TIPS

para transacciones seguras y protección de la información

1. Es importante instalar y mantener actualizado un **antivirus** en nuestros dispositivos (computador o equipos móviles) para para evitar que programas maliciosos, conocidos como Ramsomware, secuestren la información personal.

2. Evitar realizar transacciones como pagos, transferencias o consultas utilizando redes públicas, digitar siempre la dirección web de la entidad y **cerrar sesión** después de ingresar al portal de su entidad financiera.

3. Así estemos en nuestro computador personal n**o darle recordar contraseña** de los sitios transaccionales de nuestra entidad financiera.

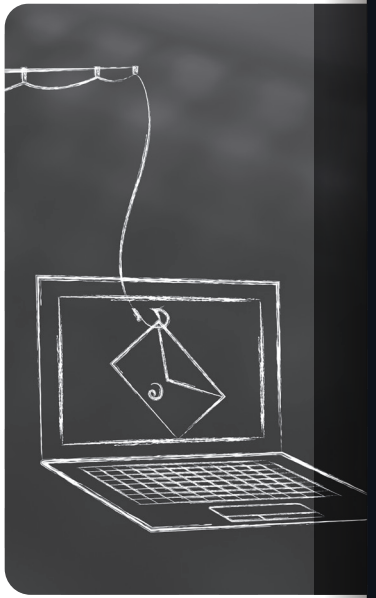
4. Cambiar con frecuencia las contraseñas de cajero o de ingreso a los servicios digitales de su entidad financiera, no usar datos personales como fechas de cumpleaños, por ejemplo.

5. Activar los **servicios de alerta** de transacciones que ofrecen las entidades financieras a través de mensajes de texto, hacer uso de las claves dinámicas y fijar topes en las transacciones cuando sea permitido.

6. No ingresar a enlaces recibidos a través de mensajes de texto y correos electrónicos en los que se pide realizar un registro del usuario y suministrar datos personales. En ocasiones los ciberdelincuentes se hacen pasar por empresas existentes o entidades financieras creando estos **falsos enlace**s para hurtar la información confidencial (phishing).

7. Nunca suministrar los datos personales o financieros (número de la tarjeta de crédito, códigos de seguridad, fecha de vencimiento) **al atender una llamada** en la que dicen ser de una entidad financiera, los inescrupulosos buscarán con cualquier argumento obtener nuestra información

8. Al realizar el cambio de plástico de una tarjeta débito o crédito **no debemos entregar** ninguna de las partes a la persona que nos la entrega, debemos destruir por completo la tarjeta anterior, incluyendo el chip.



9. Al recibir correos en los que dicen que nuestros productos financieros han sido bloqueados y agregan un enlace para **supuestamente desbloquearlos** no debemos darle clic, generalmente trae implícito un troyano o somos redireccionados a un formulario en el que nos piden digitar información personal.

10. Utilizar el **reconocimiento facial**, la huella digital o una clave de seguridad en el celular para desbloquearlo, así se evita que extraigan la información guardada en el dispositivo móvil en caso de llegar a extraviarlo.

11. Si su **celular fue robado** reporte el hecho a las autoridades competentes e informe a su entidad financiera.

12. No aceptar **ayuda de extraños** cuando se realizan transacciones en cajeros electrónicos, datáfonos o en los corresponsales bancarios.

13. El cambiazo de la tarjeta puede suceder en un cajero o al hacer una compra, por eso NUNCA se debe perder de vista y **verificar** que la que nos devuelven luego de una compra es efectivamente la nuestra.

14. **No compartir** o guardar escritas las claves de acceso a los productos financieros.

Quejas ante la Superintendencia Financiera de Colombia

Los canales disponibles para que la ciudadanía presente sus quejas ante la Superintendencia Financiera de Colombia son:

- Botón Presente su queja ubicado en la página principal del sitio web: **www.superfinanciera.gov.co**
- Desde el celular **#903**
- Centro de Contacto: **+57 601307 8042**
- Línea gratuita nacional: **018000 120100**
- Correo electrónico: **super@superfinanciera.gov.co**

En redes sociales:

- **Twitter:** @SFCsupervisor
- **Facebook:** Superintendencia Financiera de Colombia
- **Instagram:** @superfinanciera