

**ABC** para evitar ser víctima  
de **fraudes bancarios**

Tenemos la determinación de frenar y prevenir las diferentes formas  
usadas para realizar fraudes en el momento que efectuamos una  
transacción financiera por cualquiera de nuestros canales  
habilitados. Por eso te presentamos:

**Acciones por una cultura anti fraude.**

¡AVANZAMOS CONTIGO,  
juntos lo hacemos posible!





# ¿Qué hacer al inicio ***de mi gestión?***

---

**a.**

Cambiar los **usuarios y contraseñas** 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 las 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 periodos de vacaciones o licencias y, darlos de baja en caso de traslado o retiros.



# ¿Qué hacer durante **mi gestión?**



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 las que asignaron.



No utilices links sospechosos que supuestamente te llevan a la página de su banco.



Nunca envíes información personal o de tus productos a través de correos electrónicos. El banco nunca envía correos solicitando información.



Al identificar un correo sospechoso, remítelo a tu entidad financiera.



No realices descargas de programas de música, videos, juegos u otros en el PC que realizas tus transacciones bancarias.



Rechaza todos los correos que soliciten información financiera.







# 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 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.





# Recomendaciones

## — **generales** —

- a.** Memoriza las claves de tus tarjetas. Nunca las escribas.
- b.** No reveles tus contraseñas a nadie, recuerda que, tus claves son personales e intransferibles.
- 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 al realizar cualquier transacción.
- h.** No entregues a desconocidos información de tus tarjetas.
- i.** Reclama siempre el comprobante de la operación efectuada.





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.



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



No descuides tu tarjeta cuando la utilices en establecimientos comerciales.



No accedas a enlaces enviados a través de mensajes SMS/MMS no solicitados y que impliquen la descarga de contenidos de 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.



No realices transacciones en computadores de acceso público (cafés internet, centros comerciales o bibliotecas) porque es posible que estos almacenen la información de tus tarjetas y contraseñas que pueden ser utilizados por manos criminales.



Evita también, utilizar redes Wi-Fi públicas porque tu información quedará almacenada en el historial de búsqueda.



Siempre ingresa a la página web de tu entidad financiera digitando la URL completa (**Ej. [www.bancommeva.com](http://www.bancommeva.com)**) en la barra de direcciones y nunca lo hagas a través de enlaces que encuentras en buscadores como Google, Mozilla o en correos electrónicos.



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://**







**¡JUNTOS**

fortalecemos el **PODER**  
para **CUIDARNOS**  
ante el fraude!



¡AVANZAMOS CONTIGO,  
juntos lo hacemos posible!

