Cash Management

Manual del Usuario

Ecuador

Tabla de Contenido

I. Introducción

Gracias por elegir los productos transaccionales de Citi (TTS) para atender las necesidades de Cash Management de su negocio. El objetivo de este Manual de Usuario es proporcionarle un manual que contenga información detallada de los servicios disponibles para usted, el mismo que debe leerse junto con los términos y condiciones de su Cuenta. Citi y el Banco pueden usar esta Guía indistintamente para actualizar periódicamente cualquier cambio que se comunicará a través de nuestros canales regulares.

II. Servicios de Pago

A. Tipos de Servicios de Pago en Ecuador

- Transferencia de cuentas propias: Transferencias de fondos entre cuentas en Citi Ecuador
- Transferencias Interbancarias: Transferencias a cuentas en otros bancos locales que forman parte del Sistema de Pagos Interbancarios (SPI) del Banco Central del Ecuador. Una vez que hayan sido autorizados en la plataforma, los pedidos no pueden ser anulados por el Banco o el Cliente. El tiempo límite para acreditar los valores enviados pueden variar dependiendo delo los horarios de corte que disponga el beneficiario.
- Transferencias de fondos al exterior: Permite a los clientes transferir fondos a cuentas en otros países en diferentes monedas. El proceso puede involucrar el uso de bancos corresponsales u otros intermediarios y puede estar sujeto a cargos adicionales.
- Cheques: instrumentos en papel, los mismos que pueden pasar de una persona o entidad a otra e intercambiarse por dinero. Un cheque instruye incondicionalmente a un banco a pagar un monto específico en una moneda específica a una persona específica, a un "portador" o a "efectivo. El Banco, a solicitud del Cliente, emitirá libros de cheques pre impresos que se pueden utilizar para iniciar pagos a los beneficiarios de los Clientes. Los talonarios de cheques se habilitarán en el sistema del Banco 24 horas después de ser recibidos por el Cliente. El Banco llevará cheques para su retiro durante 90 días, luego de lo cual el Banco los destruirá

B. Envío de un pago

1. El cliente envía una instrucción de pago a Citi, con un formato de acuerdo a los estándares del mercado y como se describió en el momento en que se implementó el servicio de pago, a través de:
    - Canales Citi e-Banking, los mismos que incluyen CitiDirect BE® y CitiConnect®,
    - Interface SWIFT, o
    - Una solicitud manual (consulte la Sección IV para obtener detalles sobre las transacciones manuales)

    En ciertos casos, las instrucciones dadas fuera de un horario determinado serán procesadas el siguiente día hábil.

    El Banco no está obligado a sobregirar la Cuenta del Cliente para cumplir con las instrucciones de pago, pero si lo hace el Cliente debe cubrir el sobregiro y los cargos asociados.

2. Citi reenvía las instrucciones al sistema de pago correspondiente para su posterior procesamiento.

3. El sistema de pago reenvía las instrucciones al banco beneficiario en función del ciclo de compensación definido localmente.

4. El banco beneficiario acredita a la cuenta del beneficiario en un horario determinado según el ciclo de compensación y el tipo.

C. Cheques Paylink®

A través de la plataforma de banca electrónica, el Cliente puede ordenar la emisión de cheques o cheques Paylink® para ser recogidos por los beneficiarios, o sus representantes autorizados, en los cajeros del Banco. Si el cliente lo solicita, puede ver los cheques emitidos y firmados por los beneficiarios en la aplicación Biblioteca digital.

Asegurar y procesar Cheques Paylink

1. El cliente comunica instrucciones para imprimir y emitir cheques a través del canal de banca electrónica acordado.

2. Citi imprime los cheques establecidos en la Cuenta del Cliente, con las firmas de los funcionarios del Banco. Los oficiales cuyas firmas están impresas en los cheques no son responsables del contenido de los cheques, ni de su uso.

3. Citi hace que los cheques estén disponibles para ser recogidos por los beneficiarios según lo especificado en las instrucciones del Cliente. Los cheques que no se han recogido dentro de 90 días posteriores a la fecha de emisión serán devueltos al Cliente por el Banco.

4. Los cheques son depositados por el beneficiario y se presentan a Citi mediante acuerdos locales. Los cheques también se pueden presentar y cobrar en el mostrador en sucursales o ubicaciones de extensión de red del Banco.

5. Los cheques son validados y publicados en la Cuenta del Cliente para su liquidación una vez que los fondos han sido puestos disponibles.

6. Citi no realizará el pago si considera que un cheque o giro ha sido alterado, falsificado, robado, o a petición de una autoridad judicial, cuasi judicial, regulatoria, gubernamental o de supervisión competente.

7. Si los cheques o giros se pierden, son robados, destruidos, caducados o inválidos, el Cliente debe informar a Citi por escrito según los formatos acordados previamente para detener el pago. A pedido del Cliente, Citi puede emitir un nuevo cheque o acreditar en la Cuenta del Cliente. Si se encuentra más tarde el cheque o giro perdido, extraviado o robado, el Cliente debe entregar el cheque o giro original a Citi inmediatamente.

El Cliente puede solicitar ver, a través de la plataforma bancaria en línea del Banco, los cheques emitidos y firmados por el beneficiario.

D. Revocatoria y Suspensión de pagos

Toda instrucción de pago confirmada por el Cliente y aceptada por el Banco es definitiva e irrevocable a partir de la aceptación de dichas instrucciones por parte del Banco. El Banco no incurrirá en ninguna responsabilidad ante el Cliente ni ante terceros con respecto a esto, ya sea que dicho pago haya sido realizado o no.

Las órdenes de suspensión de pago se procesarán en el siguiente método:

1. Antes de realizar el pago, el Cliente enviará una orden de suspensión utilizando la plataforma de banca electrónica proporcionada por el Banco.

2. Después que se haya emitido el pago, el Cliente seguirá las instrucciones del Banco para las suspensiones de pago de acuerdo con las leyes y prácticas comerciales aplicables y enviará una solicitud por escrito al Banco.

E. Recepción de débitos directos (pagos)

Citi, como el Banco pagador del Cliente, soporta los débitos directos recibidos de otras instituciones financieras participantes o bancos asociados.

1. Si el pago de débito directo cumple con la autorización de débito, Citi procesa las instrucciones y debita la Cuenta del Cliente de acuerdo con los procedimientos del Banco Central del Ecuador para débitos directos (SCI- Sistema de Cobros Interbancarios).

2. Citi se comunica con la institución financiera recaudadora a través del sistema de compensación o con los bancos del sistema financiero para conocer sobre rechazos o retornos positivos o negativos. En el caso de que no haya fondos suficientes en la Cuenta del Cliente, Citi no procesará el pago de débito directo y enviará el estado de débito fallido nuevamente al sistema de pago de débito directo.

Citi revertirá cualquier entrada aprobada erróneamente y debitará o acreditará la Cuenta relevante.

F. Notificación al beneficiario

Las notificaciones a los beneficiarios se pueden utilizar para informar o notificar a los beneficiarios del estado y los detalles de los pagos para facilitar la conciliación de las transacciones. Las notificaciones a los beneficiarios se envían por correo electrónico a los beneficiarios respectivos, que pueden acceder a los detalles de pago a través de un enlace al Online Payment Channel (OLPC).

El Cliente, al emitir instrucciones a través del sistema bancario electrónico designado para pagos (cheques o transferencias de fondos) a sus beneficiarios, puede autorizar al Banco a notificar a los beneficiarios que identifica que utilizan el servicio de Pago en línea del nuevo pago o crédito en sus cuentas. El Banco proporcionará el método (cheque o transferencia electrónica de fondos) y la fecha en que se efectuará el pago. Esta información estará disponible hasta 3 meses desde el momento en que se ha efectuado el pago.

G. Comprobantes de impuestos y retenciones

El Banco puede poner a disposición comprobantes de retención de impuestos pre impresos que los proveedores del Cliente puedan obtener en las cajas del Banco. El Cliente debe proporcionarle al Banco todos los comprobantes de retención de impuestos 48 horas antes de la emisión de un cheque de Paylink® al proveedor. El cliente instruirá al Banco sobre el contenido de los comprobantes de impuestos y las notas de retención. Cuando un pago se realiza a través de una transferencia de fondos interbancaria, el comprobante del impuesto de retención se entregará al Cliente o se pondrá a disposición del beneficiario en las oficinas del Banco. El Cliente puede solicitar ver, a través de la plataforma en línea del banco, los comprobantes de pago que han sido firmados por los beneficiarios.

III. Servicios de Cobranza

A. Recibir un Pago

1. El sistema de compensación reenvía las instrucciones a Citi en función del ciclo de compensación definido localmente.

2. Citi acredita la cuenta.

Cualquier rechazo o devolución por parte de Citi se acreditará nuevamente a la cuenta del pagador. El motivo de la devolución se comunica al pagador.

B. Cobranza de Débito Directo

Un cobro con débito directo es una transacción financiera originada electrónicamente por el Cliente que ordena al Banco debitar fondos de la cuenta bancaria de un tercero, ya sea a través de transacciones interbancarias o de cuenta a cuenta de un mismo banco.

El Cliente puede autorizar al Banco a debitar sus cuentas con el fin de acreditar a cuentas de terceros los servicios que prestan o los pagos periódicos adeudados. Esta autorización otorga autoridad a dichos terceros para la entrega de fondos según se indique.

El Cliente necesita instruir al Banco mediante carta, y para instruir a un tercero, proveedor de servicios, para que suspenda o cancele el servicio por todos los débitos realizados por un tercero. El Banco procederá a detener los débitos una vez notificado por el proveedor del servicio. Tomará 3 días hábiles devolver las instrucciones y completar el proceso. En casos de suspensión o finalización de servicios o servicios públicos manejados por un tercero, la instrucción debe enviarse a un tercero para su procesamiento.

En el caso de que no haya fondos en la cuenta para hacer el (los) débito (s) al tercero, el Banco no realizará el débito.

C. Cobranzas Interbancarias

A través de este servicio, el Cliente puede acceder al Sistema de Cobranza Interbancario (SCI), que permite el cobro de los pedidos con cargo en las instituciones financieras participantes en Ecuador. El Cliente puede instruir al Banco para que debite la cuenta del pagador en la institución del pagador. El pagador debe haber autorizado previamente las órdenes de cobro de débito del Cliente por escrito, que el Cliente debe mantener en archivo. Las Órdenes de Cobranza confirmadas por el Cliente y aceptadas por el Banco son definitivas e irrevocables.

El Cliente obtendrá, registrará y almacenará las autorizaciones de débito por escrito emitidas por los pagadores para llevar a cabo las cobranzas a través de SCI. Si el Banco exige pruebas o copias de estas autorizaciones, el Cliente debe enviarlas dentro de las 24 horas posteriores a la solicitud.

Las cobranzas de débito de ACH pueden revertirse debido a un reclamo del pagador, por órdenes del Banco Central del Ecuador. Si por alguna razón no hay fondos suficientes en cualquiera de las cuentas del Cliente en el Banco en el momento en que se produce dicha devolución, el Cliente debe reembolsar los costos en que incurra el Banco para cumplir con la obligación, incluidos los cargos por sobregiro, si corresponde.

El Banco, de conformidad con la ley, retendrá los impuestos en la fuente para cada orden de recogida que el Cliente identifique en el sistema. Cada mes, el Banco le proporcionará al cliente una prueba del impuesto retenido que incluye los impuestos a la retención para las transacciones de orden de cobranza ejecutadas durante el mes.

El banco del pagador puede cobrarle al pagador cargos o gastos adicionales.

Proceso de Cobranzas Interbancarias

El Cliente generará pedidos de cobranza a través del canal de banca electrónica de Citi, ya sea mediante ingreso manual o archivos masivos conforme a las condiciones determinadas por el Banco.

1. El cliente enviará ordenes de cobro mediante la plataforma electrónica de Citi ya sea por ingreso manual o carga de archivos masivos bajo las condiciones determinadas por el banco.
2. Citi valida que las solicitudes de transacción contengan la información requerida para procesarlas.
3. Citi comunica las transacciones de débito de ACH a los bancos pagadores receptores a través del sistema SCI.
4. Citi acredita los fondos a la Cuenta del Cliente dentro del tiempo acordado sujeto a que el Banco reciba los fondos.
5. El Cliente podrá ver el cargo o el rechazo en el canal de banca electrónica de Citi.

D. Recaudaciones Identificadas– Speed Collect

Speed Collect es un servicio mediante el cual el Banco acepta depósitos de terceros en nombre del Cliente para que pueda realizar los detalles de la transacción, incluida cierta información sobre el depositante / pagador, disponible en el canal de banca electrónica de Citi.

El Cliente solicitará al proveedor autorizado del Banco que emita y entregue los recibos de depósito de Speed Collect en los que se establecerán los detalles de la transacción, la información del depositante / pagador y el número de referencia. Los recibos de depósito, que deben cumplir con los requisitos proporcionados por el Banco, pueden ser impresos por el Cliente antes de recibir la autorización del Banco, lo que verificará el cumplimiento de los requisitos. El costo de la impresión de los recibos de depósito de Speed Collect será cubierto directamente por el Cliente.

El Banco asignará hasta 15 cuentas (subcuentas) seleccionadas por el Cliente con el exclusivo propósito de recibir depósitos. Las cuentas de cobro no generarán ningún costo adicional para el Cliente. El Banco concentrará los fondos de la (s) subcuenta (s) a la cuenta principal del Cliente electrónicamente y diariamente. No habrá un estado de cuenta impresa para las actividades de las subcuentas de cobranza. La información estará disponible a través del canal de banca electrónica de Citi.

IV. Instrucciones manuales de pago

Citi ofrece a sus Clientes la posibilidad de iniciar instrucciones manuales o la transferencia de fondos iniciadas manualmente (MIFT) en caso de contingencia u otros escenarios que puedan implicar una instrucción manual, incluida la modificación, el retiro o la cancelación de las instrucciones previas. Regulaciones específicas de los países pueden aplicarse a MIFT.

Para habilitar esta funcionalidad, el Cliente debe completar el Formulario Global de Autorización de Transacciones Manual (GMTA), que complementa la Cuenta Maestra y los Términos del Servicio (MAST), y cualquier otro término y condición de la cuenta aplicable. El formulario GMTA debe estar firmado por los firmantes autorizados según se detalla en la Resolución del Consejo del Cliente o su equivalente.

El formulario GMTA identifica a aquellas personas que están autorizadas a iniciar y confirmar instrucciones por medios manuales, en nombre del Cliente.

Los clientes que no proporcionan un formulario GMTA al Banco y, por lo tanto, no tienen capacidad de pago de MIFT, entienden que los medios manuales de la comunicación no estarán disponibles para ellos en el caso de que se requieran para contingencia u otros escenarios aplicables que puedan implicar instrucciones manuales.

Notas para Completar el Formulario GMTA

1. La instrucción manual se puede enviar a Citi a través de cualquiera de los siguientes modos de comunicación. Seleccione la(s) opción(es) que desea activar en el formulario GMTA:

   - Carta
   - Fax

   Comuníquese con su representante de Citi para obtener detalles adicionales

2. Los iniciadores pueden hacerse disponibles solo con la Opción 1 en el formulario GMTA

3. Por favor proporcione al menos dos contactos para para confirmación telefónica. Citi recomienda que los contactos estén ubicados en la misma zona horaria del país donde se encuentra la cuenta del cliente.

4. Al completar el formulario de GMTA, el Cliente debe establecer todos los números de cuenta que se deberán habilitar para su procesamiento manual en el formato de información de la cuenta de GMTA.

Procesamiento de Instrucciones MIFT

En caso de que el Cliente requiera que el Banco procese una instrucción MIFT:

1. El cliente envía una instrucción manual, debidamente firmada, a Citi a través del modo de comunicación seleccionado. Para el movimiento de fondos de la Cuenta del Cliente, Citi recomienda utilizar el formulario de pago manual estándar de Citi. El Cliente puede obtener una copia de dicho formulario contactando al centro de atención al cliente habilitado.

2. Al recibir la instrucción manual, el banco llevará a cabo su verificación interna, que incluye, entre otros, la revisión de la integridad de los detalles requeridos para el procesamiento y la verificación de la(s) firma(s) del autorizador de las que figuran en la tarjeta de firma. El Cliente debe tener cuidado al completar el formulario estándar de Citi para el pago manual, ya que puede ser rechazado si contiene borrones.

Actualizaciones a las Autorizaciones

Si la información establecida en GMTA cambia, el Cliente debe enviar un nuevo formulario de GMTA, que reemplaza el formulario anterior. Los cambios para el Banco deben ser informados de incluir, pero no están limitados a:

· Cambios de personal

· Cambios en el nombre de una persona (por ejemplo, debido a un cambio en el estado civil)

· Nuevos números de teléfono (por ejemplo, un nuevo número de teléfono, nuevo código de área, nuevo código de ciudad)

· Nuevo número de cuenta

No se aceptará un formulario de GMTA que detalle solo la información de la actualización, carta ni ningún otro formato de documento. Esto es necesario para asegurar la integridad operacional del proceso de comunicación manual.

El Cliente debe enviar el(los) nombre(s) del(de los) contacto(s) para ser eliminados del formulario de GMTA en carta en papel con membrete de la compañía y firmada por los autorizados según la Resolución de la Junta del Cliente o equivalente. Nuevamente, en interés de la integridad operativa, el Banco solicitará un nuevo formulario de GMTA que sustituirá a todos los formularios de GMTA anteriores si hay varias eliminaciones de firmas.

V. Otras Consideraciones

El uso o requerimiento de servicios del Banco, así como los servicios descritos en este manual, están sujetos a tarifas detalladas en el catálogo general de comisiones del Banco disponible en la página web del Banco. Estas tarifas e impuestos, comisiones y gastos aplicables pueden debitarse de cualquiera de las Cuentas del Cliente.

El Banco proporcionará al Cliente un sistema de asistencia telefónica a través de CitiService, nuestro servicio al cliente, en días laborables entre las 9:00 a.m. y las 5:00 p.m.

CitiDirect BE® es una plataforma de banca electrónica segura a la que se puede acceder a través de Internet por usuarios que han sido autorizados por la empresa. Pueden hacerlo desde direcciones IP en el extranjero, conservando los atributos de perfil proporcionados en el momento de su creación.

Servicio Infopool

Infopool es una interfaz única para cuentas con Citi y bancos terceros. El servicio de Infopool permite el monitoreo diario de saldos y transacciones de cuentas mantenidas en diferentes bancos a través de fronteras y monedas. Por lo tanto, Infopool Services consiste en consolidar la información en las cuentas bancarias del Cliente y las de sus subsidiarias en las cuentas de Citi, los bancos de Citigroup y/o en las cuentas de otros bancos (en adelante, Terceros), a través del sistema de banca electrónica CitiDirect BE®.

Citi solo consolidará la información para las cuentas indicadas por él, sin hacer ajustes a la información provista por su emisor, y, como tal, Citi no es responsable por el contenido o la precisión de la información en las cuentas.

El Cliente autorizará a los bancos proveedores de servicios grupales o de terceros a proporcionar a Citi la información de la cuenta, incluidos los datos personales. Asimismo, autoriza a Citi a recibir esta información y procesarla.

VI. Procedimientos Consolidados de Seguridad de TTS

Como se menciona en la sección de Comunicaciones de la Cuenta Maestra y Términos del Servicio (u otros términos y condiciones aplicables de la cuenta) ("MAST") que se han suscrito entre el Cliente y el Banco, se describe a continuación los procedimientos de seguridad ("Procedimientos ") utilizado por Citi Treasury and Trade Solutions en relación con los siguientes servicios o canales de conectividad.

- CitiDirect BE® (que incluye la Administración de cuentas bancarias electrónicas ("eBAM"), TreasuryVision® y WorldLink®)
- Respuesta de voz interactiva ("IVR")
- Correo electrónico / fax con el Banco excluyendo la transferencia de fondos iniciada manualmente (MIFT)
- CitiConnect®
- Otros canales locales de conectividad electrónica

La disponibilidad de los servicios o los canales de conectividad variará en los mercados locales. Estos procedimientos pueden actualizarse y notificarse al Cliente por medios electrónicos o de otra manera de vez en cuando. El uso continuado por parte del Cliente de cualquiera de los servicios o canales de conectividad mencionados anteriormente después de recibir aviso de los procedimientos actualizados (que pueden incluir, pero no están limitados a, publicar los procedimientos actualizados en CitiDirect BE en conexión con el servicio o canal de conectividad) aceptación de dichos procedimientos actualizados. Estos procedimientos deben leerse junto con el MAST, ya que dicho MAST puede ser modificado de vez en cuando. Los términos en mayúscula no definidos en el presente documento tendrán los significados que se les atribuyen en el MAST.

A) Roles y Responsabilidades del Administrador de Seguridad*

Para las aplicaciones en CitiDirect BE, el Banco requiere dos personas por separado para ingresar y autorizar instrucciones; por lo tanto, se requiere un mínimo de dos administradores de Seguridad. Cualquiera de los dos administradores de Seguridad, actuando en conjunto, puede dar instrucciones y / o confirmaciones a través de los canales de conectividad en relación con cualquier función del administrador de Seguridad o en conexión a través de Internet. Tales comunicaciones, cuando estén autorizadas por dos administradores de Seguridad, serán aceptadas y actuadas por el Banco. El Banco recomienda la designación de al menos tres administradores de Seguridad para garantizar una copia de seguridad adecuada. El Cliente designará a sus administradores de Seguridad en el Formulario de incorporación de los canales TTS. Un Gestor de Seguridad del Cliente también puede actuar como Gestor de Seguridad de

una entidad externa (por ejemplo, un afiliado del Cliente) y ejercer todos los derechos relacionados con el mismo (incluida la designación de usuarios para la (s) Cuenta (s) de esa entidad externa). Sin ninguna otra designación, si esa tercera entidad ejecuta un formulario de Autoridad de Acceso Universal (o cualquier otra forma de autorización aceptable para el banco) que concede al Cliente acceso a su(s) Cuenta s). Esto solo aplica en relación con la(s) Cuenta(s) cubiertas por la autorización correspondiente.

* Los roles y responsabilidades del administrador de Seguridad pueden estar prohibidos en ciertos mercados locales. Póngase en contacto con su representante de servicio al cliente para obtener más información.

La función del administrador de Seguridad incluye, pero no se limita a:

1. Establecer y mantener el acceso de los usuarios (incluidos los propios administradores de Seguridad), incluyendo actividades tales como:
    (a) crear, eliminar o modificar perfiles de usuario (incluidos perfiles de administradores de Seguridad) y derechos de titularidad (es importante tomar en cuenta que el nombre de usuario debe alinearse con los documentos de identificación de soporte)
    (b) crear perfiles de acceso que definan las funciones y los datos disponibles para varios usuarios, y
    (c) activar y desactivar las credenciales de inicio de sesión del usuario
2. Crear y modificar entradas en bibliotecas mantenidas por el Cliente (como pagos pre formateados y bibliotecas de beneficiarios) y autorizar a otros usuarios a hacer lo mismo
3. Modificación de los flujos de autorización de pago
4. Asignación de credenciales de contraseña dinámica u otras credenciales o contraseñas de acceso del sistema a los usuarios del Cliente
5. Notificar al Banco si hay alguna razón para sospechar que la seguridad se ha visto comprometida.

Los administradores de Seguridad también asignan límites de transacción a los usuarios para aquellos productos del Banco a los que el Cliente tiene acceso. Estos límites no son monitoreados ni validados por el Banco; El Cliente debe supervisar estos límites para garantizar que cumplen con las políticas y los requisitos internos del Cliente, incluidos, entre otros, los establecidos por el Consejo de Administración del Cliente o su equivalente.

Específicamente relacionado con la **Aplicación eBAM**, se requieren los siguientes roles:

La configuración inicial del servicio eBAM requiere la designación de tres Oficiales de Seguridad y un Secretario Corporativo. Dos roles administrativos principales independientes actúan en conjunto como creador / corrector para configurar y asignar derechos de usuario / función de datos y flujos de trabajo. Estos acuerdos no son monitoreados ni validados por el Banco; los flujos de trabajo y la actividad del usuario son supervisados por el Cliente para garantizar el cumplimiento de las políticas internas, los requisitos y los niveles de autorización y aprobación

del Cliente (y los Propietarios de Cuenta), incluidos, entre otros, los establecidos por el Consejo de Administración del Cliente (y los Propietarios de Cuenta) o órgano rector equivalente.
Los siguientes roles son necesarios para el servicio eBAM:

1. **Oficial de Seguridad:** cumple las funciones descritas en (1) a-c, dentro de los roles de los Gerentes de Seguridad
2. **Secretario Corporativo:** garantiza que los flujos de trabajo, los usuarios configurados como Autoridades Designadas y sus asignaciones a los flujos de trabajo cumplan con las políticas internas, los requisitos, los niveles de autorización y aprobación establecidos por el Consejo de Administración del Cliente (y los Propietarios de Cuenta)
3. **Autorizador Designado:** tiene una amplia autoridad para iniciar y autorizar las actividades de Workflow
4. **Solicitantes:** son personas autorizadas para realizar actividades administrativas tales como ingresar solicitudes de gestión de cuenta y firmante en el sistema eBAM

Los Oficiales de Seguridad, el Secretario Corporativo y los Autorizadores Designados son responsables de:

a) Definición y administración de configuración de jerarquía y control de sitio / flujo, como el establecimiento de flujos de trabajo e identificación de usuarios y niveles de aprobación
b) Creación de funciones administrativas superiores adicionales y designación a los usuarios los mismos (que pueden o no ser empleados por el cliente)
c) Notificar al Banco si hay alguna razón para sospechar que la seguridad o la confidencialidad de cualquier credencial del Usuario (incluidas las funciones administrativas superiores) ha sido violada o comprometida
d) Cuando corresponda, completar, enmendar, aprobar y / o complementar los formularios de implementación del Cliente que el Banco pueda solicitar ocasionalmente en relación con la prestación de servicios y / o productos al Cliente.

B) Métodos de autenticación

Los procedimientos incluyen ciertos métodos de autenticación segura ("Métodos de autenticación") que se utilizan para identificar y verificar de forma exclusiva la autoridad del Cliente y / o cualquiera de sus usuarios, normalmente a través de mecanismos como pares de ID de usuario / contraseña, certificados digitales y tokens de seguridad (implementados a través de hardware o software) que generan una contraseña dinámica utilizada para acceder a los servicios o canales de conectividad cada vez que el Cliente o un usuario inicia sesión o se autentica. Es importante tener en cuenta que la disponibilidad de los métodos de autenticación descritos a continuación varía en función de los mercados locales.

Los administradores de Seguridad y todos los usuarios que quieran (a) iniciar o aprobar transacciones (y cuyo perfil de usuario lo permita) y / o (b) acceder a los sistemas de acuerdo con los derechos deben utilizar los métodos de autenticación disponibles (que pueden actualizarse) de vez en cuando, como se describe arriba).

Los siguientes métodos de autenticación están disponibles para acceder a los servicios o canales de conectividad mencionados anteriormente en combinación con una ID de usuario:

Métodos de Autenticación	**Descripción**
Token: Challenge Response	Ya sea un (i) soft token basado en la aplicación móvil (por ejemplo, MobilePASS) o (ii) ficha física (por ejemplo, SafeWord Card, Vasco) que en cada caso se usa para generar una contraseña dinámica después de la autenticación con un pin de 4 dígitos. Al acceder a CitiDirect BE, el sistema genera un desafío y el token utilizado genera una clave de acceso de respuesta que ingresa al sistema.
Token: One Time Password	Ya sea (i) soft token basado en aplicaciones móviles (por ejemplo, MobilePASS) o (ii) token físico (por ejemplo, SafeWord Card, Vasco) que se utiliza para generar una contraseña dinámica después de autenticar con un pin de 4 dígitos. Esta contraseña dinámica se ingresa en el sistema para obtener acceso.
SMS One-Time-Code	Una contraseña dinámica se entrega a un usuario a través de SMS, después de lo cual el usuario ingresa la contraseña dinámica y una contraseña segura para obtener acceso al sistema.
Voz One-Time-Code	Se entrega una contraseña dinámica a un usuario a través de una llamada de voz automática, después de lo cual el usuario ingresa la contraseña dinámica y una contraseña segura para obtener acceso al sistema
MultiFactor Authentication	Se genera una contraseña dinámica a través de una tarjeta SafeWord o un token Mobile PASS, después de lo cual se ingresa dicha contraseña dinámica junto con una contraseña segura para obtener acceso al sistema.
Certificados Digitales	Un certificado digital emitido por una autoridad de certificación aprobada que se utiliza para la autenticación. Los certificados digitales utilizan un mecanismo de almacenamiento de claves y un PIN correspondiente, y pueden ser emitidos por IdenTrust, SWIFT (3SKey) u otros proveedores acordados.
Clave segura	Un usuario ingresa su contraseña segura para acceder al sistema. Una contraseña segura generalmente limita las capacidades de un usuario en el sistema, de modo que se puede ver la información y no se habilitan capacidades de transacción.
Interactive Voice Response (“IVR”) & email	A los usuarios que se contacten con el banco se les pedirá que ingresen un número PIN o que proporcionen otra información para validar el acceso autorizado por teléfono o por correo electrónico.
Fax	La correspondencia recibida por el Banco, excluyendo las solicitudes de MIFT, se verificará con firma en función de la información contenida en la resolución del consejo del Cliente.
MTLS	MTLS crea una conexión de correo electrónico segura y privada entre el banco y la parte externa. Un correo electrónico transmitido que se envía utilizando este canal se envía a través de Internet a través de un túnel TLS cifrado creado por la conexión.
Secure PDF	Los correos electrónicos cifrados se entregan a un buzón regular como un documento PDF que se abre al ingresar una contraseña privada, tanto el cuerpo del mensaje como cualquier archivo adjunto están encriptados. Se puede configurar una contraseña privada al recibir el primer correo electrónico seguro recibido.

Para obtener más información sobre cualquiera de estos métodos de autenticación, consulte la página de ayuda de inicio de sesión en CitiDirect BE®: (https://portal.citidirect.com/portalservices/forms/loginHelp.pser)

Para CitiConnect:

- Si el Cliente opta por utilizar una conexión pública a Internet para conectarse a Citi, incluidos HTTPS, FTP seguro y FTPS, el Banco y el Cliente intercambiarán certificados de seguridad para garantizar que tanto el canal de comunicación como los mensajes intercambiados estén completamente encriptados y protegidos. El Banco solo aceptará comunicaciones provenientes de la puerta de enlace de comunicaciones segura del Cliente utilizando los certificados de seguridad intercambiados y viceversa y el Banco solo transmitirá las Comunicaciones a la puerta de enlace de comunicación del Cliente utilizando los certificados de seguridad intercambiados.

- Si el Cliente opta por utilizar CitiConnect a través de SWIFT, entonces, para cualquier orden de pago e instrucciones relacionadas con SWIFT, incluida la modificación o cancelación de dichos pedidos, los Procedimientos que se utilizarán para autenticar que una orden de pago o instrucción es la del Cliente y autorizada por el Cliente será el que se estipula en la Documentación contractual de SWIFT (según lo define SWIFT y puede ser modificado o complementado de vez en cuando) que incluye, entre otros, sus Términos y condiciones generales y la descripción del servicio de FIN o según lo establecido en cualquier otro término y condición que pueda establecer SWIFT. El Banco no es responsable de ningún error o retraso en el sistema SWIFT. Las comunicaciones con el Banco deben proporcionarse en el formato y el tipo requerido y especificado por SWIFT.

- Si utiliza una VPN, tanto el Cliente como el Banco designarán una sola dirección IP desde la cual se enviarán y / o recibirán comunicaciones entre el Cliente y el Banco. El Banco solo aceptará comunicaciones provenientes de la dirección IP designada por el Cliente, y viceversa, y el Banco solo transmitirá las Comunicaciones a la dirección IP designada por el Cliente, y viceversa.

- El Cliente y el Banco también pueden usar una Autenticación de Módulo de Seguridad de Hardware para acompañar la Autenticación VPN. Esto requiere que el Banco y el Cliente instalen cada uno de ellos en los servidores designados para las Comunicaciones entre el Banco y el Cliente.

El Banco requiere:

• Protección del Cliente de los Métodos de Autenticación, incluidas las credenciales de inicio de sesión y / o los certificados de seguridad asociados con los Métodos de Autenticación (en conjunto, las "Credenciales") y garantizar que el acceso y la distribución de las Credenciales estén limitadas solo a las personas autorizadas del Cliente. Los Métodos de Autenticación y las Credenciales asociadas son los métodos mediante los cuales el Banco verifica el origen de las Comunicaciones emitidas por el Cliente al Banco.
• El cliente debe tomar todos los pasos razonables para proteger las credenciales. En consecuencia, el Banco recomienda encarecidamente que el Cliente no comparta las Credenciales con ningún tercero.

Ciertas jurisdicciones pueden requerir que los individuos (y sus credenciales correspondientes) se identifiquen como conformes con los requisitos de la legislación control de lavado de dinero AML aplicables antes de otorgar acceso para realizar ciertas funciones.

El Banco entiende que el Cliente puede, en algunos casos, desear compartir las Credenciales del Cliente con una tercera entidad o proveedor de servicios (incluyendo, sin limitación, un proveedor de nóminas de terceros) designado por el Cliente para tener acceso a las Credenciales del Cliente (dicho tercero entidad de partido o proveedor de servicios se denominará en este documento como un "Tercero autorizado") con el fin de acceder y utilizar cualquiera de los canales electrónicos de los bancos en nombre del Cliente. En el caso de que el Cliente elija compartir sus Credenciales con un Tercero Autorizado, el Banco recomienda encarecidamente que el Cliente tome, y se asegure de que cualquier Tercero Autorizado tome, todos los pasos razonables para proteger las Credenciales de su divulgación a cualquier Persona no Autorizada Personal de terceros. El Banco está autorizado a actuar sobre cualquier Comunicación que reciba de un Tercero Autorizado en nombre del Cliente de conformidad con estos procedimientos.

C) Integridad de datos y comunicaciones seguras

- El cliente transmitirá datos en la comunicación y el intercambio con el Banco, utilizando Internet, correo electrónico y / o fax, que no son necesariamente sistemas seguros de comunicación y entrega. El Banco utiliza métodos de cifrado, líderes en la industria (según lo determina el Banco), que ayudan a garantizar que la información se mantenga confidencial y que no se modifique durante el tránsito.

- Si el Cliente sospecha o tiene conocimiento de una falla técnica o de un acceso o uso inadecuado de los servicios del Banco, los canales de conectividad o los Métodos de Autenticación por parte de cualquier persona (ya sea una persona autorizada o no), el Cliente notificará al Banco sin demora de tal ocurrencia En caso de acceso o uso indebidos por parte de una persona autorizada, el Cliente debe tomar medidas inmediatas para poner fin al acceso y uso que la persona autorizada tenga de los servicios o los canales de conectividad del Banco.

- Si el Cliente utiliza el formato de archivo, el software de encriptación (ya sea proporcionado por el Banco o un tercero), para respaldar el formateo y el reconocimiento de los datos e instrucciones del Cliente y las acciones en las Comunicaciones con Citi, el Cliente utilizará dicho software únicamente para el propósito por el cual se ha instalado

VII. Conclusión

Gracias por elegir Citi Treasury and Trade Solutions (TTS) para sus necesidades de Cash Management. No dude en ponerse en contacto con su gerente de relaciones con Citi sobre cualquier pregunta adicional que tenga en los servicios de TTS.

Treasury and Trade Solutions
citi.com/tts

Mayo de 2017