# OD-00403-003
# Política de Seguridad de la Información

| **Elaboración:** | | | **Revisión:** | **Autorización:** |
|---|---|---|---|---|
| **Coordinadora de Calidad y Asuntos Regulatorios** | | | **Comité de Seguridad de la Información** | **Director General** |
| **HISTÓRICO DE REVISIONES** | **Fecha** | **Nº Rev / Nº enmienda** | **Descripción** | |
| | 30/10/2024 | 001 | Creación del documento | |
| | 11/06/2025 | 002 | Se actualiza el epígrafe Terceras partes para incorporar los requisitos de seguridad aplicables a los proveedores de servicios de información. | |
| | 27/11/2025 | 003 | - Se actualiza el documento tras revisión estructural, conforme a UNE-EN ISO/IEC 27001<br>- Se actualiza el epígrafe OBJETO Y ALCANCE para incluir los objetivos del SGSI y de la presente política.<br>- Se actualiza el epígrafe Roles y Responsabilidades SI, de acuerdo al SGSI.<br>- Se incluye el epígrafe Compromiso de la Dirección. | |

Ferran Prat
CEO

# Índice

## 1. OBJETO Y ALCANCE

La presente Política refleja el compromiso de VITRO, S.A. con la protección de la información y de los sistemas que la gestionan. Nuestro objetivo es asegurar que la información y los sistemas que la procesan estén adecuadamente protegidos frente a amenazas internas y externas, minimizando los riesgos empresariales y garantizando la continuidad de negocio. Este compromiso se materializa mediante la implantación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI) certificado conforme a la norma internacional UNE-EN ISO/IEC 27001.

Esta Política es de aplicación a todo el personal de VITRO, S.A**.**, así como a las terceras partes que accedan, procesen o gestionen información corporativa o de clientes. Es de cumplimiento obligatorio en todos los procesos, sistemas y servicios incluidos en el alcance del SGSI.

Los **objetivos generales** del SGSI y de esta Política son:

- Proteger la información garantizando su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Cumplir con los requisitos legales, reglamentarios y contractuales aplicables, especialmente en materia de protección de datos personales.
- Reducir los riesgos asociados a las amenazas y vulnerabilidades que puedan afectar a los activos de información.
- Asegurar la resiliencia operativa y continuidad del negocio mediante la prevención, detección y respuesta ante incidentes.
- Fomentar una cultura de seguridad basada en la concienciación y en la responsabilidad individual de todos los empleados.

## 2. MARCO NORMATIVO

Esta Política de Seguridad de la Información complementa la Política de Empresa y la Política de Protección de Datos de VITRO, S.A. y se inspira en los siguientes normas y marcos de referencia:

- **ISO/IEC 27001:2022**, Sistemas de Gestión de la Seguridad de la Información.
- **ISO/IEC 27002:2022**, Controles de Seguridad de la Información.
- **Reglamento (UE) 2016/679 (RGPD)**, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.
- **Ley Orgánica 3/2018 (LOPDGDD)**, de Protección de Datos Personales y garantía de los derechos digitales.
- **Ley 34/2002 (LSSI)**, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

## 3. DESCRIPCIÓN

### 3.1. Contexto de la Organización

VITRO, S.A., es una compañía de biotecnología que desarrolla sus actividades en el campo del diagnóstico y los servicios relacionados. Somos una organización orientada a la investigación, desarrollo, producción y comercialización de productos de investigación y diagnóstico para los laboratorios de Anatomía Patológica, Microbiología, Inmunología y Biología Molecular.

Los sistemas de información constituyen un elemento esencial para la prestación de nuestros servicios y para el funcionamiento operativo de la organización. La Dirección establece esta Política como marco rector para la protección de la información y el cumplimiento de los objetivos del SGSI.

Los sistemas deben:

- Gestionarse con diligencia para protegerlos frente a daños accidentales o deliberados.
- Mantenerse protegidos contra amenazas de evolución rápida que puedan afectar a la información o a la prestación de servicios.
- Tener una estrategia de seguridad adaptativa que preserve la continuidad y calidad de los servicios.

## 3.2. Prevención

VITRO, S.A. 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 se deben implementar las medidas mínimas de seguridad, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, los roles y responsabilidades de seguridad de todo el personal deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se deberá:

- 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.

## 3.3. Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios se deben monitorizar durante su operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.

La monitorización es especialmente relevante cuando se establecen líneas de defensa. VITRO, S.A. establecerá 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.

## 3.4. Respuesta

VITRO, S.A., establecerá mecanismos para responder eficazmente a los incidentes de seguridad, definiendo para ello:

- Punto de contacto para la comunicación de incidentes de seguridad.
- Protocolos para el intercambio de información relacionada con el incidente, incluyendo comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias.

## 3.5. Recuperación

Para garantizar la disponibilidad de los servicios críticos, VITRO, S.A dispondrá de planes de continuidad de los sistemas TIC como parte de su plan general de continuidad del negocio y actividades de recuperación.

## 3.6. Roles y Responsabilidades SI

VITRO, S.A. define una estructura clara de roles para asegurar la gobernanza del SGSI. Las funciones estratégicas se recogen en esta Política y los detalles operativos en los procedimientos internos del SGSI.

### 3.6.1. Comité de Seguridad de la información:

El Comité SI es el órgano responsable de la supervisión estratégica del SGSI. Sus funciones principales son:

- Establecer directrices y prioridades en materia de seguridad de la información.
- Aprobar los criterios de evaluación y tratamiento de riesgos.
- Analizar incidentes relevantes y proponer acciones de mejora.
- Supervisar el cumplimiento normativo y la eficacia del SGSI.
- Coordinar a las áreas implicadas en la seguridad.

El Comité SI reporta al Comité de Dirección y conformado por:

- Responsable de Seguridad de la Información (CISO)
- Delegado/a de Protección de Datos (DPD)
- Director/a de Sistemas de Información (CIO)
- Administrador/a del Sistema
- Coordinador/a de Calidad y Asuntos Regulatorios

Los miembros del Comité SI de VITRO, S.A. quedan recogidos en el acta de designación del Comité SI.

### 3.6.2. Responsable de la Seguridad de la Información (CISO)

El CISO es la figura encargada de liderar la implantación, gestión y mejora continua del SGSI. Entre sus responsabilidades se encuentran:

- Proponer estrategias de seguridad y elevar informes al Comité de Dirección.
- Supervisar la gestión de riesgos de seguridad de la información.
- Asegurar que los controles definidos por el SGSI se aplican correctamente.
- Coordinar la respuesta ante incidentes de seguridad.
- Impulsar la formación y concienciación en seguridad.
- Coordinar auditorías internas y revisiones del SGSI.

### 3.6.3. Director/a de Sistemas de Información (CIO)

El CIO es el responsable estratégico de alinear la infraestructura tecnológica con los objetivos del SGSI.
Entre sus principales responsabilidades se encuentra:

- Gestiona los recursos tecnológicos para proteger los sistemas, garantiza la disponibilidad continua de los servicios TIC
- Supervisa la implementación y mantenimiento de los sistemas, y lidera la transformación digital de la organización.
- Velar por la adecuada continuidad de los servicios TIC.

### 3.6.4. Administrador del Sistema

El Administrador del Sistema es responsable de las operaciones técnicas diarias y mantenimiento de los controles técnicos de seguridad, incluyendo:

- Administración de usuarios y gestión de accesos.
- Aplicación de parches, hardening y mantenimiento técnico.
- Monitorización de sistemas y detección de incidentes técnicos.
- Aplicación de controles técnicos definidos en el SGSI.

#### 3.6.5. Delegado de Protección de Datos (DPD)

El DPD supervisa el cumplimiento del RGPD y la normativa española de protección de datos. Sus responsabilidades incluyen:

- Asesorar a la organización y supervisar el cumplimiento normativo.
- Coordinar análisis de impacto (EIPD).
- Servir de punto de contacto con la autoridad de control.
- Supervisar incidentes que afecten a datos personales.

#### 1.1.5 Responsabilidades Generales del personal

Todo el personal de VITRO, S.A. debe:

- Cumplir esta Política y las normas internas asociadas.
- Proteger la información a la que accede o gestiona.
- Reportar incidentes o debilidades de seguridad.
- Participar en acciones de formación y concienciación

## 3.7. Compromiso de la Dirección

La Dirección de VITRO, S.A. asume un papel activo en la gobernanza del SGSI, asegurando que los recursos humanos, técnicos y financieros necesarios estén disponibles para su correcta implementación. Entre sus responsabilidades se incluyen:

- Aprobar y revisar la Política y los objetivos del SGSI.
- Evaluar los resultados de auditorías, incidentes y revisiones.
- Impulsar la mejora continua y la comunicación interna sobre seguridad de la información.
- Fomentar la cultura de cumplimiento y la integración del SGSI en la gestión global de la organización.

## 3.8. Gestión de Riesgos

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

- regularmente, al menos una vez al año
- cuando cambie la información manejada o los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización del análisis de riesgos, el Comité de Seguridad de la Información establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de la Información dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

La gestión de los riesgos puede consultarse en el procedimiento de Gestión de Riesgos de Seguridad de la información .

## 3.9. Obligación del personal

Todo el personal de VITRO, S.A. es responsable de proteger la información a la que accede o gestiona, participando activamente en la preservación de la seguridad de los datos. Fomentamos la formación continua y la cultura de seguridad como pilares esenciales para un uso responsable y seguro de los sistemas y recursos corporativos.

Es obligación de todo el personal conocer y cumplir esta Política de Seguridad de la Información, las guías y directrices internas vigentes en materia de seguridad de la información que la desarrolla.

## 3.10. Terceras partes

Cuando VITRO, S.A., preste servicios a otros organismos o utilice servicios de terceros que impliquen el manejo de información confidencial, sistemas de información o datos personales, se asegurará de que dichas partes tengan acceso a la presente Política de Seguridad, así como Normativa de Seguridad aplicable.

El objetivo es garantizar que todas las terceras partes de VITRO, S.A., que proporcionen servicios o productos que impliquen el manejo de información confidencial, sistemas de información o datos personales relacionados con las operaciones de VITRO, S.A, conozcan y cumplan con los requisitos y expectativas de seguridad establecidos por la empresa.

Se establecerán canales y procedimientos específicos para el reporte y la resolución de incidentes de seguridad, así como para la interacción con los Comités de Seguridad de la Información cuando proceda. Las terceras partes podrán desarrollar sus propios procedimientos operativos para cumplir con las obligaciones establecidas. 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.

En caso de que alguna parte de esta Política no pueda ser cumplida por el tercero, se requerirá la aprobación expresa del Responsable de Seguridad (CISO), quien deberá evaluar los riesgos asociados y establecer las medidas de tratamiento pertinentes.

### 3.10.1. Requisitos de seguridad

#### 3.10.1.1. Confidencialidad e Integridad de la Información

- Los proveedores deberán garantizar que la información manejada se mantenga confidencial y se proteja contra el acceso no autorizado, modificación o divulgación.

#### 3.10.1.2. Cumplimiento de Normativas

- Los proveedores deberán cumplir con las regulaciones aplicables, incluido el RGPD (Reglamento General de Protección de Datos), y la LOPDGDD (Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales).

#### 3.10.1.3. Intercambio de información

- El intercambio de información entre VITRO, S.A., y sus proveedores se realiza dentro del marco contractual, limitando el uso exclusivo para fines del contrato, con prohibiciones

claras sobre transmisión no autorizada o ilegal, y con controles de seguridad para la protección de la información.

#### 3.10.1.4. Uso apropiado de los recursos corporativos

- Los recursos corporativos de VITRO, S.A., deberán ser usados exclusivamente para cumplir las obligaciones del servicio contratado, prohibiendo su uso para actividades no autorizadas o ilícitas, con controles y auditorías para garantizar su uso correcto.

#### 3.10.1.5. Accesos Controlados

- Los proveedores deberán establecer y mantener controles de acceso adecuados para garantizar que solo personal autorizado tenga acceso a la información confidencial de VITRO, S. A.

#### 3.10.1.6. Certificación de los servicios contratados

- Para servicios especialmente críticos VITRO, S.A., podrá exigir certificaciones referentes a la gestión de la seguridad de la información como la certificación ISO 27001, Esquema Nacional de Seguridad o equivalentes.

#### 3.10.1.7. Notificación de Incidentes de Seguridad

- Los proveedores deberán notificar cualquier incidente de seguridad relacionado con los servicios prestados o la información manejada, de acuerdo con los procedimientos establecidos por VITRO, S.A.

#### 3.10.1.8. Auditoría y Cumplimiento

- VITRO, S.A., podrá realizar auditorías o solicitar evaluaciones externas para asegurar que los proveedores cumplan con los requisitos de seguridad establecidos.

#### 3.10.1.9. Subcontratación

- Los proveedores deberán asegurar que cualquier subcontratación en la prestación de servicios a VITRO, S.A., será comunicada y cumpla también con los mismos estándares de seguridad de la información

## 3.11. Revisión de la Política de Seguridad

Esta política se revisa periódicamente, al menos una vez al año, por el Comité de Seguridad de la Información y la Dirección General, para garantizar su continua adecuación a los cambios tecnológicos, organizativos y regulatorios.

Con esta política, VITRO, S.A. reafirma su compromiso con la protección de la información, la confianza de nuestros clientes y el cumplimiento de los más altos estándares internacionales en seguridad de la información.