

DEKRETUA/DECRETO

Espediente zk./ Expediente nº: 3031/2025

Bazterrean ezarritako zenbakia eta data dituen ebazpena/ Resolución con número y fecha establecidos al margen

Prozedura/ Procedimiento: Informazioaren segurtasunari buruzko politika eta araudia/
Política y normativa de seguridad de la información

EGITATEAK ETA ZUZENBIDEKO OINARRIAK/ HECHOS Y FUNDAMENTOS DE DERECHO

Ermuko Udala IKT (Informazio eta Komunikazio Teknologiak) sistemen menpe dago bere helburuak lortzeko. Sistema horiek arretaz administratu eta neurri egokiak hartu behar dira emandako zerbitzuetan tratatzen den informazioaren erabilgarritasunari, osotasunari edo konfidentziasunari eragin diezaieketen halabeharrezko edo nahitako kalteetatik babesteko.

Informazioaren segurtasunaren helburua informazioaren kalitatea eta zerbitzuak etengabe ematen direla bermatzea da, prebentzioz jardunez, eguneroko jardura gainbegiratzuz eta gorabeherei azkar erantzunez.

IKT sistemek babestuta egon behar dute eboluzio azkarreko mehatxuetatik, baldin eta horiek eragina izan badezakete informazioaren eta zerbitzuen konfidentziasunean, osotasunean, erabilgarritasunean, aurreikusitako erabileran eta balioan. Mehatxu horietatik defendatzeko, ingurune baldintzen aldaketetara egokitzen den estrategia bat behar da, zerbitzuak etengabe ematen direla bermatzeko. Horrek esan nahi du,

El Ayuntamiento de Ermua depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada a los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que



Segurtasunaren Eskema Nazionalak eskatzen dituen gutxieneko segurtasun-neurriak aplikatzeaz gain, zerbitzuen prestazio-mailen etengabeko jarraipena egin behar dela, jakinarazitako ahultasunen jarraipena eta azterketa egin behar dela eta gorabeherai erantzun eraginkorra eman behar zaiela, ematen diren zerbitzuen jarraitutasuna bermatzeko.

Ermuko Udalak egiaztatu behar du IKTen segurtasuna sistemaren bizi-zikloko etapa bakoitzaren zati integrala dela, sistema sortzen denetik zerbitzutik kendu arte, garapen- edo eskuratze-erabakiak eta ustiapen-jarduerak barne hartuta. Segurtasun-eskakizunak eta finantzaketa-beharrak IKT proiektuetarako plangintzan, eskaintza-eskaeran eta lizitazio-pleguetan identifikatu eta sartu behar dira.

Ermuko Udalak prest egon behar du gorabeherak prebenitzeko, antzemateko, horiei erantzuteko eta horietatik erreuperatzeko, Segurtasunaren Eskema Nazionala arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuari jarraikiz.

Toki Araubidearen Oinarriak arautzen dituen apirilaren 2ko 7/1985 Legearen 21. artikuluen arabera.

se deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

El Ayuntamiento de Ermua debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC.

El Ayuntamiento de Ermua debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

En virtud del artículo 21 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

EBAZPENA/ RESOLUCIÓN

1. Informazioaren segurtasun-politika onartzea, Ermuko Udaleko pertsona guztiek nahitaez bete beharrekoa.
2. Informazioaren segurtasun-batzordea eta informazioaren segurtasun-

1. Aprobar la política de seguridad de la información, que será de obligado cumplimiento por todas las personas del Ayuntamiento de Ermua.
2. Designar al comité de seguridad de la información y a las personas responsables del sistema de



sistemaren arduradunak izendatzea, eta haien rolak eta eginkizunak zehaztea.

3. Dekretu hau Ermuko Udaleko pertsona guztiei komunikatzea, jakinaren gainean egon daitezen eta bete dezaten.

Ermuan, marjinar adierazitako data horretan.

seguridad de la información , definiendo sus roles y funciones.

3. Comunicar el presente decreto a todas las personas del Ayuntamiento de Ermua para su conocimiento y cumplimiento.

En Ermua en la fecha en el margen indicada.

**ELEKTRONIKOKI SINATUTAKO DOKUMENTUA/ DOCUMENTO FIRMADO
ELECTRÓNICAMENTE**





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

AURKIBIDEA

1.	Onartzea eta indarrean sartzea.....	5
2.	Sarrera.....	5
3.	Irismena.....	5
4.	Xedea.....	6
5.	Arau-esparrua.....	6
6.	Oinarrizko printzipioak.....	7
6.1	Segurtasuna prozesu integral gisa.....	8
6.2	Arriskueta oinarritutako segurtasunaren kudeaketa.....	8
6.3	Prebentzioa, detekzioa, erantzuna eta kontserbazioa.....	8
6.3.1	Prebentzioa.....	8
6.3.2	Detekzioa.....	8
6.3.3	Erantzuna.....	8
6.3.4	Berreskuratzea.....	9
6.4	Defentsa-lerroak.....	9
6.5	Etengabeko zaintza eta aldizkako berrebaluazioa.....	9
6.6	Erantzukizunak bereiztea.....	9
7.	Gutxieneko eskakizunak.....	9
8.	Segurtasunaren antolamendua.....	10
8.1	Informazioaren Segurtasun Batzordea.....	10
8.1.1	Informazio-arduraduna.....	11
8.1.2	Zerbitzu-arduraduna.....	11
8.1.3	Informazioaren segurtasun-arduraduna.....	11
8.1.4	Sistema-arduraduna.....	12





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

8.1.5	Datuak babesteko ordezkaria.....	12
8.1.6	Idazkaritza Teknikoa.....	13
8.2	Izendatzeko prozedurak.....	13
8.3	Gatazkak konpontzea.....	13
9.	Informazioaren Segurtasun Politika berrikustea.....	14
10.	Datu pertsonalak.....	14
11.	Arriskuen kudeaketa.....	14
12.	Dokumentazioa egituratzea.....	14
13.	Informazioaren kalifikazioa.....	15
14.	Langileen betebeharrak.....	15
14.1	Ez-betetzea.....	15
15.	Hirugarren alderdiak.....	15
1.	Aprobación y entrada en vigor.....	17
2.	Introducción.....	17
3.	Alcance.....	17
4.	Misión.....	17
5.	Marco normativo.....	18
6.	Principios básicos.....	19
6.1	Seguridad como proceso integral.....	19
6.2	Gestión de la seguridad basada en los riesgos.....	19
6.3	Prevención, detección, respuesta y conservación.....	20
6.3.1	Prevención.....	20
6.3.2	Detección.....	20
6.3.3	Respuesta.....	20





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

6.3.4 Recuperación.....	20
6.4 Existencia de líneas de defensa.....	20
6.5 Vigilancia continua y reevaluación periódica.....	21
6.6 Diferenciación de responsabilidades.....	21
7. Requisitos mínimos.....	21
8. Organización de la seguridad.....	22
8.1 Comité de seguridad de la información.....	22
8.1.1 Responsable de la Información.....	23
8.1.2 Responsable del Servicio.....	23
8.1.3 Responsable de Seguridad de la Información.....	23
8.1.4 Responsable del Sistema.....	24
8.1.5 Delegado/a de Protección de datos.....	24
8.1.6 Secretaría Técnica.....	25
8.2 Procedimientos de designación.....	25
8.3 Resolución de conflictos.....	25
9. Revisión de la política de seguridad de la información.....	26
10. Datos de carácter personal.....	26
11. Gestión de riesgos.....	26
12. Estructuración de la documentación.....	26
13. Calificación de la información.....	27
14. Obligaciones del personal.....	27
14.1 Incumplimiento.....	27
15. Terceras partes.....	27





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

KODEA	BERTSIOA
ENS.01	1.0





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

1. ONARTZEA ETA INDARREAN SARTZEA

Informazioaren Segurtasun Politika hau alkatetza-dekretua sinatzen den egunaren biharamunean jarriko da indarrean, beste politika batek ordeztu arte.

2. SARRERA

Ermuko Udala IKT (Informazio eta Komunikazio Teknologiak) sistemen menpe dago bere helburuak lortzeko. Sistema horiek arretaz administratu eta neurri egokiak hartu behar dira emandako zerbitzuetan tratatzen den informazioaren erabilgarritasunari, osotasunari edo konfidentziasunari eragin diezaieketen halabeharrezko edo nahitako kalteetatik babesteko.

Informazioaren segurtasunaren helburua informazioaren kalitatea eta zerbitzuak etengabe ematen direla bermatzea da, prebentzioz jardunez, eguneroko jarduera gainbegiratzuz eta gorabeherei azkar erantzunez.

IKT sistemek babestuta egon behar dute eboluzio azkarreko mehatxuetatik, baldin eta horiek eragina izan badezakete informazioaren eta zerbitzuen konfidentziasunean, osotasunean, erabilgarritasunean, aurreikusitako erabilieran eta balioan. Mehatxu horietatik defendatzeko, ingurune baldintzen aldaketetara egokitzen den estrategia bat behar da, zerbitzuak etengabe ematen direla bermatzeko. Horrek esan nahi du, Segurtasunaren Eskema Nazionalak eskatzen dituen gutxieneko segurtasun-neurriak aplikatzeaz gain, zerbitzuen prestazio-mailen etengabeko jarraipena egin behar dela, jakinarazitako ahultasunen jarraipena eta azterketa egin behar dela eta gorabeherei erantzun eraginkorra eman behar zaiela, ematen diren zerbitzuen jarraitutasuna bermatzeko.

Ermuko Udalak egiaztatu behar du IKTen segurtasuna sistemaren bizi-zikloko etapa bakoitzaren zati integrala dela, sistema sortzen denetik zerbitzutik kendu arte, garapen- edo eskuratzeko erabakiak eta ustiapen-jarduerak barne hartuta. Segurtasun-eskakizunak eta finantzaketa-beharrak IKT proiektuetarako plangintzan, eskaintza-eskaeran eta lizitazio-pleguetan identifikatu eta sartu behar dira.

Ermuko Udalak prest egon behar du gorabeherak prebenitzeko, antzemateko, horiei erantzuteko eta horietatik errekupeatzeko, Segurtasunaren Eskema Nazionala arautzen duen maiatzaren 3ko 311/2022 Errege Dekretuari jarraikiz.

3. IRISMENA

Segurtasun Politika hau nahitaez bete beharko dute **Ermuko Udaleko** kide guztiek, irismenaren arabera:

- **Ermuko Udalak** ematen dituen zerbitzu guztien euskarri diren informazio-sistemak, 311/2022 Errege Dekretuaren xedapenen eta indarrean dagoen aplikagarritasun-adierazpenaren arabera.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	08/05/2025

4. XEDEA

Ermuko Udalaren xedea da hiriaren eta bertan bizi diren pertsonen behar, itxaropen, erronka eta aukerei erantzungo dieten zerbitzu publikoak eskaintzea, tokiko esparrutik. Sareetan lan egiten dugu, finantzaketa lortzeko eta ezagutza sortu eta partekatzeko. Gainera, gizarte-garapena eta ekonomia- eta ingurumen-jasangarritasuna aktiboki sustatzen ditugu. Horretarako, taldean lan egiten dugu, kalitatea, metodoa, efizientzia eta berrikuntza, errespetua, entzuketa eta gardentasuna aintzat hartuz, erakundeko pertsonen hazkunde integrala bultzatzeko.

5. ARAU-ESPARRUA

Informazioaren segurtasunari dagokionez, araudi hau hartzen da oinarritzko erreferentziazat:

- 39/2015 Legea, urriaren 1ekoa, Administrazio Publikoen Administrazio Prozedura Erkidearena.
- 40/2015 Legea, urriaren 1ekoa, Herri Administrazioen Araubide Juridikoarena.
- 311/2022 Errege Dekretua, maiatzaren 3koa, Segurtasunaren Eskema Nazionala arautzen duena.
- 3/2018 Lege Organikoa, abenduaren 5ekoa, datu pertsonalak babestekoa eta eskubide digitalak bermatzekoa.
- 2016/679 EB Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2016ko apirilaren 27koa, datu pertsonalen tratamenduari dagokionez pertsona fisikoen babesari eta datu horien zirkulazio askeari buruzko arauak ezartzen dituen eta 95/46/EB Zuzentaraua (Datuak Babesteko Erregelamendu Orokorra) indargabetzen duena.
- 4/2010 Errege Dekretua, urtarrilaren 8koa, Administrazio Elektronikoen esparruan Elkarreragingarritasun Eskema Nazionala arautzen duena.
- 1671/2009 Errege Dekretua, azaroaren 6koa, herritarrek zerbitzu publikoetan sarbide elektronikoa izateari buruzko 2007ko ekainaren 22ko 11/2007 Legea partzialki garatzen duena.
- 7/1985 Legea, apirilaren 2koa, Toki Araubidearen Oinarriak arautzen dituen (1999ko apirilaren 21eko 11/1999 Legeak aldatu zuen).
- 5/2015 Legegintzako Errege Dekretua, urriaren 30ekoa, Enplegatu Publikoaren Oinarritzko Estatutuaren Legearen testu bategina onartzen duena.
- 19/2013 Legea, abenduaren 9koa, gardentasunari, informazio publikoa eskuratzeko bideari eta gobernu onari buruzkoa.
- 9/2017 Legea, 2017ko azaroaren 8koa, Sektore Publikoko Kontratuena, Europako Parlamentuaren eta Kontseiluaren 2014ko otsailaren 26ko 2014/23/EB eta 2014/24/EB Zuzentzaruen transposizioa egiten duena Espainiako ordenamendu juridikora.
- 37/2007 Legea, azaroaren 16koa, sektore publikoko informazioa berrerrabiltzeari buruzkoa.
- 203/2021 Errege Dekretua, martxoaren 30ekoa, sektore publikoaren bitarteko elektronikoen bidezko jarduketara eta funtzionamendu-erregelamendua onartzen duena.
- 59/2003 Legea, abenduaren 19koa, sinadura elektronikoari buruzkoa.
- 6/2020 Legea, abenduaren 11koa, konfiantzazko zerbitzu elektronikoen zenbait alderdi arautzen dituen.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	08/05/2025

- 1/1996 Legegintzako Errege Dekretua, apirilaren 12koa, Jabetza Intelektualari buruzko Legearen testu bategina onartzen duena.
- 2/2018 Errege Lege Dekretua, apirilaren 13koa, Jabetza Intelektualari buruzko Legearen testu bategina —1996ko apirilaren 12ko 1/1996 Legegintzako Errege Dekretuaren bidez onartua— aldatzen duena eta Espainiako ordenamendu juridikoan Europako Parlamentuaren eta Kontseiluaren 2014ko otsailaren 26ko 2014/26/ Zuzentaraua (EB) eta Europako Parlamentuaren eta Kontseiluaren 2017ko irailaren 13ko 2017/1564 Zuzentaraua (EB) txertatzen dituena.
- 34/2002 Legea, uztailaren 11koa, informazioaren gizarteko eta merkataritza elektronikoko zerbitzuei buruzkoa.
- 9/2014 Legea, maiatzaren 9koa, Telekomunikazioei buruzkoa.
- Ebazpena, 2016ko urriaren 13koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasun Jarraibide Teknikoa onartzen duena, Segurtasun Eskema Nazionalarekin bat.
- Ebazpena, 2016ko urriaren 7koa, Administrazio Publikoen Estatu Idazkaritzarena, Segurtasunaren Egoerari buruzko Txostenaren Segurtasun Jarraibide Teknikoa onartzen duena.
- Ebazpena, 2018ko martxoaren 27koa, Funtzio Publikoaren Estatu Idazkaritzarena, Informazio Sistemen Segurtasunaren Auditoretzako Segurtasun Jarraibide Teknikoa onartzen duena.
- Ebazpena, 2018ko apirilaren 13koa, Funtzio Publikoaren Estatu Idazkaritzarena, Segurtasun-intzidentziak Jakinarazteko Segurtasun Jarraibide Teknikoa onartzen duena.
- 910/2014 EB Erregelamendua, Europako Parlamentuarena eta Kontseiluarena, 2014ko uztailaren 23koa, barne-merkatuan transakzio elektronikoak egiteko identifikazio elektronikoari eta konfiantzako zerbitzuei buruzkoa (Europako eIDAS Erregelamendua).
- 1671/2009 Errege Dekretua, azaroaren 6koa, herritarrek zerbitzu publikoetan sarbide elektronikoa izateari buruzko 2007ko ekainaren 22ko 11/2007 Legea partzialki garatzen duena.
- 57/2003 Legea, abenduaren 16koa, tokiko gobernua modernizatzeko neurriei buruzkoa.
- 25/2007 Legea, urriaren 18koa, komunikazio elektronikoen eta komunikazio-sare publikoen datuak gordetzei buruzkoa.
- 1553/2005 Errege Dekretua, abenduaren 23koa, nortasun-agiri nazionala eta horren sinadura elektronikoko ziurtagiriak arautzen dituena.
- 56/2007 Legea, abenduaren 28koa, informazioaren gizartea bultzatzeko neurriei buruzkoa.
- 14/2019 Errege Lege Dekretua, urriaren 31koa, administrazio digitalaren, sektore publikoko kontratazioaren eta telekomunikazioen arloan segurtasun publikoko arrazoiengatik presako neurriak hartzen dituena.

6. OINARRIZKO PRINTZPIOAK

Oinarrizko printzipioak funtsezko segurtasun-jarraibideak dira, informazio-aktiboen erabilerarekin lotutako edozein jardueratan beti kontuan hartu beharrekoak. Honako hauek finkatu dira:





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

6.1 SEGURTASUNA PROZESU INTEGRAL GISA

Segurtasuna prozesu integral gisa ulertuko da, IKT sistemekin zerikusia duten elementu tekniko, giza elementu, antolaketa-elementu eta elementu material guztiek osatua, alde batera utzita jarduketa puntual edo tratamendu koiuntural oro. Informazioaren segurtasuna ohiko jardunbidetzat hartu behar da, eta IKT sistemen hasierako diseinutik bertatik agertu eta aplikatu behar da.

6.2 ARRISKUETAN OINARRITUTAKO SEGURTASUNAREN KUDEAKETA

Arriskuen analisia eta kudeaketa segurtasun-prozesuaren funtsezko zatia izango da. Arriskuen kudeaketak ingurunea kontrolatuta izatea ahalbidetuko du, eta arriskuak maila onargarrietara murriztuko ditu. Arrisku-maila horiek murrizteko segurtasun-neurriak hedatuko dira, oreka ezarrita datuen izaeraren eta tratamenduen artean, inpaktuaren eta arriskuen probabilitatearen artean eta segurtasun-neurrien eraginkortasunaren eta kostuaren artean. Datuen segurtasunaren inguruko arriskua ebaluatzean, datu pertsonalen tratamenduaren ondoriozko arriskuak hartu behar dira kontuan.

6.3 PREBENTZIOA, DETEKZIOA, ERANTZUNA ETA KONTSERBAZIOA

6.3.1 Prebentzioa

Ermuko Udalak saihestu egin behar du —edo, behintzat, ahal den neurrian prebenitu— segurtasun-gorabeheren ondorioz informazioa edo zerbitzuak kaltetzea. Horretarako, SENak (Segurtasun Eskema Nazionalak) zehaztutako gutxieneko segurtasun-neurriak ezarriko ditu, bai eta mehatxuen eta arriskuen bilakaeraren bidez identifikatutako edozein kontrol gehigarri ere. Kontrol horiek argi eta garbi zehaztuta eta dokumentatuta egongo dira.

Politika betetzen dela bermatzeko, hau egin behar du Teknologia Zerbitzuak:

- Sistemak baimendu, jardunean hasi aurretik.
- Segurtasuna aldizka ebaluatu, ohiko konfigurazio-aldaketen ebaluazioak barne hartuta.
- Hirugarrenen aldizkako berrikuspena eskatu, ebaluazio independentea lortzeko.

6.3.2 Detekzioa

Ermuko Udalak bere informazio-sistemen eragiketa-kontrolak ezarri ditu, zerbitzuen prestazioan anomaliak detektatzeko eta horren arabera jarduteko, SENaren 10. artikulua (etengabeko zaintza eta aldizkako berrebaluazioa) xedatutakoari jarraikiz. Aurrez normaltzat ezarri diren parametroetan (SENaren 9. artikuluan adierazitakoaren arabera, defentsa-lerroetan) desbideratze esanguratsu bat gertatzen denean, beharrezko detekzio-, analisi- eta jakinarazpen-mekanismoak ezarriko dira arduradunengana erregulartasunez irits daitezen.

6.3.3 Erantzuna

Ermuko Udalak:

- Segurtasun-gorabehereri eraginkortasunez erantzuteko mekanismoak ezarri ditu.
- Harremanetarako guneak izendatu ditu beste sail edo erakunde batzuetan antzemandako gorabehereri buruzko komunikazioetarako.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	08/05/2025

- Gorabeherarekin lotutako informazioa trukatzeko protokoloak ezarri ditu. Horrek barne hartzen ditu Larrialdiei Erantzuteko Taldeekiko (CERT) komunikazioak, bi noranzkoetan.

6.3.4 Berreskuratzea

Zerbitzuen erabilgarritasuna bermatzeko, **Ermuko Udalak** zerbitzurik kritikoenak berreskuratzea bermatzeko beharrezkoak diren baliabide eta teknikak ditu.

6.4 DEFENTSA-LERROAK

Informazio-sistemak hainbat geruzaz osatutako babes-estrategia izango du. Horrela, geruzetako bat arriskuan badago, saihestu ezin izan diren gorabeherei aurre egiteko ekintza egokia garatu ahal izango da, sistema osoa arriskuan jartzeko probabilitatea murrizteko eta azken inpaktua arintzeko.

Neurri fisikoek, logikoek eta antolamendukoek osatutako defentsa-lerroak egongo dira,

6.5 ETENGABEKO ZAINZA ETA ALDIZKAKO BERREBALUAZIOA

Ermuko Udalak etengabeko zaintza egingo du jarduera edo portaera anomaloak antzemateko eta horiei erantzun egokia emateko.

Aktiboen segurtasun-egoera etengabe ebaluatzeak aukera emango dio **Ermuko Udalari** aktiboen bilakaera neurtzeko, ahuleziak antzemateko eta konfigurazio-akatsak identifikatzeko. **Ermuko Udalak** segurtasun-neurriak aldian-aldian berrebaluatu eta eguneratuko ditu, eta horien eraginkortasuna arriskuen eta babes-sistemen bilakaerara egokituko du. Beharrezkoa bada, segurtasuna birplanteatu ere egin ahal izango du.

6.6 ERANTZUKIZUNAK BEREIZTEA

Ermuko Udalak erantzukizunak bereizteko beharra hartuko du kontuan bere informazio-sisteman, ahal den guztietan. Segurtasun Politika honetan zehar zehaztuko dira arduradun bakoitzaren eskuduntzen xehetasuna, koordinazio-mekanismoak eta gatazken ebazpena.

7. GUTXIENEO ESKAKIZUNAK

Informazioaren Segurtasun Politika honek osatu egiten ditu **Ermuko Udalak** datu pertsonalak babesteko dituen gainerako segurtasun-politikak.

Informazioaren Segurtasun Politika garatzeko, gutxieneko eskakizun hauek aplikatuko dira:

- Segurtasun-prozesua antolatu eta ezartzea, **Politika honen 8. atalean** zehaztutako antolamendu-esparruaren arabera.
- Arriskuen analisia eta kudeaketa, **PO.SEG.01 Arriskuen kategorizazioa eta analisia** prozeduran aurreikusitakoaren arabera.
- Pertsonen kudeaketa, **PO.SEG.11 Langileen kudeaketa eta prestakuntza** prozeduran aurreikusitakoaren arabera.
- Profesionaltasuna, **PO.SEG.11 Langileen kudeaketa eta prestakuntza** prozeduran aurreikusitakoaren arabera.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	08/05/2025

- Sarbideak baimendu eta kontrolatzea, **PO.SEG.05 Sarbideen kontrola** prozeduran aurreikusitakoaren arabera.
- Instalazioen babesa, **PO.SEG.07 Segurtasun fisikoa** prozeduran aurreikusitakoaren arabera.
- Produktuak eskuratzea, **PO.SEG.03 Hornitzaileen kudeaketa** prozeduran aurreikusitakoaren arabera.
- Segurtasun lehenetsia, **PO.SEG.12 Ekipamenduen babesa** prozeduran aurreikusitakoaren arabera.
- Sistemaren osotasuna eta eguneratzea, **PO.SEG.12 Ekipamenduen babesa** prozeduran aurreikusitakoaren arabera.
- Biltegiaritutako eta iragaitzazko informazioaren babesa, **PO.SEG.08 Informazioaren babesa** prozeduran aurreikusitakoaren arabera.
- Interkonektatutako beste informazio-sistema batzuen aurreko prebentzioa, **PO.SEG.14 Komunikazioen eta zerbitzuen segurtasuna** prozeduran aurreikusitakoaren arabera.
- Jardueraren erregistroa, **PO.SEG.02 Jarduera-erregistroen kudeaketa** prozeduran aurreikusitakoaren arabera.
- Segurtasun-gorabeherak, **PO.SEG.06 Gorabeheren kudeaketa** prozeduran aurreikusitakoaren arabera.
- Jardueraren jarraipena, **PO.SEG.09 Inpaktu-analisia** prozeduran aurreikusitakoaren arabera.
- Segurtasun-prozesuaren etengabeko hobekuntza, **PO.SEG.15 ISKSaren (Informazioaren segurtasuna kudeatzeko sistemaren) kudeaketa** prozeduran aurreikusitakoaren arabera.

8. SEGURTASUNAREN ANTOLAMENDUA

Ermuko Udalean Segurtasun Politika ezartzeko, erakundeko kide guztiek ulertu behar dituzte beren betebeharrak eta erantzukizunak, betetzen duten lanpostuaren arabera. Informazioaren Segurtasun Politikaren zati diren aldetik, berariazko rol bakoitzak —erabiltzaile zehatzetan pertsonalizatuta— bere ekintzen inplikazioak eta esleitura dituen erantzukizunak ulertu behar ditu. Atal honetan identifikatu eta zehazten dira, honela multzokatuta:

- a) Informazioaren Segurtasun Batzordea
- b) Zerbitzu-arduradunak
- c) Informazio-arduradunak
- d) Informazioaren segurtasun-arduraduna
- e) Sistema-arduraduna
- f) Datuak babesteko ordezkaria

Hurrengo ataletan, rol horietako bakoitzari esleitutako eginkizunak zehazten dira.

8.1 INFORMAZIOAREN SEGURTASUN BATZORDEA

Informazioaren Segurtasun Batzordeak informazioaren segurtasuna koordinatzen du **Ermuko Udalean**. Batzordea lehenago aipaturiko figurek osatzen dute.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

Informazioaren Segurtasun Batzordeak funtzio hauek ditu:

- Informazioaren eta erantzukizun nagusien Segurtasun Politika berrikusi eta onartzea.
- Informazioaren segurtasunaren estrategia eta plangintza zehaztu eta bultzatzea, eta aurrekontu eta baliabide zehatzen esleipena proposatzea.
- Informazio-aktiboak mehatxu nagusien eraginpean jartzearen ondoriozko aldaketa esanguratsuak gainbegiratu eta kontrolatzea, eta aktibo horien segurtasuna bermatzeko kontrolak eta neurriak garatu eta ezartzea.
- Informazioaren Segurtasuna hobetzeko ekimen nagusiak onartzea.
- Alderdi hauek gainbegiratu eta jarraitzea:
 - Informazioaren Segurtasuneko gorabehera nagusiak
 - Jarraipen-planak egin eta eguneratzea
 - Segurtasun Politikak bete eta hedatzea
- Arduradunen artean agertzen diren erantzukizun-gatazkak konpontzea, eta erabakitze behar besteko aginpiderik ez duenean, kasua goiko estamentuetara igotzea.

8.1.1 Informazio-arduraduna

- Kudeatutako informazioaren segurtasun-eskakizunak ezartzeko ahalmena du. Informazio horrek datu pertsonalak baditu, kontuan hartu beharko dira datuak babesteko legeriaren ondoriozko eskakizunak.
- Informazioaren segurtasun-mailak zehazten ditu.

8.1.2 Zerbitzu-arduraduna

- Ematen diren zerbitzuen segurtasun-baldintzak ezartzeko ahalmena du.
- Zerbitzuaren segurtasun-mailak zehazten ditu.

8.1.3 Informazioaren segurtasun-arduraduna

Informazioaren segurtasun-baldintzak zehazteaz, koordinatzeaz, ezartzeaz eta betetzen direla egiaztatzeaz arduratzen da, erakundearen helburu estrategikoei jarraikiz.

Segurtasun-arduraduna harremanetarako pertsona edo puntua **(PoC)** da.

Funtzio hauek ditu informazioaren segurtasun-arduradunak:

- Segurtasun Batzordearen bilerak zuzentzea, eta horien jardura eta erabakiak ezagutarazi, proposatu eta koordinatzea.
- **Ermuko Udalaren** informazioaren segurtasunerako eta datuen babeserako neurriak koordinatu eta kontrolatzea.
- Honako hauek ezartzen direla gainbegiratzeko, mantentzeko, kontrolatzeko eta betetzen direla egiaztatzea:





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	08/05/2025

- Segurtasun Batzordeak zehaztutako informazioaren segurtasun-estrategia.
- **Ermuko Udalaren** Informazioaren Segurtasun Politikan eta hura garatzeko araudian jasotako arauak eta prozedurak.
- **Ermuko Udaleko** segurtasun informatikoko gorabeherak gainbegiratzea (azken arduraduna den aldetik).
- **Ermuko Udalaren** Informazioaren Segurtasun Politikan eta hura garatzeko araudian jasotako arau eta prozedurak **Ermuko Udalean** zabaltzea, bai eta **Ermuko Udal** osoak informazioaren segurtasunaren arloan dituen eginkizun eta betebeharrak ere.
- Segurtasun Politika, garapen-araudia eta aplikatu beharreko legeak (adibidez, DBEOa) zenbateraino betetzen diren egiaztatze behar diren barne- edo kanpo-auditoretzak gainbegiratu eta haietan laguntzea.
- Informazioaren segurtasunari buruzko aholkuak ematea **Ermuko Udaleko** arlo operatiboei.

8.1.4 Sistema-arduraduna

Ermuko Udalaren jardueraren euskarri diren informazio-sistemen aktibo eta zerbitzuak bermatzeko neurriak betetzen direla ziurtatzeko azken arduraduna da, **Ermuko Udalaren** helburu estrategikoekin bat.

Informazioaren sistema-arduradunak funtzio hauek ditu:

- **Ermuko Udalaren** aktiboen segurtasunaren kudeaketa pertsonifikatzeaz arduratzen diren arduradun tekniko informatikoak hautatu eta horiei funtzioak eta betebeharrak ezartzea, zehaztutako segurtasun-estrategiari jarraikiz.
- Arduradun tekniko informatikoen jardura ezartzea, dagozkien segurtasun-inguruneetan.
- **Ermuko Udalaren** informazio-sistemen aktiboen inbentarioa eguneratzen dela bermatzea.
- Inbentariatutako aktibo bakoitzak segurtasun informatikoko maila egokia duela ziurtatzea, eta beharrezko babes-maila bermatzeko kontrol eta neurrien garapen, ezarpen, egokitzapen eta eragiketa zuzena koordinatzea.
- Sistema berriak ezartzean eta daudenak aldatzean, **Ermuko Udalak** ezarritako segurtasun-eskakizunak betetzen direla bermatzea.
- Segurtasunaren egoera monitorizatzeko prozesuak eta kontrolak ezartzea, sortzen diren gorabeherak detektatzeko eta horien ikerketa eta konponketa koordinatzeko.
- Informazio-sistemen segurtasun-gidalerroak eta -politikak eta horiei lotutako araudiak mantendu eta eguneratzea.

8.1.5 Datuak babesteko ordezkaria

DBEOaren 39.artikuluaren aurreikusitakoaren arabera, honako hauek dira datuak babesteko ordezkariaren eginkizunak:





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	08/05/2025

- Dagozkien betebeharrei buruzko informazioa eta aholkularitza ematea tratamenduaren erantzuleari edo arduradunari eta tratamenduaz arduratzen diren langileei, DBEOarekin eta Europar Batasuneko edo estatu kideetako datuak babesteko beste xedapen batzuekin bat.
- DBEOaren xedapenak, Europar Batasuneko edo estatu kideetako datuak babesteko gainerako xedapenak eta datu pertsonalak babesteko tratamenduaren erantzulearen edo arduradunaren politikak betetzen dela gainbegiratzea, barne hartuta erantzukizunen esleipena, tratamendu-eragiketetan parte hartzen duten langileen kontzientziazioa eta prestakuntza, eta dagozkion auditoretzak.
- Datuen babesaren gaineko inaktuaren ebaluazioari buruz eskatzen zaion aholkularitza eskaintzea eta horren aplikazioa gainbegiratzea.
- Kontrol-agintaritzarekin elkarlanean aritzea.
- Kontrol-agintaritzaren harremanetarako pertsona izatea, tratamenduari dagozkion gaietarako eta, hala badagokio, beste edozein gairi buruzko kontsultak egiteko.
- Tratamendu-eragiketei lotutako arriskuei behar bezalako arreta jarritz beteko ditu bere eginkizunak, tratamenduaren izaera, irismena, testuingurua eta helburuak kontuan hartuta.

8.1.6 Idazkaritza Teknikoa

- Bileren gai-zerrenda prestatzea, bilera horiek deitzea eta informazioaren segurtasunerako batzordearen saioak dinamizatzea.
- Akordioak eta zereginak aktan jasotzea, arduradunekin eta epeekin.
- Segurtasuneko arduradunarekin lankidetzan aritzea Informazioaren Segurtasun Politikan eta garapen-araudian jasotako arauak eta prozedurak Udalean bertan zabaltzeko, bai eta langile guztiek informazioaren segurtasunaren arloan dituzten eginkizun eta betebeharrei dagokienez ere.
- Segurtasun Politika, garapen-araudia eta aplikatzekoak diren legeak, hala nola DBEO, zenbateraino betetzen diren egiaztatzeko beharrezkoak diren barneko edo kanpoko auditoretzetan laguntzea.

8.2 IZENDATZEKO PROZEDURAK

Erantzukizun hauek izendatu dira:

- Zerbitzu-arduraduna:
 - Rosalía Herrera. Zuzendari orokorra
 - Nagore Domínguez. Alorreko zuzendaria
 - Josu Ansola. Alorreko zuzendaria
 - David Henares. Alorreko zuzendaria
 - Javier García Pizarro. Udaltzaingoko burua
 - Leire Moya. Alorreko zuzendaria
 - Josu Macías. Kiroletako arduraduna
 - Jon Ajuria (Kontu-hartzailea) / Mónica López (Diruzaina)
- Informazio-arduraduna: Zerbitzu-arduradun rola duten pertsona berak.
- Segurtasun-arduraduna: Antonio Bernal Calles. Teknologiako arduraduna
- Sistema-arduraduna: Juan Agustín Villafranca. Udal idazkaria
- Datuak babesteko ordezkaria: Montserrat Gutiérrez Aranbarri
- Idazkaritza Teknikoa: Montserrat Gutiérrez Aranbarri. Kalitate teknikaria





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

Izendapenak 2 urtean behin berrikusiko dira, edo posturen bat hutsik geratzen denean.

8.3 GATAZKAK KONPONTZEA

Espainiako herri-administrazioetan indarrean dagoen hierarkia-printzipioaren arabera, erakundeko arduradunen eta/edo zerbitzuen arteko gatazkarik izanez gero, Segurtasun Batzordeak ebatzi beharko du. Horrelakorik ezean, alkatearen erabakia nagusituko da.

Eztabaida horiek ebazterakoan, kontuan hartuko dira beti datu pertsonalak babestearen ondoriozko eskakizunak.

9. INFORMAZIOAREN SEGURTASUN POLITIKA BERRIKUSTEA

Segurtasun Batzordearen eginkizuna izango da Informazioaren Segurtasun Politika urtero berrikustea, eta politika hori berrikusteko edo mantentzeko proposamena egitea. Politika zabaldu egingo da, eragindako alderdi guztiek ezagutu dezaten.

10. DATU PERTSONALAK

Ermuko Udalak datu pertsonalak tratatuko ditu.

Ermuko Udalaren informazio-sistema guztiek Izaera Pertsonaleko Datuak Babesteari buruz indarrean dagoen araudiak eskatzen dituen segurtasun-mailak beteko dituzte. Araudi hori ikusgai dago Informazioaren Segurtasun Politikaren **5. Arau-esparrua** atalean.

11. ARRISKUEN KUDEAKETA

Informazioaren Segurtasun Politika honi lotutako sistema guztiei arriskuen ebaluazio egin behar zaie aldian-aldian. Analisi hori errepikatuko da:

- Erregularitasunez, urtean behin gutxienez.
- Kudeatu beharreko informazioa aldatzen denean.
- Ematen diren zerbitzuak aldatzen direnean.
- Segurtasun-gorabehera larri bat gertatzen denean.
- Ahulezia larrien berri ematen denean.

Arrisku-analisiak harmonizatzeko, Segurtasun Batzordeak erreferentziazko balorazio bat ezarriko du, kudeatu beharreko informazio-mota desberdinetarako eta ematen diren zerbitzuetarako. Segurtasun Batzordeak baliabideen eskuragarritasuna dinamizatuko du sistemen segurtasun-beharrei erantzuteko, eta inbertsio horizontalak sustatuko ditu.

12. DOKUMENTAZIOA EGITURATZEA

PO.SEG.16 ISKSaren kudeaketa prozeduran zehazten dira **Ermuko Udalaren** ISKSaren segurtasun-dokumentazioa egituratu, kudeatu eta eskuratzeko jarraibideak.

Informazioaren segurtasunaren arloko arau-esparru bat ezarri da, hainbat mailatan egituratua, erakundearen Segurtasun Politikan ezarritako printzipioek eta helburuek berariazko garapena izan dezaten:

- Lehen maila: Informazioaren Segurtasun Politika, alkateak onartu behar duena, Segurtasun Batzordeak proposatuta.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	08/05/2025

- Bigarren maila: alkateak onartutako informazioaren segurtasun-araudia. Bertan, informazio-sistemak behar bezala erabiltzeko arauak ezarriko dira.
- Hirugarren maila: informazioaren segurtasun-prozedurak. Horietan, prozesu jakin batzuk egiteko modu zuzena zehaztuko da, segurtasuna eta informazioa une oro babesteko. Prozedura horiek Segurtasun Batzordeak onartu behar ditu.
- Laugarren maila: segurtasun-estandarrak, jarraibide teknikoak, jardunbide egokiak, gomendioak, gidak, prestakuntza-ikastaroak, aurkezpenak eta abar. Segurtasun Batzordeak onartu behar ditu.

ISKSa osatzen duten dokumentuak euskarri digitalean daude, lanpostuarekin lotutako eginkizunak betetzeko behar dituzten langile guztien eskura. Kontsultatzeko eskuragarri egongo da, baina ezin izango da aldaketarik egin.

13. INFORMAZIOAREN KALIFIKAZIOA

Ermuko Udalaren informazioa kalifikatzeko, Espainia kide duten nazioarteko lege eta itunetan legez ezarritakoa eta, gai sailkatuen kasuan, aplikatu beharreko araudia hartuko dira kontuan.

Bai sistemak erabiltzen duen informazio bakoitzaren arduraduna, bai informazioa kalifikatzeko irizpideak —beharrezko segurtasun-maila zehaztuko dutenak— **PO.SEG.10 Informazioaren sailkapena** prozeduran ezarri dira.

14. LANGILEEN BETEBEHARRAK

Ermuko Udalaren informazio-sistemen erabiltzaile guzti-guztiak dira informazio-aktiboen segurtasunaren eta horiek behar bezala erabiltzearen erantzule, betiere beren eskumen profesionalen eta akademikoen arabera.

Ermuko Udaleko kide guztiek Informazioaren Segurtasun Politika eta Segurtasun Araudia ezagutzeko eta betetzeko betebeharra dute, eta Segurtasun Batzordearen ardura da informazioa dagokienengana iristeko behar diren baliabideak jartzea.

Ermuko Udaleko kideek gutxienez urtean behin jasoko dute informazioaren segurtasunari buruzko prestakuntza. Etengabe kontzientziazteko programa bat ezarriko da, **Ermuko Udaleko** kide guztiei arreta emateko, batez ere sartu berriei.

IKT sistemak erabiltzeko, horiekin lan egiteko edo administratzeko erantzukizuna duten pertsonak prestakuntza jasoko dute sistemak segurtasunez erabiltzeko, beren lana egiteko behar duten neurrian. Prestakuntza derrigorrezkoa izango da langilearentzat, erantzukizun bat bere gain hartu aurretik, bai lehenengo esleipena badu, bai lanpostuz edo lanpostu berean erantzukizunez aldatu behar badu.

14.1 EZ-BETETZEA

Informazioaren Segurtasun Politika hau betetzen ez bada, bidezko diziplina-neurriak hartu ahal izango dira, dagozkion legezko erantzukizunak alde batera utzi gabe.

15. HIRUGARREN ALDERDIAK

Zerbitzu bat emateko **Ermuko Udalarekin** lankidetzan diharduten kanpoko enpresa eta erakundeek, baldin eta **Ermuko Udalaren** edo bere erabiltzaileen informazio-aktiboak zuzenean edo zeharka (norberaren edo besteren sistemetan) eskuratu edo kudeatzen badituzte, **Ermuko**





ERMUKO UDALA

AYUNTAMIENTO DE ERMUA

INFORMAZIOAREN SEGURTASUN POLITIKA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

08/05/2025

Udalaren sistemen eta aktiboen segurtasuna bermatzeko erantzukizuna partekatuko dute, eta, beraz, betebeharrak izango dituzte:

- **Ermuko Udalari** emandako zerbitzuei buruzko informaziorik ez zabaltzea, horretarako berariazko baimenik izan ezean.
- Politika honetan ezarritako betebeharren inguruan informatzea eta langileen artean informazio hori zabaltzea.
- DBEOak ezarritako neurriak aplikatzea **Ermuko Udalaren** ardurapeko datu pertsonalen tratamenduan, baldin eta datu horiek zerbitzua ematean tratatzen badira.
- **Ermuko Udalari** emandako zerbitzuekin lotutako segurtasuna kudeatzeko prozedurak aplikatzea. Bereziki, erabiltzaileen kudeaketarekin lotutako prozedurak aplikatu behar dira, hala nola alten eta baje jakinarazpenak, erabiltzaileen identifikazioa eta pasahitzen kudeaketa, politika honetan eta aplikatu beharreko araudi erregulatzailan deskribatutakoaren arabera.
- **Ermuko Udalaren** sistema edo aktiboren baten segurtasuna mehatxatzen duen edozein gorabehera edo susmo jakinaraztea, zehaztutako mekanismoen bidez, eta erakundeko sistema, zerbitzu edo langileekin zerikusia duten gorabehera edo susmo horiek konpontzen laguntzea.
- Neurriak ezartzea beren sistema eta sare propioetan, **Ermuko Udalaren** sistemetan birusak eta/edo kode gaiztoak ez hedatzeko. Zehazki, **Ermuko Udalaren** sare korporatibora konektatutako edozein ekipamenduk antibirus eguneratua izan behar du, ahal dela automatikoki eguneratzen dena.
- Beren sistema eta sareetan neurriak ezartzea, **Ermuko Udalaren** sistemetara beste sare batzuetatik baimenik gabe ez sartzeko. Besteak beste, segurtasun-eguneraketak aplikatu behar dituzte beren sistemetan, eta suebaki-sistema bat mantendu, Interneteko konexioak eta fidagarriak ez diren beste sare batzuetakoak babesteko.

Aurreko betebeharrak betetzen ez badira, kanpoko erakundearekiko harremana berrikusteko eskubidea izango du **Ermuko Udalak**.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

1. APROBACIÓN Y ENTRADA EN VIGOR

Esta Política de Seguridad de la Información entrará en vigor el día posterior a la fecha de la firma del decreto de alcaldía y hasta que sea reemplazada por una nueva política.

2. INTRODUCCIÓN

El Ayuntamiento de Ermua depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada a los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que se deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de los servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

El Ayuntamiento de Ermua debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos TIC.

El Ayuntamiento de Ermua debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

3. ALCANCE

Esta Política de seguridad será de obligado cumplimiento para todos los miembros del **Ayuntamiento de Ermua**, de acuerdo con el alcance:

- Los sistemas de información que dan soporte a todos los servicios prestados por el **Ayuntamiento de Ermua**, de acuerdo con las disposiciones del RD 311/2022 y la declaración de aplicabilidad vigente.

4. MISIÓN

La misión del **Ayuntamiento de Ermua** es ofrecer servicios públicos desde lo local que respondan a las necesidades, expectativas, retos, oportunidades de la ciudad y de las personas que conviven en ella. Trabajamos en redes obteniendo financiación y generando y compartiendo conocimiento. Además, impulsamos activamente el desarrollo social y la sostenibilidad económica y medioambiental. Lo hacemos trabajando en equipo, con calidad, método, eficiencia e





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

innovación, con actitud de respeto, escucha, transparencia, favoreciendo el crecimiento integral de las personas de la organización.

5. MARCO NORMATIVO

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, modificada por la ley 11/1999, de 21 de abril.
- Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.
- Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.
- Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
- Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).
- Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos.
- Ley 57/2003, de 16 de diciembre, de medidas para la modernización del gobierno local
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula el documento nacional de identidad y sus certificados de firma electrónica.
- Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la sociedad de la Información.
- Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

6. PRINCIPIOS BÁSICOS

Los principios básicos son las directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

6.1 Seguridad como proceso integral

La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con los sistemas TIC, procurando evitar cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas TIC.

6.2 Gestión de la seguridad basada en los riesgos

El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	15/01/2024

medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

6.3 Prevención, detección, respuesta y conservación

6.3.1 Prevención

El **Ayuntamiento de Ermua** debe evitar, o al menos prevenir en la medida de lo posibles, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evolución de amenazas y riesgos. Estos controles, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, el servicio de Tecnología debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

6.3.2 Detección

El **Ayuntamiento de Ermua**, establece controles de operación de sus sistemas de información con el objetivo de detectar anomalías en la prestación de los servicios y actuar en consecuencia según lo dispuesto en el artículo 10 del ENS (vigilancia continua y reevaluación periódica). Cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales (conforme a lo indicado en el artículo 9 del ENS, Existencia de líneas de defensa), se establecerán los mecanismos de detección, análisis y reporte necesarios para que lleguen a los responsables regularmente

6.3.3 Respuesta

El **Ayuntamiento de Ermua**:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa puntos de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

6.3.4 Recuperación

Para garantizar la disponibilidad de los servicios, el **Ayuntamiento de Ermua**, dispone de los medios y técnicas necesarias que permiten garantizar la recuperación de los servicios más críticos.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

6.4 Existencia de líneas de defensa

El sistema de información dispondrá de una estrategia de protección constituida por diferentes capas, de forma que cuando una de las capas sea comprometida, permita desarrollar una acción adecuada frente a los incidentes que no han podido evitarse, reduciendo la probabilidad del que el sistema sea comprometido en su conjunto, minimizando el impacto final sobre el mismo.

Existirán líneas de defensa constituidas tanto por medidas organizativas, físicas y lógicas.

6.5 Vigilancia continua y reevaluación periódica

El **Ayuntamiento de Ermua** llevará a cabo una vigilancia continua que permita la detección de actividades o comportamientos anómalos y su oportuna respuesta.

La evaluación permanente del estado de la seguridad de los activos permite al **Ayuntamiento de Ermua** medir su evolución, detectando vulnerabilidades e identificando deficiencias de configuración.

El **Ayuntamiento de Ermua** reevaluará y actualizará periódicamente las medidas de seguridad, adecuando su eficacia a la evolución de los riesgos y los sistemas de protección, pudiendo llegar a un replanteamiento de la seguridad, si fuese necesario.

6.6 Diferenciación de responsabilidades

El **Ayuntamiento de Ermua** tendrá en cuenta la diferenciación de responsabilidades en su sistema de información siempre que sea posible. El detalle de las atribuciones de cada responsable, los mecanismos de coordinación y la resolución de conflictos se detallarán a lo largo de la presente política de seguridad.

7. REQUISITOS MÍNIMOS

Esta política de seguridad de la Información complementa las políticas de seguridad del **Ayuntamiento de Ermua** en materia de protección de datos de carácter personal.

Esta Política de Seguridad de seguridad se desarrollará aplicando los siguientes requisitos mínimos:

- Organización e implantación del proceso de seguridad, de acuerdo al marco organizativo definido en el **apartado 8 de esta Política**.
- Análisis y gestión de los riesgos, de acuerdo a lo previsto en el procedimiento **PO.SEG.01 Categorización y Análisis de Riesgos**.
- Gestión de personal, de acuerdo a lo previsto en el procedimiento **PO.SEG.11 Gestión de personal y formación**.
- Profesionalidad, de acuerdo a lo previsto en el procedimiento **PO.SEG.11 Gestión de personal y formación**.
- Autorización y control de los accesos, de acuerdo a lo previsto en el procedimiento **PO.SEG.05 Control de accesos**.
- Protección de las instalaciones, de acuerdo a lo previsto en el procedimiento **PO.SEG.07 Seguridad Física**.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

- Adquisición de productos, de acuerdo a lo previsto en el procedimiento **PO.SEG.03 Gestión de proveedores.**
- Seguridad por defecto, de acuerdo a lo previsto en el procedimiento **PO.SEG.12 Protección de equipos.**
- Integridad y actualización del sistema, de acuerdo a lo previsto en el procedimiento **PO.SEG.12 Protección de equipos.**
- Protección de la información almacenada y en tránsito, de acuerdo a lo previsto en el procedimiento **PO.SEG.08 Protección de la información**
- Prevención ante otros sistemas de información interconectados, de acuerdo a lo previsto en el procedimiento **PO.SEG.14 Seguridad de comunicaciones y servicios.**
- Registro de actividad, de acuerdo a lo previsto en el procedimiento **PO.SEG.02 Gestión de registros de actividad.**
- Incidentes de seguridad, de acuerdo a lo previsto en el procedimiento **PO.SEG.06 Gestión de incidentes.**
- Continuidad de la actividad, de acuerdo a lo previsto en el procedimiento **PO.SEG.09 Análisis de impacto**
- Mejora continua del proceso de seguridad, de acuerdo a lo previsto en el procedimiento **PO.SEG.15 Gestión del SGSI.**

8. ORGANIZACIÓN DE LA SEGURIDAD

La implantación de la Política de Seguridad en el **Ayuntamiento de Ermua** requiere que todos los miembros de la organización entiendan sus obligaciones y responsabilidades en función del puesto desempeñado. Como parte de la Política de Seguridad de la Información, cada rol específico, personalizado en usuarios concretos, debe entender las implicaciones de sus acciones y las responsabilidades que tiene atribuidas, quedando identificadas y detalladas en esta sección, y que se agrupan del modo siguiente:

- g) El Comité de Seguridad de la Información
- h) Responsables del Servicio
- i) Responsables de la Información
- j) Responsable de Seguridad de la Información
- k) Responsable de Sistemas
- l) Delegado de protección de datos

En los siguientes apartados se especifican las funciones atribuidas a cada uno de estos roles.

8.1 Comité de seguridad de la información

El Comité de Seguridad de la Información coordina la seguridad de la información en el **Ayuntamiento de Ermua**. Dicho Comité está compuesto por cada una de las figuras anteriormente mencionadas.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

Las funciones del Comité de Seguridad de la Información son las siguientes:

- Revisión y aprobación de la Política de Seguridad de la Información y de las responsabilidades principales;
- Definir e impulsar la estrategia y la planificación de la seguridad de la información proponiendo la asignación de presupuesto y los recursos precisos.
- Supervisión y control de los cambios significativos en la exposición de los activos de información a las amenazas principales, así como del desarrollo e implantación de los controles y medidas destinados a garantizar la Seguridad de dichos activos;
- Aprobación de las iniciativas principales para mejorar la Seguridad de la Información.
- Supervisión y seguimiento de aspectos tales como:
 - Principales incidencias en la Seguridad de la Información;
 - Elaboración y actualización de planes de continuidad
 - Cumplimiento y difusión de las Políticas de Seguridad
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

8.1.1 Responsable de la Información

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de la información gestionada. Si esta información incluye datos de carácter personal, además deberán tenerse en cuenta los requisitos derivados de la legislación correspondiente sobre protección de datos
- Determina los niveles de seguridad de la información.

8.1.2 Responsable del Servicio

- Tiene la potestad de establecer los requisitos, en materia de seguridad, de los servicios prestados.
- Determina los niveles de seguridad del servicio.

8.1.3 Responsable de Seguridad de la Información

Responsable de la definición, coordinación, implantación y verificación de cumplimiento de los requisitos de seguridad de la información definidos de acuerdo con los objetivos estratégicos de la organización.

El/La Responsable de Seguridad es el Punto de Contacto (**PoC**).

Las funciones del/ de la Responsable de Seguridad de la Información son las siguientes:

- Dirigir las reuniones del Comité de Seguridad, informando, proponiendo y coordinando sus actividades y decisiones.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

- Coordinar y controlar las medidas de seguridad de la información y de protección de datos del **Ayuntamiento de Ermua**.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de:
 - La estrategia de seguridad de la información definida por el Comité de Seguridad.
 - Las normas y procedimientos contenidos en la Política de Seguridad de la Información del **Ayuntamiento de Ermua** y normativa de desarrollo.
- Supervisar (como responsable último) los incidentes de seguridad informática producidas en el **Ayuntamiento de Ermua**.
- Difundir en el **Ayuntamiento de Ermua** las normas y procedimientos contenidos en la Política de Seguridad de la Información del **Ayuntamiento de Ermua** y normativa de desarrollo, así como las funciones y obligaciones de todo el **Ayuntamiento de Ermua** en materia de seguridad de la información.
- Supervisar y colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.
- Asesorar en materia de seguridad de la información a las diferentes áreas operativas del **Ayuntamiento de Ermua**.

8.1.4 Responsable del Sistema

Es responsable último de asegurar la ejecución de medidas para asegurar los activos y servicios de los Sistemas de Información, que soportan la actividad del **Ayuntamiento de Ermua**, de acuerdo a los objetivos estratégicos del **Ayuntamiento de Ermua**.

Las funciones del Responsable de Sistemas de la Información son las siguientes:

- Seleccionar y establecer las funciones y obligaciones a los Responsables Técnicos Informáticos encargados de personificar una gestión de la seguridad de los activos del **Ayuntamiento de Ermua**, conforme a la estrategia de seguridad definida.
- Establecer la actuación de los Responsables Técnicos Informáticos, en los distintos entornos de seguridad que se designen.
- Garantizar la actualización del inventario de activos de Sistemas de Información del **Ayuntamiento de Ermua**.
- Asegurar que existe el nivel de seguridad informática adecuado para cada uno de los activos inventariados, coordinando el correcto desarrollo, implantación, adecuación y operación de los controles y medidas destinados a garantizar el nivel de protección requerido.
- Garantizar que la implantación de nuevos sistemas y de los cambios en los existentes cumple con los requerimientos de seguridad establecidos en el **Ayuntamiento de Ermua**.
- Establecer los procesos y controles de monitorización del estado de la seguridad que permitan detectar las incidencias producidas y coordinar su investigación y resolución.





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

- Mantener y actualizar las directrices y políticas de seguridad de los Sistemas de Información y normativa asociada.

8.1.5 Delegado/a de Protección de datos

De acuerdo a lo previsto en el artículo 39 del RGPD, las funciones de la persona Delegada de Protección de Datos son las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del RGPD y de otras disposiciones de protección de datos de la Unión o de los Estados miembros.
- Supervisar el cumplimiento de lo dispuesto en el RGPD, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la autoridad de control.
- Actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, y realizar consultas, en su caso, sobre cualquier otro asunto.
- Desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

8.1.6 Secretaría Técnica

- Preparar el orden del día de las reuniones, convocar dichas reuniones y dinamizar las sesiones del comité de Seguridad de la información.
- Recoger en acta los acuerdos y tareas, con responsables y plazos.
- Colaborar con la persona responsable de Seguridad en la difusión en el propio Ayuntamiento de las normas y procedimientos contenidos en la Política de Seguridad de la Información y normativa de desarrollo, así como en lo que respecta a las funciones y obligaciones de todo el personal en materia de seguridad de la información.
- Colaborar en las Auditorías internas o externas necesarias para verificar el grado de cumplimiento de la Política de Seguridad, normativa de desarrollo y leyes aplicables tales como el RGPD.

8.2 Procedimientos de designación

Se designan las siguientes responsabilidades:

- **Responsable del Servicio**
 - Rosalía Herrera. Directora general





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA	BERTSIOA	DATA
ENS.01	1.0	15/01/2024

- Nagore Domínguez. Directora de área
- Josu Ansola. Director de área
- David Henares. Director de área
- Javier García Pizarro. Jefe de la Policía local
- Leire Moya. Directora de área
- Josu Macías. Responsable de Deportes
- Jon Ajuria (Interventor) / Mónica López (Tesorera)
- **Responsable de la Información.** Las mismas personas que tienen rol de responsable de servicio
- **Responsable de Seguridad:** Antonio Bernal Calles. Responsable de tecnología
- **Responsable del Sistema:** Juan Agustín Villafranca. Secretario municipal
- **Delegado/a de Protección de Datos:** Montserrat Guiérrez Aranbarri
- **Secretaría Técnica:** Montserrat Gutiérrez Aranbarri. Técnica de calidad

Los nombramientos se revisarán cada 2 años o cuando alguno de los puestos quede vacante.

8.3 Resolución de conflictos

De acuerdo con el Principio de Jerarquía que rige en las administraciones públicas españolas, en caso de conflicto entre los diferentes responsables y/o entre diferentes servicios de la entidad, éste será resuelto por el Comité de Seguridad. En defecto de lo anterior, prevalecerá la decisión del/ de la Alcalde/sa.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

9. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será difundida para que la conozcan todas las partes afectadas.

10. DATOS DE CARÁCTER PERSONAL

Ayuntamiento de Ermua trata datos de carácter personal.

Todos los sistemas de información de **Ayuntamiento de Ermua** se ajustarán a los niveles de seguridad requeridos por la normativa vigente en materia de Protección de Datos de Carácter Personal, identificada en el apartado **5. Marco Normativo**, de la presente Política de Seguridad de la Información.

11. GESTIÓN DE RIESGOS

Para todos los sistemas sujetos a esta Política de Seguridad de la Información debe realizarse periódicamente una evaluación de los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año
- Cuando cambie la información gestionada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

- Cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información gestionados y los diferentes servicios prestados. El Comité de Seguridad dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

12. ESTRUCTURACIÓN DE LA DOCUMENTACIÓN

Las directrices para la estructuración, gestión y acceso a la documentación de seguridad del SGSI de **Ayuntamiento de Ermua**, se definen en el procedimiento **"PO.SEG.16 Gestion del SGSI"**.

Se ha establecido un marco normativo en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por el/la Alcalde/sa a propuesta del Comité de Seguridad.
- Segundo nivel: la normativa de seguridad de la información aprobada por el Alcalde. En ella se establecerán unas normas de uso aceptable de los sistemas de información.
- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información. Estos procedimientos han de ser aprobados por el Comité de Seguridad.
- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc. Ha de ser aprobada por el Comité de Seguridad.

Los documentos que integran el SGSI se encuentran, en soporte digital, a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo. Estará disponible para su consulta, sin posibilidad de modificación.

13. CALIFICACIÓN DE LA INFORMACIÓN

Para calificar la información del **Ayuntamiento de Ermua** atenderá a lo establecido legalmente por las leyes y tratados internacionales de los que España es miembro y su normativa de aplicación cuando se trate de materias clasificadas.

Tanto el responsable de cada información manejada por el sistema como los criterios de calificación de la información, que determinarán el nivel de seguridad requerido, se establecen en el procedimiento **PO.SEG.10 Clasificación de la información**.

14. OBLIGACIONES DEL PERSONAL

Todos y cada uno de los usuarios de los sistemas de información del **Ayuntamiento de Ermua** son responsables de la seguridad de los activos de información mediante un uso correcto de los mismos, siempre de acuerdo con sus atribuciones profesionales y académicas.

Todos los miembros del **Ayuntamiento de Ermua** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Los miembros del **Ayuntamiento de Ermua** recibirán formación en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros del **Ayuntamiento de Ermua**, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

14.1 Incumplimiento

El incumplimiento de la presente Política de Seguridad de la Información podrá acarrear el inicio de las medidas disciplinarias que procedan, sin perjuicio de las responsabilidades legales correspondientes.

15. TERCERAS PARTES

Las empresas y organizaciones externas que, con ocasión de su colaboración con el **Ayuntamiento de Ermua** para la prestación de un servicio, accedan o gestionen activos de información del **Ayuntamiento de Ermua** o de sus usuarios, directa o indirectamente (en sistemas propios o ajenos), comparten la responsabilidad de mantener la seguridad de los sistemas y activos del **Ayuntamiento de Ermua**, por lo que deberán asumir las siguientes obligaciones:

- No difundir ninguna información relativa a los servicios proporcionados al **Ayuntamiento de Ermua** sin autorización expresa para ello.
- Informar y difundir a su personal las obligaciones establecidas en esta Política.
- Aplicar las medidas estipuladas por RGPD en el tratamiento de los datos personales responsabilidad del **Ayuntamiento de Ermua** que traten por razón de la prestación del servicio.
- Aplicar los procedimientos para la gestión de seguridad relacionados con los servicios proporcionados al **Ayuntamiento de Ermua**. Especialmente se deben aplicar los procedimientos relacionados con la gestión de usuarios, tales como notificaciones de altas y bajas, identificación de los usuarios, gestión de contraseñas, etc., en el sentido descrito en la presente política y normativa reguladora que sea de aplicación.
- Notificar cualquier incidencia o sospecha de amenaza a la seguridad de algún sistema o activo del **Ayuntamiento de Ermua** a través de los mecanismos que se determinen, colaborando en la resolución de las mismas relacionados con los sistemas, servicios o personal de la propia entidad.
- Implantar medidas en sus propios sistemas y redes para prevenir la difusión de virus y/o código malicioso a los sistemas del **Ayuntamiento de Ermua**. Específicamente, cualquier





ERMUKO UDALA
AYUNTAMIENTO DE ERMUA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

KODEA

ENS.01

BERTSIOA

1.0

DATA

15/01/2024

equipo conectado a la red corporativa del **Ayuntamiento de Ermua** debe disponer de un antivirus actualizado preferiblemente de forma automática.

- Implantar medidas en sus propios sistemas y redes para prevenir el acceso no autorizado a los sistemas del **Ayuntamiento de Ermua** desde otras redes. Entre otros, se deben aplicar las actualizaciones de seguridad en sus sistemas y se debe mantener un sistema cortafuegos para proteger las conexiones desde Internet y otras redes no confiables.

El Ayuntamiento de Ermua se reserva el derecho de revisar la relación con la entidad externa en caso de incumplimiento de las anteriores obligaciones.

