INSTALTEC
SERVICIOS Y MANTENIMIENTOS DE INGENIERÍA

POLÍTICA DE SEGURIDAD DE LA INFORMACION

ELABORÓ	REVISÓ	APROBÓ
Samara Camacho	Dirección	Dirección General
Coordinador de Calidad	Responsable de Revisión	Aprobación Final

REVISIÓN	FECHA	CAMBIO
REV00	21/05/2025	Emisión inicial

ÍNDICE

1. PROPÓSITO

El propósito de esta política es garantizar la confidencialidad, integridad y disponibilidad de la información manejada por INSTALTEC (Representada por Jorge Alberto Alday Arana) protegiendo los datos de clientes, proveedores, empleados y la propia empresa frente a posibles amenazas internas y externas.

2. ALCANCE

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que accedan, procesen o manejen información perteneciente a INSTALTEC. Se aplica a todos los sistemas de información, equipos y medios digitales o físicos utilizados en las operaciones de la empresa.

3. PRINCIPIOS GENERALES

- CONFIDENCIALIDAD:

Garantizar que la información sensible solo sea accesible por personas autorizadas.

- INTEGRIDAD:

Proteger la precisión y confiabilidad de la información, evitando alteraciones no autorizadas.

- DISPONIBILIDAD:

Asegurar que la información esté accesible en el momento en que sea necesaria.

4. RESPONSABILIDADES

- DIRECCIÓN GENERAL:

Proveer recursos y liderazgo para garantizar el cumplimiento de esta política.

- RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN (RSI):

Coordinar las acciones necesarias para implementar, supervisar y mejorar las medidas de seguridad.

- EMPLEADOS:

Cumplir con esta política y reportar incidentes de seguridad o comportamientos sospechosos.

- PROVEEDORES Y CONTRATISTAS:

Cumplir con los estándares de seguridad estipulados por INSTALTEC.

5. NORMAS Y PROCEDIMIENTOS

1. CONTROL DE ACCESO:

- Los sistemas de información deben contar con contraseñas seguras y actualizadas regularmente.
- El acceso debe estar restringido según roles y responsabilidades.

2. PROTECCIÓN DE DATOS:

- Se implementarán mecanismos para el cifrado de información sensible.
- Toda la información de clientes y empleados será tratada conforme a las leyes de protección de datos aplicables.

3. GESTIÓN DE INCIDENTES:

- Todos los incidentes de seguridad deberán ser reportados al RSI inmediatamente.
- Se realizará una investigación para mitigar riesgos y prevenir incidentes futuros.

4. USO APLICABLE DE RECURSOS:

- Los recursos tecnológicos (equipos, correos, software) deben utilizarse exclusivamente para fines laborales.
- Esta prohibida la instalación de software no autorizado.

5. RESPALDO Y RECUPERACIÓN:

- Los datos críticos de la empresa serán respaldados periódicamente.
- Se desarrollará y mantendrá un plan de recuperación ante desastres para garantizar la continuidad del negocio.

6. CAPACITACIÓN

Todos los empleados recibirán capacitación periódica en seguridad de la información, incluyendo buenas prácticas, identificación de amenazas y manejo de datos sensibles.

7. CUMPLIMIENTO Y SANCIONES

El incumplimiento de esta política puede derivar en medidas disciplinarias, que incluyen desde amonestaciones hasta la terminación de la relación laboral o contractual. En caso de violaciones graves, se podrán iniciar acciones legales.

8. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada al menos una vez al año o cuando se detecten cambios significativos en los procesos de negocio o en el entorno de amenazas.