Seguridad en la red

A continuación encontrarás un listado de algunos de los riesgos a los que estas expuesto como usuario de nuestros servicios y que no pueden ser controlados por **INSITEL S.A.S.**:

- Infiltración en las comunicaciones por utilizar redes de datos públicas, para transferir información.
- Robo o fuga de información al enviar datos a través de redes públicas.
- Robo o fuga de información por la falta de conocimiento y/o por el buen uso que se le dé al dispositivo móvil.
- Daño intencional del móvil y/o alguno de sus componentes de software por la utilización de software no licenciado o por el envío y/o recepción de información a través de redes de datos públicas.
- Problemas de desempeño del equipo móvil y/o alguno de sus componentes de software debido a la administración que se le dé a la información almacenada en él.
- Actividades de espionaje debido al uso que se le dé al dispositivo móvil o al intercambiar datos a través de redes públicas como Internet.
- Uso indebido de las facilidades de software y/o de la información provista por el móvil debido a la no disponibilidad o falta de configuración de las facilidades de control de acceso disponibles en el dispositivo móvil.
- Uso del medio de comunicación para la transmisión de información con fines malintencionados.
- Fomento y/o recepción de mensajes no esperados o de origen desconocido.

- No disponibilidad del servicio de telefonía móvil y/o de valor agregado por motivos de “fuerza mayor”.
- Pesca de información, se utilizan mensajes de correo electrónico "engañosos" y sitios Web falsos para pedir información personal a los usuarios. Se pueden reconocer porque ofrecen promociones para recargas. Por eso debes recordar que ese procedimiento sólo se hace a través de Servicio en Línea.
- Correos electrónicos que parecen provenir de una compañía reconocida y son fraudulentos. Estos correos deben eliminarse de inmediato porque un simple clic puede producir la instalación de un virus que graba tus actividades en el teclado y con esto obtener tus datos bancarios.
- Mensajes de texto en su celular diciendo que gano un premio y que debe responder con sus datos, debe poner mucha atención pues no es más que una nueva técnica usada por los delincuentes para cometer fraudes a su nombre. Los clientes en red necesitan que se les garantice que los proveedores aplican prácticas adecuadas de seguridad para mitigar los riesgos a los que se enfrentan el cliente y el proveedor (por ejemplo, los ataques distribuidos de denegación de servicio, o DDoS). Por este motivo, hemos expresado muchas de las recomendaciones del informe en forma de listado de cuestiones que puede ser utilizado para ofrecer o recibir aseguraciones.
- Evaluar el riesgo de utilizar servicios en red.
- Comparar las ofertas de los distintos proveedores en red.
- Obtener aseguraciones de los proveedores en red seleccionados.
- Reducir la carga de la aseguración con respecto a los proveedores en red.

- La lista de comprobación de seguridad abarca todos los aspectos de los requisitos en materia de seguridad, incluidas la seguridad física y las implicaciones legales, políticas y técnicas.

RECOMENDACIONES GENERALES

- Lea cuidadosamente las instrucciones de uso de los dispositivos de comunicación móvil que utilizará con los servicios de **INSITEL**.
- Cerciórese de la autenticidad de los sitios que visita en redes públicas como Internet.
- Utilice únicamente software licenciado en los dispositivos de comunicación móvil que utilizará con los servicios de **INSITEL.**
- Actualice el software instalado en los dispositivos de comunicación móvil que utilizará con los servicios de **INSITEL** bajo las recomendaciones del fabricante.
- No transfiera información confidencial y/o sensible a través de redes públicas como Internet.
- No almacene información confidencial y/o sensible en sus dispositivos móviles.
- Manténgase actualizado de las amenazas latentes utilizando los servicios de compañías de desarrollo de sistemas antivirus para dispositivos de comunicación móvil.
- No comparta el uso de su dispositivo móvil a personas que bajo su criterio no le brinden confianza.
- Configure y mantenga las herramientas de control de acceso en sus dispositivos de comunicación móvil.

- Legalice a través de cesiones de contrato, las líneas adquiridas por usted a nombre de terceros.
- No preste su nombre para realizar transacciones como la compra de planes ante **INSITEL**.
- Revise periódicamente su estado de cuenta en centrales de riesgo; esto alerta de cualquier anomalía en su estado de cuenta personal.
- No preste su tarjeta SIM o su teléfono a otras personas, recuerde que el suscriptor es totalmente responsable por el uso de la tarjeta SIM y del teléfono.
- Absténgase de abrir mensajes de texto y abrir o ejecutar archivos, que no provengan de fuentes reconocidas.
- Con relación al uso de Internet recuerde que no es posible guardar registros de las direcciones de Internet que desde su móvil se acceden, por lo que no se le podrá suministrar detalle de los sitios web visitados.
- Compre tarjetas prepago en sitios reconocidos por usted y verifique que el plástico esté totalmente sellado y sin enmendaduras, que los dígitos del PIN estén completos, la tarjeta debe estar en perfecto estado y cargarla en frente de la persona que se la vende, para garantizar su compra.
- No suministrar información personal por medio de correo electrónico o portales web que el cliente no conozca o sospeche que no son legales. Por eso el cliente debe recordar que ese procedimiento sólo se hace a través de la línea de servicio al cliente.
- Verifique que la dirección del portal de **INSITEL** esté correctamente escrita, no de click sobre link enviados en correos electrónicos o enlaces de buscadores de internet tipo Google.

- Es importante crear claves difíciles de identificar, recuerdo cambiarlas frecuentemente en cada uno de los portales donde tenga acceso. Memorice las claves, no las escriba ni guarde en lugares de fácil acceso. No permitas que terceros vean o conozcan sus claves.
- Determinadas cuestiones relativas a la Directiva de protección de los datos personales y a las recomendaciones del grupo de protección de las personas.
- La obligación de los proveedores en red de notificar a sus clientes los incumplimientos relativos a la seguridad de los datos.
- El mejor modo de apoyar las normas mínimas de protección de datos y los sistemas de certificación de privacidad comunes a todo los Estados miembros.