

Seguridad en nuestros Canales Electrónicos

Global Bank vela por la seguridad de las inversiones de sus clientes. En el caso particular de las consultas y transacciones electrónicas, nuestro banco ha implementado políticas y brindado recomendaciones a nuestros clientes, con el propósito de garantizar trámites seguros, auténticos, confidenciales e íntegros a través de los canales electrónicos que brinda el banco.

Políticas de Seguridad:

- **Autenticación y Autorización**

El sistema de identificación de clientes para acceder al servicio de Banca en Línea consiste en el número de identificación de usuario (username) además de la contraseña del cliente (password). Esta combinación de caracteres se introduce al inicio de cada sesión de banca en línea. Esta combinación de códigos representa la llave de acceso personalizada que identifica y valida al cliente como la persona autorizada para ingresar a ver sus cuentas y realizar transacciones entre cuentas propias. A lo cual brindamos la recomendación de no anotar dicha contraseña en ningún lugar visible o accesible a cualquier persona, y mantenerla en total confidencialidad.

- **Cifrado de datos, sinónimo de Confidencialidad**

Con relación al modo de transmitir información, cada vez que usted efectúa una transacción a través de Banca en Línea, la información que viaja de su computadora o dispositivo móvil hacia el Banco y viceversa, va cifrada utilizando una llave de 256 bits. El cifrado consiste en la codificación y decodificación de la información entre su punto de origen y el destino, brindando así la seguridad de que si la misma logra ser captada por algún tercero durante su recorrido, sea prácticamente imposible su interpretación, garantizando así la confidencialidad de la misma.

- **Certificados digital**

Un certificado digital (SSL – Secure Socket Layer) sirve para brindar seguridad al visitante de nuestro sitio web, es una forma sencilla y fácil para identificar que está ingresando a un sitio auténtico, real y confiable a fin de introducir datos de forma segura. Global Bank utiliza la reconocida autoridad certificadora de VeriSign, esta autoridad es equivalente a un “notario” en Internet, que certifica la autenticidad del sitio visitado y hace que sus datos viajen cifrados de manera segura entre el usuario web y el servidor y viceversa. Usted mismo puede verificar la vigencia del certificado que mantiene Global Bank con VeriSign, sólo presione sobre el candado ubicado en la barra de direcciones (barra de color verde), antes de ingresar cualquier tipo de dato a la Banca en Línea.

Para Global Bank, garantizar la seguridad de la información que reside en nuestras bases de datos y las transacciones que son realizadas en línea son la prioridad número uno, para ello utilizamos firewalls o murallas contrafuegos, entre otros elementos de seguridad que protegen el acceso a la red del Banco desde el exterior. En Global Bank nos mantenemos a la vanguardia de la última tecnología, para garantizar un servicio de calidad, y a tono con las necesidades y exigencias del mundo bancario actual y las regulaciones existentes.

Seguridad de TI

Acerca de la contraseña de seguridad para acceder a la Banca en Línea:

- El Banco le provee al cliente una contraseña de seguridad numérica. Al primer ingreso de la misma, el sistema solicita su cambio, para que el cliente cree una nueva contraseña o clave de forma obligatoria. El cliente deberá mantener siempre su contraseña en estricta confidencialidad.
- Aunque el cambio de contraseña no sea obligatorio luego del primer ingreso al servicio, se sugiere realizar este cambio al menos una vez cada 30 días. Permanecer mucho tiempo con una misma contraseña representa un riesgo ante el evento que la misma sea capturada, adivinada o descifrada por un tercero.
- El bloqueo de la contraseña de acceso a Banca en Línea se da luego de 5 intentos fallidos para acceder al sistema. El cliente deberá presentarse en cualquiera de nuestras sucursales para solicitar el desbloqueo de su contraseña, bajo ninguna circunstancia la misma podrá ser vía telefónica.
- Una vez hayan transcurrido 90 días consecutivos de inactividad dentro del sistema, la contraseña del cliente queda automáticamente desactivada. El mismo deberá presentarse en cualquiera de nuestras sucursales para solicitar la activación de su contraseña.
- La cancelación de la contraseña se da luego de 180 días de no hacer uso de la misma. El cliente deberá presentarse en cualquiera de nuestras sucursales para solicitar una nueva impresión de contraseña dado que la contraseña anterior ya no le funcionará ni podrá ser activada.
- En el evento que el cliente haya olvidado su contraseña (indistintamente que la misma esté activa, bloqueada o inactiva) será importante que el cliente se presente en sucursal para solicitar una nueva contraseña de Banca en Línea. La generación e impresión de la nueva contraseña sólo podrá ser realizada con el cliente o la persona autorizada presente en sucursal.

Evite el Fraude Electrónico

Para evitar al máximo ser víctima de un fraude electrónico, tenemos algunas recomendaciones que solicitamos las adopte en el uso diario de los canales electrónicos que le brinda el banco:

- No comparta con nadie información sensible tal como contraseñas o números de tarjetas de crédito; ni introduzca esta información en documentos o formularios que no provengan de la fuente legítima. Si no está seguro de su procedencia, por favor consulte de inmediato con el banco.
- Al acceder a nuestra Banca en Línea siempre deberá validar que la dirección del banco en Internet sea la correcta: www.globalbank.com.pa, de ser una dirección distinta a ésta, favor no acceda a la misma y reporte el incidente de inmediato al 800-0006.
- Siempre que se encuentre en la página para ingresar su USUARIO y CONTRASEÑA de Banca en Línea, asegúrese que la barra de direcciones indique **https**, un candado y además de que la barra de direcciones es verde, como una manera sencilla y fiable de verificar la identidad y la seguridad del sitio. Esta indicación asegura que la transmisión de la información entre su máquina y el sitio WEB se está realizando de manera segura y confiable, además de confirmarle la autenticidad del sitio web que está accediendo.
- Haga uso de programas de antivirus para evitar infecciones de virus, malware, spyware en su computadora. Es deseable que estos programas sean actualizados frecuentemente.
- Mantener su sistema operativo actualizado, con los últimos parches de vulnerabilidades a día, a fin de evitar que su equipo este comprometido y ponga en riesgo la información que en ella posea.
- Por su seguridad no responda a ningún mensaje de correo electrónico donde le soliciten sus datos personales tales como contraseñas, números de tarjeta de crédito o acceder al sitio web del banco a través de enlaces. Global Bank no solicita información confidencial de sus clientes a través de correo electrónico u otros medios no seguros.

Uso de Doble Factor de autenticación para transacciones bancarias

Global Bank, ha desarrollado nuevos mecanismos de seguridad para proteger sus transacciones bancarias, a lo que los usuarios tendrán 2 opciones de este nuevo doble factor de autenticación:

Hardtoken (llave electrónica) : es un segundo factor de autenticación al cual el cliente tiene acceso por medio de un dispositivo o llave electrónica (físico) que genera códigos de seguridad de 6 dígitos que cambian constantemente y no se repiten. Estos códigos de seguridad son requeridos para confirmar sus transacciones a terceros en nuestra Banca en Línea.

- En caso de pérdida de su llave, podrá efectuar la desactivación del dispositivo por medio de su banca en línea.
- Notificar al banco a través de Servicio al Cliente 800-0006 para dar de baja el servicio para dar de baja el servicio.
- Realizar la solicitud desde Banca en Línea y apersonarse a la sucursal de su conveniente, para la entrega del nuevo dispositivo

Softoken (contraseña digital): es un segundo factor de autenticación que permite generar desde una aplicación instalada en su equipo móvil, códigos de seguridad de 6 dígitos que cambian constantemente y no se repiten. Estos códigos de seguridad son requeridos para confirmar sus transacciones a terceros en nuestra Banca en Línea.

- En caso de pérdida de su dispositivo móvil, podrá efectuar la desactivación del dispositivo por medio de su banca en línea.
- Notificar al banco a través de Servicio al Cliente 800-0006 para dar de baja el servicio para dar de baja el servicio.
- Realizar el procedimiento de configuración en su nuevo dispositivo móvil, según lo que indica el manual de usuario.

Consejos de Seguridad para el Uso de sus Tarjetas:

Algunos consejos de seguridad de la Tarjeta SISTEMA Clave:

- No coloque su tarjeta cerca de imanes o campos magnéticos, ya que los mismos, borran la información grabada en la banda magnética.
- No exponga su tarjeta a altas temperaturas (frío o calor).
- Nunca doble su tarjeta.
- No escriba su número de PIN o contraseña en la banda de papel de la tarjeta, ésta es sólo para su firma, la cual es muy importante para efectos de verificaciones, al tiempo que, facilita la recuperación en caso de extravío.
- En el caso que su tarjeta **Clave** no funcione adecuadamente o se le extravíe por algún motivo, usted debe comunicarse con la Institución Financiera que le emitió la misma, para que sea evaluada y si es necesario, reemplazarla por una nueva.

Consejos a seguir para proteger su Número Secreto o PIN:

- No escriba su número secreto en ningún lugar. El número secreto debe ser memorizado por su propio bien, y si por algún motivo lo ha olvidado, comuníquese inmediatamente con su banco.
- Nunca le dé su número secreto (PIN) a otras personas, ni preste su tarjeta. La tarjeta Clave es para uso personal solamente.
- Si el cajero automático está fuera de servicio, no introduzca su número secreto, ya que el cajero no funcionará.
- Asegúrese que retiró su tarjeta después de realizar una transacción en un cajero automático o en algún comercio.

Seguridad de TI

- Es importante saber que en los cajeros Clave se bloquean las tarjetas de débito después de tres (3) intentos inválidos de introducción de PIN. Esta medida es para su seguridad, previniendo así, el uso fraudulento de su tarjeta en un momento dado.

Seguridad en los Cajeros Automáticos SISTEMA Clave:

- No Utilice cajeros si no hay buena iluminación, si el lugar está desolado o con poca vigilancia.
- 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.
- No permita que nadie lo observe cuando está digitando su número secreto.
- Tape con la otra mano al digitar su número secreto o PIN, aunque se encuentre solo en un cajero de cubículo.
- No acepte ayuda de nadie en los cajeros automáticos.
- Procure no contar el dinero dentro del cajero.
- Conserve los recibos que le entrega el cajero para llevar su propio control de la cuenta.
- Revise su estado de cuenta todos los meses.
- Asegúrese que el cajero automático no contenga objetos extraños (clips, cinta adhesiva) en la ranura de inserción, ni en el dispensador de efectivo.

Seguridad en las Transacciones Internacionales Clave:

Cuando va de viaje y planea utilizar su tarjeta Clave en los cajeros internacionales, recuerde lo siguiente:

- Notificar al banco a través de Servicio al Cliente 800-0006
- Revise la expiración de su tarjeta antes de partir.
- Asegúrese que sabe el número secreto (PIN).
- El cajero automático que utilice debe tener el emblema PLUS.
- Al utilizar su tarjeta Clave en países donde no circula el dólar, los cajeros automáticos dispensarán dinero correspondiente a la moneda en circulación.
- El tiempo aproximado para la ejecución de una transacción es de 10 segundos.
- Si su tarjeta es capturada en el cajero, deberá reclamarla en el banco que la emitió en Panamá.
- El costo de la transacción dependerá de la política de la Institución emisora de su Tarjeta Clave.

Para cualquier consulta que tenga referente a la seguridad de nuestros canales electrónicos, no dude en contactarnos al 800-0006 o a través de nuestro correo electrónico contactenos@globalbank.com.pa