INFORMAZIOAREN SEGURTASUN POLITIKA

Bertsioa:	1.0
Bertsioaren data:	2024-02-22
Mota:	*Publikoa*

1. SARRERA

IZT KOOP.E.k IKT sistemak ezinbesteko ditu (Informazio Teknologiak eta Komunikazioak) bere helburuak lortzeko. Sistema horiek arduraz administratu behar dira, tratatutako informazioa edo emandako zerbitzuen erabilgarritasunari, osotasunari edo konfidentzialtasunari eragin diezaieketen istripu-kalteetatik, izan nahigabe zein nahita eragindakoak, babesteko neurri egokiak hartuz.

Informazioaren segurtasunaren helburuak informazioaren kalitatea eta zerbitzuak etengabe ematen direla bermatzea, prebentzioz jardutea, eguneroko jarduera gainbegiratzea eta gertaeren aurrean azkar erreakzionatzea dira.

IKT sistemek eboluzio azkarreko mehatxuen aurka babestuta egon behar dute, konfidentzialtasuna, osotasuna eta erabilgarritasuna bermatuz, erabilera desberdinak aurreikusiz eta zerbitzuen balioan eraginez. Mehatxu horietatik babesteko, inguruneko baldintzetan gertatzen diren aldaketetara egokitzeko zein zerbitzuen etengabeko prestazioa bermatzeko estrategia bat behar da. Horregatik IZTk Segurtasun Eskema Nazionalak zein ISO 27001 arauak oinarri gisa hartuta, bere zerbitzuetan segurtasun neurriak aplikatzen ditu. Beraz, zerbitzuak emateko egoeren etengabeko jarraipena egin, kalteberatasunak antzeman zein analizatu eta intzidenteei erantzun eraginkorra emanez zerbitzuen jarraitutasuna bermatzeko jarduten du. IZTk ziurtatu behar du zerbitzuen bizi zikloaren etapa guztietan IKTen segurtasuna integrala dela eta garapen zein eskuratze erabakiak eta ustiapen-jarduerak kudeatzen direla. Segurtasun-betekizunak eta finantzaketa-beharrak identifikatu eta planginтzan sartu behar dira.

IZTk eta bertako pertsonek prestatuta egon behar dute prebenitzeko, detektatzeko, erreakzionatzeko eta suspertzeko, indarrean dagoen arautegi zein legediaren arabera.

1.1. PREBENTZIOA

IZTk saihestu behar du, edo ahal den neurrian behintzat prebenitu, segurtasun-intzidenteen ondorioz, informazioa edo zerbitzuak kaltetzea. Horretarako, ENS zein ISO 27001 arauek zehaztutako gutxieneko segurtasun-neurriak ezarri ditu, bai eta mehatxuak eta arriskuen balorazio eta analisiaren ondorioz identifikatutako beste hainbat kontrol. Kontrol horiek, eta segurtasun rol zein erantzukizunak argi eta garbi definituta zein dokumentatuta daude. Politika betetzen dela bermatzeko, IZTk honako hauek egin behar ditu, besteak beste:

- Sistemen baimentzea eragiketan hasi aurretik.
- Segurtasuna erregulartasunez ebaluatzea,
- Hirugarrenek sistema aldizka berrikustea.

1.2. DETEKZIOA

Gertaeren ondorioz zerbitzuak azkar degradatu daitezkeenez zerbitzuek monitorizatu behar dute iraunkorki anomaliak detektatzeko eko ENSko 9. artikuluan ezarritakoaren arabera jardun. Monitorizazioa bereziki garrantzitsua da ENSko 8. artikuluarekin bat defentsa lerroak eraikitzeko.

1.3. ERANTZUNA

IZTk honako hauek egin behar ditu:

- Segurtasun-intzidenteei eraginkortasunez erantzuteko mekanismoak ezarri.
- Gertakariei buruzko komunikazioetarako eta harremanetarako gunea izendatu.
- Gertaerarekin lotutako informazioa trukatzeko protokoloak ezarri.

1.4. BERRESKURATZEA

Zerbitzu kritikoen erabilgarritasuna bermatzeko, IZTk IKT sistemen jarraitutasun-planak garatu du, negozioaren jarraitutasuna orokorraren plan orokorraren baitan.

2. IZT-REN MISIOA

IZT 2005. urtetik bere bezeroen bidelagun izan da hauen transformazio digitalean zein haien esperientzia teknologikoa eraginkorra izateko eguneroko ariketan.

Zentzu horretan, eta bezeroek IKTen inguruan dituzten beharrak asebetetzeko asmoz, etika profesionalari, zerbitzuaren kalitateari eta etengabeko hobekuntzari arreta berezia jartzen diogu.

Sorreratik gure helburua bezeroei informatikaren zuzenbidean zein informazioaren segurtasun eta pribatutasun alorretan aholkularitza hurbila eta profesionala eskaintzea izan da eta, honek egun duen garrantziaz jabetuta, IZTk aterpetzen dituen zerbitzu guztietan barne biltzea.

Hiru adar zehaztu ditugu aro berri honetarako, gure bezeroei arreta espezializatuagoa eman asmoz: ***Informazio sistemak, Cloud zerbitzuak eta Aplikazioen programazioa***. Hiru adar hauen bidez, gure bezeroei atal hauetan zerbitzu bereziak eskainiko dizkiegu,

IZTk eskaintzen dituen zerbitzuetan, informazio sistemak, cloud zerbitzuak eta aplikazioen programazioan, zehar lerro gisa segurtasun irizpideak, legen betekizuna eta zaintza teknologikoa lantzen dira.

Bere langileen konfidentzialtasun eta profesionaltasunaz batera, IZT osatzen duten pertsona guztiak bere inguruarekiko sentsibilitate berezia dute.

3. HELBURUA, ALKANTZEA ETA ERABILTZAILEAK

Politika honen helburua informazioaren segurtasunerako oinarrizko irizpide eta arauak zehaztu eta kudeatzea da. Honako Politika IZT KOOP.E.ko antolakunde osoari aplikatzen zaio.

Dokumentu honen erabiltzaileak IZTko lantaldeko kideak dira eta berretsi zein, behar izanez gero eguneratu behar du gutxienez urtean behin.

4. ERREFERENTZIAZKO DOKUMENTUAK

- ISO/IEC 27001 Araua, 5.2 eta 5.3 atalak
- SEN-ENS 311/2022 Errege dekretua
- ISKSaren alkantzeari buruzko dokumentua
- Arriskuen analisi eta tratamendurako metodologia
- Aplikabilitate adierazpena
- Legezko betekizunen zerrenda zein arau edota hitzarmenen zerrenda
- Jarraikortasun Plana
- Intzidentzien kudeaketarako prozedura

5. INFORMAZIOAREN SEGURTASUNAREN KUDEAKETA

5.1. Helburuak eta neurketa

Informazioaren segurtasunerako kudeaketa sistemaren helburu orokorrak honakoak dira:

- IZT KOOP.E.ko informazio baliabideak babestea barne zein kanpo mehatxuen aurrean, informazioaren konfidentzialtasuna, osotasun, eskuragarritasuna, legalitatea eta fideltasuna bermatzeko.
- IZT KOOP.E.ek eskaintzen dituen zerbitzuetan informazioarekin zein hau kudeatzen duten sistemekin burutzen diren jarduerak modu seguruan egiten direla ziurtatzea eta bezeroei horren bermea eskaintzea.
- Merkatuan irudi egokia sortzea balizko intzidentzien kalteak ahalik eta gehien gutxituz eta segurtasun irudia islatuz.
- Segurtasun Politika honetan jasotako segurtasun neurrien inplementazioa bermatzea.
- IZT KOOP.E.ko Segurtasun Politika eguneratua mantentzea, honen eraginkortasuna bermatzeko.

IZT KOOP.E.ko ISKS arduraduna zein lan taldea helburu hauek iraunkorki berrikusi eta, behar izanez gero, berriak ezartzeko arduradunak dira. Segurtasun kontrol indibidualen helburuak ISKS arduradunak proposatuko ditu eta ISKS lan taldeak onartu beharko ditu. Helburu guzti hauek urtean behin gutxienez berrikusi beharko dira.

IZT KOOP.E.k helburu hauen betetze maila neurtuko du. Helburuen betetze maila neurtzeko metodoa zehazteko ardura ISKSaren arduradunarena izango da; helburuak gutxienez urtean behin neurtuko dira eta ISKSaren lan taldeak hauek baloratu eta IZT KOOP.E.eko zuzendaritzari emaitzak jakinaraziko dizkio.

5.2. Informazioaren segurtasunerako betebeharrak

Honako Politikak, zein ISKS osoak orohar, informazioaren segurtasunarekin zerikusia duten lege, arau zein kontratu bidezko betekizun guztiak bete behar ditu.

IZT KOOP.E.ko ISKS gunean zerrendatzen dira lege, arau zein kontratu bidezko betekizunak.

5.3. Informazioaren segurtasunerako kontrolak (babesak)

Kontrolak (babesak) aukeratzeko prozesua arriskuen balorazio eta tratamendurako metodologian zehaztua dago: IZT KOOP.E.ko ISKS gunean eta aukeratutako kontrolak zein hauen inplementazio egoera Aplikabilitate Adierazpenean zehaztuak daude.

5.4. Informazioaren segurtasuna bermatzeko prozedura eta politika zehatzak

Informazioaren segurtasuna bermatzeko hainbat arlotan prozedura eta politika zehatzak adostu eta ezarri dira. Hauek guztiak IZT KOOP.E.eko ISKS gunean jasotzen dira; hona:

- Gailu mugikorrak eta tele-lana
- Ekarri zure gailua politika
- ISKSaren dokumentuen onarpen adierazpena
- Konfidentzialtasun adierazpena

- Aktiboen inbentarioa
- Informazioaren sailkapena
- Erabilera onargarria
- Pasahitzak
- Atzipenen kontrola
- Kontrol kriptografikoen erabilera
- Ezabatze eta deuseztea
- Pantaila eta mahai gain garbia
- Gune seguruetan lan egitea
- Segurtasun kopiak
- Aldaketen kudeaketa
- IKT eta komunikazioetarako prozedura operatiboak
- Informazioaren transferentzia
- Segurtasun betebeharrak
- Garapen segurua
- Hornitzaileentzako segurtasuna
- Intzidentzien erregistroa
- Intzidentzien kudeaketa
- Negozioaren jarraikortasuna
- Negozio inpaktuen analisirako metodologia
- Negozioaren jarraikortasunerako estrategia
- Negozioaren jarraikortasunerako plana

5.5. Segurtasunaren antolaketa

ISKSaren atal desberdinen ardurak IZT KOOP.E.ko langile desberdinen artean banatzen dira. Hona arduren zehaztapenak:

5.5.1. Batzordeak

IZT antolakunde txikia izanik ISKS batzordeak segurtasun batzordearen zein sistemetako batzordearen funtzioak hartuko ditu bere gain. Honakoek osatutzen dute ISKS batzordea:

- Informazioa eta zerbitzuen arduraduna
- Segurtasun arduraduna
- Sistemetako arduraduna

5.5.2. Rolak: Funtzio eta ardurak

Adura	Funtzioa
Informazioa eta zerbitzuen arduraduna	ISKSaren arduraduna, datu pertsonalen tratamendu arduraduna, informazioaren arduraduna, zerbitzuaren arduraduna Beste funtzioak: Trebakuntza eta kontzientziazioa, betekizunak, dokumentuen sailkapen eta kontrola, giza baliabideak, hornitzaileak...
Segurtasun arduraduna	Informazioa behar bezala segurtatzen dela bermatzen duena. Segurtasun intzidentziak kudeatzen dituena Beste funtzioak: metrikak eta adierazleak, barne auditoriak, hobekuntza...
Sistemaren arduraduna	Azpiegitura eta neurri teknikoak kudeatzea, aktiboen babesa, segurtasun fisikoa, segurtasun neurriak...

5.5. Izendapen prozedura

Zehaztutako ardurak zuzendaritzak izendatuko ditu, ISKS Batzordearen proposamenak entzunez. Izendapen hauek gutxienez urtean behin berrikusi behar dira.

5.6. Politikaren komunikazioa

Informazioa eta zerbitzuen arduradunak bermatu behar du langile guztiak zein IZT KOOP.E.rekin harremana duten hornitzaile zein hirugarren parteek Politika hau ezagutzen dutela.

6. ARRISKUEN KUDEAKETA

Segurtasun politika honi lotutako sistema guztiek arriskuen analisi bat pasa beharko dute, jasan ditzaketen mehatxu eta arriskuak ebaluatzen. Honako kasuetan analisia errepikatu da:

- Iraunkorki, gutxienez urtean behin.
- Baliatzen den informazio mota aldatzen denean.
- Eskaintzen diren zerbitzuak aldatzen direnean.
- Segurtasun intzidentzia larri bat gertatzean.
- Kalteberatasun larriak antzematen direnean.

Arriskuen analisiak orekatzeko, ISKS Batzordeak erreferentziazko balorazio bat egingo du baliatutako informazio mota desberdinentzat zein eskaintzen diren zerbitzu desberdinentzat. ISKS Batzordeak sistemen segurtasun-beharrei erantzuteko baliabideen eskuragarritasuna dinamizatuko du.

7. ISKSAREN INPLEMENTAZIOARI BABESA

Honako dokumentuaren bidez Informazioa eta zerbitzuen arduradunak, ISKSaren arduradun gisa eta zuzendaritzaren ordezkari gisa, ISKSaren inplementazio zein etengabeko hobekuntza prozesuan, Politika honen helburuak erdiesteko eta identifikatu betekizunak betetzeko behar diren baliabideak jartzen ahaleginduko dela adierazten du.

7.1. ZUZENDARITZAREN BABESA

IZTko Zuzendaritza jakitun da informazioaren segurtasuna garrantzitsua dela bere negozio-helburuak arrakastaz gauzatzeko, konpromiso hauek hartzen ditu:

- Antolamenduan funtzioak eta erantzukizunak sustatzea informazioaren segurtasunaren arloan.
- Informazioaren segurtasun-helburuak lortzeko baliabide egokiak eskaintzea.
- Informazioaren segurtasun-politikaren zabalkundea eta kontzientziazioa bultzatzea IZTko bazkide eta langileen artean.
- Informazioaren segurtasunari dagokionean indarrean dagoen politika, legeria eta arautegien betetzeak bermatzea.
- Erabakiak hartzean informazioaren segurtasunaren arriskuak kontuan hartzea.

8. LANGILEEN BETEBEHARRAK

IZT KOOP.E:ko kide guztiek jakin eta bete behar dute Informazioaren Segurtasunari buruzko Politika hau eta Segurtasunari buruzko Araudia, IKTen Segurtasun Batzordearen eginkizuna izanik behar diren baliabideak jartzea informazioa iristeko behar bezala interesatu guztiei.

IZT KOOP.E. ko kide guztiek gaiari buruzko kontzientziazio-saio bat jasoko dute gutxienez urtean behin.

IKT sistemak erabiltzen edo administratzen erantzukizuna duten pertsonak sistemak segurtasunez erabiltzeko prestakuntza jasoko dute.

9. HIRUGARREN PARTEAK

IZT KOOP.E.k beste erakunde batzuei zerbitzuak ematen dizkienean edo beste batzuen informazioa erabiltzen duenean Informazioaren Segurtasun Politika honen berri emango zaie, dagozkien Segurtasun Batzordeak informatzeko eta koordinatzeko kanalak ahalbideratuko ditu, eta balizko segurtasun intzidentzien aurrean jarduteko prozedurak ezarriko dira.

IZT KOOP.E.k hirugarrenen zerbitzuak erabiltzen dituenean edo hirugarrenei informazioa lagatzen badie Segurtasun Politika honen eta Segurtasun Araudiaren berri emango zaie hirugarren aldeei. Bermatuko da hirugarrenen langileak behar bezala kontzientziatuta daudela segurtasun arloan, gutxienez politika honetan ezarritako maila berean.

Politikaren atal bat heren batean ase ezin duenean, segurtasun-arduradunak txosten bat egin beharko du arriskuak eta horiek tratatzeko modua zehaztuz.

10. INFORMAZIOAREN SEGURTASUN-POLITIKA GARATZEA

Informazioaren Segurtasunerako Politika hau beste politika edo arautegi batzuen bidez garatuko da. Politika eta araudi horien ondorioz prozedurak garatu dira horiek gauzatzeko bidea deskribatzen dutenak.

Politiken eta araudien dokumentazioa, bai eta honako Segurtasun Politika hauen ezagutza behar duten IZTko langile guztien eskura egongo da; bereziki informazio eta komunikazio sistemak erabiltzen edo administratzen dituzten langileei dagokionean

10.1. ARAUEN EGITURA

Informazioaren Segurtasun Politika nahitaez bete beharrekoa da, eta honako maila hauetan egituratzen da hierarkikoki:

1. **Lehen maila:** Informazioaren Segurtasun Politika.
2. **Bigarren maila:** Informazioaren segurtasun araudiak.
3. **Hirugarren maila:** Informazioaren segurtasunerako prozedurak eta jarraibide teknikoak.
4. **Laugarren maila:** txosten, erregistro eta ebidentzia elektronikoak.

Egitura hierarkikoari esker, maila baxuagoak eraginkortasunez egokitu daitezke IZTko inguruneetako aldaketetara segurtasun estrategia berrikusi beharrik gabe.

IZTko langileek nahitaez jakin eta bete beharko dute, Segurtasun Politika honetaz gain, beren eginkizunei eragin diezaieketen Informazioa, Araudiak eta Segurtasun Prozedura eta Jarraibide Tekniko guztiak.

11. DOKUMENTUEN KUDEAKETA ETA BALIOA

Honako dokumentua baliozkoa izango da 2024ko azaroaren 2 arte

Dokumentu honen jabea Informazioaren arduraduna da eta bera da dokumentua berrikusi eta, behar denean, eguneratzeko ardura duena; edonola gutxienez urtean behin.

Dokumentuaren eraginkortasuna eta egokitasuna neurtzeko orduan honako irizpideak hartu behar dira aintzat:

- ISKSarekin lotutako langile, hornitzaile eta hirugarrenak honakoa dokumentua ezagutzen ez dutenak.
- ISKSarekin lotutako lege, arau edo hitzarmenen ez betetzeak.
- ISKSaren inplementazio edo mantentzearen eraginkortasun falta.
- ISKSaren inplementazio edo mantentzean ardura ez egokiak.