Informazioaren segurtasun politika

BERRIKUSPENEN KONTROLA

IDAZLANA		Segurtasun Batzordea		
NORK ONARTUA:		Zuzendaritza Nagusia		
Ed.1 DATA		2025 / 02 / 18		
BERTSIOA	**EGUNA**	**ALDAKETEN ARDURADUNA**	**ALDAKETEN DESKRIBAPENA**	**NORK ONARTUA:**
1. ed.	2025/07/08	Segurtasun Batzordea	Hasierako bertsioa egitea	Zuzendaritza Nagusia

AURKIBIDEA

1. XEDEA

Informazioaren Segurtasunerako Politika honen helburua da Energiaren Euskal Erakundeak (aurrerantzean, EEE) bere informazioa eta zerbitzuak kudeatzeko eta babesteko modua arautuko duten jarraibideak eta printzipioak ezartzea, indarrean dagoen lege-esparru arautzailearen barruan, hala nola maiatzaren 3ko 311/2022 Errege Dekretua, Segurtasunaren Eskema Nazionala (aurrerantzean, ENS) arautzen duena. Sektore publikoaren administrazio elektronikoaren esparruan aplikatuko da, eta informazio-printzipio elektronikoak, informazio-babes egokirako informazio-printzipioak eta babes-politika ezartzea eskatzen du.

2. SARRERA

EEE IKT (Informazio eta Komunikazio Teknologiak) sistemen menpe dago bere helburuak lortzeko. Sistema horiek prestasunez administratu behar dira, eta neurri egokiak hartu behar dira tratatutako informazioaren edo emandako zerbitzuen erabilgarritasunari, osotasunari edo konfidentzialtasunari eragin diezaioketen istripuzko edo nahita egindako kalteen aurrean babesteko.

Informazioaren segurtasunaren helburua da informazioaren kalitatea eta zerbitzuen prestazio jarraitua bermatzea, prebentzioz jardunez, eguneroko jarduera gainbegiratuz eta gorabeherei bizkor erantzunez.

IKT sistemak babestuta egon behar dira bilakaera azkarreko mehatxuetatik, baldin eta mehatxuok eragina izan badezakete informazioaren eta zerbitzuen konfidentzialtasunean, osotasunean, erabilgarritasunean, benetakotasunean eta trazabilitatean, aurreikusitako erabileran eta balioan. Mehatxu horietatik babesteko, inguruneko baldintzen aldaketetara egokitzen den estrategia bat behar da, zerbitzuak etengabe ematen direla bermatzeko. Horrek esan nahi du sailek Segurtasun Eskema Nazionalak eskatzen dituen gutxieneko segurtasun-neurriak aplikatu behar dituztela, eta zerbitzuak emateko mailen etengabeko jarraipena egin behar dutela, atzemandako ahuleziak jarraitu eta aztertu behar dituztela, eta gorabeherei erantzun eraginkorra eman behar dietela, emandako zerbitzuen jarraitutasuna bermatzeko.

Arlo guztiek egiaztatu behar dute IKTen segurtasuna sistemaren bizi-zikloko etapa bakoitzaren zati integrala dela, hasi segurtasun hori sortzen denetik eta kendu arte, eta garapen- edo eskuratze-erabakietatik eta ustiapen-jardueretatik igaroz. Segurtasun-baldintzak eta finantzaketa-beharrak identifikatu egin behar dira, eta plangintzan eta IKT proiektuetarako eskaintzen eskaeran sartu.

3. ARAU-ESPARRUA

EEEk Informazioaren Segurtasunerako Politika honen esparruan gauzatzen dituen jardueren arau-esparrua honako arau hauek osatzen dute:

- Datuak Babesteko Erregelamendu Orokorra (EB) 2016/679, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa (DBEO/RGPD).
- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa eta Eskubide Digitalak Bermatzekoa (LOPD-GDD).

- 34/2002 Legea, uztailaren 11koa, informazioaren gizartearen zerbitzuei eta merkataritza elektronikoari buruzkoa.
- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasunaren Eskema Nazionala arautzen duena.

Era berean, kontuan hartu beharko dira Informazioaren Segurtasunerako Politika honen esparruan eragina izan dezaketen arau-aldaketak eta aurrerapen teknikoak.

4. SEGURTASUNAREN ANTOLAMENDUA

Politika hau behar bezala ezartzen dela bermatzeko, EEE informazio-aktiboei aplikatu behar zaizkien eta Informazio Sistemen arloak ezarri behar dituen segurtasun-neurriak definitzeko helburuarekin antolatuko da.

Segurtasunaren antolaketa horretan EEEren Zuzendaritza Nagusiak parte hartzen du. Zuzendaritza horrek Informazioaren Segurtasun Politika onartuko du, eta erantzukizunak esleituko eta/edo eskuordetuko dizkie egokitzat jotzen dituen pertsonei, eta aldian-aldian informazioa emango zaie, politika horren benetako ezarpenaren jarraipena egiten dela ziurtatzeko.

Era berean, erakundeak EEEko langile guztiak inplikatuko ditu neurri desberdinean, segurtasun-praktika egokien ezarpena zabaltzeko.

4.1. ANTOLAKUNTZA-EGITURA: EGINKIZUNAK ETA ERANTZUKIZUNAK

Informazio-segurtasuneko funtzio eta erantzukizun nagusiak Kudeaketa-eskuliburua dokumentuan zehazten dira.

4.1.1. SEGURTASUN BATZORDEA

Erakundeak Segurtasun Batzorde bat izango du, eta bertan parte hartuko dute Informazioaren Segurtasuneko arduradunak, Sistemen arduradunak, Zerbitzuaren arduradunak eta Informazioaren arduradunak. Batzorde horrek funtzio bikoitza izango du: datuen babesarekin lotutako gaiak lantzea eta informazioaren segurtasuna kudeatzea. Batzorde horren osaera, eginkizunak eta arduradunak Kudeaketa-eskuliburua dokumentuan daude jasota.

Segurtasun Batzordeen ohiko hiru bilera egingo dira urtean, eta hala egiten denean, ohiz kanpokoak ere egin ahal izango dira.

Segurtasun Batzordearen bilerak honela osatuko dira: lehenengo deialdian, kideen 2/3en quoruma egongo da, eta bigarren deialdian, kideen erdia + 1.

Informazioaren Segurtasuneko arduradunak aztertu beharreko gaien agenda bat jakinaraziko du batzordea baino astebete lehenago, gutxienez. Era berean, txostena amaitu ondoren, akta bat egingo da, eta kide guztiei jakinaraziko zaie. Akta hurrengo batzordean onartuko da.

5. GUTXIENEKO SEGURTASUN-BALDINTZAK

ENSa betetzeari dagokionez, gutxieneko baldintza hauek betetzea bermatuko da:

- ***Antolaketa***: informazioaren segurtasun-prozesua diseinatzea eta ezartzea.
- ***Arriskuen analisia eta kudeaketa***: zibersegurtasun-arriskuen tratamendu egokia.
- ***Langileen kudeaketa***: langileak lanean hasteko eta haiei baja emateko prozesuetan segurtasuna ezarriz, bai eta prestakuntza- eta kontzientziazio-ekintzak ere.
- ***Profesionaltasuna***: sistemen segurtasuna langile kualifikatuek zainduko, berrikusiko eta ikuskatuko dute, eta bizi-zikloaren fase guztietan (instalazioa, mantentze-lanak, gorabeheren kudeaketa eta eraispena) trebatuko dira. EEEko langileek sistemetan eta zerbitzuetan aplikatu beharreko informazio-teknologien segurtasuna bermatzeko behar den prestakuntza espezifikoa jasoko dute.
- ***Hirugarrenen segurtasuna***: EEEk eskatuko du, modu objektiboan eta bereizkeriarik gabe, segurtasun-zerbitzuak ematen dizkieten erakundeek profesional kualifikatuak eta kudeaketa- eta heldutasun-maila egokiak izan ditzatela ematen dituzten zerbitzuetan. Gainera, hirugarrenen kontratazioari buruz ENSean xedatutakoa beteko da.
- ***Sarbideak baimentzea eta kontrolatzea***: informazio-sistemarako sarbidea behar bezala baimendutako erabiltzaile, prozesu, gailu eta bestelako informazio-sistemetara kontrolatu eta mugatu beharko da, eta baimendutako funtzioetarako sarbidea murriztu.
- ***Instalazioen babesa***: sistemak eremu bereizietan instalatuko dira, sarbidea kontrolatzeko prozeduraz hornituta. Gutxienez, aretoak itxita egongo dira eta giltzen kontrola izango dute.
- ***Segurtasun-produktuak eskuratzea eta segurtasun-zerbitzuak kontratatzea:*** sistemaren kategoriaren eta segurtasun-maila jakin baten arabera erabiliko dira erosi beharreko objektuarekin lotutako segurtasun-funtzionalitatea ziurtatuta dutenak, hartutako arriskuen proportzionaltasun-eskakizunek Informazioaren Segurtasuneko arduradunaren iritziz hori justifikatzen ez duten kasuetan izan ezik.
- ***Lehenetsitako segurtasuna, gutxieneko pribilegioa***: sistemak diseinatzean eta konfiguratzean, kontuan izan behar da gutxieneko pribilegioa eta lehenetsitako segurtasuna bermatu behar direla:
    - Sistemak behar den funtzionaltasun minimoa emango du erakundeak bere helburuak lor ditzan.
- Jarduteko, administratzeko eta jarduera erregistratzeko ***funtzioak*** beharrezkoak diren gutxienekoak izango dira, eta ziurtatuko da pertsonak bakarrik irits daitezkeela haietara, edo baimendutako kokaleku edo ekipoetatik, eta, hala badagokio, ordutegi-murrizketak eta baimendutako sarbide-puntuak eskatu ahal izango dira.
- Ustiapen-sistema batean, konfigurazioa kontrolatuz, ezabatu edo desaktibatu egingo dira beharrezkoak ez diren funtzioak, baita lortu nahi den helbururako desegokiak direnak ere.
- Teknologia desberdinetarako segurtasuna konfiguratzeko gidak aplikatuko dira, sistemaren kategorizaziora egokituak, beharrezkoak ez diren edo egokiak ez diren funtzioak kentzeko edo desaktibatzeko.
- Sistemaren ohiko erabilera erraza eta segurua izatea bermatuko da, erabilera ez-seguruak erabiltzailearen ekintza kontzientea eskatzen baitu.
- ***Sistemaren osotasuna eta eguneratzea***: elementu fisiko edo logiko orok baimen formala beharko du sisteman instalatu aurretik. Sistemen segurtasun-egoera une oro ezagutu behar da, fabrikatzaileen espezifikazioei, ahultasunei eta eragiten dieten

eguneratzeei dagokienez, eta prestasunez erantzun behar da, arriskua kudeatzeko, fabrikatzaileen segurtasun-egoera ikusita.

- ***Biltegiratutako eta iragaitzazko informazioaren babesa***: sistemaren segurtasunaren egituran eta antolamenduan, arreta berezia eskainiko zaio biltegiratutako informazioari edo seguruak ez diren inguruneetatik iragaitzazkoari. Ingurune ez-segurutzat joko dira ekipo eramangarriak, tabletak, telefono mugikorrak, gailu periferikoak, informazio-euskarriak eta sare irekietako edo zifratze ahuleko komunikazioak.
- ***Paperezko euskarria***: ENSak aipatzen duen informazio elektronikoaren zuzeneko kausa edo ondorio izan den euskarri ez-elektronikoko informazio oro haren segurtasun-maila berarekin babestu beharko da. Horretarako, dauden euskarriaren izaerari dagozkion neurriak aplikatuko dira, euskarrien segurtasunari aplikatu beharreko arauen arabera.
- ***Elkarri lotutako beste informazio-sistema batzuen aurreko prebentzioa:*** sistemak perimetroa babestu behar du, bereziki, sare publikoetara konektatzen bada. Komunikazioen sare publikotzat hartuko da oso-osorik edo nagusiki herritarrentzat eskuragarri dauden komunikazio elektronikoen zerbitzuak emateko erabiltzen den komunikazio elektronikoen sarea. Nolanahi ere, sistema beste sistema batzuekin sareen bidez konektatzeak dakartzan arriskuak aztertuko dira, eta lotura-puntua kontrolatuko da.
- ***Jardueraren erregistroa eta kode kaltegarriaren detekzioa***: ENSaren xedea betetzeko helburu esklusiboarekin, ohorerako, norberaren eta familiaren intimitaterako eta kaltetuen irudirako eskubidearen berme guztiekin, eta datu pertsonalak, funtzio publikokoak edo lanekoak babesteko araudiaren eta aplikatzekoak diren gainerako xedapenen arabera, erabiltzaileen jarduerak erregistratuko dira, eta behar ez diren jarduerak monitorizatzeko, aztertzeko, ikertzeko eta dokumentatzeko behar den informazioa atxikiko da, baimendu gabeko informazio-sareei sarbidea ukatzeko, baimenik gabeko informazio-sareak saihesteko, bai eta baimenik gabeko informazio-sareei sarbidea ukatzeko, bai baimenik gabeko informazio-sareei erasoak saihesteko, bai baimenik gabeko informazio-sareak ukatzeko, baimenik gabeko erasoak saihesteko, bai baimenik gabeko informazio-sareak saihesteko.
- ***Segurtasun-intzidenteen kudeaketa eta jardueraren jarraitutasuna***: EEEren sistemek segurtasun-kopiak izango dituzte, eta operazioen jarraitutasuna bermatzeko beharrezko mekanismoak ezarriko dituzte, maila onargarrien barruan, ohiko lan-baliabideak galduz gero.
- ***Segurtasun-prozesuaren etengabeko hobekuntza***: ezarritako segurtasun-prozesu integrala etengabe eguneratu eta hobetuko da. Horretarako, informazioaren teknologien kudeaketari buruz Estatuan eta nazioartean onartutako irizpide eta metodoak aplikatuko dira.

6. SISTEMAREN KATEGORIZAZIOA

Sistemaren kategorizazioa arduradunetako bakoitzak egiten duen zerbitzuen eta informazioaren balorazioaren arabera ezartzen da.

Zerbitzuak eta informazioa baloratzeko, 311/2022 Errege Dekretuaren I. eranskineko 1. puntuko Oinarriak jarraibideei jarraituko zaie, informazio-sistema baten segurtasun-kategoria zehazteko; izan ere, bertan ezartzen da ezen, ezarritako oinarrizko printzipioak eta gutxieneko

eskakizunak betetzeko, eranskin honetan adierazitako segurtasun-neurriak aplikatuko direla, eta neurri horiek ondorengoen proportziozkoak izango dira:

- Babestu beharreko sistemako segurtasun-dimentsio garrantzitsuak.
- Babestu beharreko informazio-sistemaren segurtasun-kategoria.

Euskarri osagarri gisa, "CCN-STIC 803 - ENS Sistemen balorazioa" gida erabil daiteke.

7. INFORMAZIOAREN SEGURTASUNARI BURUZKO ARAUDIA

EEEk hainbat mailatan egituratutako dokumentu-esparrua ezartzen du, dokumentu honetan zehaztutako jarraibideek berariazko garapena izan dezaten. Nolanahi ere, garatzen diren politika, araudi eta erregulazio espezifikoek bat etorri behar dute Informazioaren Segurtasunerako Politika honekin, eta haren ondorio izan behar dute.

Aipatutako dokumentu-esparruaren osaera honako hau da:

- **Informazioaren segurtasun-politika**: Dokumentu honek osatzen du, eta nahitaez bete behar da. Zuzendaritza Nagusiak onetsiko du.
- **Araudiak**: Informazioaren segurtasunerako politika honetatik sortzen dira, eta segurtasunaren arlo guztiak hartzen dituzte. Segurtasun Batzordeak onartu behar ditu.
- **Segurtasun-prozedurak**: Informazioaren segurtasunerako politika honetatik sortzen dira, eta segurtasunaren arlo guztiak hartzen dituzte. EEEko Informazioaren Segurtasuneko arduradunak onartuko ditu.
- **ITei buruzko gida espezifikoak edo jarraibide teknikoak** Informazioaren segurtasunarekin lotutako jarduera tekniko jakin bat egiteko jarraitu beharreko jarraibide espezifikoak deskribatzen dituzten dokumentuen multzoa. EEEko Informazioaren Segurtasuneko arduradunak onartuko ditu.
- **Beste dokumentu batzuk**: Aipatutako dokumentuez gain, segurtasun-dokumentazioak beste batzuk ere izan ditzake, hala nola gomendioak, jardunbide egokiak, txostenak, erregistroak, ebidentzia elektronikoak, aurkezpenak eta abar.

Informazioaren segurtasun-politika (lehen maila) Zuzendaritza Nagusiak onartuko du, Segurtasun Batzordeak proposatuta.

Izaera orokorreko arauak (bigarren mailakoak) EEEko Segurtasun Batzordeak onartuko ditu, Informazioaren Segurtasuneko pertsona arduradunak proposatuta.

Prozedurak eta *segurtasun-gidak* edo *segurtasun-jarraibideak* (hirugarren eta laugarren mailak) Informazioaren Segurtasuneko pertsona arduradunak onartzen ditu, zerbitzuen arduradunekin eta sistemen arduradunarekin lankidetzan.

Interneten eskuragarri egon behar du Informazioaren Segurtasunerako Politika honek, eta onartzen diren araudiak dagokien zerbitzuetako arduradun guztiei jakinarazi behar zaizkie. Gainerako dokumentazio espezifikoa eskuragarri egongo da EEEren intranetean, baldin eta haren aplikagarritasunak erabiltzaile guztiei eragin badiezaieke. Baldintza horiek ez betetzeak diziplina-erantzukizuna ekar dezake.

8. GORABEHEREN KUDEAKETA

Arloek edo eremuek prestatuta egon behar dute gorabeherei aurrea hartzeko, antzemateko, erreakzionatzeko eta errekuperatzeko, ENSaren 7. artikuluaren arabera.

8.1. PREBENTZIOA

Segurtasun-gorabeherek informazioari edo zerbitzuei kalte egitea saihestu behar dute sailek, edo, gutxienez, ahal den neurrian prebenitu. Horretarako, ENSak zehaztutako gutxieneko segurtasun-neurriak ezarri behar dituzte eremuek, bai eta mehatxuen eta arriskuen ebaluazioaren bidez identifikatutako edozein kontrol gehigarri ere. Kontrol horiek eta langile guztien segurtasun-rolek eta -erantzukizunek argi definituta eta dokumentatuta egon behar dute.

Informazioaren segurtasun-politika hori betetzen dela bermatzeko, arloek hau egin behar dute:

- Sistemak baimentzea lanean hasi aurretik.
- Segurtasuna aldizka ebaluatzea, eta ohiko moduan egindako konfigurazio-aldaketen ebaluazioak egitea.
- Hirugarrenek aldizka berrikustea eskatzea, ebaluazio independentea lortzeko.

8.2. DETEKZIOA

EEEk bere informazio-sistemen eragiketa-kontrolak ezartzen ditu, zerbitzuak ematean anomaliak detektatzeko eta horren arabera jokatzeko, ENSaren 9. artikuluan ezarritakoaren arabera (aldizkako berrebaluazioa). Normaltzat aurrez ezarritako parametroen desbideratze nabarmena gertatzen denean (ENSaren 8. artikuluan adierazitakoaren arabera. Babes-lerroak), behar diren detekzio-, analisi- eta informazio-mekanismoak ezarriko dira, arduradunengana erregulartasunez irits daitezen.

8.3. ERANTZUNA

Zuzendaritza-organo arduradunek segurtasun-gorabeherei eraginkortasunez erantzuteko mekanismoak ezarri behar dituzte.

8.4. BERRESKURATZEA

Zerbitzuen eskuragarritasuna bermatzeko, EEEk beharrezko baliabide eta teknikak ditu, zerbitzu kritikoenak berreskuratzea bermatzeko. EEEren Segurtasun Araudian jasotako prozedurak eta arauak dira.

9. ZUZENDARITZAREN LIDERGOA ETA KONPROMISOA

EEEko Zuzendaritza Nagusiak erakundearen ENSa ezartzeko, ezartzeko, mantentzeko eta hobetzeko behar diren baliabideak emateko konpromisoa hartzen du, baita horrekiko lidergoa eta konpromisoa erakustekoa ere, Segurtasun Batzordea eratuz. Horren ardura izango da:

- Informazioaren segurtasunari buruzko politika hau eta informazioaren segurtasunari buruzko helburuak ezartzen direla ziurtatzea, eta helburuok EEEren estrategiarekin bateragarriak izatea.
- Konpainiaren zerbitzu eta prozesuetan ENSaren baldintza aplikagarriak integratzen direla eta betetzen direla ziurtatzea.
- ENSerako behar diren baliabideak eskuragarri daudela ziurtatzea.
- Segurtasun-kudeaketa eraginkorra eta ENSaren betekizunekin bat datorrenaren garrantzia jakinaraztea.
- ENSak aurreikusitako emaitzak lortzen dituela ziurtatzea.
- Pertsonak zuzentzea eta babestea, ENSaren eraginkortasunari laguntzeko.
- Etengabeko hobekuntza sustatzea.
- Zuzendaritzako beste rol egoki batzuei laguntzea, informazioaren segurtasuneko erantzukizun-arloak gidatuz.

10. KONTZIENTZIAZIOA ETA PRESTAKUNTZA

Segurtasun Batzordeari dagokio EEEren eremuan informazioaren segurtasunari buruzko prestakuntza eta kontzientziazioa sustatzea.

Langile guztiak informazioaren segurtasunaren arloan trebatzeko eta kontzientziatzeko jarduera espezifikoak egingo dira, bai eta Informazioaren Segurtasun Politika eta haren arau-garapena hedatzeko ere, eta langile sartu berriei zuzenduta egongo dira bereziki. Horretarako, EEEren prestakuntza-planetan informazioaren segurtasunari eta pribatutasunari buruzko jarduera espezifikoak sartuko dira.

11. INFORMAZIOAREN SEGURTASUN-ARRISKUEN KUDEAKETA

Informazioaren segurtasun-politika honi lotutako informazio-sistema guztiek informazioaren segurtasun-arriskuak aztertu behar dituzte, eta haien mehatxuak eta arriskuak ebaluatu. Azterketa hori errepikatu egingo da:

- Erregularki, gutxienez urtean behin.
- Erabilitako informazioa aldatzean.
- Egindako zerbitzuak aldatzen direnean.
- Segurtasun-gorabehera larriren bat gertatzen denean.
- Ahultasun larriak daudenean.

Zerbitzuen eta informazioaren arduradunek beren sailari eragiten dioten arriskuen aurrean erantzun behar dute, eta haien jarraipena eta kontrola bermatu behar dute. Horretarako, segurtasun-arduradun eta sistemen arduradun direnen parte-hartzea eta aholkularitza izango dute prozesuan.

Arriskuen analisia egiteko, Zentro Kriptologiko Nazionalak (CCN) egindako gidak hartuko dira kontuan. Arriskuen ebaluazio hori aldian-aldian errepikatuko da informazio-sistemetarako, zentro horrek egindako gomendioak kontuan hartuta.

EEEk konpromisoa hartu du, eta Zerbitzuen eta Informazioaren arduradunek obligazioa dute arriskuak aztertzeko eta haien ondorioei erantzuteko.

12. HIRUGARRENEN ALDEA

EEEk zerbitzuak ematen dituenean edo beste erakunde batzuetako informazioa erabiltzen duenean, Informazioaren Segurtasunerako Politika honen partaide egingo dira. Segurtasun Batzordearen txostena eta koordinazioa egiteko bideak ezarriko dira, eta segurtasun-gorabeheren aurrean erreakzionatzeko jarduera-prozedurak ezarriko dira.

EEEk hirugarrenen zerbitzuak erabiltzen dituenean edo informazioa hirugarrenei lagatzen dienean, Informazioaren Segurtasunerako Politika honen eta zerbitzu edo informazio horiei dagokien Segurtasun Araudiaren partaide egingo dira. Aipatutako hirugarren zati hori Segurtasun Araudian ezarritako betebeharren mende egongo da, eta hura betetzeko eragiketa-prozedura propioak garatu ahal izango ditu. Gorabeherak jakinarazteko eta ebazteko berariazko prozedurak ezarriko dira. Bermatu egingo da hirugarrenen langileak behar bezala kontzientziatuta egotea segurtasunaren arloan, Informazioaren Segurtasunerako Politika honetan ezarritako maila berean gutxienez.

Informazioaren segurtasun-politika honetako alderdiren bat ezin bada bete hirugarren alde baten aldetik, aurreko lerrokadetan eskatzen den moduan, informazioaren segurtasunaren arduradunaren txostena beharko da, zer arrisku dauden eta nola tratatu behar diren azaltzeko. Aurrera egin baino lehen, eragindako zerbitzuen eta informazioaren arduradunek txosten hori onartu beharko dute.

13. LANGILEEN BETEBEHARRAK

Erakundeko erabiltzaile guztiek ezagutu eta bete behar dituzte Informazioaren Segurtasunerako Politika hori eta politika horretatik abiatuta garatutako segurtasun-arauak eta -jarraibideak, eta Segurtasun Batzordearen ardura da behar diren baliabideak ezartzea informazioa ukituengana irits dadin.

EEEren erabiltzaile guztiek segurtasun informatikoaren arloko kontzientziazio-saio bat egingo dute, gutxienez urtean behin. Kontzientziazio jarraituko programa bat ezarriko da EEEren erabiltzaile guztiei arreta emateko, batez ere sartu berriei.

Sistema informatikoak eta telekomunikazioak erabiltzeko, erabiltzeko edo administratzeko ardura duten pertsonek prestakuntza jasoko dute sistemak modu seguruan erabiltzeko, beren lana egiteko behar duten neurrian. Prestakuntza derrigorrezkoa izango da erantzukizun bat bere gain hartu aurretik, bai lehenengo esleipena bada, bai lanpostua edo erantzukizunak aldatzen badira.

EEEren prozesuetan parte hartzen duten barne- edo kanpo-erabiltzaile guztiek nahitaez bete behar dute Informazioaren Segurtasunari buruzko Politika hau, eta hori ez betetzea lan-arloko arau-hauste larria izango da.

14. INFORMAZIOAREN SEGURTASUN-POLITIKA ONARTZEA ETA BERRIKUSTEKO PROZESUA

Informazioaren Segurtasunerako Politika hau eta EEEk horren ondorioz sortutako Segurtasun Araudia berrikusi eta eguneratzea sustatzen da.

Informazioaren Segurtasunerako Batzordeak berrikusiko du Informazioaren Segurtasunerako Politika tarte planifikatuen bidez. Tarte horiek bi urtetik beherakoak izan beharko dira, edo aldaketa esanguratsuak egin beharko dira, politika horren egokitasunari, egokitasunari eta eraginkortasunari eusteko. Berrikuspen-proposamena, hala badagokio, alderdi interesdun guztiek ezagutu dezaten onartu eta zabalduko da.

Dokumentu honetan egin beharreko aldaketak dagokion goi-organo eskudunak onartu beharko ditu, ENSaren 12. artikuluaren arabera. EEEren izaera dela eta, ezinbestekoa da antolaketan koherentzia kontuan hartzea eta zaintzea.

Edozein aldaketa eginez gero, eragindako alderdi guztiei jakinarazi beharko zaie.

Bilbao, 2025eko uztailaren 8a

ZUZENDARITZAREN SINADURA