Eusko Jaurlaritzaren
Informatika Elkartea

Sociedad Informática
del Gobierno Vasco

Enpresa hornitzaileetako langileentzako segurtasun-politikak

Eguna: 2018/11/26

Erreferentzia: **PSP v4.0**

Mediterraneoaren hiribidea 14 • 01010 •Vitoria-Gasteiz Posta-kutxa: 809• 01080 Vitoria-Gasteiz Tel.: 945 01 73 00* • Faxa:• 945 01 73 01 • www.ejie.eus

Bertsioa	Data	Aldaketen laburpena	Egilea:	Nork onartua:
1.0	2000/12/1	Lehenengo bertsioa	Segurtasun-arduraduna	Zuzendari nagusia
2.0	2008/5/5	ISO/IEC 27001:2005 eredura egokitzea	Segurtasun-arduraduna	Zuzendari nagusia
2.1	2008/7/31	Negozioaren Jarraipenerako Planari lotutako kontrol-klausulak sartzea	Segurtasun-arduraduna	Zuzendari nagusia
2.2	2010/10/8	Berrikuspen orokorra	Segurtasun-arduraduna	Zuzendari nagusia
3.0	2012/3/14	Hainbat zerbitzu motatara egokitzea agiria	Segurtasun-arduraduna	Zuzendari nagusia
3.1	2013/9/6	Agustín Elizegiren Onarpena	Segurtasun-arduraduna	Zuzendari nagusia
3.2	2014/5/22	Alex Etxeberriaren Onarpena	Segurtasun-arduraduna	Zuzendari nagusia
3.3	2016/1/8	3.7, 3.8, 3.11 eta 3.14 atalak egokitzea EJIEren segurtasun-politiken 3.0 bertsioak sartutako aldaketara	Segurtasun-arduraduna	Zuzendari nagusia
4.0	2018/11/26	Gaurkotze orokorra, Datuak Babesteko Erregelamendu Orokorrarekiko lerrokatzea eta betekizun bereziak (“politika bereziak” apartatua)	Segurtasun-arduraduna	Zuzendari nagusia

Aurkibidea

1 Sarrera 4
1.1 Xedea 4
1.2 Aplikazio-eremua 4
2 Hornitzaileentzako Segurtasun-politika Orokorrak 5
2.1 EJIEren Segurtasun Politika Orokorra betetzea EJIErentzat lan egiten duten kanpoko langile guztiek EJIEren Segurtasun-politika Orokorra bete beharko dute. 5
2.2 EJIEri zerbitzuak eskaintzea 5
2.3 Informazioaren konfidentzialtasuna 5
2.4 Jabetza intelektuala 7
2.5 Informazio-trukea 7
2.6 Baliabideen erabilera egokia 8
2.7 Erabiltzailearen erantzukizunak 9
2.8 Erabiltzailearen ekipamenduak 10
2.9 "Hardware" ekipamenduaren kudeaketa. 11
3 Hornitzaileentzako Segurtasun-politika Espezifikoak 12
3.1 Hornitzaileentzako segurtasun-politika espezifikoen aplikagarritasuna 12
3.2 Langileak hautatzea 14
3.3 Segurtasunari buruzko auditoria (2009). 14
3.4 Gorabeheren berri ematea 14
3.5 Segurtasun fisikoa 15
3.6 Aktiboen kudeaketa 15
3.7 Segurtasun-arkitektura 16
3.8 Sistemen segurtasuna 16
3.9 Sare-segurtasuna 17
3.10 Sistemen erabileraren trazabilitatea 18
3.11 Identitateen eta sarbideen kontrola nahiz kudeaketa 19
3.12 Aldaketen kudeaketa 20
3.13 Aldaketen kudeaketa teknikoa 20
3.14 Garapen-segurtasuna 20
3.15 Kontingentzien kudeaketa 21
4 Zerbitzuak kanpora ateratzean bete beharreko segurtasun-baldintzak 22
5 Jarraipena eta kontrola 23
6 Segurtasun-politikak eguneratzea 24

1 Sarrera

1.1 Xedea

Erakunde orok du galdu edo oker erabiliz gero haren izen ona kaltetu dezakeen informazioa. Era berean, informazio-sistemak hondatzen badira edo erabilgarri ez badaude, enpresaren ohiko martxa oztopatu egiten da, eta horrek eragin negatiboa du zerbitzuaren kalitatean eta enpresaren irabazietan.

Dokumentu honen helburu nagusia da EUSKO JAURLARITZAREN INFORMATIKA ELKARTEAren (hemendik aurrera EJIE) hornitzaileentzat informazioaren segurtasunari buruzko arau–esparrua ezartzea. Horretarako, EJIErentzat lan egiten duten —baina beste enpresa hornitzaile batzuetakoak diren, eta, beraz, EJIEren informazio, informazio-sistema edo, oro har, baliabideetara sarbidea izan dezaketen— langileengandik zer espero dugun deskribatzen dugu, EJIEk erabiltzen dituen informazio eta sistemen konfidentzialtasuna, segurtasuna eta erabilgarritasuna babestu ahal izateko.

Alde horretatik, segurtasun-politika horiek bete behar dituzten enpresa hornitzaileek beren gain hartzen dute erantzukizuna, batetik, EJIEra bidaltzen dituzten langileei politika horien berri emateko, eta, bestetik, langileek politika horiek errespetatzeko hartzen duten konpromisoa idatziz jasotzeko.

Aipatutako segurtasun-politikak legezko betekizunak eta betekizun etikoak ezartzen ditu EJIErentzat lan egiten duten —eta enpresa hornitzaileetakoak diren— langileen jarduera informaletarako, baita enpresaren jarduerarako ere.

Helburu horretarako, politika horrek EJIEko Segurtasu-politiketan jasotakoa hartzen du kontuan, eta indarreko legeriak eta bereziki 2016/679 (EB) Erregelamenduak (Europako Parlamentuaren eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituena) EJIErentzat ezarritako betebeharrak islatzen ditu.

1.2 Aplikazio-eremua

EJIEri zerbitzuak ematen dizkioten baina beste zerbitzu-enpresa hornitzaile batzuetakoak diren langileek egindako jarduerak; enpresa horiek dagokien zerbitzu-horniketarako kontratuaren bidez lotzen dira EJIEra.

Zerbitzu bat ala beste eskaini, hornitzaile guztiei aplikatuko zaie politika honetako 2. atala (Hornitzaileentzako Segurtasun-politika Orokorrak). (

Politika honetan, bestetik, bada hainbat azpiataletan banaturik dagoen Hornitzaileentzako Segurtasun-politika espezifikoak izeneko atala (3.a). Azpiatal horietako bakoitza zerbitzu mota zehatz bati dagokionez, zerbitzu hori eskaini duten hornitzaileei baino ez zaie aplikatuko hirugarren atalean xedatutakoa. Halaxe adierazi da, bederen, aipatu hirugarren atal horren hasieran. “Hornitzaileentzako Segurtasun-politika Espezifikoak”

2 Hornitzaileentzako Segurtasun-politika Orokorrak

2.1 EJIEren Segurtasun Politika Orokorra betetzea EJIErentzat lan egiten duten kanpoko langile guztiek EJIEren Segurtasun-politika Orokorra bete beharko dute.

Hau da, Segurtasun-politika orokorreko zuzentarauak bete behar dituzte eta horiek aplikatzen lagundu behar du nork bere jarduera-esparruan. Hizpide dugun segurtasun-politika orokorra, bidenabar, web-orrian da eskuragarri.

2.2 EJIEri zerbitzuak eskaintzea

a) Zerbitzuak eskaintzeari buruzko kontratuan jasotako jarduerak besterik ezin izango dituzte gauzatu hornitzaileek EJIErentzat. Hortaz, enpresa hornitzaileetako langileek EJIErentzat gauzatutako jarduera guztiak EJIEk hornitzaileekin sinatutako zerbitzu-kontratuen barruan izango direla joko da.

b) Zerbitzuak eskaintzeko kontratuan, eta EJIEren nahiz dagokion hornitzailearen artean zerbitzuak eskaintzeari buruz ezarritako arauetan nahiz prozeduretan ezarritakoarekin bat jardungo dira enpresa hornitzaileetako langileak. Kontratatutako zerbitzua eskaintzen duten pertsonen, haien profilen, eginkizunen eta zerbitzuan duten ardurei buruzko informazioa emango dio aldian aldian enpresa hornitzaileak EJIEri.

c) Horrez gain, alderdi horietakoren batean aldaketaren bat izanez gero, jakinaren gainean jarriko du enpresa hornitzaileak EJIE (eginkizun edo erantzukizun berriak jartzea, kentzea, ordezkatzea edo horiek aldatzea).

d) Zerbitzuak eskaintzeko kontratuko klausuletan ezarritakoaren arabera, agiri honetako segurtasun-politikak bete beharko dituzte EJIErentzat lan egiten duten kanpo-langile guztiek. Obligazio horietakoren bat bete ezean, EJIEk araua hautsi duten langileak betatzeko eskubidea du. Horrez gain, kasu bakoitzean egoki iritzitako zigor-neurriak hartu ahal izango ditu kontratatutako enpresaren aurka, enpresa horrekin dituen kontratuak suntsitzeraino. Langileek zerbitzua eskaintzeko beharrezkoa den prestakuntza eta gaikuntza dutela bermatu beharko du enpresa hornitzaileak.

e) Langileek prestakuntza espezifikoa izango dute, gauzatuko duten jarduerari buruzko gaietan eta, zeharka, informazioaren segurtasunari buruz. Horretarako, zerbitzua eskainiko duten langileek segurtasun-politika hauek ezagutzen eta beteko dituztela bermatu beharko du gutxienez enpresa hornitzaileak.

f) EJIEk eta enpresa hornitzaileak elkarri emandako edozein informazio zerbitzuak eskaintzeko kontratuaren esparruaren barruan trukatu dela joko da. Aipatu informazio hori, beraz, ezin izango da erabili, inola ere, esparru horretatik kanpo, ezta kontratukoez bestelako xedeetarako ere.

g) Segurtasun informatikoaren sailak EJIEren aktiboak babesteko ahalegin guztiak zentralizatzen ditu, erakundearen barneko prozesuen oinarrian dauden informazio-teknologiek behar bezala funtzionatzen dutela ziurtatzeko.

h) Oro har, aktibotzat jotzen da informazio guztia, informazio-prozesuen oinarrian dauden pertsonez eta teknologiaz gain.

2.3 Informazioaren konfidentzialtasuna

a) EJIEren informaziora sarbidea duten kanpoko langileek kontuan hartu beharko dute, besterik esan ezean, informazio hori konfidentziala dela. Informazio ez-konfidentzialtzat hartu ahal izango da,

soilik, informazioari zabalkunde publikoa emateko EJIEk berariaz jarritako bitartekoen bidez jasotako hura.

b) Informazioa ezagutzera ematea, aldatzea, suntsitzea edo desegoki erabiltzea saihestuko da, informazio horren euskarria edozein delarik ere.

c) Informazio konfidentziala mugagabeko denboraz eta zuhurtzia handienaz gordeko da eta ez da kanpora aterako, hori egiteko behar den baimenik izan ezean.

d) Informazio konfidentziala duten txostenen ahalik eta kopuru txikiena erabiliko da paperezko formatuan, eta leku seguruan edukiko dira, hirugarrenek ez eskuratzeko moduan.

e) Harremanen agenda eta EJIEk ezarritako bulegotika-tresnak erabiltzean, langileek datu pertsonal hauek bakarrik erabiliko dituzte: izen-deiturak, norberaren eginkizunak edo postua, eta posta-helbidea edo helbide elektronikoa eta telefonoa.

f) Proiektuetan, lan jakinetan eta abarretan kolaboratzaile gisa aritutako inork ezingo du eduki, bere ardurari dagozkion erabileretarako ez bada, EJIEren edo EJIEri emandako material edo informaziorik.

g) Duen lanpostuagatik, enpresa hornitzaileko langileak edozein euskarritan jasotako informazio konfidentziala eskura badu, ulertuko da informazio hori aldi baterako duela, eta langile horrek informazioa sekretupean edukitzeko obligazioa izango du; horrek ez dio ematen informazioaren edukitzaren, titulartasunaren edo kopiaren gaineko inolako eskubiderik. Gainera, langileak aipatutako euskarria edo euskarriak itzuli beharko ditu, horien aldi baterako erabilera eragin duten lanak amaitu eta berehala edo, beti ere, EJIEk langilearen enpresarekin duen harremana bukatzean. Edozein formatu edo euskarritako informazioa hitzartutakoaz bestelako modu batera eta EJIE jakinaren gainean egon gabe modu jarraituan erabiliko balitz ere, horrek inola ere ez luke puntu honetan ezarritakoa aldatuko. Baldin eta behin eta berriz erabiltzen bada edozein formatutan edo euskarritan itundutakoa ez den informazioa edo EJIEk jakin barik, puntu hau ez da aldatzen inola ere.

h) Obligazio horiek guztiek indarrean jarraituko dute kanpoko langileek EJIErentzako egindako lanak amaitzean ere.

i) Zigor Kodeko 197. artikuluan ezarritakoaren arabera, obligazio horiek ez betetzea delitua izan daiteke sekretuak agerraraztegatik, eta ordainak eskatzeko eskubidea sor dezake.

Datu pertsonalak tratatzeari dagokionez, honako jarduketa-arauak behar behar dira, lehen aipatutakoez gain:

j) Langileek datu pertsonalen aldi baterako fitxategiak sortu ahal izango dituzte soilik lan egiteko beharrezkoa denean. Aldi baterako fitxategi horiek inoiz ere ez dira jarriko lanpostuetako disko gogor lokaletan, eta sortu ziren helbururako erabilgarriak izateari uzten diotenean, suntsitu egin beharko dira.

k) Lanpostuetako disko gogor lokaletan ez da datu pertsonalik gordeko. Lanpostuetako disko gogor lokaletan ez da datu pertsonalik gordeko.

l) Trataeraren arduradunak soilik baimendu ahal izango du datu pertsonalak dituzten euskarri informatikoak informazioa dagoen lekutik ateratzea. Hori egiteko, gainera, aurrez zehaztutako prozedura bete beharko da.

m) Datu pertsonalak dituzten euskarri informatikoek aukera eman beharko dute jasotzen duten informazio-mota identifikatzeko, inbentariatuak izateko eta baimena duten langileek soilik eskura dezaketen sarbide batean gordetzeko.

2.4 Jabetza intelektuala

a) Jabetza intelektualeko arauez babestutako materialaren erabilerari ezarritako legezko murrizketak betetzen direla bermatuko da.

b) Beren eginkizunak betetzeko baino ezin izango dute EJIEk baimendutako materiala erabili langileek.

c) Erabat debekatuta dago EJIEko informazio-sistemetan lizentziarik gabeko programa informatikoak erabiltzea.

d) Era berean, debekatuta dago jabetza intelektualaz babestutako edozein obra edo asmakizun erabili, erreproduzitu, laga, aldatu edo publikoki jakinaraztea, horretarako baimenik izan gabe.

e) EJIEk soilik baimenduko du erakundeak berak ekoitzitako materiala —edo materialaren titularrak EJIEri emandako edo baimendutakoa— erabiltzea, hitzartutako moduan eta baldintzekin, eta indarrean dagoen araudiaren arabera.

2.5 Informazio-trukea

a) Inork ere ezin izango du, inola ere, bere nortasuna isildu edo manipulatu.

b) Zerbitzuak eskaintzeko kontratuan zehaztutako baliabideen bitartez banatuko da informazioa, dela euskarri digitalean, dela paperezko euskarrian. Aipatu informazioa, bidenabar, zerbitzua eskaintzeko eta kontratuarekin lotura duten funtzioak gauzatzeko baino ez da erabiliko. EJIEk beretzat gordetzen du, identifikatutako arriskuaren arabera, hedapenerako baliabideak kontrolatu, erregistratu edo ikuskatzeko neurriak ezartzeko eskubidea.

c) Zerbitzuak eskaintzeko kontratuaren esparruan informazioa trukatzeari dagokionez, ondoko jarduera hauek ez dira baimenduta egongo:

1. Copyright bidez babestutako materiala igorri edo jasotzea Jabetza Intelektuala Babesteko Legea urratuz.
2. Material pornografikoa, sexu esplizituzko mezuak, arrazakeriazko adierazpen baztertzaileak edo iraingarri edo legez kontrakotzat har daitekeen beste edozein adierazpen edo mezu igorri edo jasotzea.
3. Baimendu gabeko hirugarrenei igortzea erakundearen materiala edo nolabait konfidentziala den materiala barne hartzen duen informazioa.
4. Datu pertsonalak babesteari buruzko indarreko araudia edo EJIEren jarraibideak urratzen dituen informazioa igorri edo jasotzea.
5. Negozioarekin loturarik ez duten jolasak edota aplikazioak igorri edo jasotzea.
6. Interneteko zenbait jardueratan parte hartzea, hala nola berri-taldeetan, jolasetan edo zerbitzuarekin lotura zuzenik ez duten beste batzuetan.
7. Debekatuta dago, Interneten edo beste edozein lekutan, EJIEren izen ona kaltetu lezakeen jarduera oro.

d) Baimendutako langileek bakarrik, ez beste inork, atera ahal izango dute datu pertsonalak dituen informazioa (euskarri informatikoetan nahiz paperean zein posta elektronikoz), horretarako behar den baimena eskuratu eta zehaztutako prozedura bete beharko dute.

e) Datu pertsonalak datuak dauden lokaletatik kanpo tratatu behar badira, trataeraren arduradunak horretarako berariazko baimena eman beharko du, eta, kasu guztietan, beharrezko segurtasun-maila bermatu beharko da.

f) Goi-mailako datu pertsonalak telekomunikazio-sareen bidez igorri behar badira, datu horiek zifratu beharko dira edo bestelako mekanismoak erabili, hain zuzen ere hirugarrenek informazio hori ez dutela ulertu edo manipulatuko bermatuko duten mekanismoak.

2.6 Baliabideen erabilera egokia

a) Hornitzaileak konpromisoa hartzen du aldizka EJIEri zerbitzua eskaintzeko baliatzen dituen aktiboen berri emateko.

b) Zerbitzua eskaintzeko baliabideak horiek diseinatzeko eta ezartzeko baldintzen arabera erabiliko dituela hitz ematen du hornitzaileak.

c) EJIEk kanpoko langileen esku jartzen dituen baliabide guztiak (informatikoak, datuak, softwarea, sareak, komunikazio-sistemak eta abar) erabili ahal izango dira, soilik, baliabide horiek ematean zehaztutako obligazioak eta helburuak betetzeko. EJIEk eskubidea du kontrol- eta ikuskapen-mekanismoak ezartzeko, baliabide horiek behar bezala erabiltzen direla egiaztatze aldera.

d) Euskarri automatizatuen, Interneten edo posta elektronikoaren bidez edo beste edozein modutara EJIEren sarean edo sare horretara konektatutako edozein ordenagailutan sartutako edozein fitxategik arau hauetan ezarritako betekizunak bete beharko ditu, eta bereziki jabetza intelektualari, datu pertsonalen babesari eta software maltzurra kontrolatzeari buruzkoak.

e) Kontratua bukatu ondoren, aktibo fisiko guztiak EJIEri itzuli beharko zaizkio, eta informazio-aktibo guztiak suntsitu edo EJIEri itzuli, justifikaziorik ez duen atzerapenik gabe.

f) Berariaz debekaturik dago:

1. Zerbitzuaren xedearekin loturarik ez duten jardueretarako erabiltzea EJIEk emandako baliabideak.
2. EJIEren ekoizpen-sarera konektatzea EJIEren jabetzakoak diren edo EJIEk ikuskatzen dituen software edo baliabide informatikoen estandar gisa identifikatuta ez dauden ekipamendu edota aplikazioak.
3. Informazio-sistemetan edo EJIEren sarean eduki lizunak, mehatxagarriak, moralgabeak edo iraingarriak paratzea.
4. Baliabide informatikoetan edozein aldaketa edo kalte eragiten duen edo eragin dezakeen edozein malware (programak, makroak, appletak, ActiveX kontrolak eta abar), gailu logiko, fisiko edo bestelako edozein ordena-sekuentzia nahita sartzea EJIEren sarean. EJIEren sarean sar daitezkeen langile guztiek biruskontrako programak eta horien eguneratzeak erabiltzeko betebeharra izango dute, datu informatikoak suntsitu edo hondatzen dituen elementu oro sisteman sartzea eragozteko.
5. EJIEk esleitu dizkienez bestelako eskubide edo sarbideak berariazko baimenik gabe lortzen saiatzea.
6. EJIEren informazio-sistemetako eremu mugatuetara berariazko baimenik gabe sartzen saiatzea.
7. EJIEren Informazio-sistemetako “log” erregistroak desitxuratzen edo faltsutzen saiatzea.
8. Zifratzeko gakoak, sistemak edo algoritmoak eta EJIEren prozesu telematikoetan erabiltzen den edozein segurtasun-elementu berariazko baimenik gabe deszifratzen saiatzea.
9. Beste erabiltzaileen lanean eragin lezaketen programak eduki, garatu edo exekutatzea eta EJIEren baliabide informatikoak kaltetu edo aldatzea.
10. EJIEren ardurapean diren datu, programa edo dokumentu elektronikoak suntsitzen, aldatzen, baliogabetzen edo beste modu batera kaltetzen saiatzea (egintza horiek kalte-delitua izan litezke, Zigor Kodeko 264.2 artikuluan ezarritakoaren arabera).
11. EJIEren datu pertsonalak edo datuen trataera EJIEri agindu zaionean erabiltzaileen PC postuetako tokiko disko-unitateetan gordetzea.

2.7 Erabiltzailearen erantzukizunak

a) Zerbitzuen hornitzaileek bermatu beharko dute EJIErentzat lan egiten duten langile guztiek oinarrizko printzipio hauek beteko dituztela informatika-jardunean:

1. EJIEren informazioa eskura izan dezakeen oro erabiltzaile-identifikadorean gauzatutako jardueren eta horietatik eratorritako guztiaren erantzule izango da. Hortaz, bere erabiltzaile-identifikadoreari lotutako autentifikazio-sistemak kontrolpean izan behar ditu pertsona bakoitzak ezinbestean. Bermatu beharko da, baita ere, erabiltzailea ez den beste inork ez ezagutzea gakoa.
2. Erabiltzaileak, hortaz, ez die bere gakoa zein den esan behar beste langileei, inola ere ez.
3. Erabiltzaileek ez dute beste erabiltzaile baten identifikadorerik erabiliko, ezta jabearen baimena badute ere.

b) Eskuen artean duten informazioaren baldintzak nahiz prozedurak ezagutu eta aplikatzen dituzte erabiltzaileek. EJIEren ardurapeko informazioa eskura dezakeen orok pasahitzak kudeatzeari buruzko zuzentarau hauek bete beharko ditu:

1. Kalitatezko pasahitzak aukeratzea.
2. Sistema eta pasahitzak arriskuan egotearen zantzurik badago, pasahitza aldatzeko eskatzea.
3. Aldian aldiro pasahitzak aldatzea, eta pasahitza zaharra ez erabiltzea edo ez berreskuratzea.
4. Lehenengo saio-hasieran (“login”) programak emandako nahiz aldi baterako pasahitzak aldatzea.
5. Saioa hasteko prozesu automatizatuetan –esaterako, funtzio-tekla edo makro batean bildutakoak– pasahitzik ez jartzea.
6. Pasahitzaren segurtasuna kinkan jarriz gero, dela pasahitza galdu duelako, hura lapurtu dutelako, edo konfidentzialtasuna galdu dela uste bada, haren berri eman beharko da.

c) EJIEren ardurapeko informazioa eskura dezaketen pertsona guztiek zaindu beharko dute ekipamenduak babesturik egongo direla zaintzarik gabe geratzen direnean.

d) Idazmahaia txukun izan behar dute EJIEren ardurapeko informazioa eskura dezaketen pertsona guztiek. Horrekin lortu nahi da, batetik, paperean diren agiriak nahiz informazioa gordetzeko gailu eramangarriak babestea eta, bestetik, baimenik ez duten pertsonek horiek eskuratzeko arriskua, horiek galtzeko edota informazioa galtzeko arriskuak murriztea, lanorduen barruan nahiz lanorduetatik kanpo. Aipatu pertsonek, beraz, idazmahaia txukun izateari buruzko arau hauek bete beharko dituzte:

1. Erabiltzen ez direnean, EJIEren ardurapeko informazioa dakarten paperezko dokumentuak eta baliabide informatikoak giltzapean nahiz altzari seguruetan biltegiratzea, batez ere lan-ordutegitik kanpo.
2. EJIEren funtzio kritikoetarako ekipamenduak zaintzarik gabe ez uztea, eta behar-beharrezkoa denean horien sarbidea blokeatzea.
3. EJIEren ardurapeko informazioa erabiltzen den guztietan, informazioa jasotzeko eta bidaltzeko puntuak babestea (posta, eskaner-makinak), bai eta kopiak egiteko ekipoak ere (fotokopiagailua, eskanerra). Erabiltzailearen ardura izango da gailu horien bidez informazioa sortu edo bidaltzea.
4. Behin inprimatu ondoren, EJIEren ardurapeko edozein informazio konfidentzial gordetzea, atzerapenik gabe –betiere, atzeratzeko arrazoirik izan ez bada–.
5. EJIEren ardurapeko datu pertsonalak edo informazio konfidentziala barne hartzen dituzten zerrendak leku seguruan gordetzea, langile baimenduak bakarrik sar daitezkeen leku batean.

6. EJIEren ardurapeko datu pertsonalak edo informazio konfidentziala dituzten zerrendak beharrezkoak ez direnean, horiek modu seguruan ezabatzea.
7. Informazioaren segurtasunarekin lotura izan dezaketen jazoeraren edota okerren bat gertatuz gero, EJIEren informazioa eskuratu edota haren sistemetara sar daitezkeen pertsonek ez dute sekula berariazko baimenik gabe egingo ustezko ahulezia edota segurtasun-okerra hautemateko probarik.
8. EJIEren informazioa eskura dezaketen edota haren sistemetan sar daitezkeen pertsonak ez dira inola ere saiatuko, baimen espliziturik gabe, segurtasun-sistema eta baimenak hausten. Debekatuta dago erabiltzaileek sareko trafikoak atzitzea, berariaz baimendutako ikuskatze-lanak egiteko ez bada edo beharrezkoa bada gorabeheraren bat konpontzeko. Debekatuta dago erabiltzaileek sareko trafikoak atzitzea, berariaz baimendutako ikuskatze-lanak egiteko ez bada edo beharrezkoa bada gorabeheraren bat konpontzeko.
9. EJIEren ardurapeko datu pertsonalik ez da gordeko ez erabiltzaileen ekipamenduetan ez eta informazio-euskarrietan ere.

e) EJIEren ardurapeko informazio-sistemetara sarbidea duen langile orok jarduera-arau hauek bete beharko ditu:

1. EJIEren jabetzako edo hirugarrenek EJIEri emandako informazio konfidentzial oro baimendu gabeko jakinarazpen, aldaketa, suntsipen edo erabilera desegokietatik —halabeharrezkoak izan ala ez— babestea.
2. Informazio-sistema eta telekomunikazio-sare guztiak babestea baimendu gabeko sarbide edo erabilera, operazio-eten, suntsipen, erabilera oker edo lapurretetatik.
3. Informazio-sistemetarako sarbidea lortzeko edota informazioa eskuratzeko beharrezkoa den baimena edukitzea.
4. Arau hauek ezagutzea, onartzea eta betetzea EJIEren informazioa eskuratu edota haren sistemetan sartu aurretik.

2.8 Erabiltzailearen ekipamenduak

a) Zerbitzuak eskaintzen dituztenek bermatuko dute EJIEren ardurapeko informaziora jotzeko erabilitako ordenagailu guztiek ondoko baldintza hauek beteko dituztela:

1. Denbora laburrez postu bat zaintzarik gabe uzten bada, sistemak bere blokeoa aktibatu beharko du.
2. Erakundearen sistemen barruan, erabiltzaileen ekipamenduetan ez da izango segurtasun-sistema eta baimenak urra ditzakeen tresnarik, salbu eta zerbitzua hornitzeko beharrezkoa denean.
3. Fabrikatzailearen argibideen arabera zainduko dira erabiltzaileen ekipamenduak.
4. Malwarearen kontra egoki babesturik daude erabiltzaile-ekipamendu guztiak:
    - Biruskontrako softwarea ordenagailu guztietan instalatu eta erabili beharko da, birusek edo bestelako software kaltegarriek eragin ditzaketen arriskuak murrizteko.
    - Eskura daitezkeen segurtasunari buruzko azken eguneraketak egingo dira eta, ondorioz, ekipamenduak egunean mantenduko.
    - Biruskontrako softwareak aktibatuta egon beharko du beti. Birusen definizio-fitxategiak automatikoki eguneratuko dira.

b) Zainduko da, bereziki, EJIEren ardurapeko informazioa dakarten edota modu batera edo bestera informazio hori eskuratzeko bide ematen duten erabiltzaileen ekipamendu mugikor guztien segurtasuna:

1. EJIEren ardurapeko informaziotik behar-beharrezkoa den hura baino ekarriko ez dutela egiaztatzea.
2. Informazio horretarako sarbideak kontrolatuko direla bermatzea.
3. EJIEri eskainitako zerbitzutik kanpoko pertsonen aurrean aipatu informazioa ahalik eta gutxien ikustea.
4. Leku batetik bestera eramatean kolperik har ez dezaten, ekipamenduak egoki diren zorroetan, maleta txikietan edo antzeko ekipamenduetan sartzea.
5. EJIEren egoitzetatik kanpo, babes-neurri bereziak hartu behar dira, hirugarrenek nahigabean ikus ez dezaten EJIEren ardurapeko informazioa.

2.9 "Hardware" ekipamenduaren kudeaketa.

a) Zerbitzuen hornitzaileek ziurtatu beharko dute edozein eratako zerbitzuak eskaintzeko asmoz ekipamendu guztiak egoki kudeatuko direla. Zerbitzuen hornitzaileek ziurtatu beharko dute edozein eratako zerbitzuak eskaintzeko asmoz ekipamendu guztiak egoki kudeatuko direla. Horretarako, honako arau hauek bete beharko dituzte:

1. Hornitzaileak egunean izan beharko du ekipamenduen zerrenda bai eta aktibo horien erabiltzaileena edota, pertsona batek baino gehiagok erabiliz gero, aktibo horien arduradunena ere. EJIEk edozein unetan eska diezaioke zerrenda hori.
2. Hornitzaileak berriz erabili nahi baldin badu EJIEren ardurapeko informazioa zekarren ekipamenduren bat, datuak segurtasunez ezabatu behar dira berriz erabili baino lehen.
3. Hornitzaileren batek EJIEk emandako ekipamenduetako bat zerrendatik kendu nahi badu, hura EJIEri bueltan eman beharko dio, Erakundeak egoki izapide dezan aipatu baja hori.
4. Hornitzaileren batek zerbitzua eskaintzeari uzten badio, hari emandako ekipamendu guztiak bueltan eman beharko dizkio EJIEri, zerbitzuak eskaintzeko kontratuetan xedatu bezalaxe. Informazio-aktiboetako informazioa baino ezin izango du segurtasunez ezabatu hornitzaileak. Horrelakoetan, jakinaren gainean jarri beharko du hornitzaileak EJIE.

3 Hornitzaileentzako Segurtasun-politika Espezifikoak

3.1 Hornitzaileentzako segurtasun-politika espezifikoen aplikagarritasuna

Hornitzaileentzako segurtasun-politika orokorrez gain, hornitzaile guztiek bete beharko dituzte, baita ere, atal honetako segurtasun-politika espezifikoetatik EJIEri eskainitako zerbitzuaren ezaugarrien arabera dagozkion horiek.

Jarraian, zerbitzuen motak zehaztuko ditugu.

- **Zerbitzua egiteko lekua:** zerbitzuak bi multzotan bana daitezke, hura eskaintzen den lekuaren arabera:
  - **EJIE**: Zenbait hornitzailek EJIEren egoitzan bertan eskaintzen dute zerbitzua.
  - **Urrunetik:** Zenbait hornitzailek bere egoitzatik eskaintzen du zerbitzua. Hala ere, EJIEren egoitzan gauza dezake hornitzaileak jarduera bat edo beste.
- **Erabilitako IKT azpiegituren jabetza:** zerbitzua eskaini ahal izateko erabilitako IKT azpiegitura nagusien jabea bat ala beste izan (komunikazioak, erabiltzaile-ekipamenduak, softwarea) bi zerbitzu-mota bereiz daitezke:
  - **EJIE**: EJIE: zerbitzua eskaintzeko erabilitako IKT azpiegitura gehienak EJIErenak direnean, eta hornitzaileak azpiegitura gutxi batzuk edota azpiegitura osagarriak jarri baditu.
  - **Hornitzailea:** Hornitzailea: zerbitzua eskaintzeko erabilitako IKT azpiegitura gehienak zerbitzua eskaini duenarenak badira, eta EJIEk jarritako horiek garrantzi handirik ez badute zerbitzuaren barruan.
- EJIEko sistemetara **sartzeko maila:** EJIEren informazio-sistemetarako sarbide-mailaren arabera, hiru multzo bereiz daitezke:
  - **Sarbiderik gabe:** EJIEren informazio-sistemak erabili behar ez direnean zerbitzua eskaintzeko. Hortaz, zerbitzua eskainiko duten langileek ez dute erabiltzaile-konturik aipatu sistema horietan.
  - **Erabiltzaile moduan sartzeko eskubidea:** EJIEren informazio-sistemak erabili behar direnean zerbitzua eskaintzeko. Horrelakoetan, erabiltzaile-kontuak izango dituzte zerbitzua eskaintzen duten langileek. Kontu horien bitartez, bidenabar, sistema horietako batzuetara sartzeko aukera izango dute langileek, eta ohiko zenbait abantaila.
  - **Sarbide pribilegiatua:** EJIEren informazio-sistemetara modu pribilegiatuan sartzeko gaitasuna behar denean zerbitzua eskaintzeko. Hau da, sistema horiek edota prozesatutako ekoizpen-datuak administratzeko gaitasuna izango dute langileek.
- EJIEko **teknologien kudeaketa:** Hornitzaileak teknologiak eta plataformak kudeatzen baditu, bi kasu bereizten dira:
  - **Bai**: hornitzaileak EJIEko teknologiak erabiltzeko kredentzialak kudeatzen ditu, administratzaile jardun dezan eta/edo pribilegioak eduki ditzan teknologi eta plataforma horietan.
  - **Ez**: hornitzaileak EJIEko teknologia eta plataformak erabil ditzake erabiltzaile moduan eta horretarako, EJIEri kredentzialak eskatu behar dizkio.

Zerbitzu bakoitza, beraz, aipatu lau kategoria horietako baten barruan izango da. Hortaz, segurtasun-politika orokorrak betetzeaz gain, hornitzaile bakoitzak honako taula honetan adierazitako bere kategoriari dagozkion politika espezifikoak bete beharko ditu:

	Tokia		Azpiegitura		Sarrera			Teknologien kudeaketa	
	EJIE	Urrutikoa	EJIE	Hornitzailea	Pribilegiatua	Erabiltzailea	Sarbiderik ez	Bai	Ez
Langileak hautatzea	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Segurtasunari buruzko auditoria (2009).	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Gorabeheren berri ematea	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Segurtasun fisikoa	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Aldaketen kudeaketa	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Kontingentzien kudeaketa	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Aktiboen kudeaketa	Ez da aplikatzen	Ez da aplikatzen	BAI	BAI	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	BAI	BAI
Segurtasun-arkitektura	EZ	BAI	Ez da aplikatzen	BAI	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen
Sistemen segurtasuna	BAI	BAI	EZ	BAI	BAI	BAI	BAI	BAI	BAI
Sare-segurtasuna	EZ	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Sistemen erabileraren trazabilitatea	BAI	BAI	Ez da aplikatzen	BAI	BAI	BAI	BAI	BAI	BAI
Identitateen eta sarbideen kontrola nahiz kudeaketa	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI	BAI
Aldaketen kudeaketa teknikoa	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	BAI	EZ
Garapen-segurtasuna	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	Ez da aplikatzen	BAI **(*)**	EZ

(*) Garapen-atazak badaude soilik

3.2 Langileak hautatzea

Zerbitzuak gauzatu ahal izateko hornitzaileek sarbide pribilegiatua izan behar badute EJIEren informazio-sistemetara, hornitzaileek honako arau hauek bete beharko dituzte langileak aukeratzeko orduan:

a) Zerbitzuan arituko diren langileen lanbide-aurrekariak ezagutu beharko ditu hornitzaileak. Hornitzaileak, zehazki, EJIEri bermatu beharko dio, batetik, langileak ez duela zigorrik jaso lanbidean jokabide okerra izateagatik, landutako informazioaren konfidentzialtasunari lotutako jazoeretan artean izan ez dela, eta arrazoi horregatik zigorrik jaso ez duela.

b) Gerta daiteke, "3.2.- EJIEri zerbitzuak eskaintzea" izeneko paragrafoan ezarritako baldintzen arabera pertsonaren bat betatzeko eskubidea bete nahi izatea EJIE. Horrelakoetan, zerbitzua eskainiko duten langileen zerrendatik betatu nahi duen pertsona berehala kentzeko aukera izango duela bermatuko dio hornitzaileak EJIEri.

3.3 Segurtasunari buruzko auditoria (2009).

Zerbitzuak gauzatu ahal izateko hornitzaileek sarbide pribilegiatua izan behar badute EJIEren informazio-sistemetara, hornitzaileek honako arau hauek bete beharko dituzte segurtasuna ikuskatzean:

a) Zerbitzuaren segurtasuna urtean gutxienez behin ikuskatzen utzi behar dio hornitzaileak EJIEri. Horrela, ikuskaritza-taldeari laguntza eskainiko dio hornitzaileak, eta eskatutako proba nahiz erregistro guztiak eman beharko ditu.

b) EJIEk berariaz ezarriko du ikuskapen bakoitzaren irismena eta sakontasuna. Zerbitzua eskainiko duen hornitzaile bakoitzarekin adostutako planifikazioari jarraituz gauzatuko dira ikuskaritzak.

c) Horrez gain, ohiz kanpoko ikuskapenak egiteko eskubidea izango du EJIEk, betiere, hori egiteko berariazko arrazoirik badago.

3.4 Gorabeheren berri ematea

Badira EJIEren IKT azpiegitura erabiltzearen bidez gauzatzen diren eta horiek gauzatzeko EJIEren informazio-sistemak erabili behar diren zenbait zerbitzu (sarbide pribilegiatua nahiz sarbide ez pribilegiatua). Hortaz, zerbitzua edozein lekutan eskaintzen dutela ere, era horretako zerbitzuak eskaintzen dituzten hornitzaile guztiek honako arau hauek bete beharko dituzte jazoerak jakinarazteko orduan:

a) Zerbitzua gauzatuko duten langileak Erabiltzailearen Laguntza Zentroarekin (ELZ) harremanetan jarri behako dira, EJIEren informazioarekin edo baliabideekin zerikusia duen edozein gorabehera detektatuz gero.

b) Edozein erabiltzailek informazioaren segurtasunarekin eta politika hauetan jasotako jarraibideekin zerikusia duten iradokizun, ahulune, hauskortasun, edota arrisku-egoeraren berri eman ahal izango dio EJIEko segurtasun-arduradunari.

c) Erabiltzailearen Laguntza Zentroari (ELZ) jakinarazi beharko zaio datu pertsonalen segurtasunari eragiten dion edo eragin diezaiokeen edozer gorabehera: zerrendak edota informazioa daukaten euskarriak galtzea, beste pertsona batzuek sarbide baimendua bidegabe erabiltzearen susmoa izatea, datuak berreskuratzea eta abar.

d) Jasotako gorabeheren bilketa, analisia eta kudeaketa zentralizatzen du Erabiltzailearen Laguntza Zentroak (ELZk).

e) ELZra jotzeko aukerarik ez badago, zerbitzuaren beraren barruan ezarritako komunikazio-bideak erabili beharko dira. Hau da, EJIEren bitartekaria jarriko da harremanean ELZrekin.

3.5 Segurtasun fisikoa

EJIEren egoitzatarako ohiko sarbidea daukaten hornitzaileek behar bezala zaindu behar dute sarbide-txartela. EJIEren instalazioetatik kanpo ezin du txartel hori begi-bistan eraman.

Hornitzaileak bere egoitzatik eskaintzen duen zerbitzu orotan segurtasunari buruzko politika hauek betetzen direla bermatu beharra dago:

a) Egoitzak areto itxia behar du izan eta kontrol sistemaren bat izan beharko da sarbideetan, lapurretarik, urratzerik eta eteterik egongo ez dela bermatzeko.

b) Bisitak kontrolatuko dira, gutxienez, edonor sar daitekeen eremuetan edota zama-lanetarako guneetan.

c) Suteak hautemateko sistemak izan beharko ditu egoitzak, eta uholdeei eusteko moduan eraikita egon.

d) EJIEren ardurapeko informazioaren kopiaren bat edukiz gero, honako babes-neurri hauek dituen leku batean egon beharko dute aipatu informazio hori gordetzen eta prozesatzen duten sistemek:

   1. Sarbideak kontrolatzeko sistema berezia eta egoitzarenaz bestelakoa izan beharko du babesturiko eremuak.
   2. Kanpoko langileek sarbide mugatua izango dute babes bereziko guneetara. Soilik beharrezkoa denean eta horretarako baimena dutenean sartuko dira, betiere, baimendutako langileen zaintzapean.
   3. Kanpoko pertsonen sarbide guztien erregistro bat egongo da.
   4. Kanpoko langileek ezingo dute, ikuskapenik gabe, bereziki babestutako guneetan egon edo lanik egin.
   5. Debekaturik dago bereziki babestutako gune horietan jatea edo edatea.
   6. Elikatze-hutsegiteen aurrean babesturik egoteko neurriren bat izan behar dute gune horietan kokatutako sistemek.

3.6 Aktiboen kudeaketa

Hornitzailearen IKT azpiegiturak erabiltzearen bidez eskainitako zerbitzuen hornitzaile guztiek aktiboak kudeatzeko orduan honako arau hauek betetzen direla bermatu beharko dute:

a) Aktiboen erregistro eguneratua izan behar du hornitzaileak. Erregistro horretan, zerbitzua eskaintzean erabilitako aktibo guztiak jaso behar dira.

b) Zerbitzua eskaintzeko erabili diren aktibo guztiek arduradun bat izan behar dute. Hark bermatuko du, hain zuzen, erakundeak ezarritako gutxieneko babes-neurriak, hots, politika honetan zehaztutako babes-neurriak betetzen dituztela aipatu aktibo horiek.

c) Zerbitzua eskaintzeko erabilitako aktiboak kentzean, haren berri eman beharko dio hornitzaileak EJIEri.

d) EJIEren ardurapeko informazioa gorde duen aktibo bat bajan eman nahi izanez gero, aipatu informazioa modu seguruan ezabatu beharra dago. Horretarako, datuak ziurtasunez ezabatzeko funtzioak aplikatu behar dira edo, bestela ere, aktiboa fisikoki suntsitu, hartan gordetako informazioa berreskuratzeko modurik ez egoteko. Eskatzen bada, hornitzaileak EJIEri egiaztagiri bat emango dio informazio-fitxategiak seguru ezabatu direla egiaztatzeko.

3.7 Segurtasun-arkitektura

Badira hornitzailearen IKT azpiegitura erabiltzearen bidez gauzatzen diren eta EJIEren informazio-sistemak erabiltzen dituzten zenbait zerbitzu (sarbide pribilegiatua nahiz sarbide ez pribilegiatuaren bidez). Era horretako zerbitzuak eskaintzen dituzten hornitzaile guztiek honako arau hauek bete beharko dituzte segurtasun-arkitekturari buruz.

a) EJIErentzako garapen-lanak edota aplikazioen probak egitean edota EJIEren ardurapeko datuak erabiltzean, aipatu jarduerak gauzatzeko erabilitako inguruneak elkarren bereizi egongo dira. Inguruneok bereizita egongo dira, baita ere, EJIEren ardurapeko informazioa gordetzen edo prozesatzen duten ekoizpen-inguruneetatik.

b) EJIEren ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistema guztietarako sarbideak babesturik egon behar dira, gutxienez, sistema horietara konektatzeko gaitasuna mugatuko duen suebaki baten bidez.

c) EJIEren ardurapeko informazio berezia gordetzen edo prozesatzen duten informazio-sistemek gainerako beste sistema guztietatik isolaturik egon behar dute.

d) EJIEri zerbitzua ematen dieten informazio-sistemek erabilgarritasun-baldintzak betetzeko behar besteko erredundantzia izan behar dute.

3.8 Sistemen segurtasuna

Sistemen segurtasunak honako arau hauek betetzen dituela bermatu beharko dute beren IKT azpiegiturak erabiltzearen bidez zerbitzuak eskaintzen dituzten hornitzaile guztiek:

a) Bere funtzionamenduari buruzko jazoerarik nabarmenenak jaso beharko dituzte EJIEren ardurapeko informazioa gordetzen edota tratatzen duten informazio-sistemek. Erakundearen segurtasun-kopien politikaren barruan izango dira jarduera-erregistro horiek.

b) Elkarren artean nahiz ordu ofizialarekin sinkronizaturik egongo dira hornitzailearen sistemetatik EJIEren ardurapeko informazioa prozesatzen edo gordetzen duten horien erlojuak.

c) EJIEren ardurapeko informazioa gordetzen edo tratatzen duten informazio-sistemen edukiera egoki kudeatzen dela bermatuko du zerbitzuaren hornitzaileak. Horrela, baliabideak saturatzearen erruz hizpide ditugun sistemak etengo ez direla eta oker funtzionatuko ez dutela zainduko du hornitzaileak.

d) Software gaiztoaren kontra egoki babesturik egongo dira EJIEren ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistemak. Horretarako, ondoko neurri hauek hartuko dira aldez aurretik:

    1. Proba, garapen eta ekoizpeneko inguruneetan, sistemak eguneratuta eduki beharko dira eskura dauden azken segurtasun-eguneratzeekin.

    2. Biruskontrako softwarea zerbitzari eta ordenagailu guztietan instalatu eta erabili beharko da, birusek edo bestelako software kaltegarriek eragin ditzaketen arriskuak murrizteko.

    3. Biruskontrako softwareak aktibatuta egon beharko du beti. Birusa definitzeko fitxategien eguneratze automatikoa ezarri beharko da hala ordenagailuetan nola zerbitzarietan, baita birus informatikoak detektatzean ordenagailua blokeatzeko sistemak ere.

e) Eskainitako zerbitzuarentzat garrantzi handia duen datu edo informazio oro babesteko asmoz, segurtasun-kopiak egiteko politika ezarriko du hornitzaileak. Aipatu kopia horiek, gehienez ere, hilabetean behin egingo dira.

f) Zerbitzua eskaintzean posta elektronikoa erabiltzen bada, hornitzaileak honako baldintza hauek bete beharko ditu:

1. Ez da onartuko posta elektroniko bidez EJIEren informazio konfidentziala bidaltzea, salbu eta komunikazio elektronikoa zifratuta badago eta bidalketa berariaz onartu bada.
2. Ez da onartuko posta elektroniko bidez goi-mailako datu pertsonalak dituen informazioa bidaltzea, salbu eta komunikazio elektronikoa zifratuta badago eta bidalketa berariaz onartu bada.

g) Zerbitzua eskaintzean EJIEren e-posta erabiliz gero, printzipio hauek errespetatu beharko dira gutxienez:
   1. Posta elektronikoa langilearen esku jartzen den beste lan-tresna bat da, eta beraz kontratatutako zerbitzua eskaintzeko soilik erabili beharko da. Hala, EJIEk kontrol-sistemak ezarri ahal izango ditu baliabide hori babestu eta behar bezala erabiltzen dela ziurtatzeko. Dena den, langilearen duintasuna eta intimitaterako eskubidea zainduz baliatuko du ahalmen hori.
   2. EJIEren 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.

h) EJIEren ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistemetarako sarbidea egiaztatu beharko da beti; gutxienez, erabiltzaile-identifikadorearen eta hari lotutako pasahitzaren bidez. "Ohiko" erabiltzaileek eta, batez ere, informazio-sistema horietako administrazio-sarbidea duten erabiltzaileek bete behar dute obligazio hori.

i) EJIEren ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistemetan sarbidea kontrolatzeko sistemak izango dira. Kontrol-sistema horien bidez, bidenabar, zerbitzuan lan egiten dutenei baino ez zaie utziko aipatu informazioa eskuratzen.

j) Erabiltzaileek denbora batez jardunari uztean automatikoki blokeatuko dira EJIEren ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistemetarako sarrera-saioak.

k) EJIEk emandako softwarea erabiltzen den guztietan, ondoko arau hauek bete beharko dira:
   1. Emandako software-bertsioak bakarrik erabili beharko dituzte EJIEren informazio-sistemetara sarbidea duten langileek, eta horien erabilera-arauak bete.
   2. Langileek debekatua dute edozein programaren legez kontrako kopiarik egitea, programa estandarizatuenak barne.
   3. Debekatuta dago EJIEk baliozkotu ez duen softwarea erabiltzea.
   4. Debekatuta dago, halaber, EJIEk instalatutako edozein programa desinstalatzea.

3.9 Sare-segurtasuna

Sare-segurtasunaren honako arau hauek betetzen dituztela bermatu beharko dute beren IKT azpiegiturak erabiltzen dituzten hornitzaile guztiek:

a) Egoki kudeatu eta kontrolatu behar dira EJIEren ardurapeko informazioa dakarten sareak. Horretarako, kontrolez kanpoko sarbiderik ez dagoela eta hornitzaileak konexioen arriskuak egoki kudeatzen dituela bermatuko da.

b) Ahalik eta gehien mugatu behar dira EJIEren ardurapeko informazioa dakarten sareetako zerbitzuak.

c) EJIEren IKT azpiegiturara sartzeko bidea ematen duten sareek egoki babesturik egon behar dute. Horretarako, honako baldintza hauek bete beharko dituzte:

1. Urruneko erabiltzaileek EJIEren sarera sarbidea izateko, sarbidea baliozkotzeko eta aurretiazko kautotze-prozedurak bete beharko dira.
2. Denbora mugatu batez egingo dira konexio horiek, sare pribatu birtualak edo ardura bakarreko lineen bidez.
3. Kontroletik kanpoko aukerako beste konexio batzuk egiteko bide ematen dutenetik, ezin izango da komunikazio-ekipamendurik erabili konexio horietan (hots, txartelak, modemak, eta abar).

d) EJIEren ardurapeko informazioa dakarten sareetarako sarbidea mugaturik egongo da.

e) EJIEren ardurapeko informazioa dakarten sareetara konektatutako ekipo guztiak behar bezala identifikaturik egon behar dira, halako moduz non sare-trafikoak identifika daitezkeen.

f) Telelana, alegia kanpotik lana egitea sare korporatiborako sarbidea izanik, politika hauen bidez arautuko da:

1. Sare korporatibora modu seguruan konektatzeko bete beharreko neurriak ezarriko dira.
2. Ezarritako konexioen segurtasuna monitorizatu eta ikuskatzeko sistemak ezarriko dira.
3. Jarduerari dagokion epealdia amaitzean, sarbide-eskubideak ezeztatu direla eta ekipamendua itzulia izan dela kontrolatuko da.

EJIEk emandako Interneterako sarbidea erabiltzen den guztietan, lehen aipatutakoez gain, bete beharko dira, baita ere, ondoko politika hauek:

g) Internet lan-tresna bat da. Beraz, Interneten egiten diren jarduera guztiek lotura izan beharko dute laneko eginbeharrekin. Erabiltzaileek ez dituzte bilatu edo bisitatu behar EJIEren negozio-helburuari edo eguneroko lanari laguntzeko balio ez duten webguneak.

h) 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.

i) Erabiltzaileek ezingo dute erabili EJIEren izena, sinboloa, logotipoa edo horien antzekoak Interneteko ezein elementutan (posta elektronikoa, web-orriak eta abar), ez bada laneko jarduerei lotutako arrazoiengatik.

j) Internetera edo Internetetik datu-transferentziak egitea onartuko da, soilik, negozioko jarduerekin lotura badute. Debekatuta dago jarduera horiekin zerikusirik ez duten fitxategi-transferentziak egitea (adibidez, ordenagailuko jokoak, soinu-fitxategiak, multimedia-edukiak eta abar deskargatzea).

3.10 Sistemen erabileraren trazabilitatea

Badira hornitzailearen IKT azpiegitura erabilita gauzatzen diren eta EJIEren informazio-sistemak modu pribilegiatuan erabiltzen dituzten zenbait zerbitzu. Era horretako zerbitzuak eskaintzen dituzten hornitzaile guztiek bermatu beharko dute sistemen erabilera-trazabilitateari buruzko politika hauek betetzen direla gutxienez:

a) Sarrera pribilegiatuak erregistratuko dira. Erregistro horiek, bidenabar, Erakundearen segurtasun-kopiei buruzko politikan xedatutakoaren arabera gordeko dira.

b) Sarbide pribilegiatuak egiteko erabili izan den sistemaren jarduera erregistratuko da. Erregistro hori, bidenabar, Erakundearen segurtasun-kopiei buruzko politikan xedatutakoaren arabera gordeko da.

c) Aztertu egingo dira sistemen jardueran erregistratutako akatsak eta okerrak, eta horiek konpontzeko beharrezkoak diren neurriak ezarriko dira.

3.11 Identitateen eta sarbideen kontrola nahiz kudeaketa

EJIEren ardurapeko informazioa eskuratzeko orduan, identitateak nahiz sarbideak kontrolatzeko eta kudeatzeko politika hauek betetzen direla bermatu beharko dute beren IKT azpiegituraren bidez zerbitzua eskaintzen duten hornitzaile guztiek:

a) Informazio-sistema batera sarbidea duten erabiltzaile guztiek sarbide-baimen bakar bat izango dute, erabiltzailearen identifikadoreaz eta pasahitzaz osatua. "Ohiko" erabiltzaileek eta, batez ere, informazio-sistema horietako administrazio-sarbidea duten erabiltzaileek bete behar dute obligazio hori.

b) Erabiltzaileena da beren sarbide baimendua erabiliz egiten dituzten jarduera guztien ardura.

c) Erabiltzaileek ez dute beste erabiltzaile baten sarbide baimendurik erabiliko, ezta jabearen baimena badute ere.

d) Erabiltzaileak ez dio, inola ere, bere identifikadorea edota pasahitza inori jakinaraziko, eta ezta begi-bistan idatzita edo hirugarrenen eskura edukiko ere.

e) Pasahitzak gutxienez 6 karaktere izan beharko ditu.

f) Pasahitzak karaktere alfabetikoak eta numerikoak konbinatuz osatu beharko dira.

g) Pasahitzak aukeratzeko, komeni da jarraibide hauei lotzea:

   1. Ez erabiltzea hitz ezagunik, ezta norberarekin lotura izan dezakeenik, izena kasu.
   2. Pasahitzak ez du antzeman litekeen kontzeptu, objektu edo ideia bat gogorazi behar. Beraz, pasahitzetan ez da erabili behar data esanguratsurik, astegunik, hilabeterik, pertsona-izenik, telefono-zenbakirik eta antzekorik.
   3. Pasahitza ia asmaezina izan behar da. Baina aldi berean erraza izan behar da erabiltzaileak gogora dezan. Adibidez, egokia litzateke esaldi edo esamolde baten akronimoa erabiltzea.
   4. Gakoak, gutxienez, karaktere numeriko bat eta alfabetiko bat izan beharko lituzke.
   5. Ez da komeni erabiltzailearen identifikadorea gako sekretuaren zati modura erabiltzea.

h) EJIEren ardurapeko informaziora horretarako baimen egokia duten langileak ez beste inor ez direla sartzen aldian aldiro egiaztatzen dela bermatu behar du hornitzaileak.

Horrez gain, langileak EJIEren informazio-sistemetara sartzen diren kasuetan, arau hauek hartu beharko dira kontuan ere:

i) Ezein erabiltzailek ez du jasoko EJIEren sistemetara sarbidea izateko identifikadorerik, harik eta indarrean dagoen segurtasun-politika formalki onartzen duten arte.

j) Erabiltzaileek sarbide baimendua izango dute, soilik, beren funtzioak betetzeko behar dituzten datu eta baliabideetarako.

k) Sistemak automatikoki eskatzen ez badu, erabiltzaileak aldatu beharko du sistemara sarbide egokia egiten den lehenengo aldian esleitutako aldi baterako pasahitza.

l) Sistemak automatikoki eskatzen ez badu, erabiltzaileak gutxienez 90 egunean behin aldatu beharko du pasahitza. Hala egiten ez badu, sarbidea ukatu ahal izango zaio, eta kasu horretan Erabiltzailearen Laguntza Zentroarekin (ELZ) harremanetan jarri beharko du pasahitz berria eskuratzeko.

m) Aldi baterako sarbide baimenduak denbora-tarte labur baterako konfiguratuko dira. Epe hori amaitzean, sistematik desaktibatuko dira.

n) Datu pertsonalei dagokienez, berariaz baimendutako langileek bakarrik eman, aldatu edo ezeztatu ahal izango dute datu eta baliabideen gaineko sarbide baimendua, beti ere fitxategiaren arduradunak ezarritako irizpideen arabera.

o) Erabiltzaile batek susmatzen badu beste pertsona bat bere sarbide baimendua (erabiltzailearen identifikadorea eta pasahitza) erabiltzen ari dela, pasahitza aldatu beharko du, eta Erabiltzailearen Laguntza Zentroarekin (ELZ) harremanetan jarri beharko du gertatutakoaren berri emateko.

3.12 Aldaketen kudeaketa

Badira hornitzailearen IKT azpiegitura erabiltzearen bidez eta EJIEren informazio-sistemak erabilita gauzatzen diren zenbait zerbitzu (sarbide pribilegiatuaren nahiz sarbide ez pribilegiatuaren bidez). Era horretako zerbitzuak eskaintzen dituzten hornitzaile guztiek aldaketak kudeatzeko orduan honako arau hauek betetzen direla bermatu beharko dute:

a) Kontrolpean eta baimenduta egon behar dira IKT azpiegituran egindako aldaketa guztiak. Bermatu beharko da, baita ere, kontrolez kanpoko osagairik ez dela IKT azpiegituran.

b) Egiaztatu beharko da, baita ere, zerbitzua eskaintzeko asmoz hornitzaileak erabilitako IKT azpiegituran sartu diren osagai berri guztiek egoki funtzionatzen dutela, eta horiek sartzeko heldu ziren xede guztiak betetzen dituztela.

3.13 Aldaketen kudeaketa teknikoa

Zerbitzuak gauzatu ahal izateko hornitzaileek sarbide pribilegiatua izan behar badute EJIEren informazio-sistemetara, aldaketak kudeatzean honako arau hauek betetzen direla bermatu beharko dute hornitzaileek:

a) Formalki ezarritako nahiz dokumentatutako prozedura betez gauzatu behar dira aldaketa guztiak. Prozedura horrek bermatu behar du egoki diren urratsak eman direla aldaketa egiteko orduan.

b) Funtsezko osagaietan ezinbesteko aldaketak besterik egiten ez direla bermatu beharko du aldaketak kudeatzeko prozedurak.

c) Funtsezko osagaietan egindako aldaketa guztiak egiaztatu beharko dira, osagai horien funtzionamenduaren edo haien segurtasunaren gain kontrako albo-ondoriorik edo aldez aurretik aurreikusi ez den ondoriorik gertatzen ez dela egiaztatzeko.

d) Zerbitzua eskaintzeko erabilitako azpiegituren ahulgune teknikoak aztertu beharko dituzte hornitzaileek. Horrela, funtsezko osagaiekin lotura duten ahulezia tekniko guztien berri eman beharko diote EJIEri, biek elkarrekin kudea ditzaten aipatu ahulguneak.

3.14 Garapen-segurtasuna

Aplikazioak garatzen dituzten zenbait hornitzailek EJIEren informazio-sistemetara sarbidea (pribilegiatua nahiz ez pribilegiatua) izan behar dute zerbitzua eskaintzeko orduan. Hornitzaile horiek, beraz, aipatu jarduera horretan ondoko segurtasun-arau hauek betetzen direla bermatu behar dute gutxienez:

a) EJIEk kontrolatu eta ikuskatuko du softwarea Erakundetik kanpo garatzeko prozesu osoa. Prozesua formal horrek jarraitu beharreko arauak markatuko ditu.

b) Aplikazioak diseinatzeko, garatzeko, inplementatzeko prozesuan eta eragiketa orotan, identifikazioko, kautotzeko, sarbide-kontroleko, ikuskapeneko eta segurtasuneko mekanismoak baliatu dira.

c) Kasuan kasu, bete beharreko segurtasun-baldintza guztiak berariaz zehaztuko dira aplikazioen zehazpenetan.

d) Sarrera-datuak baliozkotu beharko dira garatzen diren aplikazio berrietan. Horrela, sarrera datuak egokiak nahiz zuzenak direla egiaztatuko da, eta kode egikarigarriak sar daitezela saihestu.

e) Aplikazioek garatutako barne-prozesuen artean izango da, baita ere, informazioa galbideratuko ez dela bermatzeko beharrezkoak diren baliozkotze guztiak.

f) Beharrezkoa den guztietan, egiaztapenak eta integritate-kontrolak egiteko funtzioak ezarri behar dira aplikazioen hainbat osagaien arteko harremanetan.

g) Aplikazioek emandako irteera-informazioa mugatu beharko da, informazio egokia eta beharrezkoa besterik ematen ez dela bermatzeko.

h) Zerbitzuan aritzen diren langileak izango dira aplikazioen iturri-kodera sar daitezkeen bakarrak.

i) Garapen eta proba faseetan, segurtasun-funtzionalitateei buruzko proba espezifikoak egingo dira.

j) Probak egitean, datu errealak erabil daitezke, baldin eta egoki disoziatu badira, edota ekoizpen-ingurunearen moduko segurtasun-neurriak aplikatu direla berma badaiteke.

k) Aplikazioen probak egitean, informazioak kontrolik gabe ihes egiten ez duela egiaztatuko da. Egiaztatuko da, baita ere, aurreikusitako informazioa baino ematen ez dela ezarritako kanaletatik.

l) Berariaz onartutako aplikazioak baino ez dira bidaliko ekoizpen-ingurunera.

3.15 Kontingentzien kudeaketa

Jardunean honako segurtasun-arau hauek betetzen dituztela bermatu beharko dute beren IKT azpiegiturak erabiltzen dituzten hornitzaile guztiek:

a) Kontingentziak egonda ere, hura eskaintzen jarraitzeko plana izan behar du zerbitzuak.

b) Zerbitzua eten dezaketen jazoeren eta horiek gertatzeko probabilitatearen arabera garatu da aurreko plana.

c) Egungo kontingentzia-plana bideragarria dela froga dezake hornitzaileak.

4 Zerbitzuak kanpora ateratzean bete beharreko segurtasun-baldintzak

EJIEk zenbait betebehar ezartzen dizkie hornitzaileei, dokumentu honetan jasoak: **“Enpresa hornitzaileentzako araudia– I. eranskina: IKT azpiegitura / Segurtasun fisikoa eta ingurunearen segurtasuna”.** Araudi honen helburuak dira zerbitzua eskaintzeko erabiltzen den azpiegitura zehaztea, derrigorrezko kontrolak zehatz-mehatz deskribatzea eta segurtasun fisikoa eta ingurunearen segurtasuna bermatzeko bestelako alderdiak azaltzea. **Dokumentua derrigorrez bete beharko da eranskin gisa sartua izan den espedienteetan,** eta erreferentziako dokumentua izango da arauak bete diren egiaztatzeko ikuskapenetan.

5 Jarraipena eta kontrola

a) Aipatutako baliabideak ondo erabiltzen direla zaintzeko, erabiltzaileek baliabide horiekin egiten duten erabilera egokia den begiratu behar du EJIEk, aldizka nahiz segurtasun- edo zerbitzu-arrazoi bereziengatik, kasu bakoitzean aukeratutako mekanismo formal eta teknikoen bidez.

b) Inork aplikazioak edota datuak –nagusiki– edo beste edozein baliabide informatiko oker erabiltzen dituela antzemanez gero, horren berri emango zaio pertsona horri, eta, hala badagokio, baliabideak behar bezala erabiltzeko prestakuntza eskaini.

c) Aplikazioak edota datuak –nagusiki– edo beste edozein baliabide informatiko oker erabiltzean fede txarra antzemanez gero, EJIEk dagozkion legezko egintzak baliatuko ditu bere eskubideak babesteko.

6 Segurtasun-politikak eguneratzea

Teknologiaren, segurtasunen inguruko mehatxuen eta arlo horretan sortzen ari diren legezko ekarpen berrien bilakaera dela-eta, EJIEk eskubidea du, behar denean, politika horiek aldatzeko. Politika horietan egindako aldaketak dagokien enpresa hornitzaile guztiei jakinaraziko zaizkie, egoki jotzen den eran. Enpresa hornitzaile bakoitzaren erantzukizuna da EJIEk segurtasunaren alorreko politiketan egindako berrikuntzak langileek irakurri eta ezagutzen dituztela bermatzea.