Fidelitas

Política de Uso Aceptable de Recursos Tecnológicos y Medios Extraíbles

Control de versiones

Código.	FIITPO019
Versión.	1.0
Fecha de la versión.	15/09/2025
Creado por.	Alejandro Burgol
Aprobado por.	Comité de seguridad
Clasificación.	Público

Historial de modificaciones

Fecha.	Versión.	Creado por.	Descripción de la modificación.
15/09/2025	1.0	Alejandro Burgol	Creación inicial del documento

Tabla de contenido

1. Objetivos y alcance

Establecer las normas de uso aceptable de los recursos tecnológicos de Fidelitas S.A., incluyendo el manejo de medios extraíbles, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información, en cumplimiento con ISO/IEC 27001:2022 y los lineamientos de ISO/IEC 27018 .
Esta política aplica a todos los colaboradores, contratistas y terceros que tengan acceso a sistemas, redes, dispositivos, aplicaciones y datos de Fidelitas S.A., tanto en entornos internos como en la nube.

2. Documentos de referencia

- Manual del SGSI de Fidelitas
- Política de Seguridad de la Información
- Política de Gestión de Activos
- ISO/IEC 27001:2022
- ISO/IEC 27018:2019

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

Colaboradores y terceros: cumplir con esta política en todo momento y reportar incidentes de seguridad.
Infraestructura y Seguridad: habilitar y controlar el uso de recursos tecnológicos y medios extraíbles, aplicar cifrado y medidas de seguridad.
Comité de Seguridad: revisar esta política anualmente y aprobar excepciones cuando corresponda.

5. Lineamientos de la política

Acceso a sistemas y datos

- Cada usuario es responsable de sus credenciales; no se comparten bajo ninguna circunstancia.
- El ingreso a sistemas o bases de datos debe hacerse siempre con usuario asignado y autorizado.
- Si se detecta un acceso indebido (intencional o por error), debe reportarse de inmediato al área de Infraestructura y Seguridad.

Uso de equipos y recursos tecnológicos

- Las computadoras, correo, internet y demás herramientas son para uso laboral. El uso personal está permitido sólo de forma ocasional y nunca debe poner en riesgo la seguridad ni interferir con el trabajo.
- Queda prohibido instalar software, extensiones o aplicaciones sin autorización de Infraestructura y Seguridad.
- No se permite descargar o almacenar en los equipos corporativos archivos que puedan afectar la seguridad (ejemplo: programas pirata, contenido malicioso o no relacionado con la actividad laboral).
- El transporte o movimiento de activos de información, equipos o medios fuera de las instalaciones de Fidelitas deberá estar previamente autorizado por la Gerencia correspondiente y documentado. Durante su traslado deberán aplicarse medidas de seguridad equivalentes a las implementadas dentro de la organización, asegurando la protección contra pérdida, acceso no autorizado o alteración.

Medios extraíbles (USB, discos externos, etc.)

- El uso de USB o discos externos es una **excepción** y sólo puede hacerse con autorización de Infraestructura y Seguridad.
- Si se autoriza, el dispositivo debe estar cifrado y libre de malware.
- Está prohibido copiar o mover información confidencial o datos personales de clientes/empleados a un USB, salvo autorización documentada y temporal.
- Bajo ningún motivo se deben conectar dispositivos personales (pendrives, discos duros, celulares) a equipos de Fidelitas.

Protección de información confidencial y PII

- Los datos de clientes, empleados y terceros solo se usan para fines laborales legítimos.
- Nunca deben ser almacenados en dispositivos personales, enviados por correo sin protección o compartidos por mensajería no autorizada.
- Cualquier información personal o sensible debe tratarse con cifrado y siguiendo las políticas de Fidelitas.

Correo electrónico y mensajería

- Se debe evitar enviar información de trabajo a cuentas personales.
- Está prohibido utilizar las cuentas de Fidelitas para suscripciones, registros personales o servicios no relacionados con la organización.

Monitoreo y cumplimiento

- Infraestructura y Seguridad puede monitorear el uso de equipos y sistemas para garantizar que se cumpla esta política.
- El incumplimiento se considera falta grave y puede tener sanciones disciplinarias o legales.

Félix El Idd	Jorge El Idd	Alejandro Burgol	Natalia Queija
Félix El Idd	Jorge El Idd	Alejandro Burgol	Natalia Queija

Registro de auditoría

Detalles

NOMBRE DEL ARCHIVO	Fidelitas - Política de Uso Aceptable de Recursos Tecnológicos y Medios Extraíbles.pdf - 16/9/25, 13:39
ESTADO	Firmado
MARCA DE TIEMPO DEL ESTADO	2025/09/16 17:43:07 UTC

Actividad

ENVIADA	natalia.queija@fidelitas.com.ar **ha enviado** una solicitud de firma a: • Félix El Idd (felix@fidelitas.com.ar) • Natalia Queija (natalia.queija@fidelitas.com.ar) • Jorge El Idd (jorge.elidd@fidelitas.com.ar) • Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/09/16 16:39:18 UTC
FIRMADO	**Firmado** por Félix El Idd (felix@fidelitas.com.ar)	2025/09/16 16:41:35 UTC
FIRMADO	**Firmado** por Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/09/16 17:25:21 UTC
FIRMADO	**Firmado** por Natalia Queija (natalia.queija@fidelitas.com.ar)	2025/09/16 17:43:07 UTC
FIRMADO	**Firmado** por Jorge El Idd (jorge.elidd@fidelitas.com.ar)	2025/09/16 17:06:09 UTC
COMPLETADO	Todos los firmantes han firmado este documento y ya se ha **completado**	2025/09/16 17:43:07 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.