



POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

05 de Octubre de 2021 POL-01-01

	POLÍTICA	FECHA
	POLÍTICA DE SEGURIDAD	05/10/2021

INDICE

1.	Antecedentes	2
2.	Objeto	
3.	Contexto del Desarrollo del SGSI en ZERTIFIKA OUTSOURCING, S.L.	2
4.	Partes Interesadas, sus necesidades y expectativas	2
5.	Marco Legal y Regulatorio en el que se desarrollan las actividades	3
6.	Alcance	3
7.	Términos y Definiciones	3
8.	Organización de la Seguridad de la Información	4
8.1.	<i>Roles y Responsabilidades</i>	<i>4</i>
9.	Objetivos de Seguridad de la Información y Planificación para su Ejecución	5
10.	Establecimiento, Implantación, Mantenimiento y Mejora del SGSI	6
11.	Revisión de la Política de Seguridad de la Información	7
12.	Aprobación, Difusión y Aplicación de la Política de Seguridad de la Información	7

	POLÍTICA	FECHA
	POLÍTICA DE SEGURIDAD	05/10/2021

1. Antecedentes

Este documento sustituye al documento denominado “MC-09 Documento de Política de Seguridad de la Información, en su edición 2 de fecha 02 de marzo de 2015”, los cambios se producen debido a la adaptación a la nueva versión de la norma UNE-ISO/IEC 27001:2014

2. Objeto

Establecer las directrices y principios que regirán el modo en que la empresa **ZERTIFIKA OUTSOURCING, S.L.** gestionará y protegerá sus servicios, a través de la implantación, mantenimiento y mejora de un Sistema de Gestión de la Información (en adelante SGSI) aplicando los requisitos de la Norma UNE ISO/IEC 27001 y de sus partes interesadas.

3. Contexto del Desarrollo del SGSI en ZERTIFIKA OUTSOURCING, S.L.

ZERTIFIKA OUTSOURCING, S.L. ha determinado las cuestiones externas e internas que son pertinentes en el propósito del desarrollo de su SGSI y son las siguientes:

- ✓ Peligros de la red por el aumento continuo de los ataques informáticos y accesos no autorizados, que obligan a tomar medidas para proteger la información.
- ✓ Los cambios continuos de la tecnología.
- ✓ El marco legal y regulatorio en el que se desarrollan las actividades de la compañía.
- ✓ Las necesidades y expectativas de las partes interesadas de la compañía.

4. Partes Interesadas, sus necesidades y expectativas

ZERTIFIKA OUTSOURCING, S.L. ha determinado las partes interesadas que son relevantes para el SGSI y son las siguientes:

- ✓ Clientes
- ✓ Proveedores
- ✓ Empleados
- ✓ Consejo de Administración
- ✓ Administración Pública
- ✓ Comité del SGSI
- ✓ Organismos Regulatorios (AEPD Agencia Española de Protección de Datos)

La información que requiera ZERTIFIKA OUTSOURCING, S.L. para satisfacer sus necesidades y expectativas de las partes interesadas antes mencionadas en el ámbito de sus funciones, encomendadas por el grupo de accionistas, deberá estar protegida en sus dimensiones de **disponibilidad, integridad y confidencialidad**, según la clasificación determinada por la

	POLÍTICA	FECHA
	POLÍTICA DE SEGURIDAD	05/10/2021

Organización y las exigencias del Real Decreto de la Ley Orgánica de Protección de Carácter Personal (LOPD) y la Ley de Propiedad intelectual (LPI).

5. Marco Legal y Regulatorio en el que se desarrollan las actividades

La definición de un sistema idóneo de la seguridad de la información ha de pasar por la consideración, de al menos, las siguientes disposiciones normativas:

- Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.

6. Alcance

El alcance de la presente política comprende las siguientes áreas y procesos de ZERTIFIKA OUTSOURCING, S.L.: **“Actividades de prestación de servicios de gestión de archivos y documentación (custodia, digitalización e indexación de documentos estructurados y no estructurados), gestión de la destrucción y gestión de notificaciones.”**

Se incluye dentro del alcance del SGSI y su certificación, a todo el personal, sistemas informáticos y activos que ZERTIFIKA OUTSOURCING, S.L. emplea para la prestación de estos servicios, la prestación de los servicios se realiza desde las oficinas de ZERTIFIKA OUTSOURCING, S.L. en:

- Oficina principal de ZERTIFIKA OUTSOURCING, S.L. ubicada en C/ Ter nº 27 3 Planta, Oficina 7, Palma. Islas Baleares.
- Almacén en C/ Siurells, 1. Polígono Marratxí. Islas Baleares.

7. Términos y Definiciones

Para los fines de este documento, se aplicarán los términos y definiciones incluidos en la Norma ISO/IEC 27000 y en la Norma ISO/IEC 31000

	POLÍTICA	FECHA
	POLÍTICA DE SEGURIDAD	05/10/2021

8. Organización de la Seguridad de la Información

La Dirección de ZERTIFIKA OUTSOURCING, S.L. se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del SGSI, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución de un Comité del SGSI que tendrá la responsabilidad de:

- ✓ Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia empresarial de la compañía.
- ✓ Asegurar la integración de los requisitos del SGSI en los procesos de la entidad.
- ✓ Asegurar que los recursos para el SGSI estén disponibles.
- ✓ Comunicar la importancia de una gestión de la seguridad eficaz y conforme a los requisitos del SGSI.
- ✓ Asegurar que el SGSI consigue los resultados previstos.
- ✓ Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI.
- ✓ Promover la mejora continua.

8.1. Roles y Responsabilidades

Todo personal de ZERTIFIKA OUTSOURCING, S.L., será responsable de la implementación de esta Política de Seguridad de la Información, dentro sus áreas de responsabilidad.

Se detallan los siguientes roles y responsabilidades dentro del SGSI:

- ✓ **COMITÉ DE SEGURIDAD**, asume las siguientes funciones principales:
 - Aprobar la política de seguridad y de autorizar sus modificaciones
 - Gestionar cambios significativos de los riesgos que afecten a los recursos de la información frente a las amenazas más importantes.
 - Tomar conocimiento y supervisar la gestión de incidentes de seguridad.
 - Garantizar que la seguridad sea parte del proceso de planificación de la información.
 - Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
 - Promover la difusión y apoyo a la seguridad de la información dentro de la empresa.
 - Nombrar y apoyar la figura del Responsable del SGSI.

	POLÍTICA	FECHA
	POLÍTICA DE SEGURIDAD	05/10/2021

- ✓ Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento y resolución de los incidentes de seguridad.
- ✓ Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de riesgos.
- ✓ La mejora de la eficacia de la formación y concienciación del personal que trabaja en ZERTIFIKA OUTSOURCING, S.L. y afecta a su desempeño en seguridad de la información.

Así mismo, la planificación para la consecución de los objetivos de seguridad de la información establecidos, se realizará teniendo en cuenta los siguientes elementos:

- ✓ Lo que se va a hacer.
- ✓ Los recursos necesarios.
- ✓ El responsable.
- ✓ Plazo de consecución.
- ✓ Indicadores para evaluar el resultado/cumplimiento.

10. Establecimiento, Implantación, Mantenimiento y Mejora del SGSI

El despliegue del SGSI se iniciará a partir del Análisis de Riesgos, que permitirá determinar el nivel de riesgo de seguridad de la información en que se encuentra la entidad e identificar los controles necesarios para el tratamiento del riesgo y llevarlo a un nivel aceptable.

Los controles de seguridad, deberán implementarse, mantenerse y mejorarse continuamente, y estar disponibles como información documentada, mediante procedimientos, normativas, registros e instrucciones técnicas. Estos serán revisados por la Dirección de la Compañía y aprobados por el Comité de Seguridad y desarrollados a través de cuatro niveles:

- a. Primer Nivel: Política de Seguridad de la Información.
- b. Segundo Nivel: Normativa de Seguridad.
- c. Tercer Nivel: Procedimiento e Instrucciones Técnicas.
- d. Cuarto Nivel: Informes, Registros y evidencias electrónicas.

Será comunicada la información documentada de los controles de seguridad al personal que trabaja en la compañía (empleados y proveedores), que tendrá la obligación de aplicarla en la realización de sus actividades laborales, comprometiéndose de ese modo, al cumplimiento de los requisitos del SGSI.

Se realizarán auditorías que revisen y verifiquen el cumplimiento del SGSI con los requisitos de la Norma ISO/IEC 27001 dentro del marco regulatorio legal aplicable en

	POLÍTICA	FECHA
	POLÍTICA DE SEGURIDAD	05/10/2021

materia de seguridad de la información, por lo que, en caso necesario, el personal afectado por el alcance del SGSI deberá colaborar en estas, así como en la aplicación de las acciones correctivas que se deriven para el mejoramiento continuo.

11. Revisión de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será examinada en las revisiones del Sistema por la Dirección, a través del Comité de Seguridad, siempre que se produzcan cambios significativos, como mínimo, una vez al año.

12. Aprobación, Difusión y Aplicación de la Política de Seguridad de la Información

La presente Política de Seguridad de la Información será aprobada por el Comité de Seguridad mediante firma y difundida a las partes interesadas de ZERTIFIKA OUTSOURCING, S.L.. Así mismo, la Dirección de ZERTIFIKA OUTSOURCING, S.L. dotará de los recursos necesarios para la aplicación efectiva de esta política, y para su buen desarrollo, tanto en las actividades de implantación como en su posterior mantenimiento y mejora del SGSI.