CAFENET COMUNICACIONES S.A.
Teléfono: 315 552 46 19
Carrera 23 No.62-39 Of.1204
Edificio Empresarial Capitalia
cafenetsa@cafenet.com.co
Manizales – Caldas

NEUTRALIDAD EN INTERNET-RIESGOS DE SEGURIDAD

CAFENET COMUNICACIONES S.A. en su condición de Prestador de Servicios de Telecomunicaciones, y con el fin de garantizar lo establecido en la Resolución 5050 de 2016 de la CRC, cumple con el principio de neutralidad en internet, informando a los usuarios 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, para esto, existe en la página web cafenet.com.co un link con estos riesgos y algunas recomendaciones para los usuarios.

Los **riesgos relativos a la seguridad en la red** son amenazas que pueden afectar la confidencialidad, integridad y disponibilidad de los sistemas informáticos conectados. Estos riesgos pueden tener consecuencias graves, como pérdida de datos, robo de información personal, laboral o financiera, interrupciones del servicio, y daños a la reputación. A continuación, se enumeran los principales:

1. Malware (software malicioso)
Tipos comunes: virus, gusanos, troyanos, ransomware, spyware, adware.
Riesgo: robo de información, cifrado de archivos, espionaje, uso de recursos sin autorización.

2. Ataques de phishing
Riesgo: robo de credenciales o información personal mediante engaños (correos o sitios web falsos).
Ejemplo: un correo que simula ser de tu banco pidiéndote iniciar sesión.

3. Ingeniería social
Riesgo: los atacantes manipulan a personas para obtener acceso o información confidencial.
Ejemplo: llamadas telefónicas pretendiendo ser soporte técnico.

4. Intercepción de comunicaciones (sniffing)
Riesgo: captura de datos mientras viajan por la red, especialmente en redes Wi-Fi públicas sin cifrado.

5. Ataques de denegación de servicio (DoS/DDoS)
Riesgo: sobrecarga de servidores o redes, provocando que los servicios legítimos no estén disponibles.

6. Vulnerabilidades en software o hardware
Riesgo: errores o fallos en los sistemas que pueden ser explotados por atacantes.
Ejemplo: sistemas no actualizados con parches de seguridad.

7. Acceso no autorizado
Riesgo: intrusos que ingresan a redes o sistemas internos sin permiso.
Puede deberse a: contraseñas débiles, configuraciones inseguras o falta de control de acceso.

CAFENET COMUNICACIONES S.A.
Teléfono: 315 552 46 19
Carrera 23 No.62-39 Of.1204
Edificio Empresarial Capitalia
cafenetsa@cafenet.com.co
Manizales – Caldas

8. Pérdida o filtración de datos
Riesgo**:** exposición pública o robo de información sensible (por ejemplo, bases de datos de clientes).
Causa común: malas prácticas en el almacenamiento o transferencia de datos.

9. Suplantación de identidad (spoofing)
Riesgo: un atacante finge ser una entidad confiable (dirección IP, MAC, correo, etc.) para obtener acceso o información.

10. Uso de redes inseguras
Riesgo: conexión a redes Wi-Fi públicas sin cifrado adecuado, que pueden ser puntos de acceso falsos (man-in-the-middle).

Recomendaciones para evitar vulnerabilidades en la red

1. Usa contraseñas fuertes y únicas
Al menos 12 caracteres, combinando letras, números y símbolos.
Usa un gestor de contraseñas para almacenarlas de forma segura.
Evita reutilizar contraseñas entre distintos servicios.

2. Activa la autenticación de dos factores (2FA)
Añade una capa extra de seguridad (por ejemplo, un código que llega a tu móvil o una app de autenticación).
Especialmente importante para correo, cuentas bancarias y redes sociales.

3. Mantén el software siempre actualizado
Aplica parches de seguridad al sistema operativo, navegadores, antivirus y programas.
Habilita actualizaciones automáticas si es posible.

4. Usa un antivirus o solución de seguridad confiable
El antivirus debe estar siempre actualizado.
Escanea regularmente el sistema en busca de malware.

5. Navega de forma segura
Asegúrate de que los sitios web usen **HTTPS** (candado en la barra del navegador).
No hagas clic en enlaces sospechosos o no verificados.
Evita descargar archivos desde fuentes no confiables.

6. Evita redes Wi-Fi públicas sin protección
Si necesitas usarlas, conéctate mediante una **VPN (red privada virtual)**.
Nunca accedas a servicios sensibles (como banca en línea) desde redes abiertas sin protección.

7. Sé cuidadoso con la información que compartes
No publiques datos personales sensibles en redes sociales o foros públicos.
Verifica siempre la identidad de quien te pide información confidencial.

CAFENET COMUNICACIONES S.A.
Teléfono: 315 552 46 19
Carrera 23 No.62-39 Of.1204
Edificio Empresarial Capitalia
cafenetsa@cafenet.com.co
Manizales – Caldas

8. Capacita a los usuarios (en caso de empresas)
Realiza entrenamientos periódicos en **ciberseguridad y phishing**.
Fomenta la cultura de "piensa antes de hacer clic".

9. Haz copias de seguridad regularmente
Utiliza servicios en la nube o discos externos.
Asegúrate de que las copias estén cifradas y protegidas del acceso no autorizado.

10. Configura bien tu red doméstica o empresarial
Cambia las contraseñas por defecto de tu router.
Usa cifrado **WPA3 o al menos WPA2**.
Desactiva servicios innecesarios y administra quién tiene acceso.

11. Desconfía del correo no solicitado
Si recibes un correo sospechoso: **no respondas, no hagas clic en enlaces ni descargues archivos adjuntos.**
Verifica siempre la dirección del remitente.