Consejos de Seguridad Básica de Aplicación General
Servicios Bancarios

Personales

- Las Tarjeta de Debito , Tokens y las correspondientes contraseñas son de USO PERSONAL. No los preste, a terceras personas y de esta forma evitará riesgos innecesarios.
- Nunca lleve consigo sus claves de acceso o contraseñas; memorícelas o manténgalas en un lugar seguro.
- Diseñe contraseñas difíciles de adivinar, utilizando combinaciones de letras mayúsculas, minúsculas, números y caracteres especiales. No utilice datos que resulten fáciles de adivinar por un tercero, como nombres de familiares, fechas de nacimiento, RFC, etc.
- Utilice claves diferentes para cada uno de los medios electrónicos que use.
- Nunca de "clic" en ligas de correos no solicitados, especialmente aquellos que le piden información personal. El simple hecho de dar clic, puede instalar programas espías que tienen por objetivo obtener las claves que haya tecleado para ingresar a la Banca Electrónica.
- Proteja en todo momento su información personal, los datos de sus cuentas bancarias y tarjetas, ya que las mismas son parte de sus bienes más importantes.
- Verifique constantemente los movimientos que presenten sus cuentas bancarias y tarjetas, e informe a su Ejecutivo de Cuenta cualquier tipo de transacción sospechosa.
- Si cambia de domicilio, notifíquelo de inmediato a su Ejecutivo de Cuenta, a fin de actualizarlo, para el envío de sus estados de cuenta.
- No facilite el número de sus tarjetas, fecha de expiración, código de seguridad o contraseñas en sitios de Internet NO Seguros, verificando que al introducir estos datos se encuentre el sitio en una conexión segura (https). Tampoco lo haga en el caso de recibir llamadas de origen extraña, ya sea de bancos, empresas de ventas de paquetes vacacionales, loterías, caridad u otros servicios de telemarketing. Esta información sólo podrá proporcionarla si usted está completamente seguro del origen de la llamada o del comercio de que se trate.
- Si recibe una llamada de CIBanco, el Operador deberá identificarse plenamente y no le solicitará
- Procure prever con anticipación cómo, cuándo y a través de qué medio realizara las operaciones que requiera hacer.
- Evite el descuido físico de dónde y bajo qué condiciones utiliza sus medios de pago.
- Verifique condiciones de seguridad, y que cuente con la información necesaria para realizar las operaciones que requiera hacer. Si tiene duda sobre algún aspecto, consúltela con su Ejecutivo de Cuenta de CIBanco.
- Analice y compare la información y diversas opciones que le ofrece la banca y elija entre éstas, aquellas que mejor satisfagan sus necesidades de funcionalidad y costo-beneficio. No dude en consultar a su Ejecutivo de Cuenta de CIBanco.
- Evite utilizar sus medios de pago en lugares de dudosa reputación o que no estén debidamente establecidos.
- Verifique y conserve sus comprobantes de operación (vouchers, estados de cuenta, folios de operación, etc.), a partir de su expedición usted tiene 90 días para presentar cualquier aclaración.

Para obtener mayor información, consulte las recomendaciones de seguridad de los siguientes medios:

Tarjeta de Debito
Cajeros Automáticos
Banca por Internet

Equipo de Cómputo

- Instale y asegúrese de mantener actualizado el siguiente software de marca reconocida:
  - **Anti-virus.** Detecta archivos y correos contaminados con virus, gusanos y troyanos.
  - **Firewall**. Ayuda a evitar que extraños entren a su equipo y depositen archivos o roben información del mismo.
  - **Anti-espía (antispyware)**. Estos programas detectan y evita la instalación de software de monitoreo de la actividad de la computadora.
- Habilite la contraseña de arranque en su computadora. Se recomienda el cambio de contraseña de manera periódica.

la información mencionada en el punto anterior, si lo hace, repórtelo a su Ejecutivo de Cuenta y no la proporcione.

- Verifique la legitimidad de toda solicitud, por cualquier medio, y en especial vía correo electrónico, de información personal, financiera o de sus cuentas bancarias y tarjetas. CIBanco nunca le solicitará que proporcione sus Claves de Acceso y contraseñas, a través de un correo electrónico. Sólo enviará correos personalizados para enviarle notificaciones de sus operaciones.
- Tenga cuidado con los links o archivos adjuntos en e-mails, recuerde que no es difícil crear un sitio web fraudulento o falsificar un correo electrónico.
- Al utilizar cajeros automáticos, cubra con su cuerpo la pantalla al momento de ingresar sus Claves de Acceso y no acepte ayuda de desconocidos.
- Mantenga actualizado su sistema operativo así como su navegador de Internet (Firefox, Internet Explorer, Safari, etc).
- Asegúrese que las direcciones de Internet desde donde instala programas, sean seguras y correctas.
- Registre las direcciones de los portales bancarios que utiliza en su lista de “favoritos” para sesiones futuras.
- Asegúrese que el técnico que le da mantenimiento a su equipo de cómputo sea de absoluta confianza.
- No se aparte de su computadora cuando se encuentre realizando operaciones bancarias por Internet.
- No realice operaciones bancarias en computadoras públicas (cafés Internet, salas VIP, hoteles, restaurantes, etc.).