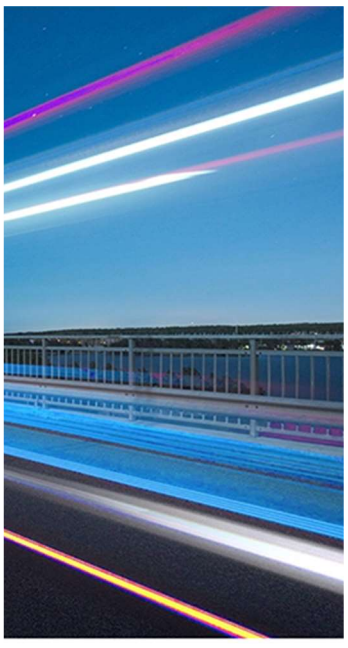
ZIBERSEGURTASUN POLITIKA

TRANSPORT SYSTEMS
TRAINS
BUSES
SIGNALLING
COMPONENTS
SERVICES

Your Way
to Future Mobility

Konpainiak helburu informatiboekin soilik ematen du hurrengo euskarazko itzulpena, Konpainiaren webgunean eskuragarri dagoen jatorrizko dokumentu ofizialean oinarrituta. Euskarazko bertsioaren eta gaztelerazko dokumentuaren artean desadostasunik egonez gero, azken hori gailenduko da.

AURKIBIDEA



1. SARRERA ETA XEDEA

CONSTRUCCIONES Y AUXILIAR DE FERROCARRILES, S.A.-ko Administrazio Kontseiluak, eskuorde ezin daitezkeen eginkizunak betez, Sozietatearen eta bere Taldearen estrategia orokorrak definitzeko (aurrerantzean «CAF» edo «Taldea») eta sustatutako arau-garapenak kontuan hartuta. Europar Batasunak eta gure herrialdean duen proiekzioa, bai eta gainbegiratze agintariek eta prestigio aitortua duten erakundeek ezarritako gomendio, praktika eta estandarrak ere, 2024ko urriaren 10eko saioan onartu ditu, Zibersegurtasun Politika hau ("Politika"), informazioaren segurtasunari eta zibersegurtasunari buruzko oinarrizko printzipioak eta konpromisoak ezartzen dituena.

Taldearen Jokabide Kodean, oro har, aurreikusitakoaren arabera, eta Jasangarritasun Politikan eta Arriskuak Kontrolatzeko eta Kudeatzeko Politika Orokorrean xedatutakoa kontuan hartuta, politika honetan ezarritako oinarrizko printzipioei esker, Taldeak zibersegurtasuneko estrategiak, prozedurak eta estandarrak erabili ahal izango ditu, negozio-helburuekin bat, CAFen datuak, sistemak eta eragiketak babesteko. Gainera, Taldeak erabiltzaileentzat, bezeroentzat eta beste interes-talde batzuentzat konfiantzazko produktuak eta zerbitzuak eskaintzeko prozesuak eta teknologiak zabaldu nahi ditu Politikak.

2. IRISMENA

Politika hau CAF osatzen duten erakunde guztiei aplikatu behar zaie, eta nahitaez bete behar dute.

Politika hau CAFeko erakunde bateko langileei, akziodunei, zuzendari edo administrazio-organo bateko kide guztiei aplikatzen zaie, haien kargua edo kokapen geografikoa edozein dela ere.

Halaber, CAFekin harreman komertzialen bat duten balio-kateko hirugarrenei (negozio-bazkideei) aplikatu behar zaie politika hau, bereziki, proiektu-bazkideei, eragileei, hornitzaileei eta bezeroei.

Negozio-bazkideen tipologien eskakizun zehatzak definitzeko, faktore objektiboak hartuko dira kontuan: Hala nola, CAFek eragiketa-kontrola izatea, hirugarrenean eragiteko gaitasun erabakigarria izatea, edo nazioarteko jardunbide egokien gida nagusietan aitortutako antzeko irizpideak. CAFek eragiketa-kontrol hori bere gain hartzen ez badu, edo eragin nabarmenik ez badu, arrazoizko neurriak eta arriskuarekiko proportzionalak hartuko dira, besteak beste, negozio-bazkideak politika honen arloan dituen politika baliokideak aztertzea, -politika horrekin bateragarritasuna eta lerrokatzea bermatzeko-, edo hirugarrenek CAFen jokabide-kode orokorraren printzipio orokorrak errespetatzen dituztela ziurtatzeko eraginkorrak izan daitezkeen beste edozein neurri.

Kontrola ziurtatzeko behar adinako parte-hartzerik ez dutelako CAFenak ez diren partaidetzako sozietateei dagokienez, haien jardun-printzipioak politika honetan ezarritakoarekin koherenteak izatea bultzatuko da, betiere kasu bakoitzean aplikatu beharreko legeria errespetatuz.

3. ZIBERSEGURTASUNAREN ARLOKO OINARRIZKO PRINTZIPIOAK ETA KONPROMISOAK

Konpromisoak martxan jartzeko, CAFek zibersegurtasunari buruzko politika honetako oinarrizko printzipioei jarraituko die: segurtasuna, konfidentzialtasuna, osotasuna, erabilgarritasuna, benetakotasuna eta informazioaren trazabilitatea.

Zentzu horretan:

- Konfidentzialtasunak bermatzen du informazioa eskuratzeko baimena duten erabiltzaileek bakarrik eskuratu ahal izango dutela, eta ezin izango zaiela hirugarrenei zabaldu baimenik gabe.
- Osotasunak ziurtatzen du datuak baimendu gabeko aldaketarik gabe mantenduko direla eta baimendu gabeko pertsonek edo prozesuek ez dutela aldatu dagoen informazioa.
- Eskuragarritasunak informazioa eta informazio-sistemak baimendutako erabiltzaileek eskatzen dutenean eskuragarri eta erabilgarri egotea bermatzen du.
- Egiazkotasuna informazioaren jatorria eta harekin lotutako identitateak haren atributuetan benetan agertzen direla bermatzeko gaitasuna da. Horri lotuta dago arbuiorik ezaren printzipioa. Horren arabera, erabiltzaileak ezin du ukatu sistemako egintza baten egiletza edo datu edo datu-multzo batekiko lotura.
- Trazabilitateak bermatzen du une oro informazioa eskuratzen dutenen identitatea eta horrekin lotuta garatzen duten jarduera zehazteko aukera, baita informazioak jarraitu dituen egoerak eta bideak ere.

Oinarri horien gainean, politika honek konpromiso hauei erantzuten die:

1. konpromisoa: Zibersegurtasunaren kudeaketa etengabe bultzatzea eta hobetzea, lege- eta kontratu-betebeharrak betetzeko aukera izan dezagun, segurtasun-jardunbide egokiak eta erakundearen baliabideen erabilera etikoa txertatuz, gure bezeroen eta gainerako interes-taldeen beharrak eta espektatibak betez.

Zibersegurtasunaren kudeaketatzat jotzen da zibersegurtasun-arriskuak eraginkortasunez kudeatzeko jardueren, kontrolen eta neurri teknikoen eta antolaketa-neurrien multzoa, sistema horietan biltegiratutako informazio-sistemen, sareen eta informazioaren segurtasun integrala bermatzen dutenak; gorabeherei aurrea hartzea, antzematea, erantzutea eta haiek berreskuratzea barnean hartuta.

Konpromiso hau lege- eta kontratu-betebeharrak betetzera, segurtasun-jardunbide egokiak betetzera eta erakundearen baliabideak etikoki erabiltzera hedatzen da, bezeroen eta gainerako interes-taldeen beharrak eta espektatibak betez.

CAFen zibersegurtasuna kudeatzeko eredua onartutako erreferenteetan eta estandarretan oinarritzen da, bai eta araudi nazionaletan eta nazioartekoetan ere. Horrek aukera ematen du bai kontrolak eta neurriak hedatzeko, bai esparru bakoitzari egokitutako arriskuen kudeaketa egiteko, kontuan hartuta gaur egungo ingurunea eta mehatxuak, bai negozioen garapenean sortzen direnak eta arau-eskakizun berrien ondorioz sortzen direnak.

Nolanahi ere, etengabe gainbegiratu eta monitorizatuko da, ereduaren eraginkortasuna eta etengabeko hobekuntza bermatzeko.

2. konpromisoa Gure pertsonen eta kanpoko kolaboratzaileen artean zibersegurtasun-kultura sustatzea, eta helburuak lortzeko inplikatzea.

Pertsonen zibersegurtasun-kulturak hau eskatzen du:

Zibersegurtasuneko politikak, arauak eta prozedurak ezartzea, hedatzea, mantentzea eta jakinaraztea, funtsezkoak baitira arlo horretako printzipioak, helburuak eta erantzukizunak zehazteko.

Elementu horiek jarraibide argiak ematen dituzte teknologia erabiltzeko, datuak kudeatzeko eta gorabeherei erantzuteko. Hala, zibersegurtasuna erakundearen eremu guztietan integratzea sustatzen da, eta diseinu bidezko zibersegurtasuna ezartzen da, aurrerago definituko den bezala, gure jardueren oinarri gisa. Gainera, funtsezkoa da erakunde osoa zibersegurtasunean gaitzen duten prestakuntza-planak definitzea, eta plan horiek erakundearen jarduera- eta erantzukizun-arloetara egokitzea. Hori osatzeko, ezinbestekoa da zibersegurtasunaren arloko kontzientziazioa. Horretarako, erakundeko pertsona guztiak zibersegurtasun-arriskuei, egungo mehatxuei eta gorabeherak prebenitzeko jardunbide egokiei buruz hezi eta sentsibilizatu behar dira.

Bestalde, jardunbide egokiak betetzen direla gainbegiratzeko, akordio argiak egin behar dira espero diren segurtasun-estandarrei buruz, ezarritako kontrolen aldizkako ebaluazioak egin behar dira, eta zibersegurtasuneko jarduna etengabe monitorizatu behar da. Testuinguru horretan, funtsezkoa da negozio-bazkideekin komunikazio erraza eta gardena izatea, edozein ahultasun-egoerari edo segurtasun-gorabeherari azkar eta eraginkortasunez aurre egiteko. Osagai horiek guztiak integratzeak zibersegurtasun sendo eta eraginkorra bermatzen du, erakundea balizko mehatxuetatik babestuz eta bere eragiketen jarraitutasuna bermatuz.

3. konpromisoa: Pertsonak babesteaz arduratzea, gure produktu eta zerbitzuekin lotutako istripu eta gertakarien aurrean.

Pertsonak gure produktu eta zerbitzu digitalekin lotutako edozein kalte edo gorabeheretatik babesteko betebeharra ezartzen da. Horrek esan nahi du diseinu bidezko zibersegurtasuna ezarri behar dela, hau da, produktuak eta zerbitzuak diseinatu, garatu eta hornitu behar direla segurtasun-neurri sendoekin, bezeroen beharrekin, araudiekin eta mehatxuekin lerrokatuta, eta zibersegurtasuna garapenen bizi-ziklo osoan integratuta. Prozesu osoan zehar ahultasunak identifikatu eta zuzentzea da helburua. Horrez gain, CAFek eragiketa- eta mantentze-faseetara hedatzen du ahulezien kudeaketa eta gorabeheren monitorizazioa, pertsonak babestuz eta gerta litezkeen gorabeherei lotutako arriskuak murriztuz.

4. konpromisoa: Zero tolerantziako irizpide bat hartzea zibersegurtasunaren kalterako diren ekintza edo jarreren aurrean, eta, interes kontrajarrien artean gatazkarik egonez gero, segurtasunari lehentasuna ematea.

Zero tolerantziako politika ezartzen da sistemen eta datuen zibersegurtasuna arriskuan jar dezakeen edozein ekintza edo jarreraren aurrean. Horrek esan nahi du arriskuak arindu eta kudeatu behar direla, edozein ez-betetzeren

aurrean berehalako neurri zuzentzaileak aplikatu behar direla, eta erabaki guztietan eta baliabideen esleipenean segurtasuna lehenetsi behar dela. Segurtasunaren eta beste interes batzuen (funtzionaltasunaren edo eraginkortasunaren) artean gatazkarik sortuz gero, segurtasuna gailendu beharko da beti. Ikuspegi horrek lidergo konprometitua, komunikazio argia, etengabeko prestakuntza eta etengabeko ebaluazioa eskatzen ditu, ingurune digital seguru eta babestua bermatzeko.

5 konpromisoa: CAFi eta haren interes-taldeei buruzko era guztietako datuak babestea, jabetza intelektualari, industrialari, sekretu komertzialei, izaera pertsonalari edo beste alor batzuei dagokienez.

CAFi eta haren interes-taldeei dagozkien datuen babes osoa ezartzen da. Besteak beste, jabetza intelektualaren, industrialaren, sekretu komertzialen eta datu pertsonalen babes zorrotza hartzen du bere baitan. Segurtasun-neurri sendoak ezartzea, hala nola zifratzea, sarbide-kontrola eta langileen prestakuntza, funtsezkoa da informazio hori baimenik gabe eskuratzea, zabaltzea edo behar ez bezala erabiltzea prebenitzeko. Era berean, beharrezkoa da informazio-sistemen eta sareen segurtasun fisikoa eta ingurunekoa kontuan hartuko dituzten neurriak ezartzea, sistema horiek babesteko sistemaren ustekabeko akatsen, giza akatsen, asmo txarreko ekintzen edo fenomeno naturalen aurrean, jardueren jarraitutasuna bermatzeko.

Aktibo ukiezin horiek babestuz, CAFek bere abantaila lehiakorra eta ospea gordetzeaz gain, interes-taldeekiko dituen erantzukizun legalak eta etikoak ere betetzen ditu. Gainera, komunikazio-kanal argiak ezarri behar dira, erabiltzaileek gorabeherak jakinarazi eta laguntza jaso dezaten, eta gorabeherei erantzuteko planak ezarri behar dira, erabiltzaileen segurtasunean eta pribatutasunean eragin kaltegarri oro arintzeko.

6. konpromisoa: Balio-kate osoan zibersegurtasuna sustatzea.

Balio-katearen maila guztietan zibersegurtasuna aktiboki sustatzen da, zibersegurtasuneko eta informazioaren segurtasuneko eta datuen babeseko estandar globalak ezartzea eta betetzea sustatuz hornitzaileen, azpikontratisten eta bezeroen artean. Aliantza estrategikoak egiten dira zibersegurtasunarekin konprometituta dauden eragileekin, eta praktika arduratsuak sustatzen dira, ezbeharren arriskua minimizatzeko eta sistemen eta datuen osotasuna babesteko.

4. METRIKAK ETA HELBURUAK

Zibersegurtasun-politikan ezarritako printzipioak eta konpromisoak betetzen direla bermatzeko, CAFek monitorizazio- eta kontrol-sistema sendo bat definitu du, errendimendu-adierazleetan eta epe labur, ertain eta luzerako argi definitutako helburuetan oinarritua.

Errendimendu-adierazleen aldian behingo jarraipenari esker, aurrez definitu diren epe laburreko, ertaineko eta luzeko helburuak lortzeko bidean egindako aurrerapena ebalua daiteke. Praktika horrek arreta eta hobekuntza behar duten arloak identifikatzen laguntzen du, erabakiak behar bezala hartzeko eta neurri zuzentzaile egokiak ezartzeko aukera emanez. Horrela, etengabeko hobekuntza-zikloa ziurtatzen da, eta errendimendua eta eraginkortasuna optimizatzen dira erakundearen maila guztietan.

Eraginkortasuna bermatzeko, errendimendu-adierazleek irizpide hauek bete behar dituzte:

- Garrantzia: Adierazleek zehatz eta modu esanguratsuan neurtu eta islatu behar dute helburu jakin bat lortzeko bidean egindako aurrerapena, eta erabakiak hartzeko eta ekintzak egiteko erabil daitekeen informazioa eman behar dute.
- Errepresentazio leiala: Datuen iturriek fidagarriak izan behar dute, eta neurketa-metodoak estandarizatu egin behar dira. Adierazleen bidez aurkeztutako informazioak osoa, neutrala eta zehatza izan behar du.
- Aukera: Adierazleak neurtzeko maiztasunak egokia izan behar du erabakiak hartzeko.
- Erabiltzeko erraztasuna: Erraz ulertzeko eta interpretatzeko modukoak izan behar dute, bai biltzen dituztenentzat, bai horiek aztertzeaz arduratzen direnentzat.
- Komunikazio eraginkorra: Adierazleen emaitzak argi eta zehatz jakinarazi behar zaizkie erakundeko maila guztiei.

Adierazle garrantzitsuenak informazio ez-finantzarioaren txostenean bilduko dira, Taldeak bere gain hartutako iraunkortasun-jardunbide onenen arabera.

Ikuspegi horren helburua da gobernu korporatibo ona, etika eta jasangarritasuna zeharkako ardatzak izatea CAFen maila guztietan erabakiak hartzeko garaian, eta, bereziki, arriskuen kudeaketan, haren jarduerek balioa sor dezaten, bai akziodunentzat, bai gainerako interes-taldeentzat.

5. ZIBERSEGURTASUNAREN ARLOKO GOBERNANTZA ETA IKUSKAPENA

CAFen gobernantza informazioaren segurtasunari dagokionez, eta, bereziki, zibersegurtasunari dagokionez, maila hauen bidez egituratzen da:

a) Administrazio Kontseilua

Administrazio Kontseiluak zibersegurtasunari buruzko Taldearen barne-gobernantzaren oinarriak finkatzen ditu, arlo horretako helburu estrategikoak definituz, eta, bereziki, eskumen hauen bidez:

- Eremu korporatiboko politika hau onartzea.
- Erakundeko zibersegurtasunaren segimendua egitea.
- Zuzendaritzarekin batera, zibersegurtasunaren kultura sustatzea erakunde osoan, zibersegurtasunaren arloko arriskuak prebenitzeko eta arintzeko jardunbide gomendagarriei buruz kontzientziatzeko.
- Auditoretza Batzordeari zibersegurtasunaren arloko zuzeneko gainbegiratzea esleitzea.
- Zibersegurtasun Funtzioaren helburuak lortzeko beharrezkoak diren gaitasunak eta baliabideak, materialak eta giza baliabideak eskuragarri daudela ziurtatzea.
- Auditoretza Batzordeak hala eskatuta, politika hau eguneratzea, 7. apartatuan aurreikusitakoaren arabera.

b) Ikuskaritza Batzordea

Ikuskaritza Batzordeak Taldearen arrisku finantzarioak eta ez-finantzarioak (teknologikoak barne) kudeatzeko eta kontrolatzeko sistemak ikuskatzeko eta ebaluatzeko ahalmena du.

Era berean, Auditoretza Batzordeari honako eskumen hauek dagozkio:

- Politika honen aplikazioa gainbegiratzea, baita Zibersegurtasunaren Funtzioa ere.
- Zibersegurtasun-funtzioaren arduradun korporatiboari aldizka eta erregulartasunez haren kudeaketari buruzko txostenak eskatzea, gutxienez urtean behin.

  Txosten horietan jasoko dira, gutxienez, zibersegurtasunaren egoera eta kudeatutako gorabehera esanguratsuak, halakorik balego.
- Politika hau eguneratzeko proposamena egitea Kontseiluari, 7. idatz-zatian aurreikusitakoaren arabera.

c) Teknologia Korporatiboko zuzendaria

Teknologia Korporatiboko zuzendaria:

- Taldearen teknologiaren arloko gidalerroak finkatuko ditu, eta, bereziki, zibersegurtasuna kudeatzeko~~,~~ eta funtzio hori Taldearen gainerako eremu teknologikoekin koordinatuko du.
- Zibersegurtasun-funtzioaren arduradun korporatiboaren zuzeneko txostena jasoko du, maila korporatiboan zehaztutako helburu estrategikoen eta funtsezko jarduera-adierazleen (KPI) betetze-mailari buruzkoa.
- Zibersegurtasunaren arloko goi-zuzendaritzaren parte-hartzea erraztuko du Zibersegurtasunaren Funtzioaren arduradun korporatiboak zuzenean parte hartzen ez duen goi-mailako foroetan.
- Zibersegurtasuneko Batzorde Korporatiboan ordezkatuta egon behar duten CAFen eremuak ezarriko ditu.

d) Zibersegurtasun-funtzioa eta Zibersegurtasun-funtzioaren arduradun korporatiboa

Zibersegurtasunaren Funtzioa Administrazio Kontseiluak zibersegurtasunaren arloan ezarritako jarraibide estrategikoak garatzeaz, ezartzeaz eta aplikatzeaz arduratzen den barne-organoa da. Funtzionalki, Administrazio Kontseiluaren, Auditoretza Batzordearen edo goi-zuzendaritzaren mende egon ahalko da, sare- eta informazio-sistemen arduradunak alde batera utzita.

Arduradun nagusia (Zibersegurtasun-funtzioaren arduradun korporatiboa) funtzioa betetzeko ezagutza, esperientzia eta gaitasun egokiak dituen pertsona bat izango da, eta erakundean erabakiak hartzeko eta eragiteko behar besteko gaitasuna izango du.

Bere eskumen nagusien artean, Zibersegurtasunaren Funtzioak zibersegurtasun-arriskuen balorazioa, kontrola, kudeaketa eta monitorizazioa ziurtatuko ditu, bai eta ziberresilientzia-mekanismo egokien ezarpena ere, foro egokiei informazio egokia ematen zaiela bermatuz. Halaber, zibersegurtasunari lotutako errendimendu-adierazleak zehaztuko ditu, eta erakundean prestakuntza- eta sentsibilizazio-ekimenak sustatuko ditu.

Zibersegurtasun-funtzioaren arduradun korporatiboak bere eginkizunen berri emango dio Teknologia Zuzendaritzari eta, nolanahi ere, Auditoretza Batzordeari aldian behin, arlo horretako jardunbide egokienekin bat etorriz.

Zibersegurtasunaren funtzioa aldizka ebaluatuko da, arriskuak kontrolatzeko eta kudeatzeko sistemaren esparruan.

e) Zibersegurtasuneko Batzorde Korporatiboa

Taldeak Zibersegurtasuneko Batzorde Korporatibo bat izango du, Taldearen jardueran funtsezko eragina izan dezaketen informazioaren segurtasunaren arloko ebazpen garrantzitsuak emateko.

Zibersegurtasuneko Batzorde Korporatiboak erakundearen arlo kopuru egokia izango du ordezkatuta, bai eta Teknologiako zuzendaria eta Zibersegurtasuneko Funtzioaren arduradun korporatiboa ere.

Zibersegurtasun-funtzioaren korporazio-arduradunaren eskumenak garatzeko beste egitura kolegiatu batzuk ere egon daitezke, eta haren koordinaziopean jardungo dute.

Halaber, zibersegurtasun-krisien batzordeak eratuko dira, eta beste krisi-batzorde batzuen Zibersegurtasun Funtzioari parte harraraziko zaio, beharren arabera.

f) Negozioaren Zuzendaritza

CAF Taldearen barruan negozio-jarduera jakin baten dibisioaz arduratzen den organo gorena da Negozio Zuzendaritza.

Zibersegurtasunaren arloan, Negozio Zuzendaritzaren funtsezko erantzukizuna politika hori ezartzea izango da, eta negozioa bera garatzeko, ikuskatzeko eta kontrolatzeko hedapen-planen definizioa bermatuko du. Horretarako, Negozioaren Zibersegurtasuneko arduraduna izendatuko da.

g) Negozioaren Zibersegurtasuneko arduraduna

Negozioaren Zibersegurtasuneko arduradunak zibersegurtasunarekin lotutako negozio mailako kudeaketa guztiak koordinatuko ditu, hala nola zibersegurtasuneko gidalerro korporatiboak Negozioan hedatzea eta zibersegurtasunaren arloko eskumenak ezartzea, prestakuntza- eta kontzientziazio-plan korporatiboak gaituz eta Negozioak izan ditzakeen behar espezifikoak identifikatuz.

6. BARNEKO INFORMAZIO-SISTEMA (SALAKETA-BIDEAK)

Taldeko kide guztiek lan- edo lanbide-testuinguruan identifikatutako portaerei edo jokabideei buruzko informazioa eman behar dute, Politika honetan ezarritako printzipio eta parametroen aurkakoak izan badaitezke, baita arriskuzantzua izan daitekeen edozein jarduera edo jokabide ezagunei buruzkoa ere.

Horretarako, Taldearen Informazioko Barne Sistema erabili beharko dute, Taldearen Informazioko Barne Sistemaren Politikan ezarritakoaren arabera, eta web orri korporatiboaren bidez sartu beharko dute sisteman. Taldearekin zerikusirik ez duen beste edozein hirugarrenek ere erabil dezake mekanismo hori, politika honen ondoriozko ez-betetzeei buruzko informazioa emateko.

Taldearen Informazioko Barne Sistemak Informazioko Barne Sistemaren Politikan islatutako konfiantza- eta konfidentzialtasun-bermeak (informatzailearen identitatearen babesa barne) eskaintzen ditu, bai eta errepresaliak debekatzeko bermeak ere, eta fede onez erabili beharko da, ez-betetzeren bat dagoela edo hura agertzeko arriskuren bat dagoela arrazoizkoa den ustean oinarrituta.

7. BERRIKUSTEA ETA EGUNERATZEA

CAFeko Administrazio Kontseiluak, Ikuskaritza Batzordeak eskatuta, politika eguneratuko du, batez ere egoera hauetakoren bat gertatzen bada:

- Politika honen edukiari eragiten dioten arau-aldaketa garrantzitsuak onartzea.
- Politika honen edukian hobekuntza-arloak edo hutsuneak aurkitzea, politika horren gainean egindako berrikuspen eta egiaztapenen ondorioz.

8. ONARTZEA ETA ZABALTZEA

Politika hau 2024ko urriaren 10ean onartu zuen Administrazio Kontseiluak, eta egun horretatik aurrera sartuko da indarrean.

Interesa dutenek eta hartzaileek errazago izan dezaten, politika hau CAFen webgunean argitaratuko da, bai eta Taldearen barruko kanaletan ere.