POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PSI01 REV.00

TEDRA GROUP C/ Moisés de León 46, oficina 1D 24006 León (oficina central)
C/ Albasanz, 71 28037 Madrid (oficina técnica)
Edificio 206 Parque tecnológico Bizkaia (oficina técnica)
Tfno: 987 830 500 www.tedra.es

INDICE

1. OBJETIVO

El objetivo de esta política es establecer un marco de trabajo que permita identificar, desarrollar e implantar las medidas técnicas y organizativas necesarias para garantizar la seguridad y protección tanto de la información relativa a servicios como de los sistemas que la gestionan, y definir la política de continuidad de **TEDRA GROUP**.

Esto implica que se deben aplicar las medidas de seguridad dispuestas en las siguientes normas:

- **ISO/IEC 27001:2015:** Sistema de Gestión de la Seguridad de la Información (SGSI).
- **Esquema Nacional de Seguridad (ENS):** Real Decreto 3/2010 de 8 de enero (en su versión consolidada por Real Decreto 951/2015), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, aplicable a empresas privadas que desarrollan funciones, misiones, cometidos o servicios para las Administraciones Públicas.

2. ALCANCE

El alcance del SGSI corresponde a:

TEDRA GLOBAL SOLUTIONS, S.L.:

Alcance para ISO 27001: Sistemas de Información que dan soporte a los Servicios de consultoría, instalación, soporte y mantenimiento de sistemas de telecomunicaciones, servicios de conectividad, comunicaciones fijas por voz, operador móvil virtual, servicios de hosting y cloud y consultoría de sistemas y seguridad para empresas y Administraciones Públicas de acuerdo con el documento de aplicabilidad.

Alcance para ENS: Los sistemas de información que dan soporte a consultoría y auditoría tecnológica global, incluyendo el ámbito de la ciberseguridad. Servicios de instalación e implementación de todo tipo de infraestructuras y soluciones TI (sistemas, comunicaciones y ciberseguridad). Servicios gestionados y soporte integral de infraestructuras TI (sistemas, comunicaciones y cloud) así como de ciberseguridad, servicios de monitorización de infraestructuras TI, y SOC.

TEDRA HOLDING SPAIN, S.L.:

Alcance para ISO 27001: Servicios generales de facturación, RRHH e infraestructuras para el resto de empresas del grupo.

Las áreas detalladas a continuación relacionan los objetivos y controles definidos en la ISO 27001 y en el ENS, ajustándose al negocio de **TEDRA GROUP**, así como a su entorno de seguridad.

- Política de Seguridad de la Información.
- Organización de Seguridad de la Información.
- Gestión de Activos.
- Seguridad relativa a los Recursos Humanos.
- Seguridad Física y del Entorno.
- Control de Acceso.

- Criptografía.
- Seguridad de las Operaciones.
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información.
- Gestión de Incidentes de Seguridad de la Información.
- Relación con proveedores.
- Gestión de Continuidad de Negocio.
- Cumplimiento legal.

3. TERMINOS Y DEFINICIONES

- **SGSI:** Son las siglas del Sistema de Gestión de la Seguridad de la Información (regulado por la Norma UNE-ISO/IEC 27001), que es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.
- **ENS:** Son las siglas del Esquema Nacional de Seguridad, regulado por el Real Decreto 3/2010, de 8 de enero y su modificación por el Real Decreto 951/2015, de 23 de octubre, siendo su aplicación en el ámbito de la administración electrónica del sector público. Su objeto es establecer la política de seguridad y crear las condiciones necesarias para la confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- **Parte interesada:** Persona o grupo que tiene un interés en el desempeño o éxito de la organización.
- **Autenticidad:** Propiedad de que una persona y o empresa que ha accedido y utilizado la información es lo que afirma ser.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser reveladas a personas y o empresas no autorizadas.
- **Integridad:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a una persona y o empresa.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable en el momento que se requiera por la persona y o empresa autorizada.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Análisis de riesgos:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Tratamiento de riesgos:** Proceso de modificar el riesgo, mediante la implementación de controles.
- **Datos personales:** Cualquier información relacionada con una persona que permita identificarla o pueda servir para identificarla.

4. MISIÓN, VISION Y VALORES

En documento anexo se establece la **Misión, Visión y Valores PSI01-1** de **TEDRA GROUP** respecto a la Seguridad de la Información.

5. MARCO LEGAL Y REGULATORIO EN EL QUE SE DESARROLLAN LAS ACTIVIDADES

Se identifican todos los requisitos, tanto legales como regulatorios, estatutarios o contractuales que son de aplicación a **TEDRA GROUP** en materia de Seguridad de la Información en el documento **FP01-4 Evaluación del cumplimiento legal,** donde se establece el estado cumplimiento de cada requisito.

Anualmente se realiza la evaluación de su cumplimiento y se registra en el documento **FP01-4 Evaluación del cumplimiento legal**.

6. LIDERAZGO Y COMPROMISO DE LA DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN

La Dirección de **TEDRA GROUP** se compromete a facilitar y proporcionar los recursos necesarios para el establecimiento, implantación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información/ENS de **TEDRA GROUP**, así como a demostrar liderazgo y compromiso respecto a este, a través de la constitución del Comité de Seguridad de la Información que tendrá la responsabilidad de:

1. Asegurar el establecimiento de la presente política y los objetivos de la seguridad de la información, y que estos sean compatibles con la estrategia de **TEDRA GROUP**.
2. Asegurar la integración y el cumplimiento de los requisitos aplicables del SGSI/ENS en los servicios y procesos de **TEDRA GROUP**.
3. Asegurar que los recursos necesarios para el SGSI/ENS estén disponibles.
4. Comunicar la importancia de una gestión de la seguridad eficaz y conforme con los requisitos del SGSI/ENS.
5. Asegurar que el SGSI/ENS consigue los resultados previstos.
6. Dirigir y apoyar a las personas para contribuir a la eficacia del SGSI/ENS.
7. Promover la mejora continua.
8. Apoyar otros roles pertinentes de la Dirección, liderando a sus áreas de responsabilidad en seguridad de la información.

9. El detalle de las funciones específicas del Comité de Calidad y Seguridad de la Información, se describen en el documento **Perfil de puesto FP03-4**.

7. FUNCIONES Y RESPONSABILIDADES DE SEGURIDAD DE LA INFORMACIÓN

El Comité de Seguridad de la Información de **TEDRA GROUP** formado por:

- Dirección/Director Técnico
- Responsable de Proyectos y Redes
- Responsable de Sistemas
- Responsable de Administración y RRHH
- Técnico de Contabilidad y Administración.

procederá a revisar y aprobar de la presente Política de Seguridad de la Información.

El Responsable de Seguridad de la Información, cuya figura recae en el Director Técnico, será el encargado de notificar la presente política al personal de **TEDRA GROUP** y de los cambios que en ella se produzcan, así como de coordinar las acciones de implantación, mantenimiento y mejora del SGSI/ENS, y de sus auditorías.
 El Delegado de Protección de Datos, servicio externalizado, será el encargado de garantizar que los datos personales se tratan y se protegen conforme al Reglamento General de Protección de Datos (RGPD UE 2016/679), por lo que trabajará en coordinación con el Responsable de Seguridad de la Información.

Todo el personal de **TEDRA GROUP**, tanto interno como externo, será responsable de cumplir con la presente Política de Seguridad de la Información dentro de su área de trabajo, así como de aplicar toda la información documentada de los controles y medidas de seguridad del SGSI/ENS en sus actividades laborales que afecta a su desempeño en seguridad de la información.

8. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de seguridad de la información se establecerán en las funciones y niveles pertinentes, enfocados a la mejora y utilizando como marco de referencia:

- Cambios en las necesidades de las partes interesadas que lleven a una mejora del alcance del sistema.
- Requisitos de seguridad de la información aplicables y los resultados de la apreciación y del tratamiento de los riesgos para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así como la protección de los datos personales.
- Factores internos como la aplicación de técnicas organizativas que mejoren el seguimiento de la tramitación y resolución de incidentes de seguridad.
- Factores externos como los avances tecnológicos, cuya aplicación mejoren la eficacia del tratamiento de los riesgos.
- La mejora de la eficacia de la formación y concienciación del personal que trabaja en la entidad 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 tomando en cuenta los siguientes elementos:

- Lo que se va hacer.
- Los recursos necesarios.
- El responsable.