Security Procedures
Procedimientos de Seguridad

1. Introduction
Introducción

These "Security Procedures", as referenced in the Communications section of the Master Account and Service Terms ("MAST") (or other applicable account terms and conditions), are designed to authenticate the Customer's log-on to the Bank's connectivity channels and to verify the origination of Communications between Bank and Customer in connection with the following Services or connectivity channels (the availability of which may vary across local markets).

Estos "Procedimientos de Seguridad", de conformidad con la sección titulada Comunicaciones del "Acuerdo Marco de Aperturas de Cuentas y Prestación de Servicios" ("MAST") (u otros términos y condiciones de cuenta aplicables), tienen como fin autenticar el inicio de sesión del Cliente en los canales de conectividad del Banco, y verificar el origen de las comunicaciones entre el Banco y el Cliente relacionadas con los siguientes Servicios o canales de conectividad (cuya disponibilidad puede variar en los distintos mercados locales).

- CitiDirect® (including WorldLink®)
  CitiDirect® (incluido WorldLink®)
- CitiConnect®
  CitiConnect®
- Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
  Society for Worldwide Interbank Financial Telecommunication ("SWIFT")
- Manual Initiated Funds Transfer ("MIFT")
  Transferencia de Fondos Iniciada Manualmente ("MIFT")
- Interactive Voice Response ("IVR")
  Respuesta de Voz Interactiva ("IVR")
- Email/Fax/Mail/Messenger/Phone with the Bank
  Correo electrónico/fax/correo postal/mensajería/teléfono con el Banco
- Other local electronic connectivity channels
  Otros canales de conectividad electrónicos locales

These Security Procedures are to be read together with the MAST and may be updated and advised to the Customer from time-to-time by electronic or other means, including but not limited to posting updates to the Security Procedures on CitiDirect®. Unless otherwise provided by law, Customer's continued use of any of the above noted Services or connectivity channels after being advised of updated Security Procedures shall constitute Customer's acceptance of such updated Security Procedures. These Security Procedures cover the following:

Estos Procedimientos de Seguridad deben interpretarse junto con el MAST y pueden actualizarse y sugerirse al Cliente periódicamente por medios electrónicos u otros, incluida, a modo de ejemplo, la publicación de las actualizaciones de los Procedimientos de Seguridad en CitiDirect®. A menos que la ley lo disponga de otro modo, el uso continuo por parte del Cliente de cualquiera de los Servicios o los canales de conectividad mencionados anteriormente, tras ser informado sobre los Procedimientos de Seguridad actualizados constituirá la aceptación por parte del Cliente de dichos Procedimientos de Seguridad actualizados. Estos Procedimientos de Seguridad abarcan lo siguiente:

A. Authentication Methods
Métodos de Autenticación

B. Customer Responsibilities
Responsabilidades del Cliente

C. Data Integrity and Secured Communications
Integridad de los datos y comunicaciones seguras

D. Security Manager and Related Functions
Administrador de Seguridad y funciones relacionadas

2. Authentication Methods *Métodos de Autenticación*

The Security Procedures include certain secure authentication methods ("Authentication Methods") which are used to uniquely identify and verify the authority of the Customer and/or any of its users authorized by the Customer typically through one or a combination of mechanisms such as user ID/password pairs, digital certificates, biometrics, security tokens (deployed via hardware or software), seal/signature verification, and/or devices associated with the Authentication Methods (collectively, the "Credentials"). Authentication Methods and associated Credentials allow the Bank to verify the origin of Communications received by the Bank.

Los Procedimientos de Seguridad incluyen determinados métodos de autenticación seguros ("Métodos de Autenticación"), los cuales se utilizan para identificar y verificar exclusivamente la autoridad del Cliente o de cualquiera de los usuarios autorizados por el Cliente. En general, a través de un mecanismo o una combinación de mecanismos, tales como pares de ID de usuario/contraseña, certificados digitales, datos biométricos, tokens de seguridad (implementados por hardware o software), verificación de sello/firma, y/o dispositivos asociados con los Métodos de Autenticación (en conjunto, las "Credenciales"). Los Métodos de autenticación y las Credenciales asociadas permiten que el Banco verifique el origen de las comunicaciones recibidas por el Banco.

More information regarding Authentication Methods for access to Services and/or connectivity channels may be accessed on the CitiDirect® Login Help website. Customer may at any time select an available Authentication Method. During implementation of Services or connectivity channels, Bank may set-up a default Authentication Method, which Customer may change at any time to another available Authentication Method.

En el sitio web de ayuda para el inicio de sesión de CitiDirect® podrá obtener más información sobre los Métodos de Autenticación para acceder a los servicios o a los canales de conectividad. En cualquier momento, el Cliente podrá elegir un Método de Autenticación disponible. Durante la implementación de los servicios o los canales de conectividad, el Banco podrá definir un Método de Autenticación predeterminado, que podrá ser cambiado por el Cliente en cualquier momento por otro Método de Autenticación disponible.

The following Authentication Methods are available to access the services and/or connectivity channels:

Los siguientes Métodos de Autenticación están disponibles para acceder a los servicios o a los canales de conectividad.

CitiDirect® Authentication Methods *Métodos de Autenticación de CitiDirect®*	
Biometrics *Datos Biométricos*	A digital authentication method that utilizes a user's unique physical traits, (such as a fingerprint and facial recognition), built-in biometric technology on the user's mobile device, and cryptographic techniques to gain access to CitiDirect®. Physical trait data is not transferred to the Bank when the user selects this authentication method. *Método de autenticación digital que utiliza características físicas únicas del usuario (por ejemplo, una huella dactilar y reconocimiento facial), tecnología biométrica integrada en el dispositivo móvil del usuario y técnicas de cifrado para acceder a CitiDirect®. Los datos de características físicas no se transfieren al Banco cuando el usuario elige este método de autenticación.*
Mobile Token (non-application based) *Token móvil* *(no basado en aplicación)*	A digital non-application based mobile authentication method (e.g. Mobile Token (Appless)) that leverages cryptographic keys and biometric authentication (such as fingerprint and facial recognition) to link a user's mobile device to their CitiDirect account via the user's mobile browser. Physical trait data is not transferred to the Bank when the user selects this authentication method. This method facilitates multi-factor authentication by verifying the user's identity with their registered mobile device. *Un método de autenticación móvil digital sin aplicación (por ejemplo, token móvil (sin app)) que utiliza claves criptográficas y autenticación biométrica (como el reconocimiento facial y de huellas dactilares) para vincular el dispositivo móvil de un usuario a su cuenta CitiDirect a través del navegador móvil del usuario. Los datos de rasgos físicos no se transfieren al Banco cuando el usuario selecciona este método de autenticación. Este método facilita la autenticación multifactor al verificar la identidad del usuario con su dispositivo móvil registrado.*
Challenge Response Token *Token de Respuesta a pregunta de comprobación*	Either (i) a mobile application based soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco) which in each case is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). When accessing CitiDirect®, the system generates a challenge and a response passcode is generated by the utilized token and entered into the system. This authentication method, when combined with a secure password results in multifactor authentication. *Puede ser (i) una aplicación móvil basada en un token de software (p. ej., MobilePASS) o (ii) un token físico (p. ej., tarjeta SafeWord, Vasco), que, en cada caso, se utiliza para generar una contraseña dinámica tras realizar una autenticación con un PIN (p. ej., PIN de 4 dígitos). Cuando se accede a CitiDirect®, el sistema genera una pregunta de comprobación, y el token utilizado genera un código de acceso de respuesta y lo ingresa en el sistema. Cuando este método de autenticación se combina con una contraseña segura da lugar a una autenticación multifactor.*
One-Time Password Token *Token de contraseña por única vez*	Either (i) a mobile application soft token (e.g. MobilePASS) or (ii) a physical token (e.g. SafeWord Card, Vasco) that is used to generate a dynamic password after authenticating with a PIN (e.g. 4-digit PIN). This dynamic password is entered into the system to gain access. *Puede ser (i) una aplicación móvil basada en un token de software (p. ej., MobilePASS) o (ii) un token físico (p. ej., tarjeta SafeWord, Vasco), que se utiliza para generar una contraseña dinámica tras realizar una autenticación con un PIN (p. ej., PIN de 4 dígitos). Esta contraseña dinámica se ingresa en el sistema para poder acceder.*

CitiDirect® Authentication Methods ***Métodos de Autenticación de CitiDirect®***	
Secure Password *Contraseña Segura*	A user enters his or her secure password to access the system. A secure password typically limits a user's capabilities on the system, for example, by only permitting that certain information be viewed by the user. This authentication method, when combined with a challenge response token results in multifactor authentication. *El usuario ingresa su contraseña segura para acceder al sistema. En general, una contraseña segura limita las capacidades del usuario dentro del sistema, por ejemplo, cuando solamente permite ver determinada información. Cuando este método de autenticación se combina con un token de respuesta a pregunta de comprobación da lugar a una autenticación multifactor.*
SMS One-Time Code *Código por SMS enviado por única vez*	A dynamic password delivered to users via SMS, after which the user enters the dynamic password and a secure password to gain access to the system. *Se envía una contraseña dinámica por SMS al usuario, quien ingresa la contraseña dinámica y una contraseña segura para obtener acceso al sistema.*
Voice One-Time Code *Código de voz enviado por única vez*	A dynamic password delivered to users via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system. *Por medio de una llamada automática, se proporciona una contraseña dinámica al usuario, quien ingresa la contraseña dinámica y una contraseña segura para obtener acceso al sistema.*
Digital Certificates *Certificados digitales*	A digital certificate is an electronic identification issued by an approved certificate authority for authentication and authorization. Digital certificates may be attributed to corporate legal entities ("Corporate Seals") or individuals ("Personal Certificates"). The Customer is responsible for properly verifying the identity of all users of Personal Certificates acting on behalf of the Customer in accordance with local law. The Bank and the Customer are required to use digital certificates provided by authorized persons, to ensure all Communications exchanged via a public internet connection or an otherwise unsecure internet connection are fully encrypted and protected. *Un certificado digital es una identificación electrónica emitida por una autoridad de certificados aprobada para realizar autenticaciones y autorizaciones. Los certificados digitales pueden atribuirse a entidades jurídicas corporativas ("Sellos Corporativos") o a personas ("Certificados Personales"). El Cliente debe verificar adecuadamente la identidad de todos los usuarios de Certificados personales que actúan en nombre del Cliente, de conformidad con las leyes locales.* *El Banco y el Cliente tienen la obligación de usar los certificados digitales provistos por las personas autorizadas, a fin de garantizar que todas las Comunicaciones intercambiadas a través de una conexión pública a Internet o una conexión a Internet no segura estén completamente cifradas y protegidas.*

CitiConnect® for Files Authentication Methods *Métodos de Autenticación de CitiConnect® para Archivos*	
Digital Certificates *Certificados Digitales*	See description above. *Vea la descripción anterior.*

CitiConnect® for Files Authentication Methods *Métodos de Autenticación de CitiConnect® para Archivos*	
IP Address Whitelist When Using CitiConnect® *Lista de de Direcciones IP Aprobadas para CitiConnect®*	Certain Internet communications received by the Bank, for example, via a Virtual Private Network (VPN), may also rely on the parties exchanging information using pre-agreed Internet Protocol (IP) addresses. The Bank will only accept communications originating from the Customer's designated IP address, and vice versa, and the Bank will only transmit Communications to the Customer's designated IP address, and vice versa. Used in conjunction with Digital Certificate method above. *Determinadas comunicaciones por Internet recibidas por el Banco, por ejemplo, a través de una red virtual privada (VPN), también podrán acudir a terceros para intercambiar información con direcciones de protocolo de Internet (IP) previamente acordadas. El Banco solo aceptará comunicaciones que se originen en la dirección IP designada por el Cliente, y viceversa, y el Banco solo transmitirá Comunicaciones a la dirección IP designada por el Cliente y viceversa. Se utiliza junto con el método de Certificados Digitales mencionado anteriormente.*

CitiConnect® API Authentication Methods ***Métodos de Autenticación de CitiConnect® API***	
Digital Certificates *Certificados Digitales*	See description above. *Vea la descripción anterior.*
IP Address Whitelist When Using CitiConnect® *Lista de Direcciones IP Aprobadas para CitiConnect®*	See description above. *Vea la descripción anterior.*

CitiConnect® for SWIFT Authentication Methods ***Métodos de Autenticación de CitiConnect® para SWIFT***	
Digital Certificates *Certificados Digitales*	See description above. Can be used in conjunction with SWIFT Authentication method below. *Vea la descripción anterior. Se puede utilizar junto con el Método de Autenticación de SWIFT detallado abajo.*

CitiConnect® for SWIFT Authentication Methods *Métodos de Autenticación de CitiConnect® para SWIFT*	
SWIFT Authentication *Autenticación de SWIFT*	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWiFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. *Las comunicaciones que se envíen entre el Banco y el Cliente a través de la red de SWIFT, incluidas pero no limitadas a información de la cuenta, órdenes de pago e instrucciones de modificación o cancelación de tales órdenes, se autenticarán con procedimientos definidos en la Documentación Contractual de SWIFT (según enmiendas y complementos periódicos), la cual abarca sin limitarse a ello, sus Términos y Condiciones Generales y la Descripción del Servicio FIN, o según se establece en otros términos y condiciones que SWIFT pueda establecer. El Banco no está obligado a hacer más de lo que consta en los procedimientos de SWIFT para determinar quién es el emisor y la autenticidad de estas Comunicaciones.* *El Banco no asumirá ninguna responsabilidad por los errores ni las demoras que pudieran ocurrir en el sistema SWIFT. El Cliente debe remitir comunicaciones al Banco en el formato y el tipo requeridos y especificados por SWIFT.* *Las transmisiones y comunicaciones enviadas o recibidas por medio de centros de SWIFT están sujetas a las normas y reglamentaciones vigentes de SWIFT, incluidas las normas de membresía. El Cliente debe conocer y acatar las normas de mensajería de SWIFT.*

SWIFT Authentication Method ***Método de Autenticación de SWIFT***	
SWIFT Authentication (Direct Connection for Financial Institutions) *Autenticación de SWIFT (conexión directa para instituciones financieras)*	Communications sent between the Bank and the Customer via the SWIFT network, including, but not limited to, account information, payment orders, and instructions to amend or cancel such orders, will be authenticated using procedures defined in SWiFT's Contractual Documentation (as amended or supplemented from time to time) which includes without limitation its General Terms and Conditions and FIN Service Description or as set forth in other terms and conditions that may be established by SWIFT. The Bank is not obliged to do anything other than what is contained in the SWIFT procedures to establish the sender and authenticity of these Communications. The Bank is not responsible for any errors or delays in the SWIFT system. The Customer is responsible for providing communications to the Bank in the format and type required and specified by SWIFT. Transmissions and Communications sent or received via SWIFT facilities are subject to SWIFT rules and regulations in effect, including membership rules. The Customer is responsible for being familiar with and conforming to SWIFT messaging standards. *Las comunicaciones que se envíen entre el Banco y el Cliente a través de la red de SWIFT, incluidas pero no limitadas a información de la cuenta, órdenes de pago e instrucciones de modificación o cancelación de tales órdenes, se autenticarán con procedimientos definidos en la Documentación Contractual de SWIFT (según enmiendas y complementos periódicos), la cual abarca sin limitarse a ello, sus Términos y Condiciones Generales y la Descripción del Servicio FIN, o según se establece en otros términos y condiciones que SWIFT pueda establecer. El Banco no está obligado a hacer más de lo que consta en los procedimientos de SWIFT para determinar quién es el emisor y la autenticidad de estas Comunicaciones.* *El Banco no asumirá ninguna responsabilidad por los errores ni las demoras que pudieran ocurrir en el sistema SWIFT. El Cliente debe remitir comunicaciones al Banco en el formato y el tipo requeridos y especificados por SWIFT.* *Las transmisiones y comunicaciones enviadas o recibidas por medio de centros de SWIFT están sujetas a las normas y reglamentaciones vigentes de SWIFT, incluidas las normas de membresía. El Cliente debe conocer y acatar las normas de mensajería de SWIFT.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Métodos de Autenticación de Firmas Electrónicas/Digitales para presentación de documentos electrónicos***	
Digital Signature *Firma Digital*	A type of electronic signature that leverages digital certificates to validate the authenticity and integrity of a signature, message, software or digital document. *Se trata de un tipo de firma electrónica que utiliza certificados digitales para validar la autenticidad e integridad de una firma, de un mensaje, de un software o de un documento digital.*

Digital/Electronic Signature Authentication Methods for Electronic Document Submission ***Métodos de Autenticación de Firmas Electrónicas/Digitales para presentación de documentos electrónicos***	
Electronic Signature *Firma Electrónica*	An electronic symbol attached to a contract or other record, unique to and used by a person with an intent to sign. Electronic signatures can be established in the form of words, letters, numerals, symbols, click of a button on a website, upload of facsimile or scan of a physical signature, signing on a touchscreen, or agreeing to any terms and conditions by electronic means. Created under the sole control of the person using it, it is logically attached to or associated with a data message capable of identifying the person who consents to the data message and certifying the person's consent. Such Electronic Signature would be submitted to the Bank through the Bank's electronic channels and in compliance with the associated Authentication Methods described above. *Se trata de un símbolo electrónico adosado a un contrato o a otro registro, que es exclusivo de una persona y es usado por esta con la intención de estampar una firma. Las firmas electrónicas pueden establecerse en forma de palabras, letras, numerales, símbolos,* *clic en un botón de un sitio web, carga de un fax o escaneo de una firma física,* *firma en una pantalla táctil o aceptación de términos y condiciones por medios electrónicos. Esta firma se genera conforme al control exclusivo de la persona que la utiliza y, lógicamente se la adjunta o asocia a un mensaje de datos, permite identificar a la persona que acepta enviar el mensaje de datos y certifica su consentimiento. Dicha Firma electrónica se remite al Banco a través de los canales electrónicos del Banco y conforme a los Métodos de autenticación asociados descritos anteriormente.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Método de Autenticación de Transferencias de Fondos Iniciadas Manualmente (MIFT)***	
MIFT Authentication *Autenticación de MIFT*	Manually Initiated Funds Transfer (MIFT), including amendments, recalls, or cancellations of previous manual instructions, may be made by fax or letter or upload to CitiDirect®. Not all forms are supported in all countries. Initiators are persons designated by the Customer who are authorized to initiate transactions in accordance with restrictions, if any, are identified by the Customer. Confirmers are person designated by the Customer that Bank may call back, at its discretion, for confirmation of manually initiated instructions for funds transfers. In certain countries, mobile telephone numbers are not accepted as call back numbers. Further details are provided in the applicable Country Cash Management User Guide, Global Manual Transaction Authorization or Universal Nomination Form. MIFT is to be used by the Customer as a contingency method to communication instructions to the Bank. *Las Transferencias de Fondos Iniciadas Manualmente (MIFT), incluidas las enmiendas, los retiros o las cancelaciones de instrucciones manuales previas, pueden realizarse por fax o por carta, o cargarse en CitiDirect®. No todos los medios están disponibles en todos los países. Los iniciadores son personas designadas por el Cliente, quien autoriza a iniciar transacciones según las restricciones que haya establecido, si corresponde. Los confirmadores son personas designadas por el Cliente, a quienes puede llamar el Banco, según su criterio, para que confirmen las instrucciones iniciadas manualmente respecto de las transferencias de fondos.*

Manual Initiated Funds Transfer (MIFT) Authentication Method ***Método de Autenticación de Transferencias de Fondos Iniciadas Manualmente (MIFT)***	
	En algunos países, no se aceptan números de teléfono celular como números de contacto para confirmación. Podrá obtener más información en la Guía de Administración de Efectivo del país que corresponda, en la Autorización Global de Transacciones Manuales o en el Formulario de Nominación Universal. El Cliente debe utilizar las MIFT como método de contingencia para impartir instrucciones al Banco.

Mail, Fax, Email and Messenger Authentication Methods ***Métodos de Autenticación por Correo Postal, Fax, Correo Electrónico y Mensajería***	
Seal Image Verification *Verificación de imagen de sello*	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are verified and collated with due care based on the seal image contained in the Customer's authority document or similar document provided to the Bank. *La correspondencia que reciba el Banco por fax, correo postal o electrónico, o mensajería, a excepción de las solicitudes de MIFT, se verifica y coteja con el debido cuidado, según la imagen del sello que consta en el documento de autoridad del Cliente o un documento similar entregado al Banco.*
Signature Verification *Verificación de firma*	Correspondence received by the Bank via fax, mail, email or messenger, excluding MIFT requests, are signature verified based on the information contained in the Customer's authority document or similar document provided to the Bank. *La correspondencia que reciba el Banco por fax, correo postal o electrónico, o mensajería, a excepción de las solicitudes de MIFT, se verifica con firma según la información del documento de autoridad del Cliente o un documento similar entregado al Banco.*
Secure PDF *PDF seguro*	Encrypted emails are delivered to a regular mailbox as PDF documents that are opened by entering a private password. Both the message and body and any attached files are encrypted. A private password can be set up upon receipt of the first secure email received. *Los mensajes de correo electrónico cifrados se entregan a una casilla de correo normal como documentos en formato PDF que se abren al introducir una contraseña privada. Tanto el cuerpo del mensaje como los archivos adjuntos están cifrados. Es posible configurar una contraseña privada al recibir el primer mensaje de correo electrónico seguro.*
MTLS *MTLS*	Mandatory Transport Layer Security (MTLS) creates what would be a secure, private email connection between the Bank and the Customer. Emails transmitted using this channel are sent over the Internet through an encrypted TLS tunnel created by the connection. *La Seguridad de la Capa de Transporte Obligatoria (MTLS) crea una conexión de correo electrónico segura y privada entre el Banco y el Cliente. Los mensajes de correo electrónico que se transmiten por este canal se envían por Internet a través de un túnel TLS cifrado creado por la conexión.*

Phone Authentication Methods *Métodos de Autenticación por Teléfono*	
PIN *PIN*	Customers contacting the Bank via phone are prompted to enter a PIN to validate authorized access. *Los Clientes que se comuniquen con el Banco por teléfono deberán introducir un PIN para validar el acceso autorizado.*
Verification Questions *Preguntas de verificación*	Customers contacting the Bank via phone are prompted by the Bank's service representatives to provide correct verbal responses to verification questions in order to validate authorized access. *Los representantes de servicio del Banco les solicitan a los Clientes que se comunican con el Banco por teléfono que respondan verbalmente de manera correcta las preguntas de verificación para validar el acceso autorizado.*

The availability of Authentication Methods described above varies based on local markets.
La disponibilidad de los Métodos de Autenticación que se describen anteriormente varía según los mercados locales.

3. Customer Responsibilities
Responsabilidades del Cliente

3.1 Identifying Authorized Users: Customer is responsible for identifying: (i) all individuals acting on the Account(s) on behalf of the Customer at an entity level for all Services and connectivity channels, and (ii) each person acting on behalf of the Customer being duly authorized by the Customer to act on the Customer's Account.

Identificar a los Usuarios Autorizados: El Cliente debe identificar: (i) a todos los individuos que interactúen con la(s) Cuenta(s) en nombre del Cliente a nivel de entidad, para todos los Servicios y canales de conectividad y (ii) a cada persona que actúe en nombre del Cliente y que esté debidamente autorizada por el Cliente para actuar en la cuenta del Cliente.

3.2 Customer is responsible for assigning and monitoring any transaction limits assigned to the Customer and/or its users and ensuring that these limits (a) do not exceed the limits as required by the Customer's internal policies and other authority and constitutive documents such as Customer's Board of Director resolutions, Bank Mandates, Power Of Attorney, or equivalent document, and (b) are properly reflected on all connectivity channels and user entitlements.

El Cliente es responsable de asignar y controlar los límites de sus transacciones y las de sus Clientes y/o usuarios, además de verificar que estos límites (a) no superen los determinados por las políticas internas del Cliente y otros documentos constitutivos o de autoridad tales como resoluciones de la Junta Directiva del Cliente, Órdenes del Banco, Poderes Notariales o documentos equivalentes, y (b) que estén registrados adecuadamente en todos los canales de conectividad y derechos del usuario.

3.3 Certain jurisdictions may require individuals (and their corresponding Credentials) to be identified by the Bank in accordance with applicable AML legislation requirements before granting access to perform certain functions. Please contact your Customer Service Representative or visit the CitiDirect® website for further information.

En determinadas jurisdicciones, se requiere que los individuos (y sus correspondientes Credenciales) sean identificados por el Banco según lo establecen los requisitos de la legislación de AML antes de que se les otorgue acceso para llevar a cabo determinadas funciones. Comuníquese con un Representante del Servicio al cliente o visite el sitio web de CitiDirect® si desea obtener más información.

3.4 Safeguarding of Authentication Methods
Protección de los Métodos de Autenticación

The Customer is responsible for safeguarding the Authentication Methods and Credentials with the highest standard of care and diligence, and ensuring that access to and distribution of the Credentials are limited only to persons that have been authorized by the Customer.

Communications sent by a third party: Where the Customer is using a Credential to identify and authenticate their Communications as originating from them as a legal entity, the Customer is responsible for exercising full control over the use of such Credentials when sending Communications to the Bank, including where such Communications are sent by applications and/or systems that are managed by a third party on behalf of the Customer. In all circumstances the Bank will (a) deem any Communication it receives through an electronic connectivity channel, that has been received by the Bank in compliance with these Security Procedures duly authenticated as originating from the Customer, as a Communication instructed by the Customer and (b) may act upon any Communication that it receives on behalf of the Customer in compliance with these Security Procedures.

El Cliente es responsable de proteger los Métodos de Autenticación y las Credenciales con el mayor nivel de atención y diligencia, y garantizar que el acceso a las Credenciales y su correspondiente distribución se limiten exclusivamente a las personas a quien el Cliente haya autorizado.

Comunicaciones enviadas por terceros: En los casos en que el Cliente utilice una Credencial para identificar sus comunicaciones y autenticarlas como originadas en este en carácter de entidad jurídica, el Cliente es responsable de ejercer el control total sobre el uso de dichas Credenciales cuando envíe Comunicaciones al Banco, incluso cuando éstas sean enviadas en nombre del Cliente por aplicaciones y/o sistemas gestionados por terceros. En todos los casos, el Banco (a) considerará que toda Comunicación enviada por un canal de conectividad electrónico ha sido recibida por el Banco de conformidad con estos Procedimientos de Seguridad, y que se autenticó debidamente que fue originada por el Cliente como una Comunicación indicada por éste y (b) podrá actuar según cualquier comunicación que reciba en nombre del Cliente de acuerdo con estos Procedimientos de Seguridad.

4. Data Integrity and Secured Communications
Integridad de los datos y comunicaciones seguras

4.1 The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the internet, mail, email and/or fax which the Customer understands are not (i) necessarily secure communications and delivery systems, and (ii) under the Bank's control. The Customer further understands that if Customer's users are entitled to access Open Banking and/or similar third-party platforms outside of the Citi systems, Customer data could be transmitted over such third-party platforms which are not under the Bank's control.

El Cliente transmitirá datos al Banco e intercambiará comunicaciones con el Banco mediante el uso de Internet, correo postal, correo electrónico o fax, que el Cliente entiende que (i) no son sistemas de comunicación y entrega necesariamente seguros y (ii) no están bajo el control del Banco. El Cliente entiende además que si los usuarios del Cliente tienen derecho a acceder a Open Banking o a plataformas similares de terceros fuera de los sistemas del Citi, los datos del Cliente podrían transmitirse a través de dichas plataformas de terceros que no están bajo el control del Banco.

4.2 The Bank, utilizes industry leading encryption methods (as determined by the Bank), which help to ensure that information is kept confidential and that it is not changed during electronic transit.

El Banco utiliza los mejores métodos de cifrado de la industria (según el criterio del Banco), los cuales garantizan la confidencialidad de la información y que ésta no sea modificada durante el tránsito electrónico.

4.3 If the Customer suspects or becomes aware of a technical failure or any improper or potentially fraudulent access to or use of the Bank's Services or connectivity channels or Authentication Methods by any person (whether an authorized person or not), the Customer shall promptly notify the Bank of such occurrence. In the event of improper or potentially fraudulent access or use by an authorized person, the Customer should take immediate actions to terminate such authorized person's access to and use of the Bank's Services or connectivity channels.

Si el Cliente sospecha que una persona (sea autorizada o no) ha producido una falla técnica, un acceso o uso inadecuado o potencialmente fraudulento de los Servicios de los canales de conectividad o de los Métodos de Autenticación del Banco, o toma conocimiento de estos hechos, el Cliente deberá notificar de inmediato al Banco. En caso de que una persona autorizada acceda a éstos o los utilice de manera inadecuada o potencialmente fraudulenta, el Cliente deberá tomar medidas de inmediato para cancelar el acceso a los Servicios o a los canales de conectividad del Banco y el uso de éstos por parte de dicha persona.

4.4 If the Customer utilizes file formatting or encryption software (whether provided by the Bank or a third party) to support the formatting and recognition of the Customer's data and instructions and acts upon Communications with the Bank, the Customer will use such software solely for the purpose for which it has been installed.

Si el Cliente utiliza software de cifrado y formato de archivos (sea este provisto por el Banco o por un tercero) para respaldar el formateo y el reconocimiento de los datos e instrucciones del Cliente y actúa conforme a las Comunicaciones con el Banco, el Cliente utilizará dicho software únicamente para el propósito para el que ha sido instalado.

4.5 The Customer accepts that the Bank may suspend or deny users' access to Services requiring the use of Credentials (i) in case of suspicion of unauthorized or fraudulent use of the Credentials and/or (ii) to safeguard the Services or Credentials.

El Cliente acepta que el Banco podrá suspender o denegar el acceso de los usuarios a los Servicios que requieren el uso de Credenciales (i) si existe la sospecha de que se las ha usado de manera fraudulenta o no autorizada o (ii) para proteger los Servicios o las Credenciales.

5. Security Manager and Related Functions *Administrador de Seguridad y funciones relacionadas*

For applications accessible in CitiDirect® and CitiConnect® (with the exception of Personal Certificates discussed below), the Bank requires the Customer to establish a "Security Manager" function. Security Managers are responsible for:

En el caso de las aplicaciones disponibles en CitiDirect® (a excepción de los Certificados Personales analizados a continuación), el Banco exige que el Cliente defina una función de "Administrador de Seguridad". Los Administradores de Seguridad tienen las siguientes responsabilidades:

5.1 Establishing and maintaining the access and entitlements of users (including Security Managers themselves) including activities such as: (a) creating, deleting or modifying user Profiles (including Security Manager Profiles) and entitlement rights (Note that user name must align with supporting identification documents); (b) building access profiles that define the functions and data available to individual users; (c) enabling and disabling user log-on credentials; and (d) assigning transaction limits (Note these limits are not monitored or validated by the Bank and Customer should monitor these limits to ensure they are in compliance with the Customer's internal policies and requirements, including but not limited to, those established by the Customer's Board of Directors or equivalent);

Establecer y mantener el acceso y los privilegios de los usuarios (incluidos los mismos Administradores de seguridad), incluidas actividades como las que se enumeran a continuación: (a) crear, eliminar o modificar los

Perfiles de usuario (incluidos los Perfiles de Gerentes de seguridad) y los derechos (Tenga en cuenta que el nombre de usuario debe ser acorde a los documentos de identificación de respaldo); (b) diseñar perfiles de acceso que definan las funciones y los datos disponibles para los usuarios individuales; (c) habilitar y deshabilitar credenciales de inicio de sesión de usuarios; y (d) asignar límites de las transacciones (estos límites no son controlados ni validados por el Banco, sino que el Cliente debe controlarlos para garantizar que cumplan con las políticas y requisitos internos del Cliente, incluidos, entre otros, aquellos establecidos por su Junta Directiva o equivalente).

5.2 Creating and modifying entries in Customer maintained libraries (such as preformatted payments and beneficiary libraries) and authorizing other users to do the same;

Crear y modificar entradas en las Librerías del Cliente (por ejemplo, pagos con formato previo y Librerías de beneficiarios) y autorizar a otros usuarios a que hagan lo mismo.

5.3 Modifying payment authorization flows;

Modificar los flujos de autorización de pagos.

5.4 Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users;

Asignar credenciales de contraseña dinámica u otras credenciales o contraseñas de acceso al sistema a los usuarios del Cliente.

5.5 Notifying the Bank, if there is any reason to suspect that security has been compromised; and

Notificar al Banco si hubiese razones para sospechar que la seguridad se ha visto amenazada y

5.6 Managing and procuring digital certificates and authorizing other users to do the same.

Gestionar y obtener certificados digitales y autorizar otros usuarios para hacer lo mismo.

Please note: Security Manager roles and responsibilities may vary or not be applicable in certain markets due to regulatory requirements and/or operational capabilities. In such markets, the Bank may require additional documentation and other information from the Customer to perform Security Manager functions on behalf of the Customer.

Tenga en cuenta lo siguiente: Los roles y las responsabilidades del Administrador de Seguridad pueden variar en determinados mercados o no aplicarse a éstos debido a requisitos reglamentarios o capacidades operativas. En tales mercados, el Banco podrá exigir que el Cliente presente documentación adicional y otra información para llevar a cabo las funciones del Administrador de Seguridad en nombre del Cliente.

6. Use of CitiDirect® and CitiConnect® by Security Managers *Uso de CitiDirect® y CitiConnect® por parte de los Administradores de Seguridad*

The Bank requires two (2) separate individuals to input and authorize instructions; therefore, a minimum of two Security Managers are required. Any two Security Managers, acting in concert, are able to give instructions and/or confirmations through the connectivity channels in relation to any Security Manager function or in connection with facilitating communications. Any such communications, when authorized by two Security Managers, will be accepted and acted on by the Bank and deemed to be given by the Customer. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate Customer's Security Managers on the TTS Channels Onboarding Form. A Security Manager of the Customer may also act as the Security Manager for a third party entity (for instance, an affiliate of the Customer) and exercise all rights relating thereto (including the appointment of users for that third party entity's Account(s)), without any further designation, if that third party entity executes a Universal Access Authority form (or such other form of authorization acceptable to the Bank) granting the Customer access to its account(s). This only applies in relation to Account(s) covered under the relevant authorization.

El Banco exige que dos (2) personas distintas ingresen y autoricen las instrucciones; por ello, se requieren dos Administradores de Seguridad como mínimo. Cualquiera de estos dos Administradores de Seguridad, que trabajen conjuntamente, pueden dar instrucciones o confirmaciones a través de los canales de conectividad en relación con cualquier función de los Administradores de seguridad o de la facilitación de las comunicaciones. Cuando dos Administradores de Seguridad autoricen este tipo de comunicaciones, el Banco las aceptará y actuará en consecuencia, y considerará que las proporcionó el Cliente. El Banco recomienda designar al menos tres Administradores de Seguridad, a fin de garantizar un respaldo adicional. El Cliente deberá designar los Administradores de Seguridad en el Formulario de Activación de Canales TTS. El Administrador de Seguridad del Cliente también puede desempeñar el mismo puesto en una entidad externa (por ejemplo, una empresa afiliada del Cliente) y ejercer todos los derechos relacionados con esta función (que incluyen la designación de usuarios para las Cuentas de la entidad externa), sin que sea necesaria ninguna otra designación, en caso de que la entidad externa ejecute el formulario de Autorización de Acceso Universal (o algún otra formulario de autorización similar que el Banco acepte) en el que se le concede acceso a las cuentas del Cliente. Esto solo corresponde a las Cuentas incluidas en virtud de la autorización relevante.

7. Use of CitiDirect® by Security Officers (For Personal Certificates only) *Uso de CitiDirect® por parte de los Oficiales de Seguridad (solo para Certificados Personales)*

The Bank requires two (2) separate individuals to manage digital certificates attributed to individuals ("Personal Certificates"). Therefore, two Security Officers are required to assign and remove Personal Certificates to users, for the purpose of authenticating and authorizing Communications on the connectivity channels. The Bank recommends the designation of at least three Security Officers to ensure adequate backup. Any Communications authorized by Personal Certificates will be accepted and acted on by the Bank and deemed to be given by the Customer.

El Banco exige que dos (2) personas distintas gestionen los certificados digitales que se asignan a individuos ("Certificados Personales"). Por ello, se requiere que dos Oficiales de Seguridad asignen y eliminen Certificados Personales, a fin de autenticar y autorizar las Comunicaciones por los canales de conectividad. El Banco recomienda designar al menos tres Oficiales de Seguridad, a fin de garantizar un respaldo adecuado. Cuando una comunicación está autorizada por un Certificado Personal, el Banco la aceptará y actuará en consecuencia, y considerará que la proporcionó el Cliente.

Treasury and Trade Solutions
citi.com/treasuryandtradesolutions