

DS-NET-002 — INFORMACIÓN AL USUARIO SOBRE RIESGOS DE SEGURIDAD DE LA RED

REDSI TELECOMUNICACIONES S.A.S. · NIT 900.374.679-1
Radicado 262135370 · Expediente 96000824

1. Obligación

Mantener a los usuarios informados sobre los riesgos relativos a la seguridad de la red en cuanto al servicio de acceso a Internet contratado y las acciones que debe adelantar el usuario para preservar la seguridad de la red.

2. Publicación

El operador mantiene informados a sus usuarios sobre los riesgos relativos a la seguridad de la red y sobre las acciones que les corresponde adelantar, mediante una sección propia publicada en <https://redsi.net/seguridad-de-la-red/>, de acceso público y enlazada desde el menú principal del sitio.

La información se difunde además por los canales de atención al usuario y se refleja en el contrato de prestación del servicio.

El contenido íntegro de la sección publicada es el que se transcribe a continuación.

Evidencia: DS-NET-002_captura_2026-08-19.png, con URL y fecha del sistema visibles.

3. CONTENIDO PUBLICADO

Seguridad de la red

Qué riesgos existen cuando usted se conecta a Internet, qué hace Redsi para protegerlo y qué le corresponde hacer a usted.

Aplica a todos los servicios de Internet de Redsi · Actualizado: agosto de 2026

Por qué existe esta página

La ley obliga a los proveedores de Internet a mantener informados a sus usuarios sobre los riesgos de seguridad de la red y sobre las acciones que están en manos del propio usuario. Esta página es el cumplimiento de ese deber, y está escrita para que sirva: sin tecnicismos innecesarios y sin vender miedo.

Hay una idea que conviene tener clara desde el principio. **La conexión que Redsi le entrega llega hasta su router.** De ahí para adentro —sus equipos, sus contraseñas, sus descargas, lo que instala— está fuera del alcance del operador. La seguridad se reparte, y una parte importante le corresponde a usted.

Los riesgos

Suplantación y engaño (phishing)

Correos, mensajes de WhatsApp o SMS que imitan a un banco, a una entidad del Estado o al propio proveedor de Internet, para que usted entregue contraseñas o datos de su tarjeta. Es hoy la causa más frecuente de pérdida de dinero de usuarios domésticos en Colombia.

Redsi nunca le va a pedir por mensaje su contraseña, su clave bancaria ni el código de verificación que le llega al celular. Si recibe un mensaje que dice ser de Redsi y le pide eso, es falso: repórtelo por los canales oficiales.

Programas maliciosos (malware y ransomware)

Software que se instala sin que usted lo note, roba información o cifra sus archivos para pedir un rescate. Llega por adjuntos de correo, por programas descargados de sitios no oficiales y por memorias USB.

Router con la contraseña de fábrica

Es el riesgo más común y el más fácil de cerrar. Un router que conserva la clave que trae de fábrica, o una clave WiFi débil, permite que un tercero se conecte a su red, use su conexión y vea el tráfico de los equipos del hogar.

Cámaras, televisores y dispositivos inteligentes

Cámaras de seguridad, timbres, televisores y asistentes conectados a Internet suelen venir con contraseñas por defecto y rara vez se actualizan. Son la puerta de entrada más descuidada de un hogar conectado.

Redes WiFi abiertas fuera de casa

Una red WiFi sin contraseña, en un café o un aeropuerto, permite que otra persona en la misma red observe parte de su tráfico. Evite hacer operaciones bancarias sobre esas redes.

Contraseñas repetidas

Cuando un servicio cualquiera sufre una filtración, quien obtiene esa lista prueba las mismas contraseñas en el correo y en el banco. Repetir contraseña convierte un problema ajeno en un problema suyo.

Riesgos para niñas, niños y adolescentes

Acceso a contenido inadecuado, contacto con desconocidos y acoso en línea. Redsi bloquea por mandato legal el material de abuso sexual infantil de los listados oficiales, pero ese bloqueo no reemplaza el control parental en los equipos del hogar: vea la [sección de mecanismos de filtrado](#).

Qué hace Redsi

Medida	En qué consiste
Filtrado de contenidos ilícitos	Bloqueo diario y automatizado de los listados oficiales de material de abuso sexual infantil y de juegos de suerte y azar no autorizados, y de las órdenes judiciales y administrativas notificadas. Ver el mecanismo
Protección del borde de la red	Filtrado de tráfico no válido y descarte de conexiones entrantes no solicitadas hacia la red del usuario, comportamiento estándar de protección.
Monitoreo de la red	Supervisión permanente de los enlaces y de los equipos de red para detectar fallas y comportamientos anómalos.
Gestión de incidentes	Sistema de Gestión de Seguridad de la Información documentado, con registro de incidentes y procedimiento de atención y escalamiento.
Segmentación	Separación lógica del tráfico de gestión, del tráfico de clientes y de los servicios internos.
Respaldo de configuraciones	Copias de seguridad periódicas de la configuración de los equipos de red.
Privacidad	Redsi no inspecciona el contenido de su tráfico, no registra los sitios que usted visita ni comercializa esa información. Ver neutralidad de red

Qué le corresponde hacer a usted

1. **Cambie la contraseña de administración de su router** y la clave de su red WiFi. Que no sea la de fábrica, ni el número del teléfono, ni la cédula. Si no sabe cómo, pídalo por soporte: se lo hacemos.
2. **Use WPA2 o WPA3** en su red WiFi. Nunca la deje abierta ni en WEP.
3. **Mantenga actualizados** el sistema operativo y las aplicaciones de sus computadores y celulares. Las actualizaciones cierran fallas que ya están siendo explotadas.
4. **Instale un antivirus** en los computadores y manténgalo activo.
5. **No reutilice contraseñas** entre el correo, el banco y las redes sociales. Active la verificación en dos pasos donde el servicio la ofrezca.
6. **Desconfíe de los enlaces no solicitados**, aunque parezcan venir de una entidad conocida. Ante la duda, entre al sitio escribiendo la dirección usted mismo.
7. **Cambie la contraseña por defecto de sus cámaras y dispositivos inteligentes** y actualícelos cuando el fabricante lo permita.
8. **Haga copia de seguridad** de lo que no puede perder: fotos, documentos, información del negocio.
9. **Configure control parental** en los equipos que usan menores de edad. [Herramientas disponibles](#)
10. **Reporte cualquier incidente** por los canales oficiales de Redsi.

Cómo reportar un incidente de seguridad

Si detecta actividad extraña en su conexión, sospecha que su red fue comprometida o recibió un mensaje que suplanta a Redsi:

- **WhatsApp y teléfono:** +57 315 560 6726 · +57 318 306 7112 · +57 315 542 7319
- **Presencialmente:** Calle 10 # 8-81, Villa de Leyva, Boyacá. Lunes a viernes de 8:00 a. m. a 12:30 p. m. y de 2:00 p. m. a 6:00 p. m.; sábados de 8:00 a. m. a 11:30 a. m.
- **Radicando una PQR:** [Soporte / PQR](#)

Todo reporte queda registrado en el sistema de gestión de incidentes de seguridad de la información de Redsi y recibe respuesta.

Denuncias ante las autoridades

- **Delitos informáticos, estafas y suplantación:** CAI Virtual de la Policía Nacional — caivirtual.policia.gov.co
- **Material de abuso sexual infantil:** [Te Protejo](#) · [CAI Virtual](#)
- **Juegos de suerte y azar ilegales:** línea 01 8000 180 417 · denunciealilegal@coljuegos.gov.co