# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN - TELCOSUR S.A.S.

En **TELCOSUR S.A.S.**, conscientes de la importancia de proteger los datos personales, la información corporativa y la infraestructura tecnológica, adoptamos la presente **Política de Seguridad de la Información** como pilar de nuestro Sistema de Gestión de Seguridad de la Información (SGSI).

## 1. Objetivo

Garantizar la **confidencialidad, integridad y disponibilidad** de la información, así como la seguridad de la infraestructura tecnológica (redes **FTTH y de RADIO**), los sistemas internos y los datos personales de nuestros usuarios, colaboradores y aliados.

## 2. Alcance

- Todos los procesos, sedes y sistemas de la organización, incluidos NOC, core, acceso y CPE provistos al usuario.
- Todo el personal (colaboradores y contratistas) y terceros con acceso a nuestros activos.
- Activos de información y tecnológicos, desde el núcleo de red hasta el usuario final, incluyendo plataformas de soporte y facturación.

## 3. Principios

- **Confidencialidad:** Acceso a la información únicamente por personas autorizadas.
- **Integridad:** Protección de la exactitud, consistencia y completitud de la información.
- **Disponibilidad:** Asegurar el acceso oportuno a la información y a los sistemas cuando se requieran.
- **Legalidad:** Cumplimiento de la normativa colombiana aplicable (Ley 1581 de 2012, Ley 1266 de 2008, Ley 1273 de 2009, Decreto 1377 de 2013, entre otras) y de estándares internacionales (ej. **GDPR**).

## 4. Evaluación de Riesgos

La compañía realiza periódicamente análisis de riesgos para identificar, valorar y tratar amenazas que puedan afectar la infraestructura, tales como:

- Acceso no autorizado a equipos de red (ONT/OLT).
- Interrupciones del servicio por daños físicos.
- Intercepción de datos en la fibra óptica.
- Ataques de denegación de servicio distribuido (**DDoS**).

- Fugas o pérdida de bases de datos de usuarios.

## 5. Controles de Seguridad

### 5.1 Controles Técnicos

- Cifrado de datos en tránsito (**TLS / extremo a extremo**).
- listas de control de acceso y segmentación por zonas.
- Autenticación multifactor (**MFA**) en accesos críticos.
- Monitoreo continuo de red y registros de eventos.

### 5.2 Controles Operacionales

- Gestión de accesos físicos y lógicos a la infraestructura.
- Respaldo periódico de configuraciones y datos críticos.
- Procedimientos de control de cambios estandarizados.

### 5.3 Controles Físicos

- Seguridad perimetral en instalaciones críticas (OLTs, nodos de red).
- Cámaras de vigilancia y alarmas en sitios estratégicos.

## 6. Gestión de Incidentes de Seguridad

Contamos con un procedimiento formal que incluye:

1. Identificación y contención del incidente.
2. Análisis y gestión.
3. Corrección, restauración y mejora posterior.
4. Documentación y lecciones aprendidas.

## 7. Capacitación y Concientización

Todos los colaboradores reciben capacitación inicial y anual sobre:

- Riesgos en redes
- Protocolos de gestión de incidentes.
- Campañas periódicas contra phishing/ingeniería social y buenas prácticas en Wi-Fi/CPE.
- Protección de datos personales y cumplimiento normativo.

## 8. Mejora Continua

La política se revisa **anualmente** o cuando existan cambios tecnológicos, normativos o en la infraestructura, garantizando su alineación con los principios de **mejora continua** del SGSI.

## 9. Contacto

Para inquietudes relaciones con esta política, puedes escribirnos al correo:
**admin@telcosur.co**