Recomendaciones de Seguridad

En tu computadora

- No ingreses a nuestro homebanking BIND24 desde búsquedas en Google o Redes Sociales, siempre recomendamos que escribas directamente en el navegador nuestra web oficial: www.bind.com.ar y ahí buscar la opción de Banca Electrónica.
- Comprobá que el sitio es seguro. Podés hacerlo validando que haya un “candadito” al lado de la dirección web o que la direccióm comience con ‘https’
- Cuando estés por ingresar a tu cuenta BIND24, verificá que la dirección en el navegador sea id.bind.com.ar o b24.bind.com.ar, que son nuestras direcciones oficiales.
- No respondas o completes pedidos de datos en ventanas emergentes.
- Deshabilitá la opción que dan los navegadores de guardar contraseñas o autocompletar información por vos.
- Protegé tu computadora con antivirus y mantené tu equipo al día con las actualizaciones de seguridad.
- Recordá siempre ingresar a nuestro sitio oficial: www.bind.com.ar
- No permitas que terceros vean tu operatoria en BIND24.
- Como buena práctica, cambiá tus claves con frecuencia y creá contraseñas seguras. No uses combinaciones fáciles como fechas de nacimiento, número de documento, etc.
- Cuando finalices tus operaciones asegurate siempre de cerrar la sesión de BIND24.

En Correos Electrónicos

- La mayoría de los emails que recibirás de nosotros son comunicaciones e información. Nunca te pediremos datos como claves, nombres de usuario, números de cuenta, contraseñas, ni que hagas clic a enlaces desconocidos.

- Siempre verificá que el destinatario seamos nosotros.
- Sí un mail te parece sospechoso o la cuenta de correo te genera duda, evitá abrir este mail y marcalo como spam.
- Si recibís mensajes ofreciendo premios, planes sociales o productos financieros que te pidan datos de manera urgente, no hagas caso, y denuncialo.
- Una buena práctica es revisar con frecuencia tus bandejas de entrada y salida y verificar que no haya actividad irregular.

En tu celular

- Si usás BIND24, recordá siempre descargar la aplicación oficial desde el App Store si usás Iphone o Google Play si tu celular es Android.
- No ingreses a nuestro homebanking BIND24 desde búsquedas en Google o Redes Sociales, siempre recomendamos que lo hagas desde nuestra aplicación oficial.
- Registrá tu dispositivo como seguro en BIND24 para reforzar la seguridad al momento de operar.
- Asegúrate de proteger tu pantalla si estás en lugar público o rodeado al momento de ingresar tus datos y hacer operaciones.
- Evitá usar redes Wi-Fi de acceso público para ingresar a BIND24.
- Recordá cerrar la sesión en la aplicación cuando termines tus operaciones.
- No guardes en tu celular información importante como claves, números de cuentas, contraseñas de emails o demás datos relevantes.
- Habilitá en tu celular la opción de bloqueo de pantalla con contraseña, patrones, reconocimiento de huellas, o el sistema de seguridad que tenga como opción.

Por teléfono

- El banco nunca te pedirá tus claves por vía telefónica. Asegurate de no darle esta información a nadie para evitar el Vishing, una práctica que consiste en engañar a personas por teléfono para obtener información sensible.

En Cajeros Automáticos

- Si recibís llamados que te indiquen ir a un cajero automático a hacer una operación, no hagas caso. No realices ninguna operación si un desconocido te guía o te lo pide por teléfono.
- No aceptes ayuda de extraños. Si necesitás, contactá al personal oficial del banco que podrá explicarte cómo hacer tu operación.
- Observá el cajero antes de usarlo. Si ves algo sospechoso o fuera de lugar, como partes sueltas, cinta adhesiva, mensajes de error en la pantalla u otro tipo de daño visible, evitá operar y denuncialo al personal del banco.
- No compartas tu clave numérica o alfabética con extraños. Es aconsejable además modificarla periódicamente.
- Recordá retirar la tarjeta al finalizar las operaciones.

En Redes Sociales

- Hacé tus consultas siempre por nuestras redes oficiales y usando las opciones de mensajes privados o directos. Te dejamos nuestras cuentas oficiales de Twitter y Facebook.
- No comentes de manera pública tus reclamos compariendo información personal como números de contacto, DNI, CUIL, emails, nombres de usuario, claves, números de reclamo o datos de tus cuentas.
- Recordá que tu información es tuya; nunca nadie te pedirá por alguno de nuestros canales tus claves, token de seguridad o información confidencial.

Claves seguras

- Elegí claves fáciles de recordar pero difíciles de suponer para tus cuentas.
- No uses información personal como tu nombre, apellido, documento, apodos o fechas importantes en tus claves.
- Evitá usar la misma clave que en otros servicios como tu casilla de email.

- Pensá en frases que signifiquen algo simple de recordar para vos y combinalas con números.
- No guardes tu nombre de usuario y clave en tu computadora ni las anotes. Memorizalas o utilizá las aplicaciones específicas para guardar contraseñas.
- Cambiá tu clave periódicamente.
- Nunca las divulgues a nadie bajo ninguna circunstancia. Ningún empleado del banco te la solicitará para acceder a tu cuenta.

¿Qué es el phishing?

- El phishing es una técnica de fraude informático que consiste en capturar tus datos mediante sitios webs o archivos que simulan ser de una entidad financiera reconocida.
- En general, el phishing se realiza a través de emails o páginas webs falsas que pueden contener el logo del banco y otros detalles que aparentan ser oficiales, además de un link a un sitio ficticio o un formulario adjunto en los cuales se solicita ingresar los datos de tu cuenta.
- Recordá que BIND Banco Industrial nunca te solicitará que reveles tus claves o información personal por email, por SMS o por teléfono. Desechá cualquier pedido de este tipo.
- Prestá especial atención al nombre de remitente desde el cual recibís el email.
- Verificá que la dirección en el navegador sea id.bind.com.ar o b24.bind.com.ar, que son nuestras direcciones oficiales del homebanking BIND24, o www.bind.com.ar, nuestra web oficial.