POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DE CAMBIOS

REVISIÓN	FECHA	CAMBIOS
01	30/09/2021	PRIMERA EDICIÓN
02	13/01/2025	Adecuación al ENS

AUTOR:	REVISADO POR:	APROBADO POR:
Gerente SGSI F. Gomez 13/01/2025	Gerente Nacional E. Spiaggi 13/01/2025	Gerente Nacional E. Spiaggi 13/01/2025

RECEPTORES
Documento de uso público y, por tanto, destinado a ser divulgado a cualquier persona interesada en la actividad de VIVISOL IBÉRICA.

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

INDEX OF CONTENTS

1. APROBACIÓN Y ENTRADA EN VIGOR 3
2. INTRODUCCIÓN Y OBJETIVOS 3
2.1. PREVENCIÓN 4
2.2. DETECCIÓN 4
2.3. RESPUESTA 4
2.4. RECUPERACIÓN 5
2.5. OBJETIVOS 5
3. ALCANCE 6
4. MISIÓN 6
5. MARCO NORMATIVO 7
6. ORGANIZACIÓN DE LA SEGURIDAD 8
6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES 8
6.2. ROLES: FUNCIONES Y RESPONSABILIDADES 9
6.3. PROCEDIMIENTOS DE DESIGNACIÓN 9
6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 10
7. DATOS DE CARÁCTER PERSONAL 10
8. GESTIÓN DE RIESGOS 10
9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 11
10. OBLIGACIONES DEL PERSONAL 11
11. TERCERAS PARTES 12
12. RESPONSABILIDAD 12
13. REVISIÓN 12

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

1. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado el día 31 de enero de 2025 por Dirección.

Esta Política de Seguridad de la Información, que anula el texto anterior, es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

2. INTRODUCCIÓN Y OBJETIVOS

Vivisol Ibérica 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 TIC 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.

Los diferentes departamentos deben 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. 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 TIC.

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

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

2.1. PREVENCIÓN

Los departamentos 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 los departamentos 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, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- 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.

2.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios 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 los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3. RESPUESTA

Los departamentos deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

2.5. OBJETIVOS

Para que VIVISOL IBÉRICA pueda desarrollar y consolidar su posición de liderazgo en los mercados, es necesario asegurar:

- la elaboración, actualización y seguimiento de los planes de desarrollo para asegurar que la infraestructura TIC, los flujos de Información y los procesos internos soporten las actividades del negocio, adoptando las políticas de seguridad adecuadas;
- la calidad y fiabilidad de los activos de Información;
- el almacenamiento seguro de la información gestionada;
- la continuidad de los procesos y flujos de información.

VIVISOL IBÉRICA reconoce la necesidad de desarrollar, mantener, supervisar y mejorar constantemente el Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) en cumplimiento de la norma ISO/IEC 27001 y del Reglamento General de Protección de Datos (GDPR).

El SGSI se realiza asegurando:

- la confidencialidad de los activos de Información gestionados, poniendo los activos a disposición únicamente de las personas y/o entidades autorizadas;
- la integridad de los activos de Información gestionados, protegiendo la propiedad, la fiabilidad y la integralidad;
- la disponibilidad de los activos de Información gestionados, que deben ser accesibles y utilizables por las entidades autorizadas;
- la continuidad de los procesos y flujos de información;
- a través de:
- el cumplimiento de los requisitos obligatorios del marco normativo y de las obligaciones contractuales;
- el cumplimiento de los requisitos de privacidad de las leyes (GDPR y leyes locales de protección de datos) y los requisitos contractuales;
- la formación adecuada del personal sobre los temas de seguridad de la información
- tla eficacia y eficiencia de las medidas de control para evitar, disuadir, gestionar y rastrear, acciones y/o eventos que puedan violar la Seguridad de la Información.

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

- La aplicación del SGSI debe:
- gestionarse dentro de un Sistema de Gestión Integrado;
- basarse en una metodología de evaluación de riesgos aprobada por la Dirección y alineada con los requisitos del negocio; según este método es necesario identificar las amenazas a las que puede estar sometida la Información;
- llevar los riesgos a un nivel aceptable, de acuerdo con las estrategias de gestión de riesgos de la organización;
- definir y aplicar las directrices operativas, reglas, funciones, herramientas, objetos y controles, que garanticen el cumplimiento de los principios de la norma ISO/IEC 27001 y de las normas definidas por VIVISOL IBÉRICA en cualquier estructura organizativa, entorno informático, proceso único;
- controlar, aprovechando cualquier indicio de mejora, el sistema implantado.

3. ALCANCE

La Política de Seguridad de la Información se aplica a todos los empleados de VIVISOL IBÉRICA, a las empresas asociadas, a los proveedores, clientes o terceros bajo contrato temporal o permanente, involucrados en el tratamiento de activos de Información Corporativa en el campo o que tengan acceso al campo de las instalaciones.

4. MISIÓN

Los factores de éxito de la estrategia de VIVISOL IBÉRICA son:

- la internacionalización del negocio para competir en un mercado global;
- la capacidad de anticiparse a las necesidades cambiantes de la aplicación;
- diversificación y desarrollo de nuevas oportunidades de mercado;
- la orientación al cliente;
- la mejora continua y la innovación del producto y del servicio, cada vez más vista como una apuesta por ofrecer soluciones "a medida".

Teniendo en cuenta la importancia estratégica que radica en la gestión de la Seguridad de la Información para su propio negocio, VIVISOL IBÉRICA adopta una política adecuada a las necesidades actuales y futuras.

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

VIVISOL IBÉRICA es consciente de que la gestión de la Seguridad de la Información es un proceso cultural complejo que debe implicar, a todos los niveles y de forma omnipresente, las operaciones individuales de todos los recursos humanos asignados a todas las unidades organizativas dentro del perímetro de certificación (en adelante, "ámbito").

5. MARCO NORMATIVO

Se toma como referencia básica en materia de Seguridad de la Información la normativa siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- 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).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Real Decreto ley 2/2018, de 13 de abril, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.
- Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.
- Reglamento (UE) 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento Europeo eIDAS).

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

6. ORGANIZACIÓN DE LA SEGURIDAD

6.1. COMITÉS: FUNCIONES Y RESPONSABILIDADES

Se constituye el Comité de Seguridad TIC, que reportará a la Dirección. El Comité de Seguridad de la Información coordina la seguridad de la información en la entidad, y estará formado por representantes de las áreas de la organización afectadas:

- El Responsable de Seguridad
- El Responsable de la información
- El Responsable del Servicio
- El Responsable del Sistema

El Comité de Seguridad TIC tendrá las siguientes funciones:

- Atender las inquietudes de la Dirección de la entidad y de los diferentes departamentos.
- Informar regularmente del estado de la seguridad de la información a la Dirección.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la organización en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, que están alineados con la estrategia decidida en la materia, evitando duplicidades.
- Elaborar (y revisar regularmente) la Política de Seguridad de la Información para su aprobación por la Dirección.
- Aprobar la Normativa de Seguridad de la Información.
- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios, desde el punto de vista de seguridad de la información.
- Monitorizar los principales riesgos residuales asumidos por la organización y recomendar posibles actuaciones.
- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de tales incidentes.
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
- Aprobar planes de mejora de la seguridad de la información de la organización. En particular velará por la coordinación de distintos planes que puedan realizarse en diferentes áreas.

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.
- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la organización, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

6.2. ROLES: FUNCIONES Y RESPONSABILIDADES

El Responsable de la Información determinará los requisitos de la información tratada, mientras que el responsable del servicio determinará los requisitos de los servicios prestados.

El Responsable de la Seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones. Las dos funciones esenciales del responsable de la seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

El 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.

6.3. PROCEDIMIENTOS DE DESIGNACIÓN

El Responsable de Seguridad de la Información será nombrado por Dirección a propuesta del Comité de Seguridad TIC. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

El Departamento responsable de un servicio que se preste electrónicamente de acuerdo a la Ley 11/2007 designará al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

De igual modo, el resto de cargos serán designados siguiendo los cauces formales habituales dentro de la organización.

6.4. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección y difundida para que la conozcan todas las partes afectadas.

7. DATOS DE CARÁCTER PERSONAL

Vivisol Ibérica trata datos de carácter personal. El documento de seguridad, al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de Vivisol Ibérica 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 Documento de Seguridad.

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
- 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 TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Se ha establecido un marco en materia de seguridad de la información estructurado en diferentes niveles, de forma que los principios y los objetivos marcados en la política de seguridad de la institución tengan un desarrollo específico:

- Primer nivel: la presente Política de Seguridad de la Información, que debe ser aprobada por Dirección a propuesta del Comité de Seguridad.
- Segundo nivel: la normativa de seguridad de la información o política específica. En ella se establecerán unas normas de uso aceptable de los sistemas de información.
- Tercer nivel: los procedimientos de seguridad de la información, en los que se detallará la manera correcta de realizar determinados procesos de modo que se proteja en todo momento la seguridad y la información.
- Cuarto nivel: estándares de seguridad, instrucciones técnicas, buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc.

Los documentos que integran el SGSI se encuentran a disposición de todo el personal al que le sea necesario para el desempeño de las funciones relacionadas con su puesto de trabajo.

10. OBLIGACIONES DEL PERSONAL

Todos los miembros de Vivisol Ibérica tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de Vivisol Ibérica atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de Vivisol Ibérica, 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.

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

11. TERCERAS PARTES

Cuando Vivisol Ibérica 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 TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Vivisol Ibérica utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha 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 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.

12. RESPONSABILIDAD

Esta política es emitida y revisada por la Alta Dirección de VIVISOL IBÉRICA.

El Responsable del SGSI, designado por la Alta Dirección, facilita la aplicación de esta política a través de normas y procedimientos adecuados. Todo el personal y los proveedores deben seguir los procedimientos establecidos por la política de Seguridad de la Información.

Todos los empleados en el ámbito de la certificación, según sus conocimientos, tienen la responsabilidad de informar al Responsable del SGSI de cualquier debilidad identificada.

Cualquier acción que intencionalmente cause o pueda causar daño a VIVISOL IBÉRICA, debe ser perseguida en la sede correspondiente.

13. REVISIÓN

Esta política se revisa anualmente durante el Comité de Gobierno de la Seguridad de la Información y siempre que sea necesario debido a la implementación de cambios relacionados con la misma, para

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.

asegurarse de que sigue siendo adecuada a los objetivos de VIVISOL IBÉRICA, a las expectativas de los usuarios y a todas las partes interesadas.

Todos los derechos reservados. La transferencia y copia de este documento, o el uso y comunicación de su contenido, no están permitidos sin autorización escrita.