

## Estimado cliente.

Nos es grato compartir las siguientes recomendaciones en materia de Ciberseguridad que entendemos pertinentes aplicar para que operes en forma segura en nuestros canales electrónicos. Estas iniciativas buscan minimizar el riesgo, protegiendo tu información personal en las transacciones financieras, ya sea las que realizás por Internet o personalmente en cajeros automáticos.

## Acceso seguro.

Evitá acceder a la banca electrónica en cibercafés, locutorios, bibliotecas u otros lugares públicos donde no existe certeza acerca de los mecanismos de ciberseguridad utilizados en el dispositivo (PC). De esta forma se previene el riesgo de fuga de información personal. Por eso te sugerimos que:

- Procures utilizar un dispositivo que cuente con la última versión de sistema operativo disponible y sus correspondientes actualizaciones. Verificá que tu navegador web esté actualizado y que cuando conectes tu equipo a Internet cuentes con un software antivirus que garantice su actualización automática.
- Ingreses manualmente y en cada oportunidad [www.bancomeridian.com.ar](http://www.bancomeridian.com.ar) para acceder a nuestros servicios financieros disponibles.
- No utilices accesos directos o enlaces recibidos por correo electrónico de remitentes desconocidos ya que podrían direccionarte a sitios falsos con la intención de obtener información personal y/o de tus cuentas bancarias.
- Evitá diligenciar formularios de encuestas o suscripciones que soliciten revelar información confidencial.

## Mantené tu contraseña a salvo.

Tu usuario y contraseña son tus credenciales para acceder a las diferentes plataformas y operar con tus cuentas; por esta razón deben ser únicas y estar muy bien protegidas.

Para ello recomendamos:

- Protegé tu contraseña, no la compartas ni la utilices para otros servicios.
- De ser posible, usá letras mayúsculas, minúsculas, números y caracteres especiales en sus credenciales de acceso ya que así serán difíciles de descifrar.
- Al generar tus contraseñas evitá utilizar información personal como nombres, fechas de nacimiento, números telefónicos, etc. Tampoco es recomendable el uso de secuencias ascendentes o descendentes de números o letras.
- Nunca anotes las contraseñas en documentos de libre acceso. Si resulta necesario hacerlo, utilizá un sistema codificado que solo vos puedas descifrar.
- Es conveniente que cambies tu contraseña periódicamente. Procedé a cambiarla de inmediato si sospechás que alguien puede conocerla.
- **NINGÚN EMPLEADO DE BANCO MERIDIAN TE SOLICITARÁ QUE REVELES INFORMACIÓN RELACIONADA CON TU USUARIO Y CONTRASEÑA.**



## **Token de seguridad (Link Token Empresas o Link Celular)**

El personal de Banco Meridian nunca solicitará que reveles información acerca de tu Token de seguridad. Adicionalmente recomendamos considerar la aplicación de las siguientes medidas preventivas en el dispositivo utilizado.

- Bloquea el equipo empleando medidas de seguridad que el dispositivo ofrezca (reconocimiento de patrones, clave PIN, huella dactilar, etc.).
- Elimina periódicamente los mensajes con información de tus cuentas.
- Nunca reveles por mensaje de texto información personal.
- Actualiza la información en caso de pérdida del dispositivo o cambio de número telefónico.
- Instala aplicaciones sólo desde los servicios oficiales para cada sistema operativo.
- Instala una solución antimalware y manténgala actualizada.
- Activa los servicios de Bluetooth y/o NFC solamente cuando sea necesario.

## **Consideraciones adicionales para operar en cajeros automáticos o con tarjeta de débito y/o crédito.**

- Procura utilizar cajeros automáticos ubicados en entidades bancarias con medidas de seguridad adecuadas.
- Asegurate que nadie observe cuando digitas tu PIN (contraseña) en un cajero automático.
- Recordá presionar "*Fin / Tecla Roja*" antes de retirarte de un cajero automático y guardá su tarjeta inmediatamente después de haberla usado. Si no pudiste completar una operación utilizá la tecla "cancelar".
- Observá los cajeros automáticos antes de operar. Verificá que nada obstruya la salida del dinero o que existan dispositivos extraños alrededor de la pantalla y/o teclado. Si notás elementos y/o personas extrañas cercanas al recinto, no lo utilices.
- No arrojes el ticket de tu transacción en el recinto del cajero automático.
- Jamás facilites tus tarjetas a desconocidos o permitas que otras personas las examinen con cualquier pretexto. Puede ocurrir que rápidamente sea reemplazada por otra similar.
- En caso de robo de tus tarjetas denunciar inmediatamente a la emisora de la misma.

**En Banco Meridian estamos comprometidos a mantener informados a nuestros clientes en materia de ciberseguridad, por esta razón recibirás periódicamente nuestras sugerencias.**