No corras riesgos…

¡La seguridad financiera está en tus manos!

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

CENTRO CIBERNÉTICO POLICIAL

REPÚBLICA DE COLOMBIA
POLICÍA NACIONAL
DIOS Y PATRIA

ASOBANCARIA
Construyendo la Confianza y Solidez del sector financiero

ABC

para evitar ser víctima de fraude bancario

ASOBANCARIA

Construyendo
la **Confianza** y **Solidez** del sector financiero

www.asobancaria.com

Diseño por: Increnta Colombia
www.increnta.com/co

tus tarjetas y contraseñas que pueden ser utilizados por manos criminales.

o. **Evita,** de igual forma utilizando redes Wi-Fi públicas porque tu información quedará almacenada en el historial de búsqueda.

p. **Siempre ingresa** a la página web de tu entidad financiera digitando la URL completa (por ejemplo www.bancoabc.com) en la barra de direcciones y nunca lo hagas a través de enlaces que encuentras en buscadores como Google o Mozilla o en correos electrónicos.

q. **Verifica** que la conexión sea segura, es decir, que el sitio web donde piensas realizar la transacción, te garantice que la información que uses sea privada por lo que contraseñas y números de tarjeta de crédito no quedarán almacenados. Puedes corroborarlo revisando que la URL o dirección web de la entidad financiera empiece por https://

i. **Reclama siempre el comprobante** de la operación efectuada.

j. **Activa los servicios de la banca *online* en tu celular** para que te notifique a través de un mensaje de texto a tu celular cualquier tipo de transacción que realices con tu tarjeta.

k. **Desconfía de las empresas de telemercadeo** que te llamen a ofrecer productos argumentando premios, bajos precios o promociones tentadoras; en ocasiones se hacen pasar por entidades financieras.

l. **No descuides tu tarjeta** cuando la utilices en establecimientos comerciales.

m. **No accedas a enlaces enviados a través de mensajes SMS/MMS** no solicitados y que impliquen la descarga de contenidos en los dispositivos; esto ayudará a prevenir que el dispositivo sea infectado con software malicioso (*malware*), el cual le permitiría al delincuente tener el control del dispositivo y la información almacenada en él.

n. **No realices transacciones** en computadores de acceso público (cafés internet, centros comerciales o bibliotecas) porque es posible que estos almacenen la información de

Con la determinación de prevenir las maniobras fraudulentas usadas por los delincuentes y fortalecer las acciones para su prevención, hemos dispuesto a los entes territoriales las principales recomendaciones de seguridad que deben tomar al momento de realizar alguna transacción financiera en cualquier canal de atención.

ASOBANCARIA te presenta:

Acciones por una cultura de prevención frente al fraude bancario en entidades territoriales

ASOBANCARIA

Construyendo
la **Confianza** y **Solidez** del sector financiero

Presentación

Esta cartilla es el producto de nuestro interés por salvaguardar la seguridad de las entidades territoriales que usan medios transaccionales para realizar cualquier operación que tiene riesgo de ser afectada por delincuentes, los cuales buscan lucrarse de forma ilegal.

Tener conciencia sobre las amenazas en cualquier tipo de escenario permitirá minimizar y/o contrarrestar posibles acciones fraudulentas que afecten no solo las finanzas de los usuarios sino su bienestar.

Recomendaciones generales

a. **Memoriza** la clave de tus tarjetas, nunca la escribas.

b. **No la reveles a nadie,** recuerda que tu clave es personal e intransferible.

c. **No permitas que durante alguna transacción** te observen al digitarla.

d. **Cámbiala periódicamente** si sospechas que ha sido revelada a una tercera persona.

e. **No asignes claves fáciles de descifrar** como fechas de nacimiento, números del documento de identidad o de teléfono.

f. **No informes a terceros** sobre las operaciones que vayas a realizar.

g. **No aceptes la ayuda de extraños** para realizar cualquier transacción.

h. **No entregues a desconocidos** información de tus tarjetas ni claves.

Recomendaciones al **realizar transacciones con cheques**

a. **No tener firmados cheques en blanco.**

b. **Guardar tu chequera** en un lugar seguro para evitar que sea falsificada.

c. **Destruye los cheques no válidos.** Si por equivocación pones un dato inexacto al diligenciarlo, asegúrate de destruirlo completamente y no arrojarlo sin más a la caneca de la basura.

d. **Revisa tu chequera periódicamente.** Verifica que no tengas saltos en la numeración consecutiva.

e. **En caso de pérdida o robo,** comunícate inmediatamente con tu entidad bancaria e informa de la situación; ellos te brindarán el apoyo necesario.

f. **Parametriza tus transacciones** de acuerdo a un horario, llevando el control de la información por la que generaste el cheque.

g. **Actualización de firmas y condiciones de pago**. Establece unos valores y personas autorizadas para confirmar los cheques que emitas.

¿Qué hacer al inicio de mi gestión?

a. **Cambiar** los usuarios y claves de la anterior administración.

b. **Notificar** las novedades a la entidad bancaria.

c. **Solicitar al banco** que ninguna transacción financiera se realice antes de las 6:00 a. m. y después de las 8:00 p. m.

¿Qué hacer durante mi gestión?

a. **Mantener los mecanismos** de comunicación con la(s) entidad(es) financiera(s) actualizados.

b. **Asegurar que las personas** que realizan transacciones con recursos de la entidades tengan capacitación en seguridad de la información. Conserva todos los comprobantes de compras y pagos realizados.

c. **Finaliza sesión** con la opción de salida segura que te ofrece cada entidad bancaria en su sitio web. Es un error desconectarse cerrando la página una vez hayas culminado la transacción.

d. **Mantén actualizado el software de seguridad** de tu equipo (antivirus, firewall, entre otros) para evitar posibles ataques informáticos.

e. **Asegúrate de la restricción de acceso** a los portales transaccionales de los usuarios durante sus períodos de vacaciones o licencias y darlos de baja en casos de traslado o retiros.

f. **Lleva un adecuado control de los usuarios y perfiles de tu equipo de cómputo.** Debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron.

g. **No utilice *links* sospechosos** que supuestamente lo llevan a la página de su banco.

h. **Nunca envíe información personal o de sus productos** a través de correos electrónicos, el banco nunca envía correos solicitando información.

i. **Al identificar un correo sospechoso,** remítalo a su entidad financiera.

j. **No realice descargas de programas** de música, videos, juegos u otros en el PC que realiza sus transacciones bancarias.

k. **Rechace todos los correos que solicitan información financiera** y datos personales, así mismo bloquee la dirección del correo de remitente como correo no deseado.