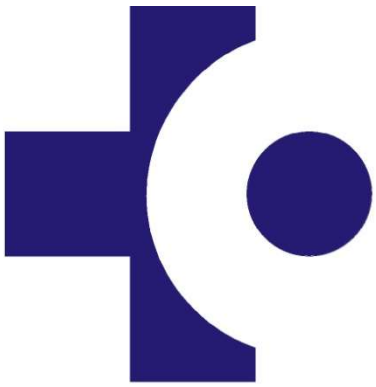

Osakidetza

SEN-NJP

Informazioaren Segurtasunari Buruzko Gidalerroa

Bertsioa: v2.0

Data: 2023/01/19

KONTROL-ORRIA

Izenburua	SEN-NJP Informazioaren Segurtasunari Buruzko Gidalerroa		
Fitxategiaren izena	Informazioaren Segurtasunari Buruzko Gidalerroa		
Egilea			
Zerbitzu-erakundea	Zuzendaritza Nagusia		
Bertsioa/Edizioa	2.0	**Bertsio-data**	23/01/19
Nork onartua		**Onarpen-data:**	uu/hh/ee
		Orrialdeak guztira	30

ALDAKETEN ERREGISTROA

Bertsioa	Aldaketaren arrazoia	Aldaketaren arduraduna	Eremua	Aldaketaren data
1.0	Dokumentua sortzea	SA	Gobernantza	2012/04/15
1.4	Esparru juridikoa aldatzea	SA	Gobernantza	2016/09/06
2.0	Aldaketa	SA	Gobernantza	2023/01/19

BANAKETA-KONTROLA

Izen-abizenak	Kargua	Eremua	Kopia kopurua
Publikoa			

ALDAKETA AIPAGARRIAK (AURREKO BERTSIOTIK)

- Esparru juridikotik arau-esparrura aldatzea eta edukia eguneratzea.
- IKT baliabidea birdefinitzearekin lotutako helmen-aldaketak.
- Aldaketak datu pertsonalen tratamendua gehitu den aplikazio-eremuan.
- Puntu berriak eta hainbat aldaketa gehitu dira oinarrizko segurtasun-printzipioen barruan.

- Informazioaren arduradunen, segurtasunaren arduradunaren eta sistemaren arduradunaren erantzukizunak eguneratzea.
- Datu pertsonalen babesa prestakuntzaren eta kontzientziazioaren barruan sartzea.
- Atal berriak sartzea.

INDIZEA

1 SARRERA ETA INFORMAZIOAREN SEGURTASUNARI BURUZKO GIDALERROAREN HELBURUAK

Dokumentu honen helburua da zehaztea Osakidetzak kudeatzen eta babesten duen informazioa eta ematen dituen zerbitzuak nola kudeatzen eta babesten dituen.

Osakidetzak, bere garaian, informazioaren segurtasuna kudeatzeko esparru bat ezarri zuen, Segurtasun Eskema Nazionala arautzen duen urtarrilaren 8ko 3/2010 Errege Dekretuaren arabera. Segurtasun Eskema Nazionala (aurrerantzean, SEN) arautzen duen maiatzaren 3ko 311/2022 Errege Dekretua argitaratzearen ondoriozko arau-esparruaren bilakaera dela-eta, Osakidetzak informazioaren segurtasun-politika eta kudeaketa-sistema eguneratu eta egokitu ditu.

Segurtasun Eskema Nazionala osatzen dute tratatutako informazioa eta haren aplikazio-eremuko erakundeek ematen dituzten zerbitzuak behar bezala babesteko beharrezkoak diren oinarrizko printzipioek eta gutxieneko eskakizunek, beren eskumenak baliatuz kudeatzen dituzten bitarteko elektronikoen bidez erabilitako datuen, informazioen eta zerbitzuen sarbidea, osotasuna, erabilgarritasuna, benetakotasuna, konfidentzialtasuna, trazabilitatea eta kontserbazioa bermatzeko.

Erreferentzia-esparru hori ezartzearen xedea da langile publikoek eta herritarrek zerbitzuak kudeaketa-ingurune seguru batean eskuratu ahal izateko oinarriak finkatzea, haien beharrei aurrea hartuz eta haien eskubideak babestuz.

Informazioaren segurtasunari buruzko gidalerroan mehatxuetatik babesten du, informazio-sistemen jarraitutasuna bermatzeko, kalte-arriskuak minimizatzeko eta Osakidetzaren helburuak eraginkortasunez betetzen direla bermatzeko.

Segurtasuna prozesu integrala da, eta informazio- eta komunikazio-sistemekin zerikusia duten elementu tekniko, giza elementu, material, juridiko eta antolakuntzakoak biltzen ditu. Segurtasuna ez da produktu bat, baizik eta egokitzeko eta hobetzeko etengabeko prozesu bat, kontrolatu, kudeatu eta monitorizatu behar dena, Osakidetzan segurtasunaren kultura ezarriz eta mantenduz.

Informazioaren segurtasuna kudeatzeko esparruak datu pertsonalen babesa ere barne hartzen du, eta kontuan hartzen du Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/679 (EB) Erregelamenduan (aurrerantzean, DBEO) xedatutakoa, bai eta arlo horretako legeria nazional eta autonomikoan jasotakoa ere.

Informazioaren segurtasunaren kudeaketak bermatu behar du azpiegitura eta instalazio orokorrak kontrolatzeko, monitorizatzeko eta mantentzeko jarduerek behar bezala funtzionatzen dutela, zerbitzuak behar bezala emateko beharrezkoak baitira, bai eta haien funtzionamendutik eratorritako informazioak ere. Horretarako, helburu orokor hauek ezartzen dira informazioaren segurtasunaren arloan:

- Informazioaren segurtasunaren kudeaketatik Osakidetzak ezarritako misioa eta helburuak betetzen laguntzea.

- Garatutako jardueraren ondorioz aplikatu beharreko legezko baldintzak betetzeko behar diren kontrol-neurriak izatea, bereziki datu pertsonalak babesteari eta zerbitzuak bitarteko elektronikoen bidez emateari dagokienez.
- Informazioaren sarbidea, osotasuna, konfidentzialtasuna, erabilgarritasuna, benetakotasuna, trazabilitatea eta zerbitzuak etengabe ematea ziurtatzea, prebentzioz jardunez, eguneroko jarduera gainbegiratuz eta gorabeherei aurre eginez.
- Osakidetzaren informazio-baliabideak eta horiek prozesatzeko erabiltzen den teknologia nahita edo nahi gabe egindako mehatxuetatik babestea, informazioaren konfidentzialtasuna, osotasuna, eskuragarritasuna, benetakotasuna eta legezkotasuna betetzen direla bermatzeko.

Segurtasun Gidalerro honek Osakidetzako agintari gorenek Politika hau zabaltzeko, sendotzeko eta betetzeko duten konpromiso nabarmena bermatzen du.

2 ESPARRU ARAUTZAILEA

Segurtasun-politika hori, besteak beste, honako arau hauek zehaztutako arau-esparruaren barruan kokatzen da:

- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena.
- 4/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.
- 39/2015 Legea, urriaren 1ekoa, Administrazio Publikoen Administrazio Prozedura Erkideari buruzkoa
- 40/2015 Legea, urriaren 1ekoa, Sektore Publikoko Araubide Juridikoa ezartzen duena.
- 9/2017 Legea, azaroaren 8koa, Sektore Publikoko Kontratuena, Europako Parlamentuaren eta Kontseiluaren 2014ko otsailaren 26ko 2014/23/EB eta 2014/24/EB zuzentarauen transposizioa egiten duena Espainiako ordenamendu juridikora.
- 679/2016 Erregelamendua (EB), 2016ko apirilaren 27koa, Europako Parlamentuarena eta Kontseiluarena, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa. (DBEO).
- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babesteari eta eskubide digitalak bermatzeari buruzkoa.
- 21/2012 Dekretua, otsailaren 21ekoa, Eusko Jaurlaritzaren Administrazio Elektronikoari buruzkoa.
- Maiatzaren 5eko 1/1982 Lege Organikoak, ohorerako, norberaren eta familiaren intimitaterako eta norberaren irudirako eskubidearen babes zibilari buruzkoak,
- 37/2007 Legea, azaroaren 16koa, sektore publikoko informazioa berrerabiltzeari buruzkoa.
- Europako Parlamentuaren eta Kontseiluaren 910/2014 (eIDAS) EBko Erregelamendua, 2014ko uztailaren 23koa, barne-merkatuko transakzio elektronikoetarako identifikazio elektronikoari eta konfiantzazko zerbitzuei buruzkoa, 1999/93/EE Zuzentaraua indargabetzen duena.
- 6/2020 Legea, azaroaren 11koa, konfiantzazko zerbitzu elektronikoen alderdi jakin batzuk arautzen dituena.
- 203/2021 Errege Dekretua, martxoaren 30ekoa, Sektore publikoak bitarteko elektronikoen bidez jarduteko eta funtzionatzeko Erregelamendua onartzen duena.
- Segurtasun Eskema Nazionalaren araberako SITa.
- Segurtasun-egoeraren txosteneko SITa.
- Informazio-sistemen segurtasuna ikuskatzeko SITa.

- Segurtasun-gorabeheren jakinarazpenaren SITa.

Era berean, aplikagarriak izango dira Osakidetzaren jarduera arautzen duten beste arau guztiak, bere eskumenen esparruan, bai eta Erakundeak bere eskumenak egikaritzean kudeatzen dituen bitarteko elektronikoetan erabilitako datuen, informazioen eta zerbitzuen sarbidea, osotasuna, erabilgarritasuna, benetakotasuna, konfidentzialtasuna, trazabilitatea eta kontserbazioa ziurtatzeko arauak ere.

Era berean, kontuan hartu beharko dira segurtasun-politika honen eremuan eragina izan dezaketen arau-aldaketak eta aurrerapen teknikoak.

3 OSAKIDETZAREN HELBURUA

Osakidetzaren lehentasunezko helburua pertsona guztientzako osasun-sistema publikoa, unibertsala eta kalitatezkoa bermatzea da. Osakidetzaren misioa pertsona guztien osasunaren alde lan egitea da, horiek baitira ekintza guztien ardatz nagusia. Osasuna babesteko eskubidea, beraz, ukaezina da, eta euskal osasun-sistema publikoaren oinarrietako bat da.

Bere funtzioak betetzeko eta teknologiak osasun-sisteman izan duen bilakaeran oinarrituta, Osakidetzak informazio-sistemetan (IS) oinarritzen du bere jarduera. Sistema horiek arretaz administratu behar dira, eta segurtasun-neurri egokiak hartu behar dira ustekabeko edo nahita eragindako kalteetatik eta azkar eboluzionatzeko mehatxuetatik babesteko, eta eskuragarritasun-, benetakotasun-, osotasun-, konfidentzialtasun- eta trazabilitate-bermeetan eragiteko edo eragiteko ahalmena dutenak.

Azken hori betetzearekin hertsiki lotuta, garrantzitsua da azpimarratzea informazio- eta komunikazio-teknologien (aurrerantzean, IKT) azpiegitura baten beharra dagoela, zeinak lehentasuna emango baitie eragiketa irekiei, funtzionaltasunari, konektibitateari eta erabiltzaileari zerbitzua emateari begira, helburu estrategikoak eta instituzionalak lortzeko lehentasunezko funtzio gisa. Ildo horretan, IKTak balio estrategiko handiko tresna dira, Osakidetzaren modernizazioa bultzatzeko ahalmena dutelako.

4 IRISMENA ETA APLIKAZIO-EREMUA

4.1 Irismena

Informazioaren Segurtasunari Buruzko Gidalerro hau Osakidetzak ematen dituen zerbitzu elektronikoei aplikatuko zaie, eta zerbitzu horiek garatzen diren informazio-sistema guztiei aplikatuko zaie.

4.2 Aplikazio-eremua

Informazioaren Segurtasunari Buruzko Gidalerro hau Osakidetzak eskaintzen dituen zerbitzu elektronikoak ematen parte hartzen duten langile guztiei aplikatuko zaie, zuzenean zein zeharka, Osakidetzako langileak edo erakundetik kanpoko langileak izan.

Politika hori aplikatzen zaie zerbitzuak ematen parte hartzen duten eta Osakidetzaren IKT baliabideak erabiltzen dituzten pertsona, erakunde, entitate edo unitate eta zerbitzu guztiei, barrukoak zein kanpokoak izan, haiekin zuzenean edo zeharka konektatuta, urruneko konexioaren bidez edo kanpoko ekipamenduen bidez, Internet bidez emandako zerbitzuak barne. Aurrerantzean, guztiak hartuko dira "erabiltzailetzat".

Gainera, informazio-sistemei eta Osakidetzaren ardurapeko datu pertsonalen tratamendu-jarduera guztiei aplikatuko zaie.

5 OINARRIZKO SEGURTASUN-PRINTZIPIOAK

Informazioaren Segurtasunari Buruzko Gidalerro honek oinarrizko babes-printzipio hauek ditu oinarri. Printzipio hauek osatzen dituzte Osakidetzak bere jardueran informazioaren segurtasunaren arloan egiten dituen jarduketa guztien oinarri eta euskarri diren zutabeak.

5.1 Segurtasuna prozesu integral gisa

Informazioaren segurtasuna prozesu integral baten emaitza da. Prozesu hori tratamenduan esku hartzen duten giza elementu, elementu tekniko, material, juridiko eta antolaketa-elementu guzti-guztien mende dago, jarduera puntualak edo tratamendu bereiziak saihestuz.

Politikak zuzendaritza-maila guztien konpromisoa izango du, informazioaren segurtasuna erakundearen erabaki estrategikoekin integratuta eta koordinatuta egon dadin.

Segurtasun-alderdiak kontuan hartuko dira zerbitzuen bizi-zikloaren fase guztietan, eta segurtasuna bermatuko da lehenetsita. Segurtasuna ohiko jardunaren zatitzat hartuko da, eta informazio-sistemen hasierako diseinutik bertan egongo da eta aplikatuko da.

5.2 Segurtasun-arriskuen kudeaketa

Informazioaren segurtasunaren kudeaketa arriskuen kudeaketan oinarritzen da, eta haren helburua da arrisku-mailak gutxieneko maila onargarrien barruan mantentzea, segurtasun-neurri egokiak eta etengabe eguneratuak hedatuz informazioaren tratamenduarekin lotutako aplikazio eta zerbitzuen bizi-zikloaren fase guztietan, oreka eta proportzionaltasuna ezarriz datuen izaeraren, egindako tratamenduen, eraginpean dauden arriskuen eta aplikatutako segurtasun-neurrien artean.

5.3 Prebentzioa, detekzioa, erantzuna eta kontserbazioa

Sistemaren segurtasunak prebentzio-, detekzio- eta erantzun-alderdiak hartu behar ditu kontuan, haren ahuleziak minimizatzeko eta haren gaineko mehatxuak ez gauzatzea lortzeko, edo, hala eginez gero, informazio-sistemek edo ematen dituzten zerbitzuek erabiltzen dituzten datuetan eragin larririk ez izatea lortzeko.

Prebentzio-neurriek mehatxuak gauzatzeko aukera ezabatu edo murriztu beharko dute, esposizio-azalera murriztuz; detekzio-neurriek, berriz, balizko ziberintzidenteak aurkitzeko aukera eman beharko dute.

Erantzuteko neurriek, behar bezala kudeatuta, segurtasun-gorabehera batek eragindako informazioa eta zerbitzuak lehengoratzeko aukera eman beharko dute.

Informazio-sistemak datuak eta informazioa euskarri elektronikoan gordeko direla bermatuko du, eta zerbitzuak informazioaren bizi-ziklo osoan egongo dira eskuragarri.

5.4 Defentsa-ildoak egotea

Segurtasun-geruza ugariz osatutako babes-estrategia bat ezartzen da. Geruza horiek antolaketa-, operazio, fisika eta logikako neurriez osatuta daude, eta neurri horietako batek huts egiten badu, sistemak ez du bere osotasunean arriskuan jarriko, eta haren gaineko azken inpaktua minimizatuko da.

5.5 Etengabeko zaintza eta aldizkako berrebaluazioa

Etengabeko zaintzari esker, ezohiko jarduerak edo portaerak detektatu ahal izango dira, eta horiei erantzun ahal izango zaie.

Aktiboen segurtasun-egoeraren etengabeko ebaluazioak haien bilakaera neurtzea ahalbidetuko du, ahuleziak hautemanez eta konfigurazio-gabeziak identifikatuz.

Segurtasun-neurriak aldian-aldian berriz ebaluatu eta eguneratuko dira, eta haien eraginkortasuna arriskuen eta babes-sistemen bilakaerara egokituko da. Beharrezkoa izanez gero, segurtasuna birplanteatu ahal izango da.

5.6 Erantzukizunak bereiztea, koordinazioa eta lankidetza

Informazio-sistemen segurtasunaren erantzukizuna eta zerikusia duten informazio-sistemen ustiapenaren gaineko erantzukizuna bereizita egongo dira: informazioaren arduradunak zehaztuko ditu tratatutako informazioaren segurtasun-betekizunak; zerbitzuaren arduradunak zehaztuko ditu emandako zerbitzuen segurtasun-betekizunak; segurtasun-arduradunak zehaztuko ditu informazioaren eta zerbitzuen segurtasun-betekizunak betetzeko erabakiak; baldintzak betetzen direla bermatzeko behar diren neurrien ezarpena gainbegiratuko du, eta gai horien berri emango du; eta sistemaren arduradunak garatuko du sisteman segurtasuna ezartzeko modu zehatza, bai eta sistemaren eguneroko eragiketa ere.

Segurtasun-prozesuan inplikatutako guztiek modu koordinatuan jardungo dute segurtasun-neurriak aplikatzen eta kontrolatzen, segurtasun-arduradunaren koordinaziopean (aurrerago zehaztuko da). Koordinazio hori Osakidetzak arlo horretan egiten dituen ekimen eta jarduera guztietara zabalduko da.

6 SEGURTASUNAREN GUTXIENEKO BALDINTZAK

Informazioaren segurtasunaren arloko jarduketa guztien oinarri eta euskarri diren oinarrizko babes-printzipioak garatzeko, honako gutxieneko baldintza hauek aplikatzen zaizkie sistema bakoitzean identifikatutako arriskuei, proportzionalki.

6.1 Segurtasun-prozesua antolatzea eta ezartzea

Informazio-sistemen segurtasunak erakundeko kide guztiak arriskuan jarri beharko ditu.

Politika erakundeko kide guztiek ezagutu beharko dute, eta politika betetzen dela zaintzeko arduradunak identifikatu beharko dira: informazioaren arduraduna, zerbitzuaren arduraduna, segurtasunaren arduraduna eta sistemaren arduraduna.

6.2 Arriskuen analisia eta kudeaketa

Organizazioak arriskuak kudeatuko ditu, sistemak jasan ditzakeen arriskuen analisia eta tratamendua eginez, nazioartean onartutako metodologia erabiliz.

Arriskuak arintzeko edo ezabatzeko hartutako neurriek justifikatuta egon beharko dute, eta proportzionaltasuna egongo da haien eta arriskuen artean.

6.3 Langileen kudeaketa

Langileek, enpresakoek zein kanpokoek, prestakuntza eta informazioa izango dute segurtasunaren arloan dituzten betebehar, betebehar eta erantzukizunei buruz. Haien jarduna gainbegiratuko da, ezarritako prozedurak betetzen direla egiaztatzeko, eta eginkizunak betetzean onartutako segurtasuneko arau eta prozedura operatiboak aplikatuko dituzte.

Sistemaren erabilera seguruaren esanahia eta irismena segurtasun-arau batzuetan zehaztu eta islatuko dira. Arau horiek zuzendaritza nagusiaren titularrak onartuko ditu, Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak proposatuta.

6.4 Profesionaltasuna

Informazio-sistemen segurtasuna langile kualifikatuek zaindu, berrikusi eta ikuskatuko dute, eta beren bizi-zikloaren fase guztietan (plangintza, diseinua, erosketa, eraikuntza, hedapena, ustiapena, mantentze-lanak, gorabeheren kudeaketa eta eraispena) jardun eta trebatuko dute.

Erakundeak zehaztuko du zer prestakuntza- eta esperientzia-baldintza bete behar dituzten langile horiek.

6.5 Sarbideak baimentzea eta kontrolatzea

Informazio-sistemetarako sarbide kontrolatua behar bezala baimendutako erabiltzaile, prozesu, gailu edo bestelako informazio-sistemetara mugatuko da, eta baimendutako funtzioetara soilik.

6.6 Instalazioak babestea

Informazio-sistemek eta haien komunikazio-azpiegiturek eremu kontrolatuetan egon beharko dute, eta sarbide-mekanismo egokiak eta proportzionalak izan beharko dituzte, arriskuen analisiaren arabera.

6.7 Segurtasun-produktuak eskuratzea eta segurtasun-zerbitzuak kontratatzea

Osakidetzak erabiliko dituen informazioaren eta komunikazioen teknologien segurtasun-zerbitzuak kontratatzeko edo segurtasun-produktuak eskuratzeko, sistemaren kategoria eta segurtasun-maila zehatzarekiko proportzioan erabiliko dira eskuraketaren xedearekin lotutako segurtasun-funtzionaltasuna ziurtatuta dutenak, Kriptologia Zentro Nazionalak ezartzen dituen baldintzak eta irizpideak betez.

6.8 Gutxieneko pribilegioa

Informazio-sistemak diseinatzerakoan, horiek behar bezala betetzeko ahalik eta pribilegio gutxien emango dira, Osakidetzak bere helburuak lortzeko ezinbesteko funtzionaltasuna emango da, eta operazio-, administrazio- eta erregistro-funtzioak horretarako beharrezkoak diren gutxienekoak izango dira, eta pertsona baimenduek bakarrik garatzen dituztela ziurtatuko da, betiere baimendutako baliabideetatik.

Teknologia desberdinetarako segurtasuna konfiguratzeko gidak aplikatuko dira, sistemaren kategorizaziora egokituta, eta beharrezkoak ez diren edo egokiak ez diren funtzioak desaktibatuko dira.

6.9 Sistemaren osotasuna eta eguneratzea

Sisteman edozein elementu fisiko edo logiko sartzeko edo aldatzeko, aldez aurreko baimen formala beharko da.

Uneoro ezagutuko da sistemen segurtasun-egoera, fabrikatzaileen zehaztapenei, konfigurazio-gabeziei, ahuleziei eta eragiten dieten eguneratzeei dagokienez, bai eta horien gaineko intzidenteak garaiz detektatzea ere, eta arduraz erreakzionatuko da arriskua kudeatzeko, haien segurtasun-egoera ikusita.

6.10 Biltegiratutako informazioa eta iragaitzazko informazioa babestea

Sistemaren segurtasunaren egituran eta antolaketan, arreta berezia jarriko zaio ingurune ez-seguruetan (ekipo edo gailu eramangarriak edo mugikorrak, periferikoak, euskarriak eta sare irekiak, etab.) biltegiratutako edo bidean den informazioari. Sistemek sortutako dokumentu elektronikoen kontserbazioa bermatuko da. Sistemen informazio elektronikoaren zuzeneko kausa edo ondorio den euskarri ez-elektronikoko informazio guztia ere maila berean babestuta egongo da.

6.11 Elkarri lotutako beste informazio-sistema batzuen aurreko prebentzioa

Informazio-sistemaren perimetroa babestuko da, batez ere sare publikoetara konektatuz gero, eta segurtasun-gorabeheren aurrean prebentzio-, detekzio- eta erantzun-lanak indartuko dira. Sistema sareen bidez beste sistema batzuekin interkonektatzearen ondoriozko arriskuak aztertuko dira eta horien lotura-puntua kontrolatuko da.

6.12 Jardueraren erregistroa eta kode kaltegarriaren detekzioa

Segurtasun Eskema Nazionalaren xedea betetzeko, eta ohorerako, norberaren eta familiaren intimitaterako eta ukituen irudirako eskubidearen berme guztiekin, eta datu pertsonalak, funtzio publikokoak edo lanekoak babesteari buruzko araudiarekin eta aplikatu beharreko gainerako xedapenekin bat etorriz, erabiltzaileen jarduerak erregistratuko dira, eta behar ez diren edo baimendu ez diren jarduerak monitorizatzeko, aztertzeko, ikertzeko eta dokumentatzeko behar-beharrezkoa den informazioa gordeko da, une bakoitzean jarduten duen pertsona identifikatzeko aukera emanez.

Behar-beharrezkoa eta proportzionala den neurrian, sarrerako edo irteerako komunikazioak aztertu ahal izango dira, eta informazioaren segurtasunerako baino ez. Horrela, informazio-sare eta -sistemetara baimenik gabe sartzea eragotzi ahal izango da, zerbitzua ukatzeko erasoak eten ahal izango dira, kode kaltegarria asmo txarrez banatzea saihestu ahal izango da, bai eta sare eta informazio-sistema horiei eragindako beste kalte batzuk ere.

Informazio-sistemara sartzen den erabiltzaile bakoitza modu bakarrean identifikatuta egongo da, une oro, sarbide-eskubideak nork jasotzen dituen, zein motatakoak diren eta jarduera jakin bat nork egin duen jakiteko.

6.13 Segurtasuneko gorabeherak

Osakidetzak segurtasun-gorabeherak kudeatzeko prozedurak izango ditu, bai eta detekzio-mekanismoak, sailkapen-irizpideak, analisi- eta ebazpen-prozedurak, alderdi interesdunekin komunikatzeko bideak eta jarduketen erregistroa ere. Erregistro hori sistemaren segurtasuna etengabe hobetzeko erabiliko da.

6.14 Jardueraren jarraipena

Segurtasun-kopiak izango dira, eta beharrezko mekanismoak ezarriko dira ohiko bitartekoak galduz gero eragiketen jarraitutasuna bermatzeko.

6.15 Segurtasun-prozesua etengabe hobetzea

Segurtasun-prozesu integrala etengabe eguneratu eta hobetuko da, eta, horretarako, IKTen segurtasunaren arloan onartutako irizpideak eta metodoak aplikatuko dira.

7 SEGURTASUNAREN ANTOLAKETA

Informazioa babesteko bizi-zikloaren etapa guztiak modu egokian egiten direla eta horiek gauzatzeko erantzukizunak behar bezala esleitzen direla bermatzeko, Osakidetzak egitura bat ezartzen du, gidalerro honen aplikazio sendoa sustatzeko eta teknologia- eta antolaketa-aldaketa ugari benetan egokitzeko aukera ematen duena.

Horretarako, SENek xedatutakoaren arabera, batzorde eta rol orokor hauek definitzen dira, informazioaren segurtasuna kudeatzen eta gainbegiratzen parte hartzeari lotuta:

- Informazioaren arduradunak.
- Zerbitzuen arduradunak.
- Informazioaren segurtasunaren arduraduna.
- Informazio-sistemen arduradunak.
- Informazioaren Segurtasunerako Batzordea, Osakidetzan: Osakidetzako Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordea.

7.1 Informazioaren arduradunak

Informazioaren arduradunek beren ardurapeko informazioari aplikatu beharreko segurtasun-baldintzak ezarriko dituzte. Eginkizun hori Zuzendaritza Nagusiko eta Alorreko Zuzendaritzetako titularrek edo haiek eskuordetzen dituzten pertsonek betetzen dute, eta honako erantzukizun espezifiko hauek hartzen dituzte beren gain:

- Bere ardurapeko informaziorako, segurtasunaren dimentsio garrantzitsuak (erabilgarritasuna, konfidentzialtasuna, osotasuna, benetakotasuna eta trazabilitatea) eta dagokion maila definitzea.
- Informazioaren tratamenduan bermatu behar diren segurtasun-arloko informazioaren betekizunak ezartzea.
- Informazioaren segurtasunaren arloan dagozkien funtzio orokorren esparruan egokitzat jotzen den beste edozein eginkizun.

7.2 Zerbitzuen arduradunak

Zerbitzuen arduradunek beren ardurapeko zerbitzuei aplikatu beharreko segurtasun-baldintzak ezarriko dituzte. Eginkizun hori honako hauek betetzen dute: Aholkularitza Juridikoko, Asistentzia Sanitarioko, Zuzendaritza Ekonomiko Finantzarioko eta Giza Baliabideen Zuzendaritzako Zuzendariordetza

korporatiboen titularrek eta zerbitzu publiko elektroniko gisa ematen diren gaietan zuzeneko eskumena izan dezaketen zerbitzu-erakundeetako zuzendariordetzek, bai eta aurrekoek eskuordetu ditzaketen pertsonek ere. Honako erantzukizun espezifiko hauek hartzen dituzte beren gain:

- Bere ardurapeko zerbitzu elektronikoetarako, segurtasunaren dimentsio garrantzitsuak (erabilgarritasuna, konfidentzialtasuna, osotasuna, benetakotasuna eta trazabilitatea) eta dagokien maila definitzea.
- Bere ardurapeko zerbitzu elektronikoen kasuan, denboraren araberako erabilezintasun baten eraginaren bilakaera zehaztea.
- Informazioaren tratamenduan bermatu behar diren segurtasun-arloko zerbitzuen betekizunak ezartzea.
- Gerta daitezkeen gorabeheren inpaktua aztertzen laguntzea, eta horien aurrean estrategiak eta babesak planteatzea.
- Informazioaren segurtasunaren arloan dagozkien funtzio orokorren esparruan egokitzat jotzen den beste edozein eginkizun.

7.3 Segurtasun-arduraduna

Segurtasunaren arduradunak informazioaren eta zerbitzuen arduradunek ezarritako segurtasun-baldintzak betetzeko behar diren erabakiak hartuko ditu. Rol hori Osakidetzako Informatika eta Informazio Sistemetako Zuzendariordeak betetzen du, eta honako erantzukizun espezifiko hauek hartzen ditu bere gain:

- Erabilitako informazioa eta emandako zerbitzuak babesteko behar diren segurtasun-neurriak zehaztea eta ezarritakoak une oro egokiak direla egiaztatzea, Aplikagarritasun Adierazpena formalki onartuta.
- Sistemaren kategoria eta aplikatu beharreko segurtasun-neurriak zehaztea, aldez aurretik zerbitzuen eta informazioaren arduradunek egindako balorazioen arabera.
- Arriskuen analisia eta eraginaren analisia berrikusi eta mantentzetik eratorritako aldizkako zereginak koordinatzea.
- Segurtasunaren egoeraren berri ematea Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeari.
- Segurtasun-arloko betebeharrak betetzen direla egiaztatzeko aukera emango duten aldizkako auditoretzak egin daitezen bultzatzea edo eskatzea.
- Segurtasun Gidalerroaren operatibaren jarraipena egitea.
- Segurtasun-gorabeheren ikerketa babestea eta gainbegiratzea, jakinarazten direnetik ebazten diren arte.
- Aldizkako segurtasun-txosten bat egitea, aldiko gorabehera garrantzitsuenak jasoko dituena.

- Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeari segurtasun-gorabehera larrien berri ematea.
- Segurtasunaren arloan beharrezkotzat jotzen dituen arau, jarraibide eta jarraibide teknikoak aldatzea proposatzea Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeari.
- Sistemen arduradunek prestatutako segurtasun-prozeduren onarpena aldi baterako erabakitzea, eta prozedura horiek behin-behinean ezartzen saiatzea, harik eta Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak behin betiko onartzen dituen arte.
- Segurtasunaren arloan egokitzat jotzen den eta dokumentu honetan aurreikusitako beste edozein organori berariaz esleitu ez zaion beste edozein eginkizun.

7.4 Sistemen arduradunak

Segurtasun-arduradunak zehaztutako izaera teknologikoko segurtasun-neurriak aplikatzeaz arduratuko dira. Rol hori Osakidetzako Informatika eta Informazio Sistemen Zuzendariordetzako zerbitzuetako arduradunek betetzen dute, eta beren eskumen-eremuaren barruan, honako erantzukizun espezifiko hauek hartzen dituzte beren gain:

- Bere ardurapeko sistemen segurtasunaren administrazioaren berezko zereginak behar bezala egiten direla bermatzea.
- Bere ardurapeko informazio-sistemak kontrolpean daudela bermatzea.
- Segurtasun-prozesuak gauzatzea bere arloaren esparruan.
- Segurtasuna ezartzea bere arloan, informazio-sistemei aplikatu beharreko segurtasun-neurriak kudeatuz eta mantenduz, SENen arabera.
- Segurtasun-auditoretzetan eta arriskuen kudeaketan laguntzea.
- Informazioaren segurtasunaren arloan dagozkien funtzio orokorren esparruan egokitzat jotzen den beste edozein eginkizun.

7.5 Segurtasun Batzordea. Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordea

Segurtasun-batzordea kide anitzeko organoa da, eta segurtasun-arloko jarduerak zuzendu, kudeatu, koordinatu, ezarri eta onartzen ditu.

Batzorde horretan ebatziko dira segurtasun-politika hau edo hura garatzen duten arau eta prozedurak aplikatzean sor daitezkeen gatazkak.

Batzorde horrek izen zehatz hau izango du: "Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordea".

Batzorde horren osaera eta funtzionamendu-araubidea Osakidetzako Administrazio Kontseiluak gai horri buruz erabakitzen dituenak izango dira, eta Zuzendaritza Nagusiko titularrak izendatuko ditu bokalak, idazkaria eta presidentea.

Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak informazioa eta laguntza eskatuko die Osakidetzako arlo guztiei, beharrezkotzat jotzen duenean.

Osakidetzako zerbitzu eta unitate guztiak behartuta egongo dira Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeari informazioa eta laguntza ematera, hark hala eskatzen duenean bere eskumeneko gaietan.

Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeari erakundearen zerbitzu-erakundeetan hautemandako segurtasun-gorabehera garrantzitsu guztien berri emango zaio, baina horrek ez du esan nahi Batzordearen esku-hartzea nahitaezkoa denik aurretiazko informazioen aldi bat irekitzea eta/edo diziplina-prozeduren instrukzioa sustatzeko, hala badagokio, baldin eta segurtasun-neurri aplikagarrien ez-betetzeren bat egiaztatu bada.

Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak honako eginkizun eta erantzukizun gehigarri zehatz hauek ditu:

- Segurtasun-gidalerro hau eta gidalerro horren arau-esparruaren barruan egindako dokumentazioa zabaltzea.
- Segurtasunaren egoeraren berri ematea Osakidetzako gobernu-organoei.
- Segurtasunaren arloan sortzen diren erantzukizun-gatazkak interpretatzea eta gatazka horien konponbidea eskatzea.
- Organo eskudunei jakinaraztea ez direla bete segurtasun–gidalerroa eta haren ondoriozko arauak, eta, hala badagokio, neurri zuzentzaileak hartzeko eskatzea.
- Segurtasunaren etengabeko hobekuntza sustatzea.
- Segurtasun-gidalerro hau eta gainerako arau orokorrak egitea, berrikustea eta aldian behin haien jarraipena egitea, eta Osakidetzako gobernu-organoei egokitzat jotzen dituzten aldaketak proposatzea.
- Estrategia eta lan-ildo berriak lantzea eta bultzatzea segurtasunari dagokionez.
- Segurtasunaren arloko jarduketak lehenestea.
- Segurtasun-prozesuaren jarraipena gainbegiratzea eta gauzatzea.
- Gerta daitezkeen segurtasun-gorabeherak eta kasu bakoitzean aplikatutako neurriak gainbegiratzea.
- Auditorien emaitzak gainbegiratzea.

- SENen jarraipen-lanak gainbegiratzea eta onartzea.

8 LOTUTAKO BETEBEHARRAK

8.1 Erabiltzaileen betebeharrak

Osakidetzako erabiltzaile guztiek ezagutu eta bete behar dute Informazioaren Segurtasunari Buruzko Gidalerro hau, bai eta horretatik abiatuta garatutako segurtasun-araudia eta -jarraibideak ere, eta Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordearen ardura da informazioa eragindakoei helarazteko behar diren bitartekoak jartzea.

Osakidetzako erabiltzaile guztiek jakin behar dute informazio-sistemen segurtasuna bermatu behar dela, eta haiek beraiek funtsezko pieza direla segurtasuna mantentzeko eta hobetzeko.

8.2 Erabiltzaileen erantzukizunak ez-betetzeen kasuan

Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak ebaluatu ahal izango du Osakidetzako erabiltzaileren batek Informazioaren Segurtasunari Buruzko Gidalerroan edo hura garatzeko araudian eta jarraibideetan aurreikusitako betebeharretan ez-betetzeren bat izan duen.

Ez-betetzeren bat antzemanez gero, prebentzio-neurriak eta neurri zuzentzaileak hartuko dira, informazio-sistemak babesteko.

Era berean, Osakidetzaren Informazioaren Segurtasunari Buruzko Gidalerroa urratu dela ikusten bada, Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak egoki iritzitako diziplina-prozedurak instruitzeko eskatu ahal izango die kasuan kasuko organoei.

Aplikatu beharreko prozedura eta zehapenak Administrazio Publikoen edo Osakidetzaren beraren zerbitzura dauden langileen diziplina-araubideari buruzko legerian ezarritakoak izango dira.

8.3 Hirugarrenekiko harremana

Osakidetzak beste erakunde batzuei zerbitzuak ematen dizkienean edo horiei buruzko informazioa erabiltzen duenean, harreman horren arduradunak segurtasun-gidalerroa horren eta horren ondoriozko arau eta jarraibideen berri emango die. Dagozkion segurtasun-arduradunen arteko komunikazio- eta koordinazio-kanalak ezarriko dira, eta segurtasun-gorabeheren aurrean erreakzionatzeko jarduketa-prozedurak ezarriko dira.

Era berean, Osakidetzak hirugarrenen zerbitzuak erabiltzen dituenean edo hirugarrenei informazioa lagatzen dienean, zerrenda horren arduradunak segurtasun-gidalerro horren eta zerbitzu edo informazio horiei eragiten dien segurtasun-araudi eta -jarraibideen berri emango die.

Hirugarren horiek kasuan kasuko arau eta jarraibideetan ezarritako segurtasun-betebehar eta -neurrien mende geratuko dira, eta horiei erantzuteko beren prozedura operatiboak garatu beharko dituzte.

Gorabeherak prebenitzeko, detektatzeko, jakinarazteko eta konpontzeko prozedura espezifikoak ezarriko dira, betiere hirugarrenak behar bezala kontzientziatuta egon daitezen segurtasunaren arloan, gutxienez, segurtasun-gidalerro honetan ezarritako maila berean.

Zehazki, hirugarrenek ikuskatu daitezkeen estandarretan oinarritutako segurtasun-gidalerroak betetzen direla bermatu beharko dute, eta gidalerro hori betetzen dela egiaztatzeko egokitzat jotzen diren kontrol eta berrikuspen guztiak egin beharko dituzte.

Segurtasun-gidalerro horren alderdiren bat hirugarrenek bete ezin dutenean, informazioaren segurtasuneko arduradunaren txostena eskatuko da, eta txosten horretan zehaztuko da zer arrisku dauden eta nola tratatu behar diren. Txosten hori eragindako informazioaren eta zerbitzuen arduradunek onartu beharko dute aurrera egin aurretik.

9 INFORMAZIOAREN SEGURTASUNARI BURUZKO GIDALERROA GARATZEA ETA HEDATZEA

Segurtasun-gidalerro hau Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak berrikusi du, eta Osakidetzako Administrazio Kontseiluak onartu, eta nahitaez bete behar du erakunde publikoan egon daitekeen edozein zerbitzu elektronikok.

Informazioaren Segurtasunari Buruzko Gidalerro hau eraginkorra da data horretatik gidalerro berri batek ordezten duen arte.

Osakidetzako Informazioaren Segurtasunari Buruzko Gidalerro hau indarrean jartzeak Osakidetzako zerbitzu-erakundeetan egon daitekeen beste edozein politika indargabetzea dakar.

Hori garatzeko, Osakidetzak hainbat mailatan egituratutako dokumentu-esparru bat ezartzen du, dokumentu honetan ezarritako gidalerroek garapen espezifikoa izan dezaten. Nolanahi ere, garatzen diren gidalerro, arau eta erregulazio espezifikoek bat etorri beharko dute segurtasun-gidalerro honekin eta haren ondorio izan beharko dute.

Hona hemen dokumentu-esparru horren osaera:

- *Lehen maila:* Osakidetzako Zerbitzu Elektronikoen Informazioaren SEGURTASUN-GIDALERRO bera.
- *Bigarren maila:* Informazioaren Segurtasunari Buruzko Gidalerrotik sortzen diren eta segurtasunaren eremu desberdinei eusten dieten SEGURTASUN-ARAU OROKORRAK.
- *Hirugarren maila:* PROZEDURA orokorrak, informazioaren segurtasunarekin lotutako jarduera jakin bat egitean jarraitu beharreko jarraibide espezifikoak deskribatzen dituzten dokumentuen multzo gisa.
- *Laugarren maila:*
  - GIDAK, Informatikako Zuzendariordetzako langileek jarraitu beharreko jarraibideak deskribatzen dituzten dokumentuak,
  - ESKULIBURUAK, Osakidetzako erabiltzaile guztiek jarraitu beharreko jarraibideak deskribatzen dituzten dokumentuak.

Informazioaren Segurtasunari Buruzko Gidalerroa Osakidetzako Administrazio Kontseiluak onartuko du, Informazioaren Segurtasun eta Datu Pertsonalen Babeserako Batzordeak proposatuta; bigarren mailako arau orokorrak eta hirugarren mailako prozedurak, berriz, Informazioaren Segurtasun eta Datu Pertsonalen Babeserako Batzordeak onartuko ditu, Informazioaren Segurtasuneko arduradunak proposatuta, Zerbitzuetako eta Sistemetako arduradunekin lankidetzan. Sistemen arduradunak onartuko ditu laugarren mailako gidak, eskuliburuak eta gainerako dokumentazioa.

Informazioaren Segurtasunerako eta Datu Pertsonalak Babesteko Batzordeak onartutako segurtasun-arau orokorrak (bigarren maila) Osakidetzako Zuzendaritza Nagusiaren ebazpen bidez hartu beharko dira, eta hori ez betetzeak dagokion diziplina-erantzukizuna ekar dezake.

Informazioaren Segurtasunari Buruzko Gidalerro hau, arau orokorrak eta onartzen den gainerako dokumentazio espezifikoa ukitutako zerbitzuen arduradun guztiei jakinarazi beharko zaizkie. Informazioaren Segurtasunari Buruzko Gidalerroa Osakidetzaren webgunean argitaratuko da; arau orokorrak eta gainerako dokumentazio espezifikoa Osakidetzaren intranetean argitaratuko dira.

10 PRESTAKUNTZA ETA KONTZIENTZIAZIOA

Osakidetzak langile guztiak informazioaren segurtasunaren eta datu pertsonalen babesaren arloan prestatzera eta kontzientziatzera bideratutako jarduerak garatuko ditu, baita informazioaren segurtasun-gidalerroa eta haren arau-garapena zabaltzera bideratutakoak ere, bereziki langile berriei zuzendutakoak, halako moldez non bermatuko baitu langileek ezagutzen, ulertzen eta betetzen dituztela segurtasunaren arloan hartutako arauak eta babes-neurriak, eta ohartaraziko baitie zer arrisku ekar ditzakeen eskura dituzten gailu eta soluzio teknologikoak gaizki erabiltzeak.

IKT sistemen erabileran, operazioan edo administrazioan erantzukizuna duten pertsona guztiek sistemen erabilera segururako gaituta egon behar dute; beraz, prestakuntza espezifikoa jasoko dute beren lana egiteko behar duten neurrian.

11 DATU PERTSONALEN BABESA

Datu pertsonalak babesteko, Datuak Babesteko Erregelamendu Orokorrean jasotakoa aplikatuko da, bai eta arlo horretako legeria nazional eta autonomikoan xedatutakoa ere.

Osakidetzako arlo bakoitza arduratuko da bere ardurapeko tratamendu-eragiketetan sartutako datu pertsonalen segurtasuna kudeatzeaz eta mantentzeaz.

Datu pertsonalak babesteko neurriak Arriskuen Analisiaren emaitzetan eta Datuak Babesteko Erregelamendu Orokorrean aurreikusitako Eraginaren Ebaluazioan oinarrituta ezarriko dira.

Osakidetzaren informazio-sistema guztiak araudi horretan ezarritako segurtasun-baldintzetara egokituko dira.

12 INFORMAZIOAREN SAILKAPENA

Informazioaren arduradunak informazioaren aktiboak izaeraren arabera sailkatu eta inbentariatuko ditu, informazioaren segurtasunari buruzko gidalerro honetan ezarritakoaren arabera. Babes-maila eta aplikatu beharreko neurriak sailkapen horren emaitzan oinarrituko dira.

Kalifikazio Gidaliburuaren arabera, informazio-sistemek tratatzen duten informazioa kategoria hauetako batean sailkatuko da, garrantziaren araberako beheranzko ordenan:

- **Ezkutukoa:**
  - *Mugatua:* Aipatu informazioa eskuragarri dago sarbide mugatua duten erabiltzaileentzat eta informazio hori galtzeak, hondatzeak edo baimenik gabe argitaratzeak kalte larria edo oso larria eragingo lioke Osakidetzaren izen onari, bere eginkizunei; edota finantza-galera edo legezko ondorio larriak edo oso larriak ekarriko lizkioke.
  - *Isilpekoa:* Honako informazioa eskuragarri dago baimendutako erabiltzaileentzat eta informazio hori galtzeak, hondatzeak edo baimenik gabe argitaratzeak finantza-galera edo legezko ondorioren bat eragingo lioke Osakidetzari edo norbanakoari.
  - *Barneko erabilera:* Honako informazioa eskuragarri dago baimendutako erabiltzaileentzat eta informazio hori galtzeak, hondatzeak edo baimenik gabe argitaratzeak sinesgarritasun edo ospe arazoak ekar ditzake norberarentzat
- **Publikoa:**
  - Informazio hori jende guztiarentzat eskuragarri dago.