POLÍTICAS DE SEGURIDAD Y RECOMENDACIONES

Contenido

Políticas de Privacidad y Seguridad

Caja de Ahorros, siempre pensando en la seguridad de sus clientes, ha implementado políticas de seguridad y de privacidad para proteger la información y datos de nuestros clientes. De igual forma tenemos a su disposición recomendaciones para evitar el fraude electrónico. Por favor lea las siguientes políticas y recomendaciones que estamos seguros serán de su beneficio.

Modificación a las Políticas de Privacidad y Políticas de Seguridad

Caja de Ahorros se reserva el derecho de realizar cambios, modificaciones o actualizaciones en las Políticas de Seguridad a su entera discreción.

Se considera que, al consultar cualquiera delas secciones del sitio de http://www.cajadeahorros.com.pa/ de la Caja de Ahorros en Internet, se aceptan los términos y condiciones expuestos en este documento. Todos los productos y servicios prestados por la Caja de Ahorros se encuentran sometidos a la legislación vigente y bajo la supervisión de la Superintendencia de Bancos de Panamá.

A. Recomendaciones para la definición y manejo seguro del número de identificación personal (PIN), contraseña o clave personal.

Generalmente los distintos productos de tarjetas (crédito, débito o prepago) así como los cajeros automáticos, puntos de venta y hasta sitios en internet, requieren que el cliente valide su identidad con la inclusión de datos que solamente el cliente conoce.

Estos productos generalmente vienen acompañado de un identificador único llámese PIN o clave personal o contraseña.

Algunos productos permiten que el usuario pueda definir un PIN, clave o contraseña de su conveniencia, sin embargo, es necesario considerar ciertos atributos que le garanticen seguridad a usted. A continuación le ofrecemos algunas recomendaciones que pueden serle útil para este propósito:

1. Verifique cuales son los requisitos para definir un PIN del producto o servicio (longitud, características de letras, números, combinaciones, restricciones). Generalmente esta información se obtiene cuando le entregan su tarjeta o cuando accede inicialmente a servicios vía internet, banca telefónica, etc.
2. La contraseña de usuario debe contener entre 6 a 10 caracteres máximo, según sea requerido por el producto o servicio. Debe ser una combinación de letras y números, y es sensible a letras y números. Los caracteres válidos son: Letras a-z (minúsculas) A-Z(mayúsculas) Números 0-9 Excepto la letra Ñ, ñ.
3. Escoja un PIN que usted pueda recordar fácilmente, pero que sea difícil de adivinar por otros.
4. No utilice nombres de personas, nombres de mascotas, ni fechas memorables, número de documento, número de teléfono, número de direcciones, números secuenciales el número de cliente, o datos que puedan ser obtenidos de su cartera, para definir su número de PIN.
5. El PIN es un elemento personal, no lo comparta, no lo escriba, memorícelo. Solamente usted debe conocer su PIN. No comunique su PIN o contraseña a nadie por ningún medio, escrito, electrónico, o telefónico, etc.
6. No almacene su PIN en forma escrita, mucho menos junto a su tarjeta de crédito o débito, o junto a su número de cliente; estos elementos en conjunto son los que generalmente le permiten acceder a los servicios bancarios.
7. No utilice el mismo PIN que ha definido en otras instituciones financieras o en otros sitios en internet, o que haya definido para tarjetas u otros servicios, o para uso en correos electrónicos.
8. Nadie está autorizado para solicitarle su número de PIN. Este número es personal, solamente usted debe saberlo.
9. Su identificación de usuario y número de PIN o contraseña son de uso estrictamente personal, y confidenciales, solo deben ser conocidos por usted, y para uso de acceso a los servicios contratados.

10. Cambie su PIN frecuentemente, se recomienda hacerlo por lo menos cada 30 días. No reutilice un número de PIN utilizado recientemente.
11. El sistema le solicitará cambio de contraseña a los clientes naturales y jurídicos cada 999 días lo que representa dos (2) años y nueve (9) meses.

B. Tarjeta de Débito, Crédito y Prepago

1. Prácticas Seguras para Tarjetas de Crédito, Débito o Prepago

1. Firme su tarjeta en la parte posterior (banda en blanco), inmediatamente le sea entregada en el Banco.
2. Memorice su número secreto o PIN, no lo escriba o almacene junto a tu tarjeta. Si por algún motivo lo ha olvidado, comuníquese inmediatamente al 800-CAJA(2252).
3. Afíliese al seguro contra fraude que le ofrece el Banco.
4. Su tarjeta es de uso personal, nunca la preste.
5. Al usar su tarjeta, procure no perder de vista la misma. Si es necesario, siga al dependiente del comercio hasta donde se encuentra el dispositivo de punto de venta (POS). Si notas alguna irregularidad, presenta tu inquietud al superior encargado en el comercio o contacta al Banco.
6. Si se encuentra en un restaurante, pregunte si tienen POS (Puntos de venta) inalámbricos, y exija que se lo traigan para que usted inserte su plástico en el mismo.
7. Vigile que su tarjeta sea utilizada solamente en la terminal Punto de Venta y que la misma siempre esté visible para usted.
8. Cubra el teclado con su mano cuando digita su número secreto o PIN, ya sea en un cajero automático o en un punto de venta. LA SEGURIDAD ESTÁ EN SUS MANOS.
9. La Tarjeta será bloqueada después de tres (3) intentos fallidos al ingresar el PIN (número secreto).
10. Conserve los comprobantes de las transacciones realizadas con su Tarjeta y compárelos con el estado de cuenta mensual o el movimiento de su cuenta. Reporte cualquier discrepancia.
11. Guarde su tarjeta y efectivo cuidadosamente antes de retirarse del cajero automático o punto de venta.
12. Utilice los servicios de banca en línea o banca telefónica frecuentemente para revisar los movimientos de su cuenta.
13. No coloque su tarjeta cerca de imanes o campos magnéticos, ya que los mismos, borran la información grabada en la banda magnética.
14. No exponga su tarjeta a altas temperaturas (frío o calor), no la exponga al agua ni la frote con cuero (el roce prolongado con el cuero hace que se pierda la información magnética).
15. No doble su tarjeta.
16. Cuide sus tarjetas como si fuera efectivo. No la descuide en ningún momento.
17. Las tarjetas de marca VISA, MasterCard u otras pueden contener un número de seguridad en la

parte posterior el cual debe utilizar solamente para compras vía internet. No suministre esta información en ningún otro caso.

18. Utilice una cuenta bancaria que sea exclusiva para sus transacciones con la tarjeta de débito en ATM y Puntos de Venta.
19. Utilice los servicios de notificación o alertas sobre sus cuentas y/o tarjetas, lo cual le ayudará a conocer cualquier movimiento que se realice sobre las mismas y prevenir el fraude.

2. Obligaciones del Tarjetahabiente

Según la Ley Nº 81 de 31 de diciembre de 2009, *'QUE TUTELA LOS DERECHOS DE LOS USUARIOS DE LAS TARJETAS DE CRÉDITO Y OTRAS TARJETAS DE FINANCIAMIENTO'*, hacemos de su conocimiento el Artículo 15. **Obligaciones del tarjetahabiente.**

El tarjetahabiente tendrá las siguientes obligaciones frente al emisor de la tarjeta de crédito y otras tarjetas de financiamiento:

1. Resguardar la tarjeta con la debida diligencia.
2. Realizar puntualmente los pagos por la utilización de su tarjeta con la debida diligencia.
3. Identificarse y usar en forma personal su tarjeta y no mostrar ni confiar a nadie las claves de acceso a los cajeros y otros sistemas electrónicos.
4. Verificar el importe y la veracidad de la información antes de firmar los comprobantes de pago.
5. Solicitar y guardar los comprobantes de pago y demás documentos de compra de bienes y utilización de servicios hasta recibir el estado de cuenta y estar conforme con este.
6. Velar por el correcto uso de las tarjetas adicionales que solicite o autorice.
7. Procurar el mantenimiento y la conservación del límite de crédito concedido por el banco o empresa financiera.
8. Indicar al banco o empresa financiera el domicilio o correo asignado a la tarjeta, a efectos de que este le remita los estados de cuenta o cualquier otra información pertinente.
9. Informar al banco o intermediario financiero cuando no reciba el estado de cuenta en el plazo que este haya establecido.
10. Verificar las tasas de interés y otros cargos que le aplique el emisor, así como los procedimientos para hacer a tiempo sus reclamos sobre los productos y servicios que adquiera por medio de la tarjeta.
11. Efectuar los reclamos en el plazo establecido en el contrato.
12. Informar de manera inmediata al banco o intermediario financiero del robo, hurto o pérdida de la tarjeta.

3. Reporte de inconvenientes con su Tarjeta

En los casos que su tarjeta se atasque o presente inconvenientes durante una transacción en el Cajero Automático, repórtelo inmediatamente al Banco. No acepte la ayuda de extraños o terceras personas.

En caso de cualquier inconveniente, robo o extravío de Tarjeta de Crédito o Débito, en horario laboral comuníquese al 800-CAJA(2252) o acérquese a cualquier sucursal.

Si el inconveniente, robo o extravío de Tarjeta Débito se presenta en horario no laborable, fin de semana o feriado, deberá comunicarse a los teléfonos 508-1971.

Si el inconveniente, robo o extravío de Tarjetas de Crédito VISA / Mastercard se presenta en horario no laborable, fin de semana o feriado, deberá comunicarse a los teléfonos 800- CAJA(2252) opción 1.

C. ATM, Puntos de Ventas y Compras en Internet (Comercio Electrónico)

1. Seguridad en el Cajero Automático

Al utilizar cualquier Cajero Automático, recuerde practicar los siguientes consejos de seguridad:

1. Antes de utilizar un Cajero Automático (ATM), haga una inspección visual del mismo y asegúrese de que no mantenga alteraciones físicas ni objetos extraños (clips o cinta adhesiva) en la ranura de la inserción, ni en el despachador de efectivo. Si nota alguna anomalía, no lo utilice y repórtelo al Banco.
2. Si va a utilizar un Cajero Automático ubicado en un área externa, estaciónese tan cerca como pueda en un lugar bien iluminado y accesible.
3. Si utiliza un Cajero Automático, ubicado en un cubículo con puerta de seguridad, cerciórese de cerrar bien la puerta antes de iniciar la transacción.
4. Use Cajeros Automáticos que estén ubicados en áreas con buena iluminación. No utilice cajeros automáticos ubicados en lugares solitarios.
5. Si ya inició la transacción y nota que algo sospechoso sucede, cancele la transacción y abandone el área a la brevedad posible.
6. Fíjese si en la pantalla del Cajero Automático hay algún mensaje con alguna instrucción inusual.
7. Si considera que el Cajero Automático que va a utilizar no está funcionando adecuadamente, oprima la tecla “Cancelar”, retire su tarjeta y diríjase a otro Cajero Automático.
8. Si el cajero automático está fuera de servicio, no introduzca su tarjeta, ni el número secreto o PIN.
9. No permita que nadie lo observe cuando está digitando su número secreto. Cubra el teclado con la otra mano al digitar su número secreto o PIN.
10. Ingrese su número de PIN, solamente cuando la pantalla del cajero lo indique.
11. Asegúrese que retira su tarjeta después de realizar la transacción en un cajero automático o en algún comercio.
12. Guarde su tarjeta y efectivo cuidadosamente antes de retirarse del cajero automático.
13. No permita que extraños se introduzcan en el cubículo del cajero automático mientras usted realiza su transacción, ni acepte ayuda de personas con teléfonos celulares al realizar

transacciones en los cajeros automáticos.

14. Procure entrar solo(a) al cajero automático para realizar sus transacciones. Esta operación es privada y sólo usted debe conocer los pormenores de la misma.
15. Conserve los recibos que le entrega el cajero para llevar su propio control de la cuenta.
16. No deje los recibos de sus transacciones en el cubículo donde está el cajero automático. El recibo contiene información que no debe quedar expuesta.

2. Seguridad en los Puntos de Venta (POS)

Los puntos de venta deben estar ubicados al lado de la caja del comercio y al alcance de usted como cliente, para que pueda realizarse la transacción y usted pueda digitar su PIN en los casos en que este es requerido. En algunas ocasiones, el comercio puede contar en la caja con un PINPAD que es un dispositivo en el cual usted puede digitar su PIN.

Observe las siguientes recomendaciones de seguridad cuando utilice Puntos de Venta:

1. Al usar su tarjeta, procure no perder de vista la misma. Si es necesario, siga al dependiente del comercio hasta donde se encuentra el dispositivo de punto de venta (POS). Si notas alguna irregularidad, presenta tu inquietud al superior encargado en el comercio o contacta al Banco.
2. Ingrese su número de PIN, solamente cuando la pantalla del punto de venta lo indique.
3. No permita que nadie lo observe cuando está digitando su número secreto. Cubra el teclado con la otra mano al digitar su número secreto o PIN.
4. No acepte ayuda de terceras personas.
5. Revise su tarjeta después de hacer el pago en un punto de venta a fin de verificar que sea la suya.
6. Solicite siempre el comprobante de compra que emite el punto de venta.
7. Si usted sospecha que ha ocurrido alguna situación inusual con su tarjeta contacte al Call Center al 800-CAJA(2252), al Departamento de Seguridad (24 horas) al 508 – 1971 o al Departamento de Riesgo y Fraude al 508-1075 o 508-1040
8. Algunas compras en punto de venta por montos bajos o con verificación con PIN ya no requieren que firme un voucher de compra.
9. En caso que autorice alguna transacción recurrente (ej: domiciliación de pago de servicio o donaciones), asegúrese de no detallar el número del CVV2 (VISA) o CVC2 (Mastercard) de su tarjeta en el formulario donde suscribe la autorización.

3. Seguridad para Compras con Tarjetas en Internet (Comercio Electrónico)

1. Verifique que el sitio web donde realiza sus compras es seguro; debe contener la información de la entidad certificadora y su URL debe iniciar con https://
2. Debe estar protegido por algún certificado digital como: Verisign o Tawte;
3. Verifique que el sitio web donde realiza sus compras contenga Políticas de Devolución, Políticas de Envío, Políticas de Privacidad y Políticas de Seguridad.
4. Tome en cuenta que usted debe registrar la información para procesar su compra en la misma forma como está descrita en su tarjeta (nombre, fecha de expiración, número

de tarjeta, CVV2 (VISA) o CVC2 (Mastercard), dirección, etc.)

5. Asegúrese que el sitio donde realiza la compra pueda enviarle por correo electrónico una constancia de la compra realizada o bien pueda desplegar una factura de compra que usted pueda imprimir como constancia. En tales casos debe aparecer el nombre de la empresa a la cual usted hace la compra respectiva.
6. Anote o guarde constancia de la compra realizada, para futuras referencias o casos de reclamos.
7. Lea su contrato de tarjeta de Débito, Crédito o Prepago, en relación al manejo de las compras vía Internet.

D. Caja Amiga

1. Asegúrese que el comercio en donde realizará su transacción está debidamente autorizado por la Caja de Ahorros para ofrecer el servicio. Todo comercio autorizado, estará debidamente identificado con el logo de Caja Amiga de Caja de Ahorros. Usted también puede verificar si el comercio está afiliado a Caja de Ahorros, llamando al 800-CAJA(2252) o consultando el buscador de Comercios afiliados que se encuentra en el sitio web de Caja de Ahorros https://www.cajadeahorros.com.pa/buscador-de-caja-amiga/
2. Al realizar una transacción en cualquier Caja Amiga, lleve su cédula de identidad personal, el número de cuenta si lo requiere o la factura si va a efectuar un pago de servicio público; el agente de Caja Amiga le solicitará esta información para procesar su transacción.
3. No pierda de vista su cédula de identidad personal cuando esté realizando una transacción; asegúrese que el comerciante no pase su cédula por un dispositivo distinto al equipo que mantiene la aplicación (APP) Caja Amiga.
4. Entregue su dinero únicamente a la persona autorizada para atender la Caja Amiga y realice la transacción solamente en la caja identificada con el logo de Caja Amiga.
5. Una vez se haya registrado la información el agente de Caja Amiga le solicitará que digite su Token de seguridad o contraseña, el cual será enviado por Correo Electrónico o por Mensaje SMS. Para confirmar la transacción: Digite personalmente su Token en la aplicación (APP) Caja Amiga.
6. Cuando digite su token en la aplicación (APP) Caja Amiga procure cubrir el teclado, tápelo con la mano al colocar los datos.
7. Conservar la distancia. Procure que las otras personas en la tienda se encuentren distantes y asegúrese de que no te estén vigilando cuando ingrese el token.
8. Por cada transacción que necesite realizar por Caja Amiga, recibirá su Token de seguridad o contraseña, como se describe en el punto 5.
9. Al hacer un depósito, cuente el dinero antes de entregarlo al encargado de atender la Caja Amiga.
10. Al hacer retiros, verifique el efectivo recibido antes de retirarse de la Caja Amiga.
11. Exija su comprobante de la transacción después de realizar cualquier operación y guárdelo como constancia de su transacción.
12. Revise su comprobante antes de salir, asegúrese de que la operación se hizo a la cuenta o proveedor de servicio indicado y verifique que el monto corresponda con el indicado.
13. Utilice los servicios de banca en línea o APP móvil frecuentemente para revisar los movimientos de su

cuenta.

14. No acepte ayuda de extraños al realizar sus transacciones.
15. El establecimiento no debe fraccionar el monto de sus pagos, debe hacerle una sola transacción por cada tipo que efectúe. Si esto ocurriera, por favor repórtelo al 800-CAJA (2252) o por nuestro asistente virtual A.N.D.R.E.A. al WhatsApp 6949-0076.
16. El establecimiento NO puede obligarle a realizar compras en el comercio, como condición por realizar alguna transacción o pago de servicio. Cualquier contrariedad al respecto, repórtelo al 800-CAJA (2252).
17. El comercio Caja Amiga no está autorizado a cobrar comisión en efectivo por transacción o pago de servicio realizado.
18. El agente de Caja Amiga no está autorizado para prestar servicios financieros por cuenta propia y respecto de estos, Caja de Ahorros, no asume ninguna responsabilidad.

F. ACH – Servicio de Transferencias Electrónicas

1. Para utilizar el servicio de débito directo vía ACH, debe completar el formulario de autorización de débito ACH y suscriba su firma en forma similar a como está en su cédula de identidad personal.
2. Defina claramente si el débito autorizado es para una o varias transacciones, la frecuencia de las mismas, si es por monto variable o por monto fijo, la vigencia y expiración de la autorización de débito.
3. Guarde una copia de la autorización de débito.
4. Verifique periódicamente el movimiento de su cuenta para asegurarse que le han aplicado la transacción de débito ACH de acuerdo a la autorización realizada por usted.
5. Utilice los servicios de banca en línea o banca telefónica frecuentemente para revisar los movimientos de su cuenta.

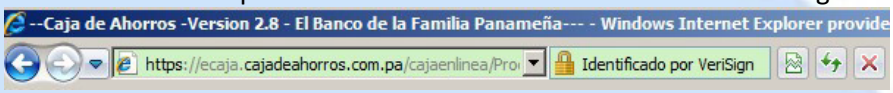
G. Caja en Línea

1. Política de Seguridad para Caja en Línea y Banca Móvil

- **Caja en Línea – Banca por Internet**: El servicio de Caja en Línea es suministrado a clientes naturales y jurídicos a Través de internet, en el sitio que corresponda a uno o más dominios del banco, mediante protocolos HTTP (Hypertext Transfer Protocol), HTTPS (Hypertext Transfer Protocol Secure), o protocolos con propósitos equivalentes, indistinto del dispositivo tecnológico de acceso.
- **Banca Móvil**: Es el servicio de Banca Móvil provisto a los clientes a través de un Equipo Móvil.

Caja de Ahorros, comprometida en proteger la privacidad y la integridad de la información personal y financiera de sus clientes ha establecido medidas de seguridad para permitir a sus clientes realizar sus transacciones desde su computadora o Banca Móvil de manera segura.

Estas medidas de seguridad contemplan la interacción que usted tiene con nosotros desde que ingresa su contraseña, hasta el momento que termina su sesión.

1. Desde el momento que accede a la página del sitio privado de Caja de Ahorros, usted se encuentra en una sesión segura. Esto lo puede confirmar verificando que en la dirección que aparece en la barra del navegador se describe de la siguiente manera: https://ecaja.cajadeahorros.com.pa/
2. Utilizamos certificado digital expedido por Verisign, Inc., compañía de certificación de sitios de Internet a nivel mundial. Usted puede verificar la vigencia y veracidad de nuestro certificado digital haciendo clic sobre el sello de Verisign que encontrará en el sitio de Banca en Línea.
3. Al entrar a Banca en Línea podrá notar en la parte inferior o superior de su pantalla (dependiendo de la versión de explorador que tenga) un candado, que al estar cerrado comprueba que está ingresando al sitio de Banca en Línea de Caja de Ahorros (puede hacer "clic" sobre el candado y se desplegará información del certificado).
    a. En las versiones de Internet Explorer 7 o mayores, verá un candado en la barra superior o también la barra pintada de verde claro como se muestra en la siguiente imagen: 

    b. En las versiones de los siguientes navegadores, verán un candado en la esquina inferior derecha:
        i. Navegador Internet Explorer inferior a 7: 
        ii. Navegador Nestcape: 
        iii. Navegador Mozilla Firefox: 

    Estos símbolos indican que el sitio posee el certificado de seguridad emitido por una autoridad certificante y está protegido por el sistema SSL.
4. Informamos y recomendamos el uso de navegadores verificados por Caja de Ahorros que garanticen el cumplimiento de estándares de seguridad:
    a. Internet Explorer
    b. Google Chrome
    c. Mozzila Firefox
    d. Safari
5. Mantenemos controles de encriptación en los datos para brindar la seguridad de la información que se maneja en la banca en línea y a nivel de la Banca Móvil.
6. Contamos con sistemas de protección como firewalls y anti malwares que permiten minimizar los riesgos relacionados con el software malintencionado.
7. Si se intenta acceder repetidamente con una palabra clave incorrecta, el sistema bloqueará su acceso. Para solicitar la activación de la misma deberá comunicarse al Call Center 800-CAJA(2252) en horario laborable.
8. Si el usuario por alguna razón necesita el cambio de contraseña lo podrá hacer ingresando en Caja en Línea en su sesión privada en la opción disponible para este efecto.
9. Si el usuario ha olvidado su contraseña:
    a. Debe solicitarse el cambio de contraseña por olvido en la sucursal más cercana, para que este le entregue una nueva contraseña en sobre de seguridad.

b. Ingresar en Caja en Línea y recuperar la contraseña en la opción disponible.
c. En ambos casos el sistema le solicitará la modificación de la contraseña de ingreso a Caja en Línea.

10. Si usted ha ingresado con su usuario y no ha cerrado la sesión o no la ha cerrado correctamente el sistema no le permitirá ingresar, indicándole que ya tienen una sesión activa. Debe verificar si ha ingresado en alguna otra estación y cerrar la sesión correctamente de lo contrario llamar a 800-CAJA(2252) para pedir apoyo u orientación al respecto.
11. A los usuarios que no ingresen al sistema por un lapso de 6 meses, se les inactivará su clave de acceso. Si el cliente desea activar su cuenta debe acercarse a la sucursal más cercana para que ésta le sea activada.
12. En cumplimiento con el Acuerdo 6-2011 emitido por la Superintendencia de Bancos de Panamá, la Caja de Ahorros implementa nuevos elementos de Seguridad para las operaciones realizadas a través de la Banca en Línea y Banca Móvil.
13. Usted puede elegir entre el uso de dispositivos físicos conocidos como "Tarjeta Electrónica" o una aplicación digital portable conocida como "Llave Móvil".
14. En cada una de nuestras sucursales se le atenderá personalmente sobre los detalles y uso de estos novedosos dispositivos.
15. El BANCO se reserva el derecho de bloquear el acceso a los usuarios que se pueda comprobar, que han proporcionado datos falsos o por cualquier otra razón de seguridad.
16. La Banca Móvil estará soportada en las siguientes versiones de dispositivos y/o sistemas operativos: iOS 6, iOS 7, iOS 8, iOS9, iOS10 y Android 2.3 o 4.x o 5 o 6. Si bien se contemplarán aquellos dispositivos con pantallas mayores a 3.5 pulgadas, las prestaciones, navegabilidad, performance e incluso factibilidad de funcionamiento estará limitada por las prestaciones de hardware de los dispositivos. Se deberán considerar prestaciones (en términos de capacidad de procesamiento, memoria y resolución) similares o superiores.
17. Evite proporcionar su información confidencial como números de cuenta, usuarios, contraseñas, entre otros, por medio de correo electrónico o formularios web.
18. Evite dejar su computadora descuidada y la sesión abierta si ha ingresado a Banca en Línea, sobre todo en lugares públicos u oficina. Siempre finalice su sesión por medio de la opción "Salir", nunca cerrando la ventana del explorador.
19. Es recomendable eliminar los archivos temporales de Internet (Cookies) siempre que salga de Banca en Línea. Recuerde que el navegador de Internet está configurado para guardar las páginas que usted visita, poniendo en riesgo su información. Revise la sección ayuda de su navegador de internet, para conocer el proceso de eliminación.
20. Revise periódicamente su estado de cuenta y asegúrese que no existan transacciones sospechosas.
21. Memoriza las claves, no las escribas ni guardes en tu celular.
22. No permitas que terceros conozcan o vean tus claves al digitarlas en el teléfono.
23. No utilices teléfonos celulares ni computadores de terceros para realizar sus transacciones.
24. Ignora los mensajes que lleguen a tu celular o correo electrónico, en los que te soliciten datos financieros o pidan descargar aplicaciones.
25. No guarde información de su Cuenta de Ahorros en tu teléfono móvil.

2. Recomendaciones para el uso de su "Llave Móvil" o "Tarjeta Electrónica"

En cumplimiento con el Acuerdo 6-2011 emitido por la Superintendencia de Bancos de Panamá, la Caja de Ahorros implementa nuevos elementos de Seguridad para las operaciones realizadas a través de la Caja en Línea y Banca Móvil.

El servicio de Caja en Línea cuenta con medidas de seguridad robustas acorde al segundo factor de autenticación. El usuario puede optar por dispositivo físico, denominado Tarjeta Electrónica o virtual denominado Llave Móvil. Los dispositivos de seguridad se integran para realizar sus transacciones monetarias en Caja en Línea.

1. No comparta o preste su celular mientras esté utilizando la aplicación de Llave Móvil.
2. En caso que extravíe o cambie su equipo móvil celular / Tablet donde tiene descargada la Llave Móvil, reporte de inmediato al Banco al Centro de Atención al Cliente 800-CAJA(2252) o ingrese a Caja en Línea para realizar el bloqueo de su dispositivo de seguridad.
3. En caso de que extravíe su Tarjeta Electrónica reporte de inmediato al Banco al Centro de Atención al Cliente 800-CAJA(2252) o ingrese a Caja en Línea para realizar el bloqueo de su dispositivo de seguridad.
4. No preste su Tarjeta Electrónica.
5. Mantenga su Tarjeta Electrónica en lugar seco.
6. No exponga su Tarjeta Electrónica a temperaturas extremas o a campos magnéticos.
7. No sumerja su Tarjeta Electrónica en agua, no la doble, no intente abrirla.
8. Evite dejarlo en la oficina o casa sin protección. Guárdelo en un lugar seguro.
9. La clave que genera no puede ser copiada ni clonada y no es necesario instalar nada en su computador.
10. EL token le permite una doble autenticación del usuario al realizar una transacción.

3. Políticas de Privacidad y Protección de Datos Personales

Caja de Ahorros ha diseñado una política de privacidad, establecido los medios y procedimientos necesarios para llevarla a cabo.

1. Se entiende por datos personales "cualquier información concerniente a personas físicas identificadas o identificables".
2. Los únicos datos personales a los que Caja de Ahorros tendrá acceso serán aquellos que el usuario facilite voluntariamente. En este sentido es preciso que el usuario conozca que para el alta y registro en algunos productos/servicios ofrecidos a través de la web, se le solicitarán datos de carácter personal.
3. Caja de Ahorros ha adoptado las medidas y procedimientos técnicos y organizativos necesarios para mantener el nivel de seguridad requerido en atención a los datos personales tratados. Así mismo está dotado de los mecanismos precisos a su alcance para evitar en la medida de lo posible los accesos no autorizados, sustracciones y

modificaciones ilícitas y la pérdida de los datos.

4. No obstante, si usted publica información personal en línea que es accesible al público, es posible que usted reciba mensajes no solicitados de otras personas y que sus datos, por tanto, sean conocidos por terceros.
5. Caja de Ahorros no utilizará sus datos para propósitos distintos de los anteriormente mencionados, ni los divulgará con fines comerciales. Todos los datos personales recibirán un tratamiento acorde con las normas de seguridad y confidencialidad de Caja de Ahorros en materia de tecnología de la información.
6. Por todo lo anterior, se le recomienda la máxima diligencia en esta materia y la utilización de todas las herramientas de seguridad que tenga a su alcance, no responsabilizándose Caja de Ahorros de sustracciones, modificaciones o pérdidas de datos en forma ilícita.
7. Así mismo, se le recomienda la lectura del Reglamento Único de Captación y Servicios, y sus adendas, en lo relativo a los servicios de Banca Electrónica en general y del Servicio de Banca por Internet – Caja en Línea.

4. Confidencialidad de notificaciones recibidas a través de Correo Electrónico

1. En nuestro sitio web hay diversas direcciones de correos electrónicos para remitir sus comentarios o consultas; los correos electrónicos recibidos de estas direcciones, son recibidos por personal especializado de la Caja de Ahorros que atiende estas comunicaciones da seguimiento y procura una respuesta a sus peticiones.
2. Si tiene alguna pregunta sobre el tratamiento que reciben sus correos electrónicos y los datos personales correspondientes, no dude en incluirla en su mensaje, o bien, llámenos al Centro de Servicio 800-CAJA(2252).

5. Política contra el Phishing

1. Caja de Ahorros no envía a sus clientes correos electrónicos solicitando datos personales, datos de cuentas, número de usuario o palabra clave, ni las actualizaciones de estos.
2. El único sitio donde puede actualizar voluntariamente su información es en http://www.cajadeahorros.com.pa y luego de ingresar mediante su número de cliente y palabra clave, al sitio privado del servicio de Banca por Internet “Caja en Línea”.
3. No descargue o abra ningún tipo de archivo que llegue en correos con adjuntos o noticias sensacionalistas enviados por remitentes que usted no conoce. Usualmente son software maliciosos que quedan instalados en sus computadoras.
4. Haga caso omiso a correos que lleguen indicando ser del Banco, donde se solicita ingresar a través de vínculos. Notifique o consulte a nuestro centro de servicio al Cliente a través de 800-CAJA(2252) y no ingrese o utilice tales vínculos.

6. Consejos de Seguridad - Tips para una navegación más segura.

Estas son algunas de las recomendaciones más importantes para el cliente:

1. Caja de Ahorros no solicitará información confidencial, personal, financiera o contraseñas de sus clientes vía correo electrónico o ingresar a través de vínculos enviados en un correo electrónico.
2. Caja de Ahorros no le solicitará en ningún momento que suministre su usuario o contraseña de acceso a la Banca en Línea o Banca Móvil.
3. Desconfíe de cualquier toma de datos personales realizada a través de Internet.
4. No entregue nunca información personal o financiera a través de un correo electrónico.
5. No entre a sitios de ninguna institución financiera en internet, a través de enlaces adjuntos en correos electrónicos.
6. Verifique que con la información recibida a través de correos electrónicos, usted logre identificar el remitente y que pueda comprobar que éste se dirige a usted.
7. No confíe en promociones que soliciten información, depósitos de dinero o entregas de información para obtener premios fácilmente, ni responda correos electrónicos solicitando información personal de forma urgente o inmediata.
8. No ejecute o instale archivos adjuntos correos electrónicos, gratuitos que provienen de sitios no confiables o desconocidos.
9. No participe en cadenas de correos, esto puede distribuir su dirección de correo de forma no autorizada.
10. Si necesita introducir datos en un sitio Web, debe asegurarse que en la parte inferior o superior de la ventana de su explorador, aparezca un candado cerrado los cuales indican una conexión segura y encriptada.

11. No deje su computadora o dispositivo móvil (Celular, Tablet, etc.) desatendido, cuando esté utilizando el servicio de banca en línea o Banca Móvil, es preferible que cierre la sesión si va a desatender su computadora o dispositivo móvil.
12. Verifique los datos de la última conexión al sistema mostrados en el sitio Web o Banca Móvil. Estos deben coincidir con el último acceso que usted tenga anotado o recuerde haber realizado.
13. Si sospecha que alguna de sus claves es conocida por una persona no autorizada, debe cambiarla inmediatamente, para que nadie, pueda utilizarla para acceder a sus cuentas.
14. Comuníquese con EL BANCO en caso que sospeche de una actividad fraudulenta a través de su clave de acceso al servicio electrónico: atencionalcliente@cajadeahorros.com.pa o al teléfono 800-CAJA(2252).
15. Es recomendable no acceder a su banca en línea desde:

    b. Redes inalámbricas públicas
    c. Computadores que usted desconozca sobre su protección

16. Proteja su computadora y equipo móvil:
    a. Actualice los programas en su computadora, según recomiende su proveedor.
    b. Utilice un Firewall. que le ayuda a prevenir que intrusos o virus ingresen a su computador.
    c. Instale un programa antivirus y manténgalo actualizado periódicamente.

d. Proteja su conexión a Internet.
e. No utilice o instale antivirus o software gratuitos bajados por internet.

17. Proteja los documentos impresos desde su banca en línea ya que contienen información valiosa sobre sus cuentas que podría ser mal utilizada si llegara a manos no autorizadas.
18. Lea periódicamente las Políticas de Privacidad y de Seguridad.
19. Caja de Ahorros le recomienda realizar la descarga de la aplicación (Banca Móvil) desde tiendas oficiales del sistema operativo de su equipo móvil que soporte la aplicación (Windows Store, App Store, Google Play, etc.)

7. Cómo Evitar que lo 'Pesquen' con una Red de Estafa Electrónica

¿Ha recibido un email con un mensaje similar a los siguientes?
"Sospechamos que se ha efectuado una transacción no autorizada en su cuenta. Para asegurar que su cuenta no ha sido comprometida, por favor haga click sobre el enlace que se presenta más abajo para que podamos confirmar su identidad".

"Durante el proceso habitual de verificación de cuentas, no pudimos verificar su información. Para actualizar y verificar su información, por favor presione aquí".

Pues se trata de una estafa llamada *"phishing"* — e involucra a estafadores que operan en Internet enviando mensajes electrónicos masivos no solicitados *(spam)* o mensajes de aparición automática *(pop-up)* para engañar a los consumidores y lograr que las víctimas inadvertidas revelen su información personal como números de tarjetas de crédito, información de cuentas bancarias, número de Seguro Social, contraseñas y demás información delicada. Los pescadores de información *(phishers)* envían un email o un mensaje *pop-up* que indica que proviene de negocios u organizaciones con los cuales usted mantiene una relación — por ejemplo, su proveedor de servicio de Internet *(ISP)*, banco, servicios de pago en línea y hasta de agencias gubernamentales. El texto del mensaje puede indicarle que "actualice," "valide" o "confirme" la información de su cuenta. Es posible que el texto del mensaje también incluya algún tipo de amenaza sobre las horribles consecuencias que puede sufrir en caso de que no responda. Estos mensajes lo dirigen a un sitio Web que luce similar al de una organización legítima, pero no lo es.

Se trata de un sitio Web falso cuyo único propósito es engañarlo para que usted divulgue su información personal y una vez que lo haga, los creadores de este correo y/o sitio falso pueden robarle su identidad y cometer fraudes en su nombre.

Siga las siguientes recomendaciones para evitar ser atrapado con este tipo de estafa de pesca de información:

1. **Si recibe un email o mensaje *pop-up* solicitándole información personal o financiera, no responda ni tampoco haga *clic* en el enlace o vínculo del mensaje.** Los BANCOS que operan legítimamente no solicitan este tipo de información por email. Si está preocupado por la actividad de su cuenta, comuníquese con su BANCO.
2. **Utilice programas antivirus y *firewall* y manténgalos actualizados.** Algunos de estos mensajes electrónicos que andan a la pesca de información contienen un software que puede dañar su computadora o hacer un seguimiento de sus actividades en Internet sin su conocimiento.

3. **No envíe información personal o financiera a través del correo electrónico.** El email no es un método seguro para transmitir información sensitiva ya sea personal o empresarial.
4. **Revise los resúmenes de sus cuentas bancarias y tarjetas de crédito tan pronto como los reciba** para verificar si le imputaron cargos no autorizados. Si su resumen de cuenta se demora más de un par de días, llame al banco o compañía de tarjeta de crédito para confirmar su domicilio de facturación y los saldos de sus cuentas.
5. **Tenga mucho cuidado al abrir o descargar los documentos o archivos que se adjuntan a los mensajes electrónicos recibidos**, sin tener en cuenta quien sea la persona u organización que los envía. Estos archivos pueden contener virus u otros programas que pueden afectar la seguridad de su computadora.
6. **Reenvíe el email recibido en la pesca de información a** bancaelectronica@cajadeahorros.com.pa
7. **Si cree que ha sido estafado, notifíquelo a través de nuestros canales de atención al cliente.**