POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

tecisa

Contenido

Fecha	Autor/es	Comentarios	Nº Ed.
3/1/22	ET	Emisión	01
	EGR	Añadido control de cambios. Cambio menor.	02

1 APROBACIÓN Y ENTRADA EN VIGOR

Esta política fue aprobada el día 3 de enero de 2022 por la Dirección de Tecisa 74 S.L. (en adelante Tecisa) 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 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, actualizado por RD 951/2015.
- 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.

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.
  - 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, criterios de nombramiento y resolución de conflictos 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

En todos los sistemas de información sujetos a esta Política se realizará una evaluación de riesgos que permita identificar las amenazas a las que están expuestos y valorar las probabilidades de su materialización.

Esta apreciación se hará regularmente, al menos, una vez al año y siempre que:

- cambie la información manejada,
- cambien los servicios prestados,
- ocurra un incidente grave de seguridad,
- se detecten e informen vulnerabilidades graves.

Para realizar la evaluación de riesgos Tecisa ha definido una metodología (basada en la metodología Magerit) en la que establece los criterios de valoración.

El Comité de Seguridad Corporativa favorecerá la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas.

11 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.

12 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.

Aprobado por la Dirección General de Tecisa:

Fecha: 3 de enero de 2022