MANUAL DE FILTRADO DIGITVNET S.A.S.

Para la Prevención de Pornografía Infantil

A continuación, **DIGITVNET S.A.S.** presenta la estructura detallada del manual para el filtro de contenido, especialmente en referencia a la **Ley 679 de 2001**, **Ley 1336 de 2009**, y reglamentaciones del **MinTIC** y la **Policía Nacional (CAI Virtual)**.

---

1. Introducción

Objetivo del Manual

Establecer los procedimientos y lineamientos técnicos y legales que **DIGITVNET S.A.S.** debe adoptar como **Proveedor de Servicios de Internet (ISP)** en Colombia para **prevenir, bloquear y reportar** el acceso a contenidos relacionados con pornografía infantil, en cumplimiento de la legislación colombiana.

Ámbito de Aplicación

Este manual aplica a **DIGITVNET S.A.S.** como ISP que opera en territorio colombiano.

---

2. Marco Normativo

- **Ley 679 de 2001:** Prevención de la explotación, pornografía y turismo sexual con menores de edad.
- **Ley 1336 de 2009:** Refuerza las medidas contra la explotación sexual infantil en medios electrónicos.
- **Ley 1098 de 2006:** Código de Infancia y Adolescencia.
- **Ley 1273 de 2009:** Crea nuevos tipos penales relacionados con delitos informáticos.
- **Resolución 3502 de 2008 – MinTIC:** Lineamientos para el control y monitoreo del tráfico de Internet en relación con la pornografía infantil.
- **Convenios internacionales** ratificados por Colombia, como el **Convenio de Budapest** sobre delitos cibernéticos.

3. Definiciones

- **Pornografía Infantil:** Toda representación, por cualquier medio, de un menor de edad participando en actividades sexuales explícitas, reales o simuladas, o cualquier representación de sus partes íntimas con fines sexuales.
- **ISP (Internet Service Provider):** Empresa que provee acceso a Internet a usuarios finales.
- **Bloqueo de contenido:** Técnica para impedir el acceso a sitios web o contenidos específicos mediante filtrado a nivel de red o DNS.
- **Lista negra (Blacklist):** Listado de dominios o direcciones IP identificadas como fuentes de pornografía infantil, actualizadas por entidades como el **CAI Virtual**.

4. Responsabilidades del ISP

1. Implementar **mecanismos de filtrado** para impedir el acceso a sitios web que contengan pornografía infantil.
2. **Reportar inmediatamente** a las autoridades competentes (Policía Nacional – CAI Virtual, Fiscalía General de la Nación) cualquier hallazgo o tráfico sospechoso.
3. **Capacitar al personal** sobre el manejo de incidentes relacionados con explotación sexual infantil.
4. **Colaborar con las autoridades** judiciales y de protección de menores en caso de investigaciones.
5. **Actualizar continuamente** las herramientas de filtrado según listas provistas por autoridades o asociaciones internacionales confiables (ej. IWF, INHOPE).

5. Mecanismos Técnicos de Filtrado

5.1. Filtrado por DNS

- Redireccionar solicitudes de DNS hacia un servidor que bloquee dominios incluidos en listas negras.
- Recomendación: utilizar listas actualizadas por el **CAI Virtual** o **IWF**.

5.2. Filtrado por IP o URL

- Inspección del tráfico HTTP/HTTPS para detectar y bloquear patrones asociados.
- Uso de **proxies transparentes** para monitoreo en tiempo real.

5.3. Inspección Profunda de Paquetes (DPI)

- Uso de tecnologías de inspección avanzada del tráfico para identificar contenido incluso si está encriptado.
- Debe aplicarse con precaución, respetando la **privacidad del usuario**.

5.4. Integración con Listas Oficiales

- Integrar sistemas automáticos de actualización de **listas negras** (CAI Virtual, IWF).
- Verificar la validez y vigencia legal de las fuentes utilizadas.

---

6. Procedimiento de Filtrado

DIGITVNET S.A.S. ofrece servicios de Internet a sus usuarios a través de una plataforma especializada para **Proveedores de Servicios de Internet (ISPs)**, la cual incluye funcionalidades de **filtrado de contenido** para proteger contra el acceso a material inapropiado, incluyendo **pornografía infantil**.

El sistema implementado cumple con las regulaciones del **MinTIC**, las disposiciones de la **Ley 679 de 2001**, y los estándares de cooperación establecidos con el **CAI Virtual** de la **Policía Nacional**.

7. Sistema de Bloqueo Basado en DNS Autoritativo

DIGITVNET S.A.S., en cumplimiento de la normatividad vigente y su compromiso con la protección de los menores de edad en el entorno digital, ha implementado un **sistema de filtrado de contenidos basado en un DNS autoritativo**, el cual constituye el núcleo técnico de su mecanismo de prevención y bloqueo de acceso a sitios con material pornográfico infantil.

Fundamento del sistema

Un **DNS autoritativo (Domain Name System Autoritativo)** es el servidor responsable de proporcionar respuestas definitivas sobre la dirección IP asociada a un dominio determinado. A diferencia de los DNS recursivos o cacheados, que consultan a otros servidores para resolver nombres de dominio, el DNS autoritativo posee el control directo sobre los registros y puede decidir, de manera inmediata, **permitir o denegar el acceso** a determinados dominios según las políticas de la organización.

En el contexto de **DIGITVNET S.A.S.**, este principio permite establecer un **mecanismo de control centralizado**, garantizando que todas las solicitudes de resolución de dominios por parte de los usuarios sean validadas frente a un registro actualizado de direcciones prohibidas y sitios bloqueados por orden legal o por inclusión en listas negras oficiales (CAI Virtual, IWF, INHOPE).

Funcionamiento operativo

El proceso de filtrado se desarrolla mediante la siguiente arquitectura:

1. **Recepción de tráfico sin filtros:** El proveedor upstream entrega la conectividad de Internet a **DIGITVNET S.A.S.** sin restricciones o filtrados previos.
2. **Ingreso al núcleo de red (CCR Mikrotik):** Todo el tráfico recibido pasa por un **router central CCR Mikrotik**, el cual actúa como **nodo principal de control** y punto de aplicación de las políticas de seguridad y filtrado.
3. **Gestión de listas de bloqueo:**
    - El CCR Mikrotik mantiene una **Address List** con los dominios y direcciones IP clasificadas como no aptas, obtenidas de fuentes oficiales nacionales e internacionales.

- Esta lista se actualiza de manera continua mediante sincronización con el sistema de gestión de filtrado de **DIGITVNET S.A.S.**, asegurando la incorporación de nuevas amenazas o sitios reportados.

4. **Aplicación de la regla de filtrado:**
   - Cuando un usuario intenta acceder a una URL o dominio incluido en la Address List, el CCR ejecuta la **regla de denegación DNS**, impidiendo la resolución de dicho dominio.
   - El resultado es que la conexión no puede establecerse, bloqueando de forma inmediata el acceso al contenido prohibido.
5. **Registro y monitoreo:**
   - El sistema genera logs y reportes automáticos que permiten la trazabilidad de los intentos de acceso, manteniendo evidencia para cooperación con las autoridades competentes.

Beneficios del enfoque autoritativo

- **Control total:** DIGITVNET gestiona directamente qué dominios pueden ser resueltos dentro de su red.
- **Bajo impacto en rendimiento:** El filtrado se realiza a nivel de resolución DNS, evitando degradación en el tráfico del usuario.
- **Cumplimiento normativo:** El modelo cumple con la **Ley 679 de 2001**, **Ley 1336 de 2009**, y la **Resolución 3502 de 2008 del MinTIC**, garantizando que los sistemas de la empresa bloqueen activamente contenido ilícito.
- **Escalabilidad y actualización:** La Address List del CCR permite incorporar o eliminar dominios en tiempo real sin afectar la disponibilidad del servicio.

Proceso de Bloqueo de URLS

Se aplica un docker, donde hay un server que aplica DNS autoritativo, consulta la Base de URLS emitida por MINTIC, consigue url en lista y manda la alerta de sitio bloqueado, o si la pagina no existe, no resuelve nada en pantalla