

SEGURIDAD DE LA INFORMACIÓN Y PREVENCIÓN DE FRAUDES

En cumplimiento de la Resolución CRC 5050 de 2016, artículo 2.9.2.4, que establece la obligación de mantener informados a los usuarios sobre los riesgos relativos a la seguridad de la red y las acciones preventivas que deben adoptar, TV ISLA LTDA presenta la presente guía de Seguridad de la Información y Prevención de Fraudes, enmarcada en los principios de la Neutralidad en Internet y el compromiso con la protección de los datos y la confianza digital de nuestros usuarios.

Principios de la Seguridad de la Información

- **Integridad:** La información no puede ser modificada sin autorización.
- **Confidencialidad:** Solo las personas autorizadas pueden acceder y leer la información.
- **Disponibilidad:** Los datos deben estar accesibles cuando se necesitan.
- **Irrefutabilidad o no repudio:** No se puede negar la autoría de la información generada o enviada.

Activos y Riesgos

Los activos de la empresa incluyen recursos tangibles (servidores, equipos, redes) e intangibles (datos, políticas, procesos). Estos pueden verse afectados por vulnerabilidades, amenazas y riesgos que comprometan la seguridad, disponibilidad o confidencialidad de la información.

Medidas de Protección Implementadas

1. Firewall de red: Filtra el tráfico y bloquea accesos no autorizados.
2. Antivirus y anti-spam: Detectan y eliminan programas maliciosos y correos no deseados.
3. Criptografía y cifrado: Protegen los datos transmitidos y almacenados, asegurando su confidencialidad.
4. Políticas de contraseñas seguras: Fomentan el uso de claves robustas y renovaciones periódicas.
5. Monitoreo NOC: Supervisión continua de la red para identificar y mitigar incidentes.
6. Actualización de sistemas: Aplicación de parches de seguridad y mantenimiento preventivo de la infraestructura.

Principales Amenazas y Prevención

- **Correo electrónico:** Medio común de propagación de virus. No abrir adjuntos desconocidos ni mensajes de origen dudoso.
- **Spam:** Envío masivo de correos no solicitados con publicidad o fraudes.



- Suplantación de identidad (phishing): Sitios falsos que imitan páginas legítimas para robar datos.
- Ingeniería social: Manipulación psicológica para obtener información confidencial.
- Códigos maliciosos: Virus, gusanos o troyanos diseñados para dañar o robar información.

Prevención del Fraude Digital

TV ISLA promueve la cultura de ciberseguridad y la educación digital entre sus usuarios. Se recomienda verificar siempre las direcciones web y certificados de seguridad, nunca entregar datos personales o financieros por correo o teléfono, y desconfiar de mensajes que prometen premios o generan presión mediante amenazas de cierre de cuentas.

Recomendaciones para los Usuarios

- Mantenga actualizado su antivirus y sistema operativo.
- Utilice contraseñas seguras y no las comparta.
- Verifique los enlaces antes de hacer clic en correos o mensajes.
- Evite conectarse a redes Wi-Fi públicas para realizar transacciones sensibles.
- Reporte cualquier sospecha de fraude al correo oficial de soporte de TV ISLA.

Conclusión

TV ISLA reafirma su compromiso con la seguridad digital, la transparencia y la protección de los datos personales de sus usuarios. A través de la implementación de políticas, tecnologías y educación preventiva, la empresa busca fortalecer la confianza en el uso del servicio de Internet, asegurando la integridad y disponibilidad de la información.

