SEGURIDAD
EN LA RED

A continuación, relacionamos algunos de los riesgos inherentes al medio de comunicación, cuya mitigación dependerá del uso adecuado que el suscriptor le dé a su equipo terminal móvil:

- Fuga o robo de información a causa de las siguientes razones:
- Uso indebido de redes públicas para el intercambio de información.
- Presencia de software malintencionado en el equipo terminal móvil.
- Alteraciones en el sistema Operativo del equipo terminal móvil para la utilización de software no licenciado.
- Falta de conocimiento en el manejo de las funcionalidades del equipo terminal móvil.
- Pérdida o robo del equipo terminal móvil.
- Daño o mal funcionamiento del equipo terminal móvil debido a mala configuración realizada por el usuario o por software malicioso.
- La utilización del dispositivo móvil para infringir aspectos de la ley colombiana como piratería, derechos de autor, pornografía infantil, terrorismo, etc. son responsabilidad del usuario.
- Eventos de fraude en compras o transacciones ocasionados como producto de la utilización de redes públicas no seguras.
- No realizamos respaldo de ningún tipo de información del cliente, por lo cual es responsabilidad de este mantener un respaldo de la misma.
- Generación o recepción de SPAM mediante herramientas maliciosas utilizando correo electrónico o SMS.
- Indisponibilidad del servicio de telefonía móvil y otros servicios a causa de eventos de Fuerza Mayor.

Recomendaciones Generales de Seguridad:

- Para la protección de su información habilite medidas de control de acceso al equipo terminal móvil como la protección con contraseña si está disponible.
- Configurar el equipo terminal móvil para su bloqueo automático pasados unos segundos de inactividad.
- Cuando vaya a instalar una nueva aplicación revisar su reputación. Sólo instalar aplicaciones que provengan de fuentes de confianza.
- Mantenga actualizado el software de su equipo terminal móvil, tanto el Sistema

Operativo como las aplicaciones que tenga instaladas.

- Configure el Bluetooth de su dispositivo móvil como oculto y con necesidad de contraseña.
- Realizar copias de seguridad periódicas de la información contenida en su equipo terminal móvil (Contactos, documentos, aplicaciones y demás). Considere no almacenar información sensible en su equipo terminal móvil. De hacerlo realice un cifrado de la información contenida en él.
- En caso de robo o pérdida del equipo terminal móvil por favor informar a las autoridades y al proveedor de servicios de telefonía.
- No abra archivos adjuntos o haga clic en enlaces de correos electrónicos o SMS de remitentes sospechosos o desconocidos.
- Evite realizar transacciones o compras en redes públicas que no cuentan con los mecanismos mínimos de seguridad.
- Procure tener instalado un software antivirus en caso de que su equipo terminal móvil lo soporte.

Recomendaciones para tener en cuenta en nuestro portal transaccional:

Antes de crear su cuenta de usuario en nuestro portal transaccional por favor tenga presente los siguientes conceptos los cuales le ayudaran a tener una experiencia segura al utilizar nuestros servicios:

- **¿Qué es el phishing?**

  El phishing es un término informático designado para cierta modalidad de estafa, la cual busca obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Para esto el criminal busca hacerse pasar por una persona o empresa de confianza mediante una aparente comunicación oficial, por lo general a través de correo electrónico, o algún sistema de mensajería instantánea, de manera que genere confianza a la persona y lo lleve a un sitio fraudulento preparado especialmente para obtener la información confidencial del usuario sin que este se dé cuenta.

- **¿Cómo protegerse?**

  El mejor comportamiento que podemos adoptar como usuarios y de esta manera estar más tranquilos y no ser estafados, es que NUNCA respondamos a NINGUNA solicitud de información personal a través de correo electrónico, llamada telefónica o mensajes de texto (SMS). Las entidades u organismos con una política responsable de la seguridad de su información, NUNCA le solicitarán contraseñas, números de tarjeta de crédito o cualquier información personal por correo electrónico, por teléfono o SMS. Nunca le solicitaremos información confidencial mediante estos medios ya que velamos por la seguridad de la información de nuestros clientes.

- **¿Qué es el Malware?**

  El Malware también es conocido como código maligno, software malicioso o software malintencionado. Es un tipo de software que tiene como objetivo infiltrarse sin el consentimiento de su propietario con el objetivo de robar información o dañar una computadora o Sistema de información. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos. El término malware incluye virus, gusanos, troyanos y otros software maliciosos e indeseables.

- **¿Cómo protegerse?**

  Existen múltiples factores por los cuales nuestros equipos podrían resultar infectados por algún tipo de malware, como por ejemplo visitar páginas sospechosas, instalar software no reconocido, abrir archivos sospechosos y demás. Por lo anterior es importante fortalecer las defensas contra cualquier tipo de código malicioso en nuestro equipo, siguiendo las siguientes recomendaciones:

  Instale programas antivirus y anti spyware de una fuente de confianza. Los programas anti malware exploran y supervisan su equipo en busca de virus y spyware conocidos. Cuando encuentran algo, le avisan y le permiten tomar medidas para remediarlo.

  Mantenga todo el software actualizado. Instale actualizaciones de todo el software con regularidad y subscríbase para recibir actualizaciones automáticas siempre que sea posible.

  Use contraseñas seguras y manténgalas en secreto. No comparta sus contraseñas con nadie, recuerde que son de uso personal. No utilice palabras comunes en sus contraseñas que sean fácilmente descifrables por un atacante malicioso.

  Nunca desactive su firewall. Un firewall establece una barrera de protección entre su equipo e Internet. Desactivarlo, incluso durante un minuto, aumenta el riesgo de que su PC resulte infectado por malware.

  Utilice los dispositivos de almacenamiento externo (Usb, tarjetas SD/microSD, etc) con cuidado. Cuando conecte su dispositivo externo de almacenamiento en un equipo público, siempre utilice un software antimalware antes de abrir cualquier archivo para evitar riesgos de infecciones por virus u otro tipo de código malicioso.

Como crear una contraseña segura:

Para acceder a nuestros servicios es importante que asigne una contraseña segura.

Para esto le recomendamos algunos aspectos importantes para elaborar su contraseña:

- La longitud de las contraseñas no debe ser inferior a ocho caracteres.
- Se debe tener en cuenta que a mayor longitud más difícil será para un atacante encontrar su contraseña y mayor seguridad ofrecerá.
- Las contraseñas deben estar formadas por una mezcla de caracteres alfabéticos (Donde se combinen las mayúsculas y las minúsculas), números e incluso caracteres especiales (@, *, +, &, /, $, etc.)
- Se deben cambiar las contraseñas regularmente (Dependiendo de la criticidad de los datos puede ser cada 3 meses)

Para mejorar la seguridad de su contraseña recuerde que esta nunca debe contener:

- Su nombre o apellidos
- Nombre de sus hijos, padres o familiares cercanos.
- Fechas especiales (Fechas de cumpleaños, aniversario, etc.)
- Número de identificación
- El mes y el año en que creó la contraseña

Recuerde que usted es parte fundamental en la protección de su información; por esto recuerde que sus contraseñas son personales y no se deben divulgar a nadie.

setroc mobile GROUP S.A.S