Fidelitas

Política General de Seguridad de la Información

Control de versiones

Código.	FIITPO006
Versión.	1.0
Fecha de la versión.	08/08/2025
Creado por.	Alejandro Burgol
Aprobado por.	Comité de Seguridad (Félix El Idd, Alejandro Burgol, Jorge El Idd, Natalia Queija)
Clasificación.	Pública

Historial de modificaciones

Fecha.	Versión.	Creado por.	Descripción de la modificación.

Tabla de contenido

1. Objetivos y alcance

Objetivo

El propósito de la "Política General de Seguridad de la Información", es declarar la posición de Fidelitas SA con respecto al buen uso y protección de los activos de información. Esto se traduce en:

- Definir lineamientos o principios generales que sirven como medio para alcanzar los objetivos de un Sistema de Seguridad de la Información.
- Establecer responsabilidades aplicables a los distintos niveles jerárquicos y a todo el personal vinculado con Fidelitas SA.
- Fijar directrices sobre las cuales se sustentan normativas e instructivos de seguridad que desarrollen con mayor grado de detalle aspectos relativos a la seguridad de un tema particular o sistema en específico.
- Definir medios de difusión al interior y exterior del servicio para alineamiento con la Dirección.
- Definir plazos y periodicidad para su revisión y evaluación de cumplimiento.

Alcance

La presente política establece un marco regulatorio aplicable a todo el personal relacionado con Fidelitas SA, ya sea colaboradores sujetos al Código del Trabajo, como a personal externo que preste servicios permanentes o temporales.

También es aplicable a todo activo de información que la organización posea en la actualidad o en el futuro, asociados a los procesos de negocio de Fidelitas SA, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger estos activos de información.

La política cubre toda la información, entre otras, la impresa o la escrita en papel, la almacenada electrónicamente, la transmitida por correo o usando medios electrónicos, mostrada en video o hablada en una conversación, entre otras formas de información.

2. Documentos de referencia

- Manual de SGSI.
- Política de SGSI.
- ISO/IEC ISO 27001:2022.
- ISO/IEC 27018:2020 – Código de práctica para la protección de la información de carácter personal en la nube pública que actúa como procesador de datos personales.

3. Vigencia del documento

Este documento es válido desde su fecha de aprobación.

El propietario del documento es el CTO, que debe verificar y actualizar, de ser necesario al menos una vez al año.

4. Roles y responsabilidades

A continuación, las responsabilidades definidas según su rol:

- Miembros del Comité: Gestionar las modificaciones al presente documento para los cuales se apoyará en el departamento de Seguridad de la Información y deberán plantear las reformas en las sesiones de Comité.
- Director de Tecnología (CTO): Responsable de la aplicación y cumplimiento de la Política de Seguridad, así como de comunicar las actualizaciones al personal.
- Dueños de los Activos: Deben identificar y clasificar la información que es crítica para la empresa.
- Personal de TI: Deben implementar y mantener los controles de seguridad.
- Todos los Empleados: Deben cumplir con la política y reportar cualquier incidente o violación.
- Proveedores Externos: Deben cumplir con los requisitos de seguridad establecidos por la empresa.

5. Definiciones

CONCEPTO	DESCRIPCIÓN
Activo de información	Aquello que tenga valor y es importante para el Fidelitas SA, sean documentos, sistemas o personas y todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la organización. Se distinguen tres niveles: La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.) Los equipos, sistemas e infraestructura que soportan o contienen esta información.

	Las personas que utilizan la información, y que tienen el conocimiento de los procesos de la organización.
Colaborador	Toda persona que tenga un vínculo contractual de trabajo con Fidelitas SA, sea éste indefinido, a plazo fijo o a honorarios.
Política	Directriz u orientación general expresada formalmente por la administración de Fidelitas SA.
Procedimiento	Sucesión cronológica de acciones concatenadas entre sí, para la realización de una actividad o tarea específica dentro del ámbito de los controles, en este caso, de Seguridad de la Información.
Riesgo	Posibilidad que ocurra un evento que afecte adversamente el logro de los objetivos de Fidelitas SA. Se mide combinando las consecuencias del evento (impacto) y su probabilidad de ocurrencia.
Amenaza	Causa potencial de un incidente no deseado, que puede dar lugar a daños a un sistema o proceso.
Vulnerabilidad	Debilidad de un activo o grupo de activos que puede ser materializada por una o más amenazas.
Evento de Seguridad de la Información	Actividad o serie de actividades sospechosas que amerita ser analizada desde la perspectiva de la Seguridad de la Información.
Incidente de Seguridad de la Información	Evento o serie de eventos de Seguridad de la Información, no deseados o inesperados, que compromete la Seguridad de la Información y amenaza la operación del negocio.
Confidencialidad	Propiedad de la información que determina que sólo podrá ser accedida por personas, entidades o procesos debidamente autorizados.
Integridad	Propiedad de la información según la cual sólo puede ser modificada, agregada o eliminada por las personas o sistemas autorizados para cada proceso, de tal forma de salvaguardar la exactitud y completitud de los activos de información.
Disponibilidad	Propiedad de la información según la cual es accesible y utilizable oportunamente por las personas o sistemas o procesos autorizados, en el formato requerido para su procesamiento.

6. Lineamientos de política

6.1. Enunciado de la Política

La información es un activo vital para nuestra organización, y su disponibilidad, integridad y confidencialidad son fundamentales para nuestras operaciones y la toma de decisiones. Por lo

tanto, nos comprometemos a implementar y mantener un sistema de seguridad de la información robusto que garantice la protección de nuestros datos y sistemas. Este compromiso incluye el cumplimiento de buenas prácticas para el tratamiento de datos personales, conforme a la norma ISO/IEC 27018, especialmente cuando dichos datos sean procesados en entornos de nube pública.

6.2. De la información interna.

- La información es un activo vital, por lo que su utilización, es decir, accesos, procesamiento y mantenimiento deberán ser consistentes con lo instruido en las políticas, normas, y procedimientos emitidos por Fidelitas SA en cada ámbito en particular.

- La información debe ser protegida de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y en las recomendaciones dadas por el responsable designado de dicha información. A este conjunto de políticas y normas se le llamará también “Marco Normativo Seguridad de la Información”.

- Toda información creada o procesada por la organización debe ser considerada como “confidencial”, a menos que se determine expresamente lo contrario. Fidelitas SA proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo con sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.

6.3. De la información de los clientes o terceros.

- Cuando la organización procese y mantenga información de datos personales y/o sensibles de acuerdo con la normativa vigente, ésta se compromete a asegurar que dicha información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna, de conformidad a lo establecido en la Ley de Protección de Datos Personales (Ley 25.326).

- Cuando se requiera compartir información de Fidelitas SA con organizaciones externas, será requisito la suscripción de un contrato, cláusula y/o convenio de confidencialidad y no divulgación previo a la entrega de la información.

- Adicionalmente, Fidelitas se compromete a adoptar los principios y controles definidos en la norma ISO/IEC 27018 para la protección de datos personales procesados en servicios de computación en la nube, asegurando transparencia, consentimiento, responsabilidad, limitación de finalidad, minimización de datos y derechos del titular de los datos.

6.4. De los objetivos de Seguridad de la Información.

- Fidelitas SA asume como objetivos prioritarios la implementación de un modelo de seguridad de la información basado en ISO/IEC 27001 y en buenas prácticas complementarias, como ISO/IEC 27018 para la protección de datos personales en servicios en la nube.
- Fidelitas SA priorizará y enfocará sus esfuerzos en la adopción de medidas y prácticas de seguridad que le permitan proteger apropiadamente tanto la privacidad como la integridad y disponibilidad de la información de sus clientes.

6.5. De las auditorías.

- Con el fin de velar por el correcto uso de los activos de información, Fidelitas SA se compromete a realizar auditorías en cualquier momento para validar el cumplimiento de las políticas y documentos vigentes que tengan relación con el acceso y uso que los usuarios hacen de los activos de información.
- Las auditorías podrán ser realizadas internamente o por auditorías a cargo de organizaciones externas, cuando sea pertinente y requerido por el CTO, en coordinación con el Comité de Seguridad de la Información.

6.6. De la gestión de la seguridad de la información.

- La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por la organización. Este proceso deberá ser aplicado a los procesos críticos del negocio.
- El cumplimiento de los objetivos del sistema de gestión de seguridad de la información de Fidelitas SA se basará en la identificación de los activos de información involucrados en los procesos de negocio críticos, lo que implica al CTO, junto a los responsables de los diferentes procesos y subprocesos de negocio de Fidelitas SA, realizar las siguientes actividades fundamentales:
    - Identificar y clasificar los activos de información involucrados.
    - Para cada activo de información, identificar un responsable.
    - Analizar el riesgo al cual están expuestos.
    - Difundir en forma planificada entre todo el personal el objetivo corporativo de la preservación de la información, sus características y las responsabilidades individuales para lograrlo, inserto esto, en planes de capacitación anuales así como en el proceso de inducción del nuevo personal.

6.7. Deberes del personal y de terceros

Los deberes del personal y de terceros son:

- La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el cumplimiento de las funciones asignadas y autorizados por la jefatura directa, debiéndose aplicar criterios de buen uso. Ver más en Política de Gestión de los Dispositivos.
- Las claves de acceso a la información y a las tecnologías de información son de carácter individual, intransferibles y de responsabilidad única de su propietario. Ver más en Política de Gestión de Accesos y Autenticación.
- El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos que se establezcan en el manejo de incidentes. Ver más en Política de Gestión de Incidentes de Seguridad.
- Se prohíbe la divulgación de información que esté considerada o clasificada como "confidencial". Ver más en Política de Ciclo de Vida del Dato.
- La toma de conciencia en materia de seguridad y asistir a las capacitaciones definidas en el Programa de Concientización y Capacitación son de carácter obligatorio. Ver más en Política de Seguridad de la información en Recursos Humanos.
- Todos aquellos colaboradores que son partícipes del Plan de Continuidad y Plan de Recuperación ante Desastres deben actuar y estar disponibles tal como lo menciona el plan. Ver más en Política de Seguridad en la Continuidad del Negocio.
- Cumplir con todas las demás políticas y procedimientos establecidos por Fidelitas SA como parte de su estrategia de seguridad de la información.
- Cumplir con toda esta política, en caso de incumplimiento, el personal tendrá medidas disciplinarias e, incluso, acciones legales. Ver más en Código de Conducta.

6.8. Organización de la seguridad.

- Con el objetivo de garantizar el cumplimiento de la presente Política General de Seguridad de la Información y las políticas y normas específicas definidas en el Marco Normativo de Seguridad de la Información, Fidelitas SA ha establecido una estructura organizacional de seguridad que contempla la definición de funciones específicas en el ámbito de seguridad, las cuales se encuentran señaladas en el documento específico "Política de Comité de la Seguridad de la Información" y documento de "Estructura de Seguridad".

6.9. Revisión de la Política.

- Una de las tareas a realizar por el Comité de Seguridad de la Información de Fidelitas SA, es la reevaluación de la Política General de la Seguridad de la Información. Esto deberá realizarse por lo menos una vez al año o ante cualquier cambio significativo de tecnología, personal o evento que amerite su reevaluación para asegurar continuidad, idoneidad, eficiencia y efectividad.

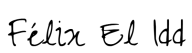
6.10. Difusión de la Política.

- La Dirección de Fidelitas SA considera fundamental integrar en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la seguridad de la información.

6.11. De las políticas/normas específicas de Seguridad de la Información

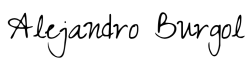
Se establecen y se consideran como parte de este marco normativo las políticas específicas de Seguridad de la Información:

- Seguridad de la información en Recursos Humanos
- Security Awareness
- Gestión de los Dispositivos
- Gestión de los Activos de información
- Ciclo de Vida del Dato
- Gestión de Acceso y Autenticación
- Gestión de la Criptografía
- Gestión de la Seguridad física
- Gestión de Inteligencia de Amenazas
- Gestión de los Servicios en Nube
- Tecnología y Operaciones
- Gestión de Logs
- Gestión de Vulnerabilidades Técnicas.
- Seguridad por Capas
- Desarrollo Seguro
- Gestión de Relaciones con los Proveedores
- Gestión de Incidentes de Seguridad de la información
- Seguridad en la Continuidad del Negocio
- Gestión del Cumplimiento Normativo y Regulatorio

Félix El Idd 

Jorge El Idd 

Natalia Queija 

Alejandro Burgol 

Registro de auditoría

Detalles

NOMBRE DEL ARCHIVO	Fidelitas - Política General de Seguridad.pdf - 8/8/25, 16:07
ESTADO	Firmado
MARCA DE TIEMPO DEL ESTADO	2025/08/08 21:00:03 UTC

Actividad

ENVIADA	natalia.queija@fidelitas.com.ar **ha enviado** una solicitud de firma a: • Jorge El Idd (jorge.elidd@fidelitas.com.ar) • Félix El Idd (felix@fidelitas.com.ar) • Natalia Queija (natalia.queija@fidelitas.com.ar) • Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/08/08 19:07:15 UTC
FIRMADO	**Firmado** por Jorge El Idd (jorge.elidd@fidelitas.com.ar)	2025/08/08 19:34:09 UTC
FIRMADO	**Firmado** por Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/08/08 21:00:03 UTC
FIRMADO	**Firmado** por Félix El Idd (felix@fidelitas.com.ar)	2025/08/08 20:40:13 UTC
FIRMADO	**Firmado** por Natalia Queija (natalia.queija@fidelitas.com.ar)	2025/08/08 19:11:51 UTC
COMPLETADO	Todos los firmantes han firmado este documento y ya se ha **completado**	2025/08/08 21:00:03 UTC

La dirección de correo indicada arriba para cada firmante puede estar asociada a una cuenta de Google. Puede ser la dirección de correo electrónico principal asociada a la cuenta o una secundaria.