HORNITZAILEENTZAKO SEGURTASUN POLITIKA

Erreferentzia: IZENPE – Hornitzaileentzako segurtasun-politika
Bertsio-zk.: v 1.00
Data: 2016ko azaroaren 10a

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

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

Bertsioen historikoa:

BERTSIOA	DATA	ALDAKETEN HISTORIKOA
1.0	2016/11/10	Hasierako bertsioa

Aurkibidea

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 enpresei aplikatzeko.

Helburua da informazioa galdu edo behar ez bezala erabiltzeko arriskua saihestea, horrek Sozietatearen ospeari kalterik ez egiteko. Horretarako, politika honek deskribatzen du Izenpek zer espero duen erakunde horretan diharduten baina beste enpresa hornitzaile batzuetakoak diren langileengandik, langile horiek euren zereginen jardunean Sozietatearen informaziorako, informazio-sistemetarako edo baliabideetarako sarbidea eduki badezakete.

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

Horretarako, enpresa 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 aplikatzekoa izango da Izenperentzat zerbitzuak egiten dituzten baina beste enpresa hornitzaile batzuetakoak (dagokion kontratu-esparruaren bidez lotetsitakoak) diren langileek egiten dituzten jarduera guztietarako.

- *2. HORNITZAILEENTZAKO SEGURTASUN POLITIKA OROKORRAK* atala aplikatzekoa izango da edozein hornitzailerentzat, egiten duen zerbitzua edozein dela ere.
- Politika honen *3. HORNITZAILEENTZAKO BERARIAZKO SEGURTASUN POLITIKAK* 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. HORNITZAILEENTZAKO SEGURTASUN POLITIKA OROKORRA

2.1 IZENPERENTZAKO ZERBITZUGINTZA

1. Enpresa hornitzaileetako langileen jarduerak egingo dira dagokion kontratu arautzailean ezarritakoaren arabera, baita Izenperen eta hornitzailearen artean horretarako finkatutako arau eta prozeduren arabera ere.

2. Enpresa hornitzaileak, aldian-aldian, 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. Kontratuan 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 enpresari dagokionez. Neurri horiek berekin ekar dezakete indarrean dauden kontratuak deuseztatzea.

4. Enpresa 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 enpresa 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 kontratuari dagozkionak ez diren xedeetarako ere.

6. *Informazioaren Segurtasun Arloak* 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. 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. Kanpoko langileek Izenpek eskura jarritako tresna ofimatikoak erabiliko ditu soilik, eta 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, enpresa 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 enpresarekin 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.

Datu pertsonalen segurtasuna bermatzeko, enpresa hornitzaileetako langileek, gainera, jardunbide-arau hauek bete beharko dituzte:

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.

2.3 JABETZA INTELEKTUALA

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

2. Beren eginkizunak betetzeko baino ezin izango dute Izenpek baimendutako materiala erabili kanpoko langileek.

3. Erabat debekatuta dago Izenpeko informazio-sistemetan lizentziarik gabeko programa informatikoak erabiltzea.

4. 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 kontratuarekin 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) Mota orotako material pornografikoa, sexuarekin lotutako mezuak, arrazakeriazko adierazpen baztertzaileak edo iraingarri 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 edo Izenperen jarraibideak urratzen dituzten 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 fitxategia Izenperen lokaletatik kanpo tratatu behar badira, erakundeak horretarako berariazko baimena eman beharko du, eta, kasu guztietan, tratatutako fitxategi motari dagokion segurtasun maila bermatu beharko da.
5. 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.

2.5 BALIABIDEEN ERABILERA EGOKIA

1. Hornitzaileak konpromisoa hartzen du Izenperi zerbitzua egiteko baliatzen dituen aktiboen berri aldizka emateko.
2. Hornitzaileak konpromisoa hartzen du zerbitzua egiteko baliabideak erabiltzeko horiek diseinatu eta ezartzeko baldintzen arabera.

3. 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.
4. Homologatutako ekipoak konektatu beharko ditu hornitzaileak Izenperen sarera. Hornitzaileak Izenperen esku jarriko ditu ekipoak, horietan software homologatua instalatu eta horiek egoki konfigura ditzan.
5. Euskarri automatizatuen, Interneten edo posta elektronikoaren bidez edo beste edozein modutara Izenperen sarean edo sare horretara konektatutako edozein ekipotan sartutako edozein fitxategik arau hauetan ezarritako betekizunak bete beharko ditu; bereziki, jabetza intelektualari, datu pertsonalen babesari eta birusen kontrolari buruzkoak.
6. Kontratua bukatu ondoren, aktibo fisiko guztiak Izenperi itzuli beharko zaizkio, eta informazio-aktibo guztiak suntsitu edo Izenperi itzuli, justifikaziorik ez duen atzerapenik gabe. Zerbitzua amaitu ondoren, softwarerik instalatu den ordenagailu guztiak formateatuko ditu Izenpek.
7. Berariaz debekatuta dago:
    a) Zerbitzuaren xedearekin loturarik ez duten jardueretarako erabiltzea Izenpek emandako baliabideak.
    b) Izenperen ekoizpen-sarera konektatzea Izenperen jabetzakoak diren edo Izenpek ikuskatzen dituen software edo baliabide informatikoen estandar gisa identifikatuta ez dauden ekipoak eta/edo aplikazioak.
    c) Izenperen informazio-sistemetan edo sarean eduki lizunak, mehatxagarriak, moralgabeak edo iraingarriak sartzea.
    d) 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.
    e) Izenperen informazio-sistemetako eremu mugatuetara berariazko baimenik gabe sartzen saiatzea.
    f) Izenperen informazio-sistemetako “log” erregistroak desitxuratzen edo faltsutzen saiatzea.
    g) Zifratzeko gakoak, sistemak edo algoritmoak eta Izenperen prozesu telematikoetan erabiltzen den beste edozein segurtasun-elementu berariazko baimenik gabe deszifratzen saiatzea.
    h) Beste erabiltzaileen lanean eragin lezaketen programak eduki, garatu edo exekutatzea eta Izenperen baliabide informatikoei kalte egin edo aldatzea.
    i) 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. 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. Gainera, gako hori ez zaie gainerako langileei jakinaraziko inola ere.

    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 eskura dezakeen edonork 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. Hala, arau hauek bete beharko ditu:

5. Erabiltzen ez direnean, 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 kentzea, justifikatutako atzerapenik gabe ez bada.

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) Informazioaren segurtasunarekin lotura izan dezaketen gorabehera edota okerren bat gertatuz gero, 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.

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-sistema eta telekomunikazio-sare guztiak babestea baimendu gabeko sarbide edo erabilera, operazio-eten, suntsipen, erabilera oker edo lapurretetatik.

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

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

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 laburraz 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:

- Birusen kontrako softwarea ordenagailu pertsonal guztietan instalatu eta erabili beharko da, birusek edo bestelako software kaltegarriek eragin ditzaketen arriskuak murrizteko.
- Eskuragarri dauden azken segurtasun-eguneraketak egingo dira. Birusen kontrako softwareak aktibatuta egon beharko du beti. Birusen definizio-fitxategiak automatikoki eguneratuko dira.

2. Zainduko da, bereziki, Izenperen ardurapeko informazioa dakarten edota nola edo hala informazio hori eskuratzeko bidea ematen duten erabiltzaileen ekipo mugikor 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) Izenperen egoitzetatik kanpo, babes-neurri bereziak hartu behar dira, hirugarrenek nahigabean ikus ez dezaten informazioa.

2.8 "HARDWARE" EKIPAMENDUAREN KUDEAKETA

Zerbitzuen hornitzaileek ziurtatu beharko dute edozein eratako zerbitzuak egiteko asmoz Izenpek emandako ekipo guztiak egoki kudeatuko direla. Horretarako, honako arau hauek bete beharko dituzte:

1) Hornitzaileak egunean izan beharko du aktibo horien ekipoen eta erabiltzaileen zerrenda bat edota, pertsona batek baino gehiagok erabiliz gero, aktibo horien arduradunena ere.

   Izenpek edozein unetan eskatu ahal izango du zerrenda hori.

2) Hornitzaileak berriz erabili nahi baldin badu Izenperen ardurapeko informazioa zekarren Izenperen ekiporen bat, aktibo hori denbora batez bueltan eman beharko dio Izenperi, ekipoa berriz erabili aurretik erakundeak datuak segurtasunez ezabatu ahal izan ditzan.

3) Hornitzaileren batek Izenpek emandako ekipoetako bat zerrendatik kendu nahi badu, aktibo hori Izenperi bueltan eman beharko dio, baja hori egoki tratatu ahal izan dadin.

4) Hornitzaileren batek zerbitzua egiteari uzten badio, hari emandako ekipo guztiak bueltan eman beharko ditu, zerbitzugintzako kontratuetan xedatzen denez. Informazio-aktiboetako informazioa baino ezin izango du segurtasunez ezabatu hornitzaileak. Horrelakoetan, jakinaren gainean jarri beharko du hornitzaileak Izenpe.

3. HORNITZAILEENTZAKO BERARIAZKO SEGURTASUN POLITIKAK

3.1 HORNITZAILEENTZAKO BERARIAZKO SEGURTASUN POLITIKEN APLIKAGARRITASUNA

Hornitzaileentzako segurtasun-politika orokorrez gain, hornitzaile guztiek bete beharko dituzte, baita ere, kasuak kasu dagozkien atal honetan jasotako berariazko segurtasun-politikak, egiten duten zerbitzuaren ezaugarriak kontuan izanda.

Jarraian adierazten dira aurreikusitako zerbitzu tipologiak.

a) Zerbitzua gauzatzeko lekua

Zerbitzuak egiten diren leku nagusiaren arabera, bi kasu hauek bereizten dira:

- Izenpe: Hornitzaileak, batez ere, Izenperen egoitzetan egiten du zerbitzua.
- Urrunetik: Hornitzaileak bere egoitzatik, batez ere, egiten du zerbitzua. Hala ere, Izenperen egoitzetan gauzatu dezake hornitzaileak jarduera bat edo beste.

b) Izenperen sistemetarako **sarbide-maila**

Informazio-sistemetarako sarbide-mailaren arabera, bi kasu hauek bereizten dira:

- Erabiltzaile-mailako sarbidearekin: Izenperen informazio-sistemak erabili behar direnean zerbitzua egiteko. Horrelakoetan, erabiltzaile-kontuak izango dituzte zerbitzua egiten duten langileek. Kontu horien bitartez, bidenabar, sistema horietako batzuetara sartzeko aukera izango dute langileek, ohiko abantailekin.
- Sarbide pribilegiatuarekin: Izenperen informazio-sistemetara modu pribilegiatuan sartzeko gaitasuna behar denean zerbitzua egiteko. Hau da, sistema horiek eta/edo prozesatutako ekoizpen-datuak administratzeko gaitasuna izango dute langileek.

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

	Lekua		Sarbide-maila	
	Izenpe	Urrunetik	Pribilegiatua	Normala
Langile-hautaketa			X	
Segurtasun-ikuskapena			X	
Gorabeherak jakinaraztea	X	X	X	X
Segurtasun fisikoa		X		
Aktiboen kudeaketa		X		
Segurtasun-arkitektura		X	X	X
Sistemen segurtasuna		X		
Sare-segurtasuna		X		
Sistemen erabileraren trazabilitatea		X	X	
Nortasunen eta sarbideen kontrola eta kudeaketa		X		
Aldaketen kudeaketa	X	X	X	X
Garapeneko segurtasuna			X	X
Gorabeheren kudeaketa		X		

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), zerbitzua nondik egiten duten kontuan hartu gabe, gorabeherak jakinarazteko politika hauek bete beharko dituzte:

1. Zerbitzuari atxikitako langile guztiek harremanetan jarri beharko dute Izenpeko segurtasun-arduradunarekin, Izenperen informazioarekin edo baliabideekin zerikusia duen edozein gorabehera hautemanez gero.
2. Edozein erabiltzailek informazioaren segurtasunarekin eta politika hauetan jasotako jarraibideekin zerikusia duten iradokizun, ahulune, hauskortasun eta/edo arrisku-egoeraren berri eman ahal izango dio Izenpeko segurtasun-arduradunari.
3. Izenpeko segurtasun-arduradunari jakinarazi beharko zaio datu pertsonalen segurtasunari eragiten dion edo eragin diezaiokeen edozer gorabehera: zerrendak eta/edo disketeak galtzea, beste pertsona batzuek sarbide baimendua bidegabe erabiltzearen susmoa izatea, datuak berreskuratzea, etab.
4. Jasotako gorabeheren bilketa, analisia eta kudeaketa zentralizatzen du Izenpeko segurtasun-arduradunak.
5. Izenpeko segurtasun-arduradunarengana jotzeko aukerarik ez badago, Izenpeko arlo teknikoaren arduradunari jakinarazi beharko zaizkio gorabeherak.

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. Zerbitzua egiteko erabilitako aktiboak kentzean, horren berri eman beharko zaio Izenperi. Gerta daiteke, bajan eman nahi den aktibo horren barruan Izenperen beste aktibo batzuk egotea (hots, hardwarea, softwarea edo bestelako aktiboak). Horrelakoetan, aktiboa Izenperi bidali behar zaio hari baja eman aurretik, Izenpek bere aktiboak bueltan har ditzan.
4. 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

Badira hornitzailearen IKT azpiegitura erabiltzearen bidez gauzatzen diren eta Izenperen 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.

1. Izenperentzako garapen-lanak eta/edo aplikazioen probak egitean edota Izenperen ardurapeko datuak erabiltzean, aipatutako jarduerak gauzatzeko erabilitako inguruneak elkarren bereizi egongo dira. Inguruneok bereizita egongo dira, baita ere, informazioa gordetzen edo prozesatzen duten ekoizpen-inguruneetatik.
2. 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.
3. Izenperen ardurapeko informazio berezia gordetzen edo prozesatzen duten informazio-sistemek gainerako beste sistema guztietatik isolaturik egon behar dute.
4. Izenperi zerbitzua egiten 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 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. Elkarren artean nahiz ordu ofizialarekin sinkronizaturik egongo dira hornitzailearen sistemetatik Izenperen ardurapeko informazioa prozesatzen edo gordetzen duten horien erlojuak.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.

8. 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.

9. 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.

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

11. 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 baliozkotu ez duen softwarerik erabiltzea.

    d) Debekatuta dago, halaber, 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 kautotze-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, txartelak, modemak, 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:
    1) Telelaneko jardueretarako ezingo da erabili Izenpek kontrolatu gabeko ekipamendua.
    2) Telelana baimentzeko irizpideak ezarriko dira, lanpostuaren beharren arabera.
    3) Sare korporatibora modu seguruan konektatzeko bete beharreko neurriak ezarriko dira.
    4) Ezarritako konexioen segurtasuna monitorizatu eta ikuskatzeko sistemak ezarriko dira.
    5) Jarduerari dagokion epealdia amaitzean, sarbide-eskubideak ezeztatu direla eta ekipamendua itzulia izan dela kontrolatuko da.

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

7. Internet lan-tresna bat da. Beraz, Interneten egiten diren jarduera guztiek lotura izan beharko dute laneko eginbeharrekin. Erabiltzaileek ez dituzte bilatu edo bisitatu behar Izenperen negozio-helburuari edo eguneroko lanari laguntzeko balio ez duten webguneak.
8. 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.
9. Erabiltzaileek ezingo dute erabili IZENPEren izena, sinboloa, logotipoa edo horien antzekoak Interneteko ezein elementutan (posta elektronikoa, web-orriak, etab.), ez bada laneko jarduerei soilik lotutako arrazoiengatik.
10. 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, etab. deskargatzea).

3.10 SISTEMEN ERABILERAREN TRAZABILITATEA

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

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 NORTASUNEN 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 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 betebehar hori.
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. Pasahitzak gutxienez 6 karaktere izan beharko ditu.
6. Pasahitzak karaktere alfabetikoak eta zenbakizkoak konbinatuz osatu beharko dira.
7. Pasahitzak aukeratzeko, komeni da jarraibide hauei lotzea:
    a) Ez erabiltzea hitz ezagunik, ezta norberarekin lotura izan dezakeenik, izena kasu.
    b) Pasahitzak ez du antzeman litekeen kontzeptu, objektu edo ideia bat gogorarazi behar. Beraz, pasahitzetan ez da erabili behar data esanguratsurik, astegunik, hilabeterik, pertsona-izenik, telefono-zenbakirik eta antzekorik.
    c) Iragartzeko ia ezinezkoa izan beharko luke gakoak. Baina, era berean, erabiltzaileak gogoratzeko erraza izan beharko luke. Adibidez, egokia litzateke esaldi edo esamolde baten akronimoa erabiltzea.
    d) Gakoak, gutxienez, karaktere zenbakizko bat eta alfabetiko bat izan beharko lituzke.
    e) Ez da komeni gakoa zenbakizko karaktere batekin hastea edo amaitzea.
    f) Ez da komeni erabiltzailearen identifikadorea gako sekretuaren zati modura erabiltzea.
8. Izenperen ardurapeko informaziora horretarako baimen egokia duten langileak ez beste inor ez direla sartzen aldian aldiro egiaztatzen dela bermatu behar du hornitzaileak.

Horrez gain, Izenperen informazio-sistemetara sartzearen kasuetan, honako arau gehigarri hauek hartu beharko dira kontuan, era berean:

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

10. Erabiltzaileek sarbide baimendua izango dute, soilik, beren eginkizunak betetzeko behar dituzten datu eta baliabideetarako.
11. Sistemak automatikoki eskatzen ez badu, erabiltzaileak aldatu beharko du sistemara sarbide baliozkoa egiten den lehenengo aldian esleitutako aldi baterako pasahitza.
12. 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 harremanetan jarri beharko du pasahitz berria eskuratzeko.
13. Aldi baterako sarbide baimenduak denbora tarte labur baterako konfiguratuko dira. Epe hori amaitzean, sistemetatik desaktibatuko dira.
14. 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.
15. 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 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 mininizatzen 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 zaurgarritasun teknikoak, eta Izenperi osagai kritikoekin lotutako guztien berri emango diote, zaurgarritasun horiek batera kudeatzeko helburuarekin.

3.13 GARAPENEKO SEGURTASUNA

Aplikazioak garatzen dituzten hornitzaile guztiek Izenperen informazio-sistemetara sarbidea (pribilegiatua nahiz ez pribilegiatua) 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. Probak egitean, 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. Berariaz onartutako aplikazioak baino ez dira bidaliko ekoizpen-ingurunera.

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 enpresa 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 enpresa hornitzaile guztiei jakinaraziko zaizkie, egoki jotzen den eran. Enpresa hornitzaile bakoitzaren erantzukizuna da Izenpek segurtasunaren alorreko politiketan egindako berrikuntzak langileek irakurri eta ezagutzen dituztela bermatzea.