

SEGURIDAD DE LA RED Y CONTROL PARENTAL

REDSI TELECOMUNICACIONES S.A.S. · NIT 900.374.679-1

Radicado 262135370 · Expediente 96000824 · Documento para el usuario · vigente desde el 21 de agosto de 2026

Una conexión a internet expone al hogar y a la empresa a riesgos que ni el operador ni el usuario pueden eliminar por separado. Este documento explica cuáles son esos riesgos, qué hace Redsi en su red, qué le corresponde hacer a usted en la suya, y qué herramientas de control parental puede instalar. Redsi publica esta información en cumplimiento del régimen de protección de usuarios de servicios de comunicaciones y de la obligación de implementar sistemas internos de seguridad para su red (artículos 5.1.2, 5.1.3 y concordantes de la Resolución CRC 5050 de 2016).

1. Los riesgos que existen hoy

- **Software malicioso.** Programas que se instalan sin que usted lo advierta y roban información, cifran sus archivos o usan su equipo para atacar a otros.
- **Suplantación y phishing.** Correos, mensajes de texto o de WhatsApp que imitan a un banco, a una entidad del Estado o al propio operador para que usted entregue sus claves.
- **Robo de credenciales.** Reutilizar la misma contraseña en varios servicios hace que la filtración de uno solo comprometa a todos los demás.
- **Dispositivos del hogar expuestos.** Cámaras, televisores, grabadores de video y domótica que salen de fábrica con clave conocida y quedan accesibles desde internet.
- **Redes Wi-Fi abiertas.** Una red sin clave, o con la clave de fábrica, permite que un tercero use su servicio y observe el tráfico de su red interna.
- **Aplicaciones de streaming ilegal.** Aplicaciones que ofrecen televisión o cine gratuito. Además de ser ilegales, varias extraen datos del usuario hacia el exterior.

Sobre las aplicaciones de streaming ilegal. No es una advertencia genérica. Un juzgado penal de Bogotá ordenó el bloqueo nacional de esas aplicaciones considerando, entre otras razones, que extraen de manera maliciosa los datos de los usuarios y los transfieren a jurisdicciones extranjeras sin su conocimiento. Si instaló alguna, conviene desinstalarla, cambiar las contraseñas que haya usado en ese dispositivo y revisar sus cuentas.

2. Qué protege Redsi en su red

Estas son las medidas que operan en la red de Redsi. Son las mismas que se describen en la política de neutralidad y gestión de tráfico, y no hay ninguna adicional que no esté publicada.

Medida	En qué consiste
Resolución de nombres propia	Las consultas de nombres de dominio de la red de acceso se atienden en los resolutores de Redsi, que aplican los listados oficiales de bloqueo. Tiene por causa exclusiva el cumplimiento de una obligación legal: no analiza ni registra los sitios que usted visita.
Bloqueo de conexiones entrantes no solicitadas	El tráfico que llega desde internet sin que usted lo haya iniciado no se reenvía a su red interna, salvo que usted lo solicite. Protege los equipos del hogar de escaneos y ataques automatizados.
Descarte de conexiones inválidas	Se descartan paquetes malformados o que no corresponden a ninguna conexión válida. Es higiene de red y no analiza contenido.
Monitoreo de la red	Se vigila el estado y la disponibilidad de los elementos de red para detectar y atender fallas y comportamientos anómalos.
Atención de incidentes	Redsi cuenta con un sistema de gestión de seguridad de la información documentado, registra los incidentes y los reporta a las autoridades competentes cuando su severidad lo exige.

Lo que Redsi no hace. No inspecciona el contenido de su tráfico, no descifra sus conexiones seguras, no clasifica el tráfico por aplicación y no vende ni perfila su navegación. Fuera de las obligaciones legales de bloqueo, no restringe el acceso a ningún contenido lícito. Puede verificarlo en la política de neutralidad y gestión de tráfico, publicada en <https://redsi.net/gestion-de-trafico/>.

3. Su red interna es suya, y ahí el operador no alcanza

La protección de Redsi llega hasta el punto de entrega del servicio. De ahí hacia adentro —su router, su Wi-Fi, sus equipos— la seguridad depende de usted. Lo que aplica en su caso depende de cómo se hizo su instalación.

Si Redsi le instaló el router y le dejó una clave propia

No comparta esa clave por WhatsApp ni la escriba en lugares visibles. Si sospecha que se divulgó, pídanos cambiarla: es un trámite sin costo.

Si su router conserva la clave de fábrica

Cámbiela. Las claves de fábrica siguen patrones conocidos y publicados. Si no sabe cómo hacerlo, escríbanos y lo acompañamos por teléfono o en visita.

Si usted puso su propio router

La configuración y la seguridad de ese equipo son suyas. Cambie la clave de administración, mantenga el firmware actualizado y no exponga servicios a internet sin necesidad.

En todos los casos

- **Mantenga actualizados sus equipos.** Computadores, teléfonos, televisores y cámaras. La mayoría de los ataques aprovecha fallas ya corregidas por el fabricante.
- **No reutilice contraseñas.** Una clave distinta por servicio, y active la verificación en dos pasos donde exista.
- **Desconfíe de quien le pide datos.** Redsi nunca le pedirá su contraseña, ni claves bancarias, ni códigos de verificación, por ningún canal.
- **Revise qué está conectado.** Si ve dispositivos que no reconoce en su red, cambie la clave del Wi-Fi.
- **Cuide los dispositivos del hogar.** Cámaras, grabadores y domótica: cambie la clave por defecto y no los publique a internet salvo que sepa lo que hace.
- **Descargue solo de tiendas oficiales.** Las aplicaciones instaladas por fuera son la vía más frecuente de entrada del software malicioso.

4. Control parental: herramientas de filtrado que usted puede instalar

El bloqueo legal que aplica Redsi cubre únicamente el material de abuso sexual infantil, los juegos de suerte y azar no autorizados y las órdenes de autoridad. Para proteger a menores de edad de otros contenidos inapropiados —que la ley no ordena bloquear y que Redsi por tanto no restringe— la herramienta adecuada es el control parental en el hogar.

- **OpenDNS FamilyShield.** Filtrado en el router, cubre toda la casa. Gratuito.
opendns.com/setupguide/?url=familyshield
- **Cloudflare for Families.** Alternativa gratuita, bloquea contenido adulto y malware.
one.one.one.one/family/
- **Google Family Link.** Control de tiempo y contenido en Android. Gratuito.
families.google/familylink/
- **Microsoft Family Safety.** Para Windows y Xbox.
microsoft.com/es-co/microsoft-365/family-safety
- **Qustodio.** Multiplataforma, con versión gratuita. qustodio.com/es/
- **Net Nanny.** Filtrado por categorías. De pago. netnanny.com

Encontrará el detalle de estas opciones, actualizado, en <https://redsi.net/bloqueo-de-contenido/>. Si necesita ayuda para configurar alguna de estas herramientas en su conexión Redsi, nuestro equipo de soporte puede orientarle sin costo.

5. Si detecta un incidente de seguridad, avísenos

Reporte cualquier actividad extraña en su conexión: lentitud inexplicable, equipos que no reconoce, mensajes que suplantán a Redsi o a su banco, o sospecha de que su red fue comprometida.

Canales de contacto: WhatsApp 315 560 6726 · líneas 315 560 6726, 318 306 7112 y 315 542 7319 · formulario de PQR en <https://redsi.net/soporte-pqr/> · Calle 10 # 8-81, Centro, Villa de Leyva.

Qué información nos ayuda

- Fecha y hora aproximada en que ocurrió.
- Qué observó, y en qué equipo o servicio.
- Capturas de pantalla del mensaje o del comportamiento extraño, si las tiene.

Con ese reporte Redsi verifica lo que ocurre en su enlace, le indica dónde está el problema y, cuando corresponde, registra el evento y adopta las medidas de contención. Los incidentes de seguridad quedan documentados y, según su severidad, se reportan a las autoridades competentes.

6. Dónde denunciar contenido ilícito

Si encuentra material de abuso sexual infantil o un sitio de juegos ilegales, dentro o fuera de la red de Redsi, repórtelo directamente ante la autoridad competente. Los reportes pueden hacerse de forma anónima y confidencial.

- **Te Protejo.** Línea de denuncia en línea de contenidos que vulneran los derechos de niñas, niños y adolescentes. www.teprotejo.org
- **Policía Nacional · CAI Virtual.** Centro de denuncia de delitos informáticos. caivirtual.policia.gov.co
- **ICBF.** Línea 141 de protección, emergencia y orientación, gratuita, 24 horas. www.icbf.gov.co
- **Fiscalía General de la Nación.** 01 8000 91 97 48 desde fijo · 122 desde celular, gratuito, 24 horas. www.fiscalia.gov.co
- **Ciberpaz · MinTIC.** Estrategia del Ministerio TIC para el uso responsable y seguro de internet. ciberpaz.gov.co
- **Coljuegos.** Denuncia de juegos de suerte y azar ilegales. 01 8000 180 417 · denunciealilegal@coljuegos.gov.co

Última actualización: 21 de agosto de 2026 · REDSI TELECOMUNICACIONES S.A.S., NIT 900.374.679-1