
Fidelitas



MANUAL DE SEGURIDAD TI

Versión 2023-11

Fidelitas S.A.
teléfono. +54 11 5254 9950
dirección. Av. Cabildo 924 (C1426AAW)
C.A.B.A., Argentina

1) Introducción

a) Propósito: El propósito de este Manual de Seguridad de la Información es establecer un marco de políticas y procedimientos destinados a proteger la integridad, confidencialidad y disponibilidad de la información de nuestra organización. En un mundo cada vez más digitalizado, la información se ha convertido en uno de los activos más valiosos de cualquier entidad. Proteger esta información de amenazas internas y externas, errores humanos, fallos tecnológicos y desastres naturales no solo es fundamental para mantener la confianza de nuestros clientes y socios, sino también para cumplir con las obligaciones legales y regulatorias. Este manual tiene como objetivo asegurar que todos los miembros de la organización comprendan su papel en la protección de nuestros activos de información y estén equipados con el conocimiento y las herramientas necesarias para implementar estas políticas de manera efectiva.

b) Alcance: Este manual se aplica a toda la información que la organización genera, adquiere, almacena, procesa y transmite, independientemente de su formato (papel, electrónico, audiovisual, etc.) y medio de almacenamiento o transmisión (sistemas informáticos, dispositivos móviles, redes, etc.). Incluye datos almacenados en bases de datos, documentos, correos electrónicos, software, hardware y cualquier otro medio relacionado con la información. El alcance del manual abarca a todos los empleados, contratistas, consultores, temporales y otras personas que tienen acceso a la información de la organización, incluidos los terceros que actúan en nombre de la organización. Todos los individuos cubiertos por este alcance están obligados a adherirse a las políticas y procedimientos descritos en este manual como condición de su acceso a la información de la organización.

c) Responsabilidades:

i) Empleados: Todos los empleados son responsables de adherirse a las políticas y procedimientos de seguridad de la información descritos en este manual. Esto incluye, pero no se limita a, proteger la información confidencial, utilizar los recursos de la organización de manera segura y reportar cualquier incidente de seguridad de la información de manera oportuna.

ii) Equipos de TI: El departamento de Tecnologías de la Información (TI) es responsable de implementar y mantener las medidas técnicas necesarias para proteger la información de la organización. Esto incluye la gestión de la seguridad de la red, la administración de sistemas y bases de datos, el cifrado de datos sensibles y la implementación de controles de acceso.

iii) Dirección: La alta dirección es responsable de establecer la visión y el compromiso con la seguridad de la información a través de la creación de políticas, la asignación de recursos adecuados y el fomento de una cultura de seguridad dentro de la organización. Además, la dirección debe revisar y evaluar periódicamente la eficacia de las políticas y procedimientos de seguridad de la información para asegurar su adecuación y eficacia continuas.

iv) Este manual es un documento vivo que debe revisarse y actualizarse regularmente para reflejar los cambios en la tecnología, las amenazas a la seguridad, las prácticas comerciales y las leyes y regulaciones aplicables. Es responsabilidad de todos en la organización familiarizarse con el contenido de este manual y adherirse a las políticas y procedimientos aquí establecidos para proteger nuestra información y mantener la confianza de aquellos con quienes hacemos negocios.

2) Políticas Generales de Seguridad

a) Clasificación de la Información: La clasificación de la información es esencial para identificar el nivel de protección requerido para cada tipo de datos manejados dentro de la organización. Nuestra política de clasificación divide la información en cuatro categorías principales:

i) Pública: Información destinada a la divulgación pública, cuya divulgación no esperada no afectaría adversamente a la organización. Ejemplos incluyen material de marketing y comunicados de prensa.

ii) Interna: Información que es interna para la organización y que, aunque no es altamente sensible, debe ser protegida para evitar la divulgación no autorizada. Esto puede incluir políticas internas, procedimientos e información sobre empleados.

iii) Confidencial: Información que requiere restricciones de acceso y controles de seguridad más estrictos debido a su sensibilidad. La divulgación no autorizada podría tener un impacto adverso significativo en la organización, sus clientes o socios. Ejemplos incluyen datos personales de clientes, información financiera y contratos. En FIDELITAS S.A. se trata de información financiera de personas y empresas, tanto positiva como negativa, siempre con origen de fuentes públicas y oficiales (Afip, BCRA, Anses, etc).

iv) Secreto: La información más sensible cuya divulgación no autorizada podría causar daños extremadamente graves a la organización o a sus partes interesadas. Esta categoría se reserva para la información más crítica, como las patentes pendientes, los secretos comerciales y la información de seguridad nacional (cuando sea aplicable). En caso de FIDELITAS S.A., se trata de información que nos proveen los Clientes junto a sus propios requerimientos, por ejemplo un plan comercial, tipo de vínculo o contrato con un tercero a evaluar, etc. Son datos exclusivos de nuestros Clientes que no deben ser compartidos, ni transmitidos, ni impresos.

(a) Cada categoría requiere un nivel de protección correspondiente, desde medidas básicas de seguridad para información pública hasta controles de seguridad extremadamente rigurosos para información clasificada como secreta.

(b) Control de Acceso: La política de control de acceso tiene como objetivo garantizar que solo las personas autorizadas puedan acceder a la información de la organización, de acuerdo con su necesidad de conocer y su clasificación de seguridad. Los principios clave incluyen:

v) Autenticación: Todos los usuarios deben verificar su identidad mediante un método de autenticación, como una contraseña, un token de seguridad o datos biométricos.

vi) Autorización: Una vez autenticados, los usuarios solo deben tener acceso a la información y los recursos que son necesarios para sus funciones laborales. Esto se gestiona mediante la asignación de roles y permisos específicos.

vii) Principio de Privilegio Mínimo: Los usuarios deben tener el mínimo nivel de acceso necesario para realizar sus tareas, reduciendo el riesgo de acceso no autorizado a información sensible.

viii) Registro y Monitoreo: Todas las actividades de acceso deben ser registradas y monitoreadas para detectar y responder a incidentes de seguridad de manera oportuna.

b) Gestión de contraseñas: La política de contraseñas fuerte es fundamental para la seguridad de la información. Los requisitos para la creación y el manejo de contraseñas incluyen:

i) Longitud y Complejidad: Las contraseñas deben tener al menos 9 caracteres y contener una combinación de letras mayúsculas, letras minúsculas, números y/o símbolos especiales, tres de las cuatro características.

ii) Renovación: Las contraseñas deben cambiarse regularmente, al menos cada 120 días, y no deben reutilizarse.

iii) Almacenamiento y Transmisión Seguros: Las contraseñas deben almacenarse y transmitirse de forma segura, utilizando técnicas de cifrado para proteger contra el acceso no autorizado.

iv) Autenticación Multifactor (AMF): Cuando sea posible, se debe utilizar AMF para proporcionar una capa adicional de seguridad, combinando algo que el usuario sabe (una contraseña) con algo que el usuario tiene (token de seguridad o un teléfono móvil)

c) Gestión de Activos y Recursos

i) Responsabilidad sobre los activos: Objetivo: Asegurar la correcta gestión y protección de todos los activos de información mediante la asignación de responsabilidades específicas.

ii) Procedimientos:

(a) Inventario de Activos: Todos los activos de información deben ser identificados y registrados en un inventario centralizado. Esto incluye hardware, software, datos y cualquier otro recurso relevante para la operación de la organización.

(b) Asignación de Responsabilidades: Cada activo listado en el inventario debe tener un propietario asignado. El propietario es responsable de la clasificación del activo, la evaluación de riesgos asociados y la implementación de controles de seguridad adecuados.

(c) Revisión y Actualización: Los propietarios de activos deben revisar regularmente la clasificación y los controles de seguridad de sus activos para asegurar su pertinencia y efectividad frente a amenazas emergentes.

iii) TELETRABAJO

(a) El Equipo de TI debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de empleados o terceros, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

(b) Toda información gestionada y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de obligaciones contractuales.

(c) Deberán establecerse criterios de ventanas horarias de acceso y permisos, según cada empleado o tercero que deba acceder.

(d) Se deberá dejar registro de cada una de las IP desde la que se realizó cada acceso.

d) Uso Aceptable de los Recursos: Objetivo: Establecer reglas claras para el uso adecuado de los recursos informáticos y prevenir comportamientos que puedan comprometer la seguridad de la información.

i) Políticas:

(1) Hardware y Dispositivos: Se prohíbe el uso de dispositivos no autorizados dentro de la red corporativa. Todo hardware debe ser aprobado y configurado por el departamento de TI.

ii) Software y Aplicaciones:

(1) Solo se permite la instalación y uso de software licenciado y aprobado por la organización. Se debe evitar la instalación de software no esencial para las funciones laborales.

iii) Internet y Redes Sociales:

(1) El acceso a Internet debe ser utilizado de manera responsable y para fines laborales. Sitios web no relacionados con las actividades de la organización y plataformas de redes sociales deben utilizarse con moderación y nunca para compartir información confidencial.

e) Seguridad Física y del Entorno

i) Acceso Físico: Objetivo: Controlar el acceso físico a las instalaciones para proteger contra el acceso no autorizado, el daño o la interferencia con la información y los activos de información.

(1) Controles:

(a) Control de Accesos: Implementar sistemas de control de acceso electrónico para restringir la entrada a áreas sensibles solo al personal autorizado.

(b) Seguridad Física: Utilizar medidas de seguridad física, como cerraduras, barreras, guardias de seguridad y sistemas de vigilancia, para proteger las instalaciones.

(c) Gestión de Visitantes: Todos los visitantes deben ser registrados y acompañados en todo momento en áreas sensibles.

f) Protección contra Desastres: Objetivo: Implementar medidas de prevención, respuesta y recuperación para proteger la información ante desastres naturales o provocados por el hombre.Estrategias:

i) Copias de Seguridad: Realizar copias de seguridad regulares de todos los datos críticos y almacenarlas en una ubicación segura y geográficamente distante.

ii) Plan de Recuperación ante Desastres: Desarrollar y mantener un plan de recuperación ante desastres que incluya procedimientos para restaurar los sistemas y recuperar los datos en caso de un desastre.

iii) Pruebas y Revisiones: Realizar pruebas regulares del plan de recuperación ante desastres y revisar las estrategias de copia de seguridad para asegurar su efectividad continua.

3) Gestión de las Operaciones y Comunicaciones

a) Procedimientos y Responsabilidades Operativas: Establecer rutinas operativas diarias para mantener la integridad, disponibilidad y confidencialidad de la información. Procedimientos:

i) Revisión Diaria de Seguridad: El equipo de TI debe realizar revisiones de seguridad para detectar actividades anómalas o no autorizadas en la red y los sistemas.

ii) Actualización de Sistemas: Programar actualizaciones regulares de software y sistemas operativos para corregir vulnerabilidades y mejorar la seguridad.

iii) Copia de Seguridad: Realizar copias de seguridad diarias de datos críticos, almacenándolas en ubicaciones seguras y separadas físicamente.

b) Responsabilidades:

i) Equipo de TI: Implementar y monitorear los procedimientos de seguridad operativa.

ii) Empleados: Seguir las políticas de seguridad y reportar cualquier incidente de seguridad.

c) Transferencia de Información: Objetivo: Garantizar la seguridad de la información durante su transferencia, dentro y fuera de la organización. Métodos:

i) Cifrado: Utilizar cifrado de datos para todas las transferencias de información sensible.

ii) Canales Seguros: Emplear VPNs y conexiones seguras (como HTTPS) para la transferencia de datos.

iii) Políticas de Compartición: Establecer y comunicar políticas sobre el intercambio seguro de información con terceros

d) Gestión de Usuarios. Objetivo: Establecer procesos para la creación, asignación y revocación de derechos de acceso de los usuarios de manera efectiva y segura. Procedimientos:

i) Registro de Usuarios: Crear procedimientos estandarizados para el registro de nuevos usuarios, asegurando la verificación de su identidad y la asignación de accesos según las necesidades laborales.

ii) Revisión de Accesos: Realizar revisiones periódicas de los derechos de acceso para asegurar que correspondan con las necesidades actuales del puesto.

iii) Desactivación de Accesos: Establecer mecanismos automáticos o manuales para la rápida revocación de accesos cuando un usuario cambia de rol o deja la organización.

iv) Gestión de Privilegios: Objetivo: Controlar la asignación de privilegios administrativos para prevenir abusos y minimizar riesgos. Políticas:

(1) Principio de Menor Privilegio: Asegurar que los usuarios reciban solo los privilegios necesarios para realizar sus tareas.

(2) Supervisión de Privilegios: Monitorear el uso de cuentas con privilegios elevados para detectar y prevenir el mal uso.

(3) Autorización y Revisión: Establecer un proceso de autorización para la asignación de privilegios elevados y revisar regularmente dichas asignaciones.

4) Adquisición, Desarrollo y Mantenimiento de Sistemas

a) Seguridad en el Desarrollo de Sistemas: Asegurar que la seguridad se integre de manera efectiva en todas las fases de desarrollo y mantenimiento de sistemas de información para proteger contra amenazas y vulnerabilidades. Directrices:

i) Integración de la Seguridad desde el Diseño: Incorporar requisitos de seguridad desde las primeras etapas de diseño de cualquier nuevo sistema o aplicación, realizando análisis de riesgos y definiendo controles de seguridad adecuados.

ii) Revisión de Código Seguro: Implementar revisiones de código regularmente para identificar y remediar vulnerabilidades de seguridad en las aplicaciones.

iii) Pruebas de Seguridad: Realizar pruebas de penetración y evaluaciones de vulnerabilidad en todas las nuevas aplicaciones y sistemas antes de su puesta en producción, así como después de cualquier actualización significativa.

b) Protección de Datos Sensibles: Implementar medidas robustas para la protección de datos sensibles tanto en reposo como en tránsito, minimizando el riesgo de divulgación no autorizada. Métodos:

i) Cifrado de Datos: Utilizar técnicas de cifrado estándar de la industria para proteger datos sensibles, especialmente durante la transmisión a través de redes públicas e incluso en almacenamiento.

ii) Gestión de Claves: Establecer una política de gestión de claves segura para garantizar que el cifrado sea efectivo y las claves no sean susceptibles a compromisos.

5) Gestión de Incidentes de Seguridad: Establecer un proceso estructurado para responder de manera rápida y efectiva a los incidentes de seguridad, minimizando el impacto y restaurando la operatividad lo antes posible. Proceso:

a) Detección y Reporte:

i) Implementar mecanismos para la detección rápida de incidentes y establecer un proceso claro para su reporte.

ii) Análisis y Contención: Evaluar rápidamente el incidente para entender su alcance y aplicar medidas de contención para limitar el daño.

iii) Erradicación y Recuperación: Eliminar la causa raíz del incidente y recuperar los sistemas afectados a su estado operativo normal.

iv) Comunicación: Informar a las partes interesadas internas y externas según sea necesario, incluyendo a la dirección, usuarios afectados y, si es aplicable, a las autoridades reguladoras.

b) Aprendizaje de Incidentes. Objetivo: Desarrollar un ciclo de mejora continua a partir de la experiencia adquirida en la gestión de incidentes, para reforzar las políticas y prácticas de seguridad. Estrategias:

i) Revisión Post-Incidente: Realizar un análisis detallado después de cada incidente para identificar las causas raíz y las lecciones aprendidas.

ii) Actualización de Políticas y Procedimientos: Ajustar las políticas, procedimientos y controles de seguridad basándose en las lecciones aprendidas para prevenir la recurrencia de incidentes similares.

iii) Capacitación y Concienciación: Utilizar la información obtenida de los incidentes para mejorar los programas de capacitación y concienciación en seguridad, asegurando que todos los empleados comprendan su papel en la protección de la información.

6) Cumplimiento Normativo o Ley Aplicable

a) Las bases de datos personales a cargo de FIDELITAS S.A. se encuentran inscriptas ante el Registro Nacional De Bases De Datos De La Dirección Nacional De Protección De Datos Personales de la Agencia De Acceso A La Información Pública, en cumplimiento de los artículos 21 y 22 de la Ley Nº 25.326,modificatorios y complementarios (RL-2019-64978065-APN-DNPDP#AAIP).

b) Datos sensibles: FIDELITAS S.A. no trata ni tratará datos sensibles como origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Sólo se darán tratamiento a datos inherentes al cumplimiento del objeto

c) Cumplimiento: FIDELITAS S.A. reconocerá y permitirá el legítimo derecho de comercial para el que se procesan.acceso a la información comercial, crediticia y financiera proveniente de las fuentes antes mencionadas. Esto se enmarca en la Ley 25.326 de Protección de Datos Personales, que establece que las personas y empresas tienen derecho a conocer la información que consta sobre sí mismas en una base de datos, de forma gratuita. FIDELITAS S.A. cumplirá con las novedades y constancias documentales que aporte el Titular del Dato, a efectos de facilitar una rápida actualización, rectificación y supresión, de conformidad con los artículos 43 de la Constitución Nacional y 16 de la Ley 25.326.

7) Continuidad del Negocio y Planificación de la Recuperación ante Desastres

a) Planificación de la Continuidad del Negocio: Desarrollar y mantener planes para asegurar la continuidad de las operaciones críticas en caso de un incidente de seguridad grave.

8) Cumplimiento

a) Revisión y Auditoría: Realizar revisiones y auditorías periódicas para asegurar el cumplimiento de las políticas de seguridad de la información.

b) Legislación y Regulaciones: Asegurar que las políticas de seguridad estén en conformidad con las leyes y regulaciones relevantes.

9) Recolección de datos

Los datos recolectados por Fidelitas se realizan dependiendo de la forma en que la fuente pública los disponibiliza. Toda la información recolectada es procesada por personal con niveles de autorización suficientes para hacerlo. Dichos niveles de autorización están basados en roles predeterminados con permisos acotados para cada tipo de fuente que se esté tratando.

Los usuarios autorizados al proceso de las diferentes fuentes verificarán la integridad del mismo con el objetivo final de garantizar su exactitud y su correspondiente confidencialidad.

10) Control de acceso a la información

Toda la información administrada por Fidelitas es alojada en servidores de máxima seguridad y el acceso a dicha información está restringida al personal de IT de la empresa.

11) Control de acceso al sistema donde se procesa la información

Fidelitas realiza el procesamiento y el tratamiento de los datos mediante un sistema de gestión basado en roles de usuarios y las fuentes de datos que los mismos pueden manipular en el mismo.

- Rol de usuario básico: En este caso los usuarios solo podrán consultar los datos que le permitan los perfiles a los cuales se los ha asociado. No podrán modificar o eliminar datos..
- Rol de usuario supervisor: En este caso los usuarios podrán consultar y modificar los datos que le permitan los perfiles a los cuales se los ha asociado. No podrán eliminar datos.
- Rol de usuario administrador: En este caso los usuarios podrán consultar, modificar y eventualmente eliminar los datos que le permitan los perfiles a los cuales se los ha asociado.
- Rol de superusuario de datos: En este caso el usuario es el encargado del anonimizado de los datos que deban ser eliminados definitivamente luego del período de retención permitido por la Ley de protección de datos personales (25.326) según cada tipo de dato en específico.

12) Usuarios del sistema

- Todos los empleados deben autenticarse en los sistemas de Fidelitas mediante usuarios previamente provistos por el área de IT de la misma.
- Dichos usuarios reciben, en ese momento, la autorización de las fuentes de datos que podrán manipular según la función que vayan a desempeñar en la estructura de la empresa.
- La autenticación del usuario deberá realizarse con contraseñas complejas que tengan un mínimo de 10 (diez) caracteres siendo obligatorio el uso de por lo menos una letra mayúscula, un número y algún caracter especial como &, %, $, @, o #.
- El procesamiento de datos se realiza exclusivamente desde puestos presenciales en las instalaciones de la empresa mediante el uso de computadoras controladas por el departamento de IT.
- Los procesos de tratamiento de datos no se realizan desde terminales remotas distribuídas o mediante el uso de redes fuera de las instalaciones físicas de la empresa.
- Todas las actividades de los diferentes usuarios son registradas en el sistema guardando la trazabilidad de las mismas. Esto permite identificar la acción realizada, el usuario que la realizó, la fecha y hora de la misma y desde la computadora que fue realizada.
- Los usuarios que no registren actividades durante un lapso de 15 días son inactivados y dados de baja a los 60 días de inactividad. Transcurrido dicho plazo se deberá dar de alta nuevamente a otro usuario para continuar con las tareas asignadas.

13) Conservación de la información

La información recolectada por Fidelitas es mantenida dentro de la infraestructura tecnológica durante el período de vigencia que estipula la Ley de protección de datos personales (25.326) para cada tipo de dato. Los mismos varían entre los dos y cinco años dependiendo el caso.

14) Resguardo y recuperación de la información

La información de los sistemas de Fidelitas es resguardada diariamente. La misma se resguarda en formato encriptado utilizando AES-256. Los datos de respaldo son almacenados en discos de estado sólido en servidores separados de la infraestructura principal los cuales solo pueden ser accedidos desde el mismo centro de datos donde se alojan los mismos. La gerencia de IT será la responsable de dichos resguardos y del control de inventario de los mismos. Dichos datos de respaldo tienen un período de retención estipulado de 7 días.

La recuperación de la información debe ser autorizada en forma conjunta por el superusuario de datos y por la gerencia de IT. Esta recuperación se realiza sobre una estructura provisoria cerrada a estos efectos. Una vez restaurados los datos se procederá a su verificación en integridad quedando registrado los participantes de esta operación y el resultado de la misma.

15) Destrucción de la información

La información recolectada por Fidelitas es eliminada de la infraestructura tecnológica luego del período de vigencia que estipula la Ley de protección de datos personales (25.326) para cada tipo de dato. Esta tarea es responsabilidad del superusuario de datos. Solo este rol de usuario puede autorizar el anonimizado del dato que se debe eliminar de los registros del sistema. La información a ser eliminada es previamente encriptada con mecanismos de encriptación simétrica utilizando AES-256. Luego dichos datos son sobreescritos con cadenas de datos aleatorios los cuales a su vez son también encriptados mediante AES-256. Una vez eliminada mediante los procedimientos estandarizados para esta tarea, la misma no puede ser accedida por los sistemas de la empresa o por personal de IT.

16) Incidentes de seguridad

La gestión de vulnerabilidades en los sistemas informáticos es un proceso continuo que debe llevarse a cabo regularmente. Un escaneo de vulnerabilidad es válido en el momento en el que el mismo se realiza. Si se realizan actualizaciones de software más tarde o se introducen cambios en la topología, éstos pueden dar lugar a nuevas vulnerabilidades.

Es importante para cualquier organización hacer un seguimiento constante, verificar y repetir los procesos de gestión de la vulnerabilidad y llevar la información pertinente al sistema de gestión de la seguridad de la información.

Para asegurar la infraestructura de TI Fidelitas gestiona las posibles vulnerabilidades y brechas de seguridad mediante un escaneo regular, sistemático y controlado de la misma. Se realizan pruebas de penetración de todos los sistemas para detectar vulnerabilidades técnicas. Las vulnerabilidades identificadas se registran en un sistema de gestión de la seguridad de la información (SGSI). Las vulnerabilidades técnicas detectadas son priorizadas en función de su importancia y clasificadas para luego poder ser remediadas.