AGINDUA, 2019KO URTARRILAREN 23KOA, SEGURTASUNEKO SAILBURUARENA, INFORMAZIOAREN SEGURTASUN-POLITIKA ONARTZEN DUENA SEGURTASUN SAILAK KUDEATUTAKO SARE- ETA INFORMAZIO-ZERBITZUEN ALORREAN.

Segurtasun Sailak bere arduraren pean du segurtasun publikoaren alorreko komunikazio-sare eta informazio-sistemen plangintza eta mantentzea, honako hauen arabera: Euskadiko Segurtasun Publikoaren Sistema Antolatzeko ekainaren 28ko 15/2012 Legearen 14. eta 17. artikuluak; 24/2016 Dekretua, azaroaren 26koa, Lehendakariarena, Euskal Autonomia Erkidegoaren Administrazioko sailak sortu, ezabatu eta aldatzen dituena eta horien egitekoak eta jardun-arloak finkatzen dituena, eta 83/2017 Dekretua, apirilaren 11koa, Segurtasun Sailaren egitura organikoa eta funtzionala ezartzen duena.

Komunikazio-sare eta informazio-sistema horiek ezinbestekoak dira segurtasun publikoa babesteko, eta beraz, haien babesa eta prestazioaren jarraikortasuna bermatu behar dira hala zerbitzuak emateko inplikatuta eta elkarrekin lotuta dauden agentzien funtzionamenduari dagokionez, nola administrazio elektronikoaren alorrean herritarrekin dauden harremanei dagokienez.

Informazioaren segurtasunaren babesa arautzera etorri dira zenbait xedapena azken urteotan. Alde batetik dugu 3/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoaren esparruko Segurtasunerako Eskema Nazionala arautzen duena, 951/2015 Errege Dekretuak aldatua, eta beste alde batetik, datuak babesteko araubide berritzailea dago: Datuak Babesteko Erregelamendu Orokorra eta haren transposizioa, Datu Pertsonalak Babesteko eta Eskubide Digitalak Bermatzeko abenduaren 5eko 3/2018 Lege Organikoaren bidez gauzatua. Kontuan hartu behar da, gainera, 12/2018 Errege Lege Dekretua, irailaren 7koa, Informazio Sare eta Sistemen Segurtasunarena, bai eta, aplikatu behar diren kasuetan, azpiegitura kritikoak babesteari buruzko araubideak duen eragina ere.

Arau horiek guztiak, nahiz eta ondasun juridiko diferenteak izan babesgai, bat datoz sare eta informazio-sistemei segurtasun-neurriak ezartzerakoan, osagarritzat ulertu behar baitira, Datu Pertsonalak Babesteko eta Eskubide Digitalak Bermatzeko abenduaren 5eko 3/2018 Lege Organikoaren lehenengo xedapen gehigarrian xedatuta dagoena betez.

Eusko Jaurlaritzak ere onartu du Eusko Jaurlaritzaren informazioaren segurtasuna kudeatzeko sistema bat, erreferentziatzat hartuta segurtasunerako eskema nazionala, eta hauek xedatu dutena kontuan hartuta: Administrazio Elektronikoari buruzko otsailaren 21eko 21/2012 Dekretua; otsailaren 26ko Agindua, zeinen bidez onartzen baita Euskal Autonomia Erkidegoko Administrazio Orokorrean eta haren Erakunde Autonomoetan informazio-segurtasuna mantentzeko Segurtasun Eskuliburua, eta Gobernu Kontseiluaren erabaki bat, 2015eko ekainaren 30ekoa, zeinaren bidez onartzen den Eusko Jaurlaritzaren Administrazio Elektronikorako egituraketa eta segurtasun-rolen

esleipena. Era berean, kontuan hartu behar da 2018ko ekainaren 19ko Gobernu Kontseiluaren Erabakia, zeinaren bidez onartzen baitira Euskal Autonomia Erkidegoko Administrazio Publikoak tratatutako datu pertsonalen babeserako egituraketa eta rolen esleipena.

Informazioaren segurtasunerako politika horren berezko eremuak, erreferentziatzat hartutako segurtasunerako eskema nazionalak bezala, ez ditu barruan hartzen segurtasun-administrazioaren funtzionamenduaren oinarri diren sare eta informazio-sistema guztiak, baizik eta administrazio elektronikoaren berezko zerbitzuak bakarrik.

Hala ere, segurtasun-administrazioaren jardunaren zati handi bat prozedurarik gabeko ekimen materialetan jorratzen da, zeinen euskarria irtenbide teknologikoak erabiltzea baita. Irtenbide teknologiko horiek ezinbestekoak dira, kritikoak, eta segurtasun-neurri batzuk behar dituzte, administrazioaren beste edozein alorretako ohiko estandarrak gainditzen dituztenak.

Bestalde, segurtasun publikoko agintaritzek datuak tratatzen dituztenean legez kontrako ekimenak prebenitzeko, ikertzeko, detektatzeko edo epaitzeko, datuak babesteko araubide komunetik salbuesten dira eta Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/680 (EB) Zuzentarauari lotzen zaizkio, arau horrek transposizioa egiteke badu ere oraindik.

Berezitasun horiek ez dute galarazten alor horretan hartzen diren neurriek koherenteak izatea, eta erreferentziatzat hartzea Administrazio osoarentzako ezarritako neurriak. Hala ere, gogoan hartu behar dira dauden berezitasunak eta segurtasun publikoa zaintzeko ekintzak, barnean hartuta sailkatutako informazioa babestekoak (bai eta ezagutaraziz gero, interes orokorraren kontrako bihurtuko litzatekeen informazioa ere), edota helburutzat dutenak ordena publikoa mantentzea eta delituak detektatu, ikertu eta jazartzea eta delitugileak epaitzea.

Horregatik, egokitzat jo da Segurtasun Sailaren barruan onartzea berak kudeatzen dituen sareen eta informazio-sistemen segurtasun-politika propioa. Segurtasun-politika horrek, herritarrekiko harreman elektronikoen alorrari dagokionez, bat egiten du Eusko Jaurlaritzaren Administrazio Orokorrarentzat eta bere erakunde autonomoentzat ezarritako informazioaren segurtasunerako politikarekin, baina kontuan hartzen ditu, bai eta babesten ere, segurtasun publikoaren alorreko berezitasunak gainerako sareetan eta informazio-sistemetan.

Horregatik guztiagatik, honako hau

EBAZTEN DUT

Lehenengoa.- Onarpena ematea Informazioaren Segurtasun Politikari (aurrerantzean ISP) Eusko Jaurlaritzako Segurtasun Sailean. Honen eranskin gisa doa.

Bigarrena.- Agindu hau Eusko Jaurlaritzaren egoitza elektronikoan, Segurtasun Sailaren webgunean eta sailetako intranetetan argitaratuko da.

Vitoria- Gasteiz, (sinadura digitala).

ESTEFANIA BELTRÁN DE HEREDIA ARRONIZ
SEGURTASUNEKO SAILBURUA

ERANSKINA

INFORMAZIOAREN SEGURTASUN-POLITIKA
EUSKO JAURLARITZAKO
SEGURTASUN SAILA

1. Xedea eta aplikazio-eremua.

1.1. Agiri honen xedea da: Informazioaren Segurtasun Politika (aurrerantzean ISP) definitzea Eusko Jaurlaritzako Segurtasun Sailean eta haren erakunde autonomoan, bai eta politika horren antolamendu- eta teknologia-esparrua ezartzea ere.

1.2. ISP hau Segurtasun Sailaren sare eta informazio-sistemetan aplikatuko da, eta derrigorrez bete beharko dute sailaren eta haren erakunde autonomoaren organo eta unitate guztiek, baita sail honen informazio-sistemetara irispidea duten langile guztiek ere, berdin dio langile horiek zer destino, adskripzio eta sailarekiko harreman duten.

1.3. Administrazio Elektronikoari buruzko otsailaren 21eko 21/2012 Dekretuaren xedapenek administrazio elektronikoari definitu dioten eremuari dagokionez, Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sisteman zehaztutakoari begiratuko zaio.

1.4.- Segurtasun Sailak kudeatzen dituen gainerako informazio-sare eta -sistemei dagokienez, agiri honetan eta bere garapen eta ezarpenetan definitutakoari begiratuko zaio.

Hala ere, erreferentetzat hartuko dira Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sistemak administrazio elektronikorako aurreikusi dituen zuzentarauak eta segurtasun-neurriak, hargatik eragotzi gabe segurtasun publikoa zaintzeko behar diren neurriak, barnean hartuta sailkatutako informazioa babestekoak (bai eta ezagutaraziz gero, interes orokorraren kontrako bihurtuko litzatekeen informazioa ere), edota helburutzat dutenak ordena publikoa mantentzea eta delituak detektatu, ikertu eta jazartzea eta delitugileak epaitzea.

2. Segurtasun-printzipioak

ISP honen garapena, oro har, printzipio hauen arabera egingo da:

a) Segurtasun integrala:

Segurtasuna prozesu integral gisa ulertuko da, sistemarekin zerikusia duten elementu tekniko, giza elementu, antolaketa-elementu eta elementu material guztiek osatua, alde batera utzita jarduketa puntual edo tratamendu koiuntural oro.

Arretarik handiena emango zaio prozesuan parte hartzen duten pertsonen eta haien arduradun hierarkikoen kontzientziazioari, ezjakintasuna, antolamendurik eta koordinaziorik eza eta jarraibide desegokiak segurtasunerako arrisku-iturri izan ez daitezen.

Aktiboen bizi-ziklo osoan zehar begiratuko zaie informazioaren segurtasunaren eskakizunei, plangintzatik hasita erretiratu arte.

b) Arriskuaren kudeaketa:

Honetan datza informazioaren segurtasunaren kudeaketa: arriskuak aztertzea, segurtasun-neurri egokiak, eraginkorrak eta neurrikoak ezartzea, eta etengabeko zuzenketa eta hobekuntza ere kontuan hartzea, erakundea gero eta prebentiboagoa izan dadin, erreaktiboa baino, segurtasun-gorabeheren aurrean, inguruneari kontrolpean eutsi ahal izateko.

Arriskuen kudeaketari esker, kontrolpean eutsiko zaio inguruneari, arriskuak maila onargarrietaraino minimizatuta. Maila horiek jaisteko, segurtasun-neurriak hedatuko dira, oreka ezarrita da datuen izaeraren eta tratamenduen artean, bai eta haiek dituzten arriskuen eta segurtasun-neurrien artean ere.

Arriskuen azterketa eta kudeaketa funtsezko atala izango da segurtasun-prozesuan, eta beti egon beharko da eguneratuta.

c) Eskuragarritasuna, jarraitutasuna eta kontserbazioa:

Ahalegina egin behar da aktiboak eskuragarri egon daitezen, haietara iristeko baimena duten pertsonek eskatzen dutenean. Horretarako, zerbitzuak etenik gabe ematea bermatuko da, bai eta, gorabehera edo kontingentziarik gertatuz gero, zerbitzuok berehala lehengoratuko direla ere, zerbitzuak eta haiei lotutako informazioa lehengoratzeko jarraitutasun-neurrien bidez.

Halaber, datuak eta informazioak euskarri elektronikoan kontserbatzea bermatuko da. Era berean, sistemak eskuragarri mantenduko ditu zerbitzuak informazio digitalaren bizi-ziklo osoan; horretarako, ondare digitala iraunarazteko oinarri izango diren kontzepzio eta prozedurak erabiliko dira.

d) Osotasuna edo integritatea:

Esku arteko informazioa osoa eta zehatza izatea segurtatu beharko da, informazioaren edukiaren eta zerikusia duten prozesuen zehaztasuna nabarmenduta.

e) Konfidentzialtasuna:

Hau bermatu beharko da: horretarako berariazko baimena dutenek bakarrik iristea aktiboetara.

f) Autentikotasuna:

Hau bermatu beharko da: informazioa solaskide egokietatik datorrela eta solaskide egokiekin trukatzen dela, eta zerbitzuak behar bezala akreditatzea.

g) Trazabilitatea:

Hau bermatu beharko da: informazioaren gaineko eragiketen eta hala eskatzen duten zerbitzuen jarraipena.

h) Prebentzioa, erreakzioa eta lehengoratzea:

Sistemaren segurtasunak kontuan hartu behar ditu prebentzioaren, detekzioaren eta zuzenketaren alderdiak, sistemaren gaineko mehatxuak gauza ez daitezen, eta larriki eragin ez diezaien esku arteko informazioari edo ematen diren zerbitzuei. Berariazko lan-plan eta -ildoak garatuko dira, segurtasunarekin zerikusia duten iruzurrak, ez-betetzeak edo gorabeherak prebenitzeko.

Prebentzio-neurriek ezabatu egin behar dute, edo gutxitu behintzat, mehatxuak sistemaren kalterako gauzatzeko aukera. Prebentzio-neurri horiek barnean hartuko dituzte, besteak beste, disuasioa eta esposizio-murrizketa.

Detekzio-neurriekin batera joango dira erreakzio-neurriak, segurtasun-intzidenteak garaiz eragozteko.

Berreskuratze-neurriek informazioa eta zerbitzuak lehengoratzeko aukera emango dute, halako moldez non aurre egin ahal izango zaien segurtasun-intzidente batek ohiko bideak desgaitzen dituen egoerei.

i) Defentsa-lerroak eta mailakatzea:

Sistemek defentsa-lerrozko babes-estrategia bat izan behar dute, segurtasun-geruza askok osatua. Honela paratuko dira geruza horiek: batek huts eginez gero, denbora irabazteko moduan egoki erantzuteko ezin saihestuzko intzidenteei; sistema osoa konprometitzeko aukera murrizteko, eta sistemarekiko azken inpaktua minimizatzeko.

Antolaketa-, fisika- eta logika-izaerako neurriek osatuko dituzte defentsa-lerroak.

j) Etengabeko hobekuntza eta berrebaluazio periodikoa:

Behin eta berriz berrikusiko da erakundean ezarritako segurtasun-kontrolen efikaziaren maila, arriskuen eta ingurune teknologikoaren etengabeko bilakaerari egokitzeko ahalmena handitzeko.

Segurtasun-neurriak aldian-aldian berrebaluatu eta eguneratuko dira, neurri horien efikazia egokitzeko arriskuen eta babes-sistemen etengabeko bilakaerara, are segurtasuna bera birplanteatzeraino, beharrezkoa izanez gero.

k) Proportzionaltasuna kostuari dagokionez:

Aktiboen segurtasun-arriskuak arintzeko neurrien ezarpena horretarako aurrekontu-esparruaren barruan egin beharko da, eta beti bilatu beharko da oreka segurtasun-neurrien, informazioaren izaeraren eta aurreikusitako aurrekontuaren artean.

l) Kontzientziazioa eta prestakuntza:

Informazioaren segurtasunaren alorreko prestakuntza-, sentsibilizazio- eta kontzientziazio-programak eratuko dira erabiltzaileentzat. Programa horiek behar bezalako oinarria hartuko dute politika korporatiboetan, eta jarraipen- eta eguneratze-prozesu egokia izango dute.

m) Funtzio bereiziak:

Informazio-sistemetan, bereizi egingo dira, alde batetik, informazio-sistemen segurtasunaren ardura, eta, bestetik, zerbitzuen prestazioaren gaineko ardura; bereizi ere, agindu honetako rol edo zereginen esleipenean ezarritakoaren arabera, arduradun bakoitzaren eskuduntzak zedarritzen baititu, bai eta koordinazio-mekanismoak eta gatazkak ebaztekoak ere.

Informazioaren arduradunak tratatutako informazioaren betekizunak zehaztuko ditu; zerbitzuaren arduradunak, berriz, emandako zerbitzuen betekizunak zehaztuko ditu, eta segurtasun-arduradunak, azkenik, informazioaren eta zerbitzuen segurtasun-betekizunak betetzeko erabakiak zehaztuko ditu.

n) Araubidea betetzea:

Informazio-sistema guztiek eta lotutako prozesu guztiek bete beharko dute informazio-segurtasunari eragiten dion eta legez aplikatzekoa den arautegi orokorra zein sektoriala; bereziki, intimitatearekin eta izaera pertsonaleko datuen babesarekin eta sistemen, datuen, komunikazioen eta zerbitzu elektronikoen segurtasunarekin zerikusia duen hori, herritarrei eta administrazio publikoei aukera ematen baitie eskubideak baliatu eta betebeharrak betetzeko teknologiaren bitartez.

3.- Antolamendu-egitura.

ISP hau antolamendu-egitura honen bitartez atontzen da:

a) Informazioaren arduraduna.
b) Zerbitzuaren arduraduna.
c) Segurtasunaren arduraduna.
d) Sistemaren arduraduna.
e) Informazioaren segurtasunerako eta pribatutasunerako goi-batzordea.
f) Informazioaren segurtasunerako eta pribatutasunerako batzorde teknikoa.

4.- Informazioaren arduraduna.

4.1. Informazioaren arduraduna pertsona edo korporazio-organo bat da, bere ahaltzat duena informazioaren betekizunak ezartzea segurtasunaren alorrean edo informazioaren segurtasun-mailak zehaztea, jaramon eginda informazioaren segurtasunerako batzordeak finkatutako jarraibideei, edo hala, badagokio Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sistemak ezarritakoei.

4.2. Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sistemarekin bat eginez, informazioaren arduradun izango dira, dagokien eremuan, Zerbitzu Zuzendaritzaren titularra eta erakunde autonomo bakoitzari dagokion pertsona bakarreko gobernu organoa.

4.3. Segurtasun publikoarekin zerikusia duten gainerako informazio-sare eta -sistema departamentaletan, Segurtasuneko sailburuordea edo haren ordezkaria edo ordezkariak izango dira informazioaren arduradun. Hauek egokituko zaizkie:

a) Tratatutako informazioaren segurtasun-mailak zehaztea, segurtasun-arduradunak txostena egin ondoren, informazioaren segurtasunari eragiten dieten intzidenteen inpaktuak baloratuta.

b) Zerbitzuen arduradunekin batera eta segurtasunaren arduradunaren parte-hartzearekin, nahitaezko arrisku-analisiak egitea eta ezarri beharreko zaintzak aukeratzea.

C) Onarpena ematea informazioari buruzko hondar-arriskuei, arrisku-analisian kalkulatu baitira.

d) Informazioaren segurtasun-mailak zehazte aldera, informazioaren arduradunak txostena eskatuko dio segurtasunaren arduradunari.

e) Informazioaren arduraduna arduratuko da pribatutasun-neurriez, datuen babesari aplikatu beharreko araubidearekin bat eginez, non eta ISP hau garatzeko dokumentuek besterik ezartzen ez duten.

5.- Zerbitzuaren arduraduna.

5.1. Zerbitzuaren arduraduna pertsona edo korporazio-organo bat da, bere ahaltzat duena emandako zerbitzuen betekizunak ezartzea. Zerbitzuaren segurtasun-mailak zehaztuko ditu segurtasun-dimentsio bakoitzean.

5.2. Zerbitzuaren arduradun izango dira Segurtasun Sailaren organoetako eta haren organismo autonomoetako titularrak, aginduta dituzten zerbitzuei dagokienez.

5.3.- Zerbitzu bakoitzaren arduradunei dagokie:

a) Zerbitzuaren segurtasun-mailak zehaztea, zerbitzuari eragiten dieten intzidenteen inpaktuak baloratuta.

b) Informazioaren arduradunarekin batera eta segurtasunaren arduradunaren parte-hartzearekin, nahitaezko arrisku-analisiak egitea eta ezarri beharreko zaintzak aukeratzea.

c) Onarpena ematea zerbitzuei buruzko hondar-arriskuei, arrisku-analisian kalkulatu baitira.

d) Zerbitzuaren segurtasun-mailak zehazte aldera, zerbitzuaren arduradunak txostena eskatuko dio segurtasunaren arduradunari.

e) Zerbitzuaren arduradunak izango du datu-tratamenduaren ardura, datuen babesari aplikatu beharreko araubidearekin bat eginez, non eta ISP hau garatzeko dokumentuek besterik ezartzen ez duten.

6.- Segurtasunaren arduraduna

6.1. Segurtasunaren arduradunak segurtasun-estandarrak eta -betekizunak ezarri behar dizkie Euskadiko Segurtasun Publikoaren Administrazioaren jarduerari eusten dioten informazio-sare eta -sistemei, eta egokiro zehaztu aplikatu beharreko segurtasun-neurriak.

6.2. Segurtasun Sailaren barruan, segurtasunaren arduradunaren rola hartuko du Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritzako titularrak edo haren ordezkariak, hargatik eragotzi gabe beste batzuek Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sisteman izan ditzaketen eskuduntzak.

6.3. Segurtasunaren arduradunak funtzio hauek izango ditu bere jarduketa-eremuan:

a) Informazioaren segurtasunerako batzordeak emandako zuzentarauak, estrategiak eta helburuak garatzea, eta aholkularitza eta laguntza ematea hari.

b) Segurtasun-araubidea prestatzea.

c) Segurtasunerako prozedura-eragileak onartzea.

d) Informazio sistemek maneiatutako informazioaren eta emandako zerbitzuen segurtasunari eustea.

e) Auditoretza periodikoak egitea edo sustatzea, informazioaren segurtasunaren alorreko betebeharrak betetzen direla egiaztatzeko.

F) Jarraipena eta kontrola egitea informazio-sistemaren segurtasun-egoerari.

g) Ziurtatzea segurtasun-neurriak egokiak direla informazioa eta zerbitzuak babesteko.

h) Laguntza eta berrikuspena ematea segurtasun-intzidenteen ikerketan, jakinarazten direnetik ebazten direnera arte.

i) Segurtasun-txostenak egitea, aldian-aldian, informazioaren segurtasunerako batzordearentzat, aldi bakoitzeko intzidente nabarmenenak jasoz.

j) Aktiboen erregistroa gainbegiratzea.

7.- Sistemen arduraduna.

7.1. Sistemen arduradunaren ardura dira:

a) Informazio-sistema horien topologia eta kudeaketa-sistema definitzea aplikatu beharreko segurtasun-sistemekin, erabilera-irizpideak eta eskuragarri dauden zerbitzuak ezarriz.

b) Ezaugarri teknikoak eta erabilera-irizpideak modu egokian zehaztea eta eskuragarri dauden zerbitzuak ezartzea.

c) Sailak kudeatutako informatika-sistemak hedatzea eta mantentzea, hargatik eragotzi gabe Eusko Jaurlaritzako zerbitzu bateratu komunak.

d) Segurtasun-neurri espezifikoak segurtasunaren esparru nagusian egoki txertatzen direla egiaztatzea.

e) Informazio jakin baten maneiua edo zerbitzu jakin bat ematea eteteko agindua ematea, baldin eta informazioa ematen badiote segurtasun-akats larriak daudela, ezarritako baldintzak betetzeari eragin diezaioketenak. Erabaki hori bete baino lehen, eragindako informazioaren eta zerbitzuaren arduradunen eta segurtasunaren arduradunaren adostasuna beharko da.

7.2. Segurtasun Sailaren barruan, sistemen arduradunaren rola hartuko du Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritzako titularrak edo haren ordezkariak, hargatik eragotzi gabe beste batzuek Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sisteman izan ditzaketen eskuduntzak.

8.- Informazioaren segurtasunerako eta pribatutasunerako goi-batzordea (ISPGB):

8.1. Informazioaren segurtasunerako eta pribatutasunerako goi-batzordearen (ISPGB) misioa da: segurtasun-alorreko politika, ekimen eta helburuen egitura sortzea, modu koordinatuan, gastua eta disfuntzioak arrazionalizatzeko, segurtasun-akatsik gerta ez dadin, sistemak puntu ahulak izateagatik, intzidenteak edo erasoak ekar ditzaketenak.

8.2. Funtzio hauek ditu:

a) ISPren aldatze eta etengabeko eguneratze-proposamenak onartzea eta horiek betetzen direla zaintzea.

b) Segurtasun-baldintzak, zerbitzuak eta helburuak identifikatzea, baliabideak esleituz eta jarduketak lehenetsiz.

d) Etengabeko hobekuntza sustatzea informazioaren segurtasunaren kudeaketan.

e) Prestakuntza eta kontzientziazioa sustatzea.

f) Informazioaren segurtasuna kudeatzeko sistema berrikustea horren egoerari buruzko ohiko txostenak jasoz.

g) Administrazio elektronikoari dagokionez, Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sistemaren organoekiko eta beste erakunde batzuekiko harremanak koordinatzea, informazio-sare eta -sistemen segurtasun-egoeraren profil orokorra prestatzeko.

h) Datuen babeserako araubidea betetzen dela sustatzea, bereziki tratamenduak identifikatzean eta diseinatzean eta kritikotasun-mailak esleitzean; segurtasun-neurriak ezartzean edo auditoretzak egitean. Euskadiko Poliziaren Datuak Prestatzeko Zentroaren berezko eremuan, haren lankidetza izango du horretarako.

f) Gatazkak ebaztea, halakorik sortuz gero antolamenduaren arduradunen edo atalen artean, eta, ebazteko eskumen nahikorik ez duenean, kasu horiek bideratzea.

g) Lantaldeak sortzea egokitzat jotako azterketak, lanak eta txostenak egiteko.

8.3. Informazioaren segurtasunerako eta pribatutasunerako batzordeko kideak:

a) Lehendakaritza: Segurtasuneko sailburuordea.

b) Lehendakariordetza: Administrazio eta Zerbitzuetako sailburuordea, zeina lehendakaritzaz arduratuko baita titularra falta denean.

c) Honako zuzendaritza-organoen titularrak:

- Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritza, sistemen, segurtasunaren eta ustiapenaren arduraduna.
- Kudeaketa Ekonomikoaren eta Baliabide Orokorren Zuzendaritza, kudeaketako zerbitzu komunen eta Segurtasun Sailaren eraikinen, instalazioen eta azpiegituren mantentzearen arduraduna.
- Segurtasuna Koordinatzeko Zuzendaritza, polizia-artxibategien sistemen eta Euskadiko Poliziaren Datuak Prestatzeko Zentroaren arduraduna.
- Araubide Juridikoaren, Zerbitzuen eta Hauteskunde Prozesuen Zuzendaritza, Eusko Jaurlaritzaren Informazioaren Segurtasuna Kudeatzeko Sistemaren arduraduna.
- Ertzaintzaren Zuzendaritza.
- EAEko Poliziaren eta Larrialdietako Zerbitzuen Ikastegia.

d) Saileko datuen babeserako erreferentea eta, halakorik sortuz gero, polizia informazioaren sistemaren datuak babesteko ordezkaria.

e) Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritzako pertsona bat, informazio-sistemetako segurtasunaren alorreko ardura duena, informazio-sistemen batzordeko idazkari izango dena. hitz egiteko eta botoa emateko eskubidearekin. Hark bermatuko du informazioaren segurtasunerako goi-batzordearen erabakiak zuzenean edo ordezkaritzaren bitartez betetzen direla. Bileretan jorratu beharreko gaiak prestatuko ditu, deialdiak egin eta bileren aktak prestatuko ditu.

8.4. ISPGB sei hilean behin batuko da, gutxienez, lehendakaritzak hala eskatuta. Larrialdirik bada ere bilduko da, lehendakaritzak egoki iritziz gero.

8.5. ISPGBren bileretan lehendakaritzak egoki irizten dien barneko edo kanpoko aholkulariek parte hartu ahal izango dute.

9.- Poliziaren informazio sistemaren segurtasunerako eta pribatutasunerako batzordea (PISSPB).

9.1. Polizia informazioaren sistemaren (PIS) alorrean poliziaren informazio sistemaren segurtasunerako eta pribatutasunerako batzordea (PISSPB) sortzen da, informazioaren segurtasunerako eta pribatutasunerako goi-batzordearen mende.

9.2. PISSPBek funtzio hau bereganatzen du: poliziaren informazio sistemaren berezko eremuan, informazioaren segurtasun-politikaren arau-garapenak proposatzea eta bultzatzea, eta, horrez gain, alor horretan goi-batzordeak erabakitako informazioaren segurtasun-politika garatu eta egikaritzea. Horretarako:

a) Araubide garapenak eta PISen berrikuspena eta eguneraketa proposatuko ditu poliziaren informazio-sistemaren eremuan.

b) Segurtasuneko baldintzak, zerbitzuak eta helburuak egokituko ditu baliabideak esleituz eta jarduketak lehenetsiz, eta poliziaren informazio-sisteman segurtasun-neurriak sustatuko eta ezarriko ditu, eta bereziki Euskadiko Poliziaren Datuak Prestatzeko Zentroan.

c) Informazioaren-segurtasun politika betetzen dela zainduko du, bai eta haren funtzionamendua berrikusi ere ohiko txostenen eta auditoretzen bitartez.

9.3. Bere misioa betetzeko, aintzat hartuko ditu zer berezitasun datorren Europako Parlamentuaren eta Kontseiluaren 2016ko apirilaren 27ko 2016/680 (EB) Zuzentarautik eta haren transposizioa egiten duten arauetatik, bai eta, Europar Batasuneko poliziaren informazio-sistemez ari garela, haiek eraentzen dituzten arauek aurreikusitako segurtasun-arau espezifikoak ere.

9.4.- PISSPBren osaera:

a) Lehendakaritza: Segurtasuna Koordinatzeko Zuzendaritzaren titularra.
b) Lehendakariordetza: Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritza.
c) Kideak:

- Poliziaren Informazio Sistemaren Segurtasun Eragiketen Zentroaren arduradun bat.
- Ertzaintzaren Zuzendaritzak izendatutako pertsona bat, Euskadiko Poliziaren Datuak Prestatzeko Zentroan dituen arduren arabera.
- Saileko erreferentea datuen babesaren alorrean.
- Poliziaren informazio-sistemaren datuak babesteko ordezkariaren funtzioak bereganatzen dituen pertsona.
- Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritzako pertsona bat, informazio-sistemetako segurtasunaren alorreko ardura duena. Batzordeko idazkaria izango da eta hitz egiteko eta botoa emateko eskubidea izango du.

9.4. PISSPB sei hilean behin batuko da, gutxienez, baita larrialdi-inguruabarrak gertatutakoan ere. Egokitzat jotzen diren barneko eta kanpoko aholkulariek ere parte hartu ahal izango dute bileretan.

9.5. Poliziaren Informazio Sistemaren Segurtasuneko Eragiketa Zentroa (PISSEZ) Telekomunikazioak eta Sistema Informatikoak Kudeatzeko Zuzendaritzaren menpekoa da eta bermatu egiten du komunikazio-zerbitzuen erabilgarritasun-maila, aldizka gertatu daitezkeen akatsak saihestuz, arrisku eta gorabeheren eta egoeraren ezagutzaren analisi dinamikoa egiten du, intzidenteak gainbegiratzen ditu, erabiltzaile-taldeei alertak zabaltzen dizkie eta intzidenteei erantzuten die.

Horretarako, PISSEZekin harremanetan jartzeko bideak argi eta garbi zehaztuko dira, eta erabiltzaile-taldeek ondo ezagutuko dituzte.

Helburu hori lortzeko askotariko bitartekoak dituzte, eta hala, beraiekin harremanetan jartzeko aukera dago une oro.

Haren instalazioak eta laguntza-informaziorako sistemenak leku seguruetan egongo dira, eta sistema erredundanteak eta erreserbako lanerako espazioak izango dituzte.

10.- Informazioaren segurtasunerako eta pribatutasunerako batzorde teknikoa:

10.1. Informazioaren segurtasunerako eta pribatutasunerako batzorde teknikoa eratuko da, eta bertan egongo dira zerikusia duten ataletako bakoitzean informazio eta pribatutasun-neurriez arduratzen diren teknikariak, zerbitzuen eta tratamenduen arduradunak eta segurtasunaren eta sistemen arduradunak.

10.2. Batzorde tekniko horrek prestatuko du sailaren eta haren erakunde autonomoaren segurtasun-egoera orokorraren profila, organo bakoitzaren segurtasun-aldagai nagusien egoera barne hartuz. Horrez gain, sailari eragiten dioten segurtasun-politika sektorialen koherentzia bermatuko du eta laguntza emango du informazio-segurtasunaren alorrean ikerketak egiten eta intzidenteak konpontzen, bai sailean baita sailetik kanpo ere.

10.3. Lantalde horretako kideek lankidetzan jardungo dute segurtasun-arduradunarekin hark aginduta dituen zereginak egikaritzen.

11. Arriskuen kudeaketa.

11.1. Etengabe egin behar zaio arriskuen kudeaketa informazio-sistemari, arriskuetan eta aldizkako berrebaluazioetan oinarritutako segurtasunaren kudeaketa-printzipioekin bat eginez.

11.2. Informazioaren arduraduna eta zerbitzuaren arduraduna dira, hurrenez hurren informazioaren eta zerbitzuen gaineko arriskuen arduradun, eta, beraz, analisian kalkulatutako hondar-arriskuak onartzeaz arduratu behar dira, bai eta haien jarraipena eta kontrola egiteaz ere, hargatik eragotzi gabe lantegi hori eskuordetzeko aukera.

11.3. Aplikatu beharreko segurtasun-neurrien aukeraketari dagokionez, segurtasun-arduradunak proposamena egingo dio informazioaren segurtasunerako batzordeari.

11.4. Arriskuak kudeatzeko prozesuak fase hauek izango ditu: sistemen kategorizazioa, arriskuen analisia eta aplikatu beharreko segurtasun-neurriak aukeratzea, zeinak arriskuekiko proportzionalak eta justifikatuak izan beharko

diren. Segurtasun-arduradunak urtero berrikusiko du prozesu hori, eta txosten bat helaraziko dio informazioaren segurtasunerako batzordeari.

12. ISParen arau-garapena. Segurtasun-agiriak.

12.1. Informazioaren segurtasunari buruzko araudia nahitaez bete behar da, eta hiru mailatan garatuko da, aplikazio-eremuaren eta zehaztasun teknikoko mailaren arabera; hala, garapen-maila jakin bateko arau bakoitzak goragoko mailako arauak izango ditu oinarri. Hona arau-garapenaren mailak:

a) Lehenengo arau-maila: Informazioaren Segurtasun Politika eta segurtasun-zuzentarau eta -arau orokorrak, Segurtasun Sail osorako.

b) Bigarren arau-maila: Informazioaren segurtasun-arau espezifikoak eta IKT segurtasun-arauak. ISPa garatu eta zehazten dute, informazioaren segurtasunaren arlo edo alderdi jakin batean zentratuta.

c) Hirugarren arau-maila: prozesu, prozedura eta jarraibide teknikoak. Dokumentu horiek erantzuna ematen diote galdera honi, ezarpen- eta teknologia-xehetasunak barne: nola egin ataza jakin bat ISPak ezarritakoa betez?

12.2. Gainera, sistemaren segurtasun-agiriek bestelako dokumentu batzuk izan ahalko dituzte, ez lotesleak, hala nola gomendioak, praktika onak, txostenak, erregistroak, ebidentzia elektronikoak, eta abar.

12.3. Segurtasun-agiriak eguneratuta eta antolatuta mantendu behar dira.

13. Datu pertsonalen babesa.

Tratamenduaren xedeko datu pertsonalak dagokien segurtasun-neurrien bitartez babestuko dira, kasu bakoitzean aplikatu beharreko datu-babeserako araubidearen arabera.

14. Hirugarren alderdiak.

14.1. Segurtasun Sailak beste erakunde batzuen zerbitzuak erabili edo informazioa maneiatzen duenean, informazioaren segurtasun-politika honen berri emango zaie, bideak ezarriko dira informazioaren segurtasunaz arduratzen diren organoen informazio eta koordinaziorako, eta jarduketa-prozedurak zehaztuko dira segurtasun-intzidenteei aurre egiteko.

14.2. Segurtasun Sailak hirugarrenei zerbitzuak eman edo informazioa lagaz gero, politika honen berri emango zaie, bai eta zerbitzu eta informazio horiei eragiten dien segurtasun-arautegiarena ere. Hirugarren horiek ere lotetsiko

dituzte araudi horretan ezarritako betebeharrek, eta hirugarren horiek bere prozedura propioak garatu ahalko dituzte arau horiek betetzeko. Gorabeherak edo intzidentziak jakinarazteko eta ebazteko prozedura espezifikoak ezarriko dira, eta hirugarrenen langileak segurtasunari dagokionez behar bezala kontzientziatuta daudela bermatuko da.

14.3. Hirugarren alderdiren batek ezin badu bete ISPren alorren bat aurreko paragrafoetan ezarri denaren arabera, segurtasun-arduradunak txosten bat egin beharko du, arriskuak eta horiek tratatzeko modua zehaztuta. Txosten horrek onespena beharko du eraginpeko informazio-arduradunen eta zerbitzu-arduradunen aldetik.

15. Prestakuntza.

15.1. Informazioarekin eta informazio-zerbitzu eta -sistemekin zerikusia duten langile guztiek prestakuntza eta informazioa jaso beharko dute informazioaren segurtasunaren alorrean dituzten betebehar eta eginbeharrei buruz.

15.2. Segurtasun Saileko sistema eta zerbitzuei aplikatu beharreko informazio-teknologien segurtasuna bermatzeari dagokionez, beharrezko diren mekanismoak ezarriko dira premiazko eta ezinbesteko kontzientziazioa eta prestakuntza espezifikoa gauzatzeko antolamendu-maila guztietan.

16. Erantzukizun-akzioak.

16.1. Langile publikoek betetzen ez badituzte agiri honetan eraginpeko langileentzako ezarritako segurtasun-betebeharrak eta -neurriak, zehapena ezarriko zaio ez-betetzeari, bat etorrita administrazio publikoen zerbitzuan ari diren funtzionarioei eta langile lan-kontratudunei aplikatu beharreko zehapen-araubidearekin.

16.2. Zerbitzu-hornitzaileen edo kontratatutako kanpoko langileen ez-betetzerik izanez gero, Sektore Publikoko Kontratuei buruzko azaroaren 8ko 9/2017 Legearen arabera jokatuko da, hargatik eragotzi gabe kontratazio-agirietan adierazitako akzioak edo egitatearen izaera eta larritasuna kontuan hartuz egoki daitekeen beste edozein akzio.