Fidelitas

Política de Seguridad Física

Control de versiones

Código.	FIITPO010
Versión.	1.0
Fecha de la versión.	03/09/2025
Creado por.	Alejandro Burgol
Aprobado por.	Comité de Seguridad (Félix El Idd, Jorge El Idd, Alejandro Burgol, Natalia Queija)
Clasificación.	Público

Historial de modificaciones

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

Tabla de contenido

1. Objetivos y alcance

Objetivo

Esta política establece las directrices para la gestión de la seguridad física en FIDELITAS SA. con el fin de proteger a los activos, información, las instalaciones y empleados de la FIDELITAS SA contra amenazas físicas, asegurando un entorno de trabajo seguro.

Alcance

Esta política aplica a todas las instalaciones de la organización, empleados, contratistas, visitantes y terceros que accedan a las áreas protegidas

2. Documentos de referencia

- Manual de SGSI
- Política de SGSI
- ISO/IEC ISO 27001:2022
- ISO/IEC ISO 27018:2019
- OWASP (https://owasp.org.)

3. Vigencia del documento

Este documento es válido desde su fecha de aprobación.

El propietario del documento, CTO, es responsable de verificar y actualizar, de ser necesario al menos una vez al año o cuando surjan aspectos de contexto interno o externo que así lo ameriten.

4. Roles y responsabilidades

A continuación, las responsabilidades definidas según su rol:

- **CTO:**Definir y supervisar la estrategia de seguridad física vinculada a la protección de la información. Asegurar la integración con la política general de seguridad de la información. Revisar auditorías de seguridad física y reportar riesgos a la alta dirección. Además, debe garantizar el cumplimiento de normas de acceso físico y vigilancia.
- **Área de Infraestructura y Seguridad:** Asegurar la protección física de servidores, centros de datos y salas de comunicaciones. Controlar el acceso a equipos críticos y

dispositivos de almacenamiento de datos. Implementar medidas de redundancia y continuidad en caso de incidentes físicos. Monitorear el acceso físico a las instalaciones y áreas restringidas. Implementar controles de CCTV y patrullas de seguridad. Responder a incidentes físicos que puedan afectar la seguridad de la información. FIDELITAS SA aloja su centro de datos en IFX NETWORKS como proveedor de nube privada.

- **Recursos Humanos:** Gestionar el proceso de credenciales y accesos físicos para empleados y terceros. Coordinar la baja de accesos físicos al finalizar la relación laboral.
- **Usuarios Finales (Empleados y Terceros)** Cumplir con las normas de seguridad física establecidas. No compartir credenciales o accesos físicos sin autorización. Reportar incidentes de seguridad física que puedan comprometer la información.

5. Lineamientos de política

FIDELITAS SA considera los siguientes aspectos:

Seguridad edilicia

- Establecer y documentar políticas y procedimientos claros para la seguridad física. Estos deben abordar el control de accesos, la protección de activos, y la respuesta a emergencias.
- Todos los activos de información físicos clasificados como críticos deben ser protegidos de accesos no autorizados, en áreas seguras y controladas.
- Los activos serán evaluados y clasificados conforme a su grado de relevancia, de forma que se pueda priorizar el establecimiento de medidas de seguridad que permitan la protección de los activos más críticos en primer lugar
- Revisar y actualizar las políticas de seguridad física regularmente para adaptarlas a nuevas amenazas y cambios en la infraestructura.
- Se debe establecer el perímetro de seguridad física de la organización, considerando la protección contra amenazas externas y ambientales.
- Realizar levantamiento e inventariar y asegurar que todas las áreas de alta seguridad, rutas de evacuación y zonas restringidas están identificadas, viabilizadas y señalizadas.
- Implementar controles de acceso físico utilizando sistemas de autenticación robustos como tarjetas de acceso, biometría, o una combinación de estos.
- Se deben utilizar barreras físicas donde corresponda para evitar el acceso físico no autorizado
- Se debe otorgar acceso restringido a los proveedores a las áreas seguras sólo cuando sea necesario. Este acceso se debe autorizar y monitorear.
- Mantener un registro detallado de todos los accesos al edificio. Este registro debe ser revisado y auditado periódicamente para identificar accesos no autorizados o inusuales.

Seguridad en el Datacenter local de desarrollo

- Se debe restringir el acceso a las instalaciones a personal autorizado.
- Se debe diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes.
- Contar con el registro de mantenimiento del suministro de electricidad y ventilación.
- Se debe exigir registro de retiro de equipos con su debida autorización.
- Colocar cámaras de seguridad en puntos críticos y áreas de entrada/salida. Asegurarse de que el monitoreo sea continuo.
- Asegurarse de que las puertas y ventanas estén reforzadas y cuenten con cerraduras seguras.
- Garantizar condiciones adecuadas de iluminación y climatización en todas las áreas, especialmente en aquellas donde se encuentran equipos críticos.
- Establecer procedimientos para responder a incidentes de seguridad física y mantener un equipo de respuesta rápida para situaciones críticas.
- Debe existir un plan de evacuación y/o de emergencia del personal cuando sea necesario y para la protección de los activos de información críticos en caso de emergencia.

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

Registro de auditoría

Detalles

NOMBRE DEL ARCHIVO	Fidelitas - Política de Seguridad Física.pdf - 5/9/25, 15:11
ESTADO	Firmado
MARCA DE TIEMPO DEL ESTADO	2025/09/05 19:01:55 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)	2025/09/05 18:11:46 UTC
FIRMADO	**Firmado** por Jorge El Idd (jorge.elidd@fidelitas.com.ar)	2025/09/05 18:13:26 UTC
FIRMADO	**Firmado** por Félix El Idd (felix@fidelitas.com.ar)	2025/09/05 19:01:55 UTC
FIRMADO	**Firmado** por Alejandro Burgol (alejandro.burgol@fidelitas.com.ar)	2025/09/05 18:47:44 UTC
FIRMADO	**Firmado** por Natalia Queija (natalia.queija@fidelitas.com.ar)	2025/09/05 18:12:09 UTC
COMPLETADO	Todos los firmantes han firmado este documento y ya se ha **completado**	2025/09/05 19:01:55 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.