POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

tecisa

Contenido

1 APROBACIÓN Y ENTRADA EN VIGOR 4
2 INTRODUCCIÓN 5
3 ALCANCE 7
4 MISIÓN, VISIÓN Y VALORES 8
5 MARCO NORMATIVO 9
6 ORGANIZACIÓN DE LA SEGURIDAD 10
7 DATOS DE CARÁCTER PERSONAL 12
8 INFORMACIÓN DOCUMENTADA 13
9 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 14
10 GESTIÓN DE RIESGOS 15
11 MEDIDAS DE SEGURIDAD 17
12 AUDITORÍAS DE SEGURIDAD 19
13 OBLIGACIONES DEL PERSONAL 21
14 TERCERAS PARTES 22
15 CUMPLIMIENTO Y ACTUALIZACIÓN NORMATIVA 23

Fecha	Autor/es	Comentarios	Nº Ver.
3/1/22	ET	Emisión	01
17/10/22	EGR	Añadido control de cambios. Cambio menor.	02
27/07/2023	EGR	Añadida jerarquía entre normas. Añadida referencia a IT dentro de la normativa aplicable. Se añade calificación del documento.	03
23/08/2024	EGR	Actualización del documento a ENS 311/2022 y aprobación nuevo gerente	04

1 APROBACIÓN Y ENTRADA EN VIGOR

Esta política fue aprobada el día de enero de 2022 por la Dirección de Tecisa 74 S.L. (en adelante Tecisa), reemplazando a la anterior "Ed. 03", siendo efectiva desde esta fecha y hasta que sea reemplazada por una nueva.

La Dirección de Tecisa, se compromete a difundirla y a revisarla periódicamente con la finalidad de introducir los cambios que sean convenientes.

2 INTRODUCCIÓN

Tecisa es una empresa constituida en el año 1.995, formada por un grupo de ingenieros y técnicos superiores de acreditada experiencia en el sector, especializada en el diseño, fabricación, desarrollo y explotación de sistemas de seguridad.

Tecisa 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 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 de información y comunicaciones (STIC) 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 los departamentos 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 servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Estos sistemas se convierten en pilares básicos para su funcionamiento, por lo que deben ser objeto de una especial protección a fin de que cumplan los requisitos definidos en el RD. 3/2010 Esquema Nacional de Seguridad (ENS).

La Política de Seguridad de la Información, que se plasma en este documento, recoge la forma en que Tecisa gestiona y protege la información y los servicios.

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

Esto implica que los diferentes departamentos en que se articula Tecisa deben cerciorarse de que la seguridad de los STIC es una parte integral de cada etapa de sus actividades y, desde su concepción hasta la retirada de servicio, deben aplicar las medidas mínimas de seguridad exigidas por el ENS para evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas y preparar una respuesta efectiva a los incidentes.

3 ALCANCE

Esta política aplica y será de obligado cumplimiento para todos los departamentos de Tecisa. Se comunicará a terceras partes con las que Tecisa comparta información o reciba algún servicio que implique el acceso a la misma.

Para facilitar su conocimiento y cumplimiento, estará disponible en el sitio web de Tecisa y en los sistemas de información internos para el personal con acceso a ellos.

4 MISIÓN, VISIÓN Y VALORES

Nuestra **Misión** es proteger a nuestros clientes, ayudándoles a gestionar integralmente sus sistemas de seguridad de forma eficiente y robusta a través de la implantación de productos y soluciones que cumplan sus necesidades y expectativas y que sean respetuosos con el medio ambiente.

Nuestra **Visión** se fundamenta en ser una compañía líder en la implantación de soluciones tecnológicas en un mercado global, capaz de ofrecer una respuesta óptima y personalizada a nuestros clientes, con un equipo humano que pueda desarrollar plenamente sus competencias y expectativas profesionales.

Nuestra actividad se fundamenta en los siguientes **Valores**:

- Orientación al cliente
- Trabajo en equipo
- Competencia del personal
- Compromiso
- Confianza
- Innovación
- Ilusión
- Experiencia
- Respeto por el medio ambiente

5 MARCO NORMATIVO

El marco normativo que regula el funcionamiento de **Tecisa** es:

- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- Ley 6/2020 de 11 de noviembre reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 5/2014, de 4 de abril, de Seguridad Privada.
- Instrucciones técnicas de seguridad: Guías del ENS, serie 800, a tener de lo dispuesto en la Disposición Adicional Segunda, del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad

La jerarquía en entre las distintas normas aplicables, ordenada de mayor a menor preminencia, se establece de la siguiente manera.

- Legislación europea
- Legislación española
- Normativa ENS
- Instrucciones técnicas de aplicación del ENS
- Normativa Interna de Tecisa

6 ORGANIZACIÓN DE LA SEGURIDAD

La gestión de la seguridad de la información implica la existencia de una estructura organizativa que, en consonancia con el artículo 10 del ENS, defina unas responsabilidades diferenciadas en relación a requisitos de la información, requisitos del servicio y requisitos de seguridad.

Tecisa gestiona la responsabilidad de los servicios, de la información, de la seguridad y del sistema mediante la implementación de dos roles:

- **Gobierno y supervisión.** Desempeñado por el Comité de Seguridad Corporativa. Se responsabiliza de alinear todas las actividades de la organización en materia de seguridad, destacándose los aspectos de seguridad física y patrimonial (seguridad de las instalaciones), seguridad de la información, Compliance (seguridad y conformidad legal) y planes de contingencia.

  Integra las siguientes funciones:
  - Responsable del Tratamiento (si hay datos de carácter personal).
  - Responsable de la Información.
  - Responsable del Servicio.
  - Responsable de la Seguridad.
  - Responsable del Sistema
  - Supervisar y coordinar al Delegado de Protección de Datos (Externalizado).

- **Operación.** Desempeñado por el Comité de Seguridad de la Información (dependiente del Comité de Seguridad Corporativa). Se responsabiliza de alinear las actividades de la organización en materia de seguridad de la información y que integra las siguientes funciones:
  - Responsable del Sistema.
  - Administrador de Seguridad.

La composición, funciones específicas de cada comité, , resolución de conflictos, los roles o funciones de seguridad, los deberes y responsabilidades del cargo, así como el procedimiento para su designación y renovación se describen en el procedimiento interno "ENS-02-RD-ROLES Y RESPONSABILIDADES".

Será misión del Comité de Seguridad Corporativa la revisión anual de esta Política de Seguridad de la Información, así como la propuesta de revisión o mantenimiento de la misma. La Política será

aprobada por dicho Comité de Seguridad Corporativa y difundida interna y externamente para que la conozcan todas las partes afectadas.

7 DATOS DE CARÁCTER PERSONAL

Tecisa trata datos de carácter personal. Como empresa de seguridad, dispone de un Delegado de Protección de Datos, cuyas funciones quedan detalladas en el sistema de gestión de cumplimento de protección de datos.

8 INFORMACIÓN DOCUMENTADA

El criterio para la calificación de la documentación, el procedimiento para su calificación, quién debe generarla y aprobarla, qué personas pueden acceder a ella, con qué frecuencia o bajo qué circunstancias debe revisarse queda descrito en el proceso "P06 Gestión de la información documentada".

9 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información establece el marco de referencia en el que se desarrollará la normativa de seguridad compuesta por políticas de segundo nivel y procedimientos e instrucciones técnicas que afrontarán 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 en sistemas de información internos de **Tecisa**.

10 GESTIÓN DE RIESGOS

Tecisa se compromete a implementar un proceso integral de gestión de riesgos como parte fundamental de todas sus actividades. Este proceso se llevará a cabo de la siguiente manera:

1. Análisis de riesgos: Se realizará de forma continua y recurrente en todos los sistemas de información sujetos a esta Política. Este análisis permitirá:

- Identificar las amenazas y vulnerabilidades a las que están expuestos los sistemas.
- Determinar la probabilidad de materialización de las amenazas.
- Evaluar el impacto potencial de dichas amenazas.

2. Periodicidad: La apreciación de riesgos se efectuará, como mínimo, una vez al año y siempre que:

- Cambie la información manejada o los servicios prestados.
- Ocurra un incidente grave de seguridad.
- Se detecten vulnerabilidades críticas.
- Se produzcan cambios significativos en la organización, los sistemas o el entorno.

3. Metodología: Para realizar la evaluación de riesgos, Tecisa utilizará una metodología basada en Magerit, adaptada para cumplir con todos los requisitos aplicables. Esta metodología establecerá los criterios de valoración y contemplará diversos escenarios de riesgo, incluyendo la ausencia de medidas de seguridad.

4. Tratamiento de riesgos: Se definirán e implementarán las medidas de seguridad necesarias para reducir o mitigar los riesgos identificados. Estas medidas serán proporcionales a los riesgos y a la categoría de los sistemas afectados.

5. Nivel de riesgo aceptable: El Comité de Seguridad Corporativa, en su rol de Responsable de la Información y del Servicio, determinará y aprobará el nivel de riesgo aceptable para la organización.

6. Coherencia con la continuidad de actividades: El proceso de gestión de riesgos se alineará y será coherente con el Plan de Continuidad de Actividades de Tecisa.

7. Recursos: El Comité de Seguridad Corporativa se compromete a proporcionar los recursos necesarios para la efectiva implementación de las medidas de seguridad derivadas del proceso de gestión de riesgos.

8. Documentación: Los resultados del análisis y tratamiento de riesgos se documentarán adecuadamente, incluyendo las amenazas y vulnerabilidades identificadas, los riesgos analizados, las medidas de seguridad adoptadas y el nivel residual de riesgo.

9. Revisión y mejora continua: El proceso de gestión de riesgos será objeto de revisión y mejora continua para garantizar su eficacia y adecuación a las cambiantes circunstancias de la organización y su entorno.

Este enfoque integral de gestión de riesgos permitirá a Tecisa proteger eficazmente sus activos de información, cumplir con los requisitos regulatorios y mantener la confianza de sus clientes y partes interesadas.

11 MEDIDAS DE SEGURIDAD

Tecisa se compromete a implementar las medidas de seguridad establecidas en el Anexo II del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad. Estas medidas se aplicarán de manera proporcional a los riesgos identificados en cada sistema de información y de acuerdo con su categoría. La implementación de estas medidas se llevará a cabo de la siguiente manera:

4.1 Marco organizativo

Se establecerán las estructuras organizativas necesarias para la gestión de la seguridad, incluyendo la definición de roles y responsabilidades, la política de seguridad, la normativa de seguridad y los procedimientos de seguridad.

4.2 Marco operacional

Se implementarán medidas para garantizar la seguridad por defecto, la integridad y actualización del sistema, la protección de las claves criptográficas, y se establecerán los servicios administrativos y técnicos de seguridad necesarios.

4.3 Medidas de protección

Se aplicarán medidas específicas para proteger las instalaciones e infraestructuras, la gestión del personal, los equipos, las comunicaciones, los soportes de información, las aplicaciones informáticas, la información, los servicios y la explotación de los sistemas.

4.4 Implementación y seguimiento

Para cada una de las áreas mencionadas, Tecisa:

a) Desarrollará políticas y procedimientos específicos que detallen cómo se implementarán las medidas de seguridad.

b) Asignará responsables para la implementación y seguimiento de cada medida.

c) Establecerá un calendario de implementación, priorizando las medidas según el nivel de riesgo y la categoría de los sistemas.

d) Realizará auditorías internas periódicas para verificar la correcta implementación y eficacia de las medidas.

e) Llevará a cabo una revisión anual de las medidas implementadas para asegurar su adecuación y actualización.

4.5 Formación y concienciación

Se desarrollará un programa de formación y concienciación continua para todo el personal sobre las medidas de seguridad aplicables y su importancia.

4.6 Cumplimiento normativo

Se asegurará que la implementación de las medidas de seguridad cumple con los requisitos legales y regulatorios aplicables, incluyendo la protección de datos personales.

4.7 Mejora continua

Se establecerá un proceso de mejora continua que permita la actualización y optimización de las medidas de seguridad en respuesta a cambios en el entorno, nuevas amenazas o mejores prácticas del sector.

4.8 Documentación

Se mantendrá documentación actualizada sobre la implementación de las medidas de seguridad, incluyendo evidencias de su aplicación y efectividad.

Tecisa se compromete a aplicar estas medidas de seguridad de manera rigurosa y sistemática, asegurando así la protección integral de sus sistemas de información y el cumplimiento con el Esquema Nacional de Seguridad.

12 AUDITORÍAS DE SEGURIDAD

Tecisa se compromete a realizar auditorías de seguridad regulares para verificar el cumplimiento del Esquema Nacional de Seguridad (ENS) y la eficacia de las medidas de seguridad implementadas, de acuerdo con lo establecido en el Anexo II del Real Decreto 311/2022.

12.1 Frecuencia de las auditorías

La periodicidad de las auditorías será cada dos años.

Adicionalmente, se llevarán a cabo auditorías extraordinarias cuando se produzcan modificaciones sustanciales en los sistemas de información, que puedan repercutir en las medidas de seguridad requeridas. La consideración de la modificación como sustancial será determinada por el Responsable de Seguridad.

12.2 Alcance de las auditorías

Las auditorías abarcarán, como mínimo, los siguientes aspectos:

a) Política de seguridad y la estructura organizativa para la gestión de la seguridad.

b) Análisis y gestión de riesgos.

c) Gestión de personal y profesionalidad.

d) Gestión de cambios.

e) Gestión de incidentes.

f) Gestión de la continuidad.

g) Monitorización del sistema.

h) Cumplimiento de las obligaciones del ENS.

12.3 Realización de las auditorías

a) Las auditorías serán realizadas por entidades certificadas para la realización de auditorías de seguridad del ENS.

b) Los auditores serán independientes del personal y actividades auditados para garantizar la objetividad.

c) Se utilizarán los criterios de auditoría establecidos en la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

12.4 Informes de auditoría

a) Los resultados de las auditorías se documentarán en un informe.

b) El informe de auditoría detallará los hallazgos, las no conformidades identificadas y las recomendaciones para la mejora.

c) Los informes de auditoría se presentarán al Responsable del Sistema y al Comité de Seguridad Corporativa.

12.5 Plan de mejora

a) Basándose en los resultados de la auditoría, se elaborará un plan de mejora que aborde las no conformidades y las áreas de mejora identificadas.

b) El plan de mejora incluirá acciones correctivas, responsables y plazos de implementación.

c) El Comité de Seguridad Corporativa supervisará la implementación del plan de mejora.

12.6 Conservación de informes

Tecisa conservará los informes de auditoría durante un mínimo de cinco años.

12.7 Auditorías internas

Además de las auditorías externas, Tecisa realizará auditorías internas periódicas, con caracter anual, para evaluar el cumplimiento continuo del ENS y prepararse para las auditorías externas.

Tecisa se compromete a utilizar los resultados de estas auditorías como una herramienta fundamental para la mejora continua de su sistema de gestión de la seguridad de la información y para garantizar el cumplimiento del Esquema Nacional de Seguridad.

13 OBLIGACIONES DEL PERSONAL

Todos los miembros de **Tecisa** tienen la obligación de conocer y cumplir tanto esta Política de Seguridad de la Información como la Normativa de Seguridad que la desarrolla. El Comité de Seguridad Corporativa dispondrá los medios necesarios para que tanto la Política como la normativa lleguen a los afectados.

Para ello, además de que la política esté disponible en los sistemas de información de **Tecisa**, al menos una vez al año, se recordará a todo el personal, ya sea de forma presencial u on-line, la necesidad de su conocimiento y cumplimiento y se notificará cualquier cambio que se haya producido. Así mismo, se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, 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 TERCERAS PARTES

Cuando TECISA utilice servicios o ceda información de/a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que afecte a dichos servicios o información. La 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 TECISA 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 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.

15 CUMPLIMIENTO Y ACTUALIZACIÓN NORMATIVA.

Tecisa reconoce la importancia fundamental del cumplimiento normativo en materia de seguridad de la información. Por ello, la organización ha establecido y mantiene un procedimiento riguroso para la identificación, seguimiento y actualización de la legislación y normativa aplicable a sus actividades y servicios.

Este procedimiento está desarrollado en el documento *ENS-SGSI-09_Legislacion y normativa* e incluye:

1. La identificación continua de nuevas normas y regulaciones relevantes para la seguridad de la información y la protección de datos.
2. El análisis del impacto de estas normas en las operaciones y sistemas de información de Tecisa.
3. La actualización permanente de un registro centralizado que contiene referencias a todas las normas aplicables, incluyendo:
   - Legislación nacional e internacional
   - Normativas sectoriales
   - Estándares y buenas prácticas adoptados por la organización
4. La revisión periódica de este registro para asegurar que todas las referencias estén actualizadas y vigentes.
5. La comunicación oportuna de los cambios normativos relevantes a las partes interesadas dentro de la organización.
6. La adaptación de las políticas, procedimientos y controles de seguridad de la información para asegurar el cumplimiento continuo con la normativa actualizada.

El Responsable de Seguridad, en colaboración con otros departamentos relevantes, es el encargado de supervisar este proceso y de informar regularmente al CSC sobre cualquier cambio significativo en el panorama normativo que pueda afectar a la seguridad de la información en Tecisa.

Este enfoque proactivo hacia el cumplimiento normativo permite a Tecisa mantener un alto nivel de conformidad legal y regulatoria, reforzando así la confianza de nuestros clientes, socios y partes interesadas en nuestra capacidad para proteger la información y los sistemas críticos.

Aprobado por la Dirección General de Tecisa:

Fecha: 14 de agosto de 2024