

POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

1. Objetivo

Establecer los lineamientos, principios y controles necesarios para proteger la información de la empresa durante todo su ciclo de vida, garantizando su confidencialidad, integridad, disponibilidad y uso adecuado, así como el cumplimiento de la legislación colombiana vigente en materia de protección de datos y seguridad de la información.

2. Alcance

La presente política aplica para:

- Todos los colaboradores, contratistas, proveedores y terceros que tengan acceso a la información de la empresa.
- Todos los activos de información, sistemas tecnológicos, redes, aplicaciones, dispositivos y medios físicos o digitales utilizados en la organización.
- Toda la información generada, procesada, almacenada o transmitida por la empresa.

3. Principios de Seguridad de la Información

La empresa adopta los siguientes principios fundamentales:

3.1 Confidencialidad

La información solo podrá ser accedida por personas autorizadas y para fines laborales legítimos.

3.2 Integridad

La información deberá mantenerse completa, precisa y protegida contra modificaciones no autorizadas.

3.3 Disponibilidad

Los sistemas y datos deberán estar accesibles cuando sean requeridos para la operación del negocio.

3.4 Legalidad y Cumplimiento

Todas las actividades relacionadas con el manejo de información deberán cumplir la normatividad colombiana vigente y los estándares internos definidos por la empresa.

4. Lineamientos Generales

4.1 Protección de Infraestructura Tecnológica

La empresa implementará mecanismos de seguridad como:

- Antivirus y antimalware corporativo.
- Firewalls.
- Copias de seguridad periódicas.
- Controles de acceso y autenticación segura.
- Actualizaciones y parches de seguridad.
- Implementación de VPN.
- Implementación de VLANs.

4.2 Gestión de Accesos

El acceso a la información será otorgado bajo el principio de mínimo privilegio, según funciones y responsabilidades de cada usuario.

4.3 Uso Adecuado de Recursos Tecnológicos

Los recursos tecnológicos deberán utilizarse exclusivamente para fines corporativos autorizados.

Se prohíbe:

- Compartir credenciales.
- Instalar software no autorizado.
- Manipular información sin autorización.
- Utilizar dispositivos externos inseguros.

4.4 Monitoreo y Prevención

La empresa podrá monitorear el uso de sus sistemas, redes y equipos con el fin de prevenir incidentes de seguridad y accesos indebidos.

4.5 Gestión de Incidentes

Todo incidente de seguridad deberá ser reportado inmediatamente al área responsable para su análisis, contención y mitigación.

4.6 Seguridad con Proveedores y Terceros

Los terceros que tengan acceso a información corporativa deberán cumplir controles y acuerdos de confidencialidad definidos por la empresa.

4.7 Capacitación y Cultura Organizacional

La empresa promoverá programas de formación y concientización sobre buenas prácticas de ciberseguridad y protección de datos.

5. Protección de Datos Personales

El tratamiento de datos personales deberá realizarse conforme a la:

- Ley 1581 de 2012.
- Ley 1273 de 2009.
- Decreto 1377 de 2013.

La empresa adoptará medidas para garantizar la privacidad, seguridad y correcto tratamiento de la información personal de clientes, empleados y proveedores.

6. Responsabilidades

Colaboradores

- Cumplir esta política y los procedimientos asociados.
- Proteger la información bajo su responsabilidad.
- Reportar incidentes o riesgos de seguridad.

Áreas de Tecnología

- Implementar y mantener controles de seguridad.
- Realizar monitoreo preventivo.
- Gestionar respaldos y recuperación de información.

Dirección

- Garantizar recursos y apoyo para el cumplimiento de esta política.

7. Incumplimiento

El incumplimiento de esta política podrá generar medidas disciplinarias, sanciones contractuales o acciones legales conforme a la normativa vigente y reglamentos internos de la empresa.

8. Vigencia

La presente Política de Seguridad de la Información entra en vigencia a partir de mayo de 2025 y será revisada periódicamente o cuando existan cambios regulatorios, tecnológicos o estratégicos que así lo requieran.

