POLÍTICA DE TECNOLOGÍAS DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

1. OBJETIVO

Establecer los lineamientos para el uso, administración, protección y control de las Tecnologías de la Información y las Comunicaciones (TIC), garantizando la confidencialidad, integridad, disponibilidad y legalidad de la información institucional y de terceros.

2. ALCANCE

Aplica a:

- Todos los trabajadores, contratistas, practicantes y terceros.
- Equipos de propiedad de la empresa.
- Equipos personales que accedan a recursos corporativos (BYOD).
- Servicios en la nube, servidores, redes, correo electrónico e internet.

3. FUNDAMENTO LEGAL

La presente política se fundamenta en:

- Ley 1581 de 2012 (Protección de Datos Personales)
- Decreto 1377 de 2013
- Ley 1273 de 2009 (Delitos Informáticos)
- Ley 1266 de 2008 (Habeas Data)
- Normativa laboral vigente
- Política interna de Tratamiento de Datos Personales

4. PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN

La gestión tecnológica se regirá por los siguientes principios:

- Confidencialidad
- Integridad
- Disponibilidad
- Legalidad
- Responsabilidad
- Trazabilidad

5. LINEAMIENTOS GENERALES

5.1 Uso institucional

Los recursos tecnológicos deben utilizarse exclusivamente para fines laborales y misionales.

Se prohíbe su uso para:

- Actividades ilegales
- Acoso, discriminación o violencia digital
- Descarga de software no autorizado
- Uso con fines lucrativos personales

5.2 Protección de Datos Personales

Todo tratamiento de datos personales realizado a través de medios tecnológicos deberá cumplir con la Política de Tratamiento de Datos Personales y la normatividad vigente.

Queda prohibida:

- La extracción no autorizada de bases de datos.
- La transmisión de información confidencial sin autorización.
- El almacenamiento de datos personales en dispositivos no autorizados.

5.3 Clasificación de la información

La información se clasifica en:

- Pública
- Uso Interno
- Confidencial
- Reservada

El usuario es responsable de proteger la información según su nivel de clasificación.

6. CONTROL DE ACCESO Y CONTRASEÑAS

- Cada usuario tendrá credenciales individuales e intransferibles.
- Las contraseñas deberán tener mínimo **12 caracteres**, combinando mayúsculas, minúsculas, números y caracteres especiales.
- Se implementará autenticación multifactor (MFA) para accesos críticos.

- El bloqueo automático se activará tras 5 minutos de inactividad.
- El cambio obligatorio de contraseña será cada 60 días o antes si existe riesgo.

7. TRABAJO REMOTO Y DISPOSITIVOS PERSONALES (BYOD)

- El acceso remoto deberá realizarse mediante VPN o canales seguros autorizados.
- Está prohibido el acceso desde redes públicas sin protección.
- Los equipos portátiles deberán contar con cifrado de disco y antivirus actualizado.
- El usuario es responsable de la custodia del equipo fuera de las instalaciones.

8. COPIAS DE SEGURIDAD Y ALMACENAMIENTO

- La información institucional deberá almacenarse prioritariamente en repositorios corporativos autorizados (servidores o nube institucional).
- Se prohíbe el almacenamiento exclusivo en discos locales.
- Se realizarán copias de seguridad periódicas automatizadas.
- Las copias estarán protegidas contra alteración y acceso no autorizado.

9. MONITOREO Y CONTROL

La empresa podrá realizar monitoreo de los recursos tecnológicos bajo criterios de:

- Legalidad
- Necesidad
- Proporcionalidad
- Transparencia

El monitoreo respetará los derechos fundamentales a la intimidad y al habeas data, informando previamente a los colaboradores.

10. GESTIÓN DE INCIDENTES DE SEGURIDAD

Todo incidente deberá reportarse inmediatamente al área de Sistemas.

Se consideran incidentes:

- Acceso no autorizado
- Robo o pérdida de equipos
- Virus o ransomware

- Filtración de información
- Intentos de suplantación

La empresa activará el protocolo interno de gestión de incidentes y evaluará la necesidad de notificación a la autoridad competente cuando aplique.

11. SOFTWARE Y LICENCIAMIENTO

- Solo el área de Sistemas podrá instalar software.
- Está prohibido el uso de software sin licencia.
- Se mantendrá inventario actualizado de licencias.
- Se realizarán auditorías periódicas.

12. PROVEEDORES TECNOLÓGICOS

Los proveedores deberán:

- Garantizar confidencialidad.
- Suscribir acuerdos de nivel de servicio (SLA).
- Cumplir estándares mínimos de seguridad.
- Proteger los datos tratados por cuenta de la empresa.

13. SANCIONES

El incumplimiento de esta política podrá generar:

- Medidas disciplinarias internas.
- Terminación del contrato.
- Acciones civiles o penales conforme a la Ley 1273 de 2009.

14. RESPONSABILIDADES

Área de Sistemas

- Administrar infraestructura tecnológica.
- Gestionar riesgos digitales.
- Implementar controles de seguridad.
- Ejecutar plan anual de mantenimiento.

Usuarios

- Usar adecuadamente los recursos.
- Proteger sus credenciales.
- Reportar incidentes.
- Cumplir esta política.

15. VIGENCIA Y ACTUALIZACIÓN

La presente política entra en vigencia a partir de su firma y será revisada anualmente o cuando exista modificación normativa relevante.

JOHN FABIO PEÑA BERMEO
REPRESENTANTE LEGAL
Fecha: 04/03/2026

CONTROL DE CAMBIOS

VERSIÓN	PÁGINA	DESCRIPCIÓN DEL CAMBIO	FECHA
1	Todas	Creación del documento	04/03/2024
2	Todas	Revisión y Actualización	04/03/2025
3	Todas	Revisión y Actualización	04/03/2026
Elaboró: Responsable del SIG		**Revisó y aprobó:** Gerente General	