Informazioaren segurtasunari buruzko eskuliburua

2025eko ekainaren 20a

Negozio Bezeroak – Espainia

Edukia

Bertsioen historia:

Bertsioa	Egilea:	Onartzailea	Egoera	Arazoaren/aldaketaren arrazoia	Data
v1	Negozio Bezeroak Espainia	CEO Negozio Bezeroak	Onartua	• Lehen bertsioa	2025/06/20

1. Sarrera

1.1. Xedea

Informazioaren segurtasunari buruzko eskuliburu honetan (Espainiako Bezero diren Negozioen Informazioaren Segurtasun Politika ere deitzen zaio) informazioaren segurtasunari buruzko jarraibide orokorrak ezartzen dira. Espainiako Bezero Negozioak (aurrerantzean, NCE) jarraibide horiek aplikatu behar ditu, informazioaren konfidentzialtasunari, osotasunari, erabilgarritasunari, trazabilitateari eta benetakotasunari nolabait eragin diezaieketen mehatxuetatik behar bezala babesteko, horrek aktiboak galtzea edo gaizki erabiltzea, haien irudia eta ospea kaltetzea eta/edo negozioaren euskarri diren prozesuak etetea ekar baitezake. Era berean, informazioaren segurtasunaren helburuak zehazten dira.

Eskuliburu hau onartuz, NCEk adierazi du bere zehaztasuna eta konpromisoa dela bere beharretara egokitutako informazioaren segurtasun-maila lortzea, aktiboak modu homogeneoan babestuko direla eta lotutako arriskuak modu egokian kudeatuko direla bermatzeko. Era berean, konpromisoa hartzen du Informazioaren Segurtasuna Kudeatzeko Sistema etengabe hobetzeko eta ezarritako helburuak eta aplikatu beharreko araudi guztia betetzeko, barnekoa zein kanpokoa.

1.2. Aplikazioa-eremua

Dokumentu hau nahitaez aplikatu behar zaie NCEko langile guztiei, bai eta NCEren jabetzako informazioa eta haren euskarri diren sistemak erabiltzen eta babesten esku hartzen duten erakunde laguntzaileei ere. Zibersegurtasuneko ez-betetzeak eta zehapenak Iberdrolaren hitzarmen kolektiboan jasota daude.

Eskuliburu honek (edo Informazioaren Segurtasun Politikak) NCEko kide guztien eskura egon behar du, eta alderdi interesdunen eskura.

Ziurtapenaren irismena, SENen, maila ertainean eta ISO 27001 arauan, honako hau da: "*Bezero Taldearen eta Espainiaren arteko negozioko kanal digitalen bidezko kontratazio-prozesuari eta karga publikoko prozesuari euskarria ematen dion informazio-sistema, ziurtagiria ematen den egunean indarrean dagoen aplikagarritasun-deklarazioaren arabera*".

1.3. Definizioak

Honako definizio hauek ematen dira, dokumentu honetan jasotako zibersegurtasun-kontzeptu garrantzitsuak elkarrekin ulertu ahal izateko:

- **CoE**: Center of Excellence. Sail honen helburua negozioari eta azken bezeroari balioa emango dioten produktu digitalak lortzea da.
- **NCE**: Negozio Bezeroak Espainia Iberdrolaren 3 negozio nagusietako bat da.
- **BISO**: Business Information Security Officer. CISOren rola du, baina lehen defentsa-ildokoa, eta BISOren negozioan dago.
- **DBEO:** Datuak Babesteko Erregelamendu Orokorra (DBEO), edo ingelesezko GDPR, Europar Batasunaren erregelamendu bat da, EBren barruan pertsona fisikoen datu pertsonalen tratamendua arautzen duena.

- **ISKS:** Informazioaren segurtasuna kudeatzeko sistema esparru egituratu bat da, informazioaren segurtasuna modu integralean kudeatzeko, kontrolatzeko eta hobetzeko erabiltzen dena.1.4. Dokumentazioa eta erreferentziako kontaktuak

1.4. Dokumentazioa eta erreferentziako kontaktuak

- Segurtasun korporatiboaren politika.
- Zibersegurtasunaren arrisku-politika.
- Datu pertsonalak babesteko politika.
- Erresilientzia Politika Operatiboa.
- CCN-STIC serieak: Kriptologia Zentro Nazionalak (CCN) Segurtasun Eskema Nazionalak eskatutako segurtasun-estandarrak betetzeko garatutako arauak, jarraibideak, gidak eta gomendioak hartu dira erreferentziatzat.
- ISO/IEC 27014.
- ISO/IEC 27001.
- Zibersegurtasunaren gobernu onaren kodea – CNMV.
- Iberdrola Taldearen Zibersegurtasun Esparrua.
- ciberseguridad_negocio_clientes_es@iberdrola.es

2. Informazioaren segurtasuna

Informazioaren segurtasuna babesteko NCEn ezarritako neurriek honako hau ziurtatzea dute ardatz:

- Konfidentzialtasuna: informazioaren jabetza, informazio hori eskuratzeko baimena duten langileek soilik eskuratu dezaketela bermatzen duena.
- Osotasuna: informazioaren jabetza, garraiatutako edo biltegiratutako datuen zehaztasuna bermatzen duena, software- edo hardware-akatsengatik edo ingurumen-baldintzengatik datu horiek ustekabean edo nahita aldatu, galdu edo suntsitu ez direla ziurtatuz.
- Erabilgarritasuna: informazioaren jabetza, erabiltzaileek edo baimendutako prozesuek, hala eskatzen dutenean, informazio hori eskuratu eta erabili ahal izatea bermatzen duena.
- Benetakotasuna: informazioaren propietatea da, eta horren bidez bermatzen da erakunde bat dela esaten duena, edo datuen iturria bermatzen duela.
- Trazabilitatea: informazioaren propietatea, erakunde baten jarduketak erakunde horri bakarrik egotzi dakizkiokeela bermatzen duena.

Halaber, **oinarrizko printzipio** hauek hartzen dira kontuan:

- Segurtasuna prozesu integral gisa.
- Arriskuetan oinarritutako segurtasunaren kudeaketa.

- Prebentzioa, detekzioa, erantzuna eta errekuperazioa.
- Defentsa-lerroak egotea.
- Etengabeko zaintza.
- Aldizkako berrebaluazioa.
- Erantzukizunak bereiztea.

Azkenik, egungo Segurtasun Eskuliburua (Segurtasun Politika) garatzeko, **gutxieneko baldintza hauek** hartzen dira kontuan (araudia osatzen duten dokumentuetan zabaltzen dira):

- Segurtasun-prozesua antolatzea eta ezartzea.
- Arriskuen analisia eta kudeaketa.
- Langileen kudeaketa.
- Profesionaltasuna.
- Sarbideak baimentzea eta kontrolatzea.
- Instalazioak babestea.
- Segurtasun-produktuak erostea eta segurtasun-zerbitzuak kontratatzea.
- Gutxieneko pribilegioa.
- Sistemaren osotasuna eta eguneratzea.
- Biltegiratutako eta iragaitzazko informazioa babestea.
- Prebentzioa elkarri lotutako beste informazio-sistema batzuen aurrean.
- Jarduera erregistratzea eta kode kaltegarria detektatz
- Segurtasun-gorabeherak.
- Jardueraren jarraitutasuna.
- Segurtasun-prozesua etengabe hobetzea.

2.1. Erakundearen misioa, ikuspegia eta testuingurua

Taldearen Misioa bere jarduera guztien garapenean modu jasangarrian balioa sortzean oinarritzen da, bere akziodun, langile, bezero eta gainerako interes-taldeentzat eta, oro har, herritarrentzat eta gizarte osoarentzat. Misioa Ikuskerarekin osatzen da, zeinak energia-sektorean talde multinazional liderra izateko nahia islatzen baitu, etorkizun hobea protagonizatuko duena, modu jasangarrian eta pertsonentzako kalitatezko zerbitzu batekin, modu eraginkorrean, seguruan, jasangarrian eta ingurumena errespetatuz. Taldearen Misioa eta Ikuskera Balio batzuekiko konpromiso irmoan oinarritzen dira, eta horien artean bultzada dinamizatzailea, indar integratzailea eta energia jasangarria nabarmentzen dira Azken balio horretan, segurtasuna funtsezko zutabea da. Azken balio horretan, Segurtasuna funtsezko zutabea da balio horiek lortzeko. Horren ondorioz, segurtasun integrala funtsezko zutabe gisa finkatu da Iberdrolak erabakiak hartzeko orduan, eta segurtasun-jardunbide berritzaileak

eta jasangarriak sustatu dira etengabe eragiketa guztietan. Horrela, taldearen erresilientzia, fidagarritasuna eta arrakasta globala lortzen lagundu da, etengabe eraldatzen ari den ingurune hibrido batean.

Negozio Clientes España Iberdrola SAren (aurrerantzean, Iberdrola edo erakundea) estrategia enpresarialaren barruan leku nabarmena du, bere negozio-lerro nagusietako bat baita. Ildo horren ardatza da energia merkaturatzea eta hornitzea, bai eta deskarbonizazioan oinarritutako produktuak eta zerbitzuak hornitzea ere.

Espainiako Bezero Negozioaren eremuan, Iberdrolak azken erabiltzailearen beharrak asetzen ditu, eta energia-irtenbide jasangarriak eskaintzen ditu. Helburua da energia garbia eta zerbitzu berritzaileak ematea, ingurumena gehiago errespetatzen duen energia-eredu bateranzko trantsizioan laguntzeko. Gainera, negozio-ildo horren barruan, Iberdrolak funtsezko zeregina betetzen du handizkako merkatuetako energia-salerosketan, eta, horrela, energia-merkatuan duen posizioa sendotzen du.

Espainiako Negozio Bezeroarekin batera, Iberdrolak beste negozio-lerro garrantzitsu batzuk garatzen ditu. Horien artean, Talde Sareen Negozioa dago. Negozio horrek azpiegitura elektrikoak eraikitzen, erabiltzen eta mantentzen ditu, hala nola transmisio-lineak, azpiestazioak eta transformazio-zentroak. Azpiegitura horiek funtsezkoak dira ekoizpen-zentroetatik azken erabiltzailearengana energia elektrikoaren hornidura eraginkorra bermatzeko.

Era berean, Iberdrola aktiboki inplikatzen da Negozio Berriztagarri Taldean, non iturri berriztagarrietatik energia elektrikoa sortzen espezializatzen baita, hala nola energia eolikoa, eguzki-termoa eta fotovoltaikoa, besteak beste. Negozio-ildo horrek islatzen du Iberdrolak energia garbia eta jasangarria sortzeko duen konpromisoa, klima-aldaketa arintzen eta ingurumena zaintzen laguntzeko.

Konpainiaren asmo korporatiboa gehiago zehazteko, argitaratutako baliabideak kontsulta daitezke: Hacia un propósito corporativo global - Iberdrola

2.2. Helburuak

Era berean, informazioaren segurtasunaren 6 helburuak identifikatzen dira, Segurtasun Korporatiboaren Politikan ezarritako oinarrizko jarduketa-printzipioak kontuan hartuta:

- Gobernua: Informazioaren segurtasuna kudeatzeko eta jarduteko gobernu-eredu bat ezartzea eta mantentzea, arriskuaren kudeaketara bideratutako ikuspegi baten bidez.
- Identifikazioa: Ingurunea ulertzea eta haren sistemetarako, aktiboetarako, datuetarako eta gaitasunetarako arriskuak identifikatzea.
- Babesa: Ziberamenaza posible bat gauzatzearekin lotutako arrisku-maila minimizatzeko babesak diseinatzea eta ezartzea.
- Detekzioa: Erakundearen informazio-gertaerak monitorizatzea eta balizko ziber mehatxu bat gauzatzea ekar dezaketen portaera anomaloak identifikatzea.
- Erantzuna: Erantzuna Ekintza egoki guztiak egitea identifikatutako gorabeherak kudeatzeko, aztertzeko, erantzuteko, mailakatzeko eta arintzeko.
- Berreskuratzea: Zibersegurtasun-gorabehera batek eragindako aktiboak eta eragiketak lehengoratzea.

2.3. Zibersegurtasunaren antolamendua

Iberdrola Kudeaketa Sistemaren segurtasuna kontrolatzeko eta bermatzeko moduan antolatzen da, informazioaren segurtasunaren arloko rolak eta erantzukizunak esleituz, komunikatuz eta koordinatuz, Kudeaketa Sistemak informazioaren segurtasunaren arloan eskatutako baldintzak betetzen dituela bermatzeko.

2.3.1. Zibersegurtasun Global Iberdrolaren defentsa-lerro hirukoitza

Iberdrolaren eta taldeko sozietateen barne-kontroleko sistema nazioarteko jardunbide onenak erreferentziatzat hartuta eratzen da. Horregatik, kontrol-sistema hori hiru defentsa-lerroren inguruko aseguramendu konbinatuan oinarritzen da, eta ikuspegi integratua ematen du erakundeko alderdiek modu eraginkor eta koordinatuan nola jarduten duten ikusteko, erakundearen arrisku garrantzitsuen kudeaketa- eta barne-kontroleko prozesuak eraginkorrago eginez.

Jarraian, xehetasun gehiago ematen dira defentsa-lerro bakoitzari buruz:

- Lehen defentsa-lerroa: arriskuen jabe diren funtzio guztiak biltzen ditu. Ildo horretan, lehen lerroek Business Information Security Officer (BISOs) izendatuko dute. Negozio-erakundeek zibersegurtasun-plan espezifiko baten definizioa gidatuko dute, eta haren ezarpena gainbegiratuko dute, zibersegurtasuneko estrategiarekin, arauekin eta esparru orokorrekin bat etorriz, eta zibersegurtasunaren arloko baliabide (pertsona eta aurrekontu) egokiek eusten dietela ziurtatuko du. Ildo horretan daude TAS (IT), negozioak eta arlo korporatiboak.
- Bigarren defentsa-lerroa: barnean hartzen ditu zibersegurtasunaren gobernuaren eta kontrolaren esparru orokorra definitzen duten funtzioak, arau, estandar eta irizpide globalak ezartzen dituztenak eta lehen lerroko zibersegurtasun-planen ezarpena babesten eta gainbegiratzen dutenak, bai eta arrisku garrantzitsuak identifikatzen dituztenak ere. Ildo horretan daude arrisku korporatiboak, segurtasun eta erresilientzia korporatiboa eta zibersegurtasuna.
- Hirugarren defentsa-ildoa: independentzia- eta objektibotasun-maila handiena ematen du gobernu korporatiboaren, arriskuen kudeaketaren eta barne-kontrolen eraginkortasuna bermatzeko, eta barne hartzen du lehen eta bigarren defentsa-lerroek arriskuak kudeatzeko eta kontrolatzeko helburuak lortzeko modua. Ildo horretan daude Barne Auditoretzako saila, Kanpo Auditoretzak eta Auditoretza Arautzaileak.

2.3.2. NCEkoInformazioaren Segurtasunerako Batzordea (1. defentsa-lerroa)

NCEren Informazioaren Segurtasun Batzordea zibersegurtasunaren gobernu-organo gorena da, eta goi-zuzendaritzak (eta zerbitzu- eta informazio-arduradunek) laguntzen diote. Segurtasun-arduradunak (BISO) zuzentzen du, eta zibersegurtasun-arriskuak kudeatzeko estrategia ezartzeaz eta gainbegiratzeaz arduratzen da. Gutxienez urtean bitan biltzen da.

Sistema Orokorraren Batzordearen eginkizunak erakundearen Kudeaketa Sistemaren araudian jasota daude, baina honako hauek nabarmentzen dira, besteak beste:

- Erakundearen bilakaera-**estrategia berrikustea eta onartzea**, **informazioaren segurtasunari** dagokionez.
- Negozio **Zuzendaritzaren** eta batzordera gonbidatzen diren sailen **kezkei erantzutea**.
- **Goi-zuzendaritzari informazioaren segurtasunaren egoeraren berri aldizka emateko foroa** izatea.
- Urtero ISO 27001 eta ENS arauek eskatzen duten **zuzendaritzaren berrikuspen-bilera egitea.**
- **Zibersegurtasuneko gobernu-eredua berrikustea eta berrestea**, bai eta aldian behin izan ditzakeen aldaketak ere. Era berean, **zibersegurtasunaren arloko erantzukizun-gatazkak ebaztea.**
- Erakundearen zibersegurtasuneko aldizkako **arriskuen analisien emaitzak monitorizatzea eta onartzea**.
- **Aldizka berrikustea eta berrestea Informazioaren Segurtasun Politika** (dokumentu hau) eta araudia osatzen duten dokumentuak.
- Aplikatu beharreko **lege-** eta sektore-**araudia betetzen dela zaintzea**.
- **Aldizkako auditoretzak egin daitezen sustatzea.**
- Zibersegurtasunaren arloko **komunikazioa, ahaleginen koordinazioa eta kontzientziazioa sustatzea**.
- IKT **proiektuetan** informazioaren **segurtasuna kontuan hartzen dela zaintzea**.
- **Segurtasun-gorabeherak** kudeatzeko prozesuen jarduna **monitorizatzea**.
- **Erakundearen informazioaren segurtasuna hobetzeko planak onartzea, etengabeko hobekuntza lortzeko.**
- Segurtasunaren arloko **jarduketak lehenestea**.
- Informazioaren segurtasuna kudeatzeko sistemaren **etengabeko hobekuntza sustatzea**.

2.3.3. Defentsaren 1. lerroko zibersegurtasuneko rolak eta erantzukizunak

Goi-zuzendaritza

- Informazioaren Segurtasuna Kudeatzeko Sistema (ISKS) planifikatzeko, ezartzeko, berrikusteko eta hobetzeko **behar diren baliabideak hornitzea** eta bermatzea, eta zibersegurtasuneko aurrekontuak onartzea.
- Informazioaren segurtasunari dagozkion roletarako **erantzukizunak** EZEren barruan **esleitzen eta jakinarazten direla ziurtatzea**.
- ISKSk informazioaren segurtasunaren arloko **helburuak eta emaitzak lortzen dituela** eta segurtasun-politika betetzen dela **ziurtatzea**.
- **Zibersegurtasun-arriskuak kudeatzeko neurriak aplikatzea eta horien ezarpen eraginkorra gainbegiratzea**. Horretarako, arriskuak onartzeko irizpide guztien eta dagozkien mailen berri izan behar dute, eta arriskuak eta salbuespenak kudeatzeko barne-prozeduretan definitutako guztia bete behar dute.
- Langile guztientzako **zibersegurtasun-arloko prestakuntzak aldizka antolatzen direla ziurtatzea**.
- Zuzendaritzaren berrikuspen-batzordean (**Espainiako Bezero Negozioen Zibersegurtasun Batzordea**) **parte hartzea eta lan hori sustatzea**.
- Aplikatzekoa den lege- eta sektore-araudia betetzen dela zaintzeaz arduratzen da.
- ISKSren aldizkako berrikuspen egokirako beharrezkoak diren **barne- eta kanpo-auditoretzak egiten direla bermatzea**.
- Espainiako Bezero Negozioaren **zibersegurtasun-batzordeko parte-hartzaile gisa dagozkion funtzio guztiak egitea**.
- Zibersegurtasunaren **etengabeko hobekuntza sustatzea.**

Informazioaren eta Zerbitzuaren arduraduna

- **Informazioaren eta zerbitzuaren betekizunak onartzea**, bere jarduera- eta eskumen-eremuaren barruan.
- **Informazioaren eta zerbitzuaren segurtasun-mailak zehaztea**, informazioaren segurtasunari eragiten dioten gorabeheren inpaktuak baloratuz. Horretarako, informazioaren eta zerbitzuaren arduradunak txostena eskatuko dio segurtasunaren arduradunari. Segurtasun-mailak finkatzeko jarraitutako irizpideak horretarako definitutako CCN-CERT gidan eta Iberdrolaren barne-dokumentazioan etorriko dira.
- Beren ardurapeko aktiboen **arriskuen nahitaezko analisiak egiten eta behar dituen zaintzak hautatzen laguntzea** (Segurtasuneko arduradunaren eta Sistemaren arduradunaren parte-hartzearekin).
- Bere ardurapeko informazioari eta zerbitzuei (edo zerbitzu aktiboei) dagokienez, **arriskuen analisian kalkulatutako hondar-arriskuak onartzeko** arduraduna.
- **Informazioa erabiltzeaz** eta, beraz, babesteaz **arduratzen da**. Horretarako, segurtasun-arduradunaren, sistemaren arduradunaren eta CoE-ko zibersegurtasun-arduradunaren laguntza izango du.
- **Aktiboen gainean beharrezkoak diren neurriak ezartzen direla ziurtatzea,** haien gaineko segurtasun-intzidenteak eragin ditzaketen **elementu kaltegarriak minimizatzen saiatzeko.** Horretarako, segurtasun-arduradunaren, CoE-ko zibersegurtasun-arduradunaren eta zibersegurtasun-taldearen laguntza izango du.
- **Zerbitzuaren bizi-zikloko segurtasun-zehaztapenak** (eta hura osatzen duten sistemak) eta dagozkien kontrol-prozedurak **jasotzen direla ziurtatzea**. Horretarako,

segurtasun-arduradunaren, CoE-ko zibersegurtasun-arduradunaren eta zibersegurtasun-taldearen laguntza izango du.
- Prestakuntza- eta kontzientziazio-planean esleitzen zaizkion **zibersegurtasuneko prestakuntza-zereginak betetzea**.

Segurtasun-arduraduna (BISO eta NCEko ISKSko arduraduna):

NCEko zibersegurtasuneko arduradun nagusia; informazioaren eta zerbitzuen segurtasun-eskakizunak betetzeko erabakiak hartzeko ardura izango du. Goi Zuzendaritzari jakinarazi behar dio.

- Informazioaren segurtasuna kudeatzeko sistemaren (ISKS) arduraduna den aldetik, **informazioaren segurtasuna kudeatzeko sistemaren plangintza, ezarpena, eragiketa, mantentzea, gainbegiratzea eta etengabeko hobekuntza gidatzeko arduraduna da**.
- **Erabilitako informazioaren eta informazio-sistemek beren erantzukizun-eremuan emandako zerbitzuen segurtasunari eustea**, erakundearen Informazioaren Segurtasun Politikan ezarritakoaren arabera.
- NCE mailako informazioaren segurtasun-**helburuak** eta horiek betetzeko eta onartzeko behar diren baliabideak **definitzea**. Era berean, helburu horiek betetzen direla gainbegiratzeaz arduratuko da.
- **Zuzendaritzak ISKSren ezarpenean, mantentze-lanetan eta etengabeko hobekuntzan parte har dezan sustatzea.** Era berean, ISKSren egoerari eta betetze-mailari buruzko aldizkako txostena Zuzendaritzari helaraztea.
- **Segurtasun-estrategia eta -politikak egitea eta goi-zuzendaritzari aurkeztea**, onar ditzan. Segurtasun-politika horietan, zibersegurtasun-arriskuak kudeatzeko neurriak jaso beharko dira, bai eta erabilitako informazio-sare eta -sistemen segurtasunerako planteatzen diren arriskuak kudeatzeko eta erakundeari eta zerbitzuei eragiten dieten zibergorabeheren ondorioak prebenitzeko eta ahalik eta gehien murrizteko neurriak ere.
- NCEren **zibersegurtasuneko gobernu-eredua diseinatzea eta ezartzea.**
- **NCE** (geografia zehatza) **ordezkatzea zibersegurtasuneko lantaldeetan** (arriskuak, kultura, etab.), Espainian eta Globalean, Iberdrolaren barruan.
- **Zibersegurtasun-saila** eta **sail horretako** giza **baliabide guztiak gidatzea**.
- NCEko **zibersegurtasun-sailerako izendatutako baliabide ekonomikoak kudeatzea**, eta eskuragarri dauden baliabideen arabera lehenestea planak.
- **Arriskuak kudeatzeko estrategia gainbegiratzea.**
- **Goi-zuzendaritzaren NCE arloko zibersegurtasunaren egoeraren berri ematea eta jakinaraztea.**
- **Araudiaren aplikazioa gainbegiratzea eta garatzea.** Era berean, aplikatu beharreko sistemetan eta zerbitzuetan aldizkako segurtasun-kontrolen ezarpena ebaluatzea eta koordinatzea.
- Markatutako onarpen-fluxuen arabera dagozkion **dokumentuak onartzea**.
- Informazio-sareen eta -sistemen segurtasunaren arloan aplikatu beharreko **araudia betetzen dela gainbegiratzea**, eta araudi hori betetzen dela bermatzeko behar diren neurri guztiak hartzea.
- ISKSren **auditoria-prozesuak gidatzea.**
- Informazio-sare eta -sistemen **segurtasuneko jardunbide egokien eta estandarren trebatzaile gisa** jardutea.

- Sistemen edo aktiboen **aplikagarritasunari buruzko dokumentua** egitea eta sinatzea.
- **Kontrol-agintaritzei bidaltzea**, erreferentziazko CSIRT nazionalen bidez, bidegabeko atzerapenik gabe, zerbitzuak ematean ondorio nahasgarriak dituzten **gorabeheren** eta hautemandako ahulezien **jakinarazpenak**.
- **Informazioa edo dokumentazioa biltzea, prestatzea eta kontrol-agintaritzari eta erreferentziazko CSIRT nazional nazionalei ematea**.
- **Kontrol-agintaritzaren jarraibideak eta gidak jasotzea, interpretatzea eta gainbegiratzea, bai ohiko jardunbiderako**, bai ikusitako akatsak konpontzeko.
- **Kanpoko enpresek eta hornitzaileek erakundeak** ezarritako informazioaren segurtasun-irizpideak **betetzen dituztela zaintzea**.
- NCE gorabeherei erantzuteko plana definitzea eta onartzea. Era berean, zibersegurtasun-gorabeherak kudeatzeaz eta gidatzeaz arduratuko da, gorabeheren kudeaketa gobernatzen duten dokumentuek ezarritako erantzukizunen arabera.

Segurtasun-arduraduna **ez dago hierarkikoki sistemen arduradunaren mende.**

CoE (Center of Excelence) zibersegurtasuneko arduraduna

CoEren aktiboen zibersegurtasuna kudeatzeaz arduratzen da, NCEren **Informazioaren Segurtasuneko arduradunarekin (BISO) lankidetza estuan** segurtasunaren arloan, eta CoEren zibersegurtasunaren etengabeko hobekuntza ziurtatzen du. Erakundearen Kudeaketa Sistemaren arau-multzoan daude jasota haren funtzioen xehetasunak.

Sistemen arduraduna

Erantzukizun nagusien artean, honako hauek nabarmentzen dira:

- **Informazio-sistemaren garapena, operazioa eta mantentze-lanak kudeatzea** eta/edo **gainbegiratzea** haren bizi-ziklo osoan. Eragiketa sistema korporatiboen erantzukizun zuzena da azpiegituran hedatutako aktiboentzat.
- **Segurtasun-arduradunak** (eta CoE-ko zibersegurtasun-arduradunak) **definitutako sisteman segurtasunaren ezarpena kudeatzeko modu zehatza garatzeaz** eta haren **eguneroko eragiketa gainbegiratzeaz arduratzen da**. **Administratzaileek, operadoreek edo sistema korporatiboek egin ahal izango dute** (espezifikazioak, instalazioa eta funtzionamendu egokiaren egiaztapena barne).
- **Informazio-sistemaren topologia eta kudeaketa definitzea**, erabilera-irizpideak eta eskuragarri dauden zerbitzuak ezarriz.
- **Bere ardurapeko aktiboen gaineko ahuleziak eta mehatxuak identifikatzea gainbegiratu eta ziurtatzea.** Horretarako, zibersegurtasun-taldean oinarrituko da.
- **Segurtasun-neurriak** segurtasun-esparru orokorrean **behar bezala txertatzen direla ziurtatzea** (zibersegurtasun-sailean oinarrituta).
- Neurri zuzentzaile egokiak **hartzea**, segurtasun-ebaluazio eta -auditoretzen arabera.
- **Informazioaren bat, zerbitzuren bat edo sistema osoa bertan behera uztea proposatzea, zuhurtzat jotzen duen denboran** eta **ezarritako baldintzak betetzeari eragin diezaioketen segurtasun-akats larriak hautemanez gero**, agindutako aldaketak bete arte. Horretarako, zibersegurtasun-taldea lagun daiteke. Azken erabakia erakundeko zuzendaritzak hartuko du, eta ukitutako informazioaren eta zerbitzuen arduradunarekin eta segurtasunaren arduradunarekin adostu beharko da.
- Prestakuntza- eta kontzientziazio-planean esleitzen zaizkion **zibersegurtasuneko prestakuntza-zereginetan laguntzea**.

Zibersegurtasuneko teknikaria

Zibersegurtasuneko teknikariaren (zibersegurtasun-taldeko kide izango da) ardura nagusiak dira **segurtasun-arduradunak** (BISO) **eta/edo CoE-ko zibersegurtasun-arduradunak esleitzen dizkioten zibersegurtasun-zeregin guztietan laguntzea**.

Aktiboaren/lotutako arriskuaren jabea

- **Aktiboari dagokion informazio garrantzitsu** guztia **ezagutzea.**
- **Aktiboa** behar bezala **inbentariatuta,** sailkatuta eta babestuta dagoela **ziurtatzea.**
- **Aktibo garrantzitsuak sartzeko eta sailkatzeko murrizketak definitzea eta aldian behin berrikustea**, sarbide-kontroleko politika aplikagarriak kontuan hartuta.
- Aktiboen egoera gainbegiratzea.

- **Esleitutako informazioaren segurtasunaren arriskuak ezagutzea.**
- Informazioaren segurtasunaren **arriskuak tratatzeko plana onartzea.**
- Informazioaren **segurtasunaren hondar-arriskuak onartzea.**
- **Arriskuen egoera gainbegiratzea.**
- **Sortzen ari diren mehatxuei eta arriskuei buruz eguneratuta egotea;** horretarako, Informazioaren Segurtasuneko arduradunaren (BISO) eta zibersegurtasun-sail osoaren laguntza jaso ahal izango da.

Espainiako negozio-bezero enplegatuak

Langileen zibersegurtasun-arloko funtzioak eta erantzukizunak erakundearen kudeaketa-sistemaren arau-multzoan jasota daude.

NCEren zibersegurtasunaren gobernu-eredua osatzen duten gainerako elementuak (organigrama, RASCI matrizea, komunikazio-fluxuak, rolen izendapena eta errebokatzea, etab.) ISKSren arau-multzoan definituta daude.

2.4. Arau-esparrua

- **Datuen pribatutasuna**
  - 3/2018 Lege Organikoa, abenduaren 5ekoa, Datu Pertsonalak Babestekoa.
  - 2016/679 (EB) ERREGELAMENDUA, EUROPAKO PARLAMENTUARENA ETA KONTSEILUARENA, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzkoa.

- **Estatuko beste lege batzuk**
  - Zibersegurtasunaren koordinazioari eta gobernantzari buruzko Legea, 2025ekoa.
  - 2022/2555 (EB) Zuzentaraua, Europako Parlamentuarena eta Kontseiluarena, 2022ko abenduaren 14koa, Batasun osoan zibersegurtasun-maila komun handia bermatzeko neurriei buruzkoa.
  - 1/1996 Legegintzako Errege Dekretua, apirilaren 12koa, Jabetza Intelektualaren Legearen testu bategina onartzen duena.
  - 34/2002 Legea, uztailaren 11koa, informazioaren gizarteko zerbitzuei eta merkataritza elektronikoari buruzkoa.
  - 59/2003 Legea, abenduaren 19koa, sinadura elektronikoari buruzkoa.
  - Prozedura Kriminalaren Legea onartzen duen Errege Dekretua.
  - 10/2021 Legea, uztailaren 9koa, Urrutiko Lanarena.
  - Kode Zibila eta Zigor Kodea.

- **Nazioarteko beste legeria edo araudi bat**
  - PCI – DSS araudia, 2024ko ekainekoa
  - Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resiliencia ence of critical entities (CER).
  - AA Act.

- **Segurtasun Eskema Nazionala**
  - 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasun Eskema Nazionala arautzen duena.
  - CCN-STIC gidak.
  - Segurtasun Jarraibide Teknikoak, Segurtasun Eskema Nazionalaren araberakoak (2016ko urriaren 13ko Ebazpena, Administrazio Publikoen Estatu Idazkaritzarena) eta Informazio Sistemen Segurtasunaren Auditoretzakoak (2018ko martxoaren 27ko Ebazpena, Funtzio Publikoaren Estatu Idazkaritzarena).

- **UNE-ISO/IEC 27001**
  - UNE-ISO/IEC 27001:2023 Informazioaren segurtasuna kudeatzeko sistemetarako zehaztapenak.
  - UNE-ISO/IEC 27002:2023 Informazioaren segurtasuna kudeatzeko jardunbide egokien kodea.

2.5. Kontzientziazioa eta prestakuntza

Informazioarekin, zerbitzuekin eta informazio-sistemekin lotutako langile guztiei prestakuntza eta informazioa eman beharko zaie informazioaren segurtasunaren arloan dituzten betebeharrei buruz, informazioaren segurtasunaren arloko politika hau ezartzeko eta haren jarraipena egiteko.

NCE sistemei eta zerbitzuei aplika dakizkiekeen informazio-teknologien segurtasuna bermatzeko, behar diren mekanismoak antolatuko dira NCEren erakundeko maila guztietan beharrezkoa eta ezinbestekoa den kontzientziazioa eta prestakuntza orokorra eta espezifikoa praktikan jartzeko.

2.6. Hondakinen kudeaketa

NCEk identifikatu eta, hala dagokionean, ebaluatu eta kategorizatu egiten ditu jardueren, prozesuen eta zerbitzuen berezko arriskuak eta aukerak, horiek tratatzeko beharrezkoak diren ekintzak planifikatuz, nahi ez diren ondorioak prebenituz eta horien ondorio onuragarriak indartuz.

Informazioaren segurtasunaren arriskuak hautemateko eta tratatzeko prozesuak NCEren dokumentu korporatiboetan daude dokumentatuta.

Datu pertsonalen tratamenduaren ondoriozko arriskuei dagokienez, datuen babesaren kudeaketa arautzen duten dokumentu guztiak beteko dira.

2.7. Dokumentua berrikustea eta onestea

Informazioaren segurtasunari buruzko eskuliburu hau (ENSren eta ISO 27001 arauaren irismenerako Informazioaren Segurtasun Politika egiten duena) formalki onartu zuen NCEko CEOk, eta aginduzkoa da NCEren antolaketari dagokionez. Berrikusketa-prozesu erregular baten mende egongo da, inguruabar tekniko edo antolamenduzko berrietara egokitzeko eta zaharkituta gera ez dadin. Gutxienez urtean behin berrikusiko da, politikak ezartzen duena etengabe egokia, egokia, osoa eta zehatza dela ziurtatzeko, eta goi-zuzendaritzak formalki onar dezan.

Era berean, NCEk barne-dokumentazioa du, araudia gobernatzeko ildo nagusiak zehazten dituena.