INFORMAZIOAREN SEGURTASUN POLITIKA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Bertsioa:	1.0
Bertsioaren data:	2024-02-22
Mota:	*Barne dokumentua*

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 istripukalteetatik, 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 plangintzan 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. Introducción

Los sistemas TIC (Tecnologías de la Información y Comunicaciones) son imprescindibles para el logro de los objetivos de IZT KOOP.E. Estos sistemas deben administrarse con diligencia, adoptando las medidas adecuadas para proteger la información tratada o de los daños accidentales, involuntarios o intencionados, que puedan afectar a la disponibilidad, integridad o confidencialidad de los servicios prestados.

Los objetivos de la seguridad de la información son garantizar la calidad de la información, la prestación continua de los servicios, actuar de forma preventiva, supervisar la actividad diaria y reaccionar rápidamente ante los acontecimientos.

Los sistemas TIC deben estar protegidos contra amenazas de evolución rápida, garantizando la confidencialidad, integridad y disponibilidad, previendo diferentes usos e incidiendo en el valor de los servicios. Para protegerse de estas amenazas es necesaria una estrategia que se adapte a los cambios que se producen en las condiciones del entorno y que garantice la prestación continuada de los servicios. Por ello, IZT, basándose tanto en el Esquema Nacional de Seguridad como en la norma ISO 27001, aplica medidas de seguridad en sus servicios. Por tanto, actúa para garantizar la continuidad de los servicios mediante el seguimiento continuo de las situaciones de prestación de servicios, la detección y el análisis de las vulnerabilidades y la respuesta eficaz a los incidentes. IZT debe asegurar que la seguridad de las TIC en todas las etapas del ciclo de vida de los servicios es integral y que se gestionan las decisiones de desarrollo y adquisición y las actividades de explotación. Se deben identificar y planificar los requisitos de seguridad y las necesidades de financiación.

IZT y sus personas deben estar preparadas para prevenir, detectar, reaccionar y estimular, de acuerdo con la normativa y la legislación vigente.

1.1. Prevención

IZT debe evitar, o al menos prevenir, en la medida de lo posible, que la información o los servicios se vean afectados por incidentes de seguridad. Para ello, se han establecido las medidas mínimas de seguridad definidas por las normas ENS e ISO 27001, así como las amenazas y otros controles identificados como consecuencia de la valoración y análisis de riesgos. Estos controles, roles y responsabilidades de seguridad están claramente definidos y documentados.

Para garantizar el cumplimiento de la política, IZT debe:

- *Autorización de sistemas antes del inicio de la operación.*
- *Evaluar regularmente la seguridad,*
- *Revisión periódica del sistema por terceros.*

1.2. Detección

Dado que los eventos pueden provocar una rápida degradación de los servicios, éstos deben monitorizar su actuación para la detección permanente de anomalías de acuerdo con lo establecido en el artículo 9 del ENS. La monitorización es especialmente importante para construir líneas de defensa de acuerdo con el artículo 8 del ENS.

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.

1.3. Respuesta

Los Departamentos deben:

• Establecer mecanismos para responder eficazmente a los incidentes de seguridad.

• Designar el punto de comunicación y contacto de incidentes

• Establecer protocolos de intercambio de información relacionada con el suceso.

1.4.- Recuperación

Para garantizar la disponibilidad de los servicios críticos, IZT ha desarrollado planes de continuidad de los sistemas TIC dentro del plan general de continuidad global del negocio.

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.

2. MISIÓN DE IZT

IZT acompaña desde 2005 a sus clientes tanto en su transformación digital como en su ejercicio diario para hacer efectiva su experiencia tecnológica.

En este sentido, y con el fin de satisfacer las necesidades de los clientes en relación con las TIC, prestamos especial atención a la ética profesional, la calidad del servicio y la mejora continua.

Desde su creación, nuestro objetivo ha sido ofrecer asesoramiento cercano y profesional a los clientes tanto en el ámbito del derecho informático como en el de la seguridad y privacidad de la información, y, consciente de su importancia actual, integrarlos en todos los servicios que alberga IZT.

*Para esta nueva etapa hemos definido tres ramas: **Sistemas de información, Servicios Cloud y Desarrollo de aplicaciones**. A través de estas tres áreas ofreceremos servicios especiales a nuestros clientes en estas secciones.*

En los servicios que ofrece IZT, los sistemas de información, los servicios cloud y la programación de aplicaciones, se trabajan como líneas transversales los criterios de seguridad, el requisito de las leyes y la vigilancia tecnológica.

Junto a la confidencialidad y profesionalidad de sus empleados, todas las personas que componen IZT tienen una especial sensibilidad hacia su entorno.

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.

3. Objetivos, alcance y usuarias

El objetivo de esta política es definir y gestionar los criterios y normas básicas de seguridad de la información. Esta Política se aplica a toda la organización de la IZT KOOP.E.

Las personas usuarias de este documento son miembros del equipo de trabajo de IZT y deben ratificarlo o, en su caso, actualizarlo al menos una vez al año.

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

4. Documentos de referencia

- *Norma ISO/IEC 27001 apartados 5.2 y 5.3*
- *Real Decreto SEN-ENS 311/2022*
- *Documento de Comunicación del SGSI*
- *Metodología de análisis y tratamiento de riesgos*
- *Declaración de aplicabilidad*
- *Relación de requisitos legales, normas y/o convenios.*
- *Plan de Continuidad*
- *Procedimiento de gestión de incidencias*

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. Gestión de la seguridad de la información

5.1. Objetivos y medición

Los objetivos generales del sistema de gestión de la seguridad de la información son:

- *Proteger los recursos de información de la IZT frente a las amenazas, tanto internas como externas, para garantizar la confidencialidad, integridad, disponibilidad, legalidad y fidelidad de la información.*
- *Asegurar que las actividades que se llevan a cabo tanto con la información como con los sistemas que la gestionan se realicen de forma segura en los servicios que ofrece la IZT KOOP.E. y ofrecer garantía a los clientes.*
- *Crear una imagen adecuada en el mercado minimizando los daños de posibles incidencias y reflejando la imagen de seguridad.*
- *Garantizar la implementación de las medidas de seguridad contempladas en esta Política de Seguridad.*
- *Mantener actualizada la Política de Seguridad de la IZT, para garantizar su eficacia.*

Tanto la persona responsable del SGSI como el equipo de trabajo de la IZT son las personas responsables de revisar de forma permanente estos objetivos e implementar, en su caso, otros nuevos. Los objetivos de los controles de seguridad individuales serán propuestos por la persona responsable del SGSI y aprobados por el grupo de trabajo SGSI. Todos estos objetivos deberán ser revisados al menos una vez al año.
IZT KOOP.E. medirá el grado de cumplimiento de estos objetivos. La determinación del método de medición del grado de cumplimiento de los objetivos será responsabilidad de la persona responsable del SGSI, los objetivos se medirán al menos una vez al año y el equipo de trabajo del SGSI los valorará e informará de los resultados a la dirección de la IZT KOOP.E.

5.2. Obligaciones de seguridad de la información

Tanto la presente Política como el SGSI en su conjunto deben cumplir todos los requisitos legales, normativos y contractuales relacionados con la seguridad de la información.

En el espacio SGSI de IZT se relacionan los requisitos legales, normativos y contractuales.

5.3. Controles de seguridad de la información (protecciones)

El proceso de selección de los controles (protecciones) está definido en la metodología de valoración y tratamiento de riesgos en el sitio SGSI de IIZT KOOP.E. y los controles seleccionados y su estado de implementación están definidos en la Declaración de Aplicabilidad.

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. Procedimientos y políticas específicas para garantizar la seguridad de la información

Se han acordado y establecido procedimientos y políticas concretas en diversos ámbitos para garantizar la seguridad de la información. Todos ellos se recogen en el espacio SGSI de IZT KOOP.E:.

- *Dispositivos móviles y tele-trabajo*
- *Política trae tú dispositivo*
- *Declaración de aceptación de documentos del SGSI*
- *Declaración de confidencialidad*
- *Inventario de activos*
- *Clasificación de la información*
- *Uso aceptable*
- *Contraseñas*
- *Control de accesos*
- *Utilización de controles criptográficos*
- *Borrado y eliminación*
- *Pantalla y sobremesa limpia*
- *Trabajar en zonas seguras*
- *Copias de seguridad*
- *Gestión de cambios*
- *Procedimientos operativos para TIC y comunicaciones*
- *Transferencia de información*
- *Obligaciones de seguridad*
- *Desarrollo seguro*
- *Seguridad para proveedores*
- *Registro de incidencias*
- *Gestión de incidencias*
- *Continuidad del negocio*
- *Metodología de análisis de impactos de negocio*
- *Estrategia de continuidad de negocio*
- *Plan de continuidad del negocio*

5.5. SEGURTASUN ANTOLAKETA

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

5.5.Organización de la seguridad

Las responsabilidades de las distintas secciones del SGSI se reparten entre los diferentes trabajadores de IZT KOOP.E. Las características de las responsabilidades son los siguientes:

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

5.5.1. Comités

Siendo IZT una organización pequeña el comité del SGSI asumirá las funciones tanto del comité de seguridad como del comité de sistemas. El Comité SGSI está compuesto por:
- *Responsable de Información y Servicios*
- *Responsable de Seguridad*
- *Responsable de Sistemas*

5.5.2. ROLAK: FUNTZIO ETA ARDURAK

5.5.2. Roles: Funciones y responsabilidades

Adura / Responsabilidad	**Funtzioa** / Función
Informazioa eta zerbitzuen arduraduna *Responsable de Información y Servicios*	ISKSaren arduraduna, datu pertsonalen tratamendu arduraduna, informazioaren arduraduna, zerbitzuaren arduraduna Beste funtzioak: Trebakuntza eta kontzientziazioa, betekizunak, dokumentuen sailkapen eta kontrola, giza baliabideak, hornitzaileak...

	Responsable del SGSI, Responsable del tratamiento de datos personales, Responsable de la información, Responsable del servicio *Otras funciones: Formación y concienciación, requisitos, clasificación y control documental, recursos humanos, proveedores...*
Segurtasun arduraduna *Responsable de seguridad*	Informazioa behar bezala segurtatzen dela bermatzen duena. Segurtasun intzidentziak kudeatzen dituena Beste funtzioak: metrikak eta adierazleak, barne auditoriak, hobekuntza... *Debe garantizar la correcta seguridad de la información. Gestor de incidencias de seguridad* *Otras funciones: métricas e indicadores, auditorías internas, mejora...*
Sistemaren arduraduna *Responsable del sistema*	Azpiegitura eta neurri teknikoak kudeatzea, aktiboen babesa, segurtasun fisikoa, segurtasun neurriak... *Gestión de infraestructuras y medidas técnicas, protección de activos, seguridad física, medidas de seguridad...*

5.5. IZENDAPEN PROZEDURA

Zehaztutako ardurak zuzendaritzak izendatuko ditu, ISKS Batzordearen proposamenak entzunez.

Izendapen hauek gutxienez urtean behin berrikusi behar dira.

5.5. Procedimiento de nombramiento

Las responsabilidades que se determinen serán designadas por la Dirección, a propuesta del Comité de SGSI.

Estos nombramientos deberán ser revisados al menos una vez al año.

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.

5.6. Comunicación de la política

La persona responsable de Información y Servicios debe garantizar el conocimiento de esta Política tanto de todo el personal como de los proveedores y terceras partes relacionados con IZT.

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.

6. GESTIÓN DE RIESGOS

Todos los sistemas asociados a esta política de seguridad deberán pasar un análisis de riesgos evaluando las amenazas y riesgos que puedan sufrir. Se ha repetido el análisis en los siguientes casos:

• Permanentemente, al menos una vez al año.

• Cuando cambia el tipo de información que se utiliza.

• Cuando se modifiquen los servicios que se ofrecen.

• Cuando se produce una incidencia grave de seguridad.

• Cuando se detecten graves vulnerabilidad.

Con el fin de equilibrar los análisis de riesgos, el Comité SGSI realizará una valoración de referencia tanto para los diferentes tipos de información utilizados como para los diferentes servicios que se ofrecen. El Comité SGSI dinamizará la disponibilidad de recursos para atender las necesidades de seguridad de los sistemas.

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. Apoyo a la implementación del SGSI

Mediante el siguiente documento la persona responsable de Información y Servicios, en calidad de Responsable del SGSI y en representación de la Dirección, indica que en el proceso de implementación y mejora continua del SGSI se procurará poner los medios necesarios para alcanzar los objetivos de esta Política e identificarlos para cumplir los requisitos.

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.

7.1 Apoyo de la dirección

La Dirección de IZT es consciente de la importancia de la seguridad de la información para llevar a cabo con éxito sus objetivos de negocio, se compromete a:

• Promover funciones y responsabilidades organizativas en materia de seguridad de la información.

• 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.

• Proporcionar los medios adecuados para alcanzar los objetivos de seguridad de la información.

• Promover la difusión y concienciación de la política de seguridad de la información entre los socios y trabajadores de IZT.

• Garantizar el cumplimiento de la política, legislación y normativa vigente en materia de seguridad de la información.

• Tener en cuenta los riesgos de la seguridad de la información.

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.

8. Obligaciones de los trabajadores

Todos los miembros de IZT KOOP.E deben conocer y cumplir esta Política de Seguridad de la Información y el Reglamento de Seguridad, siendo función del Comité de Seguridad de las TIC poner los medios necesarios para que la información llegue a todos los que estén debidamente interesados.

Todos los miembros de la IZT KOOP.E. recibirán al menos una sesión de concienciación sobre el tema una vez al año. Las personas responsables en el uso o administración de los sistemas TIC recibirán formación en el uso seguro de los sistemas.

9. HIRUGARREN ALDEAK

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.

9. Terceras partes

Cuando IZT preste servicios a otros organismos o utilice información de otros, se les informará de esta Política de Seguridad de la Información, el Comité de Seguridad correspondiente facilitará los canales de información y coordinación y se establecerán procedimientos de actuación ante posibles incidencias de seguridad.

Cuando IZT utilice servicios de terceros o ceda información a terceros se informará a las terceras partes de la presente Política de Seguridad y del Reglamento de Seguridad. Se garantizará la adecuada concienciación del personal de terceros en materia de seguridad, al menos al mismo nivel establecido en esta política.

Cuando algún aspecto de la política no pueda ser satisfecho por un tercio, la persona responsable de seguridad deberá elaborar un informe detallando los riesgos y la forma de tratarlos.

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.

Ppolitiken 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.

10. Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la Información se desarrollará a través de otras políticas o normativas. Fruto de estas políticas y normativas se han desarrollado procedimientos que describen el modo de llevarlos a cabo.

La documentación de las políticas y normativas, así como el conocimiento de las siguientes Políticas de Seguridad, estará a disposición de todo el personal de IZT que lo necesite, especialmente el que utilice o administre los sistemas de información y comunicación.

10.1. Estructura normativa

La Política de Seguridad de la Información es de obligado cumplimiento y se estructura jerárquicamente en los siguientes niveles:

1. ***Primer nivel:** Política de Seguridad de la Información.*

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.

2. ***Primer nivel:*** *Política de Seguridad de la Información.*
3. ***Segundo nivel:*** *Normativas de seguridad de la información.*
4. ***Tercer nivel:*** *Procedimientos e instrucciones técnicas para la seguridad de la información.*
5. ***Cuarto nivel:*** *Informes, registros y evidencias electrónicas.*

La estructura jerárquica permite adaptar eficazmente los niveles inferiores a los cambios en los entornos de IZT sin necesidad de revisar la estrategia de seguridad.
El personal de IZT estará obligado a conocer y cumplir, además de esta Política de Seguridad, toda la Información, Reglamentos y Procedimientos e Instrucciones Técnicas de Seguridad que puedan afectar a sus funciones.

11. Gestión y valor de los documentos

El siguiente documento será válido hasta el 2 de noviembre de 2024

La propietaria de este documento es la persona responsable de la Información y se responsabiliza de su revisión y, en su caso, actualización, al menos una vez al año. A la hora de medir la eficacia e idoneidad del documento deben tenerse en cuenta los siguientes criterios:

• Personal, proveedores y terceros relacionados con el SGSI que desconocen el documento.

• Incumplimientos legales, normativos o convencionales relacionados con el SGSI.

• Ineficacia en la implementación o mantenimiento del SGSI.

• Responsabilidades inadecuadas en la implementación o mantenimiento del SGSI.