OD-00403-002
Política de Seguridad de la Información

Elaboración:	Revisión:	Autorización:
Aída Menacho **Alba del Rocío Roca Roviralta**	**Alberto Roncero** **Fernando López**	**Comité de Seguridad de la Información**

HISTÓRICO DE REVISIONES	Fecha	Nº Rev / Nº enmienda	Descripción
	30/10/2024	001	Creación del documento
	11/06/2025	002	Se actualiza el epígrafe 3.6 Terceras partes para incorporar los requisitos de seguridad aplicables a los proveedores de servicios de información.

Índice

1. OBJETO Y ALCANCE 3
2. MARCO NORMATIVO 3
2.1. Estándares y regulaciones externas 3
2.2. Principal legislación 3
3. DESCRIPCIÓN 4
3.1. Contexto de la Organización 4
3.2. Roles y responsabilidades 5
3.3. Datos de carácter personal 7
3.4. Gestión de riesgos 7
3.5. Obligaciones del personal 7
3.6. Terceras partes 8
3.7. Revisión de la Política de Seguridad 9

1. OBJETO Y ALCANCE

La presente Política de Seguridad de la Información establece los principios y directrices para proteger la información y los sistemas de información de nuestra organización, en conformidad con los requisitos de la norma ISO 27001 y del Esquema Nacional de Seguridad (ENS).

Se aplica a los sistemas de información que soportan los procesos de DDSW, así como la instalación, mantenimiento y soporte de las soluciones TIC ofrecidas por la empresa, que incluyen: AnaPath, OVTS, HybriSpot, VitroStainer y VitroPath (mantenimiento y soporte, excluyendo DDSW), y VTS (mantenimiento y soporte, excluyendo DDSW). Este alcance garantiza la protección y gestión adecuada de la información en todos los sistemas críticos para el funcionamiento de estos servicios.

El objeto de esta política es garantizar la protección adecuada de la información y los sistemas de información de la organización, asegurando su confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y cumplimiento legal.

2. MARCO NORMATIVO

Las normas y directrices que garantizan la protección y gestión adecuada de la información son los requisitos del Esquema Nacional de Seguridad (ENS) y la norma ISO/IEC 27001.

Esta Política de Seguridad de la Información complementa la Política de Empresa y a la Política de Protección de Datos, disponibles en Web Calidad.

Esta Política se desarrollará por medio de normativa de seguridad que afronta aspectos específicos. La normativa de seguridad está a disposición de todo el personal el personal 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 está disponible en el repositorio Web Calidad de la organización.

2.1. Estándares y regulaciones externas

- ISO/IEC 27001:2022 Sistemas de Gestión de la Seguridad de la Información. Requisitos.
- ISO/IEC 27002:2022 Control de la Seguridad de la Información.

2.2. Principal legislación

- 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 (RGPD).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

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.

Desde la Dirección de la Empresa establecemos y comunicamos nuestra Política de Seguridad de la Información, que es la base en la que se fundamenta nuestro sistema de seguridad de la información y sobre la que establecemos nuestro funcionamiento y nuestros objetivos.

VITRO, S.A., se sustenta en los sistemas de información tanto para ofrecer sus productos y servicios como para su funcionamiento operativo y organizativo. Nuestro departamento de Sistemas de Información gestiona los sistemas de información para alcanzar nuestros objetivos, asegurando que los sistemas:

- Se gestionan con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados.
- Están 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 defendernos de estas amenazas se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación adecuada, continua y con la calidad definida de los servicios.

El objetivo de la seguridad de la información es garantizar:

- La continuidad de los servicios; la disponibilidad, integridad, confidencialidad y calidad de la información.
- El seguimiento continuo y monitorización de servicios.
- El seguimiento y análisis de vulnerabilidades.
- La respuesta efectiva ante incidentes.

Para garantizar la adecuada prestación de los servicios, VITRO, S.A., debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (ENS) y otras normativas internacionales de referencia, tales como RGPD, ISO 27001, etc.

Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de Tecnologías de la Información y las Comunicaciones (TIC).

Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS.

3.1.1 Misión y Objetivos de la Organización

Todos los departamentos de VITRO, S.A., y su personal deben 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 determinadas por el ENS, 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 deben poner en marcha las siguientes medidas:

- Revisar el cumplimiento de las características de los sistemas con el fin de someterlos a una autorización previa a la entrada en operación de los mismos.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria/diaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

3.1.2 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/o seguridad de estos y actuar en consecuencia según lo establecido en el Artículo 10 del ENS.
La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 9 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a las personas responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

3.1.3 Respuesta

VITRO, S.A., debe establecer 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 (CERT).

3.1.4 Conservación

Para garantizar la disponibilidad de los servicios críticos, VITRO, S.A., ha desarrollado un plan de continuidad de los sistemas TIC en el marco del plan general de continuidad del negocio establecido.

3.2. Roles y responsabilidades

Se establecen los siguientes roles, cuyas responsabilidades pueden consultarse en las actas de actas Designación de roles esenciales. La función de designación de estos roles corresponde a la Dirección de VITRO, S.A.:

- Persona Responsable de la Información
- Persona Responsable del Servicio
- Persona Responsable de Seguridad
- Persona Responsable del Sistema
- Comité de Seguridad de la Información

3.2.1. Responsable de la Información

Determina los requisitos de seguridad de la información tratada determinando los niveles de seguridad de la información y tiene la responsabilidad última del uso que se haga de esta y, por tanto, de su protección.

El Responsable de la Información es la persona responsable última de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

3.2.2. Responsable del Servicio

Determina los requisitos de seguridad de los servicios prestados determinando los niveles de seguridad de los servicios.

El Responsable del Servicio debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.

3.2.3. Responsable de Seguridad de la Información

Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por las personas responsables de la información y de los servicios.

Responsable de la Seguridad tiene las dos siguientes funciones esenciales:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

3.2.4. Responsable del Sistema

Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.

La persona responsable del sistema tiene las siguientes funciones:

- Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida, incluyendo sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y la gestión del sistema de información, estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas de seguridad se integren adecuadamente en el marco general de seguridad.

La persona responsable de cada información quedará definido en las actas de designación de roles esenciales.

3.2.5. Comité de Seguridad de la Información

El Comité de Seguridad de la Información alcanza a toda la empresa. Es el mecanismo de coordinación y resolución de conflictos en materia de Seguridad de la Información. Coordinará y ejercerá funciones relacionadas con la seguridad de la información, con objeto de velar por el cumplimiento normativo. Está conformado por personal de VITRO, S.A., y reporta al Comité de Dirección.

Las funciones y responsabilidades detallas del Comité de Seguridad de la Información se describen en el acta de designación del Comité SI, así como en el Manual de la Organización.

La composición del Comité de Seguridad de la Información, la designación de los cargos y las obligaciones de cada rol pueden consultarse en Designación de roles esenciales.

3.3. Datos de carácter personal

VITRO, S.A., trata datos de carácter personal. El registro de actividades de tratamiento, al que tendrán acceso sólo las personas autorizadas, recoge los tratamientos afectados y las personas responsables correspondientes. Todos los sistemas de información de VITRO, S.A., se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado registro de actividades de tratamiento.

3.4. 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
- cuando cambien 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 Gestion de Riesgos.

Con el objeto de garantizar un nivel de seguridad adecuado y acorde a las necesidades y riesgos específicos de nuestra organización, el Comité de Seguridad de la Información llevará a cabo la categorización de los sistemas conforme a los criterios establecidos en la Guía CCN-STIC 803 ''Valoración de los sistemas'' del Centro Criptológico Nacional (CCN).

3.5. Obligaciones del personal

Todo el personal Todo el personal de VITRO, S.A., recibirán comunicaciones en materia de seguridad de la información al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todo el personal de VITRO, S.A., en particular a los de nueva incorporación.

Todo el personal de VITRO, S.A., están obligados a conocer y cumplir con esta Política de Seguridad de la Información, así como con lo establecido en el documento BP-00033 Buenas prácticas para la seguridad de la información, garantizando de esta forma la protección y correcta gestión de los activos de información de la organización.

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.

Las medidas de seguridad atañen a todos los departamentos y las personas que trabajan en ellos, sin importar el perfil, cargo o departamento en el que se trabaja. Es por ello que es esencial la definición y distribución de una Política en materia de seguridad de la información, que permita informar y hacer conscientes a todo el personal de la necesidad de poner en marcha y vigilar las medidas definidas en dicha política, con el fin de cerciorarse de que la seguridad de la información 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.

3.6. 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, quien deberá evaluar los riesgos asociados y establecer las medidas de tratamiento pertinentes.

3.6.1. Requisitos de seguridad

3.6.1.1. 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.

3.6.1.2. Cumplimiento de Normativas

- Los proveedores deben 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).

3.6.1.3. 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.

3.6.1.4. Uso apropiado de los recursos corporativos

- Los recursos corporativos de VITRO, S.A., deben 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.

3.6.1.5. 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.

3.6.1.6. 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.

3.6.1.7. 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.

3.6.1.8. 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.

3.6.1.9. 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

3.7. Revisión de la Política de Seguridad

Corresponde al Comité de Seguridad de la Información de VITRO, S.A., supervisar el cumplimiento de esta política y realizar su revisión, al menos, una vez al año. El objetivo de esta revisión es adaptar la política a los cambios técnicos y organizativos, y prevenir su obsolescencia.

Esta Política ha sido revisada y aprobada por el Comité de Seguridad de la Información, y cuenta con el respaldo de la Dirección de VITRO, S.A., para su aplicación en toda la organización.