POLÍTICA DE SEGURIDAD DE LA RED

TELCOSUR S.A.S.

1. Introducción

En **TELCOSUR S.A.S.**, como Proveedor de Servicios de Internet (ISP), reconocemos que la **red** es el pilar fundamental de nuestro servicio. La seguridad de la infraestructura de telecomunicaciones es clave para garantizar la continuidad, estabilidad y confianza en la prestación del servicio a nuestros usuarios.
Esta política establece los lineamientos para proteger la **red de acceso, distribución y núcleo**, frente a amenazas internas y externas, cumpliendo con la normativa vigente y los estándares del sector TIC.

2. Objetivos

- Proteger la infraestructura de red frente a ataques cibernéticos, accesos indebidos y daños físicos.
- Garantizar la disponibilidad, continuidad y calidad de los servicios de conectividad.
- Reducir la exposición a vulnerabilidades mediante controles técnicos y operativos.
- Cumplir la normativa sectorial y mantener evidencia de su cumplimiento

3. Alcance

- Elementos de red propiedad o administrados por la compañía (núcleo, transporte, distribución y acceso).
- Sistemas de gestión, monitoreo y soporte (NMS/OSS/BSS).
- Personal interno, contratistas y proveedores con acceso a la red.

4. Marco Normativo

La política se fundamenta en:

- **Ley 1341 de 2009** (Ley TIC).
- **Ley 1273 de 2009** (delitos informáticos).
- **Ley 1581 de 2012** (protección de datos personales).
- **Decreto 1078 de 2015** (sector TIC).
- **Resolución 5050 de 2016 – CRC** (indicadores de calidad).
- **Política Nacional de Seguridad Digital – CONPES 3854 de 2016**.
- Buenas prácticas internacionales: **ISO/IEC 27001** y guías de ciberseguridad aplicables.

5. Principios Rectores

- **Disponibilidad:** mantener la red en operación continua, minimizando interrupciones.
- **Resiliencia:** garantizar que la red pueda recuperarse rápidamente tras incidentes.
- **Prevención:** implementar controles proactivos frente a riesgos y amenazas.
- **Legalidad:** cumplimiento estricto de la normativa colombiana y regulaciones del sector TIC.
- **Mejora continua:** actualización constante de procedimientos y tecnologías de seguridad.

6. Medidas de Seguridad

6.1 Infraestructura

- Firewalls y sistemas de detección y prevención de intrusos (**IDS/IPS**).
- Segmentación de red en **zonas seguras** para servicios críticos.
- Monitoreo continuo del tráfico y alarmas de seguridad.

6.2 Gestión de Accesos

- Controles de acceso basados en roles y privilegios mínimos.
- **Autenticación multifactor (MFA)** en accesos remotos y críticos.
- Auditoría periódica de permisos y credenciales.

6.3 Continuidad Operacional

- Respaldos frecuentes de configuraciones y datos críticos.
- Plan de recuperación ante desastres y redundancia en equipos clave.
- Procedimientos estandarizados de mantenimiento y cambios.

6.4. Respuesta a Incidentes

- Plan formal de gestión de incidentes de red.
- Registro, análisis y corrección de eventos.
- Comunicación oportuna a usuarios y autoridades competentes, según el caso.

6.4 Capacitación

- Formación continua en seguridad de redes para el personal técnico.
- Campañas de buenas prácticas dirigidas a usuarios y aliados.

7. Responsabilidades

- **Gerencia General:** asignar recursos y apoyar la implementación de la política.
- **Área Técnica de Red:** ejecutar y supervisar las medidas de seguridad definidas.
- **Contratistas y proveedores:** cumplir con las políticas y protocolos de acceso a la red.

8. Revisión y Actualización

- La política será revisada de manera **anual**, o antes si ocurren cambios tecnológicos, normativos o de amenazas que lo requieran.