TERMINOS Y CONDICIONES DEL INTERNET BANKING
DE BANCO CARIBE

POR FAVOR, LEA DETENIDAMENTE LOS TÉRMINOS Y CONDICIONES:

POLÍTICA DE SEGURIDAD

1.- Para salvaguardar la información financiera de nuestros clientes, Banco Caribe proporciona seguridad, privacidad, confiabilidad e integridad para cada transacción que EL CLIENTE realice. La mismo para las transacciones a través de cajeros automáticos, teléfonos o en locales comerciales. En tal sentido, a continuación, presentamos las medidas de Seguridad que se encuentran publicadas en nuestra página web.

2.- La información que EL CLIENTE suministra al banco es confidencial; su uso está limitado a prácticas bancarias y el personal que tiene acceso a ella conoce, respeta y está sujeto a las disposiciones de nuestro Código de Ética y las leyes. La información sólo será divulgada como cumplimiento de una obligación legal solicitada por los órganos reguladores o al poder judicial siempre que se encuentre fundamentada en una orden o sentencia ejecutoria.

3.- EL CLIENTE puede visitar la página web de Banco Caribe y encontrar información acerca de los productos y servicios disponibles, sin necesidad de facilitar información alguna sobre su persona o finanzas.

4.- El CLIENTE, declara, reconoce y acepta que EL BANCO no es responsable de pérdidas o retrasos en la transmisión de las instrucciones como resultado del uso de cualquier proveedor de servicio o causado por el programa del navegador de internet.

5.- El CLIENTE, declara, reconoce y acepta que EL BANCO no es responsable de interrupciones ni alteraciones en el sistema, incluyendo interrupciones causadas por cualquier virus informático o problemas similares, siempre y cuando las mismas no le sean imputables al Banco.

6.- El CLIENTE, acepta colaborar con EL BANCO en las investigaciones que inicie por causa de acceso no autorizado a las cuentas de EL CLIENTE.

7.- EL CLIENTE tiene la responsabilidad de mantener la confidencialidad y seguridad de la información y aplicaciones que estén en su dispositivo electrónico, asegurando el mismo mediante el bloqueo con contraseñas y asegurándose de que los mismos no sean de conocimiento de terceras personas. EL CLIENTE debe mantener en estricta confidencialidad los datos de acceso. Como titular del usuario y contraseña, EL CLIENTE es responsable de todas las operaciones generadas utilizando los mismos, salvo los casos en que EL CLIENTE notifique al Banco de la pérdida o sustracción del dispositivo o de los elementos de autenticación que un tercero pudiera tener conocimiento. Incluso antes de la notificación, EL BANCO será responsable de las transacciones fraudulentas, siempre y cuando provenga de una falta imputable al Banco y sin perjuicio del derecho de reclamaciones que dispone EL CLIENTE.

8.- EL CLIENTE libera de toda responsabilidad a BANCO CARIBE si facilita su contraseña a un tercero no autorizado para el uso de la plataforma.

9.- Cortafuegos Web (WAF) & DDoS

Sistemas que custodian la integridad del flujo de información generada cuando EL CLIENTE se registra, solicita información o realiza cualesquier transacciones financieras, previniendo e interceptando la filtración de datos.

10.- Zona de Conexión Segura (Secure Socket Layer)

Es un área de alta seguridad, proporcionada por el servidor que alberga la página en red de EL BANCO, en la cual podrá realizar transacciones comerciales con capacidad para codificar según el método criptográfico **de 256 bits,** garantizando así privacidad en la transmisión de datos.

11.- Certificado de Seguridad Digital (Digital Security Certificate)

Banco Caribe utiliza como proveedor de criptografía a **Digicert** para solucionar los requisitos de autentificación y certificación en las transacciones electrónicas. El criptograma se completa cuando aparece el icono de candado en la barra inferior derecha de su pantalla.

12.- Sistema para la Detección de Intrusos en la Red (IPS)

Estos programas y equipos funcionan como centinelas y los mismos se encargan de proteger los servidores para repeler ataques, intrusiones o intentos de acceso sin autorización. Banco Caribe Periódicamente implementa nuevas actualizaciones para mantener la protección de estos vigente.

13.- Centro de Monitoreo

A través de un sistema que opera las veinticuatro (24) horas, los siete (7) días de la semana, contamos con un equipo que se dedica a vigilar cualquier alerta, intentos de acceso sin autorización, ataques y demás actividades sospechosas.

14.- Requerimientos

Su dispositivo electrónico sólo necesita tener instalados el servicio de Internet y un programa de navegación web.

15.- Recomendaciones de seguridad

La seguridad de las transacciones también depende de las precauciones que tome EL CLIENTE, para ello conviene adoptar medidas de seguridad y le recomendamos las siguientes:

1.- Mantenerse alerta: Banco Caribe nunca solicita que facilite su nombre de usuario o contraseña. En sentido general, jamás envíe información confidencial por correo electrónico, redes sociales o la divulgue por teléfono.

2.- Mantener en estricta confidencialidad los datos de acceso.

3.- Para crear su nombre de usuario y contraseña haga combinaciones de números y letras con un mínimo de ocho (8) caracteres.

4.- Descarte usar en la contraseña sus datos personales (nombres, apellidos, teléfono, cedula, edad), los de sus relacionados, las fechas importantes y números o letras repetidas. En fin, no utilizar información relacionada que pueda resultar fácil de descifrar.

5.- Modifique su contraseña periódicamente. Es recomendable cambiarla cada treinta (30) días.

6.- Nunca deje el dispositivo electrónico solo mientras se encuentra con la sesión abierta en la página de Internet Banking. Si debe movilizarse lejos de esta, entonces cierre sesión.

7.- Verifique la hora y fecha del último acceso electrónico a su cuenta. Cambie su contraseña si presume que alguien la ha descubierto.

8.- No deberá revelar sus datos como usuarios y contraseña a nadie, ni siquiera a los miembros de su familia, amigos, empleados, contadores o auditores ni a ninguna otra persona.

9.- Validar la vigencia de los contratos de los que forme parte, formalidades de su rescisión y causas de terminación del mismo.