cyber zaintza

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

Oinarrizko gida

Euskal sektore publikoko entitateentzat, zibersegurtasun-gorabeheren kudeaketari buruz

2024-2029

EUSKO JAURLARITZA
GOBIERNO VASCO

Aurkibidea

1.1 Datuak Babesteko Euskal Agintaritza

Datuak Babesteko Euskal Agintaritza (DBEA) kontrol-agintaritza independentea da, nortasun juridiko propioarekin eta erabateko gaitasun publiko eta pribatuarekin sortua. Administrazio publikoekiko inongo loturarik gabe betetzen ditu bere eginkizunak, eta euskal sektore publikoa osatzen duten administrazio eta instituzioek euren eginkizunak egikaritzean datu pertsonalen tratamendu egokia egin dezatela zaintzen du.

Gainera, tratamendua egiten denean administrazio publikoen edo edozein eratako zuzeneko zein zeharkako kudeaketaren bidez zerbitzuak ematen dituzten zuzenbide pribatuko entitateen eskumeneko gaietako eginkizun publikoak egikaritzeko, pertsona fisikoek edo juridikoek datu pertsonalak nola erabiltzen dituzten kontrolatzen eta gainbegiratzen du.

DBEAk datu pertsonalen babesarekin zerikusia duten kontsultei erantzuten die, eta zabalkunde- eta prestakuntza-jardueretan parte hartzen du arlo hori eraentzen duen araudian onartutako eskubideak ezagutzera emateko eta pribatutasunaren balioari buruzko kontzientzia publikoa areagotzeko.

DBEAk, halaber, pertsonen eskubideak babesten ditu, datu pertsonalen babeserako araudian eskubide horiek onartzen baitira.

Herritarren eskubide eta askatasunen benetako babesa bermatzeko, DBEAk, kontrol-agintaritza den aldetik dauzkan eginkizunak betetze aldera, euskal sektore publikoko entitateen eskura jartzen du datu pertsonalen arrakalak jakinarazteko prozedura elektronikoa.

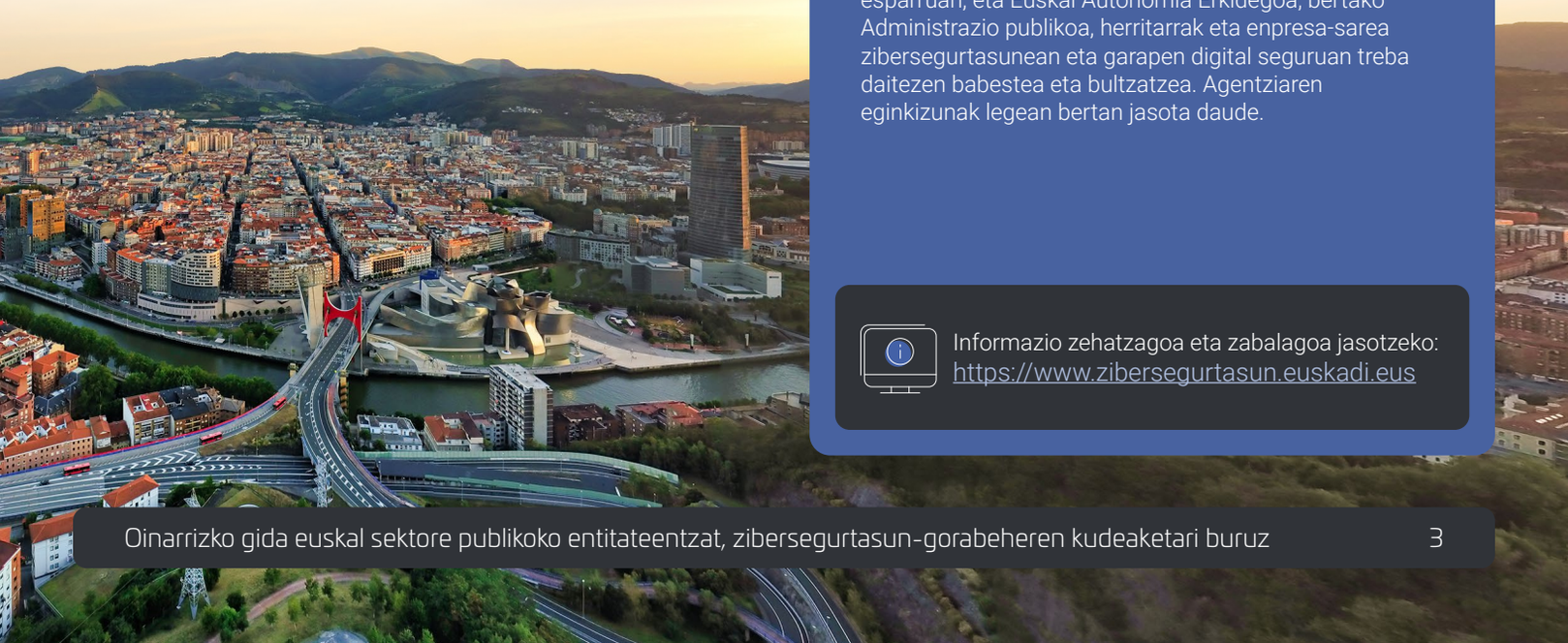
Informazio zehatzagoa eta zabalagoa jasotzeko:
https://www.avpd.eus

1.2 Cyberzaintza

Cyberzaintza, Zibersegurtasunaren Euskal Agentzia, nortasun juridiko propioa duen erakunde publikoa da, Euskadin Internet eta teknologia berriak erabiltzeak eragindako mehatxuei modu integral eta zeharkakoan aurre egiteko sortua. Euskal Zibersegurtasun Agentzia sortzeari buruzko ekainaren 29ko 7/2023 Legearen bidez sortu zen.

Agentziaren xedea da zibersegurtasuna sustatzea eta koordinatzea Euskal Sektore Publikoaren maiatzaren 12ko 3/2022 Legeak mugatutako euskal sektore publikoan, sektore horren eskumeneko informazio-sistemen segurtasunaren eta sare elektronikoen segurtasunaren esparruan; eta Euskal Autonomia Erkidegoa, bertako Administrazio publikoa, herritarrak eta enpresa-sarea zibersegurtasunean eta garapen digital seguruan treba daitezen babestea eta bultzatzea. Agentziaren eginkizunak legean bertan jasota daude.

Informazio zehatzagoa eta zabalagoa jasotzeko:
https://www.zibersegurtasun.euskadi.eus



2. Glosarioa

Datu pertsonalak
Pertsona fisiko identifikatu edo identifikagarri («interesdun») bati buruzko informazio guztia; pertsona fisiko identifikagarria da zuzenean edo zeharka, eta batez ere identifikatzaile baten bitartez, identifika daitekeen pertsona oro; identifikatzaile hori izen bat izan daiteke, identifikazio-zenbaki bat, kokapen-datuak, online identifikatzaile bat edo pertsona horren nortasun fisikoari, fisiologikoari, genetikoari, psikikoari, ekonomikoari, kulturalari edo sozialari buruzko elementu bat edo gehiago.

Datu pertsonalen segurtasun-arrakala
Segurtasunaren urraketa oro (aurrerantzean, arrakala), zeinak eragin baitezake transmititutako, kontserbatutako edo beste moduren batez tratatutako datu pertsonalak ustekabean edo legez kontra suntsitzea, galtzea edo aldatzea, edo datuok baimenik gabe lagatzea edo irispidean jartzea.

Datuak babesteko ordezkaria (DBO)
Datu pertsonalen segurtasun-arrakalen arloan dauzkan eginbeharren eta erantzukizunen berri ematen dio tratamenduaren arduradunari eta/edo eragileari. DBEArekin elkarlanean aritzen da segurtasun-arrakalak kudeatzen.

Gorabehera
Enpresaren informazio-aktiboen konfidentzialtasuna, osotasuna edo eskuragarritasuna ukitzen duen edozein gertaera, adibidez: sistemetara sartzea edo sartzen saiatzea, informazioa baimenik gabe erabiltzea, zabaltzea, aldatzea edo suntsitzea.

Gorabeherei erantzuteko plana
Jarraibide-multzo bat da, zeinak antolakunde bati laguntzen baitio jasan ditzakeen zibersegurtasun-gorabeherak detektatzen, gorabehera horiei erantzuten eta haiek gainditzen.

Intzidentzia
Gerta litekeen arazo bat, antolakundearen ingurunean informazioaren teknologietako zerbitzuetan eragin negatiboa sor dezakeena.

Kalteberatasuna
Mehatxu batek balia dezakeen ahultasun oro, edo, zehatzago esatearren, aktiboen ahultasunak edo aktiboen babes-neurrien ahultasunak, zeinek erraztasuna ematen baitute balizko mehatxu batek arrakasta izan dezan.

Mehatxua
Sistema bati edo antolakunde bati kaltea eragin diezaiokeen nahi gabeko gorabehera bat sorraraz dezakeen kausa bat.

Tratamendua
Datu pertsonalen gainean edo datu pertsonalen multzoen gainean egiten den edozein eragiketa eta eragiketa-multzo, prozedura automatizatuak erabilita zein erabili gabe, hala nola: datu-bilketa, erregistratzea, antolatzea, egituratzea, kontserbatzea, egokitzea edo aldatzea, ateratzea, kontsultatzea, erabiltzea, transmisioz lagatzea, hedatzea edo irispidean jartzeko beste edozein forma, datuak alderatzea edo interkonektatzea, mugatzea, ezabatzea edo suntsitzea.

Tratamenduaren arduraduna
Bakarrik edo beste batzuekin batera, fitxategiaren helburuak eta bitartekoak erabakitzen dituen pertsona fisiko edo juridikoa, agintaritza publikoa, zerbitzua edo bestelako erakundea; Batasuneko edo estatu kideetako zuzenbideak erabakitzen baditu tratamenduaren helburuak eta bitartekoak, Batasuneko edo estatu kideetako zuzenbide horrek berak ezarri ahalko du nor izango den tratamenduaren arduraduna edo zein izango diren hura izendatzeko irizpide espezifikoak.

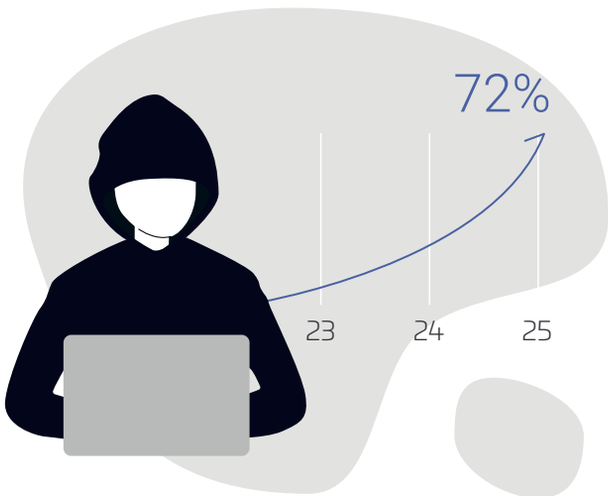
Tratamendu-eragilea
Tratamenduaren arduradunaren izenean, datu pertsonalak tratatzen dituen pertsona fisiko edo juridikoa, agintaritza publikoa, zerbitzua edo beste edozein erakunde.

Tratamendu-jardueren erregistroa
Tratamenduen zerrenda, entitateak baliabide elektronikoen bidez irisgarri egoteko moduan argitaratu behar duena. Tratamendu-jarduerak zehaztu behar dira haien helburuen arabera.

Zibererasoa
Eraso-maniobra bat, edozein motatakoa, norbanako zein antolakundeek egina, informazio-sistemei erasotzeko helburuz, halako sistemak direla azpiegiturak, sare konputazionalak edo urruneko zerbitzarietan gordetako datu-baseak. Hori egiteko, ekintza maltzurrak erabiltzen dira, normalean iturri anonimoetan sortuak, sistema kaltebera bat hackeatuz jomuga espezifiko bat lapurtzeko, hondatzeko edo suntsitzeko.

3. Testuingurua

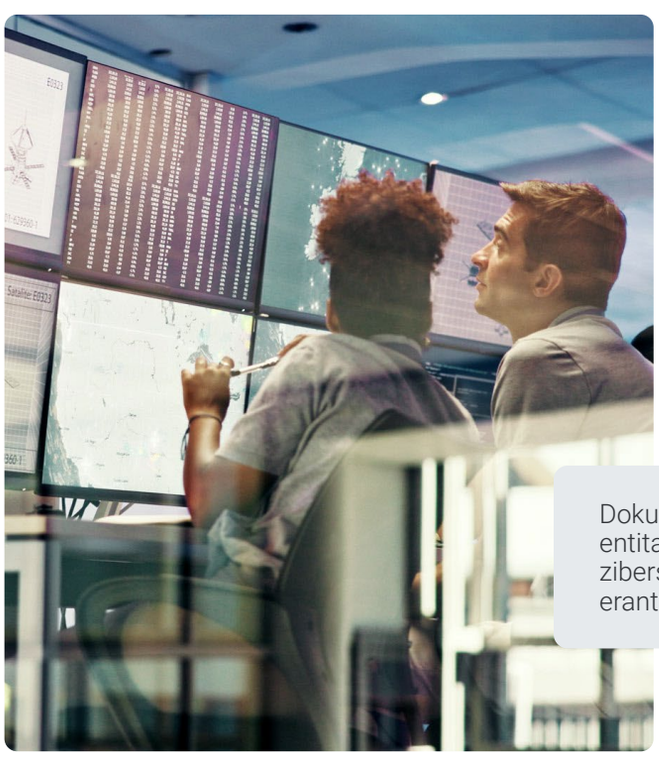
Azken urteotan, nabarmen areagotu dira Euskadin jasandako zibererasoak eta zibersegurtasun-gorabeherak. «Euskal Poliziaren Delinkuentzia Memoria» delakoaren datuen arabera, azken 3 urteotan % 72 egin du gora delitu informatikoekin zerikusia duten salaketen kopuruak. DBEAri jakinarazitako segurtasun-arrakalen kopuruak ere gora egin du, aurreko urteekin alderatuta.



Instituzio publikoek, entitate pribatuek eta herritarrek ikusi dutenez, handitu egin da gorabehera bat jasateko arriskua, eta askotarikoak dira faktoreak, hala nola ziberkriminalak profesionalizatzea, eraginpean dagoen azalera kontrolik gabe handitzea, teknologia berriak ezartzea –adibidez, adimen artifiziala– segurtasunaren eta pribatutasunaren ikuspegia kontuan hartu gabe, konfigurazioetan huts egitea edo sistemak lehenespenez seguruak izateko konfiguratuta daudela onartzea, kalteberatasunak, kontzientziazio falta eta, horren ondorioz, babes-neurririk eza; espezializaziorik eza, eta delitua jazartzeko laguntzarik eza.

Euskal administrazio publikoaren kasuan, zibersegurtasunaren arriskurik behinenei buruz xehetasun gehiago izateko eta arrisku horiei aurre egiten ikasteko, gauzatuz gero arriskuok murriztea eta arintzea helburu dela, «Euskal Administrazio Publikoaren zibersegurtasun-arrisku nagusiak» izenburuko txostena irakurtzea gomendatzen da.

Puntu honetara helduta, albiste batzuk normal bihurtu dira. Adibidez, gure datu pertsonalak arriskuan eta agerian egon direla Interneteko zerbitzu-hornitzaile batek, sare sozial batek, enpresa teknologiko batek eta abarrek zibersegurtasun-gorabehera bat jasan duelako. Edo iruzurrei buruzko albisteak; izan ere, horren ondorioz, galera ekonomikoak egon daitezke, eta horrek ondorio zuzenak izan ditzake entitateen iraupenean edo euren ospean.

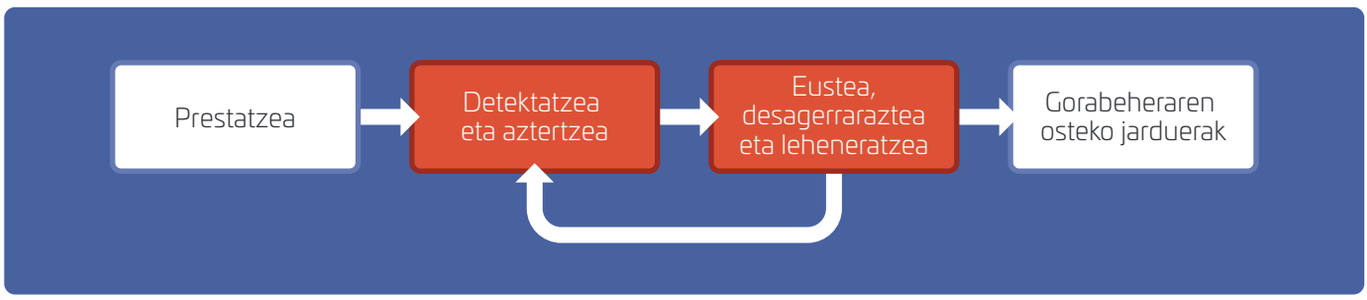


Nabarmentzekoa da gauza bat: Datuak Babesteko Erregelamendu Orokorraren (DBEO) 33. artikuluaren arabera, tratamenduaren arduradunak jakiten duenean segurtasun-arrakala batekin zerikusia duen zibergorabehera bat gertatu dela (informazio gehiago «Segurtasun-arrakalak jakinaraztea» izenburuko gidan) eta horrek datu pertsonalei eragin ahal diela, DBEAri jakinarazi behar dio. Atzerapenik gabe jakinarazi behar da, beranduenez hurrengo 72 orduen barruan, asteburuetan eta jaiegunetan igarotako orduak ere zenbatu behar direla. Halaber, Segurtasunaren Eskema Nazionalak ezartzen duenez, maila handia, oso handia edo kritikoa duten gorabeherak jakinaraztea nahitaezkoa da.

Dokumentu honen helburua da euskal sektore publikoko entitateei oinarrizko laguntza ematea, presta daitezen, eta, zibersegurtasun-gorabeherak gertatuz gero, horiei behar bezala erantzun diezaieten.

4. Gorabeherei eman beharreko erantzunaren bizi-zikloa

Zibersegurtasun-gorabeherei eman beharreko erantzunaren bizi-zikloak zenbait fase dauzka. Fase horietako bakoitzak berebiziko garrantzia du, behar bezalako erantzuna emateko eta izan litekeen eragina murrizteko. Jarraian, fase horietako bakoitza zehaztuko da.

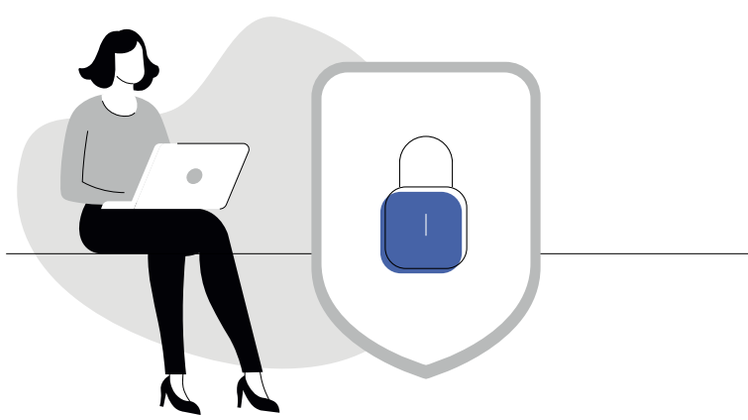


4.1 Prestatzea

Zibersegurtasun-gorabehera bati eman beharreko erantzunaren bizi-zikloaren lehenengo fasea da prestatzea. Etapa horretan, antolakundeek gorabeherak kudeatzeko gaitasunak garatzen eta hobetzen dituzte. Horretarako, datu pertsonalak babesteko araudira moldatzen dira; bestalde, politikak eta prozedurak sortzen dituzte eta babes-tresna egokiak hedatzen eta konfiguratzen dituzte.

Alde horretatik, ataza hauek egiten dituzte:

- Arriskuak behar bezala ebaluatu eta kudeatzea; horretarako, antolakundearentzat kritikoak diren aktiboak/sistemak identifikatzea eta horiei lehentasuna ematea.
- Ohikoak diren gorabeheren tipologiak identifikatzea. Horretarako, I. eranskinean eskuragarri dago CCN-STIC 817 gida. Bertan ezartzen da taxonomia estandarizatu bat, zeinean jasotzen baitira kategoria nagusiak eta kategoria horietarako gorabeheren mota batzuk.
- Gorabeheren tipologiaz harago, komenigarria da irizpide batzuk ezartzea, horietatik abiatua gorabeheraren eragin-atalasea ezartzeko: Kritikoa, Oso Handia, Handia, Ertaina eta Txikia. Irizpideak hauek izan daitezke: eragindako eremua, eragindako sistemen ehunekoa, gorabeherak sorrarazi duen jarduerarik gabeko denbora, kalteen tipologia: ekonomikoak, ospeari dagozkionak eta abar, eta, bereziki, zibergorabeherak kaltetutako pertsonen eskubide eta askatasunek jasandako kaltea.
- Gorabeheren aurrean zereginak eta ardurak esleitzea, eta, halaber, harremanetarako datu guztiak biltzea eta komunikazio-kanalak ezartzea.
- Kontaktu-puntu gehigarriak identifikatzea: hornitzaileak, interes-taldeak eta abar.
- Antolakundearentzako zibersegurtasunaren arloko arau-betekizunak identifikatzea eta betetzea.
- Alertarako eta gorabeherei erantzuteko politikak eta prozedurak garatu eta dokumentatzea, hala nola negozioaren jarraipenerako planak edo hondamendien aurkako leheneratze-planak, aldizkako berrikuspenerako epeak ezarriz.
- Prozeduren informazioa inprimatzea.
- Mehatxuen aurrean babeserako eta monitorizaziorako tresnak eta teknologiak inplementatu eta erabiltzea.
- Langileei gaitasunak ematea zibersegurtasunerako eta gorabeheren aurkako erantzunerako jardunbiderik onenen inguruan, eta datu pertsonalen babesaren esparruari garrantzia ematea.
- Simulakroak eta ariketak egitea, taldearen prestaketa ebaluatzeko.



DBEO betetzeari dagokionez, ataza hauek aurreikusten dira:

- Entitatearen tratamendu-jardueren erregistroa argitaratzea, datuen babeserako araudiak eskatzen duen gutxieneko edukiarekin.
- Pertsona bat antolakundearen DBO izendatzea, DBEOk ezartzen dituen betekizunen arabera.
- DBOren harremanetarako datuak entitatearen webgunean argitaratu, ikusteko moduko leku batean, eta datu horiek DBEAri komunikatu, Agintaritzaren webgunean eskura dagoen prozeduraren bitartez.
- Tratamenduen eraginaren ebaluazioak egitea, beharrezkoa izanez gero.

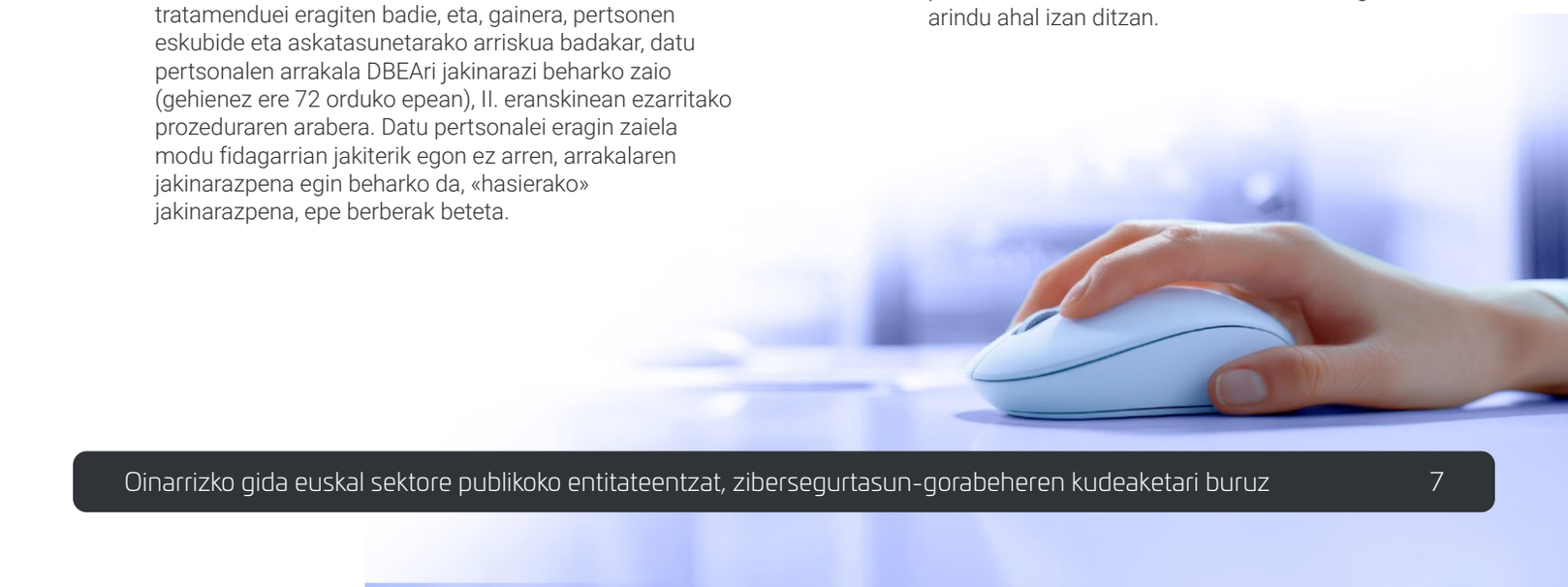
Segurtasunaren Eskema Nazionala betetzeari dagokionez, gorabeherei erantzuteko prestatzearekin zerikusia duten honako ataza hauek aurreikusten dira:

- Segurtasunaren kudeaketan zeregin eta ardura espezifikoak definitzea: segurtasuneko arduraduna, sistemaren arduraduna, informazioaren arduraduna eta abar.
- Gorabeherak kudeatzeko prozedura formal eguneratu bat edukitzea, CCN-STIC 817 gidaren ildotik.
- Planaren efikazia aldiro ebaluatzea, simulakroetatik eta gorabehera errealen egoeretatik abiatuta, halakorik gertatzen denean.
- Gertaerak detektatzeko, erregistratzeko eta aztertzeko mekanismoak eskura izatea.

4.2 Detektatzea eta aztertzea

Detektatzea eta aztertzea da hurrengo fasea. Fase honetan, zibersegurtasun-gorabeherak identifikatzen eta ulertzen dira. Horrekin lotuta, normalean, sistemak eta sareak monitorizatu behar izaten dira jarduera susmagarriak detektatzeko, software berezia erabili behar da mehatxuak detektatzeko, eta gertaera-korrelazioa ezarri, gorabeheraren izaera eta norainokoa zehazteko. Bildutako informazioa xehetasunez aztertzea, gorabeherak antolakundean izan dezakeen eragina ebaluatzeko. Azkar identifikatu eta aztertzea funtsezkoa da gorabeherari eusteko eta eragina arintzeko.

- Mehatxuak detektatzeko tresnak erabiltzea, gerta litezkeen gorabeherak identifikatzeko.
- Sistemak eta sareak etengabe monitorizatzea, ohikoak ez diren jarduerak detektatzeko.
- Logak biltzea, sistemetan gertatzen denaren trazabilitatea edukitzeko.
- Segurtasun-gertaerak korrelazioan jartzea, gorabeheraren jatorria eta izaera zehazteko.
- Gorabehera bat identifikatuz gero, funtsezkoa da arin jokatzea eta gorabehera hori kudeatzeko gaitasuna duten pertsonei/entitateei berehala jakinaraztea.
- Azterketa sakona egitea, gorabeheraren norainokoa eta eragina ulertzeko.
- Aztertzea ea gorabeherak datu pertsonalen tratamendu bat ukitzen duen: gorabeherak datu pertsonalen tratamenduei eragiten badie, eta, gainera, pertsonen eskubide eta askatasunetarako arriskua badakar, datu pertsonalen arrakala DBEAri jakinarazi beharko zaio (gehienez ere 72 orduko epean), II. eranskinean ezarritako prozeduraren arabera. Datu pertsonalei eragin zaiela modu fidagarrian jakiterik egon ez arren, arrakalaren jakinarazpena egin beharko da, «hasierako» jakinarazpena, epe berberak beteta.
- Tratamenduaren arduradunek arrakalaren idatzoharra jaso behar dute entitatearen gorabeheren erregistroan, eta DBEAri jakinaraztearen gainean zein kaltetutako pertsonei komunikatzearen gainean hartutako erabakiei buruzko informazioa ere jaso behar dute.
- Arrakalak pertsona fisikoen eskubide eta askatasunetarako arrisku handia ekar dezakeenean, pertsona fisiko horiei jakinarazi beharko zaie, honako alderdi hauek beteta:
  - Epea: DBEOren arabera, kaltetutakoei jakinarazi behar zaie bidegabeko atzerapenik gabe, beharrezkoak diren neurriak hartu ahal izan ditzaten.
  - Hizkera argia eta erraza erabiliz, datu pertsonalen segurtasun-arrakalaren izaera deskribatu behar da, eta gomendioak azaldu behar dira, kaltetutako pertsona fisikoak arrakalaren ondorio kaltegarriak arindu ahal izan ditzan.



4.3 Eustea, desagerraraztea eta leheneratzea

Fase honetan, elkarren arteko harremana duten hiru azpifase daude:

Eustea

Eustearen helburu nagusia da gorabeheraren norainokoa mugatzea eta heda dadila eragoztea. Epe laburreko euste-estrategiak daude, hala nola arriskuan dauden sistemak isolatzea, eta epe luzekoak ere bai: adibidez, segurtasuneko eguneraketak inplementatzea. Alde horretatik, ataza hauek egin behar dira:

- Gorabeheraren norainokoa zehaztea, entitatearentzat berarentzat ez ezik herritarrentzat, bezeroentzat, hornitzaileentzat eta abarrentzat ere bai, bereziki datu pertsonalak eraginpean egon badira.
- Euste-neurriak inplementatzea, gorabehera kontrolatzeko. Horren haritik, baliteke hau egin behar izatea:
  - Babes perimetraleko neurriak sendotzea: suebakietan arauak aplikatzea, IP helbide edo domeinu jakin batzuetarako sarbidea blokeatzeko.
  - Sareari segmentazio gehigarria aplikatzea.
  - Beharrezkoa izanez gero, kaltetutako sistemak osorik isolatzea.
  - Kaltetutako erabiltzaileen pribilegioen maila aldatzea.
  - Erabiltzaile-kontuak blokeatzea edo pasahitzak txandakatzea.

Desagerraraztea

Mehatxuari eutsi ostean, desagerraraztearen ardatza da gorabehera sorrarazi duen kode maltzurra osorik ezabatzea, tipologia horretakoak diren kasuetan. Alde horretatik, ataza hauek egin behar dira:

- Sistemak babesteko mekanismoak inplementatzea; adibidez, EDR.
- Malwarea eta beste tresna maltzur batzuk –esate baterako scriptak– ezabatzea.
- Gorabeherarekin zerikusia duten ataza automatizatuak, erregistroko sarrerak eta abar ezabatzea.
- Segurtasuneko eguneraketak aplikatzea.

Leheneratzea

Leheneratze-fasearen helburua da sistemen funtzio normalak oneratzea eta baliozkotzea. Alde horretatik, ataza hauek egin behar dira:

- Leheneratzeko estrategia bat diseinatzea, lehentasunak ezarrita.
- Kaltetutako sistema eta zerbitzuak egoera normalera bueltatzea.
- Neurri zuzentzaile guztiak behar bezala inplementatu direla egiaztatzea, eta leheneratutako sistemen osotasuna baliozkotzea.
- Leheneratutako sistemak monitorizatzea, berriro gorabeherarik gertatuko ez dela ziurtatzeko.

DBEAri datu pertsonalen segurtasun-arrakalak JAKINARAZTEAN, zera egin behar da:

- Segurtasun-arrakalari buruzko informazio esanguratsu guztia eskura dagoenean, DBEAri jakinarazpen «osoa» egingo zaio; informazio hori eskura ez badago, «hasierako» jakinarazpena egin beharko da (horrek esan nahi du geroago jakinarazpen «osagarria» egin beharko dela). Prozesu horri buruz argibiderik behar izanez gero, DBEArekin harremanetan jartzea dago. Horretarako, posta elektroniko bat idatzi behar da teknologia.ebaluazioa@avpd.eus helbidera, edo 945 016 230 zenbakira deitu.
- Jakinarazpen osagarria egin behar da hasierako jakinarazpenetik hilabete bat igaro baino lehen.
- Tratamenduaren arduradunak azaldu beharko du zer erabaki hartu duen, datu pertsonalen arrakala kaltetutako pertsonei komunikatzearen gainean.

4.4 Gorabeheraren osteko jarduerak

Zibersegurtasun-gorabehera bati eman beharreko erantzunaren bizi-zikloaren azken fasea da gorabeheraren osteko jarduerena. Etapa horretan, gorabehera zehatz-mehatz aztertzen da, zer ikasi den eta hobetzeko zein aukera dagoen identifikatzeko. Alde horretatik, ataza hauek egin behar dira:

- Xehetasunez aztertzea bai gorabehera bai hari eman zaion erantzuna.
- Ikasitakoak eta hobetzeko aukerak identifikatzea.
- Ikasitakoan oinarrituta, politikak eta prozedurak eguneratzea.
- Babes-maila handitzen lagundu ahal duten teknologia eta tresnak inplementatzea: MFA, segmentazioa eta abar.
- Txosten zehatzak prestatzea goi-zuzendaritzarentzat, CSIRT-entzat, kontrol-agintaritzentzat, interesa duten entitateentzat eta abarrentzat.
- Kanpoko alderdiei gorabeheraren eta hartutako neurrien berri ematea.
- DBEAk datu pertsonalen arrakala ixteari buruz bidali duen txostena jasotzea, eta emandako gomendioei jaramon egitea.

Ikasitakoa ekintza-plan bihurtzea funtsezkoa da. Plan horretan, hobetzeko ekintzak identifikatuko dira, mugarriak ezarriko dira eta mugarri horien lorpenaren jarraipena egingo da.

4.5 Gorabehera kudeatu bitartean egin beharreko ataza arruntak

- Ebidentzia digitalak bildu eta gordetzea, eta zaintza-katea gordetzea, gorabehera judizializatzea beharrezkoa balitz ere.
- Aurkikuntza guztiak eta egindako ekintza guztiak dokumentatzea, eginbideak justifikatzeko (eginbiderik egin behar izatekotan), eta gorabehera behar bezala kudeatzeko.
- Jakinarazteko eginbeharra betetzea, eta, horretarako, jakinaraztea dagokion CSIRT-ari eta kontrol-agintaritzei, antolakundea zein araudiren mendean dagoen eta horretan ezartzen den agintaritzari, alegia.
- Ertzain-etxe batean salaketa jartzea.
- Cyberzaintzari jakinaraztea, sektore publikoko gainerako entitateak babesteko neurriak hartu ahal izan ditzaten (900 104 891 – incidencias@cyberzaintza.eus). Autobabeserako Euskal Araua aplikatu behar den kasuetan, hori egitea nahitaezkoa izango da.
- Datu pertsonalen segurtasun-arrakala kudeatzeak, DBEO betetzeak eta DBEAren errekerimenduei jaramon egiteak ez du esan nahi zehapen bat ezarri behar denik; aitzitik, jakinarazteak, eta, hala badagokio, eraginpean dauden pertsonei garaiz eta behar den moduan komunikatzeak, agerian jartzen du antolakundeak arduraz jokatzen duela, DBEOn jasotako erantzukizun proaktiboaren eginbeharra modu efikazean bete baitu. Aldiz, jakinarazteko eta interesdunei komunikatzeko eginbeharrak ez betetzea arau-hauste gisa tipifikatuta dago.

5. Maiz gertatzen diren hutsegiteak

Jarraian, zibersegurtasun-gorabeherak aztertu ondoren ikusi diren hutsegiterik ohikoenak azalduko ditugu:

- Zibersegurtasun-gorabeherak guri edo gure antolakundeari ez baizik eta beste batzuei gertatzen zaizkiela pentsatzea. Horren ondorioz gertatzen dena da plangintza falta eta prestaketa falta.
- Dokumentazioa inprimatuta ez edukitzea. Hori bereziki kritikoa da ransomware kasuetan, halakoetan sistemetako informazioa zifratzen baita, informazioa irispidean izatea eragozteko.
- Zibersegurtasun-gorabeherak kudeatzea soilik informatika-atalaren ardura dela uste izatea. Gorabeheretan beste atal batzuk ere daude tartean, hala nola zuzendaritza nagusia, lege-atala, araudia betetzeaz arduratzen den atala, komunikazio-atala, kontrol ekonomikoko atala, giza baliabideen atala, eta, orokorrean, antolakundeko langile guztiak.
- Gorabehera bat jasanez gero araudiaren eta legearen esparruan dauden eginbeharren berri ez izatea.
- Gorabehera kudeatzen parte hartzen duten pertsonen arteko komunikazioa eskasa izatea.
- Gertatutakoaren azalpen sinplistak onartzea edo gertatutakoaren arrazoia identifikatzen ez saiatzea. Horren ondorioz, askotan, sistemak lehengoratzen dira gorabeheraren arrazoia zehaztu gabe, eta, horregatik, baliteke berriro ere gertatzea.
- Logik ez edukitzeak ezinezko bihurtzen du gorabeheraren arrazoiak aztertzea, eta gorabehera kudeatzea eragozten du.
- Dokumentaziorik ez egoteak nabarmen eragozten du araudia betetzea eta ikastea.
- Jada gertatu zaigunez gero, berriro gertatuko ez zaigula pentsatzea.
- Ikasitakoari jaramonik ez egitea. Horren ondorioz, askotan, zera gertatzen da: berriro gerta dadila eragozteko neurriak inplementatzeko inbertsio nahikorik ez egitea, etengabeko prestakuntzan eta entrenamenduan eta abarretan inbertsio nahikorik ez egitea.
- Kontuan ez hartzea segurtasun-gorabeherak datu pertsonalen tratamenduei eragin ahal diela eta, beraz, segurtasun-arrakala DBEAri jakinarazi behar zaiola. Datu pertsonalen segurtasun-arrakalak ez jakinaraztea DBEOren 33. artikuluaren urraketa da, eta DPBEDBLOren 73.r artikuluaren arabera arau-hauste ASTUNA da. Halaber, arduradunak modu fidagarrian jakin ez arren datu pertsonalak ukitu diren ala ez, arrakalaren jakinarazpena egin beharko da, «hasierako» jakinarazpena.
- Kaltetutako pertsonei segurtasun-arrakala ez komunikatzea, kontrol-agintaritzak hala eskatu duenean, arau-hauste ASTUNA da DPBEDBLOren 73.s artikuluaren arabera.
- Datuak babesteko ordezkaria izendatzeko betebeharra ez konplitzea, hori nahitaezkoa denean, arau-hauste ASTUNA da, DPBEDBLOren 73.v artikuluaren arabera.

6. Arau-aipamenak

- 2024ko ekainaren 7ko Agindua, Jaurlaritzako lehenengo lehendakariorde eta Segurtasuneko sailburuarena, zeinaren bidez arautzen baita zibersegurtasun-arloko jarraitutasun-planak egitea autobabeserako euskal arauaren mende dauden zenbait jardueratarako.
- 443/2024 Errege Dekretua, apirilaren 30ekoa, zeinaren bidez onartzen baita 5G sare eta zerbitzuen Espainiako Segurtasun Eskema.
- 16/2023 Legea, abenduaren 21ekoa, Datuak Babesteko Euskal Agintaritzarena.
- 7/2023 Legea, ekainaren 29koa, Euskal Zibersegurtasun Agentzia sortzekoa.
- 2022/2555 (EB) Zuzentaraua, Europako Parlamentuaren eta Kontseiluarena, 2022ko abenduaren 14koa, Europar Batasun osoan zibersegurtasun-maila bateratua bermatzeko neurriei buruzkoa.
- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasunaren Eskema Nazionala arautzen duena.
- 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa eta Eskubide Digitalak Bermatzekoa.
- 2016/679 Erregelamendua (EB), Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa; eta 95/46/CE Zuzentaraua indargabetzen duena.
- Hutsen zuzenketa: 2016/679 Erregelamendua (EB), 2016ko apirilaren 27koa, Europako Parlamentuarena eta Kontseiluarena, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa; eta 95/46/CE Zuzentaraua indargabetzen duena (2018ko maiatzaren 18a)
- Hutsen zuzenketa: 2016/679 Erregelamendua (EB), 2016ko apirilaren 27koa, Europako Parlamentuarena eta Kontseiluarena, datu pertsonalen tratamenduari eta datu horien zirkulazio askeari dagokienez pertsona fisikoak babesteari buruzkoa; eta 95/46/CE Zuzentaraua indargabetzen duena (2021eko martxoaren 4a)

I. ERANSKINA: Zibergorabeheren taxonomia

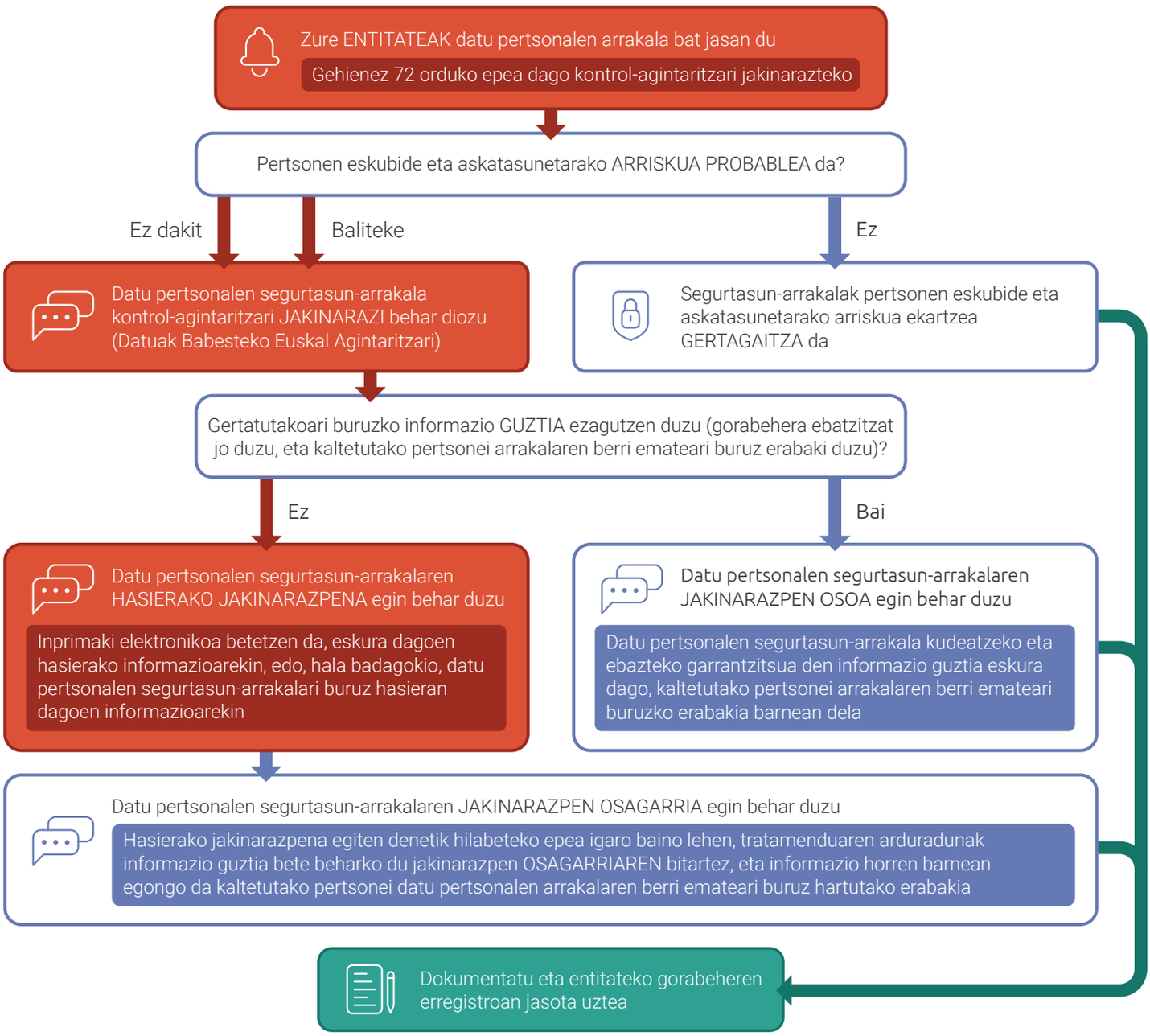
Zibergorabeheren sailkapena/taxonomia		
Sailkapena	Gorabehera-mota	Deskribapena eta adibide praktikoak
Abusuzko edukia	Spama	Eskatu gabe masiboki bidalitako posta elektronikoa. Edukiaren hartzaileak ez du baliozko baimenik eman mezu kolektibo bat jasotzeko.
	Gorroto-delitua	Eduki iraingarria edo diskriminatzailea. Adib.: ziberjazarpena, arrazakeria, pertsonen edo taldeen aurkako mehatxuak.
	Haurren pornografia, eduki sexual edo indarkeriazko eduki desegokia	Haurren pornografiarekin, indarkeriaren apologiarekin eta abarrekin zerikusia duen edukia modu bisualean irudikatzen duen materiala.
Eduki kaltegarria	Infektatutako sistema	Malwarearekin infektatutako sistema. Adib.: Rootkit batekin infektatutako sistema, ordenagailu edo telefono mugikor bat.
	C&C (Agintea eta Kontrola) zerbitzaria	Malwarearen bidez edo infektatutako sistemen bidez Aginte eta Kontroleko (C&C) zerbitzari batekin egindako konexioa.
	Malwarea banatzea	Malwarea banatzeko erabilitako baliabidea. Adib.: antolakunde baten baliabide bat, malwarea banatzeko erabiltzen dena.
	Malwarea konfiguratzea	Malwarea konfiguratzeko fitxategiak gordetzen dituen baliabidea Adib.: troiarrerako webinject erasoa.
Informazioa eskuratzea	Sareak eskaneatzea (scanning)	Sistema bati eskariak bidaltzea, egon daitezkeen ahultasunak aurkitzeko. Barnean dira, halaber, egiaztapen- eta testeatze-prozesuak, ostatatzeen, zerbitzuen eta kontuen informazioa biltzeko. Adib.: DNS, ICMP, SMTP eskariak, atakak eskaneatzea.
	Paketeak aztertzea (sniffing)	Sareetako trafikoa behatzea eta grabatzea.
	Gizarte-ingeniaritza	Informazio pertsonala biltzea, teknologia erabili gabe. Adib.: gezurrak, trikimailuak, eroskeriak, mehatxuak.
Bidegabe sartzen saiatzea	Kalteberatasun ezagunak ustiatzea	Identifikatzaile estandarizatu batekin kalteberatasunak ustiatuz sistema bat arriskuan jartzen edo zerbitzu bat eteten saiatzea (ikus CVE). Adib.: buferra gainezkatzea, atzeko ateak, cross site scripting (XSS).
	Egiaztagiriak hautsiz sartzen saiatzea	Egiaztagiriak hausteko askotariko saiakerak. Adib: pasahitzak apurtzeko saiakerak, indarrezko erasoa.
	Eraso ezezaguna	Exploit ezezagun bat erabiliz egindako erasoa.
Bidegabe sartzea	Pribilegioak dauzkan kontu bat arriskuan	Erasotzaileak pribilegioak dauzkan sistema bat arriskuan jartzea.
	Pribilegiorik ez daukan kontu bat arriskuan	Sistema bat arriskuan jartzea, pribilegiorik gabeko kontuak erabiliz.
	Aplikazioak arriskuan jartzea	Aplikazio bat arriskuan jartzea, softwarearen kalteberatasunak ustiatuz. Adib: SQL injekzioa.
	Lapurreta	Intrusio fisikoa. Adib.: Datuak Prozesatzeko Zentro batera baimenik gabe sartzea.

Zibergorabeheren sailkapena/taxonomia

Sailkapena	Gorabehera-mota	Azalpena eta adibide praktikoak
Eskuragarritasuna	DoS (Zerbitzu-ukatzea)	Zerbitzu-ukatzearen bidezko erasoa. Adib.: web aplikazio batera eskariak bidaltzea, eta, hala, zerbitzu bat etetea edo moteltzea.
	DDoS (Zerbitzu-ukatze banatua)	Zerbitzu-ukatze banatuaren bidezko erasoa. Adib.: SYN paketeen uholdea, UDP-n oinarritutako zerbitzuak erabiliz egindako erreflexio- eta anplifikazio-erasoak.
	Konfigurazio txarra	Softwarea behar ez bezala konfiguratuta egotea, eta, horren ondorioz, zerbitzuan eskuragarritasun-arazoak sortzea. Adib.: DNSSEC-ren erro-eremuaren KSK zaharkitua duen DNS zerbitzaria.
	Sabotajea	Sabotaje fisikoa. Adib.: ekipoen kableak moztea edo suteak eragitea.
	Etenaldiak	Kanpoko arrazoiengatik gertatutako etenaldiak. Adib.: hondamendi naturala.
Informazioa arriskuan jartzea	Informazioa baimenik gabe eskuratzea	Informazioa baimenik gabe eskuratzea. Adib.: trafikoa atzemanez edo dokumentu fisikoetara sartuz sarbide-egiaztagiriak lapurtzea.
	Informazioa baimenik gabe aldatzea	Informazioa baimenik gabe aldatzea. Adib.: erasotzaile batek aldaketak egitea, sistema batetik edo aplikazio batetik ostutako egiaztagiriak erabiliz, edo ransomware bidez datuak enkriptatzea.
	Datuak galtzea	Informazioa galtzea. Adib.: disko gogor batek huts egiteagatik edo lapurreta fisiko bat jasateagatik informazioa galtzea.
Iruzurra	Baliabideak baimenik gabe erabiltzea	Baliabideak helburu desegokietarako erabiltzea, irabazteko asmoa duten ekintzak barnean direla. Adib.: posta elektronikoa erabiltzea, iruzur piramidaletan parte hartzeko.
	Egile-eskubideak	Lizentziarik gabeko softwarea edo egile-eskubideek babestutako bestelako materiala eskaini edo instalatzea. Adib.: Warez.
	Identitatea ordeztea	Mota horretako erasoetan, entitate batek beste baten identitatea ordezten du, legitimoak ez diren onurak lortzeko.
	Phishinga	Beste entitate baten identitatea ordeztea, erabiltzailea konbentzitzeko bere egiaztagiri pribatuak ezagutzera eman ditzan.
Kaltebera	Kriptografia ahula	Publikoki irispidean izan daitezkeen zerbitzuak, kriptografia ahula dutenak. Adib.: POODLE/FREAK erasoak jasan ditzaketen web zerbitzariak.
	DDoS anplifikatzailea	Publikoki irispidean izan daitezkeen zerbitzuak, DDoS erasoen erreflexiorako edo anplifikazio erabili ahal direnak. Adib.: Open resolver erako DNSak, edo monlist monitorizazioa duten NTP zerbitzariak.
	Zerbitzu batzuk erabiltzea, nahiz eta halakoetara sartzea komenigarria ez izan	Adib.: Telnet, RDP edo VNC.
	Informazioa agerraraztea	Publikoki irispidean izatea zerbitzu batzuk, zeinetan bereziki zaindu beharreko informazioa agerian geratu ahal baita. Adib.: SNMP edo Redis.
	Sistema kaltebera	Sistema kaltebera. Adib.: proxy konfigurazio txarra bezeroan (WPAD), sistemaren bertsio zaharkituak.
Beste batzuk	Beste batzuk	Aurreko kategorietan sartzen ez diren gorabehera guztiak.
	APT	Antolakunde jakin batzuei zuzendutako erasoak, ezkutatze-, anonimotasun- eta iraunkortasun-mekanismo oso sofistikatuetan oinarrituak. Mehatxu horretan, helburuak lortzeko, normalean gizarte-ingeniaritzako teknikak erabiltzen dira, eta, horrez gain, eraso-prozedura ezagunak edo beren-beregi sortuak erabiltzen dira.

II. ERANSKINA: Arrakalak jakinarazteko prozedura

Segurtasun-arrakalak kontrol-agintaritzari (DBEA) jakinaraztea.



Sarean ere, auzolana.
Por ti hacemos red.

cyber zaintza

Zibersegurtasuneko gorabeherak

900 104 891

incidencias@cyberzaintza.eus

Autobabeserako planak

jarraipena@cyberzaintza.eus

Informazio orokorra

945 236 636

info@cyberzaintza.eus

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

Segurtasun-arrakalak / Datuak Babesteko Ordezkariaren komunikazioa

Zalantzetarako posta elektronikoa: **teknologia.ebaluazioa@avpd.eus**

Jakinarazpenak: **DBEAren egoitza elektronikoa**

Informazio orokorra

945 016 230

avpd@avpd.eus

Datuak Babesteko Euskal Agintaritza
Autoridad Vasca de Protección de Datos

EUSKO JAURLARITZA
GOBIERNO VASCO

cyber zaintza

www.ciberseguridad.euskadi.eus

www.avpd.eus