



Eusko Jaurlaritzako Informazioaren Segurtasuna Kudeatzeko Sistema

Eusko Jaurlaritzako erabiltzaileen betebehar orokorrak

Onartua

Aprobado por

Segurtasun Batzordea

Erreferentzia

Referencia

Erabiltzaileen betebehar
orokorrak

Data

Fecha

2017-02-27

Jasotzaileak

Distribución

Langile guztiak

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

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

SEGURTASUN SAILKAPENA / CLASIFICACIÓN DE SEGURIDAD

Erabilgarritasuna Disponibilidad	ERTAINA	Osotasuna Integridad	ERTAINA	Konfidentzialtasuna Confidencialidad	TXIKIA	Benetakotasuna Autenticidad	ERTAINA	Trazabilitatea Trazabilidad	TXIKIA
-------------------------------------	---------	-------------------------	---------	---	--------	--------------------------------	---------	--------------------------------	--------

Edukia

Atala / Saila	Orrialdea
1. Sarrera	3
1.1 Dokumentuaren helburua	3
2. Ikuspegi orokorra	4
2.1 Definizioa	4
2.2 Irismena	4
2.3 Helburuak	4
2.4 Aplikazio-eremua	4
2.5 Salbuespenak	5
3. Erabiltzaileen betebeharrak orokorrak	6
3.1 Informazioaren sailkapena eta tratamendua	6
3.2 Identifikazioa eta autentifikazioa	10
3.3 Baliabideen erabilera egokia	10
3.4 Lanpostua	11
3.5 Erabiltzailearen ekipamendu informatikoa	12
3.6 Segurtasuna kanpoan	13
3.7 Sareko baliabideak	13
3.8 Posta elektronikoa	14
3.9 Internet	15
3.10 Webgune korporatiboak	16
3.11 Euskarrien kudeaketa	17
3.12 Erosketak	18
3.13 Gorabeheren kudeaketa	19
3.14 Sekretu-eginbearra	19
4. Eranskinak	20
I. Eranskina: Lotutako dokumentu eta prozedurak	20
II. Eranskina: Terminoen eta laburduren glosarioa	20

I. Sarrera

Arau hauek datu pertsonalen babesaren (DBLOGE) eta zerbitzu elektronikoen segurtasunaren (ENS eta MSPLATEA) arloetan aplikatu beharreko legezko betebeharren ondorio dira. Hala, arau hauek Eusko Jaurlaritzako arloko zuzendaritza bakoitzeko DBLO Segurtasun Dokumentuetan eta Eusko Jaurlaritzaren segurtasun arauketan (araudi hori GureSeK-ek garatu du, eta «*Informazioaren Segurtasun Politika*» dokumentuan jaso da) eta Eusko Jaurlaritzaren segurtasun Araudian (PLATEA segurtasun-eskuliburuan jaso da) biltzen dira.

1.1 Dokumentuaren helburua

Dokumentu honen helburua da **Eusko Jaurlaritzako erabiltzaileek Eusko Jaurlaritzako zerbitzu elektronikoen lotutako informazioa edo agiriak maneiatzean zaindu behar dituzten betebeharrak zehaztea.**

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

Dokumentu hau Eusko Jaurlaritzak emandako zerbitzuei buruz eta, bereziki, zerbitzu horiek bitarteko elektronikoen bidez emateari buruz dauden dokumentu guztiei edo bestelako informazio guztiei (egituratuta zein ez) aplikatu behar zaie.

2. Ikuspegi orokorra

2.1 Definizioa

“Eusko Jaurlaritzako erabiltzaileen betebeharrak” izeneko dokumentu hau zera da: Eusko Jaurlaritzak eman beharreko zerbitzuekin lotutako mota guztietako dokumentuak, datu pertsonalak edo, orokorrean, informazioa erabiltzerakoan informazioaren segurtasunaren ikuspuntutik bete beharreko gidalerroak ezartzen dituen dokumentua.

2.2 Irismena

Dokumentu honetan jasota dauden erabiltzaileen betebeharrak Euskal Autonomia Erkidegoko Administrazio Orokorreko (sailak) eta Eusko Jaurlaritzako Erakunde Autonomoetako langile guztiek bete behar dituzte administrazio elektronikoen arloan, eta Eusko Jaurlaritzako zerbitzuetako bati lotutako dokumentuak edo informazioa eskura ditzaketen kanpoko enpresa azpikontratatuak langile guztiek ere bai.

2.3 Helburuak

Eusko Jaurlaritzako erabiltzaileen betebeharrak dokumentuaren helburuak honako hauek dira:

- Eusko Jaurlaritzako zerbitzuak ematen nola edo hala parte hartzen duten pertsona guztien betebeharrak bilduma izatea.
- Eusko Jaurlaritzako zerbitzuak emateari lotutako informazioa edo dokumentazioa tratatzean jarraitu beharreko jokabide-arau orokorrak ezartzea.

2.4 Aplikazio-eremua

Erabiltzaileen betebeharrak hauek Eusko Jaurlaritzako langileek eta hark administrazio elektronikoen arloan azpikontratatuak dituen langile guztiek aplikatu beharko dituzte jarraian ageri diren egoeretan:

- Erabiltzaileen ekipamendu informatikoa erabiltzea
- Eusko Jaurlaritzak emandako bitarteko elektronikoko mugikorrek erabiltzea

- Eusko Jaurlaritzak lanbide-jarduera egiteko emandako baliabide eta zerbitzuak eskuratzea
- Eusko Jaurlaritzaren dokumentuak erabiltzea, bai formatu elektronikoan, bai inprimatuta
- Eusko Jaurlaritzak ematen dituen zerbitzuei lotutako informazioa kudeatzea

2.5 **Salbuespenak**

Hemen jasotako betebeharrak inolako salbuespenik gabe betetzekoak dira. Betebeharren bat urratuz gero, Eusko Jaurlaritzako Segurtasun Korporatiboko Batzordeak berariaz aztertuko du urraketa hori.

3. Erabiltzaileen betebeharrak 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 jokabide-arauak bete beharko dituzte.

3.1 Informazioaren sailkapena eta tratamendua

#	Informazioaren sailkapena eta tratamendua
1	Erabiltzaile guztiek lanean erabiltzen duten informazioa eta dokumentazioa (hala balitz) zein mailatan sailkatuta dagoen jakin beharko dute, eta dena delako informaziorako ezarritako gidalerroen arabera maneiatu beharko dute.
2	Informazioaren sailkapena Eusko Jaurlaritzako 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.

#	Informazioaren sailkapena eta tratamendua
4	<p>Sailkatutako informazio edo dokumentazioa maneiatzerakoan zaindu behar diren jokabide-arauak honako hauek dira:</p> <ol style="list-style-type: none"> Dokumentazioa garatzerakoan, txantilo ofizialak eta Eusko Jaurlaritzaren barruan estandarizatutako formatuak erabili beharko dira beti. Erabilitako txantilo 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. Informazioa eta dokumentazioa kudeatzeko, ezarrita dauden prozedura eta protokoloei jarraitu beharko zaie, eta une oro bermatu beharko da lotutako administrazio-prozedurak betetzen direla. 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. 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 utilitateak erabili beharko dira. 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. Informazio edo dokumentu jakin batek duen kopia kopurua ahalik eta txikiena izango da, eta kopia horiek aldi baterakoak direla kontuan hartu beharko da. Arreta berezia izan 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 Eusko Jaurlaritzaren bulegoetatik kanpo ez maneiatzeko, ez ahoz, ez formatu elektronikoko edo inprimatuaren. Kontu handiz jokatu beharko da informazio sailkatua izan ahal duen agiri inprimaturik ez galtzeko. Datu pertsonalei aplikatu beharreko gidalerroak bete beharko dira, Eusko Jaurlaritzako arloko zuzendaritza bakoitzaren DBLO segurtasun-dokumentuan ezarrita dagoenaren arabera.
5	<p>ERABILGARRITASUN ERTAIN edo HANDIarekin baloratutako informazio sailkatuta maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, honako beste neurri hauek ere bete beharko dira:</p> <ol style="list-style-type: none"> 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 aldaketak, eskuragarri dauden erabilera-estatistikak 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	<p>OSOTASUN ERTAINarekin baloratutako informazio sailkatua maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, honako beste neurri hauek ere bete beharko dira:</p> <ol style="list-style-type: none"> 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 horri buruz, aldaketen eta bertsioen aldaketak kudeatzeko ezarritako prozedurak zorrozki bete beharko dira.

#	Informazioaren sailkapena eta tratamendua
7	<p>OSOTASUN HANDIarekin baloratutako informazio sailkatua maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez eta OSOTASUN ERTAINeko informaziorako espezifikoki ezarritakoez gain, honako beste neurri hau ere bete beharko da:</p> <ol style="list-style-type: none">Eusko Jaurlaritzaren Sinadura Elektronikokoaren Politika aplikatu beharko da osotasun maila horrekin sailkatutako informazioa sinatzeko.
8	<p>KONFIDENTZIALTASUNA BALORATU GABE duen informazio guztia informazio publikotzat jo beharko da. Halako informazioa tratatzeko, atal honen 5. eta 6. puntuetan egindako oharrek bete beharko dira, hurrenez hurren erabilgarritasun eta osotasun betekizun bereziak dituen informazioari buruz. Informazio hori maneiatzeko, neurri horiez gain, honako hau bete beharko da:</p> <ol style="list-style-type: none">Informazio publiko gisa katalogatuta dagoen informazioa edo dokumentazioa soilik argitaratu ahalko da Interneten.
9	<p>KONFIDENTZIALTASUN ERTAINarekin baloratutako informazio sailkatua maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, honako beste neurri hauek ere bete beharko dira:</p> <ol style="list-style-type: none">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.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.Informazioa konfidentzialtasun maila horrekin kokatzen edo tratatzen den inguruneetara sartzeko baimenak aldizka berrikusi beharko dira, arduradunek sartzeko baimen horiek egiazta ditzaten.Ahal dela, konfidentzialtasun maila hori duen informazioa Eusko Jaurlaritzaren 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 mahaletan biltegitratuta dauden kopiei eragiten die batez ere.

#	Informazioaren sailkapena eta tratamendua
10	<p>KONFIDENTZIALTASUN HANDIarekin baloratutako informazio sailkatua maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez eta KONFIDENTZIALTASUN ERTAINeko informaziorako espezifikoki ezarritakoez gain, honako beste neurri hauek ere bete beharko dira:</p> <ol style="list-style-type: none">Konfidentzialtasun-maila hori duen informazio guztia zifratu egin beharko da, bai biltegitzean, bai transmititzean. Horretarako, Eusko Jaurlaritzak ingurune batzuetan eta besteetan horretarako ezarritako zifratze-utilitateak erabiliko dira:<ol style="list-style-type: none">Komunikazioetan VPN erabiltzeaOrdenagailu eramangarrietan diskoa zifratzeaOrdenagailu pertsonaletan, bitarteko erazgarrietan (CDak, DVDak, USB memoriak eta abar) eta zerbitzarietan fitxategiak, karpetak eta unitateak zifratzeko tresnakAplikazioek beraiek inplementatutako zifratzea, beharrezkoa badaKonfidentzialtasun-maila hori duen informazioa konpartitua bada, ez da informazio horri buruz hitz egin beharko leku publikoetan edo eremu irekietan, ezta Eusko Jaurlaritzaren bulegoetan ere. Elkarriketa horiek behar bezala itxitako gela pribatuetan egin beharko dira, hirugarrenek ezer ere entzun ez dezaten.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.Konfidentzialtasun-maila horretako informazioa duten dokumentuek behar bezala babestuta egon beharko dute. Espresuki baimenduta dauden erabiltzaileek soilik eskuratu ahalko dituzte halako dokumentuak.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 babes-neurriak jatorrizkoen berberak izango dira.
11	<p>BENETAKOTASUN ERTAIN edo HANDIA duen informazio sailkatua maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, honako beste neurri hau ere bete beharko da:</p> <ol style="list-style-type: none">Eusko Jaurlaritzaren Sinadura Elektronikoaren Politika aplikatu beharko da benetakotasun maila horrekin sailkatutako informazioa sinatzeko.
12	<p>TRAZABILITATE ERTAINarekin baloratutako informazio sailkatua maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez gain, honako beste neurri hau ere bete beharko da:</p> <ol style="list-style-type: none">Informazio hori tratatzeko, edukien kudeaketarako, dokumentuen kudeaketarako edo bertsioen kudeaketarako plataformak edo antzekoak erabili beharko dira. Horien bidez, informazioak jasaten dituen aldagetak eta ondoz ondoren dituen egoerak automatikoki erregistratu ahalko dira.

#	Informazioaren sailkapena eta tratamendua
13	<p>TRAZABILITATE HANDIarekin baloratutako informazio sailkatua maneiatzeko, informazio sailkaturako ezarritako jokabide-neurri orokorrez eta TRAZABILITATE ERTAINeko informaziorako espezifikoki ezarritakoez gain, honako beste neurri hauek ere bete beharko dira:</p> <ol style="list-style-type: none"> Informazio hori tratatzeko, edukiaren 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 motatako eskurapena 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 Identifikazioa eta autentifikazioa

#	Identifikazioa eta autentifikazioa
1	Erabiltzaileak, informazio-sistemetara sartzeko, erabiltzaile-izenaren eta pasahitzaren bidez baimendutako sarbidea izan beharko du orokorrean. Sarbide horri dagokionez, PLATEA segurtasun-eskuliburuko segurtasun-araudian aurreikusitako jarduketa-arauak bete beharko dira, bereziki M-7-2 – Sarbideen kontrola neurrian jasota daudenak.
2	Pasahitzak JAKINAN « <i>Informatika eta Telekomunikazioak</i> » atalean dagoen SARguneren Pasahitzen Politika bete beharko du.
3	Erabiltzaileak sinadura elektronikoa aurreratua edo, informazioaren ezaugarrien arabera, bere burua identifikatzeko egokia den beste baliabide bat eduki beharko du, informazioaren edo fitxategiaren arduradunak hori eskatzen badu. Horrelakorik erabiltzen duenean, aurreko zenbakian (2) ezarritako jarduketa-arauak aplikatu beharko dira, behar bezala egokituta.

3.3 Baliabideen erabilera egokia

Eusko Jaurlaritzak 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, Eusko Jaurlaritzak kontrol-sistemak 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	Informatika eta Telekomunikazioetako 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 kopiari; eta ezin dituzte inolaz ere ezabatu legez instalatu direnak.
3	Pertsonen buruzko identifikazio-datuak eta helbideak bulegotika-tresnetako (adibidez, Outlook) harremanetarako agendetan baino ez dira sartuko.

Xede hori betetzeko, honako 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 (<i>applet</i>), ActiveX kontrolak, usnariak, <i>crackinga</i> eragiteko aplikazioak edo informatika-sistemetan aldaketak edo kalteak 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 (<i>log</i>) okertzen edo faltsutzen saiatzea.

3.4 Lanpostua

Erabiltzaile guztiek euren lanpostuetan idazmahai garbiaren politika hau bete beharko dute:

#	Idazmahai garbiaren politika
1	Lanpostuek garbi egon beharko dute. Mahai gainean egongo diren dokumentu bakarrak unean uneko jarduera egiteko beharrezkoak direnak izango dira.

#	Idazmahai garbiaren politika
2	Paperezko dokumentu guztiak nahiz informazio elektronikoko euskarri guztiak, leku itxi batean gordeko dira erabiltzen ari ez direnean.

3.5 Erabiltzailearen ekipamendu informatikoa

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

#	Betebeharrak
1	Atzitzen 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 pantailak 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 eragoziko duen egoera batean utzi beharko du ekipamendu hori, adibidez, ekipamendua blokeatuz. Lanari berriz ekiteko, aurrena blokeoa desaktibatu beharko du, pasahitza sartu ondoren. 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 sailkatuak, ezta bereziki datu pertsonalak dauzkan fitxategirik.
7	Inprimagailuetako irteera-erretiluan datu babestuek dauzkan agiri inprimaturik ez egotea ziurtatu behar dute. Inprimagailuak informazioa eskuratzeko baimenik ez duten beste erabiltzaile batzuekin konpartitzen badira, ekipamendu bakoitzaren arduradunek dokumentuak jaso beharko dituzte inprimatu ahala, edo ahal izanez gero, atxikitako inprimaketa erabili (pasahitz batez babestua, ikus « <i>Funtzio anitzeko gailuak konfiguratu eta erabiltzeko jardunbide egokien gida</i> »).
8	Erabiltzailearen ekipamendu informatikoek konfigurazio finkoa izango dute beren aplikazioetan, sistema eragileetan eta abarretan. Informazioaren edo fitxategiaren arduradunak edo administratzaile baimenduek baino ezin dute aldatu konfigurazio hori.
9	Erabiltzaile guztiek euren ekipamendu informatikoetan instalatutako segurtasun-tresnak (suebakiak, antibirusak, antimalwareak, informazioa zifratzeko tresnak, VPN tresnak eta abar) behar bezala erabili beharko dituzte.

#	Betebeharrak
10	Debekatuta dago erabiltzailearen ekipamendu informatikoetan instalatutako edozein motatako tresna, programa, utilitate edo softwareak (segurtasuna xede dutenak) desgaitzea.
11	Ordenagailu eramangarrien erabiltzaileak ahal den neurrian saiatuko dira Eusko Jaurlaritzaren barneko baliabideetarako sarbide-gakorik ez jartzen ekipamendu horietan.
12	KONFIDENTZIALTASUN-maila HANDIarekin sailkatutako informazioa ordenagailu eramangarri batean aldi baterako biltegitratuta badago, zifratuta gorde beharko da, xede horrekin ekipamenduan ezarrita dauden tresnak erabiliz.

3.6 Segurtasuna kanpoan

Erabiltzaile batek, Eusko Jaurlaritzaren bulegoetatik kanpo dagoela, edozein motatako informazio sailkatua 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 ikus dezatela (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-maila ERTAIN edo HANDIarekin sailkatutako informazioarekin lan eginez gero, arreta bereziaz bete beharko dira 3.1 Informazioaren sailkapena eta tratamendua ataleko 9. eta 10. puntuetan xede horretarako ezartzen diren gidalerroak.
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 Gorabeheren kudeaketa atalean ezarrita dagoenaren arabera.

3.7 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, ISak atzitzeko aukera duten pertsonak honako segurtasun-neurri hauek bete beharko dituzte:

#	Segurtasun-neurria
1	Bidezko baimenik gabe, informatika-baliabideekin ez konektatu sare korporatiborako konexioa ahalbidetzen duen inolako komunikazio-tresnarik.
2	Informatika eta Telekomunikazioetako Zuzendaritzak, EJIek edo eskumena duen beste erakunde batek (tratamenduaren arduraduna EJI ez denean) zehaztu edo eman dituen baliabideez bestelako baliabiderik ez erabili sare korporatiboan sartzeko.
3	Ez saiatu norberaren edo beste batzuen informazio-sistemetak 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 eduki, garatu edo egikaritu beste erabiltzaile batzuen lanean eragin lezakeen programarik, ez eta baliabide informatikoetako edozein kaltetu edo eraldatu ere.

3.8 Posta elektronikoa

Posta elektronikoa erabiltzeari dagokionez, honako printzipio hauek ezartzen dira:

#	Printzipioa
1	Posta elektronikoa erabiltzailearen lan-tresnatzat joko da, zein erabileretarako sortu den eta horretarako erabili behar da.
2	Eusko Jaurlaritzaren posta elektronikoko sistema ezingo da erabili iruzurrezko mezuak, mezu lizunak, mehatxagarriak eta antzekoak bidaltzeko.
3	Erabiltzaileek ezingo dituzte publizitate-mezuak edo mezu piramidalak (erabiltzaile askori heltzen zaizkienak) sortu, bidali edo birbidali.
4	Posta elektroniko bidez informazioa trukatzeari dagokionez, jarduera hauek ez dira baimenduta egongo: <ol style="list-style-type: none"> Copyright bidez babestutako materiala igorri edo jasotzea Jabetza Intelektuala Babesteko Legea urratuz. Material pornografikoa, sexu esplizituzko mezuak edo txantxak, arrazakeriazko adierazpen baztertzailak edo iraingarri edo legez kontratatzat har daitekeen beste edozein adierazpen edo mezu igorri edo jasotzea. Baimendu gabeko hirugarrenei igortzea erakundearen materiala edo nolabait konfidentziala den materiala. Datu Pertsonalak Babesteko Legea edo Eusko Jaurlaritzaren jarraibideak urratzen dituzten fitxategiak igorri edo jasotzea. Eusko Jaurlaritzaren jarduerarekin zerikusirik ez duten mota guztietako datu eta informazioak igorri edo jasotzea.

#	Printzipioa
5	Bereziki jaramon egingo zaie informazio-bidalketaren arloan indarrean dauden legezko xedapenei, eta ahal den neurrian, posta elektronikoa erabiliko da soilik betekizun berezirik zehaztu ez bada datuen babesaren, trazabilitatearen, benetakotasunaren, konfidentziasunaren edo onarpenaren aldetik. Hala egin ezean, lehentasunez erabiliko dira Eusko Jaurlaritzak komunikazio eta jakinarazpen elektronikoak bidaltzeko ezarritako bide ofizialak.
6	Posta elektronikoa babesteko ezarritako segurtasun-utilitate guztiak erabili beharko dira: <ol style="list-style-type: none"> Kanpora bidali beharreko posta elektronikoko mezuetan sinadura elektronikoa erabiltzea, mezu horien benetakotasuna eta osotasuna bermatu nahi badira. Posta elektronikoko mezu baten konfidentziasuna bermatu nahi bada, zifratzea erabiltzea. Antivirusaren utilitateak erabiltzea posta elektronikoko mezuek birusik ez daukatela egiaztatzeko.
7	Ez da onartuko KONFIDENTZIALTASUN HANDIarekin sailkatuta dagoen informazioa edo datu pertsonalak dituen informazioa posta elektronikoz bidaltzea, salbu eta komunikazio elektronikoa zifratuta badago eta bidalketa berariaz onartu bada.
8	Beren-beregi egiaztatuko dira hartzaile diren posta elektronikoko helbideak, behar ez diren helbidetara edo helbide okerretara posta elektronikoko mezuek bidaltzea ahal den neurrian eragozteko.
9	Arreta berezia jarriko da CCO (kopia ezkutua) eremuak erabiltzen direnean honako hauei zuzendutako mezuen hartzaile diren pertsona edo erakundeak definitzeko: Eusko Jaurlaritzatik kanpoko erabiltzaile edo erakundeei eta banaketa-zerrenda edo hartzaileen kopuru handiei.
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.

3.9 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 Eusko Jaurlaritzaren eginbeharrei laguntzeko balio ez duten 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 Eusko Jaurlaritzaren izena, sinboloa, logotipoa edo horien antzekoak Interneteko ezein elementutan (posta elektronikoa, web-orriak eta abar), ez bada laneko jardueri lotutako arrazoiengatik.

#	Gidalerroa
4	Internetera edo Internetetik datu-transferentziak egitea onartuko da, soilik, Eusko Jaurlaritzaren jarduerekin lotura badute. Debeztatuta 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 dira baimenduta egongo: <ul style="list-style-type: none"> a. Copyright bidez babestutako materiala igorri edo jasotzea Jabetza Intelektuala Babesteko Legea urratuz. b. Material pornografikoa, sexu esplizituzko mezuak edo txantxak, arrazakeriazko adierazpen baztertzailak 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 Eusko Jaurlaritzaren jarraibideak urratzen dituzten fitxategiak igorri edo jasotzea. e. Eusko Jaurlaritzaren jarduerarekin zerikusirik ez duten mota guztietako datu eta informazioak igorri edo jasotzea. f. Interneteko zenbait jardueratan parte hartzea, hala nola berri-taldeetan, jolasetan edo Eusko Jaurlaritzaren jarduerarekin lotura zuzenik ez duten beste batzuetan. g. Eusko Jaurlaritzaren izen ona kalte dezaketen jarduerak egitea. Halakotzat jotzen dira Eusko Jaurlaritzako langileek euren onura ekonomikorako edo hirugarrenen onura ekonomikorako egindako jarduerak, jarduera politikoak edo antzeko beste batzuk.
7	Eusko Jaurlaritzako langileek gizarte-sareetan parte hartzen badute, Lehendakaritza Sailak argitaratutako «Eusko Jaurlaritzaren gizarte-sareetako erabileren eta estiloaren gida» izenburuko dokumentuan ezarritakoa bete beharko dute.

3.10 Webgune korporatiboak

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

#	Gidalerroa
1	Webgunean argitaratutako informazioaren osotasuna babesteko neurriak hartuko dira, Eusko Jaurlaritzaren izen ona kalte dezaketen baimenik gabeko aldaketak prebenitzeko.
2	Informazioa publiko objektiboaren esku jarri aurretik baimen formala emateko prozedura bat inplementatuko da.

#	Gidalerroa
3	<p>Sarbide publikoko sistema guztietan hau hartu beharko da kontuan:</p> <ol style="list-style-type: none"> Informazioa lortu, prozesatu eta emateko indarreko legeria bete behar da, bereziki DBLO eta IGMEZL. Argitaratzen edo prozesatzen den informazioak zuzena izan behar du. Informazio konfidentziala argitaratu aurreko urratsean babestu behar da. Argitalpen-sistemak ez du aukerarik eman behar ezbeharrez beste ingurune batzuetara sartzeko. Informazioa webgune publikoan argitaratzeko ardura duen pertsona identifikatu behar da. Argitaratutako informazioa baliozkoa dela eta indarrean dagoena bermatu behar da.
4	<p>Interneten informazio publikoa soilik argitaratu ahalko da, informazio horren KONFIDENTZIALTASUNA BALORATU GABE gisa sailkatu bada. Kasu horretan, Eusko Jaurlaritzako langileek informazio hori jendaurrean jartzeko betebeharra izango dute.</p>
5	<p>Estraneteko ingurunean KONFIDENTZIALTASUN-maila TXIKI edo ERTAINarekin sailkatutako informazioa soilik argitaratu ahalko da, eta bigarren kasu horretan, baldin eta informazio eta dokumentazio hori atzitzeko baimena duten kanpoko pertsonak informazio eta dokumentazio hori eskuratu behar badute.</p>
6	<p>Intranet orokorreko ingurunean (<i>Jakina</i>) KONFIDENTZIALTASUN-maila TXIKIarekin sailkatutako informazioa soilik argitaratu ahalko da. KONFIDENTZIALTASUN-maila ERTAINarekin sailkatutako informazio eta dokumentazioa atzitzeko kontrola duten <i>Jakina</i> inguruneetan ere argitaratu ahalko da; sarbidea, betiere, informazio eta dokumentazio hori eskuratu behar duten pertsona-taldeen soilik izango dute.</p>
7	<p>KONFIDENTZIALTASUN-maila HANDIarekin sailkatutako informazioa inola ere ez da argitaratuko ingurune ireki batean.</p>

3.11 Euskarrien kudeaketa

Erabiltzaileek honako segurtasun-neurri hauek bete behar dituzte informazioaren kanpoko euskarrien kudeaketari dagokionez:

#	Segurtasun-neurria
1	<p>Datu pertsonalak aldi batean erabili beharra eragiten duten zereginak amaitu ondoren, berehala itzultzea informazioa –eta, bereziki datu pertsonalak– dauzkaten euskarriak.</p>
2	<p>Informazioa daukaten euskarriak, erabili behar ez direnean, leku seguruan eta giltzapean gorde beharko dituzte, lanaldia amaitutakoan batez ere. Nolanahi ere, euskarri horiek toki seguruetan gorde behar dira, datu horiek erabiltzeko baimenik ez duten pertsonak leku horietan ez sartzeko.</p>
3	<p>Euskarriak erabiltzen eta biltegitratzen 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.</p>

#	Segurtasun-neurria
4	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. Gainera, datu pertsonalak barnean badituzte, etiketak adierazi beharko du zein fitxategi den, zein motatako datuak dituen, datu horiek zein prozesuk sortu dituen eta zein datatan sortu den.
5	KONFIDENTZIALTASUN-maila ERTAIN edo HANDIko informazioa duten euskarriek zifratuta egon beharko dute. Horretarako, xede horrekin ezarrita dauden tresnak erabiliko dira.
6	Berrerabil daitezkeen euskarrietan bildutako informazio guztia ezabatu beharko da euskarria berriz erabili baino lehen.
7	Berrerabil daitezkeen informazio-euskarriak, eta bereziki datu pertsonalen kopiak barnean izan dituztenak, guztiz formateatu beharko dira (ezin da formatu azkarra erabili) aurreko erabiltzailea ez den beste pertsona batek erabili baino lehen. Hala, bilduta zeuden datuak ezingo dira berriz ere berreskuratu. Kasu horietan, komenigarria litzateke alderdi fisikoan ezabatze segurua (modu arruntan "wipe egitea" deritzona) egiteko utilitatereen bat erabiltzea.
8	Informazioa barnean duten euskarrien sarrera guztiak erregistratu beharko dira, eta entrega egin behar duen garraiolaria identifikatu beharko da.
9	Informazioa barnean duten euskarrien irteera guztiak erregistratu beharko dira, eta lekualdaketa egin behar duen garraiolaria identifikatu beharko da.
10	Maila HANDIarekin sailkatutako informazioa kanporatu behar denean, datu pertsonalak nahiz sailkapen hori duen bestelako informazioak direla ere, informazio hori zifratu egin behar da, edo datuak garraiatu bitartean ez jakinaraztea eta ez manipulaztea bermatzeko beste mekanismo bat erabili.
11	Datu pertsonalak posta elektronikoz kanporatzen direnean, helbide elektronikoko horretako direktorioaren historian edo irteerak erregistratzeko beste sistema batean jaso behar da bidalketa egin dela.
12	Langile baimenduek baino ezin dute datu pertsonalak dituen informazioa kanporatu.
13	Datu pertsonalak posta elektronikoaren bidez edo sareko transferentzien bitartez bidaltzen badira, bidalketak erregistratu behar dira: nondik bidali diren, zer datu mota den, euskarria, bidalketaren eguna eta ordua eta hartzaile den pertsona edo erakundea ezagutu ahal izateko.

3.12 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 eskuratzean, Erosketen Segurtasun Gida aplikatu beharko da.
2	Segurtasun-zerbitzuak edo segurtasunak zeregin garrantzitsua duen zerbitzuak kontratatzean, Erosketen Segurtasun Gida aplikatu beharko da

3.13 **Gorabeheren kudeaketa**

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

#	Segurtasun-neurria
1	Erabiltzailearen Laguntza Zentroari (ELZ) 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).
1	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.

3.14 **Sekretu-eginbearra**

Maneiatzen den informazioaren konfidentziasuna mantendu behar da; horretarako, erabiltzaileek honako segurtasun-neurri hauek bete behar dituzte:

#	Segurtasun-neurria
1	Langile guztiek zuhurtzia handienaz jokatu 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 apirilaren 12ko 7/2007 Legearen VI. kapituluaren (Enplegatu publikoen eginbearrak. Jokabide-kodea) ezarrita dagoenez.
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

I. Eranskina: Lotutako dokumentu eta prozedurak

#	Dokumentua / Prozedura
1	Aldaketak edo bertsioak kudeatzeko prozedurak
2	DBLO Segurtasun Dokumentua (Arloko Zuzendaritza bakoitzarena)
3	Dokumentuak garbitzeko utilitateak
4	Erosketen segurtasun-gida
5	Eusko Jaurlaritzak ezarritako zifratze-utilitateak
6	Eusko Jaurlaritzaren gizarte-sareetako erabileren eta estiloaren gida
7	Eusko Jaurlaritzaren sinadura elektronikoaren politika
8	Funtzio anitzeko gailuak konfiguratu eta erabiltzeko jardunbide egokien gida.
9	Informazioa eta dokumentazioa kudeatzeko prozedurak
10	Informazioa Sailkatzeko Politika
11	Informazioaren Segurtasun Politika

II. Eranskina: Terminoen eta laburduren glosarioa

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

#	Termino	Definizioa
1	Aktiboa	Erakundearentzat balioa duen osagaia, funtzioa edo baliabidea —informazioa, datuak, zerbitzuak, aplikazioak, ekipamenduak, komunikazioak, administrazio-baliabideak, baliabide fisikoak eta giza-baliabideak...—
2	Arriskua	Mehatxu batek erakundearen aktibo bati edo gehiagori ekar diezaikeen kalteen probabilitatearen zenbatespena [ENS].

#	Terminoa	Definizioa
3	Arriskuen azterketa	Informazio-sistema batek jasan ditzakeen mehatxuak, kalteberatasunak, arriskuak eta eraginak aztertzeko prozesua, kontuan hartuta jada dauden segurtasun-neurriak. Segurtasun-neurrien hobekuntzak eraginkortasunari eta kostuei dagokienez identifikatzeko abiapuntu gisa erabiltzen da.
4	Arriskuen kudeaketa	Erakunde bat arriskuen aurrean gidatzeko eta kontrolatzeko jarduera koordinatuak [ENS].
5	Benetakotasuna	Entitate batek adierazitako identitatea egiazkoa dela edo datuen iturria bermatzen duela adierazten duen ezaugarria [ENS].
6	Data-orduen zigilua ematea	Data-multzo bat une jakin baten aurretik existitu zela eta orduz geroztik datu horietako bat ere aldatu ez dela frogatzeko metodoa da data-orduen zigilua.
7	Datu pertsonalak	Identifikaturiko edo identifika daitezkeen pertsona fisikoen gaineko edozein informazio [DBLO].
8	DBLO	Datu Pertsonalak Babesteko Lege Organikoa (15/1999 LO).
9	DBLOGE	DBLO garatzen duen Erregelamendua (1720/2007 Errege Dekretua)
10	DOKUSI	Eusko Jaurlaritzako Dokumentu Kudeaketa Sistema Integrala (DO kumentu KU deaketa S istema I ntegrala).
11	ELZ	Erabiltzaileei arreta emateko zerbitzua, Eusko Jaurlaritzan erabilgarri dauden sistema informatikoei buruzko gorabeherak artatzeko (kontsultak, arazoak edo matxurak). Zerbitzu horrek, detektatzen diren gorabeherak jasotzen, tratatzen eta konpontzen ditu (posta elektronikoa, aplikazioak, sistemak...)
12	ENS	Segurtasun Eskema Nazionala (3/2010 Errege Dekretua)
13	Erabilgarritasuna	Entitate edo prozesu baimendunek behar dutenean aktiboetara irispidea dutela adierazten duen ezaugarria [ENS].
14	Erabiltzailea	Zerbitzu elektronikoak ematen zeharka edo zuzenean parte hartzen duen pertsona, edo zerbitzu elektroniko horiei lotutako dokumentazio edo informazioa eskura dezakeena.
15	Euskarria	Informazioa biltegitartzeko erabilitako edozein motatako bitarteko fisikoa (papera, DVDak, disko eramangarriak eta abar).
16	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.
17	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 dituzten betebeharrak, erantzukizunak, arau-hausteak eta zehapenak ezartzen dira. Posta elektronikoko mezuak merkataritza-xedeekin bidaltzea ere berenberegiri arautzen du.

#	Terminoa	Definizioa
18	Informazioaren segurtasuna	Informazioa eta informazio-sistemak babestea baimendu gabeko atzipen, erabilera, dibulgazio, aldaketa edo suntsipenaren aurka.
19	Informazio-sistema	Informazioa bildu ahal izateko, eta, orobat, biltegitatu, prozesatu edo tratatu, mantendu, erabili, partekatu, banatu, eskuragarri jarri, aurkeztu edo transmititu ahal izateko antolatutako baliabide-multzoa [ENS].
20	ISak	Informazio Sistemak
21	Jakina	Eusko Jaurlaritzaren Intranet Korporatiboaren izena.
22	Kalteberatasuna	Aktibo baten ahulgunea, mehatxu batek aprobetxatu ahal duena [ENS].
23	Konfidentzialtasuna	Informazioa baimenik ez duten pertsonen, erakundeen eta prozesuen eskura ez dela jartzen, ez jakinarazten, adierazten duen ezaugarria [ENS].
24	Kontserbazioa	Segurtasun-bermea, informazioa egonkortzean eta bere bizitza-ziklo osoan denboraren ziozko narriaduratik babestean datzana.
25	Mehatxua	Informazio-sistema bat edo erakunde bat kaltetu ahal duen gorabehera baten kausa [UNE 71504:2008] Mehatxuen presentzia beti gogoan izatekoa da, baina mehatxuak agertzearen ondorioak saihesten edo arintzen saiatzea dago.
26	Metadatu	Dokumentu edo fitxategi jakin bati atxikitako edo lotutako datua, dokumentu edo fitxategi horri buruzko informazio gehigarria ematen duena.
27	MSPLATEA	PLATEA Segurtasun Eskuliburua
28	Osotasuna	Informazioaren aktiboa baimenik gabe ez dela aldatu adierazten duen ezaugarria [ENS].
29	PLATEA	Eusko Jaurlaritzaren Administrazio Elektronikorako plataforma.
30	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].
31	SARgune	Eusko Jaurlaritzaren Sare Korporatiboaren zerbitzuetara sartzeko sistema. Duen helburu nagusia segurtasuna eta kalitatea hobetzea da eta, era berean, errazago egiten du zerbitzu horiek eskuratzea.
32	Segurtasun Korporatiboko Batzordea	Administrazio Elektronikoaren eraginpean dauden erakunde eta pertsona guztien interesak segurtasunaren arloan zuzentzeko eta koordinatzeko zeregina duen kide anitzeko erakundea.
33	Segurtasun-gertakaria	Ezusteko edo nahi gabeko gertakaria, informazio-sistemaren segurtasunari kalte egiten diona [ENS].
34	Segurtasun-neurriak	Informazio-sistemak izan ditzakeen arriskuetatik babesteko xedapenak, sistemaren segurtasun-helburuak ziurtatzeko hartuak. Neurriak hainbat eratakoak izan daitezke: prebentziozkoak, disuasiozkoak, babesgarriak, detekziozkoak eta erreakziozkoak edo berreskuratzezkoak [ENS].

#	Terminoa	Definizioa
35	Segurtasun-politika	Maila handiko dokumentua, erakunde batek segurtasun arloan dituen helburuak azaltzen dituena eta zuzendaritzak helburu horiek betetzeko duen konpromisoa agerrarazten duena.
36	Trazabilitatea	Entitate baten jardunak entitate horri baino ez dakizkiokeela egotzi adierazten duen ezaugarria [ENS].
37	VPN	Sare Pribatu Birtuala (« <i>Virtual Private Network</i> »en ingelesezko siglak)