POLÍTICA DE SEGURIDAD DIGITAL

1. OBJETIVO

Establecer las directrices que orienten el uso seguro, responsable y confiable de la información y los recursos tecnológicos de **UT GLOBALCOTEL**, con el fin de prevenir incidentes digitales, proteger los activos de información y garantizar la continuidad de las operaciones, conforme a la normatividad colombiana vigente.

2. ALCANCE

Esta política aplica a todos los colaboradores, contratistas, proveedores y terceros que, por sus funciones, tengan acceso a la infraestructura tecnológica, sistemas de información, bases de datos, redes o cualquier recurso digital de la empresa.

Incluye el uso de equipos institucionales, dispositivos móviles, correo electrónico, aplicaciones corporativas y servicios en la nube.

3. MARCO NORMATIVO

La presente política se fundamenta en las siguientes disposiciones:

- Ley 1273 de 2009, sobre la protección de la información y los datos.
- Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013, sobre protección de datos personales.
- Ley 1712 de 2014, de Transparencia y Acceso a la Información Pública.
- Decreto 2106 de 2019 y la Política de Gobierno Digital.
- CONPES 3975 de 2019, Política Nacional de Confianza y Seguridad Digital.
- Resolución 500 de 2021 del Ministerio TIC.

4. PRINCIPIOS

La gestión de la seguridad digital en **UT GLOBALCOTEL** se rige por los siguientes principios:

- **Confidencialidad:** La información solo será accesible a personas autorizadas.

- **Integridad:** Se garantizará que los datos no sean alterados o modificados de manera no autorizada.
- **Disponibilidad:** La información y los sistemas deberán estar disponibles cuando sean requeridos.
- **Trazabilidad:** Toda acción sobre los sistemas deberá poder ser auditada y verificada.
- **Legalidad:** Todas las actuaciones deberán ajustarse a la legislación colombiana vigente.
- **Responsabilidad compartida:** Todos los miembros de la organización son responsables de la seguridad digital.

5. LINEAMIENTOS GENERALES

- Los usuarios deberán utilizar credenciales personales y mantenerlas bajo estricta confidencialidad.
- Está prohibido compartir contraseñas o acceder con las credenciales de otra persona.
- Las contraseñas deberán renovarse periódicamente y cumplir con los parámetros de seguridad establecidos.
- Los recursos tecnológicos deberán utilizarse exclusivamente para fines laborales.
- Todo incidente de seguridad (virus, pérdida de información, accesos no autorizados, entre otros) deberá reportarse de inmediato al área de sistemas o al responsable designado.
- La información institucional solo podrá almacenarse y respaldarse en medios o plataformas autorizadas por la empresa.
- Se realizarán copias de seguridad de manera periódica, conforme al plan de respaldo establecido.
- No se permitirá la instalación de programas o aplicaciones sin autorización previa del área de tecnología.
- Se deberá mantener actualizado el software y antivirus en todos los equipos institucionales.
- La información clasificada como confidencial no podrá ser divulgada ni transmitida por medios no seguros.

6. ROLES Y RESPONSABILIDADES

- **Gerencia General:** Aprobar la política y garantizar los recursos para su implementación.
- **Área de Tecnología o Sistemas:** Administrar los recursos tecnológicos, aplicar las medidas de seguridad y mantener actualizado el plan de protección digital.
- **Talento Humano:** Coordinar la capacitación y socialización de esta política entre los colaboradores y contratistas.
- **Colaboradores y Contratistas:** Cumplir las disposiciones aquí establecidas y reportar cualquier anomalía o incidente.

7. GESTIÓN DE INCIDENTES DIGITALES

UT GLOBALCOTEL contará con un procedimiento interno para la gestión de incidentes digitales, que incluirá las fases de detección, análisis, contención, recuperación y reporte.

Todos los eventos deberán documentarse para aplicar las acciones correctivas y preventivas necesarias.

8. CAPACITACIÓN Y CONCIENTIZACIÓN

La empresa promoverá actividades periódicas de sensibilización y formación en temas de seguridad digital, protección de la información y buenas prácticas de uso de herramientas tecnológicas, buscando fortalecer la cultura de seguridad en todos los niveles organizacionales.

9. CUMPLIMIENTO Y SANCIONES

El incumplimiento de los lineamientos de esta política podrá generar sanciones disciplinarias, contractuales o legales, según la gravedad del hecho y lo establecido en el reglamento interno de trabajo o los contratos suscritos.

10. REVISIÓN Y ACTUALIZACIÓN

Esta política será revisada y actualizada cada año, o cuando existan cambios normativos, tecnológicos o estructurales que lo requieran.



GABRIEL A. CARDENAS CARDENAS
Representante Legal
UT GLOBALCOTEL
Fecha: 08 octubre del 2025.