SEGURIDAD INFORMÁTICA PARA LOS USUARIOS

OBJETIVO

Este documento tiene como finalidad mantener informados a los usuarios del servicio de acceso a Internet de **CABLEXPAND S.A.S.** sobre los riesgos asociados a la seguridad de la red, así como ofrecer recomendaciones y acciones básicas que deben ser adoptadas por los usuarios para contribuir con la protección y el correcto uso de los servicios contratados, conforme a estándares internacionales como la Norma ISO/IEC 27001:2022 y las buenas prácticas definidas en ISO/IEC 27002:2022.

1. ¿QUÉ ES LA SEGURIDAD INFORMÁTICA?

La seguridad informática es el conjunto de prácticas, medidas y tecnologías destinadas a proteger la confidencialidad, integridad y disponibilidad de la información y de los sistemas digitales que la procesan. En el contexto del servicio de internet de TuCable, implica proteger:

- La red WiFi del hogar
- Los dispositivos conectados (celulares, televisores, computadores, etc.)
- La información personal del usuario (como contraseñas, datos bancarios, fotos o conversaciones)

Una red insegura puede convertirse en una puerta abierta para los delincuentes digitales. Por eso, este documento busca que cada usuario se convierta en un aliado activo para preservar la seguridad desde su hogar

2. PRINCIPALES AMENAZAS O RIESGOS PARA LA RED DOMICILIARIA

Phishing: Técnica utilizada para engañar al usuario mediante correos o mensajes falsos que simulan ser de una entidad confiable (como un banco, empresa o incluso TuCable), con el fin de robar datos personales, contraseñas o números de tarjetas.

¿Cómo evitarlo?

- No abras enlaces de remitentes desconocidos.
- Verifica siempre el correo del remitente.
- No ingreses contraseñas en sitios sospechosos.

Malware (virus, troyanos, spyware): Programas maliciosos que se instalan sin permiso en tus dispositivos. Pueden dañar archivos, espiar tus actividades o tomar el control de tu red.

¿Cómo evitarlo?

- Instala un buen antivirus.
- No descargues archivos de páginas dudosas.
- No conectes USBs desconocidos.

Red WiFi sin protección: Si tu WiFi no tiene contraseña o tiene una muy débil, cualquiera puede conectarse y usar tu red para actividades ilegales, espiarte o robar tu información.

¿Cómo evitarlo?

- Cambia la contraseña de tu módem regularmente.
- Usa contraseñas seguras (mínimo 8 caracteres, con letras, números y símbolos).
- Activa el cifrado WPA2.

Accesos no autorizados: Personas que se conectan sin tu consentimiento a tu red, acceden a tus archivos o controlan dispositivos como cámaras o asistentes inteligentes.

¿Cómo evitarlo?

- Cambia el nombre de tu red (SSID) para que no diga el nombre del operador o del módem.
- Desactiva funciones de acceso remoto si no las usas.
- Revisa los dispositivos conectados desde la configuración del módem.

Suplantación de identidad (spoofing): Alguien se hace pasar por ti en internet usando tu correo, red o datos robados.
¿Cómo evitarlo?

- No compartas tus claves.
- Activa la autenticación en dos pasos cuando sea posible.
- Revisa frecuentemente tu actividad de inicio de sesión en correos y redes sociales.

Falsos puntos WiFi gratuitos (man-in-the-middle): Redes públicas falsas que se hacen pasar por legítimas para interceptar tu tráfico y robar información.
¿Cómo evitarlo?

- Nunca te conectes a redes públicas sin protección.
- Usa datos móviles o VPN si debes conectarte fuera de casa.

3. ¿QUÉ ACCIONES DEBE TOMAR EL USUARIO PARA PRESERVAR LA SEGURIDAD?

3.1 Buenas prácticas básicas

- Cambia la contraseña predeterminada del módem o router.
- No compartas tu WiFi con personas desconocidas.
- Revisa regularmente qué dispositivos están conectados a tu red.
- Apaga el WiFi si te vas a ausentar por varios días.

3.2 Educación digital

- Habla con tus hijos y personas mayores sobre los riesgos.
- Asegúrate de que sepan identificar mensajes sospechosos.
- Usa control parental si hay menores en casa.

3.3 Mantenimiento y actualización.

- Actualiza tu módem o router y dispositivos con regularidad.
- Usa antivirus y mantén tu software al día.
- Si notas lentitud, dispositivos extraños conectados o cambios no autorizados, repórtalo.

4. COMPROMISO DE TUCABLE

TuCable S.A.S. se compromete con la mejora continua en la gestión de seguridad de la información y la protección de sus usuarios, implementando controles técnicos y administrativos conforme a las normas ISO/IEC 27001:2022. No obstante, la seguridad completa requiere de la colaboración activa de cada usuario.

5. CONTACTO PARA SOPORTE Y REPORTES

- Línea de atención al cliente: **301 2171257**
- Correo electrónico: **cablexpand@gmail.com**
- Sitio web: **www.cablexpand.com**

6. MENSAJE FINAL

¡Cuidar tu red también es tu responsabilidad!

Juntos protegemos lo que más importa: tu conexión, tu información y tu tranquilidad.