recomendaciones de seguridad

A CONTINUACIÓN LE PRESENTAMOS ALGUNAS MEDIDAS QUE PUEDE LLEVAR A CABO PARA CONTAR CON UNA MAYOR SEGURIDAD, TANTO EN SUS TRANSACCIONES POR INTERNET, ASÍ COMO EN SU VIDA PERSONAL:

Seguridad Informática
Navegue seguro…

- Evite almacenar información financiera (usuarios, contraseñas, NIP, estados de cuenta, etc.) en su computadora personal. Le sugerimos deshabilitar la opción de Autocompletar de su explorador (Herramientas / Opciones de internet / Contenido / Autocompletar), quitar la marca de las opciones Formularios, Nombres de Usuarios y Contraseñas de Usuarios.

- Mantenga actualizado el software de seguridad (use al menos antivirus, firewall, antispyware) en su computadora.

- La contraseña de acceso a su computadora y demás sistemas (correo electrónico, bancos, afores, sitios para trámites de gobierno, comercios por Internet, etc.) debe ser segura. Por lo tanto, no debe conformar sus claves con fechas de cumpleaños, aniversarios, registro federal de causante, CURP o cualquier otra que sea fácil de obtener.

- No debe repetir contraseñas recientemente utilizadas. Cambie su contraseña de forma periódica, máximo cada 90 días, o antes, si presume que ha perdido la confidencialidad. Procure tener diferentes contraseñas para cada servicio.

- Evite navegar por sitios de Internet inseguros. Estos sitios normalmente descargan software malicioso en las computadoras que se conectan a ellos.

- Evite que personas desconocidas conecten memorias USB u otro equipo móvil a su computadora o laptop, ya que pueden no tener protección antivirus y contaminar con virus su sistema, dañar o robar información personal.

- No instale o utilice software “pirata” en su computadora.

- Al descargar archivos adjuntos de correo electrónico, verifique siempre que no estén contaminados con virus.

- No descargue archivos de Internet o los archivos adjuntos de correo electrónico, en especial cuando el remitente es desconocido o el contenido le resulte sospechoso.

- Mantenga un respaldo de información sensible disponible en buenas condiciones.

Banca Segura por Internet
Además de las buenas prácticas para navegar seguro en Internet, le sugerimos…

- Evite realizar transacciones bancarias, financieras, compras por Internet en sitios públicos.

- Evite acceder al sitio de servicios bancarios por Internet de su banco a través de hipervínculos. Teclee directamente la dirección de Internet de su banco en la barra de direcciones.

- Nunca de clic o responda a una ventana emergente (pop-up) o correo sospechoso, porque puede conducirlo a una imitación de página web de su banco y solicitarle información personal, financiera o datos de sus contraseñas.

- Una vez que esté dentro de una sesión realizando operaciones o consultas en su portal de banca por Internet, no se retire de su equipo hasta que haya terminado. Se recomienda bloquear su sesión con contraseña.

- En caso de ser necesario acceder a su portal de banca por Internet usando equipos en cafés Internet o centros de negocio, asegúrese de borrar todos los archivos temporales de Internet y apague la computadora al terminar.

- Acceda periódicamente a su usuario de servicios bancarios por Internet de su banco y revise las cuentas que tiene registradas para hacer traspasos a cuentas de terceros del mismo banco e interbancarias. Asegúrese que no existan cuentas que usted no ha dado de alta.

- Consulte regularmente el saldo de sus cuentas, en caso de que existan diferencias, repórtelo de manera inmediata a su banco.

- Si cuenta con token (generador de claves dinámicas) para el acceso a servicios bancarios por Internet, guárdelo de manera segura, no lo deje a la vista de otras personas, no lo comparta con nadie, si se le extravía repórtelo

2022 **Bansí** Todos los Derechos Reservados

inmediatamente a su institución financiera, llévelo con usted únicamente cuando sea necesario, por ningún motivo escriba su contraseña en él.

• Bansí en ningún momento le solicitará información personal o confidencial por correo electrónico o vía telefónica. En caso de que usted reciba algún correo de este tipo, no envíe información y por favor reporte este evento a su ejecutivo de cuenta.

• Si recibe un correo electrónico supuestamente de su banco solicitándole que se ponga en contacto a un determinado teléfono, no lo haga, puede ser que sea falso. Utilice el número de teléfono habitual que tenga de su Banco y pregunte si son ellos los que le han enviado el correo.

OTRAS RECOMENDACIONES DE SEGURIDAD

Medidas de seguridad en Cheques
Cuide su chequera…

• Al recibir su chequera, revise que esté debidamente empacada.

• Cuente el número de cheques que recibe y verifique que el folio sea consecutivo, asegurándose que no falte ninguno.

• Si no es estrictamente necesario, no autorice a terceras personas para que recojan sus talonarios.

• Verifique que los cheques recibidos no tengan tachaduras o alteraciones en algunos de sus datos.

• En caso de alguna anomalía en su chequera, no la reciba y notifíquelo de inmediato al gerente de su sucursal.

• Utilice bolígrafo para llenar sus cheques.

• Evite expedir cheques al portador.

• De preferencia, trate de expedir cheques nominativos y con la leyenda “Para abono en cuenta” o coloque dos líneas transversales paralelas.

• Proteja con una línea el principio y el final de los datos del importe con letra, así como del beneficiario.

• Asegúrese de que coincidan el importe con número y con letra.

• Cuente regularmente sus cheques para asegurarse de que no le falte alguno.

• Reporte de inmediato cualquier robo o extravío de sus cheques, ya sean en blanco o llenados.

• Concilie oportunamente los movimientos que aparecen en su estado de cuenta.

• Si cuenta con el servicio en su Banco, active sólo los cheques que vaya a utilizar.

Medidas de seguridad en tarjetas de débito y crédito
Tenga cuidado con sus tarjetas…

• Al recibir su tarjeta, asegúrese que el sobre no haya sido abierto y firme de inmediato su tarjeta con bolígrafo de tinta negra.

• Lleve consigo sólo su identificación y las tarjetas de crédito o débito que va a utilizar.

• No preste su tarjeta, ni permita que otras personas la usen en su nombre.

• Guarde sus comprobantes de operación por lo menos hasta que reciba sus estados de cuenta, podría requerir alguna aclaración, una vez que haya verificado sus consumos destruya sus comprobantes.

• Evite dejar su tarjeta o documentación personal con firmas en el automóvil, especialmente en los vallet parking.

• Evite perder de vista su tarjeta al realizar pagos en comercios. Procure que la transacción se realice siempre en su presencia y cuando se la regresen asegúrese de que sea su tarjeta.

2022 **Bansí** Todos los Derechos Reservados

recomendaciones de seguridad

- Eventualmente podrá recibir llamadas de su banco para verificar si se realizó transacciones diferentes a su patrón de comportamiento, no proporcione información personal y confidencial de sus tarjetas.

- Consulte su buró de crédito por lo menos una vez al año y verifique que no existan créditos no solicitados a fin de descartar que haya sido víctima de un robo de identidad. Recuerde que tiene derecho a una consulta gratuita por año.

- Si su estado de cuenta llegó tarde o simplemente no llegó, llame al Banco para informar la situación y asegure que su dirección sea la correcta.

- Si cambia de domicilio, teléfono o tiene algún problema con la recepción de su correspondencia, llame para actualizar y/o validar que sus datos estén correctos.

- Por su seguridad, cancele las cuentas que no utilice. En algunos bancos, incluso podrá solicitar una reducción de su línea de crédito y restablecerla en el momento que lo requiera de manera inmediata.

- Si su tarjeta venció, se deterioró o la canceló, destrúyala raspando la firma y cortando el plástico en fragmentos.

- En caso de robo o extravío de su tarjeta, repórtela de inmediato a su Banco.

- Llame a su Banco si no recibe la tarjeta de crédito que esperaba vía correo.

Medidas de seguridad en Cajeros Automáticos (ATM)
Manténgase alerta en los cajeros automáticos…

- Proteja y resguarde sus claves confidenciales (NIP)

- El NIP es exclusivo para operaciones en cajeros automáticos, o disposiciones en ventanilla en algunos bancos, no lo proporcione a ninguna persona.

- Al asignar su NIP, evite números fácilmente identificables, no lo anote en ningún sitio y por lo menos cámbielo 1 vez cada 3 meses.

- Antes de introducir su tarjeta en el cajero automático, verifique que éste NO tenga aditamentos extraños en el dispositivo de acceso al cubículo o en el dispensador de efectivo.

- Recuerde seguir únicamente las instrucciones que aparecen en pantalla.

- Al teclear su número confidencial, cubra el teclado con una mano para evitar ser visto por alguien más.

- No acepte asesoría de personas extrañas y asegúrese de no dejar su sesión abierta antes de retirarse del cajero.

- Guarde su tarjeta y dinero antes de salir del cajero automático

- No deje dentro del cajero automático los comprobantes de sus operaciones sin antes romperlos.

- Utilice cajeros automáticos que estén bien iluminados y preferentemente con vigilancia.

- Cuando el cajero no le devuelva su tarjeta, cancele su operación y repórtela de inmediato en la sucursal o vía telefónica al Centro de Atención a Clientes de su Banco.

2022 **Bansí** Todos los Derechos Reservados