SITELINKS SAS	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO: SGSI-FOR-05
EVIDENCIA:	NEUTRALIDAD DE LA RED	VERSIÓN: 1.0

FECHA 13 ABRIL 2025

OBJETIVO

Dar cumplimiento al principio de **Neutralidad de Red** exigido por la normativa colombiana (Ley 1450 de 2011 y Resoluciones de la CRC), garantizando que SITELINKS SAS no bloquea, interfiere, discrimina ni restringe el acceso de los usuarios a contenidos, aplicaciones o servicios legales a través de Internet.

EVIDENCIA DE CONFIGURACIÓN TÉCNICA (FIREWALL MIKROTIK)

El control se ejecuta a nivel de capa 3 y 4 mediante el firewall del Core, asegurando que el tráfico fluya sin restricciones, salvo las excepciones legales obligatorias.

Análisis del Script y Reglas de "Accept"

De acuerdo con el script analizado y la consola Winbox, la política configurada es de **"Apertura por Defecto"**:

- **Tráfico Sin Restricciones:** Se identifican reglas action=accept para flujos de datos generales, permitiendo el libre tránsito de protocolos TCP/UDP.
- **Cumplimiento de Neutralidad:** El script muestra la ausencia de reglas de "Drop" basadas en contenido comercial, garantizando transparencia al usuario.

Excepciones Legales Aplicadas

SITELINKS SAS solo interfiere en el tráfico bajo los siguientes parámetros legales identificados en el script de firewall:

- **Seguridad de Red:** Bloqueo de puertos críticos de Windows (SMB: 445, 135-139, 1900) para proteger la **integridad y disponibilidad** del servicio del usuario final contra Virus y Botnets.

MATRIZ DE CUMPLIMIENTO (SITELINKS VS. NORMATIVA)

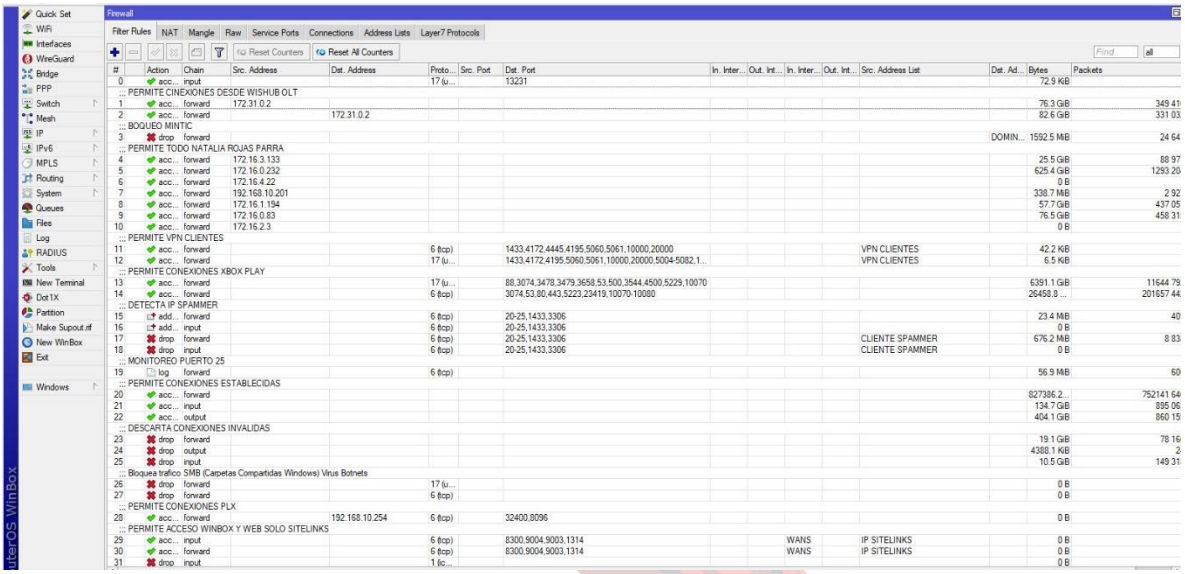
Requisito Normativo	**Implementación en SITELINKS SAS**
No Bloqueo / Interferencia	Las reglas de firewall permiten por defecto el tráfico hacia cualquier destino IP (action=accept chain=forward).
No Discriminación	No existe priorización de tráfico basada en el tipo de contenido o proveedor externo.
Consentimiento del Usuario	El usuario navega libremente; cualquier restricción obedece a mandatos legales o protección técnica.

CONCLUSIÓN TÉCNICA

Se certifica que **SITELINKS SAS** utiliza una configuración de red abierta. El script de firewall y las capturas gráficas de Winbox demuestran que la infraestructura actúa como un canal de transporte neutral, donde las únicas restricciones existentes obedecen estrictamente al cumplimiento normativo colombiano y a la protección técnica del usuario contra ciberamenazas.

ANEXO 1.0

EVIDENCIA DE CONFIGURACION



SCRIP UTILIZADO

/ip firewall filter

add action=accept chain=input dst-port=13231 protocol=udp

**add action=accept chain=forward comment="PERMITE CINEXIONES DESDE WISHUB OLT" **

src-address=172.31.0.2 src-address-type=""

add action=accept chain=forward dst-address=172.31.0.2 src-address-type=""

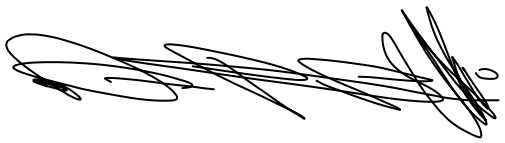
add action=drop chain=forward comment="BOQUEO MINTIC" dst-address-list=

"DOMINIOS BLOQ MINTIC"

```
add action=accept chain=forward comment="PERMITE TODO NATALIA ROJAS PARRA" \
   src-address=172.16.3.133
add action=accept chain=forward src-address=172.16.0.232
add action=accept chain=forward src-address=172.16.4.22
add action=accept chain=forward src-address=192.168.10.201
add action=accept chain=forward src-address=172.16.1.194
add action=accept chain=forward src-address=172.16.0.83
add action=accept chain=forward src-address=172.16.2.3
add action=accept chain=forward comment="PERMITE VPN CLIENTES" dst-port=\
   1433,4172,4445,4195,5060,5061,10000,20000 protocol=tcp src-address-list=\
   "VPN CLIENTES"
add action=accept chain=forward connection-limit=5,32 dst-port=\
   1433,4172,4195,5060,5061,10000,20000,5004-5082,1701 protocol=udp \
   src-address-list="VPN CLIENTES"
add action=accept chain=forward comment="PERMITE CONEXIONES XBOX PLAY" \
   dst-port=88,3074,3478,3479,3658,53,500,3544,4500,5229,10070 protocol=udp
add action=accept chain=forward dst-port=3074,53,80,443,5223,23419,10070-10080 \
   protocol=tcp
add action=add-src-to-address-list address-list="CLIENTE SPAMMER" \
   address-list-timeout=1d chain=forward comment="DETECTA IP SPAMMER" \
   connection-limit=20,32 dst-port=20-25,1433,3306 protocol=tcp
add action=add-src-to-address-list address-list="CLIENTE SPAMMER" \
   address-list-timeout=1d chain=input connection-limit=20,32 dst-port=\
```

```
   20-25,1433,3306 protocol=tcp
add action=drop chain=forward dst-port=20-25,1433,3306 protocol=tcp \
   src-address-list="CLIENTE SPAMMER"
add action=drop chain=input dst-port=20-25,1433,3306 protocol=tcp \
   src-address-list="CLIENTE SPAMMER"
add action=log chain=forward comment="MONITOREO PUERTO 25" log-prefix=\
   "correo saliente" port=25 protocol=tcp
add action=accept chain=forward comment="PERMITE CONEXIONES ESTABLECIDAS" \
   connection-state=established,related,new
add action=accept chain=input connection-state=established,related,new
add action=accept chain=output connection-state=established,related,new
add action=drop chain=forward comment="DESCARTA CONEXIONES INVALIDAS" \
   connection-state=invalid
add action=drop chain=output connection-state=invalid
add action=drop chain=input connection-state=invalid
add action=drop chain=forward comment=\
   "Bloquea trafico SMB (Carpetas Compartidas Windows) Virus Botnets" port=\
   19,135-139,161-162,445,389,1900 protocol=udp
add action=drop chain=forward port=19,135-139,445,389,1900 protocol=tcp
add action=accept chain=forward comment="PERMITE CONEXIONES PLX" dst-address=\
   192.168.10.254 dst-port=32400,8096 protocol=tcp
add action=accept chain=input comment=\
   "PERMITE ACCESO WINBOX Y WEB SOLO SITELINKS" dst-port=8300,9004,9003,1314 \
```

```
   in-interface-list=WANS protocol=tcp src-address-list="IP SITELINKS"
add action=accept chain=forward dst-port=8300,9004,9003,1314 in-interface-list=\
   WANS protocol=tcp src-address-list="IP SITELINKS"
add action=drop chain=input protocol=icmp
add action=drop chain=input comment="BLOQUEO TOTAL WAN INPUT" \
   in-interface-list=WANS
add action=drop chain=forward comment="BLOQUEO TOTAL WAN FORWARD" \
   in-interface-list=WAN
```



JUAN PABLO RODRIGUEZ CORCHUELO
GERENTE GENERAL