---

1. Introducción

El presente documento describe las políticas, procedimientos y controles de seguridad implementados por **SUMERTEL COMUNICACIONES S.A.S.** en la operación de su red de telecomunicaciones. El objetivo es garantizar la **confidencialidad, integridad y disponibilidad** de los servicios prestados a los usuarios, en cumplimiento de los lineamientos del **Ministerio de Tecnologías de la Información y Comunicaciones – MinTIC** y las buenas prácticas internacionales en seguridad de la información (ISO/IEC 27001).

---

2. Alcance

Este documento aplica a la infraestructura de red administrada por **SUMERTEL COMUNICACIONES S.A.S.**, incluyendo:

- Routers de borde (Mikrotik v6.49.15).
- Red de acceso para clientes residenciales y corporativos.
- Servicios de DNS y NAT administrados por la compañía.

---

3. Políticas de Seguridad Implementadas

3.1 Políticas Generales

- Todo el tráfico de Internet de los clientes pasa por filtros de firewall y reglas de seguridad perimetral.
- Se emplean listas de bloqueo para prevenir acceso a sitios no autorizados y contener incidentes de seguridad.
- Se monitorea permanentemente el tráfico de red con el fin de detectar anomalías o ataques.

3.2 Seguridad en Firewall Mikrotik

Ejemplo de configuración aplicada:

/ip firewall filter

add chain=forward connection-state=established,related action=accept comment="Permitir trafico existente"

add chain=forward connection-state=invalid action=drop comment="Eliminar conexiones invalidas"

add chain=input protocol=tcp dst-port=8291 connection-limit=3,32 action=drop comment="Proteger acceso Winbox"

add chain=input protocol=tcp psd=21,3s,3,1 action=drop comment="Bloquear escaneo de puertos"

3.3 Prevención de Ataques DoS/DDoS

/ip firewall filter

add chain=input protocol=icmp limit=50,10 action=accept comment="Permitir ICMP limitado"

add chain=input protocol=icmp action=drop comment="Descartar exceso de ICMP"

add chain=forward connection-limit=100,32 action=drop comment="Limitar exceso de conexiones por IP"

3.4 Control de DNS y Bloqueo de Sitios

/ip dns

set allow-remote-requests=yes

/ip firewall nat

add chain=dstnat protocol=udp dst-port=53 action=redirect to-ports=53

add chain=dstnat protocol=tcp dst-port=53 action=redirect to-ports=53

/ip dns static

add name="xvideos.com" address=127.0.0.1 comment="Bloqueo contenido adulto"

add name="hitomi.la" address=127.0.0.1 comment="Bloqueo contenido adulto"

3.5 Bloqueo de IPs Prohibidas

/ip firewall address-list

add list=blocked_sites address=134.122.136.9 comment="Contenido prohibido"

add list=blocked_sites address=173.214.250.43 comment="Contenido prohibido"

add list=blocked_sites address=173.214.250.46 comment="Contenido prohibido"

add list=blocked_sites address=173.214.250.34 comment="Contenido prohibido"

add list=blocked_sites address=173.214.250.45 comment="Contenido prohibido"

add list=blocked_sites address=173.214.250.41 comment="Contenido prohibido"

add list=blocked_sites address=89.248.162.213 comment="Contenido prohibido"

/ip firewall filter

add chain=forward dst-address-list=blocked_sites action=drop comment="Bloqueo acceso a IPs maliciosas"

---

4. Gestión de Incidentes de Seguridad

- **Detección:** se realiza mediante revisión de logs y monitoreo de tráfico en Mikrotik (Torch, Traffic Flow).
- **Respuesta:** bloqueo inmediato del tráfico sospechoso en listas negras (blacklist).
- **Escalamiento:** notificación al área de seguridad y administración de red.
- **Recuperación:** limpieza de reglas, restablecimiento de servicio y análisis post-incidente.

---

5. Cumplimiento y Mejora Continua

Las medidas descritas cumplen con:

- Lineamientos del **MinTIC** sobre seguridad en redes de telecomunicaciones.
- Buenas prácticas internacionales (**ISO/IEC 27001**, **MANRS**).
- Política interna de seguridad de **SUMERTE COMUNICACIONES S.A.S.**

La empresa se compromete a mantener una **mejora continua** en la protección de su infraestructura frente a amenazas emergentes.