



## **ELEMENTOS DE SEGURIDAD EN LA WEB.**

La seguridad en internet son todas aquellas precauciones que se toman para proteger todos los elementos que hacen parte de la red, como infraestructura e información, que suele ser la más afectada por delincuentes cibernéticos. La seguridad informática se encarga de crear métodos, procedimientos y normas que logren identificar y eliminar vulnerabilidades en la información y equipos físicos, como los computadores. Este tipo de seguridad cuenta con bases de datos, archivos y equipos que hacen que la información importante no caiga en manos de personas equivocadas.

### **Principales riesgos en internet**

Algunas de las cosas que los cibercriminales buscan conseguir por medio de internet son:

- Robo de información
- Daño de información
- Ataques a sistemas o equipos
- Suplantación de identidad
- Venta de datos personales
- Robo de dinero

Los delincuentes cibernéticos usan varios modos para atacar a una víctima en la red como los virus con los que logran vulnerar sistemas y alterar el funcionamiento de los dispositivos electrónicos, o el phishing, que consiste en que un cibercriminal se hace pasar por una persona diferente por medio de correos electrónicos, mensajería instantánea o redes sociales para adquirir información confidencial como contraseñas, tarjetas de crédito, entre otros.

### **¿Cómo prevenirlo?**

Si se maneja mucha información y se cuenta con varios equipos, como en los casos de las empresas, lo mejor es solicitar ayuda a profesionales encargados de la seguridad en internet. De otro lado, como usuario se pueden tomar varias medidas preventivas como mantener activados y actualizados los antivirus en



nuestros dispositivos con conexión a internet, evitar realizar operaciones financieras en redes abiertas o computadores públicos y verificar los archivos adjuntos de mensajes de desconocidos y evitar descargarlos si no se tiene plena seguridad de su contenido.

Mantenga siempre un antivirus actualizado en su equipo(s), procure correr éste periódicamente, de la misma manera, tenga en su equipo elementos como anti-spyware y bloqueadores de pop- up (ventanas emergentes).

Evite visitar páginas no confiables o instalar software de dudosa procedencia. La mayoría de las aplicaciones peer-to-peer contiene programas espías que se instalan sin usted darse cuenta.

Asegúrese que se aplican las actualizaciones en sistemas operativos y navegadores Web de manera regular.

Si sus programas o el trabajo que realiza en su computador no requieren de pop-up, Java support, ActiveX, Multimedia Autoplay o auto ejecución de programas, deshabilite estos.

Si así lo requiere, obtenga y configure el firewall personal, esto reducirá el riesgo de exposición.

Para **TELNET ISP S.A.S** la seguridad informática de nuestros clientes es primordial, por tal motivo hemos implementado herramientas de software y hardware que nos permiten cumplir con los más altos estándares de seguridad en nuestra red y con los términos establecidos por la regulación. Es indispensable contar con las medidas de seguridad necesarias para evitar posibles ataques de hackers, virus o cualquier otro acto de intervención de terceros. Por esta razón, deben contener mecanismos que protejan y reduzcan los riesgos de seguridad alojados, distribuidos y potencializados a través del mismo servicio de Internet.

“**TELNET ISP S.A.S**” cuenta con sistemas de autenticación y autorización para controlar el acceso a los diferentes servicios de la red, al igual que controles de autenticación para los usuarios (equipos terminales de acceso del cliente).