentze-lanerako ezartzen dituen eskakizunak aintzat hartuko dira tenperaturari, hezetasunari eta ingurumeneko beste erasotzaile batzuei dagokienez.
7	Informazioa daukaten euskarriek argi eta garbi identifikatuta egon beharko dute, kanpoko etiketa batekin. Etiketa horrek zuzenean edo zeharka adieraziko du euskarriak duen informazioaren sailkapen-mailarik handiena.
8	Berrerabil daitezkeen euskarrietan bildutako informazio oro ezabatu beharko da, euskarria berriz erabili baino lehen.
9	Berrerabil daitezkeen informazio-euskarriak, batez ere barruan datu pertsonalen kopiak eduki dituztenak, guztiz formateatu behar dira (ezin da formatu azkarra erabili) beste pertsona batek erabili baino lehen. Beraz, datuak berreskuratzeko modurik ez dagoela utzi behar dira euskarriak. Kasu horietan, komenigarria litzateke modu fisikoan ezabatzeko tresna segururen bat («wipe» egitea deritzona) erabiltzea.
10	Informazioa barnean duten euskarrien sarrera guztiak erregistratu beharko dira, eta entrega egin behar duen garraiolaria identifikatu beharko da.

3.13 *Erosketak*

Hardwareko edo softwareko produktuak erosten eta zerbitzuak kontratatzen dituzten pertsona guztiek honako gidalerro hauek bete beharko dituzte:

#	Gidalerroa
1	Segurtasunak zeregin garrantzitsua duen hardwareko edo softwareko produktuak erosten direnean, eta hardware- eta software-produktuak datu pertsonalak tratatzeko erabili nahi direnean, Erosketen Segurtasun eta Pribatutasun Gida aplikatu beharko zaie.
2	Segurtasun-zerbitzuak, segurtasunak zeregin garrantzitsua duen zerbitzuak edo datu pertsonalak tratatu behar diren zerbitzuak kontratatzen direnean, Erosketen Segurtasun eta Pribatutasun Gida aplikatu beharko da.

3.14 *Gorabeheren kudeaketa*

Erabiltzaileek gorabeheren kudeaketa egokia bideratu behar dute. Horretarako, segurtasun-neurri hauek bete beharko dituzte:

#	Segurtasun-neurria
1	ELZri jakinarazi beharko diote informazioaren segurtasunari eragiten dion edo eragin diezaiokeen edozer gorabehera (beste pertsona batzuek sarbide baimendua bidegabe erabiltzearen susmoa izatea, datuak berreskuratzea eta abar). Paperezko zerrendak edo agiriak edo informazio-euskarri elektronikoak –disketeak, CDak, DVDak, USB memoriak edo beste edozein motatako euskarri elektronikoak– galduz gero, horren berri eman beharko zaio informazioaren arduradunari (Antolaketa-egitura eta segurtasun-rolak onesten dituen Jaurlaritzaren 2015eko ekainaren 30eko Erabakiaren arabera).
2	Erabiltzaile batek gorabehera baten berri izan arren, jakinarazten ez badu, fitxategiaren segurtasunaren aurkako falta bat egin duela joko da.

3.15 *Sekretu-eginbeharra*

#	Segurtasun-neurria
1	Langile guztiek zuhurtzia handienaz jokatuko dute mugagabeko denboraz, informazio sailkatua edo datu pertsonalak ez dituzte erabiliko baimendu gabeko xedeetarako eta ez dituzte kanpora aterako, hori egiteko behar den baimenik izan ezean, Enplegatu Publikoaren Oinarrizko Estatutuari buruzko urriaren 30eko 5/2015 Legegintzako Errege Dekretuan ezarrita dagoen bezala.
2	Lanpostuaren zereginak direla eta, erabiltzaileak isilpeko informazioa atzitzen badu – euskarri batean dagoelako, edo beste baliabide baten bitartez–, informazio hori aldi batean baino ezin izango duela eduki joko da, eta, horrez gain, isilpean eduki beharra izango du, eta ez da jabetza-, titulartasun-, kopia- edo banaketa-eskubiderik sortuko.

4. Eranskinak

4.1 I. eranskina: Lotutako dokumentuak eta prozedurak

#	Dokumentua / Prozedura
1	Funtzio anitzeko gailuak (DMF) konfiguratu eta erabiltzeko jardunbide egokien gida
2	Erosketen segurtasun eta pribatutasun gida
3	Eusko Jaurlaritzaren gizarte-sareetako erabileren eta estiloaren gida
4	Informazioa sailkatzeko politika
5	Sinadura elektronikoko politika
6	Informazioaren segurtasun- eta pribatutasun-politika
7	Aldaketak edo bertsioak kudeatzeko prozedurak
8	Informazioa eta dokumentazioa kudeatzeko prozedurak
9	Eusko Jaurlaritzak ezarritako zifratze-tresnak
10	Dokumentuak garbitzeko tresnak
11	Zifratze-gida

4.2 II. eranskina: Terminoen eta laburduren glosarioa

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

#	Terminoa	Definizioa
1	Aktiboa	Erakundearentzat balioa duen osagaia, funtzioa edo baliabidea —informazioa, datuak, zerbitzuak, aplikazioak, ekipamenduak, komunikazioak, administrazio-baliabideak, baliabide fisikoak eta giza baliabideak...—
2	Mehatxua	Informazio-sistema bati edo erakunde bati kalte egin ahal dion gorabehera baten kausa [UNE 71504:2008]. Mehatxuak beti daude presente, baina mehatxuak gauzatzearen ondorioak saihesten edo arintzen saia daitezke.

#	Terminoa	Definizioa
3	Arriskuen azterketa	Informazio-sistema batek izan ditzakeen mehatxuak, ahulguneak, arriskuak eta eraginak aztertzeko prozesua, kontuan hartuta jada ezarrita dauden segurtasun-neurriak. Eraginkortasunari eta kostuei dagokienez, segurtasun-neurrien hobekuntzak identifikatzeko abiapuntu gisa erabiltzen da.
4	Benetakotasuna	Entitate batek adierazitako identitatea egiazkoa dela edo datuen iturria bermatzen duela adierazten duen ezaugarria da [ENS].
6	ELZ	Erabiltzaileei laguntza emateko zerbitzua da, Eusko Jaurlaritzan erabilgarri dauden sistema informatikoei buruzko gorabeherak artatzeko (kontsultak, arazoak edo matxurak). Posta elektronikoan, aplikazioetan, sistemetan eta abarretan detektatzen diren gorabeherak jasotzen, tratatzen eta konpontzen ditu zerbitzu horrek.
7	Segurtasun Korporatiboko Batzordea	Administrazio Elektronikoaren eraginpean dauden erakunde eta pertsona guztien interesak segurtasunaren arloan zuzentzeko eta koordinatzeko zeregina duen kide anitzeko erakundea.
8	Konfidentzialtasuna	Ezaugarri horrek adierazten du informazioa ez dela jartzen baimenik ez duten pertsonen, erakundeen eta prozesuen eskura, ezta haiei jakinarazi ere [ENS].
9	Kontserbazioa	Segurtasun-bermea, informazioa egonkortzean eta bere bizitza-ziklo osoan denboraren ziozko narriaduratik babestean datzana.
10	Datu pertsonala	Pertsona fisiko identifikatu edo identifikagarri («interesdun») bati buruzko informazio guztia; pertsona fisiko identifikagarria da zuzenean edo zeharka, eta batez ere identifikadore baten bitartez, identifika daitekeen pertsona oro; identifikadore hori izen bat izan daiteke, identifikazio-zenbaki bat, kokapen-datuak, online identifikadore bat edo pertsona horren nortasun fisikoari, fisiologikoari, genetikoari, psikikoari, ekonomikoari, kulturalari edo sozialari buruzko elementu bat edo gehiago (DBEO).
11	Erabilgarritasuna	Entitate edo prozesu baimendunek, behar dutenean, aktiboetara irispidea dutela adierazten duen ezaugarria da [ENS].
12	DOKUSI	Eusko Jaurlaritzaren Dokumentuak Kudeatzeko Sistema Integrala (**DO**kumentu **KU**deaketa **S**istema **I**ntegrala)

#	Terminoa	Definizioa
13	ENS	Segurtasun Eskema Nazionala (311/2022 Errege Dekretua)
14	Gorabeheren kudeaketa	Zerbitzuaren ohiko funtzionamendua lehengoratzea eta ahal den neurrian erakundeak jasan dezakeen eragin txarra murriztea xede duten prozesuak, zerbitzuaren kalitatea eta eskuragarritasuna mantentzeko helburuz.
15	Arriskuen kudeaketa	Erakunde bat arriskuen aurrean gidatzeko eta kontrolatzeko jarduera koordinatuak [ENS].
16	Segurtasun-intzidentea	Ezusteko gertaera edo gertatzea nahi ez den gertaera bat da, eta ondorio txarrak izaten ditu informazio-sistemaren segurtasunean [ENS]; bereziki, transmititutako, kontserbatutako edo beste moduren batez tratatutako datu pertsonalak ustekabean edo legez kontra suntsitzea, galtzea edo aldatzea, edo datuok baimenik gabe lagatzea edo irispidean jartzea berekin ekartzen duenean [DBEO].
17	Osotasuna	Ezaugarri horrek adierazten du informazio-aktiboa ezin dela aldatu baimenik gabe [ENS].
18	Jakina	Eusko Jaurlaritzaren Korporazioaren Intraneta
19	DBEO	Datuak babesteko Erregelamendu Orokorra: EUROPAKO PARLAMENTUAREN ETA KONTSEILUAREN 2016/679 (EB) ERREGELAMENDUA, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituena eta 95/46/EB Zuzentaraua indargabetzen duena.
20	IGMEZL	Uztailaren 11ko 34/2002 Legea, Informazio Gizartearen eta Merkataritza Elektronikoaren Zerbitzuei buruzkoa. Web-orri bat duten edo eragiketak Interneten egiten dituzten enpresek eta, orokorrean, partikularrek izaten dituzten betebeharrak, erantzukizunak, arau-hausteak eta zehapenak ezartzen dira. Posta elektronikoko mezuak merkataritza-xedez bidaltzea ere beren-beregi arautzen du.
21	Segurtasun-neurriak	Informazio-sistemak izan ditzakeen arriskuetatik babesteko xedapenak, sistemaren segurtasun-helburuak ziurtatzeko hartuak. Neurriak hainbat eratakoak izan daitezke: prebentzio-, disuasio-, babes, detekzio-, erreakzio- edo berreskuratze-neurriak [ENS].

#	Terminoa	Definizioa
22	Metadatua	Dokumentu edo fitxategi jakin bati atxikitako edo lotutako datua, dokumentu edo fitxategi horri buruzko informazio gehigarria ematen duena.
23	Erabiltzailea	Zerbitzu elektronikoak ematen zeharka edo zuzenean parte hartzen duen edozein pertsona; edo zerbitzu elektroniko horiei lotutako dokumentazio edo informazioa eskura dezakeen edozein pertsona.
24	Segurtasun- eta pribatutasun-politika	Maila handiko dokumentua, erakunde batek segurtasun arloan dituen helburuak azaltzen dituena eta zuzendaritzak helburu horiek betetzeko duen konpromisoa agerrarazten duena.
25	Prozesua	Produktu edo zerbitzu bat sortzeko egiten diren jardueren multzo antolatua. Prozesuak hasiera eta amaiera jakin bat du, baliabideak erabili beharra eskatzen du, eta emaitza bat dakar beti [ENS].
26	DPBEDBLO	Abenduaren 5eko 3/2018 Lege Organikoa, Datu pertsonalak babestekoa eta eskubide digitalak bermatzekoa.
27	Arriskua	Mehatxu batek erakundearen aktibo bati edo gehiagori ekar diezaiekeen kalteen probabilitatearen zenbatespena [ENS].
28	SARgune	Eusko Jaurlaritzaren Sare Korporatiboaren zerbitzuetara sartzeko sistema. Haren helburu nagusia segurtasuna eta kalitatea hobetzea da eta, era berean, errazago egiten du zerbitzu horiek eskuratzea.
29	Informazioaren segurtasuna	Informazioa eta informazio-sistemak babestea baimendu gabeko atzipen, erabilera, dibulgazio, aldaketa edo suntsipenaren aurka.
30	Data-orduen zigilua ematea	Data-orduen zigilua metodo bat da, aurrez zegoen data-multzo bat harrezkero ez dela aldatu frogatzeko.
31	Informazio-sistema	Informazioa bildu ahal izateko, eta, orobat, biltegiratu, prozesatu edo tratatu, mantendu, erabili, partekatu, banatu, eskuragarri jarri, aurkeztu edo transmititu ahal izateko antolatutako baliabide-multzoa [ENS].
32	ISak	Informazio-sistemak
33	Euskarria	Informazioa biltegiratzeko erabilitako edozein bitarteko fisiko (papera, DVDak, disko eramangarriak eta abar).

#	Terminoa	Definizioa
34	Datu pertsonalen tratamendua	Datu pertsonalen gainean edo datu pertsonalen multzoen gainean egiten den edozein eragiketa eta eragiketa-multzo, prozedura automatizatuak erabilita zein erabili gabe: esaterako, datu-bilketa, erregistratzea, antolatzea, egituratzea, kontserbatzea, egokitzea edo aldatzea, ateratzea, kontsultatzea, erabiltzea, transmisioz lagatzea, hedatzea edo irispidean jartzeko beste edozein forma, datuak alderatzea edo interkonektatzea, mugatzea, ezabatzea edo suntsitzea [DBEO].
35	Trazabilitatea	Ezaugarri horrek adierazten du entitate baten jardunak entitate horri baino ezin zaizkiola egotzi [ENS].
36	VPN	Sare Pribatu Birtuala («*Virtual Private Network*»en ingelesezko siglak)
37	Kalteberatasuna	Aktibo baten ahulgunea, mehatxu batek aprobetxatu ahal duena [ENS].