Vicomtech-eko Informazioaren Segurtasunerako Politika

INDIZEA

1. Onartzea eta indarrean jartzea

Vicomtech-eko **Informazioaren Segurtasunerako Batzordeak** proposatu eta berrikusi du politika hori, eta **Vicomtech**-eko Zuzendaritzak 2025/11/27 onartu du.

Segurtasun Politika hau onartzeak Vicomtech behartzen du, bai barruan, bai **hirugarrenen aurrean**. Segurtasunaren Eskema Nazionala (SEN) betez, eta interesdun guztiek hartutako konpromisoaren irismena ezagutzen dutela bermatzeko, politika hau **Vicomtecheko** webgunearen bidez **argitaratuko da**.

Informazioaren Segurtasunerako Politika hori eraginkorra da data horretatik Informazioaren Segurtasunerako Politika berri batek ordezten 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 erakundean 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 erakundeen Ikerketa Aplikatuko, 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 aplikatuko 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 dituena, 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 gainbegiratuz 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. kapituluan adierazitako oinarrizko 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 GUTXIENEKO 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 nazionalean 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 jarduera 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 jarduera 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. Arriskuetan oinarritutako segurtasunaren kudeaketa

Arriskuen analisia eta kudeaketa segurtasun prozesuaren funtsezko parte izango da, eta etengabe eguneratuta egon beharko da, ingurune kontrolatu bat mantentzeko aukera emanez, arriskuak maila onargarrietaraino 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 egokitzeko, eta, behar izanez gero, segurtasuna birplanteatzera ere iritsiko dira.

6.6. Segurtasuna, funtzio bereizi gisa

Segurtasun Eskema Nazionalaren 10. artikuluarekin 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.

6.7. Segurtasuna lehenetsita eta diseinutik

Sistemak berez segurtasuna bermatzeko diseinatuta eta konfiguratuta egon behar dira.

Printzipio honek zera dakar:

- Informazioaren segurtasuna ohiko operatibaren zatitzat hartu behar da, eta IT sistemen hasierako diseinutik aplikatu behar da.
- Sistemek zerbitzua emateko behar den gutxieneko funtzionaltasuna eman beharko dute.

7. Informazioaren segurtasuna antolatzea

Vicomtechek **erantzukizunen bereizketan** oinarritutako Informazioaren Segurtasunaren Gobernantza eredu bat hartu du.

Eredu hori modu arrazoituan hautatu eta egituratu da segurtasuna koordinatzeko, bai IT sistemetan, bai beste arlo batzuetan, eta informazioa behar bezala banatzen dela eta Vicomtechen erabaki korporatiboak hartzen direla ziurtatzeko.

Gobernantzaren egitura **Informazioaren Segurtasunerako Batzordea**ren bidez egituratzen da, segurtasuna kudeatzeko eta koordinatzeko eta SENen (311/2022 Errege Dekretua) definitutako **pertsona bakarreko rolak** izendatzeko funtsezkoa den kide anitzeko organo baten bidez:

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 datozela ziurtatzeko eta bikoiztasunak saihesteko.
- Informazioaren Segurtasunerako Politika egitea (eta aldizka berrikustea), Zuzendaritza Batzordeak onar dezan.
- **Segurtasun Politikaren publizitate egokia ziurtatzea**, barne zabalkundea eta, bereziki, **kanpo argitalpena** zainduz, interesdun guztiek ezagut dezaten, barnekoek zein erakundeaz kanpokoek.

- 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 ahala.

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.
- Sisteman 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.
- Sisteman erabilgarri dauden erabilera-irizpideak eta zerbitzuak definitzea.
- Erabiltzaileak sistemara sartzeko politikak definitzea.
- Sistemaren jarduteko moduaren segurtasunari eragiten dioten aldaketak onartzea.
- Sisteman 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 aplika 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 jarduera 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 datozela 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.

7.3. Gatazkak konpontzea

Informazioaren arduradunaren, zerbitzuaren arduradunaren, segurtasunaren arduradunaren edo sistemaren arduradunaren arteko gatazken kasuan, **Informazioaren Segurtasunerako Batzordeak izango du desadostasunak ebazteko** eta erabaki loteslea hartzeko **ardura**. Segurtasun Batzordeak behar besteko aginpiderik ez badu, **Vicomtecheko Zuzendaritza Batzordeari helaraziko zaio** desadostasuna, behin betiko ebatz dezan.

7.4. Dokumentuak egituratzeko jarraibideak

Vicomtecheko Informazioaren Segurtasunerako Politika goi mailako dokumentu bat da, erakundeak segurtasunari buruz duen jarrera definitzen duena.

- Behar bezala aplikatzen eta operatiboki garatzen direla bermatzeko, Vicomtechek segurtasun-neurriak ezartzeko erabiliko diren prozedurak definitzen ditu, eta prozedura horiek koherenteak dira politika horrekin eta Vicomtecheko Kudeaketa Integraleko Sistemarekin (KSI).
- Sistemaren segurtasunari, kudeaketari eta sarbideari buruzko dokumentazioa honako garapen-tresna hauetan egituratuko da hierarkikoki:

1. **Kudeaketa Integraleko Eskuliburua eta P-05.14-Informazioaren segurtasuneko eragileak**:
   - Informazioaren segurtasunari buruzko eta Kudeaketa Integraleko Sisteman integratzeari buruzko dokumentu-zerrenda jasotzen dute.
2. **Prozedura orokorrak eta espezifikoak**:
   - Nahitaezko dokumentuak dira.
   - Sistemaren alderdi zehatzen erabilera bateratzea dute helburu.
   - Erabiltzaileen erabilera zuzena eta erantzukizun espezifikoak adierazten dituzte.
   - Erabiltzaileei segurtasun neurriak behar bezala aplikatzen laguntzea du helburu.
   - Segurtasun-alderdi garrantzitsuak alde batera uztea saihesten laguntzen dute.
3. **Jarraibideak**:
   - Zeregin zehatz eta errepikakorrei aurre egiten diete.
   - Eragiketa segurua bermatzeko urratsez urrats egin behar dena adierazten dute.

Garapeneko segurtasun-araudi guztia erakundeko kide guztien eskura egongo da, hura ezagutu behar badute, batez ere informazio- eta komunikazio-sistemak erabiltzen, jardun edo administratzen dituzten pertsonentzat. Vicomtechek argi eta garbi bereiziko ditu politika abstraktua eta haren aplikazio zehatza, aldaketa teknologikoaren eta emaitzen uniformetasunaren aurrean malgutasunari eusteko.

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 kudeaketak Datuak Babesteko araudiaren ondoriozkoak ere jaso behar ditu, Datuak Babesteko Ordezkariaren iritzia eta aholkularitza kontuan hartuta, eta, gainera, arriskua tratatzeko planak koordinatuko dira.

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.
- Datuak babesteko arriskuen analisian edo inpaktuaren ebaluazioetan aldaketak gertatzen direnean.

Informazioaren Segurtasunerako Batzordea izango da arriskuaren neurketa estandarizatzeaz eta erakunde osoan segurtasuna modu global eta eraginkorrean lantzeko baliabideak ziurtatzeaz arduratuko den organo nagusia.

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

pertsonei 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 estatuek edo erakundeek 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 nazionalean 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. Segurtasun-intzidenteen kudeaketa

Zerbitzuen jarraitutasuna bermatzeko eta mehatxuen aurrean prestutasunez jarduteko, Vicomtechek konpromisoa hartzen du prozedura formal eta dokumentatu bat izateko, informaziorako eta zerbitzuetarako mehatxu diren segurtasun-gertaerak eta -gertakariak arin kudeatzeko:

- Prozedura horrek intzidenteak detektatzea, eustea, arintzea eta konpontzea bermatuko du.
- Behar diren neurriak hartuko dira antzemandako gertakariak berriro gerta ez daitezen.
- Sailek prest egon behar dute gertakariak prebenitzeko, detektatzeko, erreakzionatzeko eta lehengoratzeko.

11.1. Erantzukizunak eta barne-koordinazioa

Segurtasun-intzidenteak kudeatzea erantzukizun partekatua da:

1. **Informazioaren Segurtasunaren arduraduna** (ISS): ISSak segurtasun-intzidenteak kudeatzen ditu, jakinarazten direnetik konpontzen diren arte. Gainera, gorabehera

garrantzitsuenei buruzko aldizkako txostenak egin behar dizkio Informazioaren Segurtasunerako Batzordeari.

2. **Informazioaren Segurtasunerako Batzordea**: Batzordeak segurtasun-intzidenteak kudeatzeko prozesuen jarduna monitorizatu behar du, eta egin daitezkeen jarduerak gomendatu. Bereziki, informazio-intzidenteen kudeaketan segurtasun-arloak koordinatzen direla zainduko du Batzordeak.

3. **Vicomtecheko langileak**: Erakundeko langile guztiek segurtasun-intzidenteak jakinarazteko ezarritako prozedurak erabili behar dituzte, gorabeheraren bat antzemanez gero.

4. **Kudeaketa Integraleko Teknikaria eta Segurtasun-Administratzailea**: Bi figura hauek segurtasun-intzidenteak ikertzen eta konpontzen lagunduko dute, atzematen direnetik konpontzen diren arte.

11.2. Integrazioa eta hirugarren aldeak

Vicomtecheko gertakariak kudeatzeko prozedura beste arau sektorial batzuetatik eratorritako betekizunekin integratuko da, hala nola datu pertsonalak babesteari buruzkoarekin, erantzuna ikuspegi desberdinetatik koordinatzeko.

Hirugarren alderdiak, zerbitzu-emaileak edo konponbide-hornitzaileak tartean sartzen diren gorabeheren kasuan:

- Hirugarrenekin izandako gorabeheren berri emateko eta konpontzeko prozedura espezifikoak ezarriko dira.
- Gorabehera hauek inplikatutako hirugarrenen Kontaktu Puntuaren (POC) bidez bideratu beharko dira nahitaez.
- Gertakariak datu pertsonalei eragiten badie, Datuak Babesteko Ordezkariaren bidez ere bideratu beharko da komunikazioa.

Beharrezkoa denean, Informazioaren Segurtasunerako Batzordeak erantzuna eta komunikazioa koordinatuko ditu, kontrol-erakundeei behar ez bezalako atzerapenik gabe informazioa ematen zaiela ziurtatzeko. Estatuko Segurtasun Indar eta Kidegoei ere jakinaraziko zaie, edo epaitegiei, beharrezkoa denean.

12. Kontzientziazioa 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 daitezen.

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 espezifikoa 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.

13. Hirugarren Alderdiak / Zerbitzu Emaileak / Soluzio Hornitzaileak

Atal honek segurtasun jarraibideak ezartzen ditu, Vicomtechek kudeatutako informazioa eta zerbitzuak hirugarrenek parte hartzen dutenean babesten direla bermatzeko, 311/2022 Errege Dekretuaren arabera.

13.1. Vicomtech, Zerbitzu-Emaila gisa

Vicomtechek beste erakunde batzuei zerbitzuak ematen dizkienean edo beste erakunde batzuen informazioa maneiatzen duenean, Informazioaren Segurtasunerako Politika honen berri emango zaie:

- Datuak babesteko araudiaren ondoriozko betebeharrak errespetatuko dira, Vicomtechek zerbitzu horiek ematean tratamenduaren arduradun gisa jarduten badu.
- Informazioa emateko eta segurtasun-batzordeekin koordinatzeko bide espezifikoak ezarriko dira.
- Segurtasun-gorabeheren aurrean erreakzionatzeko jarduketa-prozedurak ezarriko dira.
- Vicomtecheko Informazioaren Segurtasunerako arduraduna (gertaerak@vicomtech.org) komunikazio horietarako Harremanetarako Gunea (POC) izango da.

13.2. Vicomtech, Zerbitzuen Bezero gisa edo Soluzioak Eskuratzeko

Vicomtechek hirugarrenen zerbitzuak erabiltzen dituenean, hirugarrenei informazioa lagatzen dienean edo produktu eta soluzioak erosten dituenean, horiek Segurtasun Politika honetan eta haiei dagokien Segurtasun Araudian ezarritako betebeharren mende geratuko dira.

- **Kontratua betetzea**: Zerbitzu-emaileak kontratatzean edo produktuak eskuratzean, esleipendunak SENarekin betetzeko duen betebeharra hartuko da kontuan.
- **Hodeiko zerbitzuak**: Hodeian aktiboak erabiltzeko eskubideak eskuratzean, erakundeak kontuan hartuko ditu SENaren II. eranskineko segurtasun-neurrietan eta dagozkion garapen-gidetan ezarritako baldintzak, arriskuen analisia eta erantzukizun partekatuaren azterketa.
- **Gainbegiratzea eta Auditoria**: Hirugarren zatia, araudia betetzeko bere prozedura operatiboak garatu arren, Vicomtechek horiek gainbegiratu edo betetze ebidentziak eskatu ahal izateko betebeharren mende geratuko da. Horrek bigarren edo hirugarren parteko auditoretzak eskatzeko aukera ematen du.
- **Kontzientziazioa**: Hirugarrenen langileak segurtasun arloan behar bezala kontzientziatuta daudela bermatuko da, gutxienez politika honetan ezarritako maila berean edo kontratuan berariaz eska daitekeenaren maila berean.

13.3. Hirugarrenekiko Intzidenteak Kudeatzea

Hirugarrenekin izandako gorabeheren berri emateko eta konpontzeko prozedura espezifikoak ezarriko dira. Prozedura horiek honako hauen bidez bideratu beharko dira nahitaez:

1. Inplikatutako hirugarrenen POCa (Harremanetarako Gunea).
2. Datuak Babesteko Ordezkaria (DPO), gertakariak datu pertsonalei eragiten badie.

13.4. Hirugarrenen Ez-Betetzeagatiko Arriskuak Onartzea

Politikaren alderdiren bat ezin badu bete hirugarren batek (zerbitzu-emaileak edo konponbide-hornitzaileak), prozedura formal bati jarraituko zaio arriskuak bere gain hartzeko:

1. Segurtasunaren arduradunak txosten bat egingo du, zer arrisku dauden eta nola tratatu behar diren zehazteko.
2. Txosten hau informazioaren arduradunek eta eragindako zerbitzuek onartu beharko dute.

3. Txostena Informazioaren Segurtasunerako Batzordeari helaraziko zaio, eta hark baimena eman beharko du hirugarrena kontratatzeko izapideekin jarraitzeko, antzemandako arriskuak formalki bere gain hartuta.

13.5. Adimen Artifizialeko (AA) Sistemak Eskuratzea eta Hedatzea

Vicomtechek Adimen Artifizialeko sistema bat eskuratzen, garatzen edo ezartzen duenean, indarrean dagoen araudia betetzeaz gain (2024/1689 (EB) Erregelamendua barne), prozesu horrek honako hauek izan beharko ditu:

- Eskuraketaren kasuan, Zuzendaritza Batzordeak Kudeaketa Sistema Integralaren barruan Software Erabilgarriaren jarraibideei buruz zehaztutakora egokitu beharko da. Datuak Babesteko ordezkariak bere iritzia eman beharko du.
- Garatzeari eta ezartzeari dagokionez, Kudeaketa Integraleko Sistemaren barruan softwarea garatzeko jarraibideei dagokienez Zuzendaritza Batzordeak zehaztutakora egokitu beharko da.

14. 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 antzemanez gero.

Donostian, 2025ko azaroaren 27a

Sinatua: Zuzendaritza Orokorra

72429210W JULIAN FLOREZ (R: G75051912)

Digitally signed by 72429210W JULIAN FLOREZ (R: G75051912)
Date: 2025.11.27 15:52:43 +01'00'

Data	Deskribapena	Egileak	Berrikuspena	Bertsioa
28/03/2025	Informazioaren Segurtasunerako Politika sortzea	Informazioaren Segurtasunerako Batzordea	-	1
27/11/2025	2025eko ekaineko gida berrira egokitzea	Informazioaren Segurtasunerako Batzordea	-	2