POLÍTICA DE SEGURIDAD DE LA RED Y PROTOCOLOS DE RESPUESTA
VIRUS COMUNICACIONES DEL CAUCA S.A.S.
Protección de Infraestructura y Continuidad del Servicio

1. Objetivo General
Documentar formalmente los procedimientos técnicos y operativos implementados por VIRUS COMUNICACIONES DEL CAUCA S.A.S. para asegurar la estabilidad, alta disponibilidad y protección integral de toda la infraestructura de telecomunicaciones y redes de transmisión de datos.

2. Cobertura y Alcance
Las medidas de seguridad técnica y física descritas en este documento se aplican a la totalidad de la red de fibra óptica, nodos de radioenlace y equipos de borde desplegados en los municipios de operación, garantizando el servicio en Nátaga y La Plata (departamento del Huila), así como en Páez, Belalcázar e Inzá (departamento del Cauca).

3. Estabilidad y Protección de la Infraestructura
Se mantienen políticas estrictas de control de acceso lógico y físico a los centros de datos y nodos principales. Los equipos de enrutamiento y conmutación cuentan con configuraciones de seguridad endurecidas (hardening) para prevenir accesos no autorizados, alteraciones en las configuraciones y garantizar un entorno de operación estable para el tráfico de los usuarios.

4. Protocolo de Mitigación ante Ataques (DDoS)
Frente a eventos internos o externos malintencionados, como los ataques de Denegación de Servicio Distribuido (DDoS) que buscan saturar el ancho de banda, VIRUS COMUNICACIONES DEL CAUCA S.A.S. Cuenta con sistemas de monitoreo y firewalls perimetrales capaces de identificar anomalías en el tráfico. Ante una alerta, se aplican reglas dinámicas de filtrado y descarte de paquetes maliciosos para mitigar el impacto y mantener el servicio operativo.

5. Protocolo de Respuesta ante Cortes Físicos y Eventos Externos
Para garantizar la resiliencia de la red frente a incidentes de fuerza mayor (como rupturas de fibra por obras civiles, vandalismo o condiciones climáticas extremas), la empresa dispone de:
• Cuadrillas técnicas de respuesta rápida desplegadas estratégicamente para atención de emergencias en terreno.
• Sistemas de respaldo de energía (baterías UPS y generadores) en nodos vitales para mitigar cortes de fluido eléctrico.
• Topologías de red con redundancia siempre que la geografía lo permite, facilitando el enrutamiento alternativo del tráfico.

6. Monitoreo Continuo
La infraestructura es supervisada 24/7 a través de plataformas de gestión de red que miden la disponibilidad de los enlaces, la latencia y la saturación. Esto permite a nuestro equipo técnico anticiparse a posibles fallas y ejecutar acciones correctivas antes de que se afecte la experiencia de conexión de los suscriptores.