izertis

SGSI28

POLITICA DE SEGURIDAD DE LA INFORMACION TERCEROS

Elaborado: 20/11/2023

Revisado y aprobado: 15/09/2025

izertis

Índice

1. INTRODUCCIÓN 3

2. ALCANCE 4

3. RESPONSABILIDADES 5

3.1. Jefes de proyecto 5

3.2. Contratista, empresas, autónomos 5

3.3. Instalación de Herramientas de Seguridad 5

3.4. Auditorías de seguridad 5

3.5. Notificación de incidentes de seguridad 6

4. REQUISITOS DE LOS EQUIPOS A UTILIZAR 7

4.1. Sistema operativo y aplicaciones: 7

4.2. Seguridad y protección: 7

4.3. Gestión de usuarios: 7

4.4. Contraseñas: 7

4.5. Condiciones de Conexión Remota 8

5. RESTRICCIONES PARA EL EQUIPO 9

6. RESTRICCIONES GENERALES 10

7. CUMPLIMIENTO Y SANCIONES 11

8. REVISIÓN Y ACTUALIZACIÓN 12

9. CONTROL DE VERSIONES 13

1. INTRODUCCIÓN

Esta Política de Seguridad de la Información (en adelante la "**Política**") establece las directrices y procedimientos para proteger la información de IZERTIS, S.A. (en adelante "**IZERTIS**), así como de sus clientes en sus relaciones de prestación de servicios de carácter mercantil.

En consecuencia de lo anterior, resultará de aplicación la presente Política a todas las personas físicas o jurídicas (entidades externas, incluyendo empresas, contratistas y autónomos; en adelante, los "**Proveedores**") con las que IZERTIS formalice un contrato de prestación de servicios de carácter mercantil para que dichos Proveedores presten servicios en proyectos para la matriz IZERTIS, S.A. o cualquiera de las sociedades de IZERTIS o para nuestros clientes. Además de las medidas de seguridad establecidas, los Proveedores otorgan el derecho al IZERTIS de realizar directamente, o mediante terceros designados por IZERTIS, auditorías de seguridad para verificar el correcto cumplimiento de esta Política, siempre que así se estipule en el contrato entre las partes.

2. ALCANCE

Esta Política se aplica a todas las formas de información y a todos los dispositivos y sistemas utilizados para procesar, almacenar y transmitir la información a la que el Proveedor tenga acceso para llevar a cabo la prestación de servicios objeto del contrato que haya podido suscribir el Proveedor con IZERTIS.

En relación con el alcance temporal, esta Política será de aplicación y estará limitada al periodo temporal en que esté vigente el contrato de prestación de servicios de carácter mercantil mencionado anteriormente entre IZERTIS y el Proveedor de que se trate.

Una vez finalizado este periodo temporal, el Proveedor deberá proceder inmediatamente a la eliminación segura de toda la información perteneciente a IZERTIS o sus CLIENTES que se haya podido transferir, almacenar o procesar en sus dispositivos y sistemas utilizados para la prestación del servicio, salvo que el contrato de servicios indique otras consideraciones particulares.

3. RESPONSABILIDADES

3.1. Jefes de proyecto

Los jefes de proyecto de IZERTIS designados para cada caso concreto son los responsables de identificar los requisitos de seguridad de la información para el proyecto y garantizar que se implementen medidas adecuadas y requeridas por el cliente.

3.2. Contratista, empresas, autónomos

Los Proveedores contratados para la prestación de servicios de que se trate (contratistas, autónomos, empresas, etc.) deben asegurar que todas las herramientas de seguridad necesarias, actuales o futuras, según lo determine IZERTIS en función de las necesidades dinámicas y adaptativas en materia de ciberseguridad, estén instaladas y configuradas en todos los equipos y sistemas utilizados por el Proveedor para el trabajo contratado. DIRECTRICES DE SEGURIDAD

3.3. Instalación de Herramientas de Seguridad

Todos los equipos utilizados para el trabajo contratado a los Proveedores en régimen de contratación mercantil a través de un contrato de prestación de servicios deben tener instaladas todas las herramientas de seguridad, actuales o futuras, consideradas necesarias por IZERTIS para garantizar la seguridad de la información.
Las herramientas pueden incluir, pero no se limitan a, software antivirus, firewalls, sistemas de detección y prevención de intrusiones, y software de cifrado según sea necesario.

3.4. Auditorías de seguridad

IZERTIS - como empresa contratante - tiene el derecho, si así lo estipula en el contrato estipulado con el proveedor de realizar auditorías de seguridad sobre los equipos y sistemas utilizados para los trabajos asignados con el fin de verificar el cumplimiento de esta Política, así como la correcta instalación del software y las herramientas de seguridad.

3.5. Notificación de incidentes de seguridad

Independientemente de la vigilancia que pueda realizar IZERTIS, el Proveedor deberá notificar a IZERTIS, a través de los canales y mecanismos establecidos para ello, cualquier incidente de seguridad que haya detectado y que afecte al equipo o sistemas utilizados para la prestación del servicio. De no hacerlo así, se enfrenta a una posible vulneración de esta Política y posible rescisión del contrato vigente.

4. REQUISITOS DE LOS EQUIPOS A UTILIZAR

4.1. Sistema operativo y aplicaciones:

- El equipo deberá utilizar un sistema operativo actualizado y soportado por el fabricante.
- Todas las aplicaciones, especialmente aquellas relacionadas con la navegación por Internet, deben estar actualizadas, así como estar soportadas por el fabricante.

4.2. Seguridad y protección:

- Debe de existir un antivirus activo y actualizado instalado en los equipos, con firmas y una política de actualización de al menos 1 vez al día. Se priorizará el uso de una solución tipo EDR (detección y respuesta extendida).
- La solución antivirus o EDR debe estar configurado para realizar un escaneo completo del disco al menos semanalmente, así como tener activados todos los sistemas de detección de código dañino, incluyendo heurísticas de comportamiento.
- Debe emplearse un mecanismo de cifrado de discos para garantizar la confidencialidad de los datos en reposo.

4.3. Gestión de usuarios:

- El acceso al equipo para actividades relacionadas con IZERTIS se realizará con un usuario estándar.
- Habrá otro usuario adicional privilegiado (Administrador) que se utilizará exclusivamente para la administración del sistema o del equipo.

4.4. Contraseñas:

- Todas las contraseñas deben cumplir con las mejores prácticas de seguridad, incluyendo una complejidad adecuada, longitud suficiente y caducidad regular.

- Las contraseñas deben tener al menos 12 caracteres y deben incluir una combinación de letras (mayúsculas y minúsculas), números y caracteres especiales.
- Las contraseñas deben ser cambiadas cada 90 días y no pueden ser reutilizadas dentro de un período de 12 meses.
- Se debe evitar el uso de contraseñas fácilmente adivinables, como nombres comunes, fechas de nacimiento o palabras del diccionario.
- Además de las contraseñas, se requiere la implementación del doble factor de seguridad (autenticación de dos factores) en el acceso a aquellos servicios que vayan a procesar o almacenar información del IZERTIS o sus CLIENTES.

4.5. Condiciones de Conexión Remota

Se establecerán condiciones específicas para la conexión remota para la realización de las tareas encomendadas, las cuales deben ser designadas y autorizadas por IZERTIS.

5. RESTRICCIONES PARA EL EQUIPO

No estará permitido en los equipos que se utilicen para la prestación de servicios por el Proveedor o el personal del Proveedor:

- Uso de software ilícito o que suponga una vulneración de la propiedad intelectual.
- Conexión a redes públicas o fuera del control del usuario.
- Conexión a redes tipo Darknet.
- Instalación o uso de juegos o aplicaciones similares en el equipo.
- Instalación o uso de aplicaciones tipo P2P.
- Instalación o uso de sistemas de mensajería, salvo los autorizados por IZERTIS.
- Utilización del equipo por usuarios o personas ajenas al servicio prestado.

6. RESTRICCIONES GENERALES

En general, no está permitido:

- Subir información o tratar datos de IZERTIS y/o sus clientes en sistemas no autorizados por IZERTIS.

- Divulgar información o datos de IZERTIS y/o sus clientes en sistemas no autorizados por IZERTIS.

- Utilizar sistemas de IA públicos para el tratamiento de datos de IZERTIS y/o sus clientes en sistemas no autorizados por IZERTIS.

- Utilizar sistemas de traductores públicos para subir información de IZERTIS y/o sus clientes en sistemas no autorizados por IZERTIS.

- Almacenar información en medios extraíbles, a menos que estos tengan mecanismos de cifrado robustos que garanticen la confidencialidad en caso de pérdida o robo.

7. CUMPLIMIENTO Y SANCIONES

El incumplimiento de estos requisitos y restricciones, así como la negativa a las autorizaciones específicas, puede dar lugar a la decisión unilateral de IZERTIS de terminar el contrato de prestación de servicios con el Proveedor de forma anticipada y automática, así como la reclamación de los daños y perjuicios que la actuación del Proveedor o de su personal en incumplimiento de la presente Política haya podido generar a IZERTIS o a sus clientes.

8. REVISIÓN Y ACTUALIZACIÓN

Esta Política será revisada regularmente para asegurar su relevancia y eficacia, incluyendo la pertinencia de los requisitos para el equipo y las autorizaciones específicas. Las actualizaciones serán comunicadas a todas las partes interesadas de manera oportuna.

9. CONTROL DE VERSIONES

Todo usuario de este fichero que encuentre un error u oportunidad de mejora deberá comunicarlo al responsable de este para su evaluación y, en su caso, modificación.

La versión en vigor del fichero es la que se encuentra en el repositorio documental de la empresa.

VERSIÓN	FECHA	MODIFICACIONES
01	20/11/2023	Versión inicial.
02	06/09/2024	Revisión y actualización política. Actualización del formato.
03	15/09/2025	Actualización formato.

izertis

ONE TECH AHEAD