1. Objetivo

Establecer los lineamientos y controles de seguridad de la información para garantizar la **confidencialidad, integridad y disponibilidad** de los servicios de internet prestados por SUMERTEL COMUNICACIONES S.A.S, en cumplimiento de la normatividad aplicable y buenas prácticas internacionales (ISO/IEC 27000).

2. Alcance

Este protocolo aplica a:

- Infraestructura tecnológica (servidores, routers, switches, enlaces, centros de datos, equipos de cliente).
- Información de clientes, contratos y datos personales.
- Personal administrativo, técnico y comercial que intervenga en el tratamiento de información.
- Proveedores y aliados estratégicos con acceso a sistemas o datos.

3. Marco Normativo y Referencias

- ISO/IEC 27000 – Sistema de Gestión de Seguridad de la Información.
- ISO/IEC 27001 – Requisitos para la gestión de seguridad.
- Ley 1581 de 2012 – Protección de datos personales en Colombia.
- Decreto 1377 de 2013 – Reglamentación sobre habeas data.
- Resoluciones y lineamientos del MinTIC aplicables a ISPs.

4. Principios de Seguridad

- **Confidencialidad:** La información de clientes y de la empresa solo será accesible por personal autorizado.
- **Integridad:** Los datos y servicios no podrán ser modificados sin autorización.
- **Disponibilidad:** Los servicios de internet deben estar disponibles para los clientes de acuerdo a los SLA definidos.

5. Roles y Responsabilidades

- **Gerente General:** Aprueba y supervisa el cumplimiento del protocolo.
- **Responsable de Seguridad de la Información:** Diseña y aplica controles de seguridad.
- **Personal Técnico:** Ejecuta medidas de seguridad en infraestructura y redes.
- **Todos los colaboradores:** Cumplir las políticas de uso aceptable de la información.

6. Controles de Seguridad Implementados

6.1 Seguridad Física y Ambiental

- Acceso restringido a salas de equipos y servidores mediante llaves/cerraduras.
- Cámaras de videovigilancia en las instalaciones principales.
- Equipos de red en gabinetes cerrados con control de acceso.

6.2 Seguridad de Redes

- Uso de **firewalls y reglas de filtrado** para proteger la red interna.
- Segmentación de redes (administrativa, técnica, clientes).
- Monitoreo de tráfico y alertas de intentos de intrusión.
- VPN segura para acceso remoto del personal autorizado.

6.3 Seguridad de la Información

- Respaldos automáticos de configuraciones de red y bases de datos de clientes.
- Cifrado de información sensible (contraseñas, credenciales).
- Políticas de contraseñas robustas y cambio periódico.
- Control de accesos por roles (principio de mínimo privilegio).

6.4 Continuidad del Negocio

- Plan de respaldo de energía (UPS/planta eléctrica).
- Procedimiento de recuperación ante fallos de red.
- Redundancia de enlaces en caso de caída del servicio principal.

6.5 Cumplimiento Legal

- Protección de datos personales bajo la Ley 1581 de 2012.
- Autorización de uso de datos firmada por los clientes.
- Custodia segura de la información de facturación y contratos.

7. Gestión de Incidentes

- Registro de incidentes de seguridad en bitácoras.
- Notificación inmediata al responsable de Seguridad.
- Procedimiento de análisis, corrección y reporte.

8. Plan de Concientización

- Capacitaciones internas al personal sobre seguridad de la información.
- Campañas de uso seguro de contraseñas y correos electrónicos.
- Comunicación de políticas a nuevos colaboradores.

9. Evaluación y Mejora Continua

- Revisión semestral de este protocolo.
- Auditorías internas para verificar cumplimiento.
- Actualización según nuevas amenazas y requisitos regulatorios.