

Vicomtech-eko Informazioaren Segurtasunerako Politika

INDIZEA

1. Onartzea eta indarrean jartzea	3
2. Vicomtech-en misioa, helburuak eta gobernu ona	3
3. Informazioaren segurtasunari buruzko politikaren helburuak eta misioa	4
4. Irismena	5
5. Arau-esparrua.....	6
6. Informazioaren segurtasunaren printzipioak	6
7. Informazioaren segurtasuna antolatzea	8
8. Arriskuen analisia eta Kudeaketa	13
9. Informazioaren sailkapena	13
10. Datu pertsonalak.....	14
11. Kontzientziazioa eta prestakuntza	14
12. Langileen betebeharrak	15

1. Onartzea eta indarrean jartzea

Vicomtech-eko **Informazioaren Segurtasunerako Batzordeak** proposatu eta berrikusi du politika hori, eta **Vicomtech**-eko Zuzendaritzak 2025/03/28 onartu du.

Informazioaren Segurtasunerako Politika hori eraginkorra da data horretatik Informazioaren Segurtasunerako Politika berri batek ordeztu duen arte.

Vicomtech-en Informazioaren Segurtasunerako Politika hau indarrean jartzeak lehendik zegoen beste edozein politika indargabetzea dakar.

Informazioaren Segurtasunerako politika hori **gutxienez urtean behin berrikusiko da**, betiere erakundearen aldaketa garrantzitsuak badaude, erakundearen estrategiara eta beharretara egokitzen dela ziurtatzeko.

Gatazkak badaude edo Informazioaren Segurtasunerako Politika honen interpretazio desberdinak badaude, Zuzendaritzara joko da horiek ebazteko, **Informazioaren Segurtasunerako Batzordeari** kontsulta egin ondoren.

2. Vicomtech-en misioa, helburuak eta gobernu ona

Vicomtech-en misioa da:

- Gure inguruneko enpresa eta erakundearen Ikerketa Aplikatuak, Garapeneko eta Informazio Teknologien Berrikuntzako beharrei erantzutea, bereziki Computer Graphics eta Computer Vision (Visual Computing), Data Analytics & Intelligence, Interactive Digital Media eta Language Technologies teknologien arteko konbergentziari dagokionez, erronka ekonomiko eta sozial berriei aurre egiteko aukera izan dezaten, haien lehiakortasuna hobetuz merkatu global honetan.
- Ezagutzaren sormena eta gure teknologien transferentzia bultzatzea, produktu berrien prototipoak garatuz eta negozio-ildo berriak ahalbidetuz industriarekin elkarlanean, jatorrizko Jabetza Intelektualean jasota daudenak.
- Alderdi zientifiko eta teknikoetan eta barne-antolamenduko eta bezeroari zerbitzua emateko alderdietan bikaintasuna lortzea, zientziaren eta industriaren eremuetan aintzatetsitako estandar gorenak eta kalitate-araudiak betez.
- Ezagutza unibertsalari laguntzea, ikertzaileen prestakuntzaren bidez eta ikerketa aplikatuak lanetatik lortutako emaitzak nazioartean ospea duten aldizkari eta

kongresuetan argitaratuz.

- Aliantzak garatzea erreferentziazko bazkide estrategikoekin (akademikoak, ikerketa aplikatukoak eta industrialak), bai bertakoekin, bai nazioartekoekin, sareko ikerketa aplikatua sustatzeko, ikertzaileak prestatzeko eta ezagutza elkarrekin sortzeko.
- Kalitatezko jardun profesional bikainerako ingurunea sustatzea, gure lantaldean elkarlanerako beharrezkoak dituzten gaitasunak garatzeko eta aldaketa teknologikoaren eta oro har berrikuntzaren sustatzaile izateko aukera izan dezaten, zentroan bertan eta industrian zein beste eremu zientifiko-teknologikoetan. Vicomtech-en helburu nagusiak hauek dira::
- Ikertzaile-masa kritiko bat izatea, Eusko Jaurlaritzak ezarritako irizpideekin homologatuta egongo dena eta Ikertzaile Bikainen Profilak izango dituen, euskal unibertsitateekin lankidetzan egindako doktoretza-tesien baterako zuzendaritzaren bidez.
- Lehen mailako aldizkarietan ikerketa-artikuluak argitara daitezen sustatzea.
- Sortutako ezagutza industriari eta gizarteari transferitzea, honako hauen bidez: ikerketa aplikatuko proiektuak kontratatzea, aktiboak babestea eta transferitzea, giza talentua transferitzea edo oinarri teknologikoko enpresa berrietan eragina izatea.

Helburu horiek lortzeko, Zentroaren Gobernu Ona zaindu behar da. **Gobernu Onaren** helburuak honako hauek dira: kultura, etika, erantzukizuna, gardentasuna, efizientzia, arriskuaren kudeaketa eta osotasuna.

Vicomtech-ek modu eraginkor eta efizientean babestu behar diren informazio-sistemak erabiltzen ditu.

3. Informazioaren segurtasunari buruzko politikaren helburuak eta misioa

Politika honek Informazioaren Segurtasunaren arloko jarraibideak eta jarduera ildoak ezartzen ditu, **Vicomtech**-ek bere informazioa eta zerbitzuak kudeatzeko eta babesteko modua arautzen dutenak, bai eta bezeroekiko eta beste interes talde batzuekiko komunikazioa ere.

Vicomtechek informazioaren segurtasuna kudeatzeko esparru bat ezarri du, maiatzaren 3ko 311/2022 Errege Dekretuak ezarritakoaren arabera, zeinaren bidez arautzen baitira Segurtasun Eskema Nazionala (aurrerantzean, **ENS**) eta **ISO/IEC 27001** Informazioaren Segurtasuna Kudeatzeko Sistema (aurrerantzean, **SGSI**), Kudeaketa Integraleko Sistemaren barruan (aurrerantzean, **SGI**).

Informazioaren segurtasunaren kudeaketak bermatu behar du zerbitzuak behar bezala emateko beharrezkoak diren azpiegitura eta instalazio orokorrak kontrolatzeko, monitorizatzeko eta mantentzeko jardueren funtzionamendu egokia, bai eta horien funtzionamendutik eratorritako informazioarena ere. Horretarako, informazioaren segurtasunaren arloko **helburu orokor** hauek ezarri dira:

- Informazioaren segurtasunaren kudeaketatik Vicomtech-ek ezarritako misioa eta Gobernu Ona betetzen laguntzea.
- Garatutako jardueraren ondorioz aplikatzekoak diren legezko baldintzak betetzeko beharrezkoak diren kontrol-neurriak izatea, bereziki datu pertsonalak babesteari eta zerbitzuak bitarteko elektronikoen bidez emateari dagokienez.
- Informazioaren irisgarritasuna, osotasuna, konfidentzialtasuna, erabilgarritasuna, benetakotasuna, trazabilitatea eta zerbitzuen etengabeko prestazioa ziurtatzea, prebentzioz jardunez, eguneroko jarduera gainbegiratzuz eta gertakariei prestutasunez erreakzionatuz.
- Vicomtech-en informazio-baliabideak eta horiek prozesatzeko erabilitako aktiboak babestea, barneko edo kanpoko mehatxuen aurrean, nahita edo ustekabean, informazioaren konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna eta legezkotasuna betetzen direla ziurtatzeko.

Vicomtech-eko Zuzendaritza Batzordeak konpromiso argia hartzen du **Informazioaren Segurtasunerako Politika** hau zabaldu, finkatu eta betetzeko.

4. Irismena

Politika hori nahitaez aplikatu eta bete beharko da Vicomtech-en jarduera guztietan, haren baliabide eta lantoki guztietan eta SEN/SGSIk eta DBEOk eragindako prozesuetan, erakundearekin kontratu edo akordioen bidez lotutako barnekoak edo kanpokoak izan.

Sailek egiaztatu behar dute informazioaren segurtasuna sistemaren bizi-zikloaren etapa bakoitzaren zati integrala dela, sortzen denetik zerbitzua kentzen den arte, bai eta garatzeko edo eskuratzeko erabakiak eta ustiapen-jarduerak ere.

SEN/SGSIren irismenak eragindako **Vicomtech-eko kide bakoitzak segurtasun-politika hori ezagutu eta bete behar du**, bai eta politika hori osatzen duten informazioaren segurtasun-prozedurak ere, eta Informazioaren Segurtasunerako Batzordearen ardura izango da informazioa ukitutako langileengana iristeko behar diren bitartekoak izatea.

5. Arau-esparrua

Segurtasun politika hori maiatzaren 3ko 311/2022 Errege Dekretuaren II. kapituluaren adierazitako oinarriko printzipioen arabera ezartzen da (311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena eta 12. ARTIKULUAN ezarritako gutxieneko baldintzak aplikatuz garatuko dena). SEGURTASUN-POLITIKA ETA GUTXIENEO SEGURTASUN-BALDINTZAK.

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

Era berean, bat etorriko da 59/2003 Legean ezarritakoarekin (Europako Parlamentuaren eta Kontseiluaren 2014ko uztailaren 23ko 910/2014 (EB) Erregelamendua, identifikazio elektronikoari eta barne-merkatuko transakzio elektronikoetarako konfiantzazko zerbitzuei buruzkoa) eta “Konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituen azaroaren 11ko 6/2020 Legea” gehitzearekin.

Gainera, aplikatzekoak izango dira **Vicomtech**-en jardura arautzen duten beste arau guztiak, bere eskumenen esparruan, bai eta Zentroak kudeatutako bitarteko elektronikoetan erabilitako datu, informazio eta zerbitzuen irisgarritasuna, osotasuna, erabilgarritasuna, benetakotasuna, konfidentzialtasuna, trazabilitatea eta kontserbazioa ziurtatzera bideratutakoak ere, bere eskumenak betez.

6. Informazioaren segurtasunaren printzipioak

6.1. Segurtasun integrala

Segurtasuna erakundearen jardura guztiei aplikatzen zaien prozesu integral gisa ulertuko da, eta informazio-sistemekin lotutako elementu tekniko, giza elementu, material eta antolamenduzko elementu guztiek osatzen dute.

6.2. Arriskueta oinarritutako segurtasunaren kudeaketa

Arriskuen analisia eta kudeaketa segurtasun prozesuaren funtsezko parte izango da, eta etengabe eguneratuta egon beharko da, ingurune kontrolatu bat mantentzeko aukera emanaz, arriskuak maila onargarriaraino minimizatuz.

6.3. Prebentzioa, detekzioa, erantzuna eta berreskuratzea

Vicomtech-ek, ahal den neurrian, informazioa edo zerbitzuak segurtasun-gorabeherengatik kaltetuak izatea **saihestu eta saihestuko** du. Horretarako, organo arduradunek SEN/SGSIk eta DBEOk zehaztutako gutxieneko segurtasun-neurriak ezarriko dituzte, bai eta mehatxuen eta arriskuen ebaluazio baten bidez identifikatutako edozein kontrol gehigarri ere.

Neurri eta kontrol horiek, bai eta langile guztien segurtasun-rolak eta -erantzukizunak ere, argi eta garbi definituta eta dokumentatuta egongo dira **Kudeaketa Integralaren Eskuliburuan**, eta ziurtatuko da prebentzio, detekzio, erantzun eta kontserbazio egokia bermatzen dela, **Informazioaren Segurtasun Politika** hau betetzen dela bermatzeko.

6.4. Defentsa-lerroak

Sistemak hainbat segurtasun-geruzaz osatutako babes-estrategia bat izango du, geruzetako batek huts egiten duenean honako hauek ahalbidetzeko moduan antolatuta:

- Saihestu ezin izan diren gertakarien aurrean erreakzio egokia garatzea, sistema osoa konprometitzeko probabilitatea murriztuz, negozioaren jarraipena ziurtatzeko.
- Azken inpaktua minimizatzea.

Defentsa-lerroak antolamendu-, fisika- eta logika-neurriek osatuko dituzte.

6.5. Etengabeko zaintza eta aldizkako berrebaluazioa

Vicomtech-en SGSI/ENS betetzen dela berrikusteko eta egiaztatzeko auditoriak egingo dira, SGSIrako ISO/IEC 27001 Arauaren eta Segurtasun Eskema Nazionala arautzen duen 311/2022 Errege Dekretuaren eskakizunekin; beraz, auditoria horien irismenak eragindako langileek lankidetzan jardun beharko dute auditoria horien eraginkortasunerako, bai eta etengabeko hobekuntzarako ondorioztatzen diren ekintza zuzentzaileak aplikatzeko ere.

Segurtasun-neurriak eta -kontrolak aldian-aldian ebaluatu eta eguneratuko dira Informazioaren Segurtasuna Kudeatzeko Sistemaren barruan, haien eraginkortasuna arriskuen eta babes-sistemen etengabeko bilakaerara egokitze, eta, behar izanez gero, segurtasuna birplanteatzera ere iritsiko dira.

6.6. Segurtasuna, funtzio bereizi gisa

Segurtasun Eskema Nazionalaren 10. artikuluekin bat etorriz, informazioaren arduraduna, zerbitzuaren arduraduna, informazioaren segurtasunaren arduraduna eta sistemaren arduraduna bereiziko dira. Informazio-sistemen segurtasunaren erantzukizuna eta zerbitzuak ematearen gaineko erantzukizuna desberdinak izango dira.

Informazioaren arduradunak tratatutako informazioaren betekizunak zehaztuko ditu; zerbitzuaren arduradunak, berriz, emandako zerbitzuen baldintzak zehaztuko ditu; eta informazioaren segurtasunaren arduradunak erabakiko du zer erabaki hartu behar diren informazioaren eta zerbitzuen segurtasun-betekizunak betetzeko. Sistemaren arduraduna arduratuko da informazio-sistemaren eragiketaz, zehaztutako segurtasun-neurriak kontuan hartuta.

7. Informazioaren segurtasuna antolatzea

Oro har, **Vicomtech**-en **informazio-sistemen erabiltzaile guztiak informazio-aktiboen segurtasunaren erantzule dira**, horiek behar bezala erabiliz, betiere beren eskuduntza profesional eta akademikoen arabera.

Segurtasun-gorabehereri hobeto erantzuteko, Vicomtech-ek lankidetzaharremanak izango ditu segurtasunaren arloan agintaritza eskudunekin, informatika- edo komunikazio-zerbitzuen hornitzaileekin eta informazio-sistemen segurtasuna sustatzen duten erakunde publiko edo pribatuekin.

7.1. Batzordeak: Eginkizunak eta erantzukizunak

7.1.1. Zuzendaritza Batzordea

Informazioaren segurtasunaren arloan, **Vicomtech**-eko **Zuzendaritza Batzordeak** eginkizun hauek ditu:

- Vicomtech-en Informazioaren Segurtasunerako Politika eta aurrekoaren osagarri den beste edozein politika sektorial onartzea, Segurtasun Eskema Nazionalak eta Datuak Babesteko Erregelamendu Orokorra bete ahal izateko.
- **Informazioaren Segurtasunerako Batzordeak** proposatutako antolaketa-garapena onartzea.
- **Informazioaren Segurtasunerako Batzordeko** kideak izendatzea eta kargutik kentzea.
- Informazioaren segurtasunaren arloan neurri egokiak hartzea, **Informazioaren Segurtasunerako Batzordeak** proposatuta.
- **Vicomtech**-eko datuak babesteko ordezkaria izendatzea.

7.1.2. Informazioaren Segurtasunerako Batzordea

Informazioaren Segurtasunerako Batzordea arduratuko da Vicomtech-eko informazioaren

segurtasuna koordinatzeaz.

Honako arduradun hauek osatuko dute, eta Zuzendaritza Batzordeak zehaztuko ditu:

- ✓ Informazioaren arduraduna
- ✓ Zerbitzuaren arduraduna
- ✓ Informazio segurtasunaren arduraduna
- ✓ Sistemaren arduraduna
- ✓ Sistemaren segurtasunaren administratzailea
- ✓ Kudeaketa Integraleko teknikaria

Informazioaren Segurtasunerako Batzordeak eginkizun hauek izango ditu:

- **Vicomtech**-en bilakaera-estrategia lantzea informazioaren segurtasunari dagokionez, eta etengabeko hobekuntza sustatzea.
- Arlo guztiek informazioaren segurtasunaren arloan egiten dituzten ahaleginak koordinatzea, ahaleginak sendoak direla eta gaian erabakitako estrategiarekin bat datoze la ziurtatzeko eta bikoiztasunak saihesteko.
- Informazioaren Segurtasunerako Politika egitea (eta aldizka berrikustea), Zuzendaritza Batzordeak onar dezan.
- Administratzaileen, operadoreen eta erabiltzaileen prestakuntza- eta kalifikazio-baldintzak lantzea eta onartzea, informazioaren segurtasunaren ikuspegitik.
- Ez-betetzeak identifikatzea eta zehapenak proposatzea.
- Arrisku-maila onargarria ezartzea, hondar-arriskuak onartzea eta aktiboen arduradunei jakinaraztea.
- **Vicomtech**-ek bere gain hartutako hondar-arrisku nagusiak monitorizatzea eta horiei buruzko jarduketa posibleak gomendatzea.
- Segurtasun-intzidenteak kudeatzeko prozesuen jarduna monitorizatzea eta horri buruzko jarduketa posibleak gomendatzea. Bereziki, informazioaren segurtasuneko gorabeherak kudeatzeko segurtasun-arloak koordinatzen direla zaintzea.
- Segurtasunari buruzko aldizkako auditoriak egitea sustatzea, erakundeak segurtasunaren arloan dituen betebeharrak betetzen direla egiaztatzeko.
- Vicomtech-en informazioaren segurtasuna hobetzeko planak onartzea eta, bereziki, hainbat arlotan egin daitezkeen planen koordinazioa zaintzea.

- Segurtasun-arloko jarduerak lehenestea, baliabideak mugatuak direnean.
- Informazioaren segurtasuna proiektu guztietan kontuan hartzen dela zaintzea, hasierako zehaztapenetik abian jarri arte.
- Arduradunen artean ager daitezkeen erantzukizun-gatazkak ebaztea, eta erabakitzeko behar besteko aginpiderik ez duten kasuak areagotzea.
- Zuzendaritza Batzordeari informazioaren segurtasunaren egoeraren berri ematea aldizka.

7.2. Rolak: funtzioak eta erantzukizunak

Hauek izango dira Informazioaren Segurtasunerako Batzordeko figura bakoitzaren funtzioak eta erantzukizunak:

7.2.1. Informazioaren arduraduna

Informazioaren arduradunak izango du informazio jakin bat erabiltzeko eta, beraz, babesteko azken erantzukizuna, eta konfidentzialtasun- edo osotasun-gorabehera bat eragiten duen edozein akats edo zabarkeriaren azken erantzulea izango da.

Eginkizun hauek ditu:

- Informazioa behar bezala erabiltzen dela eta, beraz, babesten dela zaintzea.
- Konfidentzialtasun- edo osotasun-gorabehera batera daraman edozein akats edo zabarkeriaren azken erantzulea izatea.
- Segurtasunaren arloko informazioaren betekizunak ezartzea.
- Informazioaren segurtasun-mailak zehaztea.
- Informazioaren segurtasun-maila formalki onartzea.

7.2.2. Zerbitzuaren arduraduna

Zerbitzuaren segurtasun-baldintzak ezartzeko ahalmena du, hau da, zerbitzuen segurtasun-mailak zehazteko ahal.

Eginkizun hauek ditu:

- Zerbitzuaren segurtasun-baldintzak ezartzea, irisgarritasun- eta erabilgarritasun-baldintzak barne.
- Zerbitzuen segurtasun-mailak zehaztea.
- Zerbitzuaren segurtasun-maila formalki onartzea..

7.2.3. Informazioaren segurtasunaren arduraduna

Vicomtech-en informazio-sistemen segurtasunari buruzko funtzioak beteko ditu, eta, horren barruan, informazioaren eta Vicomtech-en erabilitako zerbitzuen segurtasun-baldintzak betetzeko erabakiak zehaztuko ditu.

Eginkizun hauek ditu:

- Erabilitako informazioaren eta sistemek emandako zerbitzuen segurtasun-maila egokia mantentzea.
- ENSek behartzen dituen aldizkako auditoriak egitea edo sustatzea, SENen baldintzak betetzen direla egiaztatzeko.
- Sistemaren arriskuen analisia eta kudeaketa egitea.
- Informazioaren segurtasunaren arloko prestakuntza eta kontzientziazioa kudeatzea.
- Dagoen segurtasun-neurriak erakundearen beharretarako egokiak direla egiaztatzea.
- Sistemaren segurtasunarekin lotutako dokumentazio guztia berrikustea eta osatzea.
- Sistemaren kategoria zehaztea, sistemaren arduradunarekin lankidetzan, Informazioaren Segurtasunerako Batzordeak onar dezan.
- Segurtasun-intzidenteak kudeatzea, jakinarazten direnetik ebazten diren arte, eta Informazioaren Segurtasunerako Batzordeari garrantzizkoenei buruzko aldizkako txostenak egitea.

7.2.4. Sistemaren arduraduna

Figura hori arduratuko da sistemaren eragiketez, eta honako funtzio hauek izango ditu:

- Informazio Sistema bere bizi ziklo osoan kudeatzea, zehaztapenetik, instalaziotik eta funtzionamenduaren jarraipeneraino.
- Sistemaren erabilgarri dauden erabilera-irizpideak eta zerbitzuak definitzea.
- Erabiltzaileak sistemara sartzeko politikak definitzea.
- Sistemaren jarduteko moduen segurtasunari eragiten dioten aldaketak onartzea.
- Sistemaren erabili beharreko hardware eta softwarearen konfigurazio baimendua zehaztea eta konfigurazio horren aldaketa garrantzitsuak onartzea.
- Sistemaren kategoria zehazteko aholkularitza emango dio informazioaren segurtasunaren arduradunari eta/edo Segurtasun Batzordeari.
- Informazio Sistemaren indarreko konfigurazioan egindako aldaketak onartzea.
- Sistemaren segurtasun-neurri espezifikoak ezartzea eta kontrolatzea.

- Kontingentzia eta larrialdi planak ezartzea, langileak ohitzeko ariketak maiz eginez.
- Informazio jakin bat erabiltzeari edo zerbitzu jakin bat emateari uztea, ezarritako baldintzak betetzeari eragin diezaioketen segurtasun-akats larriak detektatzen baditu.

7.2.5. Sistemaren segurtasunaren administratzailea

Aurreko arduradunek zehaztutako segurtasun-funtzionalitateak administratuko ditu. Eginkizun hauek izango ditu:

- Informazio-sistemari aplikatu dakizkiokeen segurtasun-neurriak ezartzea, kudeatzea eta mantentzea.
- Informazio Sistemaren segurtasun mekanismo eta zerbitzuen oinarri diren hardwarea eta softwarea kudeatzea, konfiguratzea eta eguneratzea, hala badagokio.
- Sistemaren erabiltzaileei emandako baimenak kudeatzea, bereziki emandako pribilegioak, sisteman garatutako jardura baimendutakora egokitzen dela monitorizatzea barne.
- Segurtasuneko prozedura operatiboak aplikatzea.
- Ezarritako segurtasun-kontrolak zorrotz betetzen direla ziurtatzea.
- Informazio-sistema maneiatzeko onartutako prozedurak aplikatzen direla ziurtatzea.
- Hardware eta software instalazioak, horien aldaketak eta hobekuntzak gainbegiratzea, segurtasuna arriskuan ez dagoela eta une oro dagozkion baimenekin bat datoze la ziurtatzeko.
- Segurtasun-gertaerak kudeatzeko tresnek eta sisteman ezarritako auditoria teknikoko mekanismoek emandako sistemaren segurtasun-egoera monitorizatzea.
- Segurtasunaren eta Sistemaren arduradunei jakinaraztea segurtasunarekin lotutako edozein anomalia, konpromiso edo ahultasun.

Segurtasun-intzidenteak ikertzen eta konpontzen laguntzea, detektatzen direnetik konpontzen diren arte.

7.2.6. Kudeaketa Integraleko Teknikaria

Eginkizun hauek ditu:

- Sistemaren segurtasunarekin lotutako dokumentazio guztia berrikusi, osatu eta osatzea.
- Informazioaren segurtasunaren arloko prestakuntzaren eta kontzientziazioaren kudeaketan laguntzea.
- Segurtasun-intzidenteen ikerketa babestea eta gainbegiratzea, jakinarazten direnetik ebazten

diren arte, eta Informazioaren Segurtasunerako Batzordeari aldizka txostenik garrantzitsuenak egitea.

7.2.7. Beste rol posible batzuk

Informazioaren Segurtasun Batzordeak egokitzat jotzen duenean, Vicomtech-eko beste arduradun batzuei eman ahal izango die bere bileren berri, kontsulta gisa.

7.2.7.1. Datuak Babesteko ordezkaria

Datu pertsonalak Datuak Babesteko Erregelamendu Orokorraren arabera tratatzen eta babesten direla bermatzeaz arduratzen den pertsona (EB 2016/679 DBEO).

7.2.7.2. Segurtasuneko ofiziala

Vicomtech-en, batzuetan, segurtasun nazionalari eragin diezaiokeen Informazio Sailkatua erabiltzen da. Segurtasuneko ofiziala arduratzen da kategoria horretan sailkatutako zentroko zein proiektu dauden eta bete beharreko baldintzak ezagutzeaz.

8. Arriskuen analisia eta Kudeaketa

Politika honen mendeko sistema guztiei arriskuen azterketa eta kudeaketa egin beharko zaie, eraginpean dauden aktiboak, mehatxuak eta ahultasunak ebaluatuz eta arriskuak arintzeko kontraneurri egokiak proposatuz.

Arriskuen analisia aldizkakotasun honekin berrikusiko da:

- Urtean behin gutxienez, eta akta bidez onartuko da Informazioaren Segurtasunerako Batzordean.
- Informazioan eta/edo emandako zerbitzuetan aldaketa esanguratsuak gertatzen direnean.
- Segurtasun-gorabehera larri bat gertatzen denean edo ahultasun larriak detektatzen direnean.

9. Informazioaren sailkapena

Informazio dokumentatua honela sailkatuko da: publikoa, barnekoa, mugatua, konfidentziala eta sailkatua, eta sailkapen horren arabera erabilera egokia emango zaio.

- **Informazio Publikoa:** negozio-prozesuen parte gisa, edozein bitarteko hirugarrenei helaraztea helburu duen informazioa da, eta, jakinaraziko balitz, ez luke ondoriorik izango erakundearentzat.

- **Barne erabilera:** Vicomtech-eko langileek bakarrik eskuratu behar duten informazio mota da, hau da, ez dago baimenduta erakundetik kanpo jendeak zirkulatzea. Kontrolatu gabe eta/edo galduta jakinaraztea kudeaketarako eragozpen bat izan liteke, baina ez luke galera ekonomikorik edo irudi kalterik ekarriko.
- **Informazio murriztua:** Sail batek, proiektuko kideek, batzorde batek eta abarrek soilik, baina ez enpresa osoak, kontrolpeko sarbidea izan behar duten arlo edo proiektuen barneko informazio sentikorra. Baimenik gabeko langileek informazioa zabaltzeak edo erabiltzeak galera arinak eragin ditzake.
- **Informazio Konfidentziala:** Pertsona talde txiki eta baimendu batek bere eginkizunak betetzeko soilik ezagutu eta erabil dezakeen informazio sentikorra. Baimenik gabeko pertsonen informazio konfidentziala zabaltzeak galera larriak ekar diezazkioke erakundeari, bai materialak, bai irudiarenak, bai legezko erantzukizunak. Datu pertsonalak dituen informazioa barne hartzen du.
- **Informazio Sailkatua:** Segurtasun nazionalari eragin diezaiokeen informazioari eragiten dio. Nazioz gaindiko estatuak edo erakundeak bakarrik erabaki dezakete informazio bat sailkatuta dagoela eta zer mailatan. Vicomtech-en kasuan, kasuen ehuneko oso txikiari eragiten dio, eta, beraz, kasu horietan jarraitu beharreko protokoloaren xehetasuna Vicomtech-eko segurtasun-ofizialaren koordinaziopean tratatzen da. Proiektuko lider edo kide orok (baita proposamena egiteko fasean dagoenak ere) informazio sailkatua erabiltzen ari dela jakin, sortu edo zalantzan badago, informazio horrekin harremanetan jarri behar du.

10. Datu pertsonalak

DBEOn aurreikusitakoa eta legeria nazionalen ondorio horietarako xedatutakoa aplikatuko da.

Vicomtech-ek datu pertsonalak jaso eta tratatuko ditu, baldin eta egokiak, bidezkoak eta gehiegizkoak ez badira eta datu horiek lortu diren eremuari eta helburuei lotuta badaude. Era berean, Datuak Babesteko araudiak betetzeko beharrezkoak diren neurri teknikoak eta antolakuntzakoak hartuko ditu.

11. Kontzientziaketa eta prestakuntza

Segurtasun-prozesuan parte hartzen duten pertsonak eta horien arduradun hierarkikoak kontzientziatzeari arreta handiena eskainiko zaio, ezagutzarik eza, antolaketarik eta koordinaziorik

eza eta jarraibide desegokiak informazio-sistemen segurtasunerako arrisku-iturri izan ez daitezzen.

Informazioarekin eta sistemekin zerikusia duten langile guztiek segurtasunaren arloan dituzten betebeharrei buruzko prestakuntza eta informazioa jaso beharko dute. Haien jarduerak gainbegiratu egin behar dira, ezarritako segurtasun-prozedurak jarraitzen direla egiaztatzeko.

Vicomtech-eko langileek beharrezko prestakuntza eta informazio espezifikoak jasoko dute ematen diren sistemei eta zerbitzuei aplikatu beharreko informazioaren teknologien segurtasuna bermatzeko.

Kontzientziazio jarraituko programa bat ezarriko da Vicomtech-eko kide bakoitzarentzat, bereziki langile berrientzat.

Sistemen segurtasuna beren bizi-zikloaren fase guztietan (instalazioan, mantentze-lanetan, gorabeheren kudeaketan eta eraistean) lan egiten duten eta trebatuta dauden langile kualifikatuek artatu, berrikusi eta ikuskatuko dute.

12. Langileen betebeharrak

Vicomtech-ek kontratatutako edo nolabait Vicomtech-en kontrolpean eta/edo Zuzendaritzaren pean ematen diren edozein motatako zerbitzuak egiten dituzten erakundeko kide eta/edo alderdi interesdun bakoitzak **Informazioaren Segurtasunerako Politika** hau eta Kudeaketa Sistema Integratuan dokumentatutako **Informazioaren Segurtasunerako Araudia** ezagutu eta bete behar ditu.

Langileek segurtasun-intzidenteak jakinarazteko ezarritako prozedurak erabili beharko dituzte, gorabeheraren bat antzemanaz gero.

Donostian, 2025ko apirilaren 3a

Sinatua: Zuzendaritza Orokorra

Data	Describapena	Egileak	Berrikuspena	Bertsioa
28/03/2025	Informazioaren Segurtasunerako Politika sortzea	Informazioaren Segurtasunerako Batzordea	-	1

--