



GUÍA DE SEGURIDAD EN INTERNET

¿Por qué leer esta guía?

Internet es hoy una herramienta esencial para estudiar, trabajar, comunicarse y hacer trámites. Sin embargo, también existen personas y programas maliciosos que buscan robar su información, engañarle o dañar sus dispositivos. En EMTEL S.A. E.S.P. nos comprometemos con su seguridad digital, y por eso le ofrecemos esta guía práctica, clara y actualizada.

1. Riesgos más frecuentes en la navegación por Internet

A continuación, encontrará una descripción ampliada de las principales amenazas que existen en la red, su funcionamiento y cómo puede identificarlas.

Amenaza	Descripción	Señales de alerta
Malware	Software malicioso que se instala en su dispositivo sin su permiso. Puede robar datos, bloquear el equipo o usarlo para atacar otros sistemas.	El equipo se vuelve lento, aparecen ventanas emergentes, programas desconocidos se abren solos.
Virus	Programa que se propaga copiándose en archivos y carpetas. Puede corromper o eliminar sus documentos y fotos.	Archivos dañados, mensajes enviados desde su correo sin que usted los haya escrito.
Spyware	Programa espía que recopila en secreto sus contraseñas, hábitos de navegación y datos bancarios, y los transmite a terceros.	Mayor consumo de datos, cambios en la página de inicio del navegador, anuncios personalizados inesperados.



Amenaza	Descripción	Señales de alerta
Phishing	Correos, mensajes o páginas falsas que imitan entidades reales (bancos, entidades gubernamentales) para que usted entregue sus datos.	Correo con urgencia exagerada, enlaces con dirección web sospechosa, errores de ortografía en el remitente.
Ransomware	Tipo de malware que bloquea o cifra todos sus archivos y exige un pago para devolverle el acceso.	Archivos con extensión desconocida, mensaje en pantalla exigiendo dinero para desbloquear el equipo.
Scam / Estafa	Enganos que prometen premios, empleos o inversiones milagrosas a cambio de dinero o datos personales.	Mensajes de desconocidos ofreciendo dinero fácil, concursos que usted no recuerda haber ingresado.
Ciberacoso	Uso de medios digitales para hostigar, amenazar o humillar a una persona. Afecta especialmente a niños y adolescentes en redes sociales.	Mensajes hostiles repetidos, publicación sin consentimiento de información o imágenes privadas.
Grooming	Práctica de acoso y abuso en línea dirigida a niños y jóvenes. El agresor se hace pasar por alguien de confianza para aislar y manipular a la víctima.	Adultos desconocidos que buscan contacto frecuente con menores, solicitudes de imágenes o encuentros.
Robo de identidad	Uso no autorizado de sus datos personales (nombre, cédula, cuentas) para cometer fraudes en su nombre.	Cargos no reconocidos, llamadas de cobro por deudas desconocidas, cuentas que no puede acceder.

2. Amenazas en detalle: cómo funcionan y cómo protegerse

2.1 Phishing y suplantación de identidad

El phishing es uno de los ataques más comunes y exitosos porque apela a la urgencia y la confianza. Los delincuentes envían mensajes que aparentan venir de su banco, de la DIAN, de plataformas de compras o incluso de EMTEL, solicitándole que "verifique su cuenta" o "actualice sus datos".



Cómo reconocerlo:

- El remitente tiene un correo muy parecido al real pero con letras cambiadas (ej. emte1.com.co en lugar de emtel.com.co).
- El mensaje crea urgencia: "su cuenta será bloqueada en 24 horas".
- El enlace lo lleva a una página diferente a la oficial. Pase el cursor sobre el enlace sin hacer clic para ver la dirección real.
- Le piden contraseñas, números de tarjeta o códigos de verificación por correo o mensaje de texto.

Cómo protegerse:

- Nunca haga clic en enlaces de correos no solicitados. Vaya directamente al sitio web oficial escribiendo la dirección en el navegador.
- Verifique siempre que el sitio web use HTTPS (candado en la barra de dirección) antes de ingresar cualquier dato.
- Si recibe un correo sospechoso que aparenta ser de EMTEL, contáctenos directamente por los canales oficiales antes de responder o hacer clic.
- Active la verificación en dos pasos (2FA) en sus cuentas más importantes: banco, correo, redes sociales.

Recuerde

EMTEL S.A. E.S.P. NUNCA le solicitará su contraseña, datos bancarios ni códigos de verificación por correo electrónico, mensaje de texto o llamada telefónica.

2.2 Malware, virus y ransomware

El malware puede llegar a su dispositivo a través de archivos adjuntos en correos, descargas de programas de sitios no oficiales, memorias USB infectadas o incluso anuncios publicitarios en páginas web. El ransomware, una variante especialmente destructiva, puede cifrar todos sus archivos (fotos, documentos, videos) en segundos.



Cómo protegerse:

- Instale y mantenga actualizado un antivirus confiable. Existen opciones gratuitas de buena reputación como Avast, AVG o Windows Defender (ya incluido en Windows 10 y 11).
- Descargue programas únicamente desde las tiendas oficiales (Google Play, App Store, Microsoft Store) o los sitios web del fabricante.
- No abra archivos adjuntos de correos de remitentes desconocidos, especialmente si tienen extensiones .exe, .zip, .rar o documentos de Office que le piden "habilitar macros".
- Haga copias de seguridad periódicas de sus archivos importantes en un disco externo o en la nube. Así, aunque sufra un ataque, no perderá su información.
- Mantenga actualizado su sistema operativo y aplicaciones. Las actualizaciones corrigen vulnerabilidades que los atacantes aprovechan.

2.3 Fraude en banca y comercio electrónico

Las transacciones en línea son cómodas, pero también son objetivo frecuente de delincuentes. Los fraudes pueden ocurrir a través de redes WiFi inseguras, dispositivos compartidos o páginas de tiendas falsas.

Buenas prácticas para compras y banca en línea:

- Realice operaciones bancarias siempre desde una conexión de confianza, preferiblemente su propia red de casa, idealmente con cable (no WiFi).
- Nunca use redes WiFi públicas (centros comerciales, cafés, parques) para acceder a su banco o realizar compras.
- Verifique que la página de la tienda o banco tenga HTTPS y un candado visible en la barra del navegador.
- Prefiera tarjetas virtuales o de prepago para compras en línea. Muchos bancos colombianos las ofrecen sin costo.
- Revise periódicamente los movimientos de su cuenta bancaria para detectar cargos no autorizados a tiempo.
- Cierre siempre la sesión de su banco al terminar. No guarde las contraseñas en el navegador en equipos compartidos.



2.4 Protección en redes sociales y privacidad digital

Las redes sociales son espacios de comunicación valiosos, pero exponen información personal que puede ser usada para engañarle a usted o a sus seres queridos. La sobreexposición de datos personales facilita el robo de identidad, el acoso y las estafas dirigidas.

Recomendaciones de privacidad:

- Configure sus perfiles en redes sociales como “privado” o “solo amigos”. Revise periódicamente qué información es visible para extraños.
- No publique datos sensibles como su dirección, número de cédula, teléfono, lugar de trabajo o rutinas diarias.
- Piense antes de publicar fotos que revelen su ubicación exacta en tiempo real, especialmente si tiene menores en casa.
- Sea selectivo al aceptar solicitudes de amistad o seguimiento de personas que no conoce personalmente.
- Desactive la geolocalización de sus publicaciones cuando no sea estrictamente necesaria.

2.5 Seguridad de contraseñas y cuentas

Una contraseña débil es la puerta de entrada más fácil para un atacante. Según estudios de ciberseguridad, las contraseñas más usadas aún son "123456", "password" o el nombre propio. Estos ejemplos son los primeros que prueban los programas de ataque automático.

Cómo crear y gestionar contraseñas seguras:

- Use contraseñas de al menos 12 caracteres que combinen letras mayúsculas, minúsculas, números y símbolos (ej. @, #, \$, !).
- No use la misma contraseña para varias cuentas. Si una es comprometida, todas lo estarán.
- Cambie sus contraseñas al menos una vez al año, y de forma inmediata si sospecha que una cuenta fue comprometida.
- Considere usar un gestor de contraseñas (como Bitwarden, gratuito y de código abierto) para generar y recordar contraseñas complejas.
- Active la verificación en dos pasos (2FA) siempre que el servicio lo permita. Esto añade una capa extra: aunque alguien robe su contraseña, no podrá entrar sin el código adicional enviado a su teléfono.



3. Protección de los menores de edad en Internet

Niños y adolescentes son usuarios activos de internet y, al mismo tiempo, el grupo más vulnerable frente a ciertos riesgos como el grooming, el ciberacoso y el acceso a contenidos inapropiados. La supervisión activa y el diálogo abierto son las herramientas más efectivas.

3.1 Grooming: el riesgo del contacto de desconocidos

El grooming es un proceso gradual en el que un adulto (o adolescente mayor) se gana la confianza de un menor a través de internet, con el fin de manipularle emocionalmente y, en muchos casos, llegar a la explotación sexual. Suele ocurrir en juegos en línea, chats y redes sociales.

Enseñe a los niños a:

- Nunca compartir con desconocidos su nombre completo, dirección, colegio, número de teléfono ni fotos personales.
- Avisar inmediatamente a un adulto de confianza si alguien desconocido les pide ese tipo de información.
- Bloquear y reportar a cualquier persona que les haga sentir incómodos o que les pida guardar secretos de sus padres.
- Entender que las personas en internet no siempre son quienes dicen ser.

En caso de grooming o abuso en línea

Contacte de inmediato a la Policía Nacional (línea 112) o al ICBF (línea gratuita 018000 918080). Conserve capturas de pantalla como evidencia.

3.2 Control parental: herramientas prácticas

El control parental le permite supervisar y limitar el uso que hacen los menores de los dispositivos y de internet. No reemplaza la conversación y el acompañamiento, pero es una herramienta complementaria muy útil.



Opciones de control parental disponibles:

- Sistema operativo Windows 10/11: desde Configuración → Cuentas → Familia y otros usuarios, puede establecer límites de tiempo de uso, bloquear aplicaciones inapropiadas y supervisar la actividad web del menor con su cuenta de Microsoft.
- Dispositivos Android: Google Family Link permite gestionar las aplicaciones que puede instalar el menor, su ubicación y el tiempo de pantalla.
- Dispositivos iOS (iPhone/iPad): el menú Tiempo en Pantalla (Configuración) permite establecer límites por categoría de aplicación y bloquear contenido adulto en el navegador.
- Router del hogar: algunos modelos de módem/router permiten configurar filtros de contenido directamente desde el panel de administración. Consulte el manual de su equipo o contáctenos.
- Aplicaciones especializadas: Qustodio, Net Nanny y Kaspersky Safe Kids ofrecen opciones avanzadas de supervisión multiplataforma.

4. Buenas prácticas generales de higiene digital

La seguridad digital no depende de una sola herramienta o configuración. Es el resultado de hábitos sostenidos. A continuación, un resumen de las prácticas más importantes:

✓ Buenas prácticas	✗ Evite siempre
Actualizar sistema operativo y apps regularmente	Usar la misma contraseña en varias cuentas
Usar antivirus actualizado	Abrir archivos adjuntos de remitentes desconocidos
Hacer copias de seguridad periódicas	Conectarse a WiFi público para operaciones bancarias
Verificar el HTTPS antes de ingresar datos	Publicar datos personales o ubicación en tiempo real
Activar verificación en dos pasos (2FA)	Instalar programas desde sitios no oficiales
Cerrar la sesión al terminar en equipos compartidos	Hacer clic en enlaces de correos no solicitados



Reportar incidentes a las autoridades

Pagar rescates en caso de ransomware (no garantiza recuperación)

5. Qué hace EMTEL para protegerle

En cumplimiento de la Resolución CRC 5050 de 2016, EMTEL S.A. E.S.P. ha implementado los siguientes sistemas de seguridad en su red para garantizar la integridad y confidencialidad del servicio:

- Protección antispam y antivirus para las cuentas de correo con dominio @emtel.com.co, previniendo la pérdida e integridad de su información.
- Autenticación en tiempo real de todos los usuarios del servicio de acceso a internet, garantizando que solo usuarios autorizados puedan navegar.
- Registro de sesiones (Accounting / no repudio): se generan registros detallados por cada sesión (IP, identidad, fecha y duración), almacenados hasta por un año.
- Sistemas de almacenamiento masivo con protección contra intrusos. Los datos biográficos de los usuarios solo se entregan a entes de seguridad del Estado mediante orden judicial.
- Plataforma de firewall perimetral FORTINET que filtra el tráfico no deseado, bloquea accesos no autorizados y monitorea intentos de intrusión en tiempo real.
- Filtrado de contenido de pornografía infantil según el listado publicado por el Ministerio de Comunicaciones (Ley 679).

Seguridad en la verificación de identidad con EMTEL

Para la contratación de servicios, EMTEL exige fotocopia de la cédula de ciudadanía ampliada al 150% y valida la información antes de cualquier instalación o modificación del servicio. Esto le protege a usted ante posibles suplantaciones de identidad.

6. ¿Qué hacer en caso de incidente?

Si usted o un miembro de su hogar es víctima de un delito informático, actúe con rapidez:

- No pague ningún rescate. Pagar no garantiza recuperar su información y financia a los delincuentes.
- Desconecte el dispositivo afectado de la red (WiFi y cable) para evitar que el daño se propague.



- Tome capturas de pantalla o fotografías de los mensajes o pantallas sospechosas como evidencia.
- Cambie inmediatamente las contraseñas de sus cuentas más importantes desde un dispositivo seguro.
- Reportel el incidente al Centro Cibernético de la Policía Nacional: línea 112 o denuncias en la página cc.policia.gov.co.
- Si el robo involucra datos financieros, notifique de inmediato a su banco para bloquear tarjetas y cuentas.
- Para incidentes relacionados con su servicio EMTEL, contáctenos a través de los canales oficiales indicados en su contrato de servicio.

7. Recursos y canales de apoyo

Estos son algunos recursos confiables donde puede profundizar o buscar ayuda:

Entidad / Recurso	Descripción	Contacto
Centro Cibernético Policía	Recibe denuncias de delitos informáticos en Colombia	cc.policia.gov.co / Línea 112
ICBF	Protección de menores. Grooming y ciberacoso infantil	018000 918080 (gratuito)
Ministerio TIC (MinTIC)	Campañas y recursos de seguridad digital para ciudadanos	mintic.gov.co
SocialTIC	Buenas prácticas de seguridad digital en español	socialtic.org
EMTEL S.A. E.S.P.	Soporte técnico y reporte de incidentes con su servicio	www.emtel.com.co