GUÍA DE SEGURIDAD DE RED PARA USUARIOS DEL SERVICIO DE INTERNET FIJO

GLOBAL NET TV ZOMAC S.A.S.
NIT 901.490.938-2

Documento para publicación y consulta de usuarios, suscriptores y beneficiarios del servicio de internet fijo

Campo	Información
Empresa	GLOBAL NET TV ZOMAC S.A.S.
NIT	901.490.938-2
Servicio	Internet fijo
Versión	1.0
Fecha de emisión	18 de mayo de 2026
Clasificación	Documento público informativo
Consulta web sugerida	https://globalnettv.com.co/seguridad-de-red/

1. Presentación

GLOBAL NET TV ZOMAC S.A.S. pone a disposición de sus usuarios esta guía para explicar, en lenguaje sencillo, los principales riesgos que pueden afectar la seguridad de la red de internet fijo y las acciones básicas que cada usuario puede adoptar para proteger su conexión, sus equipos, sus claves y su información.

Esta guía no reemplaza el soporte técnico ni modifica el contrato del servicio. Su finalidad es orientar al usuario para que use el internet de forma segura, responsable y adecuada.

2. ¿Por qué es importante proteger la red?

La red instalada en una casa, negocio u oficina puede conectar celulares, computadores, televisores inteligentes, cámaras, consolas, impresoras, tabletas y otros dispositivos. Si la red no se protege, terceros podrían acceder sin permiso, consumir el servicio, afectar la velocidad, intentar fraudes digitales o poner en riesgo información personal.

La seguridad de la red es una responsabilidad compartida: GLOBAL NET TV ZOMAC S.A.S. administra y presta el servicio, y el usuario debe cuidar sus claves, sus dispositivos y los equipos instalados en su predio.

3. Recomendaciones esenciales para el usuario

Tema	Qué debe hacer el usuario
Clave Wi-Fi	Use una contraseña segura, no la deje visible y cámbiela si sospecha que otras personas la conocen.
Acceso a la red	No comparta la clave con terceros no autorizados y revise si hay dispositivos desconocidos conectados.

Mensajes sospechosos	No abra enlaces extraños ni entregue claves, códigos o datos bancarios por llamadas, mensajes o redes sociales.
Descargas	Descargue aplicaciones y archivos solo desde fuentes confiables. Evite software pirata o archivos de origen desconocido.
Equipos instalados	No abra, resetee, traslade ni modifique el router, módem, ONT o cableado sin soporte autorizado.
Dispositivos	Mantenga actualizados celulares, computadores, televisores inteligentes y demás equipos conectados.
Reporte oportuno	Informe por canales oficiales cualquier acceso sospechoso, falla inusual, mensaje falso o manipulación no autorizada.

4. Riesgos comunes y cómo prevenirlos

4.1. Acceso no autorizado a la red Wi-Fi

Ocurre cuando una persona que no está autorizada logra conectarse a la red del usuario. Esto puede pasar por contraseñas débiles, claves compartidas sin control o manipulación del router.

¿Qué puede causar? Disminución de velocidad, consumo no autorizado del servicio, riesgo para los dispositivos conectados y posibles actividades realizadas desde la conexión del usuario.

- No comparta la contraseña con vecinos, visitantes ocasionales o terceros no autorizados.
- Cambie la contraseña si sospecha que fue conocida por personas que ya no deben tener acceso.
- Reporte a soporte si observa dispositivos desconocidos o cambios extraños en la red.

4.2. Contraseñas débiles o compartidas

Una contraseña fácil de adivinar facilita el acceso indebido. Evite claves como nombres, fechas de nacimiento, número de cédula, números consecutivos o palabras obvias.

- Use combinaciones de letras, números y símbolos.
- No escriba la contraseña en lugares visibles al público.
- No envíe la contraseña por grupos, chats o mensajes abiertos.
- Solicite apoyo a GLOBAL NET TV ZOMAC S.A.S. cuando requiera cambiar la clave Wi-Fi.

4.3. Phishing, mensajes falsos y fraude digital

El phishing es una forma de engaño. Puede llegar por correo electrónico, mensajes de texto, llamadas, WhatsApp, redes sociales o páginas falsas. Generalmente busca que el usuario entregue claves, datos personales, información bancaria o códigos de seguridad.

- No abra enlaces sospechosos o mensajes que generen urgencia injustificada.
- No entregue claves, códigos o datos bancarios por llamadas o mensajes no verificados.
- Verifique directamente con la empresa cualquier mensaje sobre pagos, suspensión del servicio, actualización de datos o soporte técnico.
- Use únicamente los canales oficiales de atención.

4.4. Malware, virus y programas maliciosos

El malware es un programa malicioso que puede afectar computadores, celulares, televisores inteligentes u otros dispositivos. Puede entrar por archivos descargados, enlaces falsos, aplicaciones inseguras, memorias USB o páginas no confiables.

- No instale programas de origen desconocido.
- No abra archivos adjuntos enviados por remitentes que no reconoce.
- Mantenga actualizado el sistema operativo y las aplicaciones.
- Use antivirus o herramientas de seguridad cuando sea posible.
- Reporte comportamientos extraños en sus dispositivos o en la conexión.

4.5. Páginas falsas o sitios inseguros

Algunas páginas imitan bancos, plataformas de pago, entidades públicas o empresas de servicios para obtener información del usuario. Antes de ingresar datos personales o financieros, revise que se trate del sitio correcto.

- Revise que la dirección web esté escrita correctamente.
- No ingrese datos personales o bancarios desde enlaces recibidos por mensajes sospechosos.
- Cierre la página si solicita información innecesaria o si genera desconfianza.
- Ante dudas sobre pagos o servicios, comuníquese por canales oficiales.

4.6. Descargas inseguras

Descargar aplicaciones, juegos, programas o archivos desde páginas no confiables puede instalar virus, programas espía o software no deseado en los dispositivos conectados a la red.

- Descargue aplicaciones desde tiendas o sitios oficiales.
- Evite programas piratas, “cracks” o archivos ejecutables desconocidos.
- Revise los permisos que solicita una aplicación antes de instalarla.
- No abra archivos comprimidos si no conoce su origen.

4.7. Equipos desactualizados

Los dispositivos desactualizados pueden tener fallas de seguridad. Esto incluye celulares, computadores, tabletas, televisores inteligentes, cámaras, consolas, navegadores y aplicaciones.

- Active actualizaciones automáticas cuando sea posible.
- Actualice navegadores y aplicaciones frecuentes.
- Revise también cámaras, repetidores, extensores de señal y otros equipos conectados.

4.8. Manipulación del router, módem, ONT o cableado

Los equipos instalados para prestar el servicio deben cuidarse y no deben ser manipulados por terceros no autorizados. Abrir, resetear, trasladar o modificar equipos puede generar fallas, pérdida de configuración, afectación de la calidad del servicio o riesgos de seguridad.

- No abra ni resetee el router, módem u ONT sin autorización.
- No cambie configuraciones técnicas sin acompañamiento de soporte.

- No permita que terceros no autorizados manipulen equipos o cableado.
- Reporte cualquier daño, desconexión, traslado o manipulación sospechosa.

5. Protección de niños, niñas y adolescentes

El usuario debe promover un uso seguro y responsable del internet en el hogar. Para proteger a niños, niñas y adolescentes, se recomienda acompañar su navegación, activar controles parentales cuando sea posible y reportar contenidos ilegales ante las autoridades competentes.

- Configure controles parentales en dispositivos, navegadores o plataformas cuando estén disponibles.
- Evite que menores descarguen aplicaciones o archivos sin supervisión.
- Dialogue sobre riesgos digitales, mensajes de desconocidos y páginas no apropiadas.
- Denuncie contenidos de abuso sexual contra niñas, niños y adolescentes ante los canales oficiales de autoridad.

6. ¿Cuándo debe reportar el usuario?

El reporte oportuno ayuda a revisar la situación y orientar al usuario. Se recomienda contactar a GLOBAL NET TV ZOMAC S.A.S. cuando se presente cualquiera de estas situaciones:

- Dispositivos desconocidos conectados a la red Wi-Fi.
- Lentitud repentina sin causa aparente o fallas inusuales repetidas.
- Cambios no solicitados en la configuración del router o del nombre de la red.
- Mensajes sospechosos relacionados con pagos, suspensión del servicio, claves o actualización de datos.
- Solicitud de contraseñas, códigos o datos personales por canales no oficiales.
- Sospecha de virus, redireccionamientos extraños o páginas falsas.
- Manipulación de equipos por personas no autorizadas.

7. Canales oficiales de soporte y atención

Para solicitar soporte, cambio de contraseña Wi-Fi, orientación sobre seguridad de red, radicar PQR o reportar situaciones sospechosas, use únicamente los canales oficiales de GLOBAL NET TV ZOMAC S.A.S.

Canal	Información
Oficina física	Carrera 9B No. 6-50, barrio Las Avenidas, Florencia, Caquetá.
Línea principal	311 776 8852
Contacto adicional	322 255 4747
Correo comercial	ventas@globalnettv.com.co
Notificaciones	notificacionesjudiciales@globalnettv.com.co
PQR	https://globalnettv.com.co/pqr/
Página web	https://globalnettv.com.co/

GLOBAL NET TV ZOMAC S.A.S. recomienda no entregar contraseñas, códigos o información bancaria por canales no verificados. Ante cualquier duda, confirme directamente con la empresa.

8. Lista rápida de buenas prácticas

No.	Revise si cumple esta recomendación
1	Protejo mi contraseña Wi-Fi y no la comparto con terceros no autorizados.
2	Cambio la contraseña si sospecho que alguien más la conoce.
3	No abro enlaces, archivos o mensajes sospechosos.
4	No entrego claves, códigos ni datos bancarios por mensajes no verificados.
5	Mantengo actualizados mis dispositivos y aplicaciones.
6	No manipulo router, módem, ONT o cableado sin soporte autorizado.
7	Superviso el uso de internet por niños, niñas y adolescentes.
8	Reporto a GLOBAL NET TV ZOMAC S.A.S. cualquier comportamiento extraño o acceso no autorizado.

9. Vigencia y actualización

Esta guía rige a partir de su publicación o puesta a disposición de los usuarios. GLOBAL NET TV ZOMAC S.A.S. podrá actualizarla cuando existan cambios técnicos, operativos, regulatorios o de seguridad que hagan necesaria su modificación.

La guía deberá estar disponible para consulta en la página web de la empresa o mediante los canales oficiales de atención, y podrá ser complementada con piezas informativas, recomendaciones, preguntas frecuentes, mensajes de soporte o anexos contractuales dirigidos a los usuarios.

Mensaje final para el usuario
Proteger la red también depende de usted. Cuide sus claves, revise sus dispositivos, no manipule los equipos instalados y reporte oportunamente cualquier situación sospechosa.