POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

PSI01 REV.02

TEDRA GROUP C. la Cepeda, 10 24008 León (oficina central)
C/ Albasanz, 71 28037 Madrid (oficina técnica)
C/ Acero, 30-32 08038 Barcelona (oficina técnica)
Tfno: 902.04.28.00 www.tedra.es

INDICE

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 27 de noviembre de 2023 por la Dirección de **TEDRA GROUP**. Esta Política se Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

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 311/2022 de 3 de mayo 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. PRINCIPIOS BASICOS

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia y tiene en cuenta los siguientes principios básicos.

a) Seguridad como proceso integral.
b) Gestión de la seguridad basada en los riesgos.
c) Prevención, detección, respuesta y conservación.
d) Existencia de líneas de defensa.
e) Vigilancia continua.
f) Reevaluación periódica.
g) Diferenciación de responsabilidades

TEDRA GROUP depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos.
Estos sistemas son administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la confidencialidad, trazabilidad, autenticidad, disponibilidad e integridad o confidencialidad de la información tratada o 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, autenticidad, trazabilidad, 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 en **TEDRA GROUP** se deben aplicar las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, el Reglamento Europeo de Protección de Datos y la Ley Orgánica de Protección de Datos, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

TEDRA GROUP debe cerciorarse de que la seguridad de la información 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 son identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.
TEDRA GROUP está preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 7 del ENS, la LOPD y la ISO 27001.

TEDRA GROUP debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, RGPD, LOPD y la ISO 27001 así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, los departamentos deben:

- 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.

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.
La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS.
Se establecen mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

TEDRA GROUP:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente con clientes y proveedores.

Para garantizar la disponibilidad de los servicios críticos, **TEDRA GROUP** dispone de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a:
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.

Y a los activos vinculados a este alcance:

- A las áreas, tanto a sus responsables como a empleados.
- A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de la organización.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- A la información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- A todos los sistemas utilizados para administrar y gestionar la información, sean propios o alquilados o licenciados por la misma.

Esta política de seguridad se establece de acuerdo a los principios básicos establecidos en el apartado 2 de esta política y se desarrolla aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad.
h) Mínimo privilegio.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de la actividad y detección de código dañino.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

4. MISIÓN

El resultado de unir el conocimiento de expertos en la función de RRHH y expertos en tecnología de **TEDRA GROUP** para crear soluciones que ofrecen al usuario`:

- FLEXIBILIDAD para hacer lo que necesita y no lo que le dejan sus soluciones tecnológicas.
- AUTONOMÍA para desarrollar sus organizaciones sin depender de quienes suministran la tecnología que las sustentan.
- RAPIDEZ para adaptarse con inmediatez a los cambios de su entorno.
- POTENCIA para tomar decisiones en base a hechos y no a creencias.
- COSTES justos, razonables y asequibles, para que la tecnología que impulse a las empresas al máximo nivel no esté sólo al alcance de unos pocos.

Bebemos del Grupo empresarial y humano al que pertenecemos, con una fuerte cultura en la que se basan todas nuestras actuaciones, cuyos pilares fundamentales son la innovación, la ética profesional y el compromiso a largo plazo con nuestros clientes.

Todo ello nos ha permitido contar con la confianza de nuestros clientes provenientes de los más diversos sectores (Banca, Industria, Administración pública, Servicios...). **TEDRA GROUP** crea, implanta y mantiene servicios y productos con un alto componente diferencial para el mercado, adaptándose siempre a la realidad y necesidad de nuestros clientes.

Fruto de esta filosofía y del objetivo de contribuir al desarrollo de las personas a través de la tecnología, surge la necesidad de implantar un Sistema de Seguridad de la Información que dé respuesta a la preocupación cada vez más evidente de nuestros clientes y sus usuarios.

5. MARCO NORMATIVO

Marco normativo al que está sujeto **TEDRA GROUP** por el desarrollo de su actividad:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- 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.
- Reglamento (UE) 2016/679 del parlamento europeo y del consejo sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual.
- Ley 34/2002, de 11 de julio, Servicios de la Sociedad de la Información y de Comercio Electrónico

- Ley 11/2022, de 28 de junio, General de Telecomunicaciones.
- UNE EN ISO/IEC 27001:2017 Sistemas de Gestión de Seguridad de la Información. Requisitos.
- Resolución de 27 de marzo de 2018: ITS de Seguridad de Auditoria de la Seguridad de los Sistema de Información
- Resolución de 13 de abril de 2018: ITS de Notificación de Incidentes de Seguridad.

Anualmente se realiza la evaluación del cumplimiento de esta normativa. **TEDRA GROUP** cumple con esta legislación.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. Comités: Funciones y responsabilidades

El Comité de Seguridad está formado por:

- C.G: Dirección/ Responsable de Seguridad/ Responsable de información/POC
- D.V.: Responsable de servicios.
- P.H: Responsable de Administración y RRHH y Responsable de sistemas.

El Comité de Seguridad tendrá las siguientes funciones:

- Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información.
- Elaborar la estrategia de evolución de **TEDRA GROUP** en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de los diferentes departamentos en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la organización.
- Aprobar la normativa de seguridad de la información.
- Elaborar y aprobar los requisitos de formación y calificación de los responsables de área, técnicos y usuarios desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por **TEDRA GROUP** y recomendar posibles actuaciones respecto de ellos.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones al respecto. En particular, velar por la coordinación de las diferentes áreas en la gestión de incidentes de seguridad de la información.
- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de **TEDRA GROUP**. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes departamentos.
- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

6.2. Roles: Funciones y Responsabilidades

De acuerdo al artículo 13 del RD 311-2022 las funciones y responsabilidades de las personas responsables de velar por el cumplimiento de la Política de Seguridad y de acuerdo al principio de diferenciación de responsabilidades a las que se refiere el artículo 11, son:

Responsable del Sistema

- Gestionar el Sistema de Información durante todo su ciclo de vida, desde la especificación, instalación hasta el seguimiento de su funcionamiento.
- Definir los criterios de uso y los servicios disponibles en el Sistema.
- Definir las políticas de acceso de usuarios al Sistema.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema y aprobar las modificaciones importantes de dicha configuración.
- Realizar el análisis y gestión de riesgos en el Sistema.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Implantar y controlar las medidas específicas de seguridad del Sistema.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Suspensión del manejo de cierta información o la prestación de un cierto servicio si detecta deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos.

Responsable de Seguridad

- Mantener el nivel adecuado de seguridad de la información manejada y de los servicios prestados por los sistemas.
- Realizar o promover las auditorías periódicas a las que obliga el ENS para verificar el cumplimiento de los requisitos del mismo.
- Gestionar la formación y concienciación en materia de seguridad TIC.
- Comprobar que las medidas de seguridad existente son las adecuadas para las necesidades de la entidad.
- Revisar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución, emitiendo informes periódicos sobre los más relevantes al Comité.

Responsable del Servicio

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.
- Aprobar formalmente el nivel de seguridad del servicio.

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.
- Aprobar formalmente el nivel de seguridad de la información.

POC (Punto o Persona de Contacto)

Para el caso de servicios externalizados designamos un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuenta con el apoyo de los órganos de dirección, y que realiza las funciones de canalizar y supervisar, tanto el cumplimiento de los requisitos de seguridad del servicio que prestamos, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio.
Este POC de seguridad es el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma.

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.

Ocupan estos puestos:

- C.G: Responsable de Seguridad/ Responsable de información/POC
- D.V.: Responsable de servicio.
- P.H: Responsable del sistema
- Servicio externalizado: Delegado de Protección de Datos.

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.

6.3. Procedimientos de designación

El Responsable de Seguridad de la Información se nombra a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

6.4. 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 aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

TEDRA GROUP trata datos de carácter personal. El Documento de Seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los datos afectados y los responsables correspondientes.
Todos los sistemas de información de **TEDRA GROUP** se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.
Para garantizar dicha protección, se han adoptado las medidas de seguridad que se correspondan con las exigencias previstas en la legislación de aplicación.
Todo usuario interno o externo que, en virtud de su actividad profesional, pudiera tener acceso a datos de carácter personal, está obligado a guardar secreto sobre los mismos, deber que se mantendrá de manera indefinida, incluso más allá de la relación laboral o profesional con **TEDRA GROUP**.

8. GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política realizan un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se realizará:

- al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- 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 manejados 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.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de **TEDRA GROUP** en diferentes materias:

- Política de Seguridad de la Información FP01-1
- Política de uso aceptable de recursos TI FP03-6
- Política de contraseñas PS02 punto 2.2
- Política de backups PS04 punto 2.3
- Política de uso de controles criptográficos PS02 punto 2.3

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.
La normativa de seguridad estará disponible para todo el personal de **TEDRA GROUP**.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de **TEDRA GROUP** tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros de **TEDRA GROUP** atenderán a una sesión de concienciación en materia de seguridad al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de **TEDRA GROUP**, 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.

11. TERCERAS PARTES

Cuando **TEDRA GROUP** preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando **TEDRA GROUP** utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.
Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

APROBADA:

Tedra Global Solutions, S.L.
B-24436351
24008 León (España)

FIRMADO: CHRISTIAN GARCIA
CARGO: CEO TEDRA GROUP
22 DE ENERO DE 2024