

Favor leer cuidadosamente los términos y condiciones de uso de Banco Múltiple Caribe Internacional, S. A., en línea.

Para tener acceso, debe darle a aceptar

Política de Seguridad:

- 1.** Para salvaguardar la información financiera de nuestros clientes, Banco Múltiple Caribe Internacional, S. A. (en lo adelante EL BANCO), proporciona seguridad, privacidad, confiabilidad e integridad para cada transacción que EL CLIENTE realice, incluidas transacciones a través de cajeros automáticos, teléfonos o en locales comerciales.
- 2.** En tal sentido, a continuación, le presentamos las medidas de Seguridad que se encuentran publicadas en nuestra página web <https://www.bancocaribe.com.do>
- 3.** La información que EL CLIENTE suministra a EL 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 normativas vigentes. La información sólo será divulgada como cumplimiento de una obligación legal solicitada por los órganos reguladores o el poder judicial, siempre que se encuentre fundamentada en una orden o sentencia ejecutoria.
- 4.** EL CLIENTE al acceder a la página web de EL BANCO encuentra información acerca de los productos y servicios disponibles, sin necesidad de facilitar información alguna sobre su persona o finanzas.
- 5.** El CLIENTE, declara, reconoce y acepta que EL BANCO no es responsable de pérdidas o retrasos que se produzcan en la transmisión de sus instrucciones como resultado del uso de cualquier proveedor de servicio o causado por el programa del navegador de internet.
- 6.** El CLIENTE, declara, reconoce y acepta que EL BANCO no es responsable de interrupciones ni alteraciones en el sistema, causadas o no por cualquier virus informático o problemas similares, siempre y cuando las mismas no le sean imputables al Banco.
- 7.** El CLIENTE, acepta colaborar con EL BANCO en las investigaciones que inicie por causa de acceso no autorizado a las cuentas de EL CLIENTE.
- 8.** EL CLIENTE reconoce y acepta que EL BANCO se reserva, a su única opción, el derecho de activar, limitar o eliminar el acceso a EL CLIENTE de los servicios solicitados, sin que de ninguna forma comprometa su responsabilidad.
- 9.** EL CLIENTE reconoce y acepta que EL BANCO podrá en cualquier momento y previa notificación por escrito, o requerimiento de aceptación de los nuevos términos, modificar la naturaleza de esta herramienta y podrá adicionar nuevos servicios a la misma, a los cuales cuáles podrá acceder, conforme lo previsto. La notificación podrá ser por escrito, incluyendo redes sociales, llamadas, SMS, correo electrónico o cualquier medio fehaciente que EL BANCO considere pertinente, con un mínimo de treinta (30) días de antelación a la entrada en vigor de las modificaciones. La notificación incluirá detalles específicos sobre los cambios, la fecha de vigencia y la opción para que el cliente cancele el contrato antes de que entren en vigor sin costo adicional.
- 10.** EL CLIENTE reconoce, declara y acepta que, a los fines de usar la herramienta de referencia, debe contar con uno o varios productos o servicios de los que ofrece EL BANCO.

11. EL CLIENTE reconoce, declara y acepta que, a los fines de obtener los servicios de Internet Banking debe cubrir con todos los gastos de adquisición, instalación de telecomunicación; cumplir con todos los recursos técnicos requeridos por EL BANCO, y muy especialmente la conexión a internet a través de una de las compañías de comunicación que ofrecen tal servicio, a los fines de lograr el acceso a los sistemas de EL BANCO, utilizando su código de usuario y clave de acceso.

12. El cliente reconoce y acepta que es totalmente responsable de todas las actividades que se realicen después que el sistema haya autorizado su acceso sobre la base de una verificación electrónica de su identidad.

13. EL CLIENTE reconoce que tiene la responsabilidad y la asume, de tomar todas las medidas de lugar para proteger el soporte electrónico recibido con el propósito de identificación. En ese sentido, EL CLIENTE deberá mantener en secreto los códigos PIN, código de acceso (nombre de usuario), claves de acceso (contraseña/password) y cualquier otro medio de identificación. EL CLIENTE no deberá grabar en su computadora personal o de terceros, ni en cualquier material de computadora o en cualquier otro dispositivo de acceso, sus medios de identificación, ni permitir que terceros los conozcan o utilicen. Los códigos de PIN y las claves de acceso deberán ser elegidos de una manera tal que no dificulte su detección (por ejemplo, no deben estar basadas en números de teléfono, fechas de nacimiento, número de placas, etc.).

Reclamaciones:

14. Derecho de reclamar, interponer quejas y denuncias: EL CLIENTE reconoce que le asiste el derecho presentar a EL BANCO cualquier reclamación o queja que considere amerita de una respuesta o acción de parte de EL BANCO, debiendo canalizarla vía cualesquiera de los canales de los que disponga EL BANCO a esos fines, tales como: a través del canal digital App, Sucursales, centro de contacto. Es responsabilidad de EL BANCO canalizar y gestionar la misma a los fines de dar respuesta a EL CLIENTE dentro del plazo de 30 días calendarios y 45 días calendarios en casos complejos. La presentación de reclamaciones está sujeta al cumplimiento de los requisitos de forma y fondo establecidos por los reglamentos e instructivos emitidos por los órganos regulatorios y EL BANCO en la materia. En virtud de lo anterior, EL CLIENTE deberá presentar la reclamación correspondiente, mediante suscripción del “Formulario de Reclamaciones”, depositado por alguno de los canales de reclamaciones habilitados a tales fines, por sí mismo o por un representante apoderado, autorizado en virtud de un poder de representación que cumpla con las formalidades legales en la materia. EL CLIENTE podrá presentar las reclamaciones, quejas y denuncias que considere pertinentes respecto a los productos, facilidades o servicios contratados, por cualquiera de los siguientes medios: (a) Vía presencial: En la oficina principal de EL BANCO o cualquiera de sus sucursales, a través del representante de Servicios de Atención al Usuario; (b) Vías digitales o electrónicas: A través de la página web oficial de Banco Múltiple Caribe Internacional, S.A., <http://www.bancocaribe.com.do>, Banco Caribe App, (c) Vías telefónica: Mediante llamada al número telefónico del centro de contacto, (809) 378-0505 y canales alternos de EL BANCO. A la vez, EL CLIENTE reconoce que si EL BANCO no le responde dentro del plazo indicado o la respuesta no le satisface, le asiste el derecho de escalar su reclamación vía la Superintendencia de Bancos de la República Dominicana, por ante la Oficina de Servicios de Protección al Usuario (Prousuuario) de dicha entidad, a través de los canales habilitados al efecto, con los documentos que lo respalden, contando con un plazo de sesenta (60) días calendario para tales fines. EL CLIENTE reconoce que, si la reclamación presentada no resultare a su favor, deberá asumir los costos, comisiones de gestión, y gastos por la investigación incurridos por EL BANCO.

Sin perjuicio de lo antes mencionado, EL CLIENTE reconoce, declara y acepta que, de conformidad con lo establecido en el Reglamento de Protección al Usuario de los Productos y Servicios Financieros, posee un plazo de cuatro (4) años máximo, contados a partir del momento en que se produzca el hecho que considere desfavorable o tome conocimiento de este, para presentar una reclamación respecto al mismo. Al vencimiento de dicho plazo, la actuación, se reputará como aceptada, buena y válida.

15. EL CLIENTE reconoce que EL BANCO hará esfuerzos razonables por mantener barreras de seguridad electrónicas que impidan el acceso no autorizado por terceros a las informaciones que se generen con motivo de la ejecución de este contrato. Sin embargo, EL CLIENTE reconoce que el intercambio de información mediante acceso por Internet y mediante conexiones telefónicas, pueden posibilitar que terceros logren acceder o conectarse sin autorización. En consecuencia, EL CLIENTE libera a EL BANCO de cualquier responsabilidad originada o derivada del acceso no autorizado de terceros a las bases de datos, transacciones y sistemas de EL CLIENTE y de EL BANCO.

16. EL CLIENTE reconoce, declara y acepta que EL BANCO está comprometido en mantener debidamente actualizada toda la información que le sea requerida por EL CLIENTE y que formen parte de los servicios y productos contratados.

17. EL CLIENTE reconoce, declara y acepta que podrá obtener evidencia de las operaciones que realice y a tales fines podrá imprimir todas las informaciones a las cuales tenga acceso en virtud de este contrato, en el entendido de que tales impresiones servirán como referencia y solo serán válidas y oponibles a EL BANCO cuando sean cotejados y comprobados de manera directa con los datos que estén almacenados en los sistemas electrónicos o físicos de EL BANCO.

18. EL CLIENTE reconoce y acepta que los beneficios otorgados por el presente contrato y el uso de la herramienta son personales e intransferibles, EL BANCO no reconoce a otro beneficiario que no sea a EL CLIENTE.

19. EL CLIENTE reconoce que, en principio, EL BANCO no será responsable por daños directos, indirectos, especiales, incidentales o consecuenciales que puedan ocurrir por demora en la ejecución de las instrucciones dadas por EL CLIENTE, incluyendo daños a la imagen o prestigio comercial de éste, ni responsabilidad en que pueda incurrir EL CLIENTE frente a terceros por dicha causa. La responsabilidad de EL BANCO estará en todos los casos limitada a ejecutar las instrucciones de EL CLIENTE en la forma en que las mismas sean dadas, tan pronto como las circunstancias lo permitan.

20. EL CLIENTE se obliga y compromete a mantener, en todo momento, a EL BANCO actualizado de sus datos de contacto, estando, en consecuencia, obligado a notificar oportunamente a EL BANCO cualquier cambio de domicilio, dirección de correo electrónico, número de teléfono celular y cualquier otro medio de contacto registrado. Sin perjuicio de lo anterior, EL BANCO, en cumplimiento de sus obligaciones de debida diligencia, realizará las gestiones razonables y a su alcance para procurar la actualización de los datos de EL CLIENTE.

Confidencialidad:

21. 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 a EL 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 se produzca por una falta imputable a EL BANCO y sin perjuicio del derecho de reclamaciones que dispone EL CLIENTE.

21. EL CLIENTE libera de toda responsabilidad a EL BANCO si facilita o expone su contraseña o datos personales o de acceso a un tercero no autorizado para el uso de la plataforma.

Acceso Electrónico para Nuevos usuarios

22. Para la autorización de acceso a los servicios y productos vía electrónica, EL CLIENTE deberá registrarse en Internet Banking en <https://www.bancocaribeenlinea.com.do>.

23. El presente contrato tendrá una vigencia por tiempo indefinido, iniciando a partir de la fecha en que EL CLIENTE complete su registro en los canales digitales de EL BANCO. EL CLIENTE podrá solicitar en cualquier momento la eliminación de su usuario y la desvinculación de los servicios digitales, mediante los mecanismos establecidos por EL BANCO para tales fines. Asimismo, EL BANCO se reserva el derecho de suspender o eliminar el acceso de EL CLIENTE a los canales digitales, total o parcialmente, en cualquier momento, por razones de seguridad, incumplimiento de los términos y condiciones, sospecha de uso fraudulento, inactividad prolongada o cualquier otra causa que EL BANCO considere pertinente, a su entera discreción.

Parámetros de Seguridad

23. EL BANCO posee una plataforma tecnológica compuesta por varios mecanismos, los cuales, protegen la información y previenen el acceso de intrusos. Éstos son:

24. Nombre de usuario (Username): Es el nombre único y visible creado por EL CLIENTE, como titular de la cuenta, para fines de acceso a la plataforma y se compone de una combinación de letras y números.

25. Contraseña (Password): Es una serie de caracteres confidenciales y uso personal de EL CLIENTE, que sirve de contraseña o llave de acceso, la cual le garantiza privacidad. La misma se forma con una combinación de letras y números.

26. Token Caribe Digital: es un segundo factor de autenticación que permite generar desde una aplicación instalada en el dispositivo de EL CLIENTE, códigos de seguridad numéricos que cambian constantemente en forma automática y nunca se repite. Estos códigos de seguridad serán requeridos al momento de agregar un nuevo beneficiario e ingresar a través de un equipo no registrado por la institución, pudiendo ser incorporado a futuro para otras transacciones a través de canales alternos.

27. Código de Seguridad (Security Code): conjunto de caracteres que le servirá a EL CLIENTE como proceso de autenticación para la instalación del Token Caribe Digital en su dispositivo.

28. Identificación Bloqueada (User Blocked): Al tercer (3) intentos de acceso fallido (incapacidad de identificar correctamente su nombre de usuario y contraseña), el sistema bloqueará completamente el acceso a su cuenta. Para reestablecer el acceso deberá llamar a los teléfonos Nos. (809)-378-0505 o al 1-(809)-200-0505 desde el interior sin cargos. La nueva clave de acceso aleatoria y generada por el sistema

sólo podrá ser enviada por EL BANCO al correo electrónico de EL CLIENTE, existente en el sistema de EL BANCO.

29. Desconexión de la Sesión (Expirad Session): La sesión segura de la página transaccional se desconectará, automáticamente-, un (1) minuto después que haya quedado inactiva.

30.- Cortafuegos Web (WAF) & DDoS: Sistemas que custodian la integridad del flujo de información generada cuando EL CLIENTE se registra, solicita información o realiza cualesquiera transacciones financieras, previniendo e interceptando la filtración de datos.

31.- 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, la privacidad en la transmisión de datos.

32.- Certificado de Seguridad Digital (Digital Security Certificate): EL BANCO utiliza como proveedor de criptografía a Digicert para solucionar los requisitos de autenticación y certificación en las transacciones electrónicas. El criptograma se completa cuando aparece el icono de candado en la barra inferior derecha de su pantalla.

33. 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. EL BANCO Periódicamente implementa nuevas actualizaciones para mantener la protección de estos vigente.

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

Requerimientos

35. El dispositivo electrónico de EL CLIENTE sólo necesita tener instalados el servicio de Internet y un programa de navegación web.

Recomendaciones de seguridad

36. La seguridad de las transacciones e informaciones personales y de acceso depende de las precauciones que tome EL CLIENTE, dentro de las cuales, le recomendamos adoptar las medidas de seguridad que le indicamos de manera enunciativa, mas no limitativas:

1. Leer las medidas de seguridad antes de proceder a darle uso a cualquier herramienta digital.
2. Mantenerse alerta: EL BANCO nunca solicita que facilite su nombre de usuario o contraseña. En sentido general, no envíe información confidencial por correo electrónico, redes sociales o la divulgue por teléfono.
3. Mantener en estricta confidencialidad los datos de acceso.
4. Realizar combinaciones de números y letras con un mínimo de ocho (8) caracteres de Para crear su nombre de usuario y contraseña.

5. No 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.
6. Modificar su contraseña periódicamente. Es recomendable cambiarla cada treinta (30) días o cuando lo considere oportuno.
7. Bajo ningunas circunstancias dejar el dispositivo electrónico solo mientras se encuentra con la sesión abierta en la página de Internet Banking.
8. Verificar la hora y fecha del último acceso electrónico a su cuenta, a los fines de detectar usos indebidos y Cambiar la contraseña si presume que alguien la ha descubierto.
9. No revelar los datos como de usuarios y contraseña a nadie, aún sean miembros de su familia, amigos, empleados, contadores o auditores.
10. Validar la vigencia de los contratos de los que forme parte, formalidades de su rescisión y causas de terminación de los mismos.
12. Contactar inmediatamente a EL BANCO si considera que sus medios de identificación o autenticación han sido robados, o si se han extraviado, o si sospecha que una persona no autorizada ha tenido acceso a los mismos.
13. Informar a EL BANCO, si considera que se ha producido algún error en cualquiera de las transacciones realizadas de manera electrónica.
14. Actualizar los datos que le ha aportado a EL BANCO en caso de cambio o modificación de los mismos y aportarlos cuando le sean requeridos.

Descripción de funcionalidades de canales digitales

Grupo 1: Registro y Autenticación de Usuarios, Administración de empresa	Registro de usuarios	Registro de usuarios nuevos individuales
		Registro de usuarios corporativos administradores
	Login	Ingreso de usuarios individuales
		Ingreso de usuarios corporativos administradores
		Ingreso de usuarios corporativos no administradores
		Utilizar teclados virtuales
		Posición consolidada
	Configuración de usuarios	Cambio de contraseña
		Cambio de datos personales

		Cambio de opciones de registro
		Configuración de usuarios
		Cambio de contraseña
		Cambio de datos personales
		Cambio de opciones de registro
	Administración	Administración de usuarios
		Administración de permisos
		Administración de esquema de firmas
Grupo 2: Consultas	Cuentas Corrientes y de Ahorro	Listado principal de cuentas
		Consulta detalle de cuentas
		Consulta de movimientos
		Exportar movimientos
		Consulta de estado de cuenta en PDF
		Imagen de cheques
		Bloqueo de cheques
	Tarjetas de Crédito (solo aplica a Banca Individual)	Listado principal de tarjetas de crédito
		Ver información de tarjetas adicionales
		Consulta detalle de tarjetas de crédito
		Consulta de detalle extralímite
		Consulta de estados de tarjeta de crédito en PDF
		Consulta de movimientos de tarjeta de crédito
		Exportar movimientos de tarjeta de crédito (Excel y TXT)
	Préstamos	Listado principal de préstamos
		Consulta de detalle de préstamos
	Inversiones	Listado principal de certificados de depósito
		Consulta de detalle de certificados de depósito
Grupo 3: Transacciones	Transferencias	Pagos de tarjeta de crédito
		Transferencias propias
		Transferencias ACH
		Transferencias LBTR
		Transferencias Regionales
		Transferencias a Puesto de bolsa
		Beneficiarios Banco Multiple
		Beneficiarios otros banco
		Beneficiarios Regionales
		Historial de transferencias

		Historial de Regionales
		Historial de Puestos de bolsa
		Lista de operaciones pendientes de aprobación
		Autorizar transferencias
		Rechazar transferencias
	Solicitudes	Solicitud de chequeras
Grupo 4: Generales y BackOffice	BackOffice	Ingreso de usuario
		Administración de usuarios individuales
		Administración de usuarios empresas
		Administración de usuarios internos
		Configuración - Mantenimiento de pool de imágenes
		Configuración -Mantenimiento de variables de configuración y catálogos
		Administración de Transferencias
		Comunicación - Mensajes a usuarios o grupos de usuarios
		Auditoría -Bitácora de usuarios internos
		Registro -Aprobar/Declinar solicitud de registro de clientes individuales y corporativos
		Gestión de Solicitudes
		Solicitudes de chequera
		Solicitudes de transferencias regionales y a puesto de bolsa