POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Propósito

Establecer el marco de gobierno, controles, protocolos operativos y evidencias para proteger la confidencialidad, integridad y disponibilidad de la información propia y de terceros, cumpliendo con las exigencias contractuales de aliados y mejores prácticas ISO/IEC 27001:2022.

Alcance

Aplica a todo el personal, contratistas, proveedores y sistemas bajo control de la empresa, tanto en las sedes como en la nube, redes corporativas y dispositivos utilizados para acceder a activos de información.

Referencias normativas

- ISO/IEC 27001:2022 y 27002:2022.
- Guías internas de Aplicaciones e Infraestructura (seguridad de TI).
- Requisitos del aliado ENEL (SGL 08 – SaaS; SGL 10 – Infra; SGL 11 – IaaS).
- Ley de Protección de Datos Personales aplicable (p. ej., Ley 1581/2012 en Colombia) y normativa local vigente.
- NIST 800 88 (Saneamiento de medios).
- PCI DSS v3 (si aplica a datos de pago).

PRESENCIA Colombo Suiza, en su compromiso con la seguridad de la información, establece las siguientes reglas generales para el uso de los activos de información:

1. Uso Exclusivo para Fines Laborales

Los activos de información, incluidos dispositivos, aplicaciones y datos, deben utilizarse exclusivamente para fines laborales relacionados con las actividades de la organización.

2. Protección de Información Confidencial

Se debe proteger la información confidencial y sensible de la organización, evitando su divulgación no autorizada. Esto incluye el uso de contraseñas fuertes y el cifrado de datos cuando sea necesario.

3. Acceso y Autenticación

El acceso a los activos de información debe estar limitado a los empleados autorizados. Se deben utilizar métodos de autenticación adecuados (como contraseñas y autenticación de dos factores) para garantizar la seguridad.

4. Uso Responsable de Recursos

Los empleados deben utilizar los activos de información de manera responsable y eficiente, evitando el uso excesivo de recursos como ancho de banda, almacenamiento y tiempo de procesamiento.

5. Prohibición de Instalación de Software No Autorizado

Está prohibido instalar o utilizar software no autorizado en los dispositivos de la organización. Solo se deben utilizar aplicaciones y herramientas aprobadas por el departamento de TI.

6. Mantenimiento de la Integridad de los Datos

Los empleados son responsables de mantener la integridad y precisión de los datos. Cualquier error o inconsistencia debe reportarse al jefe inmediato.

7. Cumplimiento de Políticas y Normativas

Todos los empleados deben cumplir con las políticas de seguridad de la información y las normativas legales aplicables. Esto incluye regulaciones como GDPR (reglamento general de protección de datos).

8. Responsabilidad en el Uso de Dispositivos Móviles

Los dispositivos móviles (como celulares, tablets, y equipos portátiles) utilizados para acceder a información corporativa deben estar protegidos con contraseñas y mecanismos de seguridad. No se deben hacer conexiones a redes públicas no seguras con los equipos de la Organización y para el caso de equipos personales no se debe acceder a información si no se está conectado a una red segura.

9. Devolución de Activos de Información

Al finalizar la relación laboral o cuando se cambien de cargo, los empleados deben devolver todos los activos de información (dispositivos, documentos, credenciales, etc.) en su estado original.

10. Reporte de Incidentes de Seguridad

Cualquier incidente de seguridad, como pérdida, robo o uso indebido de activos de información, debe ser reportado de inmediato al área de TI y al jefe inmediato para su gestión y mitigación.

11. Gobierno, roles y responsabilidades

Se establece un marco de gobierno que define claramente los roles y responsabilidades para la gestión segura y eficiente de los recursos tecnológicos. La alta dirección garantiza la alineación de las estrategias de TI con los objetivos institucionales, los responsables de TI administran la infraestructura y los servicios, y los usuarios finales cumplen con las normas de uso y seguridad establecidas. Este enfoque asegura una gestión transparente, controlada y orientada a la mejora continua.

- Dirección General: aprueba la política; provee recursos.
- Comité de Seguridad: supervisa riesgos, cumplimiento y planes.
- Líder de TI: implementa y mantiene el SGSI (sistema de gestión de seguridad de la información).
- Líder de Desarrollo: gestiona SoA (arquitectura orientada a la información) y evidencias.
- Dueños de Activo: definen requisitos de acceso y clasificación.
- Responsables de TI (custodios): operan controles técnicos (logs, parches, respaldos, redes, etc.).
- Usuarios: cumplen políticas, procedimientos y reportan incidentes.

12. Gestión de riesgos

Presencia hace identificación, evaluación y mitigación de riesgos que puedan afectar la disponibilidad, integridad y confidencialidad de la información y registra los aspectos de riesgos con sus respectivos planes de mitigación en la Matriz de Riesgos General . La gestión de riesgos en TI se desarrolla de forma continua, asegurando que se implementen controles preventivos y correctivos adecuados. La alta dirección supervisa el proceso, mientras que los responsables de TI ejecutan las acciones necesarias para minimizar el impacto de posibles incidentes y garantizar la continuidad operativa de los servicios tecnológicos.

13. Clasificación y manejo de la información

La información se clasifica según su nivel de sensibilidad y criticidad, asignando controles de acceso y protección acordes a cada categoría. Todo el personal es responsable de manejar los datos conforme a estas directrices, asegurando su uso ético, seguro y conforme a la normativa vigente sobre protección de la información.

14. Gestión de activos

El área de TI es responsable de mantener actualizada la base de datos donde se registra el inventario de equipos y licencias utilizadas en PRESENCIA.

15. Privacidad y datos personales

La organización garantiza la protección de la privacidad y el adecuado tratamiento de los datos personales, conforme a la Ley 1581 de 2012 y las demás normas que la complementan. La

organización se compromete a recolectar, almacenar, usar y eliminar los datos personales de manera lícita, segura y transparente, asegurando que se utilicen únicamente para los fines autorizados por el titular. Todo el personal debe cumplir con las medidas de seguridad y confidencialidad establecidas, previniendo el acceso, uso o divulgación no autorizada de la información personal.

16. Concientización y formación

La organización se compromete a desarrollar programas de capacitación periódicos que fortalezcan la cultura de seguridad de la información, el cumplimiento de las normas internas y la adopción de buenas prácticas digitales. Cada empleado es responsable de aplicar los conocimientos adquiridos para prevenir incidentes y contribuir a la protección de los activos tecnológicos e informativos de la entidad.

17. Realización de Auditorías

Con el fin de garantizar el cumplimiento de las políticas establecidas en materia de seguridad de la información, la organización podrá realizar auditorías internas y/o externas de forma periódica o cuando se considere necesario. Estas auditorías tendrán como objetivo verificar la correcta aplicación de los controles, identificar posibles desviaciones y proponer acciones de mejora que fortalezcan la protección de los activos de información y aseguren la confidencialidad, integridad y disponibilidad de los datos.

18. Verificación del cumplimiento

El incumplimiento de las políticas, normas y procedimientos de seguridad de la información será considerado una falta disciplinaria y estará sujeto a las sanciones establecidas en el Reglamento Interno de Trabajo y demás disposiciones legales vigentes. Dichas sanciones podrán aplicarse según la gravedad de la infracción y el impacto generado sobre los activos de información, con el propósito de promover la responsabilidad, la confidencialidad y el uso adecuado de los recursos informáticos de la organización.

Medellín, 15 de noviembre de 2025.

JUAN FELIPE RENDÓN OCHOA

Director General