

POLITICA DE SEGURIDAD ALTO NIVEL

© IZENPE 2023

Este documento es propiedad de Izenpe. Únicamente puede ser reproducido en su totalidad

■ Beato Tomás de Zumárraga
71 - 1ª Planta
01008
Vitoria - Gasteiz

www.izenpe.eus
izenpe@izenpe.eus



Histórico de versiones:

VERSION	FECHA	CAMBIO
1	10/10/2005	Versión inicial
2	15/05/2006	Inclusión de la seguridad de los activos
3	03/03/2009	Inclusión de Webtrust/EV como referencia Actualizada localización en E-Sinergy
4	22/05/2009	Cambios realizados debido a la auditoria ISO27001
5	11/12/2013	Incluidas normas CABForum
6	15/03/2015	Modificada versión de ISO a la 2013 y añadida la norma ETSI TS 102 023
7	4/03/2022	Incluido RGPD como norma aplicada en el SGSI de Izenpe
8	28/03/2023	Revisión general sin cambios

Control de aprobaciones:

VERSIÓN	PRESENTADO	REVISIÓN	APROBACIÓN
1.0	Responsable Seguridad	Comité de Seguridad	13/10/2022



ÍNDICE

1. INTRODUCCIÓN	4
2. POLÍTICA DE SEGURIDAD DE ALTO NIVEL.....	4



1. INTRODUCCIÓN

El presente documento establece la Política de Seguridad de alto nivel, así como los principios a aplicar para cumplir con los requisitos de seguridad establecidos en Izenpe.

2. POLÍTICA DE SEGURIDAD DE ALTO NIVEL

La Dirección de Ziurtapen eta Zerbitzu Enpresa, Mmpresa de Certificación y Servicios, Izenpe S.A. (en adelante, Izenpe) está comprometida a establecer y cumplir con las necesarias garantías de integridad, confidencialidad, autenticidad, trazabilidad, disponibilidad y privacidad de datos de la seguridad de la información, así como a generar la mayor confianza en los servicios prestados por Izenpe.

Protegiendo los activos de información de la empresa como son las personas, los certificados, los sistemas, los documentos, etc. tanto propios como de los clientes

Garantizando la mayor fiabilidad posible en la operación de la entidad de certificación

Para ello ha creado un Sistema de Gestión de Seguridad de la Información (SGSI) de las operaciones de la entidad de certificación que se basan en los siguientes estándares y normas técnicas:

- *ISO 27001:2013, como marco de gestión global de la seguridad.*
- *ETSI EN 319 411-2 (Policy requirements for certification authorities issuing qualified certificates) y*
- *ETSI EN 319 411-1 (Policy requirements for certification authorities issuing certificates)*
- *ETSI EN 319 421 (Policy requirements for time-stamping authorities)*
- *CABForum Baseline Requirements for the issuance and management of publicly-trusted certificates*
- *CABForum Guidelines for the issuance and management of Extended Validation Certificates*
- *CABForum Network and Certificate System Security Requirements*
- *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 (RGPD).*
- *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.*

Asimismo, son aplicables los requisitos legales específicos a la actividad de Izenpe y generales descritos en el procedimiento correspondiente.

Como fundamento para la definición de las medidas de seguridad se realizan periódicamente evaluaciones de riesgos. El criterio para evaluar y reducir los riesgos será asegurar que los servicios de Izenpe se presten cumpliendo con las obligaciones legales aplicables a la actividad de certificación y los estándares técnicos vigentes.

La Dirección de Izenpe y la persona responsable de seguridad realizan revisiones periódicas de esta Política y las directrices derivadas de la misma, para lo cual se han definido el procedimiento y responsabilidades pertinentes. De este modo se pretende su adaptación continua a las expectativas y requerimientos de la entidad.