



Documento	Política de Seguridad		Codificación	PO 00
Elaborado	Responsable de Seguridad	Revisado	Responsable de la Información	24-02-2026 Dirección
Versión	Revisión 00	Clasificación de la Información		Uso Público

POLÍTICA DE TISA S.A.L.

- ENTRADA EN VIGOR -

Esta Política de Seguridad es efectiva desde la fecha de aprobación y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

TISA¹ (en adelante, "**Organización**") sustenta el cumplimiento de sus objetivos en el uso de los sistemas y servicios de Tecnologías de la Información y las Comunicaciones (TIC). Por tanto, dichos sistemas deben ser gestionados con el máximo rigor y responsabilidad, aplicando las medidas necesarias para protegerlos frente a posibles riesgos que pudieran materializarse comprometiendo la disponibilidad, integridad, confidencialidad, autenticidad y/o trazabilidad.

El **propósito** de la gestión de la seguridad en la Organización es asegurar la fiabilidad de los datos y la continuidad operativa de los servicios a través de un enfoque preventivo que incluya la supervisión constante de las actividades y la capacidad de responder eficazmente ante cualquier incidente de seguridad. Los sistemas y servicios TIC deben mantenerse protegidos frente a amenazas en constante evolución capaces de afectar a las dimensiones de seguridad y para ello, resulta esencial adoptar una estrategia y compromiso firme en la seguridad, orientada a garantizar la continuidad, calidad y protección de los servicios prestados. Dado el contexto, los procesos y activos de información en la Organización deben ser conformes con el conjunto de medidas y requisitos establecidos por el RD 311/2022, de 3 de mayo; por el que se regula el Esquema Nacional de Seguridad (ENS).

Todo el personal debe cerciorarse de que la seguridad TIC 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. En consecuencia, la Organización debe estar preparada para **prevenir, detectar, reaccionar y recuperarse** ante **incidentes**.

PREVENCIÓN

El personal que interviene en el uso, gestión o administración de los sistemas de información debe prevenir y evitar cualquier circunstancia que pueda afectar a cualquier dimensión de seguridad. Para ello, la Organización implementa las **medidas de seguridad** exigidas por el ENS y cualesquiera controles adicionales que se identifiquen a través del análisis y evaluación de amenazas y riesgos. De igual forma, los roles, responsabilidades y obligaciones en materia de seguridad que sean asignados al personal, se definen, comunican y documentan de manera clara y accesible. Con la finalidad de garantizar el cumplimiento preventivo, resulta necesario:

- 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.

¹ Sedes: San Vicente 8 edificio Albia 2 7ª planta (Bilbao) y De Pinares Plaza, 1 (Donostia).



Documento	<i>Política de Seguridad</i>		Codificación	<i>PO 00</i>
Elaborado	Responsable de Seguridad	Revisado	Responsable de la Información	24-02-2026 Dirección
Versión	Revisión 00	Clasificación de la Información		Uso Público

DETECCIÓN

Tomando en cuenta que los servicios son susceptibles de degradarse como consecuencia de incidentes, resulta imprescindible **monitorizar** de forma continua la operación de los sistemas y servicios con el fin de detectar a tiempo cualquier anomalía o desviación que pueda afectar a los niveles de prestación establecidos; estableciendo mecanismos de detección, análisis y reporte que notifiquen a los responsables designados de forma regular y cuando se produzcan desviaciones.

RESPUESTA

Los incidentes de seguridad son gestionados adecuadamente a través de los mecanismos necesarios para asegurar un óptimo tratamiento. Además, se contemplan **protocolos** para el intercambio de información relacionada con los incidentes tomando en consideración a los Equipos de respuesta a Emergencias Informáticas (CERT).

RECUPERACIÓN

Puesto que se debe garantizar la **disponibilidad** de los servicios críticos, se identifican y analizan las necesidades, los requisitos y las capacidades del negocio, especialmente en aquellos servicios cuya operación dependa de las TIC. Gracias a este análisis, se aumenta la resiliencia de los sistemas ante los incidentes.

ALCANCE

Esta Política aplica a “El sistema de información que da soporte a las infraestructuras, servicios y procesos para la recepción y gestión de edificios, personal auxiliar, organización de congresos, eventos y tareas de traducción e interpretación, según Declaración de Aplicabilidad en su versión 00 del 24 de febrero del 2026”.

SISTEMA DE INFORMACIÓN

Para garantizar que el proceso de seguridad será actualizado y **mejorado** de **forma continua**, se implanta y documenta un Sistema de Gestión de Seguridad de la Información. De esta forma, el contenido de la Política de Seguridad será desarrollado en normas y procedimientos complementarios de seguridad.

MISIÓN

TISA es una compañía **especializada** en ofrecer servicios integrales y personalizados en organización de eventos, traducción, interpretación y personal auxiliar, creando experiencias que unen personas, ideas y proyectos.

Documento	Política de Seguridad		Codificación	PO 00	
Elaborado	Responsable de Seguridad	Revisado	Responsable de la Información	Aprobado	24-02-2026 Dirección
Versión	Revisión 00	Clasificación de la Información		Uso Público	

MARCO NORMATIVO

Marco	Resumen
Reglamento (UE) 2016/679 (RGPD)	La normativa aplicable establece obligaciones para la protección de datos personales y la privacidad de las personas, define derechos y responsabilidades para quienes gestionan información, e impone medidas de seguridad para garantizar las distintas dimensiones de seguridad de la información. Asimismo, regula la prestación de servicios electrónicos y el comercio en línea, y pretende proteger los derechos de propiedad intelectual sobre obras, programas y contenidos, asegurando su uso legítimo y la salvaguarda de los derechos de autores y titulares.
Ley Orgánica 3/2018 (LOPDGDD)	
Real Decreto 311/2022, Esquema Nacional de Seguridad (ENS)	
Ley 34/2002, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE) (Revisión vigente desde 23 de Enero de 2025)	
Real Decreto Legislativo 1/1996, de Propiedad Intelectual (y modificaciones posteriores del texto refundido)	

Sin perjuicio del marco normativo identificado, se tendrán en cuenta las **modificaciones** y **derogaciones** de dicha **normativa** que afecten a esta Política de Seguridad. Además, la Organización cuenta con un registro actualizado en su Sistema de Información específico para la identificación y evaluación periódica (al menos, de forma anual) de los requisitos legales.

ORGANIZACIÓN DE LA SEGURIDAD²

	Rol (ENS)	Designación	Cargo / Puesto
COMITÉ DE SEGURIDAD	Responsable de la Información	P.G.	Dirección
	Responsable de Seguridad	P.G.	Dirección
	Responsable del Servicio	D.E.	Planificación Estratégica
	Responsable del Sistema	D.E.	Planificación Estratégica

La **Dirección** asume el rol de **Responsable de la Información**, en tanto que es quien lidera las decisiones estratégicas sobre los servicios prestados a los clientes y cuenta con un conocimiento y visión global del valor de la información en la organización, determinando los requisitos de la información tratada. Asimismo, se le designa como **Responsable del Servicio**, ya que establece

² Con el objetivo de no indicar más información y datos personales de los necesarios, no se identifican nombres y apellidos de las designaciones. No obstante, la parte interesada podrá solicitar, siempre que exista legitimación, información específica sobre los nombramientos. Para ello, TISA podrá facilitar el acta de nombramiento del Comité firmada por la Dirección.

Documento	Política de Seguridad		Codificación	PO 00
Elaborado	Responsable de Seguridad	Revisado	Responsable de la Información	Aprobado 24-02-2026 Dirección
Versión	Revisión 00	Clasificación de la Información		Uso Público

y/o comunica los requisitos en materia de seguridad de las prestaciones desempeñadas a satisfacer las necesidades de los clientes, determinando los niveles de seguridad de los servicios cuando sea necesario.

El puesto de Planificación Estratégica asume el rol de **Responsable de Seguridad**, puesto que cuenta con la potestad para determinar las decisiones enfocadas hacia la satisfacción de los requisitos de seguridad de la información y de los servicios además de asegurar que el sistema es conforme con el Esquema Nacional de Seguridad. Del mismo modo, es el responsable de organizar las **funciones y responsabilidades**, facilitar los **recursos** adecuados para alcanzar los objetivos y la **protección** de la información. Del mismo modo, se designa también como **Responsable del Sistema**, pues es el encargado de la infraestructura técnica de los sistemas, así como de su control y mantenimiento operativo.

FUNCIONES Y RESPONSABILIDADES

Rol / Órgano	Finalidad	Detalle de funciones y responsabilidades
Responsable de la Información	Establecer los requisitos de seguridad sobre la información	Potestad de determinar los niveles de seguridad de la información.
	Determinar niveles de seguridad en cada dimensión	Categorizar los sistemas en todas sus dimensiones (confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad).
	Responder ante errores	Responsable último de cualquier negligencia o error que conlleve un incidente en la confidencialidad o en la integridad.
	Adoptar medidas sobre los datos personales	Garantizar la seguridad de los datos personales.
Responsable del Servicio	Establecer los requisitos de seguridad del servicio	Potestad de determinar los niveles de seguridad de los servicios.
	Planificar y gestionar los Riesgos	Colaborar en la aprobación del RR (Riesgo Residual) de la matriz de riesgos.
	Asegurar el tratamiento de los datos personales	Desarrollar tareas relacionadas con la gestión de los distintos tratamientos de datos personales que se llevan a cabo.
	Proteger el uso de los servicios	Responsabilidad última del uso que se haga de determinados servicios y de su protección.
Responsable de la Seguridad	Participar en la política, procedimientos, guías y normativas	Participar en la elaboración de la Política, procedimientos, guías, normativas o cualquier documentación relevante en el cuadro del Sistema de Información; además de elaborar en colaboración con los implicados necesarios, documentación (procedimientos, instrucciones técnicas...) así como revisar y aprobar dicha información documentada cuando sea pertinente.
	Formar y concienciar	Promover la formación y concienciación en materia de seguridad de la información en la Organización, garantizando la participación y la eficacia de los planes realizados <i>ad hoc</i> .
	Gestionar de la Seguridad	Categorizar el Sistema, determinar el apetito de riesgo y realizar (o revisar, según necesidad) la evaluación de riesgos y el tratamiento de estos. Determinar.

Documento	Política de Seguridad		Codificación	PO 00	
Elaborado	Responsable de Seguridad	Revisado	Responsable de la Información	Aprobado	24-02-2026 Dirección
Versión	Revisión 00	Clasificación de la Información		Uso Público	

	Comité de Seguridad	Facilitar y comunicar de forma regular al Comité de Seguridad las actualizaciones pertinentes del sistema.
	Reportar	Informar al Responsable del Servicio de las decisiones e incidentes de seguridad.
Responsable del Sistema	Tomar las decisiones operativas	En relación con la arquitectura del sistema, responsable de la instalación y mantenimiento de sistemas y operaciones habituales relacionadas con la gestión del sistema además de integrar las medidas de seguridad necesarias.
	Documentar	Participar en la elaboración de la documentación operativa sobre seguridad.
	Monitorizar	Mantener la monitorización del Sistema de Información
	Reportar	Reportar de forma periódica al resto de Responsables
Comité de Seguridad	Coordinar	Atender las inquietudes de la Alta Dirección y de los diferentes departamentos.
	Informar	Comunicar regularmente el estado de la seguridad de la información a la Dirección.
	Mejorar	Promover la mejora continua del sistema de gestión de la seguridad de la información.
	Aprobar	Aprobar la normativa de seguridad de la información.
	Liderar	Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección.
	Planificar	Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
	Supervisar	Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos desde su especificación inicial hasta su puesta en operación.
	Revisar	Revisar de forma anual la Política de Seguridad.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad es aprobada por la Dirección y ampliamente difundida para que la conozcan todas las partes interesadas pertinentes. Podrán participar en la elaboración, revisión y/o modificación de la Política de Seguridad aquellos puestos y/o roles específicos que Dirección considere relevantes en cada caso. Esta Política de Seguridad es pública y se encuentra disponible en la página web de la Organización.

DATOS DE CARÁCTER PERSONAL

La Organización recoge datos de carácter personal que son adecuados, pertinentes y en ningún caso excesivos dentro del marco necesario en base a la finalidad para los que se hayan obtenido. Se mantienen actualizados los **registros** de actividad, así como la consideración de nuevos **tratamientos** derivados de esta dentro de la normativa aplicable en vigor.



Documento	Política de Seguridad		Codificación	PO 00
Elaborado	Responsable de Seguridad	Revisado	Responsable de la Información	24-02-2026 Dirección
Versión	Revisión 00	Clasificación de la Información		Uso Público

GESTIÓN DE RIESGOS e INCIDENTES

Todos los sistemas sujetos a esta Política deben realizar un análisis de riesgos, evaluando las **amenazas** y los riesgos a los que están expuestos. Este análisis se actualiza:

- regularmente, 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 establece una **valoración de referencia** para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad dinamiza la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal. La Organización establece los **mecanismos** necesarios para responder y atender de manera eficaz a los incidentes y eventos de seguridad, identificando los contactos necesarios para su comunicación cuando así proceda.

DESARROLLO DE OTRAS POLÍTICAS DE SEGURIDAD

Esta Política de Seguridad **complementa** otras políticas (por ejemplo; Política de Control de Accesos, Política de Gestión de Contraseñas, Política de Uso Aceptable de Activos, etc.) de seguridad que se encuentran **disponibles** a los grupos de interés pertinentes dentro de la documentación controlada del Sistema de Información de la Organización.

GESTIÓN Y ESTRUCTURA DE LA DOCUMENTACIÓN

La Organización establece las directrices para la elaboración, estructuración, gestión y acceso a la documentación relativa al Sistema de Información a través del proceso de Gestión de la **Información Documentada** previamente definido. La documentación del sistema se soporta de manera digitalizada en SOFIDYA (SaaS) garantizando todas las dimensiones de seguridad (confidencialidad, integridad, trazabilidad, autenticidad y disponibilidad), sujeta a un proceso de elaboración, revisión y aprobación formal. Asimismo, garantiza a toda su plantilla la **accesibilidad** a la lectura y/o edición (según necesidad) de la información contenida atendiendo a las funciones de cada puesto, participación en procesos y necesidades operativas. Dicha accesibilidad se configura a través de la creación de usuarios y otorgación de permisos específicos en cada caso.

OBLIGACIONES DEL PERSONAL

La totalidad de la plantilla de TISA tienen la obligación de **conocer y cumplir** esta Política de Seguridad y cualesquiera otras políticas, guías y/o manuales, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a las partes interesadas.

Todos los miembros de la Organización se toman en cuenta en la elaboración del **Plan Continuo de Formación y Sensibilización** en Seguridad, adaptando las sesiones formativas y/o de sensibilización a las competencias, necesidades, funciones y responsabilidades en cada caso. En este sentido, los puestos con responsabilidad en el uso, operación y/o administración de la Seguridad de la Información deben recibir acciones de formación y/o sensibilización específicas adaptadas al contexto de la Organización.



Documento	<i>Política de Seguridad</i>		Codificación	<i>PO 00</i>
Elaborado	Responsable de Seguridad	Revisado	Responsable de la Información	24-02-2026 Dirección
Versión	Revisión 00	Clasificación de la Información		Uso Público

TERCERAS PARTES

Cuando se **presten servicios** a otros organismos o se maneje información de otras entidades, se les hará partícipes de esta Política de Seguridad, estableciendo los canales necesarios para el reporte y la coordinación de los respectivos roles y Comités de Seguridad tomando en cuenta los procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o se **ceda información** a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad relacionada con dichos servicios y/o información. La tercera parte quedará sujeta a las **obligaciones** establecidas en dicha normativa, siendo posible desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Además, 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, así como la forma de aplicar el tratamiento adecuado.