Cirtel Comunicaciones SAS

POLÍTICAS Y MECANISMOS DE FILTRADO DE CONTENIDO

COMPAÑÍA INTEGRAL DE RECURSOS
EN TELECOMUNICACIONES S.A.S

VIGENTE HASTA EL 31 DE DICIEMBRE DEL 2025

POLÍTICAS Y MECANISMOS DE FILTRADO DE CONTENIDO

En cumplimiento del artículo 7 del Decreto 1524 de 2002 y la Ley 679 de 2001

1. Introducción

Este documento describe las políticas y mecanismos de seguridad implementados por **CIRTEL COMUNICACIONES SAS**, en su rol de Proveedor de Redes y Servicios de Telecomunicaciones (PRST), con el fin de restringir el acceso a contenidos de abuso sexual infantil (pornografía infantil) y otros sitios maliciosos, cumpliendo así con la obligación legal establecida por el artículo 7 del **Decreto 1524 de 2002** y la **Ley 679 de 2001**.

2. Enfoque de Seguridad: MikroTik y DNS

La solución de seguridad de CIRTEL se basa en la implementación de un **firewall MikroTik** como defensa perimetral, y en un sistema de **filtrado de contenidos basado en DNS** como estrategia central para bloquear el acceso a sitios no permitidos desde la red interna.

3. Componentes de la Solución

3.1. Firewall MikroTik

La configuración del firewall incluye:

- **Filtrado de tráfico por reglas**: control del tráfico entrante y saliente según puertos, protocolos y direcciones IP.
- **Políticas de acceso**: solo IP autorizadas pueden interactuar con la red.
- **Protección por NAT**: enmascaramiento de direcciones IP privadas.
- **Defensa ante ataques DoS/DDoS**: mecanismos de detección y bloqueo.
- **Registro de eventos**: monitoreo detallado de actividad para auditoría.

3.2. Sistema de Filtrado de Contenidos por DNS

Como medida principal de control de contenido, CIRTEL ha implementado un **servidor DNS especializado** para bloquear el acceso a dominios restringidos. Este sistema opera de la siguiente manera:

- Se mantiene una **lista actualizada de dominios prohibidos**, que incluye sitios con material de abuso sexual infantil, malware, phishing y contenido inapropiado.

- Cuando un usuario intenta acceder a uno de estos dominios desde la red interna, la petición DNS es interceptada y redirigida automáticamente hacia un **servidor proxy reverso**.
- El proxy entrega una **página de advertencia o bloqueo**, informando al usuario que el sitio solicitado está restringido por políticas de seguridad y cumplimiento normativo.
- Este filtrado DNS se aplica de forma centralizada para todas las conexiones gestionadas por CIRTEL, sin necesidad de instalar software adicional en los dispositivos de usuario.

Este enfoque permite controlar de manera eficaz el acceso a contenidos en tiempo real y con bajo impacto en el rendimiento de red.

4. Beneficios del Filtrado DNS

- **Prevención del acceso a contenidos ilegales o peligrosos**, especialmente aquellos relacionados con explotación infantil.
- **Reducción del riesgo de infecciones y ataques** desde sitios maliciosos.
- **Alineación con la regulación nacional**, garantizando el cumplimiento de las obligaciones del ISP.
- **Intervención rápida y transparente** mediante redirección automática e informativa.

6. Evidencias y Redireccionamiento con Notificación Informativa

Para garantizar la transparencia y cumplimiento legal en el bloqueo de sitios web con contenidos ilegales, especialmente aquellos relacionados con material de abuso sexual infantil, se implementa un mecanismo de **redireccionamiento automático** hacia una página informativa, la cual cumple las siguientes funciones:

- **Notificación clara al usuario:** Al intentar acceder a un sitio bloqueado, el usuario es redirigido a una página donde se informa que el acceso está restringido conforme a la normativa vigente, especificando las causas del bloqueo (por ejemplo, distribución de software ilegal, juegos de azar no autorizados, o contenido ilegal relacionado con la protección de menores).
- **Referencia a la normatividad aplicable:** La página incluye un resumen de las leyes y decretos que respaldan el bloqueo, como la Ley 679 de 2001, modificada por la Ley 1336 de 2009, que previenen y sancionan la explotación sexual comercial de menores, entre otras disposiciones relevantes.

- **Canales oficiales de denuncia:** Se proporcionan enlaces y datos de contacto para denunciar estos casos ante las autoridades competentes, como la Policía Nacional (CAI Virtual), la Fiscalía General de la Nación y el Ministerio TIC a través de la plataforma TeProtejo Colombia.

Ejemplo de la obligación cumplida:



Este mecanismo no solo bloquea el acceso, sino que cumple una función educativa y preventiva, garantizando que los usuarios comprendan el motivo del bloqueo y conozcan las vías formales para reportar irregularidades.

5. Conclusión

La integración de un **firewall MikroTik** con un **sistema robusto de filtrado por DNS** permite a CIRTEL ofrecer un entorno de navegación seguro, ético y alineado con la legislación vigente en Colombia. Esta estrategia cumple con los deberes del proveedor de servicios de telecomunicaciones y contribuye activamente a la protección de niñas, niños y adolescentes en el entorno digital.

CANAL DE REPORTES INSTITUCIONALES

En concordancia con las disposiciones legales sobre la protección de niñas, niños y adolescentes en entornos digitales, cualquier persona puede reportar sitios con contenido de abuso sexual infantil o violaciones relacionadas con el uso de redes y servicios de telecomunicaciones, directamente ante el **Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC)**, a través de los siguientes canales oficiales:

- **Sitio web de denuncias del MinTIC:**
  https://www.teprotejo.org – canal oficial para reportar contenido inapropiado o ilegal relacionado con menores de edad.
- **Correo electrónico institucional (para operadores e ISP):**
  contacto@mintic.gov.co
  Asunto sugerido: *Reporte de cumplimiento – Decreto 1524 de 2002 – Filtrado de Contenidos*
- **Línea de atención al ciudadano MinTIC:**
  Bogotá: (601) 344 34 60
  Línea gratuita nacional: 01 8000 910 742

Estos canales garantizan la recepción formal de denuncias y reportes conforme al marco legal establecido, y permiten a los Proveedores de Servicios de Telecomunicaciones mantener comunicación directa con la autoridad competente en caso de incidentes o solicitudes de verificación.