SYSTEL COMUNICACIONES CARTAGO S.A.S.

NIT: 900.217.277-0 | Cartago, Valle del Cauca
www.systelcomunicaciones.com | comercial@systelcomunicaciones.com

SISTEMA DE POLÍTICAS Y GESTIÓN DE SEGURIDAD DE LA RED

Código: DOC-SYS-SPGSR-01 | Versión: 01 | Fecha: Mayo de 2026

1. OBJETO

Definir el marco de gestión de seguridad de la red de SYSTEL COMUNICACIONES CARTAGO S.A.S., estableciendo las políticas y controles para proteger la infraestructura de red y garantizar la continuidad del servicio.

2. ARQUITECTURA DE SEGURIDAD

La red de Systel Comunicaciones cuenta con: (a) Firewall perimetral de próxima generación; (b) Sistemas de detección y prevención de intrusos (IDS/IPS); (c) Segmentación de redes por VLANs; (d) Monitoreo 24/7 de la infraestructura crítica; (e) Sistemas de respaldo de energía (UPS) en nodos principales.

3. PROTECCIÓN CONTRA ATAQUES

Se implementan medidas de protección contra: ataques de denegación de servicio (DDoS); accesos no autorizados; escaneo de puertos y reconocimiento de red; inyección de tráfico malicioso; suplantación de identidad en la red (ARP spoofing).

4. GESTIÓN DE VULNERABILIDADES

Se realiza monitoreo continuo de vulnerabilidades en la infraestructura de red, con aplicación oportuna de parches y actualizaciones de seguridad en todos los equipos activos.

5. CONTROL DE ACCESO A LA RED

El acceso a la infraestructura de red está restringido al personal técnico autorizado, mediante autenticación robusta, VPN para acceso remoto y registro de todas las actividades de administración.

6. RESPUESTA A INCIDENTES

Ante incidentes de seguridad en la red, se activa el protocolo de respuesta a incidentes que incluye: detección, contención, erradicación, recuperación y análisis post-incidente. Reporte: comercial@systelcomunicaciones.com.

7. CONTINUIDAD DEL SERVICIO

Se mantienen planes de continuidad que incluyen rutas de red redundantes, equipos de respaldo en sitios críticos y procedimientos documentados de recuperación ante desastres.

8. AUDITORÍAS DE SEGURIDAD

Se realizan auditorías periódicas de seguridad de la red, incluyendo pruebas de penetración y revisión de configuraciones, para identificar y corregir vulnerabilidades.