GRUPO SUPERVIELLE


# Política de Seguridad de la Información

## Grupo Supervielle S.A.

14 de septiembre de 2023

# TABLA DE CONTENIDOS

## 1. INTRODUCCIÓN

Grupo Supervielle S.A. reconoce como un activo estratégico a la información y los medios que la soportan y define, como objetivo particular, alcanzar los niveles de seguridad necesarios que garanticen su adecuada protección, en función de los pilares de la Confidencialidad, Integridad, Disponibilidad, Autenticación, Autorización y No Repudio.

Esta Política Corporativa de Seguridad de la Información es la política de mayor nivel en este ámbito. De manera subyacente a esta, Grupo Supervielle S.A. establece varias políticas globales para las distintas funciones relacionadas con la protección de la información.

Las empresas de Grupo Supervielle S.A. están sujetas a ciertas leyes, reglamentaciones y obligaciones contractuales que estipulan controles para la seguridad de la información.

Con el objetivo de velar por la protección de los activos de información, se instauran los principios que rigen la protección de los datos y de la información para evitar los riesgos inherentes en su procesamiento, transmisión, almacenamiento y destrucción. Todo ello con el fin de evitar su pérdida, divulgación, malversación, no disponibilidad, destrucción indebida, repudio, accesos y/o modificaciones no autorizadas.

Asimismo, se privilegia la protección integral de los datos, independientemente del medio que los contenga, promoviendo un entorno de manejo ético y controlado de manera de garantizar el cumplimiento reglamentario y una ventaja competitiva en el mercado.

Por consiguiente, surge la necesidad de inventariar, clasificar y proteger la información en función de su criticidad, grado de exposición y apetito de riesgo, asignando responsables según la instancia de gestión en que intervengan, recurso utilizado y tipo de información accedida.

## 2. GOBIERNO

El Directorio de Grupo Supervielle S.A. será el órgano encargado de revisar y aprobar esta política, considerando los lineamientos y/o recomendaciones del Comité de Ciberseguridad.

Es responsabilidad de Seguridad de la Información asegurar el cumplimiento de esta Política y mantenerla actualizada con el fin de reflejar fielmente los lineamientos establecidos, realizándose su revisión una vez al año o ante cambios relevantes.

## 3. APLICACIÓN Y ALCANCE

La presente política se aplica a Grupo Supervielle S.A. y a sus empresas vinculadas y la referencia a Grupo Supervielle S.A. en este documento incluirá a cada una de sus empresas vinculadas. Su incumplimiento podrá implicar sanciones laborales y, llegado el caso, la recisión de personal contratado, o de los contratos con proveedores o consultores.

La Política de Seguridad de la Información y todos los contenidos documentales que de ella se originen son de aplicación obligatoria para Grupo Supervielle S.A. y, por ende, aplica a todos los colaboradores de planta permanente, contratados por plazos, proveedores, consultores y otras personas que realicen actividades en Grupo Supervielle S.A.

Comprende la protección de los activos de información en lo que respecta a la seguridad de la información obtenida, creada o mantenida por los usuarios en cualquier medio escrito, impreso o electrónico y todos los procesos relativos a actividades desarrolladas por medio de componentes tecnológicos. Esta información abarca la información de clientes, colaboradores e información propietaria de Grupo Supervielle S.A., como ser datos sobre sus productos, estrategias, procesos, servicios.

Toda excepción a la presente Política deberá ser analizada por el Comité de Ciberseguridad, el cual proporcionará sus recomendaciones al Comité de Riesgos Operacionales para que tome decisiones en línea con el apetito de riesgo de la organización. Posteriormente, dará conocimiento al Comité de Ética, Compliance y Gobierno Corporativo sobre las decisiones tomadas.

## 4. EXTENSIÓN A TERCEROS

Los colaboradores y prestadores de servicios directamente contratados por Grupo Supervielle S.A. deben adherirse formalmente a un documento en que se comprometen a actuar de acuerdo con la presente Política de Seguridad de la Información.

Asimismo, los contratos deben poseer una cláusula que asegure la confidencialidad de la información.

## 5. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información se rige por los siguientes principios:

- **Confidencialidad:** La información que fuera propiedad de Grupo Supervielle S.A. o que estuviera bajo su custodia debe protegerse en todo momento ante un acceso no autorizado.
- **Integridad:** Deben implementarse medidas que impidan la modificación o destrucción no autorizada de la información, ya sea en forma accidental o intencional.
- **Disponibilidad:** Debe asegurarse que la información requerida se encuentre disponible en forma oportuna para las personas autorizadas a acceder a dicha información.

- **Autenticación:** La identidad de cada individuo o proceso que acceda a la información de Grupo Supervielle S.A. debe verificarse adecuadamente antes de permitirse el acceso.
- **Autorización:** El acceso a la información debe limitarse sólo a lo necesario para dar soporte a las funciones autorizadas de negocios.
- **No Repudio:** Provee las garantías necesarias que permiten asegurar indudablemente la participación de las partes emisor y receptor.

- **Accesos por función:** El acceso a la información debe obedecer el principio del mínimo privilegio, a través del cual se le otorga al usuario los niveles (o permisos) mínimos necesarios para desempeñar sus funciones laborales.
- **Control de acceso cerrado por defecto:** Se encuentra ligado al principio anterior. Se deben cerrar todos los accesos por defecto y abrirlos (para un usuario) solo cuando sea necesario.
- **Accesos Intransferibles:** La asignación de permisos de acceso debe ser realizada sobre usuarios individuales y es intransferible, de forma que la responsabilidad por las acciones ejercidas con los accesos otorgados sea directamente atribuible a ese usuario.
- **Segregación de funciones:** Ningún usuario debe tener el control total de un proceso o transacción crítica de negocios.
- **Identificación de responsabilidad:** Los sistemas y procesos deben estar sujetos a controles que permitan detectar accesos no autorizados e identificar al responsable de la actividad realizada en dicho sistema o proceso.
- **Estrategia de Seguridad de Información:** Debe asegurarse la definición e implementación de una estrategia para la protección de los activos de información.
- **Clasificación de la Información:** La información, ya sea verbal, escrita, impresa o electrónica, debe clasificarse en función de su confidencialidad, integridad y disponibilidad.
- **Divulgación de la Información:** La información, ya sea verbal, escrita, impresa o electrónica, debe divulgarse de acuerdo con los requerimientos de confidencialidad de dicha información.
- **Concientización:** Todos los individuos con acceso a la información de Grupo Supervielle deben comprender sus roles y responsabilidades en lo que respecta al manejo y protección de la información de Grupo Supervielle.

## 6. OBLIGACIONES

El área de Seguridad de la Información del Grupo Supervielle fija los siguientes controles principales:

- Desarrollará, mantendrá y comunicará esta Política, y la documentación que la respalda.
- Mantendrá informado al Directorio sobre el desempeño del gobierno de la Seguridad de la Información, las políticas de alto nivel, sus proyectos estratégicos y toda acción relacionada con la misión, metas y objetivos relacionados con el gobierno de la Seguridad de la Información.
- Identificará e implementará un marco de gestión de riesgos para la protección de información y establecerá los controles necesarios para resolver los mismos de manera aceptable a efectos de respaldar los objetivos de negocio del Grupo Supervielle S.A.

- Verificará que los procesos de protección de la información sean los adecuados en función de los requisitos comerciales, normativos y reglamentarios vigentes.
- Gestionará los programas de capacitación y concientización en seguridad de la información.
- Gestionará y responderá a eventos e incidentes de seguridad de la información de manera oportuna para reducir el impacto en, accionistas, clientes y socios comerciales.
- Desarrollará y publicará normas y procedimientos de seguridad de la información necesarios para mantener un entorno operativo seguro, protegido y conforme a las reglamentaciones.
- Realizará evaluaciones de riesgos para identificar amenazas, vulnerabilidades y medidas para mitigar el riesgo.
- Contribuirá en identificar e implementar una segregación de tareas y funciones adecuada para minimizar riesgos superpuestos de autorización.
- Gestionará evaluaciones de vulnerabilidades, pruebas de intrusión, revisiones de código y pruebas de los sistemas de seguridad.
- Velará por una adecuación de sus procesos con el modelo de las tres líneas de defensa adoptado por la entidad, implementando aquellos controles y medidas de seguridad que permitan preservar de manera razonable la confidencialidad, integridad y disponibilidad de la información.

Los usuarios a su vez se comprometen a:

- Tratar la Información de Grupo Supervielle S.A., de los clientes y del gran público de modo ético y secreto y con arreglo a la legislación en vigor y las normas internas para evitar el mal uso y la exposición indebida.
- Utilizar la información de modo transparente y solamente a los efectos para los cuales la recolectaron.
- Contribuir en la ejecución de procesos que permitan ejecutar y controlar un proceso o transacción desde su creación hasta su conclusión para asegurar la división de funciones.
- Solo acceder a la información y los recursos a los cuales se haya formalmente autorizado.
- Su identificación como empleado en los sistemas debe ser única, personal e intransferible y lo identifica como responsable de las acciones efectuadas.
- El otorgamiento de accesos debe obedecer el criterio de menor privilegio, según el cual los usuarios solamente acceden a los recursos de información que son imprescindibles para el pleno desempeño de sus actividades.
- Su contraseña tiene la calidad de firma electrónica y debe mantenerla en secreto, es decir que se prohíbe su difusión.
- Documentar e informar fehacientemente aquellos riesgos (siendo el usuario el responsable o no) que afecten los principios mencionados en el punto 5 de este documento ante la Gerencia de Seguridad de la Información y la Gerencia de Riesgos Operacionales.
- No utilizar para fines particulares ni transmitir a otras tecnologías, marcas, metodologías y cualquier información perteneciente al Grupo Supervielle S.A., aunque hayan sido obtenidas o desarrolladas por el mismo empleado en su ambiente de trabajo. Solo difundir la información clasificada como pública cuando sea necesario, absteniéndose de difundir información

sensible o interna de Grupo Supervielle S.A., como por ejemplo políticas, información sobre herramientas de seguridad, standards o normativas/procedimientos internos.
- Informar y trabajar en conjunto con la Gerencia de Seguridad de la Información en la evaluación de cualquier herramienta, aplicativo, servicio y/o proveedor que pueda tener impacto en algún activo de información de la entidad, a fin de determinar su impacto sobre la postura de seguridad, definir los controles mitigantes que se consideren necesarios y realizar el seguimiento correspondiente.

## 7. PROGRAMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Programa de Gestión de Seguridad de la Información ("PGSI", según sus siglas) es un conjunto de disciplinas dispuestas por Grupo Supervielle S.A. con la finalidad de asegurar un enfoque centralizado y uniforme en la definición y aplicación de la de Política Corporativa de Seguridad de la Información.

Estas disciplinas incluyen:

**Acceso Lógico a los Activos de la Información:** Se debe administrar la seguridad sobre los distintos tipos de accesos (locales y/o remotos), y la autenticación segura de usuarios y perfiles de todo el personal del Grupo Supervielle S.A. Dicha seguridad debe ser aplicada sobre la totalidad de los activos de información (aplicaciones y plataformas tecnológicas homologadas), tanto para los ambientes productivos como contingencia.**Monitoreo y Control de Seguridad:** Está orientado a asegurar las plataformas de procesamiento y operaciones de TI, con el fin de mitigar posibles riesgos de seguridad, de acuerdo con los procedimientos de control y monitoreo de seguridad definidos. Los accesos y las actividades en los activos de información deben ser monitoreadas periódicamente, reportando los incidentes o cualquier anomalía detectada a quien corresponda, y procediendo a la toma de acciones necesarias para su resolución.Los servicios de sistemas y tecnología que Grupo Supervielle S.A. tercerice deben ser controlados con el objetivo de velar por la correcta administración de la seguridad de la información de los activos gestionados por los prestadores.

- **Gestión de Virus y Vulnerabilidades:** Tiene por objeto proteger a Grupo Supervielle S.A. contra código malicioso y establecer estándares y procedimientos para la detección y remediación de vulnerabilidades.

- **Soporte, prevención y mantenimiento de arquitecturas y ciclo de vida de desarrollo seguro:** Se debe garantizar que los aspectos de seguridad sean considerados en todas la fases del ciclo de vida de los sistemas informáticos para lo que se debe asegurar razonablemente que todas las aplicaciones informáticas a desarrollar o adquirir incorporen, según sus características y alcance, sistemas de control de accesos y mecanismos que garanticen la seguridad de la información y permitan su correcta gestión, administración, control y auditabilidad con el propósito de prevenir la pérdida, modificación o uso inadecuado de los datos en las aplicaciones informáticas y proteger la confidencialidad, disponibilidad y la integridad de la información.

- **Seguimiento de Observaciones:** Implica realizar un correcto y oportuno seguimientos de los planes de acción

que pudiesen surgir producto de los hallazgos y/u observaciones realizadas por los diferentes entes de contralor.

- **Gestión de Incidentes de Seguridad:** Consiste en contar con un proceso para la atención, detección, análisis, control, tratamiento y mitigación y respuesta - recuperación de incidentes de seguridad, y su correcta comunicación a las partes involucradas, para la mejora continua de los procesos.

- **Plan de Concientización de Seguridad de la Información:** Busca impulsar una cultura de cumplimiento de la Política de Seguridad de la Información, como así también de las mejores prácticas en materia de seguridad de la información.

- **Gestión de Riesgos de Seguridad de la Información:** los anteriores puntos destacados se encuentran vinculados a la correcta gestión de los riesgos de Seguridad de la Información, proporcionando controles relacionados con puntos de referencia que se pueden utilizar para identificar deficiencias en el diseño y la implementación en el activo. Se realizan revisiones periódicas que derivan planes de acción si así lo requiera.

## 8. LÍNEA ÉTICA & VALORES

Cualquier incumplimiento de esta Política podrá ser denunciado a través de la Línea Ética & Valores:
0800-777-7813
www.eticagruposupervielle.lineaseticas.com.ar
Usuario: Supervielle
Contraseña: Supervielle

## 9. ANEXO - GLOSARIO

**Activo:** En relación con la Seguridad de la Información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tengan valor para la organización.

**Aprobador:** Es el responsable de autorizar el pedido de alta o modificación de los permisos de un usuario. Cuando un usuario corresponda a un servicio brindado por terceros o prestado por un proveedor, el aprobador será el responsable primario del servicio en cuestión.

**Aplicativo o Sistema Aplicativo:** Es todo desarrollo de programación que procese datos y se ejecute en una plataforma tecnológica a efectos de proveer soporte a los procesos de negocios internos y externos.

**Componentes Tecnológicos:** Es todo servicio, producto o aplicación que forme parte del entorno informático de Grupo Supervielle S.A., tales como, pero sin limitar: aplicativos, software, hardware, componentes de conectividad, herramientas de desarrollo, herramientas de monitoreo, componentes de seguridad y protocolos.

**Custodios de la Información:** Se refiere a personas o terceras partes que manipulan información de Grupo Supervielle.

**Dueños de la Información:** Son los representantes de las Unidades de Negocios responsables de la confidencialidad, integridad y disponibilidad de la información, y de definir accesos a los sistemas, agrupados en lo que se denomina "Grupo/Perfil", contando también con la responsabilidad de controlar y validar periódicamente los usuarios asignados a los mismos. Cuando fuera necesario, Seguridad de la Información podrá designar Dueños de los Grupos/Perfiles para el sistema aplicativo que así lo requiera.

Los Dueños de la Información deben ser designados por el Gerente de la Unidad de Negocios. Los Dueños de la Información deben ser colaboradores de Grupo Supervielle S.A. y pertenecer a las áreas operativas responsables por el manejo de dicha información. El Gerente de la Unidad de Negocios designa además un reemplazante, que posee las mismas facultades y responsabilidades.

En el caso de servicios brindados por terceros o prestados por un proveedor, la responsabilidad del Dueño de la Información recae sobre la Unidad de Negocios dueña del servicio en cuestión.

**Dueños de los Componentes Tecnológicos:** son los miembros de Tecnología de la Información (TI) designados por el Responsable de TI, con autoridad para requerir, crear, mantener y eliminar los componentes tecnológicos. Los Dueños de los Componentes Tecnológicos deben ser colaboradores efectivos de Grupo Supervielle S.A. El Responsable de TI designa además un reemplazante, que posee las mismas facultades y responsabilidades.

**Usuarios:** son todos los colaboradores, contratados, proveedores, consultores y otras personas que realicen actividades en Grupo Supervielle S.A. y a quienes se les haya otorgado acceso a su información y componentes tecnológicos.

**Supervisores:** son las personas de la Unidad de Negocios con responsabilidad por sus usuarios o por el servicio, producto, información o sistema suministrado por la unidad de negocios o unidad de soporte.

**Datos personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

**Datos personales sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.