HORNITZAILEENTZAKO SEGURTASUN-POLITIKA

Erreferentzia:	IZENPE – Hornitzaileentzako segurtasun-politika
Bertsio-zk.:	v 1.1
Data:	2020ko otsailaren 3a

Beato Tomás de Zumárraga
71 - 1ª Planta
01008 Vitoria - Gasteiz

www.izenpe.com
info@izenpe.com
Tel.: 945 06 77 23

Bertsioen historikoa:

BERTSIO	DATA	ALDAKET
1.0	10/11/2016	Hasierako bertsioa
1.1	03/02/2020	• Lekuaren araberako zerbitzu mota aldatu da 3.1 atalean • "identifikazio-puntua" erabiltzaile mota gehitu da 3.1 atalean • Politika espezifikoei buruzko atalean eskaintzen den zerbitzu motaren sailkapena aldatu da

Aurkibidea

1. SARRERA 4
   1.1 XEDEA 4
   1.2 APLIKAZIO-ESPARRUA 4
2. SEGURTASUN-POLITIKA OROKORRAK 5
   2.1 IZENPERENTZAKO ZERBITZUGINTZA 5
   2.2 INFORMAZIOAREN KONFIDENTZIALTASUNA 5
   2.3 JABETZA INTELEKTUALA 6
   2.4 INFORMAZIO-TRUKEA 6
   2.5 BALIABIDEEN ERABILERA EGOKIA 7
   2.6 ERABILTZAILEAREN ERANTZUKIZUNAK 8
   2.7 ERABILTZAILEEN EKIPOAK 10
3. SEGURTASUN-POLITIKA ESPEZIFIKOAK 11
   3.1 HORNITZAILEENTZAKO SEGURTASUN-POLITIKA ESPEZIFIKOEN APLIKAGARRITASUNA 11
   3.2 LANGILE-HAUTAKETA 12
   3.3 SEGURTASUN-IKUSKAPENA 12
   3.4 GORABEHERAK JAKINARAZTEA 12
   3.5 SEGURTASUN FISIKOA 13
   3.6 AKTIBOEN KUDEAKETA 13
   3.7 SEGURTASUN-ARKITEKTURA 14
   3.8 SISTEMEN SEGURTASUNA 14
   3.9 SARE-SEGURTASUNA 16
   3.10 SISTEMEN ERABILERA-TRAZABILITATEA 16
   3.11 IDENTITATEEN ETA SARBIDEEN KONTROLA ETA KUDEAKETA 17
   3.12 ALDAKETEN KUDEAKETA 18
   3.13 SEGURTASUNA GARAPENEAN 18
   3.14 GORABEHEREN KUDEAKETA 19
4. JARRAIPENA ETA KONTROLA 19
5. SEGURTASUN-POLITIKAK EGUNERATZEA 19

1. SARRERA

1.1 XEDEA

Dokumentu honen xedea da informazioaren segurtasuna bermatuko duten jarraibideak ezartzea, *Ziurtapen eta Zerbitzu Enpresa-Empresa de Certificación y Servicios, Izenpe SA*ren (aurrerantzean, Izenpe) hornitzaile diren erakundeei aplikatzeko.

Helburua da informazioa galdu edo behar ez bezala erabiltzeko arriskua saihestea, horrek Izenpek eskaintzen duen zerbitzuari edo haren ospeari kalterik ez egiteko. Horretarako, politika honek erakunde hornitzaileei aplika dakizkiekeen eskakizunak deskribatzen ditu, haien eginkizunak betetzean Izenperen informazioa edo baliabideak eskura ditzaketenean.

Asmoa da Izenperen konfidentzialtasuna, segurtasuna eta informazioaren eta sistemen eskuragarritasuna babestea.

Horretarako, erakunde hornitzaileek erantzukizuna hartuko dute Izenperentzat lan egiten dutenek politika hau ezagutu dezaten eta berori errespetatzeko konpromisoa idatziz har dezaten.

1.2 APLIKAZIO-ESPARRUA

Politika hau erakunde hornitzaileetako langileek egiten dituzten jarduera guztiei aplikatuko zaie, baldin eta Izenperen informazioa badute edo Izenperentzat garapenak egiten badituzte, eta jarduera horiek dagokion kontratu-esparruaren bidez lotuta badaude.

- "SEGURTASUN-POLITIKAK" atala edozein hornitzaileri aplikatuko zaio (lehen adierazitako esparruan), egindako zerbitzu mota edozein dela ere.
- Politika honen "SEGURTASUN-POLITIKA ESPEZIFIKOAK" atalean bildutako azpiataletako bakoitza aplikatzekoa izango da, soilik, kasuak kasu adierazitako zerbitzu motarekin bat datozen zerbitzuak egiten dituzten hornitzaileentzat, aipatutako atalaren hasieran adierazten denez.

2. SEGURTASUN-POLITIKA OROKORRAK

2.1 IZENPERENTZAKO ZERBITZUGINTZA

1. Erakunde hornitzailearen jarduerak egingo dira dagokion kontratu erregulatzailean ezarritakoaren arabera, baita Izenperen eta hornitzailearen artean horretarako finkatutako arau eta prozeduren arabera ere.

2. Erakunde hornitzaileak, akordioaren hasieran, Izenperi jakinaraziko dio hornitutako zerbitzuarekin lotutako pertsonen, profilen, zereginen eta erantzukizunen zerrenda, eta unean-unean emango dio zerrenda horretan izaten den edozein aldaketaren berri (alta, baja, ordezkapena edo zereginen edo erantzukizunen aldaketak).

3. Akordioan ezarritako epearen arabera, Izenperentzat lanak egiten dituzten kanpoko langile guztiek dokumentu honetan zehaztutakoa bete beharko dute.

   Ezarritakoa beteko ez balitz, Izenpek beretzat gordetzen du arau-haustea egin duten langileen gaineko beto-eskubidea, eta bidezkotzat jotzen dituen zigor-neurriak hartzekoa ere, kontratatutako erakundeari dagokionez. Neurri horiek berekin ekar dezakete indarrean dauden akordioak deuseztatzea.

4. Erakunde hornitzaileak ziurtatu beharko du bere langile guztiek prestakuntza eta trebakuntza egokia dutela zerbitzua egiteko, bai maila zehatzean, zerbitzugintzari lotutako jarduerari dagozkion gaietan, bai zeharka, informazioaren segurtasunari dagokionez. Horretarako, ziurtatu beharko du zerbitzuarekin lotutako langile guztiek ezagutzen dutela politika hori. Gainera, berori betetzeko konpromisoa hartuko du.

5. Izenperen eta erakunde hornitzaileen artean dagoen edozein motatako informazio-trukea hartuko da bi aldeen artean dagoen kontratu-esparruaren barruan gauzatutzat. Hala, informazio hori ezin izango da erabili, inola ere, esparru horretatik kanpo, ezta aipatutako akordioari dagozkionak ez diren xedeetarako ere.

6. *Informazioaren Segurtasun Arloa*k bateratu egiten ditu Izenperen aktiboak babesteko ahalegin orokorrak, erakundearen prozesuen oinarri diren informazio-teknologien funtzionamendu egokia ziurtatzearren.

2.2 INFORMAZIOAREN KONFIDENTZIALTASUNA

1. Izenperen informaziorako sarbidea duten kanpoko langileek kontuan hartu beharko dute informazio hori, berez, konfidentziala dela.

   Informazio ez-konfidentzialtzat hartu ahal izango da, soilik, informazioaren hedapen publikoko bitartekoen bidez Izenpek lortutako informazioa.

2. Saihestu egingo da informazioa jakinaraztea, aldatzea, suntsitzea eta gaizki erabiltzea, hura jasota dagoen euskarria edozein dela ere.

3. Erreserba handiena mugagabe gordeko da, berariazko baimenik ezean.

4. Minimizatu egingo da informazio konfidentziala duten paper-formatuko txostenak, eta leku seguruan eta hirugarrenengandik babestuta gordeko dira.

5. Izenpek edo erakunde hornitzaileak eskura jarritako tresnak erabiliko dituzte soilik kanpoko langileek, eta betiere erabilera profesionaletarako besterik ez.

6. Kolaboratzaileetako inork ere ezin izango du eduki, bere erantzukizunari ez dagokion erabileretarako, Izenperena den edo bere ardurapean utzi den inolako material edo informaziorik.

7. Duen lanpostuarekin zuzenean lotutako arrazoiengatik, erakunde hornitzaileko enplegatuak edozein euskarritan jasotako informazio konfidentziala eskura badu, ulertuko da informazio hori aldi baterako duela, eta enplegatu horrek informazioa sekretupean edukitzeko betebeharra izango du; horrek ez dio ematen informazioaren edukitzaren, titulartasunaren edo kopiaren gaineko inolako eskubiderik.

   Gainera, enplegatuak aipatutako euskarria edo euskarriak itzuli beharko ditu, horien aldi baterako erabilera eragin duten lanak amaitu eta berehala eta, nolanahi ere, Izenpek enplegatuaren erakundearekin duen harremana bukatzean.

   Hitzartutakoaz bestelako edozein formatu edo euskarritan jasotako informazioa Izenpe jakinaren gainean egon gabe erabiliko balitz ere, horrek inola ere ez du puntu honetan ezarritakoa aldatuko.

8. Betebehar horiek guztiek indarrean jarraituko dute kanpoko langileek Izenperentzat egindako lanak amaitzean ere.

9. Zigor Kodeko 197. artikuluan ezarritakoaren arabera, betebehar horiek ez betetzea delitua izan daiteke sekretuak agerrarazteagatik, eta konpentsazioak eskatzeko eskubidea sor dezake.

10. Langileek datu pertsonalen aldi baterako fitxategiak sortu ahal izango dituzte soilik lan egiteko beharrezkoa denean. Aldi baterako fitxategi horiek inoiz ere ez dira jarriko langileen PC postuetako disko-unitate lokaletan, eta sortu ziren helbururako erabilgarriak izateari uzten diotenean, suntsitu egin beharko dira.

11. Datu pertsonalak dituzten euskarri informatikoak informazio hori jasotzen duten lokaletatik atzeratzeko, Izenperen baimena beharko da eta zehaztutako prozeduraren arabera egingo da hori. Datu pertsonalak dituzten euskarri informatikoek aukera eman beharko dute jasotzen duten informazio mota identifikatzeko, inbentariatuak izateko eta baimena duten langileek soilik eskura dezaketen sargune batean gordetzeko.

12. Izenpek datu pertsonalei ematen dizkien tratamendu guztiei buruzko informazioa eskuragarri dago www.izenpe.eus/datos helbidean.

2.3 JABETZA INTELEKTUALA

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

2. Erabat debekatuta dago lizentziarik gabeko programa informatikoak erabiltzea.

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

2.4 INFORMAZIO-TRUKEA

1. Inork ere ezin izango du, inola ere, bere nortasuna ezkutatu edo manipulatu.

2. Adierazitako akordioarekin lotutako eginkizunak errazteko helburu bakarraz banatuko da informazioa, dela euskarri digitalean, dela paperezko euskarrian. Izenpek beretzat gordetzen du, identifikatutako arriskuaren arabera, kontrolatu, erregistratu eta ikuskatzeko neurri gehigarriak ezartzeko eskubidea.

3. Informazioa trukatzeari dagokionez, aldeen artean dagoen kontratu-esparruaren barruan, honako jarduera hauek ez dira baimenduta egongo:

    a) Copyright bidez babestutako materiala igorri edo jasotzea Jabetza Intelektualari buruzko Legea urratuz.

    b) Izaera sexualeko mezuak, arrazakeriazko adierazpen baztertzaileak edo iraingarritzat edo legez kontrakotzat har daitekeen beste edozein adierazpen igorri edo jasotzea.

    c) Baimendu gabeko hirugarrenei igortzea erakundearen materiala edo nolabait konfidentziala den materiala barne hartzen duten fitxategiak.

    d) Datu pertsonalak babesteko araudia urratzen duten fitxategiak igorri edo jasotzea.

    e) Negozioarekin loturarik ez duten aplikazioak igorri edo jasotzea.

    f) Interneteko zenbait jardueratan parte hartzea, zerbitzuarekin zuzeneko loturarik ez badute.

    g) Debekatuta dago Izenperen izen onari kalte egin diezaiokeen jarduera oro.

4. Datu pertsonalak Izenperen lokaletatik kanpo tratatuko balira, tratamendu motari dagokion segurtasun-maila bermatu beharko da.

5. Datu pertsonalen tratamenduari buruzko Europako 2016/679 Erregelamenduaren arabera bereziki babestutako datu pertsonal gisa kategorizatutako datu pertsonalak transmititzeko, datu horiek zifratu edo beste edozein mekanismo erabiliko da, informazioa hirugarrenek ulertu edo manipulatu ezingo dutela bermatzeko.

2.5 BALIABIDEEN ERABILERA EGOKIA

1. Hornitzaileak konpromisoa hartzen du zerbitzua egiteko baliabideak erabiltzeko horiek diseinatu eta ezartzeko baldintzen arabera.

2. Izenpek kanpoko langileen esku jartzen dituen baliabideak (informatikoak, datuak, softwarea, sareak, komunikazio-sistemak, etab.) erabili ahal izango dira, soilik, baliabide horiek ematean zehaztutako betebeharrak eta helburuak betetzeko. Izenpek eskubidea du kontrol- eta ikuskapen- mekanismoak ezartzeko, baliabide horiek behar bezala erabiltzen direla egiaztatzearren.

3. Izenperen sare korporatibora fisikoki edo VPN bidez konektatzen diren hornitzailearen ekipo guztiek homologatuta egon beharko dute. Hornitzaileak Izenperen esku jarriko ditu ekipoak, horietan software homologatua instalatu eta horiek egoki konfigura ditzan.

4. Euskarri automatizatuen, Interneten edo posta elektronikoaren bidez edo beste edozein modutara Izenperen sare korporatiboan edo sare horretara konektatutako edozein ekipotan sartutako edozein fitxategik arau hauetan ezarritako eskakizunak bete beharko ditu; bereziki, jabetza intelektualari, datu pertsonalen babesari eta birusen kontrolari buruzkoak.

5. Akordioa amaitzean, Izenpek emandako informazio eta software guztia ezabatu beharko da, justifikatu gabeko atzerapenik gabe.
6. Berariaz debekatuta dago:
    a) Zerbitzuaren xedearekin loturarik ez duten jardueretarako erabiltzea Izenpek emandako baliabideak.
    b) Izenperen sare korporatibora konektatzea (fisikoki edo VPN bidez) Izenperen jabetzakoak diren edo Izenpek ikuskatzen den softwarearen partetzat zehaztuta ez dauden ekipoak eta/edo aplikazioak.
    c) Izenperen sarean nahita sartzea baliabide informatikoetan edozein aldaketa edo kalte eragiten duen edo eragin dezakeen edozein malware (programak, makroak, appletak, ActiveX kontrolak, etab.), gailu logiko, fisiko edo bestelako edozein ordena-sekuentzia. Esleitutakoez bestelako eskubide edo sarbideak berariazko baimenik gabe lortzen saiatzea.
    d) Izenperen informazio-sistemetako eremu mugatuetara berariazko baimenik gabe sartzen saiatzea.
    e) Izenperen informazio-sistemetako “log” erregistroak desitxuratzen edo faltsutzen saiatzea.
    f) Zifratzeko gakoak, sistemak edo algoritmoak eta Izenperen prozesu telematikoetan erabiltzen den beste edozein segurtasun-elementu berariazko baimenik gabe deszifratzen saiatzea.
    g) Beste erabiltzaileen lanean eragin lezaketen programak eduki, garatu edo exekutatzea eta Izenperen baliabide informatikoei kalte egin edo aldatzea.
    h) Izenperen ardurapean diren datu, programa edo dokumentu elektronikoak suntsitzen, aldatzen, baliogabetzen edo beste modu batera haiei kalte egiten saiatzea.

2.6 ERABILTZAILEAREN ERANTZUKIZUNAK

1. Zerbitzuen hornitzaileek bermatu beharko dute Izenperentzat lan egiten duten langileek oinarrizko printzipio hauek beteko dituztela informatika-jardunean:
    a) Izenperen informazioa eskura izan dezakeen oro erabiltzaile-identifikadorean gauzatutako jardueren eta horietatik eratorritako guztiaren erantzule izango da. Beraz, ezinbestekoa da pertsona bakoitzak bere kredentzialak kontrolpean izatea.
    b) Erabiltzaileek ez dute beste erabiltzaile baten identifikadorerik erabiliko, ezta jabearen baimena badute ere.
    c) Eskuen artean duten informazioaren baldintzak nahiz prozedurak ezagutu eta aplikatzen dituzte erabiltzaileek.
2. Izenperen ardurapeko informazioa eskura dezakeen edonork pasahitzak kudeatzeari buruzko jarraibide hauek bete beharko ditu:
    a) Kalitatezko pasahitzak aukeratzea.
    b) Sistema eta pasahitzak arriskuan egotearen zantzurik badago, pasahitza aldatzeko eskatzea.

c) Aldian aldiro pasahitzak aldatzea, eta pasahitza zaharra ez erabiltzea edo ez berreskuratzea.

d) Lehenengo saio hasieran ("login") emandako nahiz aldi baterako pasahitzak aldatzea.

e) Saioa hasteko prozesu automatizatuetan –esaterako, funtzio-tekla edo makro batean bildutakoak– pasahitzik ez jartzea.

f) Pasahitzarekin lotutako edozein segurtasun-gorabehera, dela pasahitza galtzea, hura lapurtu izatea nahiz konfidentzialtasuna galdu dela ustea, haren berri ematea.

3. Izenperen ardurapeko informazioa eskuratzeko baimena duen edozein erabiltzailek zaindu beharko du ekipoak babesturik egongo direla zaintzarik gabe geratzen direnean.

4. Idazmahaia txukun izan behar du, behinik behin, Izenperen ardurapeko informazioa eskura dezakeen edonork. Horrekin lortu nahi da, batetik, paperean diren agiriak nahiz informazioa gordetzeko gailu eramangarriak babestea eta, bestetik, baimenik gabeko sarbidearen eta informazioa galdu edo hondatzearen arriskuak murriztea, lanorduen barruan nahiz lanorduetatik kanpo.

5. Erabiltzen ez direnean, Izenperen erantzukizunpeko informazioa jasotzen duten paperezko dokumentuak eta baliabide informatikoak giltzapean nahiz altzari seguruetan biltegiratzea, batez ere lan-ordutegitik kanpo.

   a) Izenperen eginkizun kritikoetarako ekipoak zaintzarik gabe ez uztea eta horien sarbidea blokeatzea.

   b) Informazioa jasotzeko eta bidaltzeko puntuak babestea (posta, eskaner- eta fax-makinak), baita kopiak egiteko ekipoak ere (fotokopiagailua, faxa eta eskanerra). Erabiltzailearen ardura izango da gailu horien bidez informazioa erreproduzitu edo bidaltzea.

   c) Behin inprimatu ondoren, edozein informazio konfidentzial edo datu pertsonalak dituena kentzea, justifikatu gabeko atzerapenik gabe.

   d) Datu pertsonalak edo informazio konfidentziala barne hartzen dituzten zerrendak leku seguruan gordetzea, langile baimenduak bakarrik sar daitezkeen leku batean.

   e) Datu pertsonalak edo informazio konfidentziala dituzten zerrendak beharrezkoak ez direnean, modu seguruan ezabatu beharko dira.

   f) Sistemetara eta/edo informaziora sar daitezkeen pertsonek ez dute sekula berariazko baimenik gabe egingo ustezko ahulezia edota segurtasun-okerra hautemateko probarik.

   g) Inor ere ez da saiatuko, baimen espliziturik gabe eta edozein bitarteko erabilita ere, segurtasun-sistema eta baimenak hausten. Debekatuta dago erabiltzaileek sareko trafikoak atzitzea, berariaz baimendutako ikuskatze-lanak egiteko ez bada.

   h) Ez da inolako datu pertsonalik gordeko ez erabiltzaileen ekipoetan, ezta informazio-euskarrietan ere, Izenperen berariazko baimenarekin ez bada.

6. Izenperen ardurapeko informaziora eta/edo sistemetara sartzen den langile orok jardunbide-arau hauek bete beharko ditu:

a) Izenperen jabetzako edo hirugarrenek Izenperi lagatako informazio konfidentziala baimendu gabeko jakinarazpen, aldaketa, suntsipen edo erabilera desegokietatik –ustekabekoak izan ala ez– babestea.

b) Informazio-sistemetarako sarbidea lortzeko eta/edo informazioa eskuratzeko beharrezkoa den baimena edukitzea.

c) Arau hauek ezagutzea, onartzea eta betetzea Izenperen informazioa eskuratu eta/edo haren sistemetan sartu aurretik.

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

2.7 ERABILTZAILEEN EKIPOAK

1. Zerbitzuen hornitzaileek bermatu beharko dute Izenperen ardurapeko informaziora jotzeko baliatzen dituzten erabiltzaileen ekipo informatiko guztiek honako politika hauek beteko dituztela:

   a) Denbora luzez postu bat zaintzarik gabe uzten bada, sistemak blokeoa aktibatu beharko du.

   b) Erakundearen sistemen barruan, erabiltzaileen ekipoetan ez da izango segurtasun-sistema eta baimenak urra ditzakeen tresnarik.

   c) Fabrikatzailearen argibideen arabera zainduko dira erabiltzaileen ekipoak.

   d) Malwarearen kontra egoki babesturik daude erabiltzaile-ekipo guztiak.

   e) Birusen definizio- fitxategiak automatikoki eguneratuko dira.

   f) Segurtasuna eguneratzeko politika bat ezarriko da, eguneratzeak hilean behin gutxienez kontsultatu eta instalatzea eskatu beharko duena.

2. Zainduko da, bereziki, Izenperen ardurapeko informazioa dakarten edota nola edo hala informazio hori eskuratzeko bidea ematen duten ekipo eramangarri guztien segurtasuna:

   a) Behar-beharrezkoa den informazioa baino ekarriko ez dutela egiaztatuko da.

   b) Informazio horretarako sarbide-kontrolak aplikatzen direla bermatuko da.

   c) Izenperi hornitutako zerbitzutik kanpoko pertsonen aurrean informazioa horretarako sarbideak ahalik eta gehien murriztuko dira.

   d) Kolpeen aurrean babesteko, zorro, maleta txiki edo antzeko ekipamendu egokietan eramango dira ekipoak.

   e) Hornitzailearen egoitzetatik kanpo, babes-neurri bereziak hartu behar dira, hirugarrenek nahigabean ikus ez dezaten informazioa.

3. SEGURTASUN-POLITIKA ESPEZIFIKOAK

3.1 HORNITZAILEENTZAKO SEGURTASUN-POLITIKA ESPEZIFIKOEN APLIKAGARRITASUNA

Hornitzaileentzako segurtasun-politika orokorrez gain, hornitzaile guztiek bete beharko dituzte, baita ere, kasuak kasu dagozkien atal honetan jasotako segurtasun-politik espezifikoak, informazio-sistemetarako sarbide-maila eta egiten duten zerbitzuaren ezaugarriak kontuan izanda.

- **Sistemetarako sarbiderik gabe:** Egin beharreko zerbitzuak ez du eskatzen Izenperen informazio-sistemak erabiltzea, eta, hortaz, zerbitzua egiten duten langileek ez dute erabiltzaile-konturik sistema horietan.
- **Identifikazio-postua (inprimakien aplikazioa edo baliokidea):** Egin beharreko zerbitzua identifikazio-bitartekoen eskatzaileak identifikatzean eta erregistratzean datza (adibidez, herritarraren ziurtagiria, BAKQ, etab.). Zerbitzua egiten duten langileek erregistro-aplikazioetara sartzeko aukera ematen dieten erabiltzaile-kontuak dituzte. Izenperen aplikazioen urrutiko operadorearen kasu berezia da.
- **IZENPEren aplikazioen urrutiko operadorea (adibidez, artxiboa, administrazioa, etab.):** Egin beharreko zerbitzuak Izenperen informazio-sistemak erabili behar dituenez, zerbitzua egiten duten langileek erabiltzaile-kontuak dituzte, Izenperen aplikazioetara urrutitik sartzeko (ez da sare korporatibora sartzeko beharrik).
- **Erabiltzaile-mailaz sare korporatiborako sarbidea izanda:** Egin beharreko zerbitzuak sare korporatiboaren bitartez (fisikoki edo VPN bidez) erabiltzaile-pribilegioak dituen Izenperen informazio-sistemetako batera sartzea eskatzen du.
- **Maila pribilegiatuaz sare korporatiborako sarbidea izanda (adibidez, gordetegiak):** Egin beharreko zerbitzuak eskatzen du Izenperen informazio-sistemetara modu pribilegiatuan sartzea, sistema horiek eta/edo prozesatzen diren ekoizpen-datuak administratzeko gaitasunaz.

Zerbitzu bakoitza zein kategoriatan sartutako dagoen, segurtasun-politika orokorrak betetzeaz gain, hornitzaileak honako taula honetan adierazitako ataletako politika espezifikoak bete beharko ditu:

	Sistemetarako sarbiderik gabe	**Identifikazio-postua**	**Aplikazioen urrutiko operadorea**	**Erabiltzaile-maila duen sare korporatiborako sarbidea**	**Sare korporatiborako sarbidea maila pribilegiatuaz**
Langile-hautaketa	BAI	BAI	BAI	BAI	BAI
Segurtasun-ikuskapena	BAI	BAI	BAI	BAI	BAI
Gorabeherak jakinaraztea	BAI	BAI	BAI	BAI	BAI
Segurtasun fisikoa	EZ	EZ	BAI	BAI	BAI (1)
Aktiboen kudeaketa	EZ	EZ	EZ	BAI	BAI
Segurtasun-arkitektura	EZ	EZ	EZ	EZ	BAI (1)
Sistemen segurtasuna	EZ	EZ	BAI	BAI	BAI

Sare-segurtasuna	EZ	EZ	EZ	BAI	BAI
Sistemen erabilera-trazabilitatea	EZ	EZ	EZ	EZ	BAI (1)
Identitateen eta sarbideen kontrola eta kudeaketa	EZ	EZ	EZ	EZ	BAI (1)
Aldaketen kudeaketa	EZ	EZ	EZ	EZ	BAI (1)
Segurtasuna garapenean	EZ	EZ	*EZ*	BAI (2)	BAI (2)
Gorabeheren kudeaketa	EZ	EZ	EZ	EZ	BAI (3)

(1) Zerbitzua bere IKT azpiegituraren bidez gordetzen edo egiten bada bakarrik
(2) Garapen-atazak badaude bakarrik
(3) Izenperen Negozioaren Jarraitutasun Planean kritikotzat jotzen diren zerbitzuak eskaintzen badira bakarrik.

3.2 LANGILE-HAUTAKETA

Izenperen informazio-sistemetara sartu nahi duten Izenperen hornitzaileek langileak hautatzeko politika hauek bete beharko dituzte:

1. Langileen lanbide-aurrekariak egiaztatu beharko dituzte. Zehazki, Izenperi bermatu beharko diote langileek iraganean ez duela zigorrik jaso lanbidean jokabide okerra izateagatik, landutako informazioaren konfidentzialtasunari lotutako gorabeheren artean izan ez daudela, eta arrazoi horregatik zigorrik jaso ez dutela.
2. Izenperi bermatuko diote zerbitzuari atxikitako langileei berehala baja emateko aukera.

3.3 SEGURTASUN-IKUSKAPENA

Izenperen informazio-sistemetara sartu nahi duten Izenperen hornitzaile guztiek segurtasuneko ikuskapen-politika hauek bete beharko dituzte:

1. Zerbitzuaren segurtasuna urtean gutxienez behin ikuskatzen utzi behar dio hornitzaileak Izenperi. Horrela, ikuskapen-taldeari laguntza eskainiko dio hornitzaileak, eta eskatutako proba nahiz erregistro guztiak eman beharko ditu.
2. Izenpek berariaz ezarriko du ikuskapen bakoitzaren irismena eta sakontasuna. Zerbitzuaren hornitzailearekin kasuak kasu adostutako plangintzari jarraituz egingo dira ikuskapenak.
3. Horrez gain, ohiz kanpoko ikuskapenak egiteko eskubidea izango du Izenpek, betiere, hori egiteko berariazko arrazoirik badago.

3.4 GORABEHERAK JAKINARAZTEA

Izenperen informazio-sistemetan sartzen diren zerbitzu-hornitzaile guztiek (bai pribilegiatuek, bai pribilegiatu ez direnek) gorabeherak jakinarazteko politika hauek bete beharko dituzte:

1. Zerbitzuari atxikitako langile guztiek harremanetan jarri beharko dute Izenpeko erabiltzailearen arreta-zentroarekin (EAZ), Izenperen informazioarekin edo baliabideekin zerikusia duen edozein gorabehera hautemanez gero.
2. Edozein erabiltzailek informazioaren segurtasunarekin eta politika hauetan jasotako jarraibideekin zerikusia duten iradokizun, ahulezia, hauskortasun eta/edo arrisku-egoeraren berri eman ahal izango dio Izenpeko segurtasun-arduradunari.

3. Izenperen EAZi jakinarazi beharko zaio hautematen den eta datu pertsonalen segurtasunari eragiten dion edo eragin diezaiokeen edozein gorabehera.
4. EAZera sarbiderik ez badago, zerbitzuaren barruan ezarritako komunikabideak erabili beharko dira, Izenperen solaskidea izan dadin EAZekin harremanetan jarriko dena.

3.5 SEGURTASUN FISIKOA

Hornitzaileek bere egoitzatik egiten duten zerbitzu orotan segurtasunari buruzko politika hauek, gutxienik, betetzen direla bermatu beharko dute:

1. Egoitzak areto itxia behar du izan beharko du eta kontrol-sistemaren bat eduki beharko du sarbideetan, lapurretaren, suntsitzearen edo zerbitzua etetearen aurreko prebentzioa bermatzeko.
2. Bisitak kontrolatuko dira, gutxienez, edonor sar daitekeen eremuetan eta/edo zamalanetarako guneetan.
3. Gutxienik, suteak hautemateko sistemak izan beharko ditu egoitzak, eta uholdeei eusteko moduan eraikita egongo da.
4. Izenperen ardurapeko informazioaren kopiaren bat edukiz gero, honako segurtasun-neurri hauek, gutxienik, izango dituen bereziki babestutako eremu batean egon beharko dute informazio hori gordetzen eta/edo prozesatzen duten sistemek:
    a) Sarbideak kontrolatzeko sistema eta egoitzarenaz bestelakoa izan beharko du bereziki babestutako eremuak.
    b) Kanpoko langileek sarbide mugatua izango dute babes bereziko eremuetara. Soilik beharrezkoa denean eta horretarako baimena dutenean sartuko dira, betiere, baimendutako langileen zaintzapean.
    c) Kanpoko pertsonen sarbide guztien erregistro bat egongo da.
    d) Kanpoko langileek ezingo dute, ikuskapenik gabe, bereziki babestutako guneetan egon edo lanik egin.
    e) Debekaturik dago bereziki babestutako gune horietan jatea edo edatea.
    f) Elikatze-hutsegiteen aurrean babesturik egoteko neurriren bat izan behar dute gune horietan kokatutako sistemek.

3.6 AKTIBOEN KUDEAKETA

Euren IKT azpiegitura propioak erabilita egindako zerbitzuen hornitzaile guztiek, aktiboak kudeatzeko garaian, honako arau hauek betetzen direla bermatu beharko dute:

1. Aktiboen erregistro eguneratua izatea. Erregistro horretan, zerbitzua egiteko erabilitako aktibo guztiak identifikatu ahal izan behar dira.
2. Zerbitzua egiteko 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 aipatutako aktibo horiek.

3. Izenperen ardurapeko informazioa gorde duen aktibo bati baja eman nahi izanez gero, aipatutako informazioa modu seguruan ezabatu beharko du hornitzaileak. Horretarako, datuak ziurtasunez ezabatzeko funtzioak aplikatu behar ditu edo, bestela ere, aktiboa fisikoki suntsitu, hartan gordetako informazioa berreskuratzeko modurik ez egoteko.

3.7 SEGURTASUN-ARKITEKTURA

Izenperen informazio-sistemetara sartzen diren eta zerbitzua beren IKT azpiegituraren bidez egiten duten zerbitzu-hornitzaile guztiek bermatu beharko dute segurtasun-arkitekturako eskakizun hauek, gutxienez, betetzen direla:

1. Izenperen ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistema guztietarako sarbideek babesturik egon behar dute, gutxienez, sistema horietara konektatzeko gaitasuna mugatuko duen suebaki baten bidez.
2. Izenperen ardurapeko informazio berezia gordetzen edo prozesatzen duten informazio-sistemek gainerako beste sistema guztietatik isolaturik egon behar dute.
3. Izenperi zerbitzua egiten dieten informazio-sistemek erabilgarritasun-baldintzak betetzeko behar besteko erredundantzia izan behar dute.
4. Elkarren artean nahiz ordu ofizialarekin sinkronizaturik egongo dira hornitzailearen sistemetatik Izenperen ardurapeko informazioa prozesatzen edo gordetzen duten horien erlojuak.

3.8 SISTEMEN SEGURTASUNA

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

1. Bere funtzionamenduari buruzko jazoerarik nabarmenenak jaso beharko dituzte Izenperen ardurapeko informazioa gordetzen edota tratatzen duten informazio-sistemek. Erakundearen backup-politikaren barruan izango dira jarduera-erregistro horiek.
2. Izenperen 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.
3. Software gaiztoaren kontra egoki babesturik egongo dira Izenperen ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistemak. Horretarako, honako neurri hauek hartuko dira aldez aurretik:
    a) Proba, garapen eta ekoizpeneko inguruneetan, sistemak eguneratuta eduki beharko dira eskura dauden azken segurtasun-eguneratzeekin.
    b) Birusen kontrako softwarea zerbitzari eta ordenagailu guztietan instalatu eta erabili beharko da, birusek edo bestelako software kaltegarriek eragin ditzaketen arriskuak murrizteko.
    c) Birusen kontrako softwareak aktibatuta egon beharko du beti. Birusa definitzeko fitxategien eguneratze automatikoa ezarri beharko da hala ordenagailu pertsonaletan, nola zerbitzarietan, baita birus informatikoak detektatzean ordenagailua blokeatzeko sistemak ere.

4. Egindako zerbitzuarentzat garrantzi handia duen datu edo informazio oro babesteko asmoz, segurtasun-kopiak egiteko politika ezarriko du hornitzaileak. Kopia horiek, gehienez ere, hilabetean behin egingo dira.

5. Zerbitzua egitean posta elektronikoa erabiltzen bada, hornitzaileak honako baldintza hauek bete beharko ditu:

    a) Ez da onartuko posta elektronikoaren bidez Izenperen informazio konfidentziala bidaltzea, salbu eta komunikazio elektronikoa zifratuta badago eta bidalketa berariaz onartu bada.

    b) Ez da onartuko posta elektroniko bidez goi-mailako datu pertsonalak dituen informazioa bidaltzea, salbu eta komunikazio elektronikoa zifratuta badago eta bidalketa berariaz onartu bada.

6. Zerbitzua egitean Izenperen posta elektronikoa erabiliz gero, printzipio hauek errespetatu beharko dira gutxienez:

    a) Posta elektronikoa esku jartzen den beste edozein lan-tresnatzat jotzen da; beraz, kontratatutako zerbitzua egiteko soilik erabili beharko da. Hala, Izenpek kontrol-sistemak ezarri ahal izango ditu baliabide hori babestu eta behar bezala erabiltzen dela ziurtatzeko. Dena den, pertsonen duintasuna eta intimitaterako eskubidea zainduz baliatuko da ahalmen hori.

    b) Izenperen posta elektronikoko sistema ezingo da erabili iruzurrezko mezuak, mezu lizunak, mehatxagarriak eta antzekoak bidaltzeko.

    c) Erabiltzaileek ezingo dituzte publizitate-mezuak edo mezu piramidalak (erabiltzaile askori heltzen zaizkienak) sortu, bidali edo birbidali.

7. Izenperen 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 betebehar hori.

8. Izenperen 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 aipatutako informazioa eskuratzen.

9. Erabiltzaileek denbora batez jardunari uztean automatikoki blokeatu beharko dira Izenperen ardurapeko informazioa gordetzen edo prozesatzen duten informazio-sistemetarako sarrera-saioak.

10. Izenpek emandako softwarea erabiltzen den guztietan, arau hauek bete beharko dira:

    a) Emandako software-bertsioak bakarrik erabili beharko dituzte Izenperen informazio-sistemetara sarbidea duten langileek, eta horien erabilera-arauak bete.

    b) Langile guztiek debekatua dute edozein programaren legez kontrako kopiarik egitea, programa estandarizatuenak barne.

c) Debekatuta dago Izenpek instalatutako edozein programa desinstalatzea.

3.9 SARE-SEGURTASUNA

Izenperen ardurapeko informazioari dagokionez, sare-segurtasunaren honako arau hauek betetzen dituztela bermatu beharko dute beren IKT azpiegiturak erabiltzen dituzten hornitzaile guztiek:

1. Egoki kudeatu eta kontrolatu behar dira Izenperen ardurapeko informazioa dakarten sareak. Horretarako, kontrolez kanpoko sarbiderik ez dagoela eta hornitzaileak konexioen arriskuak egoki kudeatzen dituela bermatuko da.
2. Ahalik eta gehien mugatu behar dira informazioa dakarten sareetako zerbitzuak.
3. Izenperen IKT azpiegiturara sartzeko bidea ematen duten sareek egoki babesturik egon behar dute. Horretarako, honako baldintza hauek bete beharko dituzte:
    a) Urruneko erabiltzaileek Izenperen sarera sarbidea izateko, sarbidea baliozkotzeko eta aurretiazko autentifikazio-prozedurak bete beharko dira.
    b) Denbora mugatu batez egingo dira konexio horiek, sare pribatu birtualen edo ardura bakarreko lineen bidez.
    c) Kontroletik kanpoko aukerako beste konexio batzuk egiteko bide ematen dutenetik, ezin izango da komunikazio-ekiporik erabili konexio horietan (hots, hub-ak, switch-ak, etab.).
4. Informazioa dakarten sareetarako sarbidea mugaturik egongo da.
5. Informazioa dakarten sareetara konektatutako ekipo guztiak behar bezala identifikaturik egon behar dira, halako moduz non sare-trafikoa identifika daitekeen.
6. Telelana, alegia kanpotik lana egitea sare korporatiborako sarbidea izanik, politika hauen bidez arautuko da:
    a) Telelana baimentzeko irizpideak ezarriko dira, lanpostuaren beharren arabera.
    b) Sare korporatibora modu seguruan konektatzeko bete beharreko neurriak ezarriko dira.
    c) Ezarritako konexioen segurtasuna monitorizatu eta ikuskatzeko sistemak ezarriko dira.
    d) Jarduerari dagokion epealdia amaitzean, sarbide-eskubideak ezeztatu direla eta ekipamendua itzulia izan dela kontrolatuko da.

3.10 SISTEMEN ERABILERA-TRAZABILITATEA

Izenperen informazio-sistemetarako sarbidea eskatzen duten zerbitzu-hornitzaile guztiek, zerbitzuak hornitzailearen IKT azpiegitura erabiliz egiten badira, sistemen erabilera-trazabilitateko politika hauek, gutxienez, betetzen direla bermatu beharko dute:

1. Sarrera pribilegiatuak erregistratuko dira. Erregistro horiek, bidenabar, erakundearen segurtasun-kopiei buruzko politikan xedatutakoaren arabera gordeko dira.

2. Sarbide pribilegiatuak egiteko erabili izan den sistemaren jarduera erregistratuko da. Erregistro hori, bidenabar, erakundearen segurtasun-kopiei buruzko politikan xedatutakoaren arabera gordeko da.
3. Aztertu egingo dira sistemen jardueran erregistratutako akatsak eta okerrak, eta horiek konpontzeko beharrezkoak diren neurriak ezarriko dira.

3.11 IDENTITATEEN ETA SARBIDEEN KONTROLA ETA KUDEAKETA

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

1. Informazio-sistema batera sarbidea duten erabiltzaile guztiek pertsona bakarreko sarbide-baimen bat izango dute.
2. Erabiltzaileena da beren sarbide baimendua erabiliz egiten dituzten jarduera guztien ardura.
3. Erabiltzaileek ez dute beste erabiltzaile baten sarbide baimendurik erabiliko, ezta jabearen baimena badute ere.
4. Erabiltzaileak ez dio, inola ere, bere identifikadorea eta/edo pasahitza inori jakinaraziko, eta ezta begi-bistan idatzita edo hirugarrenen eskura edukiko ere.
5. Pasahitzen segurtasun-politika bat egon beharko da.
6. Izenperen ardurapeko informaziora horretarako baimen egokia duten langileak ez beste inor ez direla sartzen aldian aldiro egiaztatzen dela bermatu behar du hornitzaileak.
7. Horrez gain, Izenperen informazio-sistemetara sartzearen kasuetan, honako arau gehigarri hauek hartu beharko dira kontuan, era berean:
    a) Erabiltzaileek sarbide baimendua izango dute, soilik, beren eginkizunak betetzeko behar dituzten datu eta baliabideetarako.
    b) Sistemak automatikoki eskatzen ez badu, erabiltzaileak aldatu beharko du sistemara sarbide baliozkoa egiten den lehenengo aldian esleitutako aldi baterako pasahitza.
    c) 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 EAZekin harremanetan jarri beharko du pasahitz berria eskuratzeko.
    d) Aldi baterako sarbide baimenduak denbora tarte labur baterako konfiguratuko dira. Epe hori amaitzean, sistemetatik desaktibatuko dira.
    e) Datu pertsonalei dagokienez, berariaz baimendutako langileek bakarrik eman, aldatu edo ezeztatu ahal izango dute datu eta baliabideen gaineko sarbide baimendua, betiere fitxategiaren arduradunak ezarritako irizpideen arabera.
    f) Erabiltzaile batek susmatzen badu beste pertsona bat bere sarbide baimendua (erabiltzailearen identifikadorea eta pasahitza) erabiltzen ari dela, pasahitza aldatu beharko du, eta EAZekin harremanetan jarri beharko du gorabeheraren berri emateko.

3.12 ALDAKETEN KUDEAKETA

Izenperen informazio-sistemetara sartzea dakarten zerbitzuen hornitzaile guztiek bermatu beharko dute aldaketak kudeatzeko arau hauek, gutxienik, betetzen dituztela:

1. Egiten diren aldaketa guztietarako, formalki ezarri eta dokumentatutako prozedura bati jarraitu beharko zaio. Horrek bermatu beharko du aldaketa egiteko urrats egokiak ematen direla.
2. Aldaketak kudeatzeko prozedurak bermatu beharko du osagai kritikoen gaineko aldaketak minimizatzen direla; hau da, behar-beharrezkoak soilik izango direla.
3. Osagai kritikoen gaineko aldaketa guztiak egiaztatuko dira, osagai horien funtzionamenduaren edo segurtasunaren gainean zeharkako eragin kaltegarriak edo aurreikusi gabekoak sortzen ez direla ziurtatzeko.
4. Hornitzaileek analizatu egin beharko dituzte zerbitzua egiteko erabilitako azpiegiturek dituzten kalteberatasun teknikoak, eta Izenperi osagai kritikoekin lotutako guztien berri emango diote, kalteberatasun horiek batera kudeatzeko helburuarekin.

3.13 SEGURTASUNA GARAPENEAN

Aplikazioak garatzen dituzten hornitzaile guztiek Izenperen informazio-sistemetara sarbidea izan behar dute zerbitzua egiteko orduan. Hornitzaileek, beraz, jarduera horretan honako segurtasun-arau hauek, gutxienez, betetzen direla bermatu behar dute:

1. Izenpek kontrolatu eta ikuskatuko du softwarea erakundetik kanpo garatzeko prozesu osoa. Prozesua formal horrek jarraitu beharreko arauak ezarriko ditu.
2. Aplikazioak diseinatzeko, garatzeko eta inplementatzeko prozesuan, eta eragiketa orotan, identifikazioko, autentifikatzeko, sarbide-kontroleko, ikuskapeneko eta segurtasuneko mekanismoak baliatu dira.
3. Kasuan kasu, bete beharreko segurtasun-baldintza guztiak berariaz zehaztuko dira aplikazioen zehazpenetan.
4. Sarrera-datuak baliozkotu beharko dira garatzen diren aplikazio berrietan. Horrela, sarrera datuak egokiak nahiz zuzenak direla egiaztatuko da, eta kode exekutagarriak sar daitezela saihestu.
5. Aplikazioek garatutako barne-prozesuen artean izango da, baita ere, informazioa galbideratuko ez dela bermatzeko beharrezkoak diren baliozkotze guztiak.
6. Beharrezkoa den guztietan, egiaztapenak eta integritate-kontrolak egiteko funtzioak ezarri behar dira aplikazioen hainbat osagairen arteko komunikazioetan.
7. Aplikazioek emandako irteera-informazioa mugatu beharko da, informazio egokia eta beharrezkoa besterik ematen ez dela bermatzeko.
8. Zerbitzuan aritzen diren langileak izango dira aplikazioen iturri-kodera sar daitezkeen bakarrak.
9. Garapen eta probako faseetan, segurtasun-funtzionalitateei buruzko proba espezifikoak egingo dira.

10. Proba- eta garapen-inguruneetan datu errealak erabiliko dira soilik, baldin eta egoki disoziatu badira, edota ekoizpen-ingurunearen moduko segurtasun-neurriak aplikatu direla berma badaiteke.
11. Aplikazioen probak egitean, informazioak kontrolik gabe ihes egiten ez duela egiaztatuko da. Egiaztatuko da, baita ere, aurreikusitako informazioa baino ematen ez dela ezarritako kanaletatik.
12. Kodearen garapenaren gaineko trazabilitatea ahalbidetuko duten bertsioak kontrolatzeko sistema bat ezarriko da.
13. Garapenak gauzatzen diren inguruneek beren artean isolatuta egon beharko dute, baita informazioa gordetzen edo prozesatzen den ekoizpen-inguruneetatik isolatuta ere.

3.14 GORABEHEREN KUDEAKETA

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

1. Gorabeherak egonda ere, berori egiten jarraitzeko plana izan behar du zerbitzuak.
2. Zerbitzua eten dezaketen jazoeren eta horiek gertatzeko probabilitatearen arabera garatu da aurreko plana.
3. Gorabeheretarako egungo plana bideragarria dela froga dezake hornitzaileak.

4. JARRAIPENA ETA KONTROLA

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

a) Inork aplikazioak eta/edo datuak edo beste edozein baliabide informatiko oker erabiltzen dituela antzemanez gero, horren berri emango zaio erakunde hornitzaileari, eta, hala badagokio, baliabideak behar bezala erabiltzeko prestakuntza eskainiko zaio.

b) Aplikazioak, datuak edo beste edozein baliabide informatiko oker erabiltzean fede txarra antzemanez gero, Izenpek dagozkion legezko egintzak baliatuko ditu bere eskubideak babesteko.

5. SEGURTASUN-POLITIKAK EGUNERATZEA

Teknologiaren, segurtasunen inguruko mehatxuen eta arlo horretan sortzen ari diren legezko ekarpen berrien bilakaera dela-eta, Izenpek eskubidea du, behar denean, politika hori aldatzeko.

Politika horietan egindako aldaketak erakunde hornitzaile guztiei jakinaraziko zaizkie, egoki jotzen den eran. Erakunde hornitzaile bakoitzaren erantzukizuna da Izenpek segurtasunaren alorreko politiketan egindako berrikuntzak langileek irakurri eta ezagutzen dituztela bermatzea.