

**PROZEDURA:** Entitate hornitzaileentzako informazioaren segurtasuneko araudia

AURKIBIDEA

1. XEDEA.....	3
2. HEDAPENA.....	3
3. ZUZENTARAU OROKORRAK.....	3
3.1 ZERBITZUA ESKAINTZEA.....	3
3.2 INFORMAZIOAREN KONFIDENTZIALTASUNA.....	4
3.3 JABETZA INTELEKTUALA.....	6
3.4 INFORMAZIOA ELKARRI TRUKATZEA.....	7
3.5 BALIABIDEEN ERABILERA EGOKIA.....	8
3.6 ERABILTZAILEAREN ERANTZUKIZUNAK.....	10
3.7 ERABILTZAILEAREN EKIPAMENDUAK.....	12
3.8 HARDWARE EKIPAMENDUAREN KUDEAKETA.....	13
4. ZUZENTARAU ESPEZIFIKOAK.....	14
4.1 APLIKAZIO EREMUA.....	14
4.2 LANGILEAK HAUTATZEA.....	17
4.3 SEGURTASUNARI BURUZKO KONTU-IKUSKAPENA.....	17
4.4 GORABEHEREN BERRI EMATEA.....	17
4.5 SEGURTASUN FISIKOA.....	18
4.6 AKTIBOEN KUDEAKETA.....	19
4.7 SEGURTASUN-ARKITEKTURA.....	20
4.8 SISTEMEN SEGURTASUNA.....	20
4.9 SARE-SEGURTASUNA.....	23
4.10 SISTEMEN ERABILERAREN TRAZABILITATEA.....	25
4.11 IDENTITATEEN ETA SARBIDEEN KONTROLA ZEIN KUDEAKETA.....	25
4.12 ALDAKETEN KUDEAKETA.....	27
4.13 ALDAKETEN KUDEAKETA TEKNIKOA.....	27
4.14 GARAPEN-SEGURTASUNA.....	28
4.15 KONTINGENTZIEN KUDEAKETA.....	29
5. JARRAIPENA ETA KONTROLA.....	29
6. DOKUMENTAZIO APLIKAGARRIA.....	30

Onetsia:





Berrik.: 2

Data: 2018.06.04

Orrialdea: 2.a 30etik

**PROZEDURA:**

Entitate hornitzaileentzako informazioaren  
segurtasunerako araudia

AZTERKETA	DATA	EGINDAKO ALDAKETAK
0	2012.05.02	HASIERAKO IGORPENA
1	2015.06.24	ISO ARAUEN BERRIKUSPENAREKIN ETA ANTOLAMENDU -ALDAKETEKIN BAT EGUNERATZEA
2	2018.06.04	ANTOLAMENDUZKO ALDAKETEN ARABERAKO EGUNERATZEA

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren  
segurtasunerako araudia**

## **1. XEDEA**

Agiri honen helburua ZUGAZTEL M.P., S.A.ren entitate hornitzaileentzako informazio-segurtasunari buruzko arauzko esparrua ezartzea da. Hornitzaile horiek bertako informazioa, informazio-sistemak edo -baliabideak aztertzen dituzte horien konfidentzialtasuna, segurtasuna eta eskuragarritasuna babeste aldera.

Horretarako, entitate hornitzaileek euren langile eta subkontratastei ZUGAZTELi eskaintzen dioten zerbitzuaren berri emateko ardura hartzen dute.

## **2. HEDAPENA**

Informazioa, informazio-sistemak edo -baliabideak aztertzen dituzten entitate hornitzaileek ZUGAZTELentzat garatutako jarduera guztiak.

3. atala "Zuzentarau orokorrak" edozein entitate hornitzaileari aplikatu dakioke, eskaintako zerbitzu mota edozein izanda ere.

4. atala, "Zuzentarau espezifikoak" kasu bakoitzean adierazitako zerbitzu motari dagokion zerbitzuak eskaintzen dituzten entitate hornitzaileei bakarrik aplikatu dakieke, atalaren hasieran azaltzen den moduan.

## **3. ZUZENTARAU OROKORRAK**

### **3.1 Zerbitzua eskaintzea**

Entitate hornitzaileek ZUGAZTELentzat zerbitzuak eskaintzeko dagokion kontratuaren mende babestutako jarduerak bakarrik garatu ahalko dituzte.

Entitate hornitzaileak noizean behin ZUGAZTELi eskaintako zerbitzuari lotutako pertsona, profil, funtzio eta erantzukizunen zerrenda eskainiko dio eta unean unean zerrenda horretan gertatutako edozein aldaketa (funtzio edo erantzukizunen alta, baja, ordezkapen edo aldaketa) helaraziko dio.

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

Zerbitzuak eskaintzeko kontratuari loturiko klausuletan ezarritakoaren arabera, ZUGAZTELen lanak garatzen dituen kanpoko langile orok agiri honetan jasotako segurtasun arauak bete beharko ditu. Betebehar horietako edozein urratuz gero, ZUGAZTELek arau-haustea egin duen langileari betoa jartzeko eskubidea gordetzen du, baita entitate hornitzailearen inguruan egokitzat jotzen diren zehapen neurriak hartzeko eskubidea ere.

Entitate hornitzaileak bermatu beharko du bere langile guztiek eskaintako zerbitzua garatzeko ahalmen egokia dutela.

ZUGAZTELen eta entitate hornitzailearen artean gertatutako edozein informazio truke zerbitzuak eskaintzeko dagokion kontratuak ezarritako esparruaren barnean egin dela ulertuko da, beraz, informazio hori ezingo da erabili esparru horretatik kanpo ezta beste helburuekin ere.

Antolamendua eta Sistemen Arloak ZUGAZTELen aktiboak babesteko ahalmen globalak zentralizatzen ditu.

Orokorrean, aktiboek zera barne hartzen dute:

- Informazio babestua, hau da, pertsona fisiko edota juridikoak identifikatzeko aukera eskaintzen duen informazioa eta informazio-sistemen eta komunikazio sareen konfigurazioari buruzkoa.
- Informazio babestuaren tratamendurako loturikoak (softwarea, hardwarea, komunikazio sareak, informazio euskarriak, ekipamendu osagarria eta instalazioak).

### 3.2 Informazioaren konfidentzialtasuna

ZUGAZTELen informazioa eskura dezaketen kanpoko langileek informazio hori, berez, babestua dela kontuan hartu beharko dute. Informazio ez babestutzat jo ahalko da ZUGAZTELek helburu horrekin ezarritako informazioko hedapen publikoko bitartekoen bidez eskuratu den informazioa bakarrik.

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

Informazioa ezagutaraztea, aldatzea, apurtzea edo gaizki erabiltzea ekidingo da edozein euskarritan egonda ere.

Denbora tarte mugagabea erreserbarik handiena gordeko da eta informazio babestua ez da kanpora igorriko, behar bezala baimenduta egon ezean.

Informazio babestua duten paperezko formatuko txosten kopurua murriztuko da eta horiek leku seguruan eta hirugarrenek eskuratu ezin duten tokian mantenduko dira.

Lanpostuarekin zuzenean loturiko arrazoiak direla-eta, entitate hornitzaileko langileak edozein euskarritan jasotako informazio babestua eskuratuz gero, eskuratze hori aldi baterako dela ulertu beharko du, sekreturako betebeharrarekin eta horrek informazio horren gaineko jabetza, titulartasun edo kopiarako inolako eskubiderik eskaini gabe. Era berean, langileak aipatutako euskarria edo euskarriak itzuli beharko ditu horien aldi baterako erabilera sortu duten zereginak amaitu bezain laster eta, nolana ere, bere enpresak ZUGAZTELekin harremana amaitzean.

Betebehar horiek guztiek indarrean jarraituko dute kanpoko langileek ZUGAZTELezentzat garatutako jarduerak amaitu ostean.

Betebehar horiek urratzeak sekretuak ezagutaraztearen delitua sor dezake.

Datu pertsonalen segurtasuna bermatze aldera, entitate hornitzaileko langileek honako jarduera arauak bete beharko dituzte, dagoeneko aipatutako gogoetaz gain:

- Bere lana burutzeko beharrezkoa denean soilik sortu ahalko ditu fitxategiak. Aldi baterako fitxategi horiek ez dira inolaz ere langileen PC postuen tokiko disko-unitateetan gordeko eta sortutako helburuarentzat erabilgarriak izateari utzi diotenean apurtu beharko dira.
- Ez dira datu pertsonalak gordeko erabiltzailearen PC postuen tokiko disko-unitateetan.

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Euskarriak eta agiriak informazio hori jasotzen duten lokaletatik kanpo irtetea (posta elektronikoa bidaltzea barne) ZUGAZTELeK bakarrik baimendu ahalko du, eta definitutako prozeduraren arabera egingo da.
- Euskarriek eta agiriak biltzen duten informazio mota identifikatzeko, inbentariatzeko eta baimendutako langileei mugatutako leku batean biltzeko aukera eskaini beharko dute.
- Maila altuko datu pertsonalak (adib. Osasuna), telekomunikazio sareen bidez (adib. posta elektronikoa), datu horiek zifratuz edo informazioa hirugarrenek ulertu eta manipulatu ezin dutela bermatzen duen beste edozein mekanismo erabiliz bidaliko dira.

### 3.3 Jabetza intelektual

Jabetza intelektualeko arauz babestutako materialaren erabilerari ezarritako legeko murrizketak betetzen direla bermatuko da.

Beren eginkizunak betetzeko baino ezin izango dute ZUGAZTELeK baimendutako materiala erabili erabiltzaileek.

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

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

ZUGAZTELeK soilik baimenduko du erakundeak berak ekoiztutako materiala —edo materialaren titularrak ZUGAZTELi emandako edo baimendutakoa— erabiltzea, hitzartutako moduan eta baldintzekin, eta indarrean dagoen araudiaren arabera.

**PROZEDURA:**

Entitate hornitzaileentzako informazioaren segurtasunerako araudia

### 3.4 Informazioa elkarri trukatzea

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

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

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

- Egile-eskubideen bidez babestutako materiala igorri edo jasotzea Jabetza Intelektuala Babesteko Legea urratuz
- Material pornografikoa, sexu esplizituzkoak, arrazakeriazko adierazpen baztertzailak edo iraingarri edo legez kontrakotzat har daitekeen beste edozein adierazpen edo mezu igorri edo jasotzea
- Baimendu gabeko hirugarrenei informazio babestua igortzea.
- Negozioarekin loturarik ez duten aplikazioak igorri edo jasotzea.
- Interneteko zenbait jardueratan parte hartzea, hala nola berri-taldeetan, jolasetan edo zerbitzuarekin lotura zuzenik ez duten beste batzuetan.

Debekatuta dago, Interneten edo beste edozein lekutan, ZUGAZTELen izen ona kaltetu lezakeen jarduera oro.

**PROZEDURA:**

Entitate hornitzaileentzako informazioaren segurtasunerako araudia

### 3.5 Baliabideen erabilera egokia

Entitate hornitzaileak konpromisoa hartzen du aldizka ZUGAZTELi zerbitzua eskaintzeko baliatzen dituen aktiboen berri emateko.

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

ZUGAZTELeK 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. ZUGAZTELeK eskubidea du kontrol- eta ikuskapen-mekanismoak ezartzeko, baliabide horiek behar bezala erabiltzen direla egiaztatze aldera.

Homologatutako marka eta modeloetako ekipoa konektatu beharko ditu entitate hornitzaileak ZUGAZTELen ekoizpen-sarera. Entitate hornitzaileak ZUGAZTELen esku jarriko ditu ordenagailuak, horietan software homologatuaren instalazioa koordinatu eta horiek egoki konfiguratu dituzan

Euskarri automatizatuen, Interneten edo posta elektronikoen bidez edo beste edozein modura ZUGAZTELen sarean edo sare horretara konektatutako edozein ordenagailutan sartutako edozein fitxategi arau hauetan ezarritako betekizunak bete beharko ditu, eta bereziki jabetza intelektualari, datu pertsonalen babesari eta birusak eta malware kontrolatzeari buruzkoak.

Kontratua bukatu ondoren, aktibo guztiak ZUGAZTELi itzuli beharko zaizkio, justifikaziorik ez duen atzerapenik gabe. ZUGAZTELeK softwarea instalatu dien ordenagailu pertsonal guztiak ZUGAZTELera eramango dira, zerbitzua amaitu ondoren disko gogorra formateatzeko.

Berariaz debekaturik dago:



**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Zerbitzuaren xedearekin loturarik ez duten jardueretarako erabiltzea ZUGAZTELEk emandako baliabideak.
- ZUGAZTELEn ekoizpen-sarera konektatzea ZUGAZTELEn jabetzakoak diren software edo baliabide informatikoen estandar gisa identifikatuta ez dauden ekipamendu edota aplikazioak.
- Informazio-sistemetan edo ZUGAZTELEn sare korporatiboan eduki lizunak, mehatxagarriak, moralgabeak edo iraingarriak paratzea.
- 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 ZUGAZTELEn sare korporatiboan. ZUGAZTELEn sarean sar daitezkeen langile guztiek birusen aurkako programak eta horien eguneratzeak erabiltzeko betebeharra izango dute.
- ZUGAZTELEk esleitu dizkienez bestelako eskubide edo sarbideak berariazko baimenik gabe lortzea.
- ZUGAZTELEn informazio-sistemetako eremu mugatuetara berariazko baimenik gabe sartzea.
- ZUGAZTELEn Informazio-sistemetako "log" erregistroak desitxuratu edo faltsutzea.
- Zifratzeko gakoak, sistemak edo algoritmoak eta ZUGAZTELEn prozesu telematikoetan erabiltzen den edozein segurtasun-elementu berariazko baimenik gabe deszifratzea.
- Beste erabiltzaileen lanean eragin lezaketen programak eduki, garatu edo exekutatzeko eta ZUGAZTELEn baliabide informatikoak kaltetu edo aldatzea.

<b>PROZEDURA:</b>	<b>Entitate hornitzaileentzako informazioaren segurtasunerako araudia</b>
-------------------	---

- Informazio babestua duten datu, programa edo dokumentu elektronikoak suntsitu, aldatu, baliogabetu edo beste modu batera kaltetzea (egintza horiek kalte-delitua izan litezke).
- Informazio babestua gordetzea erabiltzaileen PC postuetako tokiko disko-unitateetan.

### 3.6 Erabiltzailearen erantzukizunak

Zerbitzuen entitate hornitzaileek bermatu beharko dute ZUGAZTELeentzat lan egiten duten langile guztiek oinarritzko printzipio hauek beteko dituztela informatika-jardunean:

- ZUGAZTELe 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. Erabiltzaileak, hortaz, ez dio bere gakoa zein den esan behar beste langileei, inola ere ez.
- Erabiltzaileek ez dute beste erabiltzaile baten identifikadorerik erabiliko, ezta jabearen baimena badute ere.
- Eskuen artean duten informazioaren baldintzak nahiz prozedurak ezagutu eta aplikatzen dituzte erabiltzaileek.

Informazio babestua eskura dezakeen orok pasahitzak kudeatzeari buruzko zuzentarau hauek bete beharko ditu:

- Kalitatezko pasahitzak aukeratzea, hau da, gainontzeko erabiltzaileek asmatu ezin dituztenak.
- Beste erabiltzaileek pasahitza ezagutzearen zantzurik badago, pasahitza aldatzeko eskatzea.

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Gutxienez 90 egunetan behin pasahitzak aldatzea eta pasahitza zaharrak ez erabiltzea.
- Lehenengo saio-hasieran (“login”) programak emandako nahiz aldi baterako pasahitzak aldatzea.
- Saioa hasteko prozesu automatizatueta –esate baterako, funtzio-tekla edo makro batean bildutakoak– pasahitzik ez jartzea.
- Pasahitzaren segurtasuna kinkan jarritz gero, dela pasahitza galdu duelako, hura lapurtu dutelako, edo konfidentzialtasuna galdu dela uste bada, haren berri eman beharko da.

Informazio babestua eskura dezaketen pertsona guztiek zaindu beharko dute ekipamenduak babesturik egongo direla zaintzarik gabe geratzen direnean.

Informazio babestua eskura dezaketen pertsona guztiek idazmahai txukuneko honako arauak errespetatu beharko dituzte, paperean edo euskarri informatikoetan diren agiriak nahiz informazioa gordetzeko gailu eramangarriak babesteko eta, baimenik ez duten pertsonak horiek eskura dezatela, horiek gal daitezela edota informazioa galtzeko arriskuak murrizteko, lanorduen barruan nahiz lanorduetatik kanpo:

- Erabiltzen ez direnean, paperezko dokumentuak eta baliabide informatikoak giltzapean biltegitratzea, batez ere lan-ordutegitik kanpo.
- Erabiltzaile saioak blokeatzea edo ordenagailua itzaltzea zaintzarik gabe uzterakoan.
- Informazioa jasotzeko eta bidaltzeko puntuak babestea (posta, eskaner- eta fax-makinak), bai eta kopiak egiteko ekipoak ere (fotokopiagailua, faxa eta eskanerra). Erabiltzailearen ardura izango da gailu horien bidez informazioa sortu edo bidaltzea.
- Behin inprimatu ondoren, edozein informazio babestu gordetzea, atzerapenik gabe –betiere, atzeratzeko arrazoirik izan ez bada–.

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Informazio babestua apurtzea beharrezkoa ez denean.
- ZUGAZTELen informazioa eskuratu edota haren sistemetara sar daitezkeen pertsonak ez dute sekula idatzizko baimenik gabe egingo ustezko ahulezia edota segurtasun-okerra hautemateko probarik.
- ZUGAZTELen informazioa eskura dezaketen edota haren sistemetan sar daitezkeen pertsonak ez dira inola ere saiaturiko, idatzizko baimen espliziturik gabe, segurtasun-sistema eta baimenak hausten. Debekatuta dago erabiltzaileek sareko trafikoak atzitzea, idatziz baimendutako ikuskatze-lanak egiteko ez bada.

Informazio babestura sarbidea duen langile orok jarduera-arau hauek bete beharko ditu:

- Informazio babestua baimendu gabeko jakinarazpen, aldaketa, suntsipen edo erabilera desegokietatik –halabeharrezkoak izan ala ez– babestea.
- Informazio-sistema eta telekomunikazio-sare guztiak babestea baimendu gabeko sarbide edo erabilera, operazio-eten, suntsipen, erabilera oker edo lapurretetatik.
- Informazio-sistematarako sarbidea lortzeko edota informazioa eskuratzeko beharrezkoa den baimena edukitzea.

### 3.7 Erabiltzailearen ekipamenduak

Zerbitzuak eskaintzen dituzten entitate hornitzaileek bermatuko dute informazio babestura jotzeko erabilitako ordenagailu guztiek ondoko baldintza hauek beteko dituztela:

- Erabiltzailea geldi dagoenean, ekipamendua automatikoki blokeatu beharko da gehienez ere 15 minutuko epean.
- Erabiltzaileen ekipamenduetan ez da izango segurtasun-sistemak eta baimenak urra ditzakeen tresnarik.
- Fabrikatzailearen argibideen arabera zainduko dira erabiltzaileen ekipamenduak.
- Malwarearen kontra egoki babesturik daude erabiltzaile-ekipamendu guztiak:

<b>PROZEDURA:</b>	<b>Entitate hornitzaileentzako informazioaren segurtasunerako araudia</b>
-------------------	---

- o Birusen aurkako softwarea ordenagailu guztietan instalatu eta erabili beharko da, birusek edo bestelako software kaltegarriek eragin ditzaketen arriskuak murrizteko.
- o Eskura daitezkeen segurtasunari buruzko azken eguneraketak egingo dira eta, ondorioz, ekipamenduak egunean mantenduko.
- o Birusen aurkako softwareak aktibatuta eta eguneratuta egon beharko du beti.

Zainduko da, bereziki, informazio babestua dakarten edota modu batera edo bestera informazio hori eskuratzeko bide ematen duten erabiltzaileen ekipamendu mugikor guztien segurtasuna:

- Informaziotik behar-beharrezkoa den hura baino ekarriko ez dutela egiaztatzea.
- Informazio horretarako sarbideak kontrolatuko direla bermatzea.
- Eskainitako zerbitzutik kanpoko pertsonen aurrean aipatu informazioa ahalik eta gutxien ikustea.
- Leku batetik bestera eramatean ingurumeneko eragileetatik babesteko, ekipamenduak egoki diren zorroetan, maleta txikietan edo antzeko ekipamenduetan sartzea.

### 3.8 Hardware ekipamenduaren kudeaketa

Zerbitzuen entitate hornitzaileek ziurtatu beharko dute edozein eratako zerbitzuak eskaintzeko asmoz ZUGAZTELek emandako ekipamendu guztiak egoki kudeatuko direla. Horretan hurrengo arau hauek bete beharko dituzte:

- Entitate hornitzaileak egunean izan beharko du ZUGAZTELek emandako ekipamenduen zerrenda bai eta aktibo horien erabiltzaileena edota, pertsona batek baino gehiagok erabiliz gero, aktibo horien arduradunena ere. ZUGAZTELek zerrenda hori eskatu ahalko du.

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Entitate hornitzaileak berriz erabili nahi baldin badu informazio babestua zekarren ZUGAZTELen ekipamenduren bat, denbora batez bueltan eman beharko du, ekipamendua berriz erabili aurretik erakundeak datuak segurtasunez ezabatu ditzan.
- Entitate hornitzaile batek ZUGAZTELek emandako ekipamenduetako bat zerrendatik kendu nahi badu, buelta eman beharko du, ZUGAZTELek egoki izapide dezan aipatu baja hori.
- Entitate hornitzailearen batek zerbitzua eskaintzeari uzten badio, hari emandako ekipamendu guztiak bueltan eman beharko dizkio ZUGAZTELi, zerbitzuak eskaintzeko kontratuetan xedatu bezalaxe. Paperean eta euskarri informatikoan dauden agiriak baino ezin izango ditu segurtasunez ezabatu hornitzaileak. Horrelakoetan, jakinaren gainean jarri beharko du entitate hornitzaileak ZUGAZTEL.

#### **4. ZUZENTARAU ESPEZIFIKOAK**

---

##### **4.1 Aplikazio eremua**

Arau orokorrez gain, entitate hornitzaile guztiek bete beharko dituzte, baita ere, atal honetako arau espezifikoetatik ZUGAZTELi eskainitako zerbitzuaren ezaugarrien arabera dagozkion horiek.

Jarraian zerbitzuen motak zehaztuko ditugu.

- Zerbitzua non eskaintzen den: Zerbitzuak bi multzotan bana daitezke, hura eskaintzen den lekuaren arabera:
  - ZUGAZTEL: Zenbait hornitzailek ZUGAZTELen egoitzan bertan eskaintzen dute zerbitzua.
  - Urrunetik: Zenbait entitate hornitzailek bere egoitzatik eskaintzen du zerbitzua. Hala ere, ZUGAZTELen egoitzan gauza dezake entitate hornitzaileak jarduera bat edo beste.

**PROZEDURA:**
**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- 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:
  - ZUGAZTEL.
  - Entitate hornitzailea.
- ZUGAZTELen sistemarako sarbide-maila: ZUGAZTELen informazio-sistemarako sarbide-mailaren arabera hiru multzo bereiz daitezke:
  - Sarbide pribilegiatua: ZUGAZTELen informazio-sistemara modu pribilegiatuan sartzeko gaitasuna behar denean zerbitzua eskaintzeko. Hau da, sistema horiek edota prozesatutako ekoizpen-datuak administratzeko gaitasuna izango dute langileek.
  - Erabiltzaile-mailako sarbidearekin: ZUGAZTELen 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.
  - Sarbiderik ez: ZUGAZTELen informazio-sistemak erabili behar ez direnean zerbitzua eskaintzeko. Hortaz, zerbitzua eskainiko duten langileek ez dute erabiltzaile-konturik aipatu sistema horietan.

Zerbitzu bakoitza, beraz, aipatu hiru kategoria horietako baten barruan izango da. Hortaz, segurtasun-arau orokorrak betetzeaz gain, hornitzaile bakoitzak beteko bere kategoriari dagozkion arau espezifikoak bete beharko ditu, hau da:

	TOKIA		AZPIEGITURA		SARBIDEA		
	ZUGAZTEL	Urrutikoa	ZUGAZTEL	Hornitzailea	Pribilegiatua	Arrunta	Sarbiderik ez
langileak aukeratzea	EZ	EZ	EZ	EZ	BAI	EZ	EZ

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

	TOKIA		AZPIEGITURA		SARBIDEA		
	ZUGAZTEL	Urrutikoa	ZUGAZTEL	Hornitzailea	Pribilegiatua	Arrunta	Sarbiderik ez
segurtasuneko kontu- ikuskapena	EZ	EZ	EZ	EZ	BAI	EZ	EZ
gertakariak jakinaraztea	BAI	BAI	BAI	EZ	BAI	BAI	EZ
segurtasun fisikoa	EZ	BAI	EZ	EZ	EZ	EZ	EZ
aktiboen kudeaketa	EZ	EZ	EZ	BAI	EZ	EZ	EZ
segurtasun-arkitektura	EZ	EZ	EZ	BAI	BAI	BAI	EZ
sistemen segurtasuna	EZ	EZ	EZ	BAI	EZ	EZ	EZ
sare-segurtasuna	EZ	EZ	EZ	BAI	EZ	EZ	EZ
sistemen erabileraren trazabilitatea	EZ	EZ	EZ	BAI	BAI	EZ	EZ
identitateen eta sarbideen kontrola eta kudeaketa	EZ	EZ	EZ	BAI	EZ	EZ	EZ
aldaketen kudeaketa	EZ	EZ	EZ	BAI	BAI	BAI	EZ
aldaketen kudeaketa teknikoa	EZ	EZ	EZ	EZ	BAI	EZ	EZ
garapen-segurtasuna	EZ	EZ	EZ	EZ	BAI	BAI	EZ
kontingentzien kudeaketa	EZ	EZ	EZ	BAI	EZ	EZ	EZ



**PROZEDURA:**

Entitate hornitzaileentzako informazioaren  
segurtasunerako araudia

#### 4.2 Langileak hautatzea

Entitate hornitzaileak zerbitzuari esleitutako langileen aurrekari profesionalak egiaztatu beharko ditu eta ZUGAZTELen aurrean bermatu beharko du iraganean ez dutela zigorrik jaso praxi profesional okerraren ondorioz edo ez dutela zigor motaren bat eragin duen inolako gorabeherarik eduki esku artean izan duten informazioaren konfidentzialtasuna dela-eta.

Gerta daiteke, "3.1.Zerbitzua eskaintzea" izeneko paragrafoan ezarritako baldintzen arabera, pertsonaren bat betatzeko eskubidea bete nahi izatea ZUGAZTELeK. Horrelakoetan, zerbitzua eskainiko duten langileen zerrendatik betatu nahi duen pertsona berehala kentzeko aukera izango duela bermatuko dio entitate hornitzaileak ZUGAZTELI.

#### 4.3 Segurtasunari buruzko kontu-ikuskapena

Entitate hornitzaileak ZUGAZTELI eskatutako segurtasuneko kontu-ikuskapenak burutzeko aukera eman behar dio, kontu-ikuskari taldearekin lankidetzan arituz eta eskatzen diren ziurtasun eta erregistro guztiak aurkeztuz.

Kasu bakoitzean, kontu-ikuskapen bakoitzaren hedapena eta sakontasuna ZUGAZTELeK berariaz ezarriko du. Kontu-ikuskapenak kasu bakoitzean zerbitzuaren hornitzailearekin adostutako plangintzari jarraiki burutuko dira.

ZUGAZTELeK ezohiko kontu-ikuskapen gehigarriak egiteko eskubidea bere gain hartu du, betiere, hori justifikatzen duten arrazoi zehatzak baldin badaude.

#### 4.4 Gorabeheren berri ematea

Informazioaren segurtasunari lotutako edozein gorabehera antzemanaz gero, berehala horren berri eman beharko da [segurtasuna.zugaztel@bizkaia.eus](mailto:segurtasuna.zugaztel@bizkaia.eus) posta elektronikoko helbidearen bitartez.

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

Edozein erabiltzailek informazioaren segurtasunari eta arau hauetan jasotako jarraibideei lotutako gertakariak, iradokizunak, zaurgarritasunak... helarazteko aukera edukiko du aipatutako helbidearen bitartez.

Antzematen den eta izaera pertsonaleko datuen segurtasunean eragina duen edo eragina eduki dezakeen edozein gorabehera aipatutako helbidearen bidez jakinarazi beharko du (adibidez, zerrendak eta/edo euskarri informatikoak galtzea, beste pertsona batzuen eskutik baimendutako sarbidea behar ez bezala erabiltzen ari dela susmatzea, segurtasun kopietako datuak berreskuratzea...).

Aipatutako gutunontziak bidalitako gertakarien jasotzea, azterketa eta kudeaketa zentralizatu egiten du.

Ezin bada helbide hori erabili, zerbitzuaren barruan ezarritako komunikazio bideak erabili beharko dira, beraz, ZUGAZTELeko hizketakidea izango da segurtasunari lotutako gorabeheraren berri emango duena.

#### 4.5 Segurtasun fisikoa

Egoitza itxita egon beharko da eta sarrera kontrolatzeko sistemaren bat eduki beharko du.

Bisitak nolabait kontrolatuko dira, behintzat sarbide publikoa duten guneeetan eta/edo zamalanak egiteko eremuan.

Egoitzak, gutxienez, suteak antzemateko sistemak eduki beharko ditu eta uholdeen aurrean erresistentzia nahikoa eskaintzeko moduan eraiki beharko da.

Segurtasun kopiaren bat baldin badago, informazio hori bildu eta/edo prozesatzen duten sistemak modu berezian babestuta dagoen eremu batean kokatu beharko dira. Eremu horrek, gutxienez, ondorengo segurtasun neurriak bete beharko ditu:

- Modu berezian babestuta dagoen eremuak egoitzaren sistemarekiko independentea den sarrera kontrolatzeko sistema eduki beharko du.

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Modu berezian babestutako eremuetan kanpoko langileen joan-etorriak mugatuko dira. Beharrezkoa denean eta baimenduta dagoenean besterik ezingo dira sartu eta beti egongo dira baimendutako langileen zaintzapean.
- Kanpoko pertsona guztien sarreraren eta irteeren erregistroa egingo da.
- Kanpoko langileak ezingo dira modu berezian babestutako eremuetan geratu, ezta bertan lanak burutu ere, inoren zaintzapean ez bada.
- Modu berezian babestutako eremuetan jatea edo edatea debekatuta egongo da.
- Eremu horretan kokatuta dauden sistemak nolabait babestuta egon beharko dira elikatze-akatsen aurrean.

#### 4.6 Aktiboen kudeaketa

Entitate hornitzaileak eguneratutako aktiboen erregistro bat eduki beharko du. Bertan, zerbitzua emateko erabili diren aktiboak identifikatu ahalko dira.

Zerbitzua emateko erabili diren aktibo guztiek arduradun bat eduki beharko dute. Arduradunak ziurtatu beharko du aktibo horiek erakundeak ezarritako gutxieneko segurtasun neurriak (gutxienez, araudi honetan zehaztutakoak izan beharko dira) barne hartu dituztela.

Entitate hornitzaileak ZUGAZTELi jakinarazi beharko dizkio zerbitzua emateko erabilitako aktiboen bajak. Aktibo horrek ZUGAZTELen jabetzakoak diren beste batzuk baldin baditu (hardware, software edo beste aktibo mota bat) ZUGAZTELi eman beharko zaio baja burutu baino lehen. Modu horretan, ZUGAZTELe bere jabetzakoak diren aktiboak kenduko ditu.

Aktibo batek babestutako informazioa duen bakoitzean, entitate hornitzaileak aktiboen bajak burutu beharko ditu informazio hori modu seguruan desagerrarazten dela bermatuz, hau da, modu seguruan ezabatzeko funtzioak aplikatuz edo aktiboa fisikoki ezereztuz bertan jasota zegoen informazioa berreskuragarri izan ez dadila.

**PROZEDURA:**

Entitate hornitzaileentzako informazioaren  
segurtasunerako araudia

#### 4.7 Segurtasun-arkitektura

Zerbitzuen entitate hornitzaileak ZUGAZTELeentzako babestutako informazioa barne hartzen duten garapen lanak eta/edo aplikazioen probak burutzen dituen bakoitzean, jarduera horien testuinguruak elkarrekiko isolatuta egon beharko dira, bai eta babestutako informazioa barne hartzen duen edo informazio hori prozesatzen duen ekoizpen testuinguruetatik isolatuta ere.

Babestutako informazioa daukaten edo prozesatzen duten sistemen sarbide guztiak babestuta egon beharko dira, gutxienez, horietara konektatzeko ahalmena mugatzen duen su-ebaki baten bidez.

Bereziki babestutako informazioa gordetzen edo prozesatzen duten informazio-sistemek gainerako beste sistema guztietatik isolaturik egon behar dute.

#### 4.8 Sistemen segurtasuna

Babestutako informazioa barne hartzen duten edo jorratzen duten informazio sistemek euren funtzionamenduaren gaineko gertaerarik esanguratsuenak erregistratu beharko dituzte. Jarduketa erregistro horiek hornitzailearen segurtasun kopiei buruzko araudiaren barruan jasoko dira.

Babestutako informazioa barne hartzen duten edo prozesatzen duten hornitzailearen sistemetako erlojuak euren artean sinkronizatuta egon behar dira, ordu ofizialarekin.

Zerbitzuaren entitate hornitzaileak bermatuko du babestutako informazioa bildu edo jorratzen duten informazio sistemen edukiera behar bezala kudeatzen dela, etete posibleak edo baliabideen saturazioaren ondorioz sistema horien funtzionamendu okerra saihestuz.

Babestutako informazioa bildu edo jorratzen duten informazio sistemak behar bezala babestuko dira software maltzurren aurrean. Horretarako, honako jarraibide hauek bete beharko dira:

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Sistemak eguneratuta mantenduko dira, eskuragarri dauden azken segurtasun eguneraketekin garapen, proba eta ekoizpen inguruneetan.
- Birusen aurkako softwarea instalatu beharko da eta zerbitzari eta ordenagailu pertsonal guztietan erabili beharko da birusei edo beste software maltzurrei lotutako eragiketa-arriskua murrizteko.
- Birusen aurkako softwareak une oro aktibatuta eta eguneratuta egon beharko du.

Astean behin, entitate hornitzaileak segurtasun kopien gaineko araudia ezarriko du, emandako zerbitzuarentzat garrantzitsua den edozein datu edo informazioaren babesa bermatzen duena.

Emandako zerbitzuari lotuta posta elektronikoa erabiltzen den bakoitzean entitate hornitzaileak ondorengo premisak errespetatu beharko ditu:

- Ezingo da babestutako informazioa posta elektronikoa bidez helarazi, komunikazio elektronikoa zifratuta ez baldin badago eta bidalketa idatziz baimenduta ez badago behintzat.
- Maila altuko (hala nola, osasuna) izaera pertsonaleko datuak barne hartzen dituen informazioa ezingo da posta elektronikoa bidez helarazi, komunikazio elektronikoa zifratuta ez baldin badago eta bidalketa idatziz baimenduta ez badago behintzat.

Zerbitzua emateko ZUGAZTELen posta elektronikoa erabiltzen den bakoitzean, gutxienez, ondorengo printzipioak errespetatu beharko dira:

- Posta elektronikoa langilearen esku jartzen den beste lan-tresna bat da, beraz, kontratatutako zerbitzua eskaintzeko soilik erabili beharko da. Hala, ZUGAZTELeK 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.
- ZUGAZTELen posta elektronikoko sistema ezingo da erabili iruzurrezko mezuak, mezu lizunak, mehatxagarriak eta antzekoak bidaltzeko.

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren  
segurtasunerako araudia**

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

Babestutako informazioa gordetzen edo prozesatzen duten informazio-sistemarako sarbidea egiaztatu beharko da beti; gutxienez, erabiltzaile-identifikadorearen eta hari lotutako pasahitzaren bidez.

Babestutako informazioa gordetzen edo prozesatzen duten informazio-sistematan sarbidea kontrolatzeko sistemak izango dira. Kontrol-sistema horien bidez, bidenabar, zerbitzuan lan egiten denei baino ez zaie utziko aipatu informazioa eskuratzen.

Erabiltzaileek denbora batez jardunari uztean automatikoki blokeatuko dira babestutako informazioa gordetzen edo prozesatzen duten informazio-sistemarako sarrera-saioak.

ZUGAZTELEk emandako softwarea erabiltzen den guztietan, ondoko arau hauek bete beharko dira:

- Emandako software bertsioak bakarrik erabili beharko dituzte ZUGAZTELEn informazio-sistemara sarbidea duten langileek, eta horien erabilera arauak bete.
- Langileek debekatua dute edozein programaren legez kontrako kopiarik egitea, programa estandarizatuenak barne.
- Debekatuta dago ZUGAZTELEk baliozkotu ez duen softwarea erabiltzea.
- Debekatuta dago, halaber, ZUGAZTELEn instalatutako edozein programa desinstalatzea.

|

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

#### 4.9 Sare-segurtasuna

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

Ahalik eta gehien mugatu behar dira babestutako informazioa dakarten sareetako zerbitzuak.

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

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

Babestutako informazioa dakarten sareetarako sarbidea mugaturik egongo da.

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

Teledana, alegia, kanpotik lana egitea sare korporatiborako sarbidea izanik, ondorengo araudiaren bidez arautuko da:

- Teledaneko jardueretarako ezingo da erabili ZUGAZTELEK kontrolatu gabeko ekipamendua.
- Teledana baimentzeko irizpideak ezarriko dira, lanpostuaren beharren arabera.

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

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

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

- Internet lan-tresna bat da. Beraz, Interneten egiten diren jarduera guztiek lotura izan beharko dute laneko eginbeharrekin. Erabiltzaileek ez dituzte bilatu edo bisitatu behar ZUGAZTELen negozio-helburuari edo eguneroko lanari laguntzeko balio ez duten webguneak.
- 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.
- Erabiltzaileek ezingo dute erabili ZUGAZTELen izena, sinboloa, logotipoa edo horien antzekoak Interneteko ezein elementutan (posta elektronikoa, web-orriak eta abar), ez bada laneko jarduerari lotutako arrazoiengatik.
- Internetera edo Internetetik datu-transferentziak egitea onartuko da, soilik, negozioko jarduerekin lotura badute. Debekatuta dago jarduera horiekin zerikusirik ez duten fitxategi-transferentziak egitea (adibidez, programak, multimedia-fitxategiak...deskargatzea).



**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia****4.10 Sistemen erabileraren trazabilitatea**

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

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

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

**4.11 Identitateen eta sarbideen kontrola zein kudeaketa**

Informazio-sistema batera sarbidea duten erabiltzaile guztiek sarbide-baimen bakar bat izango dute, erabiltzailearen identifikadoreaz eta pasahitzaz osatua.

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

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

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

Pasahitzak gutxienez 6 karaktere izan beharko ditu eta ezin du izan erabiltzailearen ez izenik ez abizenik ezta identifikatzailearik (userid) ere. 45 egunean behin aldatuko da aurreko 8 pasahitzak errepikatu gabe.

Pasahitzak karaktere alfabetikoak eta numerikoak konbinatuz osatu beharko dira.

Halaber, konplkexuak izango dira, asmatzen zailak. Beraz, lehen 8 karakteretan 4 aukera hauetatik, gutxienez honako 3 izan behar ditu:

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Letra larriak
- Letra xeheak
- Zenbakiak
- Karaktere bereziak

Komeni da jarraibide hauei lotzea:

- Ez erabiltzea hitz ezagunik, ezta norberarekin lotura izan dezakeenik, izena kasu.
- 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.
- Gakoak ia asmaezina izan behar du, baina, aldi berean, erabiltzaileak erraz gogoratzeko modukoa. Adibidez, egokia litzateke esaldi edo esamolde baten akronimoa erabiltzea.

Babestutako informazioa horretarako baimen egokia duten langileak ez beste inor ez direla sartzan aldian aldiro egiaztatzen dela bermatu behar du entitate hornitzaileak.

Horrez gain, langileak ZUGAZTELEN informazio-sistemetara sartzan diren kasuetan, ondoko arau hauek hartu beharko dira kontuan ere:

- Ezein erabiltzailek ez du jasoko ZUGAZTELEN sistemetara sarbidea izateko identifikadorerik, harik eta indarrean dagoen segurtasun-politika formalki onartzen duten arte.
- Erabiltzaileek sarbide baimendua izango dute, soilik, beren funtzioak betetzeko behar dituzten datu eta baliabideetarako.
- Sistemak automatikoki eskatzen ez badu, erabiltzaileak aldatu beharko du sistemara sarbide egokia egiten den lehenengo aldian esleitutako aldi baterako pasahitza.

**PROZEDURA:**

**Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

- Sistemak automatikoki eskatzen ez badu, erabiltzaileak gutxienez 90 egunean behin aldatu beharko du pasahitza.
- Aldi baterako sarbide baimenduak denbora-tarte labur baterako konfiguratuko dira. Epe hori amaitzean, sistematik desaktibatuko dira.
- 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.
- Erabiltzaile batek susmatzen badu beste pertsona bat bere sarbide baimendua (erabiltzailearen identifikadorea eta pasahitza) erabiltzen ari dela, pasahitza aldatu beharko du, eta gertatutakoaren berri eman beharko du [segurtasuna.zugaztel@bizkaia.eus](mailto:segurtasuna.zugaztel@bizkaia.eus) posta elektronikoaren bitartez.

#### 4.12 Aldaketen kudeaketa

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

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

#### 4.13 Aldaketen kudeaketa teknikoa

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

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

**PROZEDURA:****Entitate hornitzaileentzako informazioaren segurtasunerako araudia**

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.

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

#### 4.14 Garapen-segurtasuna

ZUGAZTELeK kontrolatu eta ikuskatuko du softwarea Erakundetik kanpo garatzeko prozesu osoa.

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

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

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

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

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

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

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

**PROZEDURA:**

Entitate hornitzaileentzako informazioaren segurtasunerako araudia

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

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

Berariaz onartutako softwarea baino ez da bidaliko ekoizpen-ingurunera.

Web zerbitzuei dagokienez, Owasp-en Top 10 kudeaketa hartuko da aintzat.

#### **4.15 Kontingentzien kudeaketa**

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

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

Egungo kontingentzia-plana bideragarria dela frogatu dezake entitate hornitzaileak.

### **5. JARRAIPENA ETA KONTROLA**

---

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



Berrik.: 2

Data: 2018.06.04

Orrialdea: 30.a 30etik

PROZEDURA:	Entitate hornitzaileentzako informazioaren segurtasunerako araudia
------------	--

## 6. DOKUMENTAZIO APLIKAGARRIA

---

- Zugaztelen Plan Estrategikoa.