V. 1 | 2025-03-03

Informazioaren Segurtasun Politika

ONARTZEA ETA INDARREAN JARTZEA

[Urteko] [hilabetean] [egunean] [onartzen duen organoak] onartutako testua.

Informazioaren Segurtasunerako Politika hau eraginkorra da data horretatik politika berri batek ordezten duen arte.

BERTSIOEN KONTROLA

Bertsioa	Indarrean jartzeko data	Berrikuspenaren data	Aldaketaren arrazoia	Onarpena
1.1	…./…./…….		Hasierako edizioa	[Segurtasun Batzordeko lehendakariaren eta idazkariaren sinadura digitala]

Aurkibidea

1. Sarrera

1.1 Informazioaren Segurtasun Politikaren arrazoia

Informazioaren Segurtasun Politika goi-mailako dokumentua da, eta gure erakundean, Bergarako Udalean (aurrerantzean, "Udala"), "Informazioaren segurtasuna" zer esan nahi duen definitzen du.

Dokumentua erakundeko kide guztien eskura egon behar du, modu erraz, zehatz eta ulergarrian idatzita.

Informazioaren Segurtasunerako Politika hau Segurtasun Eskema Nazionala (SEN) arautzen duen maiatzaren 3ko 311/2022 Errege Dekretua (aurrerantzean, “SEN”), ezartzen dituen eskakizunak betez egiten da. SEN araudiak 12. artikuluan ezartzen duenez, Administrazio Publikoek gutxieneko betekizunak adierazten duen segurtasun politika bat eduki behar dute.

Horregatik, SEN araudiak hainbat puntutan aipatzen du Segurtasun Politika:

Bere 12. Artikuluan, gutxieneko segurtasun baldintzak ezartzen dira, hau da:

> *“1. Administrazio publiko bakoitzak segurtasun-politika bat izango du, organo eskudunak formalki onartua.”.*

Gainera, bere 13. Artikulua ezartzen du:

> *"1. Informazio-sistemen segurtasunak erakundeko kide guztiak konprometitu beharko ditu.*
>
> *2. Segurtasun-politika, 11. artikuluan aipatzen den erantzukizunak bereizteko printzipioa aplikatuz eta II. eranskinaren 3.1 atalean zehazten denaren arabera, erakundea osatzen duten pertsona guztiek ezagutu beharko dute, eta zalantzarik gabe identifikatu beharko dituzte politika betetzen dela zaintzeko arduradunak. Pertsona horiek honako eginkizun hauek izango dituzte:*
>
> *a) Informazioaren arduradunak zehaztuko ditu tratatutako informazioaren betekizunak.*
>
> *b) Zerbitzuaren arduradunak zehaztuko ditu emandako zerbitzuen betekizunak.*
>
> *c) Segurtasunaren arduradunak informazioaren eta zerbitzuen segurtasun-baldintzak betetzeko erabakiak zehaztuko ditu, baldintzak betetzen direla bermatzeko beharrezko neurriak ezartzen direla gainbegiratuko du eta gai horiei buruzko informazioa emango du.*
>
> *d) Sistemaren arduraduna arduratuko da, bere kabuz edo baliabide propioen edo kontratatuen bidez, sisteman segurtasuna inplementatzeko modu zehatza garatzeaz eta sistemaren eguneroko eragiketa gainbegiratzeaz, eta bere ardurapeko administratzaile edo operadoreei eskuordetu ahal izango die.. "*

SEN araudiaren helburua Administrazio publikoek bitarteko elektronikoak erabiltzeko behar duten konfiantza sortzea da. Konfiantza hau sistemen, datuen, komunikazioen eta zerbitzu elektronikoen segurtasuna bermatzeko neurrien bidez lortuko da. Horrela, aukera emango zaie, bai aipatutako Administrazio publikoei, bai herritarrei, bitarteko horien bidez eskubideak baliatzeko eta betebeharrak betetzeko.

Horretarako, SEN araudira egokitzeak Udalak eta bertako langileek araudian eskatzen diren segurtasun neurriak aplikatu behar dituztela esan nahi du. Era berean, zerbitzuen prestazio mailen etengabeko jarraipena egitea, ahultasunen jarraipena eta analisia egitea eta gorabeheren aurrean erantzun eraginkorrak presatzea, emandako zerbitzuen jarraitutasuna bermatuz, ere esan nahi du.

Horregatik guztiagatik, Udaleko arlo eta sail guztiek IKT-en segurtasuna sistemaren bizi zikloko etapa bakoitzaren guztizko zatia dela ziurtatu behar dute; sortzen denetik zerbitzua kentzen den arte, garatzeko edo eskuratzeko erabakiak eta ustiapen jarduerak barne.

Era berean, Udaleko sailek prest egon behar dute gertakariak aurreikusteko, antzemateko, eta erantzuteko, baita datuen kontserbaziorako SEN araudiaren 8. artikuluaren arabera.

1.2 Helburua eta emandako zerbitzuak

Udala IKT (Informazio eta Komunikazio Teknologiak) sistemen mende dago bere zerbitzuen zati handi bat emateko, eta beraz, tratatutako informazioa lehen mailako aktiboa da erakundearentzat berarentzat. Ildo beretik, informazioaren eta komunikazioaren teknologia horiek ezinbestekoak bihurtu dira Udalaren eguneroko jardunean.

Bestalde, IKT-ek informazioaren tratamenduari dakarzkioten hobekuntza ukaezinekin batera, arrisku berriak sortzen dira, eta, beraz, beharrezkoa da aipatutako sistemak behar bezalako arduraz administratzea, neurri egokiak hartuz horiek babesteko tratatutako informazioaren eskuragarritasunean, osotasunean edo konfidentzialtasunean eragina izan dezaketen ustekabeko edo nahita eragindako kalteetatik.

Informazioaren segurtasunaren helburua informazioa eta zerbitzuak babestea da, informazioaren kalitatea eta zerbitzuak etengabe ematea bermatuz, prebentzioz jokatuz, eguneroko jarduera gainbegiratuz eta gertaeren aurrean prestutasunez erantzunez.

Udalak, bere eskumenen esparruan eta administrazio publiko gisa, bere interesak kudeatzeko interes orokorrak objektibotasunez ematen ditu eta eraginkortasun, hierarkia, deszentralizazio eta koordinazio printzipioen arabera jarduten du, era guztietako jarduerak sustatzen ditu eta udalerriko biztanleen beharrak eta nahiak asetzen laguntzen duten zerbitzu publikoak ematen ditu.

Segurtasun Politika hau Udalak bitarteko elektronikoen bidez parte hartzen duen jarduerei aplikatzen zaie, zehazki:

- Herritarren eta Udalaren arteko harreman juridiko ekonomikoak.
- Herritarrek Udalaren esku dauden administrazio informazio publikoaren eta administrazio datuen kontsulta.
- Udalaren egoitza elektronikoan izapidetzeko sartutako administrazio izapideak eta prozedurak burutzea.
- Udalaren botereen barnean lortutako informazioaren tratamendua.

2. Arau esparrua eta irismena

2.1 Arau esparrua

Segurtasun politika honen garapenean eta ezarpenean, Udalaren jarduera arautzen duten arauak kontuan hartuko dira, bere eskumenen esparruan, baita datuen, informazioaren eta zerbitzuen eskuragarritasuna, osotasuna, erabilgarritasuna, benetakotasuna, konfidentzialtasuna, trazabilitatea eta kontserbazioa ziurtatzera bideratutakoak ere.

Zehazki, arau esparrua honako arau hauek osatzen dute:

- *Segurtasun Eskema Nazionala (SEN) arautzen duen maiatzaren 3ko 311/2022 Errege Dekretua*. Oinarrizko printzipioak eta gutxieneko baldintzak ezartzen ditu, bai eta Administrazioaren sistemetan ezarri beharreko babes neurriak ere.

- *4/2010 Errege Dekretua, urtarrilaren 8koa,* Administrazio Elektronikoaren eremuan Elkarreragingarritasunaren Eskema Nazionala arautzen duena. Araudi honen helburua Administrazio publikoek erabiltzen dituzten sistemen eta aplikazioen elkarreragingarritasun tekniko, semantiko eta antolamenduzko maila egokia bermatzeko beharrezkoak diren baldintzak sortzea da, zerbitzu publikoetarako sarbide elektronikoaren bidez eskubideak baliatzeko eta betebeharrak betetzeko aukera ematen duena, eta, aldi berean, zerbitzu publikoetarako sarbide elektronikoa izatea. Aldi berean, eraginkortasunaren eta efizientziaren onerako da.

- *2016/679 (EB) Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa,* datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzkoa (aurrerantzean, “DBEO”).

- *3/2018 Lege Organikoa, abenduaren 5ekoa,* Datu Pertsonalak Babesteari eta eskubide digitalak bermatzeari buruzkoa (aurrerantzean, “DBEDBLO”).

- *39/2015 Legea, urriaren 1ekoa,* Administrazio Publikoen Administrazio Prozedura Erkidearena.

- *40/2015 Legea, urriaren 1ekoa,* Sektore Publikoaren Araubide Juridikoarena.

- *Martxoaren 30eko 203/2021 Errege Dekretua,* sektore publikoak bitarteko elektronikoen bidez jarduteko eta funtzionatzeko erregelamendua onartzen duena. .

- *7/1985 Legea, apirilaren 2koa,* Toki-araubidearen oinarriak arautzen dituena, apirilaren 21eko 11/1999 Legeak aldatua.

- *57/2003 Legea, abenduaren 16koa,* tokiko gobernua modernizatzeko neurriei buruzkoa.

- *1/1996 Legegintzako Errege Dekretua,* apirilaren 12koa, Jabetza Intelektualari buruzko Legearen testu bategina onartzen duena.

- *5/2015 Legegintzako Errege Dekretua, urriaren 30ekoa,* Enplegatu Publikoaren Oinarrizko Estatutuaren Legearen testu bategina onartzen duena. .

- *6/2020 Legea, azaroaren 11koa, konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituena.*.
- *19/2013 Legea, abenduaren 9koa,* Gardentasunari, informazio publikoa eskuratzeko bideari eta gobernu onari buruzkoa.
- *34/2002 Legea, uztailaren 11koa,* informazioaren gizartearen eta merkataritza elektronikoaren zerbitzuei buruzkoa.
- *37/2007 Legea, azaroaren 16koa*, sektore publikoko informazioa berrerabiltzeari buruzkoa.
- *25/2007 Legea, urriaren 18koa,* komunikazio elektronikoei eta komunikazio-sare publikoei buruzko datuak gordetzeari buruzkoa.
- *56/2007 Legea, abenduaren 28koa,* Informazioaren Gizartea Bultzatzeko Neurriei buruzkoa.
- 9/2014 Lege Orokorra, maiatzaren 9koa, Telekomunikazioei buruzkoa.
- *9/2017 Legea, azaroaren 8koa, Sektore Publikoko Kontratuena, Europako Parlamentuaren eta Kontseiluaren 2014ko otsailaren 26ko 2014/23/EB eta 2014/24/EB Zuzentarauen transposizioa Espainiako ordenamendu juridikora egiten duena* .
- *14/2019 Errege Lege Dekretua, urriaren 31koa,* administrazio digitalaren, sektore publikoaren kontratazioaren eta telekomunikazioen arloan segurtasun publikoko arrazoiengatik premiazko neurriak hartzen dituena.
- *Ebazpena, 2016ko urriaren 13koa,* Herri Administrazioen Estatu Idazkaritzarena, Segurtasuneko Jarraibide Teknikoa onartzen duena, Segurtasuneko Eskema Nazionalaren arabera.
- *Ebazpena, 2016ko urriaren 7koa,* Herri Administrazioen Estatu Idazkaritzarena, Segurtasunaren Estatuaren Txostenaren Segurtasunerako Jarraibide Teknikoa onartzen duena.
- *Ebazpena, 2018ko martxoaren 27koa,* Funtzio Publikoaren Estatu Idazkaritzarena, Informazio Sistemen Segurtasunaren Auditoretzako Segurtasunaren Jarraibide Teknikoa onartzen duena.
- *Ebazpena, 2018ko apirilaren 13koa,* Funtzio Publikoaren Estatu Idazkaritzarena, Segurtasun-gorabeherak jakinarazteko Segurtasuneko Jarraibide Teknikoa onartzen duena.

Udaleko Administrazio Elektronikoari aplika dakizkieken gainerako arauak ere arau esparruaren parte dira.

Udalaren erantzukizuna izango da eguneratutako araudiaren eranskin bat eguneratuta edukitzea, betiere, nahitaez bete beharreko segurtasun-jarraibide teknikoak barneratuz eta Herri Administrazioen Estatu Idazkaritzaren ebazpen bidez argitaratuaz, Ogasun eta Herri Administrazio Ministerioak onarturik.

Era berean, Udalaren ardura izango da Kriptologia Zentro Nazionaleko (KZN) segurtasun-gidak identifikatzea, Segurtasun Eskema Nazionalean ezarritakoa hobeto bete dadin.

2.2 Irismena

Segurtasun Politika hau udaleko IKT sistema guztiei eta bertako langile guztiei aplikatuko zaie, inolako salbuespenik gabe, beren baliabideei eta SEN araudiak eta DBEOk eragindako prozesuei, kontratu eta/edo akordioen bidez erakundeari lotutakoak, kanpokoak zein barnekoak badira ere.

3. Segurtasun antolaketa

Segurtasunaren antolaketa, sistemen segurtasuneko kudeaketaren arloko jarduera eta erantzukizunen identifikazio eta definizioaren bidez ezartzen da, hauei, euskarria izango duen egitura bat ezarriz.

Oro har, Udaleko informazio-sistemen erabiltzaile guztiak informazio-aktiboen segurtasunaz arduratzen dira, aktibo horiek behar bezala erabiliz, betiere beren eskudantzien arabera, SEN legearen 13. artikuluak adierazten duen bezala.

Segurtasun-gorabeheren aurrean ematen den erantzuna hobetzeko, Udalak lankidetza harremanak izango ditu agintari eskudunekin, informatika edo komunikazio zerbitzuen hornitzaileekin eta informazio sistemen segurtasuna sustatzen duten erakunde publiko edo pribatuekin.

3.1 Segurtasun Egitura

Udalaren organigramaren barnean hiru (3) maila bereiz ditzakegu, maila horiek, erantzukizun bloke desberdinak izango dituzte:

Gobernu – Maila:

Erakundearen eginkizuna ulertzen du, lortu nahi diren helburuak zehazten ditu eta horiek lortzeko erantzuna ematen du.

Maila honi, legezko erantzukizuna dagokio, bai eta beharrak zehazteko erantzukizuna ere.

Gainbegiratze – Maila

Kudeaketa unitate bakoitzaren zeregina ulertzen duten zerbitzuak dira, bai eta unitateak nola koordinatzen diren ezarritako helburuak lortzeko.

Eragiketa – Maila:

Jarduera zehatzetan ardazten da, gauzak nola egiten diren kontrolatuz.

3.2 Rolen definizioa

Ildo beretik, SEN legearen II. Eranskineko 3.1 atalean zehazten den moduan, Segurtasun Politikak, **erakundeko langile guztiek ezagutu behar dituzten arduradun argi batzuk identifikatzen ditu, araudia betetzen dela zaindu beharko duten arduradunak izango direnak.**

Zentzu honetan, Informazioaren Segurtasunarekin lotutako honako rol hauek ezartzen dira erakundean maila bakoitzarekiko:

Gobernu – Maila:

3.2.1 Informazioaren eta zerbitzuaren Arduraduna

Informazioaren eta zerbitzuaren Arduraduna Udaleko Alkatea izango da.

Informazioaren eta zerbitzuaren arduradunak Udaleko zerbitzuen bidez emandako informazioari buruzko betekizunak ezarriko ditu, eta, beraz, azken hitza izango du informazio eskuragarriaren mota eta eman dakiokeen erabilera erabakitzeko orduan, betiere, indarrean dagoen araudiari eta datuen babesaren arloko jardunbide egokiei jarraiki.

Honako eginkizun hauek dagozkio:

- Datu pertsonalen tratamenduen segurtasuna bermatuko duten neurri teknikoak eta antolamendukoak hartzea, datu horiek galtzea, aldatzea, tratatzea edo baimenik gabe eskuratzea saihestuaz eta, betiere, teknologiaren egoera, biltegiratutako datuen izaera eta arriskuak kontuan harturik, giza ekintzatik edo ingurune fisiko edo naturaletik erator daitezkeelarik.

- Informazio edo zerbitzu jakin bat erabiltzearen eta, beraz, babestearen azken erantzukizuna du.

- Segurtasunaren arloko informazioaren gutxiengo betekizunak ezartzea, SEN araudiaren esparruan, informazioaren segurtasun-mailak zehazteko ahalmenaren baliokidea da.

- Dimentsio bakoitzeko segurtasun-mailak zehaztea, Segurtasun Eskema Nazionalaren I. Eranskinean ezarritako esparruaren barruan.

- Informazioari eragiten dioten hondar-arriskuaren mailak onartzea.

- Mailen onarpen formala Informazioaren eta Zerbitzuaren arduradunari badagokio ere, Informazioaren Segurtasunerako Batzordearen proposamenpean egingo du.

- Zerbitzuek segurtasunaren arloan bete beharreko baldintzak ezartzea, SEN araudiaren esparruan, informazioaren segurtasun-mailak zehazteko ahalmenaren baliokidea izango dena.

- Informaziorako Segurtasun Batzordearen funtzionamendua zehaztea eta SEN-k aurreikusitako rolak esleitzea.

- Hobekuntza plana onartzea.

Gainbegiratze – Maila

3.2.2 Segurtasunaren Arduraduna

Digitalizazio eta antolakuntza arduradunak Udaleko Segurtasunaren Arduradunaren rola izango du, eta eginkizun hauek izango ditu:

- Maneiatutako informazioaren eta IKT sistemek emandako zerbitzuen segurtasuna eustea.

- Erakundeak segurtasunaren arloan dituen betebeharrak betetzen direla egiaztatzeko aukera ematen duten aldizkako auditoriak egitea.
- Informazioaren segurtasunari buruzko prestakuntza eta kontzientziazioa sustatzea, bere erantzukizun-eremuaren barruan.
- Ezarritako segurtasun-neurriak, erabilitako informazioa eta emandako zerbitzuak babesteko egokiak direla egiaztatzea.
- Sistemen segurtasunarekin lotutako dokumentazio guztia onartzea.
- Sistemen segurtasun-egoeren monitorizazio eta auditoretza txostenak egiaztatzea.
- Segurtasun-gertakarien ikerketa babestu eta gainbegiratzea, jakinarazten direnetik ebazten diren arte eta kanpo erakundeekin bitartekari lana egitea.
- Segurtasun Batzorderako aldizkako segurtasun-txostena egitea eta Informazioaren Segurtasun Batzordeari aurkeztea, aldi horretako gertakari garrantzitsuenak barneraturik.
- Sistemen Arduradunek egindako segurtasun-prozedurak onartzea, edukiaren arabera Segurtasun Batzordearen onespenik behar ez denean.
- Formalizatu beharrekotzat jotzen duen Udaleko segurtasun araudiaren idazketa proposatzea.
- Sistemaren kanpoko edo barruko berrikuspenak kudeatzea eta auditorien kasuan bitartekari aritzea.
- Ziurtapen-prozesuak kudeatzea.
- Sistemaren aldaketen eta bestelako eskakizunen onarpena Segurtasun Batzordeari helaraztea.
- Arriskuen analisia eta aplikagarritasun adierazpena egiteko arduradunak izendatzea, segurtasun-neurriak identifikatzea, beharrezko konfigurazioak zehaztea eta sistemaren dokumentazioa egitea.
- Segurtasuna hobetzeko planak egiten eta ezartzen parte hartzea, eta, hala badagokio, jarraipen-planetan parte hartzea, eta baliozkotzea.
- Sistemen kategorizazioa eta segurtasun-baldintzak zehaztea, SEN araudiari lotutako zerbitzu berri bat abian jarri aurretik.

Eragiketa – Maila:

3.2.3 Sistemaren Arduraduna

Informatika teknikaria, Udaleko Sistemaren Arduradunaren rola izango du, eta eginkizun hauek izango ditu:

- Informazio Sistemaren bizi-ziklo osoa garatzea, lantzea eta mantentzea, bai eta haren zehaztapenak, instalazioa eta funtzionamendu egokia egiaztatzea ere.
- Segurtasun-prozedura operatiboen aplikazioa egiaztatzea informazio-sistemetan.
- Sistemaren erabiltzaileei emandako baimenak kudeatzea, bereziki emandako pribilegioak, sisteman garatutako jardueraren monitorizazioa eta baimendutakoarekin bat etortzea barne.
- Informazio sistemaren indarreko konfigurazioaren aldaketak onartzea.
- Hardwareko eta softwareko instalazioak, horien aldaketak eta hobekuntzak gainbegiratzea, segurtasuna arriskuan ekiditeko eta uneoro ezarritako prozeduretara egokitu ahal izateko
- Sistemen segurtasunaren egoera ikuskatzea.
- Segurtasunarekin zerikusia duen edozein anomalia, konpromiso edo kalteberatasunen berri ematea segurtasun-arduradunari.
- Segurtasun gorabeherak ikertzen eta ebazten laguntzea, detektatzen direnetik ebazten diren arte.
- Segurtasunaren Arduradunei aholkuak ematea, ezarritako segurtasun-baldintzak bete daitezen.

3.2 Informazioaren Segurtasunerako Batzordea

Informazioaren Segurtasunerako Batzordeak (aurrerantzean, "Segurtasun Batzordea") informazioaren segurtasuna koordinatzen du antolakuntza mailan.

Aparteko bilerak deitu ahal izango dira, larritasunak edo egoera zehatzak hala eskatzen duten bakoitzean.

Segurtasun Batzordeak eginkizun hauek izango ditu:

- Udalaren eta haren arlo, unitate eta zerbitzuen **Informazio Segurtasunaren arloko kezkei erantzutea**, Alkatetzari aldizka Informazioaren Segurtasunaren egoeraren berri emanaz.
- **Informazioaren Segurtasunaren arloko aholkularitza ematea**, betiere, eskatzen zaionean eta erabaki behar duenean edo iritzia eman behar duen kasuetan. Aholkularitza hau kasu-kasu zehaztuko da, hainbat modu desberdinetan gauzatu ahal izango delarik:
    - Barneko, kanpoko edo mistoak izan daitezkeen lantalde espezializatuak.
    - Barneko eta/edo kanpoko aholkularitza
- **Arduradunen artean eta/edo Udaleko arlo/unitate/zerbitzuen artean sor daitezkeen erantzukizun gatazkak ebaztea**, erabakitzeko autoritate nahikorik ez duten kasuak aurkeztu eta jasoaz.

- **Informazioaren Arduradunen eginkizunak eta betebeharrak eta SEN zerbitzuak jasotzea**, eskatzen zaizkion eta/edo beharrezkotzat jotzen diren zeharkako ekintzetan.

- **Informazioaren Segurtasuna kudeatzeko sistemaren etengabeko hobekuntza sustatzea**. Horretarako, honako hauek egingo ditu:

    - Ahaleginen Koordinazioa: Arlo/unitate/zerbitzuek Informazioaren Segurtasunaren arloan egiten dituzten ahaleginak koordinatzea, arlo/unitate/zerbitzu horiek sendoak direla ziurtatzeko, gai horretan erabakitako estrategiarekin bat datozela, eta bikoiztasunak saihesteko.
    - Hobekuntza planak proposatzea: Udaleko informazioaren segurtasuna hobetzeko planak proposatzea, dagokion aurrekontu zuzkidurarekin, eta lehentasuna ematea segurtasun-arloko jarduerei, baliabideak mugatuak direnean.
    - Informazioaren Segurtasuna zaintzea: Proiektu guztietan informazioaren segurtasuna kontuan hartzen dela zaintzea, hasierako zehaztapenetik abian jarri arte (Privacy by Design). Bereziki, zerbitzu horizontalak sortzen eta erabiltzen direla zaindu beharko du, bikoiztasunak murrizteko eta IKT sistema guztien funtzionamendu homogeneoa bultzatzeko.
    - Arrisku nagusien jarraipena egitea: Udalak bere gain hartutako hondar-arrisku nagusien jarraipena egitea eta arrisku horiei dagokienez egin daitezkeen jarduerak gomendatzea.

- **Informazioaren Segurtasun Politika egitea (eta aldizka berrikustea**), Udaleko Alkateak onar dezan.

- **Informazioaren segurtasunari buruzko araudia prestatzea,** Udalarekin koordinatuta onar dadin.

- **Informazioaren eta gainerako dokumentazioaren segurtasun prozedurak egokiak direla egiaztatzea.**

- **Langileak informazioaren segurtasunaren eta, bereziki, datu pertsonalen babesaren arloan prestatzeko eta sentsibilizatzeko prestakuntza programak prestatzea edo proposatzea.**

- **Administratzaile, operadore eta erabiltzaileen prestakuntza eta kalifikazio baldintzak prestatzea eta onartzea,** informazioaren segurtasunaren ikuspegitik.

- Udalaren segurtasun-arloko betebeharrak betetzen direla egiaztatzeko **SEN araudiaren eta DBLO-REN aldizkako auditoriak sustatzea.**

SEN-k aurreikusitako rolen eta Batzordearen funtzionamendu araudia Alkate dekretuz zehaztu eta onartuko dira.

4. Datu pertsonalak

Udalak datu pertsonalak erabiltzen dituen tratamenduak egiten ditu, betiere, DBEOren gidalerroak eta DBO pertsonaren jarraibideak betetzeko beharrezko segurtasun-neurriak hartuz. Honela, egungo segurtasun-araudiak ezartzen duen erantzukizun proaktiboaren eta accountability-aren printzipioak betetzeko behar besteko arreta mantentzen dela bermatzen da.

Era berean, Udalak egokiak, beharrezkoak eta ezinbestekoak diren datuak soilik jasoko ditu, eta betiere, datu horiek lortu diren alorrarekin eta helburuekin lotuta daudenean. Zentzu berdinean, datu horiek Udaleko Tratamenduko Jardueren Erregistroan erregistratuko dira.

Bere ardurapeko tratamendu-eragiketetan sartutako datu pertsonalen segurtasuna kudeatzeaz eta mantentzeaz Udaleko sail bakoitza arduratuko da.

Informazio sistema guztiak araudiak datu pertsonalen izaera eta helbururako eskatzen dituen segurtasun-mailetara egokituko dira, Tratamendu Jardueren Erregistroan jasotako helburuei loturik.

5. Arriskuen kudeaketa

5.1 Justifikazioa

Segurtasun politika honen mende dauden sistema guztiei arriskuen analisia egingo zaie, horien eraginpean dauden mehatxuak eta arriskuak ebaluatuz. Informazioaren segurtasunaren gobernua eta kudeaketa arriskuak aztertzeko eta kudeatzeko prozesuen emaitzen arabera gidatuko dira. Azterketa hau errepikatu egingo da:

- Urtero gutxienez.
- Informazioa eta/edo erabilitako zerbitzuak nabarmen aldatzen direnean.
- Segurtasun gorabehera larriren bat gertatzen denean edo urrakortasun larriak antzematen direnean.

5.2 Arriskuak ebaluatzeko irizpideak

Arriskuen analisiak bateratzeko, Informazioaren Segurtasunerako Batzordeak erabilitako informazio mota ezberdinetarako eta emandako zerbitzu ezberdinetarako erreferentziazko balorazio bat ezarriko du.

Arriskuak ebaluatzeko irizpide zehatzak erakundeak egingo duen arriskuak ebaluatzeko metodologian zehaztuko dira, onartutako estandarretan eta jardunbide egokietan oinarrituta.

Gutxienez, zerbitzuak ematea edo erakundearen eginkizuna modu larrian betetzea eragotz dezaketen arrisku guztiak tratatu beharko dira.

Herritarrei zerbitzuak emateari uztea dakarten arriskuak bereziki lehenetsiko dira.

5.3 Tratamendurako jarraibideak

Segurtasun Batzordeak sistemen segurtasun beharrei erantzuteko baliabideen eskuragarritasuna dinamizatuko du, inbertsio horizontalak sustatuz.

5.4 Hondar arriskua

Segurtasun arduradunak zehaztuko ditu hondar arriskuak.

Aurreikusitako tratamendu aukerak ezarri ondoren (SEN araudiaren II. eranskinean aurreikusitako segurtasun neurriak ezartzea barne), informazio bakoitzean espero diren hondar arriskuen mailak aldez aurretik onartu beharko ditu informazio arduradunak.

Aurreikusitako tratamendu aukerak ezarri ondoren (SEN araudiaren II. eranskinean aurreikusitako segurtasun neurriak ezartzea barne) zerbitzu bakoitzean espero diren hondar arriskuen mailak aldez aurretik onartu beharko ditu zerbitzuko arduradunak.

Segurtasun arduradunak Segurtasun Batzordeari aurkeztuko dizkio hondar arriskuen mailak, honek proposatutako tratamendu aukerak ebaluatu, onetsi edo zuzendu ditzan.

5.5 Arriskuen ebaluazioak egitea edo eguneratzea

Arriskuen analisia egiteko, Administrazio Publikoaren eremurako argitaratutako gomendioak hartuko dira kontuan, eta, bereziki, Kriptologia Zentro Nazionalak (KZN) egindako gidak. Arriskuen ebaluazio hori aldizka errepikatuko da informazio sistemetarako, aipatutako zentroak emandako gomendioak kontuan hartuta.

Udalak konpromisoa hartu du eta informazioaren arduradunek betebeharra hartu dute arriskuen analisiak egiteko eta ondorioei erantzuteko. Politika honen mende dauden sistema guztiek arriskuen analisia egin beharko dute, aktiboen mehatxuak eta arriskuak ebaluatuz.

Era berean, arriskuen analisiak eta horien tratamenduak erregulartasunez errepikatutako jarduera izan behar dute, SEN araudiaren 10. artikuluan ezarritakoaren arabera. Azterketa hori errepikatu egingo da:

- Erregularki, gutxienez urtean behin.
- Erabilitako informazioan aldaketa esanguratsuak gertatzen direnean.
- Emandako zerbitzuetan aldaketa esanguratsuak gertatzen direnean.
- Informazioa tratatzen duten eta zerbitzuak ematean esku hartzen duten sistemetan aldaketa esanguratsuak gertatzen direnean.
- Segurtasun gorabehera larriren bat gertatzen denean.
- Urrakortasun larriak daudenean.

6. Segurtasun gertakarien kudeaketa

6.1 Prebentzioa

Udalak informazioa edo zerbitzuak kaltetu dezaketen segurtasun gertakariak, ahal duen neurrian, prebenitu eta saihestu behar ditu. Horretarako, zuzendaritza organoek, SEN arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuak zehaztutako gutxieneko segurtasun-neurriak inplementatu behar dituzte, baita mehatxuen eta arriskuen ebaluazioaren bidez identifikatutako edozein kontrol gehigarri ere. Kontrol hauek, eta langile guztien segurtasun rol eta erantzukizunak argi zehaztuta eta dokumentatuta egon beharko dira.

Politika betetzen dela bermatzeko, Udalak:

- Eragiketa hasi aurretik, dagokion sistema baimentzen du.
- Segurtasuna aldian-aldian ebaluatzen du, ohiko konfigurazio-aldaketen ebaluazioak barne.
- Hirugarrenek aldian behin berrikustea eskatzen du, ebaluazio independente bat lortzeko.
- Informazio kritikoko edo konfidentzialeko sistemetarako eremu seguruak ezartzea.

6.2 Monitorizazioa eta detekzioa

Udalak bere informazio sistemen eragiketa kontrolak ezartzen ditu, zerbitzuak ematean anomaliak detektatzeko eta horren arabera jarduteko, SEN araudiko 10. artikuluan ezarritakoaren arabera (etengabeko zaintza eta aldizkako berrebaluazioa). Aurrez normaltzat ezarri diren parametroen desbideratze esanguratsua gertatzen denean (SEN araudiaren 9. artikuluan adierazitakoaren arabera). Defentsa-lerroen existentzia), behar diren detekzio, analisi eta txosten mekanismoak ezarriko dira, aldian-aldian arduradunengana irits daitezen.

Sarkinak detektatzeko sistemek, funtsean, erakundearen baliabideak gainbegiratzen eta ikuskatzen dituzte, segurtasun politika ez dela urratzen egiaztatuz eta edozein jarduera maltzur, modu goiztiar eta eraginkorrean, identifikatzen saiatuz,.

Beharren arabera, sailkapen hauek ezarri beharko dira:

- Sarkinak sare mailan detektatzeko sistemak.
- Sarkinak sistema mailan detektatzeko sistemak.

6.3 Erantzuna

Udalak ondorengo neurri hauek ezarriko ditu:

- Segurtasun gertakariei eraginkortasunez erantzuteko mekanismoak.
- Beste sail batzuetan edo beste erakunde batzuetan antzemandako gertakariei buruzko komunikazioetarako harremanetarako puntu edo gune bat izendatzea.
- Gertakariarekin lotutako informazioa trukatzeko protokoloak ezartzea. Horren barruan sartzen dira, bi noranzkoetan, Larrialdiei Erantzuteko Taldeekin (CERT) egindako komunikazioak.

6.4 Berreskurapena

Zerbitzuen erabilgarritasuna bermatzeko, Udalak zerbitzu kritikoenak berreskuratzea bermatzeko beharrezko bitarteko eta teknikak ditu. Hauek Udalaren Segurtasun Dokumentuan jasotako prozedurak eta arauak direlarik.

7. Langileen betebeharrak eta erantzukizunak

Informazio sistemetara sarbidea duten langile guztiek informazioaren segurtasun politika eta ezarritako segurtasun araudia ezagutu eta bete behar dituzte.

Horretarako, informazioaren segurtasun politika modu egoki, irisgarri eta ulergarrian jakinaraziko zaie administrazio elektronikoaren eremuko informazio sistemen erabiltzaile guztiei. Ez betetzea dagokion diziplina araudiaren arabera zehatu ahal izango da.

Era berean, azpikontratatutako kanpoko enpresetako langileek, udalaren zerbitzuren bati lotutako dokumentazioa edo informazioa eskuratu ahal badute, informazioaren segurtasun politika hori ezagutu eta bete beharko dute.

Informazioaren eta komunikazioaren teknologia sistemak erabiltzen dituzten langile guztiek sistema horiek segurtasunez erabiltzeko prestakuntza jasoko dute. Politika hori benetan betetzen dela bermatuko duten kontrol prozedurak ezarri beharko dira. Prozedura horiek udaleko arlo, sail eta zerbitzuek eta erakunde autonomoek egingo dituzte.

Jarraian, erakundeko langile guztien **erantzukizunak** zehaztuko dira:

- Langileak gorabehera oro jakinarazteko ardura izango du, gorabeherak kudeatzeko prozeduraren arabera. Gorabehera bat ez jakinaraztea langileen betebeharraren ez-egitetzat hartuko da.
- Langileak bere identifikatzailearekin eta pasahitzarekin egiten diren sarbide guztien ardura izango du; beraz, ez du pasahitza jakinaraziko.
- Langilea, lanpostua uzten badu, saioa ixteaz edo pasahitza duen ekipoa blokeatzeaz arduratuko da.
- Enplegatua erakundeari lotutako datu pertsonalen eranskinak dituzten mezu elektroniko guztien kopiak gordetzeaz arduratuko da.
- **Mahai garbiaren politika** betetzeko betebeharra izango du.

Ildo beretik, informazio sistemak eta informazioa bera enplegatuek hasieran sortu diren eta pertsona horiei jakinarazi zaizkien helburuetarako bakarrik erabili ahal izango dituzte.

Horrenbestez, **ez da onargarritzat jotzen**:

- Datuak babesteko edo jabetza intelektualeko legeak urratuz materiala sortzea edo transmititzea, bai eta erakundearen datu pertsonalak eta konfidentzialak zabaltzea ere. Informazioa isilpean gordetzeko betebeharra du, baita lan harremana amaituta ere.
- Software sistemen konfigurazioa instalatzea, aldatzea edo ordezkatzea (sistema administratzaileek bakarrik dute horretarako baimena).
- Internet helburu pertsonaletarako erabiltzea (webgunean oinarritutako posta elektroniko pertsonala barne) baimendutako atseden denboretara mugatuko da. Egiten den edozein transakzio elektroniko pertsonal erabiltzaileen ardurapean egongo da.
- Instalazioetarako edo zerbitzuetarako sarbidea baimendu gabeko pertsonei nahita erraztea.
- Sareko baliabideak aldez aurretik pentsatuta xahutzea.
- Beste erabiltzaile batzuen datuak galtzea edo suntsitzea, edo pribatutasuna nahita urratzea.
- Birusak edo nahita egindako software maltzurraren beste forma batzuk sartzea. Informazioa biltegiratzeko edozein bitarteko erabili aurretik, birusik edo antzekorik ez dagoela egiaztatu beharko da.

- Pasahitzak eta bitartekoetan sartzekoak borondatez jakinaraztea.
- Ekipokoak onura pertsonalerako erabiltzea.
- Material iraingarria, lizuna edo mingarria sortzea, erabiltzea edo transmititzea.
- Posta-mezu oso handiak edo jende askori bidaltzea (komunikazioak gainezka jarri ahal izateko).
- Mezuek birusik ez dutela ez egiaztatzea.

8. Hirugarrenak

Udalak beste erakunde batzuei zerbitzuak ematen dizkienean edo beste erakunde batzuen informazioa erabiltzen duenean, Informazioaren Segurtasunerako Politika honen partaide egingo dira. Informazioaren Segurtasun Batzordeak informatzeko eta koordinatzeko kanalak ezarriko dira, eta segurtasun gorabeheren aurrean erantzuteko jarduketa prozedurak ezarriko dira.

Udalak hirugarrenen zerbitzuak erabiltzen dituenean edo hirugarrenei informazioa ematen dienean, zerbitzu edo informazio horiei eragiten dien segurtasun politika eta segurtasun araudia jakinaraziko zaie. Hirugarren partea araudi horretan ezarritako betebeharren mende geratuko da, eta araudi hori betetzeko bere prozedura operatiboak garatu ahal izango ditu. Gorabeherak jakinarazteko eta konpontzeko prozedura espezifikoak ezarriko dira. Hirugarren parteetako langileak segurtasun arloan behar bezala kontzientziatuta daudela bermatuko da, gutxienez segurtasun politika honetan ezarritako maila berean.

Era berean, erakunde publikoei zerbitzuak ematen dizkieten edo konponbideak ematen dizkieten sektore pribatuko operadoreek, baldin eta Segurtasun Eskema Nazionala betetzea eska badaiteke, SEN araudiarekiko Egokitasun Adierazpena erakusteko moduan egon beharko dira, betiere, OINARRIZKO kategoriako sistemak direnean, edo kategoria ERTAIN edo ALTUKO sistemak direnean, SEN araudiarekiko Egokitasun Ziurtagiria erakusteko moduan.

Aurreko paragrafoetan eskatzen denaren arabera, segurtasun politika honen alderdiren bat hirugarren batek ezin badu bete, segurtasun arduradunaren txosten bat beharko da, arriskuak zeintzuk diren eta nola tratatuko diren zehazteko. Aurrera jarraitu aurretik, informazioaren arduradunek eta eragindako zerbitzuek txosten hori onartu beharko dute.

9. Segurtasun politikaren garapena

Segurtasun Batzordeak informazioaren segurtasun politika berrikusiko du planifikatutako denbora tarteetan, edo aldaketa esanguratsuak gertatzen diren guztietan, hauen egokitasunari, egokitasunari eta eraginkortasunari eusten zaiola ziurtatzeko.

Segurtasun araudia ezagutu behar duten erakundeko langile guztien eskura dago, bereziki informazio eta komunikazio sistemak erabiltzen, lan egiten edo administratzen dituztenen eskura, eta araudi horren gaineko edozein aldaketa eragindako alderdi guztiak zabaldu beharko zaizkie.

9.1 Giza baliabideen kudeaketaren segurtasuna

Langileei lotutako segurtasuna ezinbestekoa da giza akatsak, lapurretak, iruzurrak edo instalazioak eta zerbitzuak gaizki erabiltzeko arriskuak murrizteko. Hori dela eta, giza baliabideen arduradunek SEN araudiari eta segurtasun politika honetan ezarritakoari erreparatu behar diote, eta segurtasun neurri egokiak hartu behar dituzte, hala nola enplegatu guztiekin konfidentzialtasun hitzarmen bat sinatzea, isilpeko informazioa zabaltzea saihesteko.

Segurtasun arloko politika eta prozedura guztiak aldizka jakinarazi behar zaizkie langile guztiei eta, hala badagokio, hirugarrenei. Langileen edo kanpoko langileen lan harremana edo kontratu harremana amaitzen denean, instalazioetan sartzeko baimenak eta informazioa kentzen zaizkie, eta lanak egiteko eman zaien edozein informazio edo ekipo itzultzeko eskatzen zaie.

9.2 Segurtasun fisikoa eta ingurunearen segurtasuna

Instalazio fisikoek hainbat babes neurri izan ditzakete: oztopo fisikoak, zaintza neurri teknikoak, inteligentzia sistemak eta zaintzaileak eta/edo segurtasun langileak.

Segurtasun logikoaren eraginkortasuna ziurtatzeko, segurtasun fisiko zuzenetik hasi behar da; hori baimenik gabeko sarbiderik, kalterik edo sarbiderik ez gertatzeko modua baita.

Horretarako, Udalak instalazioetarako sarbide baimendua bermatzen du eta bertan dauden baliabideak bermatzeko oztopo fisikoak ditu.

9.3 Komunikazioen eta eragiketen kudeaketa

Udalak sarearen erabilera maltzurra saihesten du, eta horretarako, sare zerbitzuetarako sarbidea kontrolatzen du, bai barnekoak bai kanpokoak, erabiltzaileek zerbitzu horiek arriskuan jar ez ditzaten. Ildo horretan, sareko baliabideak nork eskura ditzakeen jakiteko baimen prozedurak eta sarerako sarbideak babesteko kudeaketa prozedurak erabiltzen dira.

Egin beharreko prozedura guztiak behar bezala dokumentatuta daude, eta hasieran ezarritako aldaketak nabarmen aldatzen badira, berrikusi eta behar bezala aldatuko dira.

Gorabeherarik izanez gero datuak berreskuratzeko artxibatu egiten diren segurtasun kopiak egiteko prozedurak daude. Beraz, datuak zerbitzarietan gordetzen dira, normalean segurtasun kopiak egiten direla ziurtatzeko. Informazioa ordenagailu baten disko gogorrean gordetzen bada, ordenagailu horri esleitutako

erabiltzailea segurtasun kopiak egiteaz arduratuko da. Kopia horiek argi eta garbi identifikatuta daude eta leku seguruan gordetzen dira.

10. Sarbideen kontrola

Informazio sistemarako sarbidea behar bezala baimendutako erabiltzaile, prozesu, gailu eta bestelako informazio sistemetara mugatzen da, baimendutako eginkizunetarako sarbidea murriztuz. Horrela baino ezin da ziurtatu informazioa baimenik gabeko sarbideetatik babestea. Zerbitzuaren arduraduna informazioa eskuratzeko beharrak definitzeaz arduratzen da, arlo guztiei dagozkienak eta erabiltzaile bakoitzari dagozkionak bereiziz.

Langileei egin beharreko jarduera garatzeko beharrezkoa den informazioa baino ez zaie ematen. Udalak baliabideen segurtasuna ziurtatuta dagoela uneoro zaindu behar du.

10.1 Erabiltzaileen erantzukizuna

Udaleko langileek, baimendu gabeko sarbideen eta balizko kalteen arriskuak saihesteko eta murrizteko prebentzioz jardun behar dute. Horretarako, erabiltzaileek honako hauek egin behar dituzte, besteak beste:

- Paperak eta informazioa biltegiratzeko beste bitarteko batzuk libre edukitzea.
- Informazioa leku itxietan gorde (batez ere lan ordutegitik kanpo).
- Ekipo informatikoak konfiguratu, erabiltzailea bere lanpostuan ez dagoenean blokeatuta gera daitezen.
- Posta, faxa eta inprimagailu makinak, eskanerrak eta abar sartzeko eta irteteko puntuak babestu.

11. Dokumentazio osagarria

Informazioaren Segurtasunerako Politika hau hainbat araudi eta segurtasun gomendioren bidez osatuko da (politikak, protokoloak, prozedurak, jarraibide teknikoak, Jardunbide Egokien Dekalogoa, etab.).

Era berean, Informazioaren Segurtasunerako Politika honek Udalak datu pertsonalak babesteko dituen segurtasun politikak osatzen ditu.

Segurtasun araudia ezagutu behar duten erakundeko langile guztien eskura egongo da, batez ere informazio eta komunikazio sistemak erabiltzen, lan egiten edo administratzen dituztenen eskura.

Hemen kontsultatu ahal izango duzu: https://www.bergara.eus/eu/Lege-informazioa