Guía de Usuario
Cash Management

Banco CMB (Costa Rica) S.A.

Treasury and Trade Solutions

citi

Índice

I. Introducción

Gracias por elegir las soluciones de Citi Treasury and Trade Solutions (TTS) para las necesidades de su empresa en administración de efectivo. El objetivo de esta Guía del Usuario es proporcionar a los clientes información detallada sobre los servicios disponibles para ellos. En esta guía, Citi Costa Rica, Banco CMB (Costa Rica) S.A (subsidiaria de Citi en Costa Rica) y Banco se pueden usar indistintamente. Esta guía se puede actualizar periódicamente y la versión más actualizada está disponible en el sitio web oficial del Banco. En la Sección VII de esta guía, se incluye un enlace directo al sitio.

II. Servicios de Pago

A. Tipos de Servicios de Pago

- Transferencias entre cuentas Citi: Transferencias electrónicas de fondos de una cuenta corriente en Citi Costa Rica a otra cuenta corriente en Citi Costa Rica.
- Transferencias SINPE (RTGS) en Tiempo Real: También conocido como TEF; transferencia electrónica de fondos con débito en tiempo real a través de SINPE (Sistema Nacional de Pagos Electrónicos), el sistema nacional de pagos electrónicos.
- Transferencias de Crédito SINPE de la Cámara de Compensación Automatizada (ACH): También conocidas como Pago predeterminado o estandar, son transferencias electrónicas de fondos interbancarios a través de SINPE.
- Cheques: Instrumentos negociables en papel que pueden pasarse de una persona o entidad a otra y cambiarse por dinero. Un cheque instruye incondicionalmente a un banco a pagar una cantidad específica en una moneda específica a una persona específica, o para “hacerlo efectivo” al presentarlo. Los cheques se pueden presentar para ser depositados en la cuenta del Cliente a través de un cajero de Citi o en una sucursal de un aliado comercial. El Banco, a pedido del Cliente, emitirá un talonario de cheques preimpresos que le permitirán al Cliente realizar pagos a los beneficiarios. Los Talonarios de Cheques se entregarán en la dirección indicada por el Cliente en la solicitud. Los Talonarios de Cheques se habilitarán en el sistema del Banco 24 horas después de la recepción por parte del Cliente.
- Transferencias Transfronterizas de Fondos: Permite que los clientes transfieran fondos a cuentas en otros países en diferentes monedas. El proceso puede implicar el uso de bancos corresponsales u otros intermediarios y puede estar sujeto a cargos adicionales.
- Débitos Directos: Un medio para cobrar el dinero adeudado por un pagador, donde el beneficiario (originador) genera la transacción para ser procesada por el banco del pagador contra la cuenta del pagador. Los débitos directos están sujetos a la autorización del pagador (si es diferente del originador) y normalmente se utilizan para pagos recurrentes, tales como tarjetas de crédito y facturas de servicios públicos, donde los montos de pago varían de un pago a otro.

B. Envío de un Pago

1. El Cliente envía una instrucción de pago a Citi, con los datos mínimos requeridos por SINPE e indicados en el formato estándar de pagos interbancarios, proporcionado por el banco al Cliente cuando se implementa el servicio de pago. Las instrucciones se pueden enviar a través de:
    - Los canales electrónicos del Banco, incluidos CitiDirect BE® y CitiConnect®,
    - Una interfaz SWIFT

- Una solicitud manual (consulte la Sección IV para obtener detalles sobre las transacciones manuales)

El procesamiento de transacciones está sujeto a horas límite específicas.

El Banco no está obligado a sobregirar la cuenta del Cliente para cumplir con las instrucciones de pago a menos de que el Cliente tenga un sobregiro previamente aprobado por el Banco. En el caso de que la cuenta esté sobregirada, el Cliente puede estar sujeto a cargos adicionales.

2. Citi reenvía las instrucciones al sistema de pago correspondiente para su posterior procesamiento.
3. El sistema de pago envía las instrucciones al banco beneficiario en función del ciclo de compensación definido localmente.
4. El banco beneficiario acredita la cuenta del beneficiario según lo determinado por el ciclo y el tipo de compensación del servicio solicitado.

   En el caso de que la información en las instrucciones de pago sea incorrecta, el SINPE rechazará el pago. Citi devolverá los fondos en tiempo real y acreditará la cuenta corriente del Cliente. El Cliente puede ver, a través de CitiDirect BE®, el estado de los pagos SINPE (RTGS) en tiempo real. Los detalles del pago SINPE de las transferencias de crédito y la Cámara de Compensación Automatizada (ACH) están disponibles a través de CitiDirect BE® después de las 10 a.m. de la fecha de valor del pago.

   A partir de la fecha de envío del pago por parte de Citi, cualquier retraso dependerá exclusivamente de la operación de SINPE y de donde se encuentre la cuenta bancaria del destinatario.

C. Cheques de Gerencia de PayLink®

El Cliente puede solicitar, dando instrucciones al Banco a través de canales electrónicos autorizados, la emisión de un Cheque de Gerencia de PayLink® a nombre de un beneficiario para retirarlo en una sucursal de Citi o para enviarlo a las oficinas del Cliente. El banco emitirá el Cheque de Gerencia de PayLink® de acuerdo con las instrucciones del cliente. Los Cheques de Gerencia PayLink® se cruzan indicando "|BANCO|" o el nombre del Banco por lo cual el dinero deberá ser cobrado a través de una entidad bancaria únicamente mediante el depósito del cheque de gerencia en su cuenta corriente. Los funcionarios del Banco, cuyas firmas aparecen en el cheque, no son responsables del contenido del cheque ni de su uso.

En general, un cheque es un documento que el Banco emite con los recursos que el Cliente tiene en el banco en su cuenta de cheques.

Para que el Banco emita un cheque, el Cliente debe tener recursos en su cuenta con el Banco o un sobregiro previamente aprobado por el Banco.

Emisión y Procesamiento de los Cheques de Gerencia de PayLink®

1. El Cliente instruye al banco a emitir el(los) cheque(s) de PayLink® a través del canal electrónico acordado y el proceso definido por el administrador de la plataforma electrónica del Cliente.

2. Citi debita los fondos de la cuenta del Cliente e imprime el(los) cheque(s) con una firma facsímil de los funcionarios del Banco y cruza el (los) cheque(s).

3. Citi entrega los cheques por medio de una de las siguientes opciones, que debe ser incluida en la instrucción del Cliente:

   - Entrega en las oficinas del Cliente, incluyendo la(s) persona(s) autorizada(s) para recibir los cheques

   - Entrega en la sucursal corporativa de Citi para su retiro por parte del beneficiario u otra persona(s) previamente autorizada por el Cliente

   Al momento de la recolección, la persona autorizada debe proporcionar un documento de identificación oficial. En caso de que la persona autorizada se niegue a presentar una identificación, Citi no entregará los cheques.

   Si un cheque no se retira dentro de los 60 días posteriores a la fecha de emisión, el Banco lo devolverá al Cliente.

4. Los cheques se depositan por el beneficiario y el banco receptor los envía a Citi según los acuerdos locales del SINPE.

5. Citi no realizará un pago si considera que un cheque fue alterado, falsificado o robado, o si lo solicita una autoridad competente.

   El Cliente puede solicitar que el Banco suspenda el pago de un cheque de conformidad con los procedimientos del Banco mediante la presentación de una solicitud por escrito firmada por el representante legal del Cliente, indicando el número de serie del cheque, la fecha de emisión, el nombre del destinatario (si está disponible) y el monto, y un Certificado de Poder Notarial para el representante autorizado. Además, el cheque original debe enviarse para su anulación.

   En caso de pérdida o robo de un cheque de gerencia emitido por el Banco, el cheque se reemplazará por el Banco a petición del Cliente, previo al cumplimiento de una garantía a satisfacción del Banco por el plazo de la prescripción del certificado perdido. Esta garantía bancaria debe cubrir el monto del(los) cheque(s). El Cliente deberá enviar al Banco una solicitud por escrito firmada por el representante legal del Cliente junto con una Certificación de Poder Notarial. Además, el Cliente debe publicar una notificación del cheque perdido tres veces consecutivas en un periódico de circulación nacional y en el Boletín Oficial. El Banco deberá reemplazar el(los) cheque(s) quince (15) días después de la última fecha de publicación.

   El período de validez de un cheque PayLink® está determinado por las leyes y prácticas bancarias aplicables. Si un cheque PayLink® no se presenta para el pago en o antes de la fecha límite de la prescripción, el Banco no pagará la cuenta sujeta a las leyes y prácticas bancarias aplicables.

El Cliente será informado a través de CitiService en caso de cualquier problema con el(los) cheque(s).

D. Revocación y Suspensión de Pagos

Todas las instrucciones de pago confirmadas por el Cliente y aceptadas por el Banco son y deberán ser definitivas e irrevocables. El Banco no deberá incurrir en ninguna responsabilidad con el Cliente o con terceros con respecto a esto, independientemente de si el pago se ha realizado o no.

El Cliente tiene la opción de enviar una orden de cancelación de pago al Banco a través de CitiDirect BE® o mediante una solicitud por escrito que siga las instrucciones del Banco para suspensiones de pago en concordancia con las leyes y prácticas comerciales aplicables.

E. Recibir Débitos Directos (Pagos)

Citi, como banco o entidad de destino que paga al cliente, respalda los mandatos de débito directo recibidos de otras instituciones financieras a través de SINPE. Estos incluyen:

- Débidos en Tiempo Real: Una entidad envía un débito directo a la cuenta de Citi para acreditar una cuenta en otro banco en Costa Rica o un tercero autorizado (es decir, cargos por impuestos y servicios públicos).
- Débitos Directos: Una entidad envía una orden de débito directo a cargar la cuenta de Citi para acreditar una cuenta en otro banco en Costa Rica o un tercero autorizado (es decir, cargos por impuestos y servicios públicos). Estas transacciones se procesarán el mismo día hasta las 10 p.m.

Los débitos directos de SINPE están sujetos a la autorización del pagador y, como tal, el Cliente debe aprobar y presentar una Autorización de Débito Automático (ADA) al Banco para asegurarse de que la cuenta esté configurada para permitir débitos directos de este.

Proceso de Débito Directo

1. En concordancia con la Autorización de Débito Automático (ADA), Citi procesa las instrucciones y debita la cuenta del Cliente de acuerdo con los procedimientos de SINPE para débitos directos.
2. Citi se comunica con la institución financiera recaudadora a través del SINPE para los avisos positivos o negativos (rechazos y devoluciones). En el caso de que no haya fondos suficientes en la cuenta del Cliente, Citi no procesará el pago mediante débito directo y devolverá el estado de "fallido".

El procedimiento para autorizar débitos de un tercero es el siguiente:

1. El Cliente firma una Autorización de Débito Automático (ADA, por sus siglas en inglés) que autoriza a una cuenta de terceros a cobrar a la cuenta de Citi del Cliente para realizar los pagos respectivos de las obligaciones del Cliente.
2. El Cliente presenta a Citi la ADA en original y dos copias firmadas de acuerdo con los requisitos vigentes.
3. Citi permite el débito directo en sus sistemas dentro de 24 horas, cuando la cuenta del Cliente puede ser debitada por el originador de débito directo autorizado.

A. Cronograma de Pagos

El siguiente cuadro detalla las horas límite y las fechas de valor de diferentes tipos de pago:

Tipo de Pago	Horas Límite	Fecha de Valor
Transferencias entre cuentas Citi	6:00 p.m.	T + 0 (Mismo día)
Transferencias SINPE (RTGS) en tiempo real	2:00 p.m.	Tiempo Real
Transferencias Automáticas de Crédito de la Cámara de Compensación de SINPE (ACH)	6:00 p.m.	T + 1 (Siguiente día hábil)
Débitos Directos	6:00 p.m.	T + 1 (Siguiente día hábil)
Débitos Directos en tiempo real	2:00 p.m.	Tiempo Real
Cheques de Gerencia de PayLink®	6:00 p.m.	T + 2. (Dos días hábiles)

III. Servicios de Colecturía

A. Recibir un Pago

- La cámara de compensación remite las instrucciones a Citi en función del ciclo de compensación definido localmente.
- Citi acredita la cuenta del Cliente. 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.

Para cualquier pago rechazado o devuelto por Citi, la cámara de compensación o el banco beneficiario, devuelve los fondos a la cuenta del pagador. El motivo de la devolución se comunica al pagador.

B. Recaudaciones de Débito Directo

Un cobro de débito directo es una transacción financiera originada electrónicamente por el Cliente que ordena al banco retirar fondos de la cuenta bancaria de un pagador (tercero).

Órdenes de Débito Directo

Las órdenes de débito directo constituyen una autorización al Banco para que un tercero cobre en la cuenta corriente del Cliente. Los pedidos firmados deben ser enviados por cada una de las agencias de pago del Cliente para que tengan el valor legal apropiado.

La Orden de Débito Directo de Citi puede descargarse directamente del sitio web de Citi en la sección de Débito Directo o puede ser diseñada por el Cliente de acuerdo con los requisitos mínimos establecidos por las normas y procedimientos del Banco Central de Costa Rica, conocidos como la "estandarización de orden física de Débito Directo para Débitos Directos".

Los pedidos de débito directo recibidos después de las 6:00 p.m. se procesarán el siguiente día hábil.

Como mínimo, la orden de débito directo debe contener:

- El número de cuenta del cliente al que se realiza el débito
- El servicio bajo el cual se debita la cuenta
- La firma del titular de la cuenta, que debe registrarse junto con su número de cédula jurídica o física.
- Monto y fecha máxima autorizada para débito de fondos.

Este es un acuerdo entre el Cliente y el recaudador en la entidad de origen. Citi sirve solo como canal de una queja ante el SINPE.

Proceso de Cobro por Débito Directo

1. Para cobrar fondos mediante el débito directo, el Cliente (beneficiario) emite una instrucción de débito directo a través del sistema de banca electrónica CitiDirect BE®.

2. El Cliente debe enviar a Citi las órdenes de débito directo debidamente firmadas por cada una de las agencias pagadoras del Cliente para que Citi pueda comunicar las transacciones a los bancos de los pagadores.

3. Una vez que se autoriza una transacción de pago, el pago se envía para su procesamiento. La transacción se puede ejecutar en tiempo real o al final del día a través del SINPE, de acuerdo con la opción seleccionada por el Cliente.

Si un débito directo no se procesa correctamente a través de la cámara de compensación, el Cliente puede ver el estado de la transacción y el motivo del rechazo a través de CitiDirect BE®. Las causas más comunes de rechazo son:

1. El banco pagador no ha autorizado efectivamente al colector en su sistema

2. Cuenta inválida, inexistente o cerrada

3. Información inválida

4. Las cuentas no tienen fondos o éstos no son suficientes

5. Problemas de comunicación con la entidad pagadora

El Cliente debe comunicarse con CitiService con cualquier pregunta relacionada con las transacciones de débito directo rechazadas.

C. Depósito de Cheques y Efectivo

Las Cuentas de Citi en Costa Rica pueden recibir depósitos de cheques y/o efectivo a través de las siguientes opciones:

1. En la Sucursal Corporativa de Citi: Centro Corporativo Plaza Tempo, al lado de San Rafael de Escazú, Edificio B, Piso 5.

2. En las agencias de nuestros socios comerciales (Network Extension) para servicio de cobro o colecturía).

La información relacionada con estos servicios está disponible a través de CitiDirect BE®.

Recaudación a través de Socio Comercial (Network Extension).

Los servicios de recolección se ofrecen según la ubicación, las políticas, las fechas y los horarios aplicables a cada punto de recolección.

El servicio de recolección aceptará pagos en efectivo en dólares estadounidenses y colones (hasta $ 9,999 o el equivalente en colones) y cheques de cualquier institución del sistema bancario nacional. Los cheques internacionales no son aceptados bajo este modo de pago.

Los recaudos en efectivo realizados a través de los puntos de recolección entre lunes y jueves (inclusive) estarán disponibles en la cuenta correspondiente el siguiente día hábil. Los cobros hechos el viernes se acreditarán el lunes siguiente. Los recaudos realizados los sábados, domingos o días festivos se acreditarán el martes o el siguiente día hábil. Los cheques cobrados se compensarán y liquidarán según los procesos establecidos por el Banco Central de Costa Rica.

D. Central de Pagos (Central Payments)

Central de pagos es una plataforma web que permite a los clientes de Citi publicar facturas pendientes y cuentas por cobrar a sus respectivos clientes, que pueden acceder a ellas a través de contraseñas personalizadas e individuales.

Los deudores del Cliente también pueden personalizar su tipo de pago o completar el pago a través de la plataforma de Central de Pagos. Con esta opción, el Cliente recibió información detallada para procesos automatizados de conciliación, reduciendo e incluso eliminando procesos operativos y manuales.

Concesión de Acceso a los Clientes

A través de las capacidades de intercambio de archivos seguros de CitiDirect BE®, el Cliente proporcionará al Banco la lista de sus clientes e instrucciones para concederles el acceso a la plataforma de Central de Pagos.

Carga de Cuentas por Cobrar

El Cliente transmitirá al Banco a través de CitiDirect BE® el monto que pagará cada usuario de Central de Pagos. Como método de contingencia, el Cliente puede cargar manualmente el archivo con esta información en Central de Pagos.

Los archivos compartidos con el Banco entre las 8:00 a.m. y las 6:00 p.m. en días hábiles se procesarán el mismo día y actualizarán la base de la deuda durante el proceso por *batch*. Si el archivo se recibe el fin de semana, un feriado o después de la hora límite, se procesará al día siguiente. El cliente puede actualizar la información de la deuda a través de estos archivos. Cada archivo reemplaza la información anterior.

Anunciar un Pago en la Plataforma

Todos los usuarios con acceso a Central de Pagos podrán consultar sus pagos pendientes comerciales, elegir las facturas que se pagarán e imprimir recibos de depósito con la información de su deuda.

Dichas facturas se pueden pagar a través de este tipo de transacciones:

- Transferencias SINPE
- Transferencias entre cuentas Citi (Book to book).
- Débitos directos (a través de Pagos Centrales en Línea)
- Depósito en sucursales de Citi
- Depósito en sucursales de otros bancos (si el cliente de Citi posee una cuenta en otros bancos).
- Cualquier otro medio que en el futuro sea aprobado.

El Banco informará al Cliente de los pagos que reciba a través de Central de Pagos.

IV. Iniciación Manual de Instrucciones

Citi ofrece a sus Clientes la posibilidad de iniciar instrucciones manuales o Transferencia de Fondos Iniciada Manualmente (MIFT) en el caso de una contingencia u otros escenarios que pueden implicar una instrucción manual, incluida la modificación, revocación o cancelación de instrucciones anteriores.

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

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

Los clientes que no proporcionan un formulario GMTA a Citi y, por lo tanto, no tienen capacidad de pago MIFT, entienden que los medios manuales de comunicación no estarán disponibles para ellos en caso de que sean necesarios para imprevistos u otros escenarios aplicables que puedan implicar instrucciones manuales.

Además, Citi comparte su preocupación sobre el riesgo operacional relacionado con el envío de cartas físicas a las oficinas de Citi, lo que permite a los clientes enviar instrucciones manuales a través de CitiDirect BE® como imágenes escaneadas. Para habilitar esta capacidad, el Cliente debe solicitar el paquete de solución de Pagos Manuales en el Formulario de activación de CitiDirect BE®, donde debe indicar a qué usuarios de CitiDirect BE® se les otorgará este perfil y cómo pueden enviar instrucciones manuales.

Pagos manuales a través de CitiDirect BE® (Pagos Manuales Virtuales)

1. El servicio de Pagos Manuales Virtuales le permite al cliente ingresar, ver, y autorizar las instrucciones a través de imágenes (cartas) a través del CitiDirect BE®, CitiDirect BE® Móvil y CitiDirect BE® sistema de Banca Electrónica para Tablets, utilizando un canal de transmisión segura y siguiendo el proceso de autenticación actual (uso de Safeword Card/MobilePASS) como medio de acceso y autenticación de usuarios y procesamiento (con niveles preparadores y aprobadores previamente solicitados y autorizados por el Cliente).

2. El envío de instrucciones a través del servicio de Pagos Manuales Virtuales se limita a las transacciones que el Banco define para este fin.

3. Las imágenes de instrucciones ingresadas en el servicio de Pagos Manuales Virtuales deben estar previamente firmadas por los representantes autorizados del Cliente y seguirán el procedimiento establecido en el contrato de la cuenta de validación de la firma.

4. Las imágenes solo se pueden procesar en dos tipos de formato: PDF y JPG

Notas para Completar el Formulario de 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 de GMTA:
   - Carta

- Fax:
- CitiDirect BE®

2. Los iniciadores pueden estar disponibles solo con la Opción 1 en el formulario GMTA.
3. Proporcione al menos dos candidatos de devolución de llamada. Citi recomienda que los nominados estén ubicados en el mismo huso horario del país donde se encuentra la cuenta del cliente.
4. Al completar el formulario de GMTA, el Cliente debe enumerar todos los números de cuenta que se habilitarán para el procesamiento manual en el Cronograma de información de la cuenta de GMTA.

Procesamiento de Instrucciones MIFT

En caso de que el Cliente requiera que Citi 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.
2. Una vez recibidas las instrucciones manuales, Citi realiza su verificación interna, que incluye, entre otras, la revisión de la integridad de los detalles de procesamiento requeridos y la verificación de las firmas de los iniciadores frente a 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/correcciones.
3. Citi puede realizar un control adicional llamando a los nominados incluidos en el formulario de GMTA, con la excepción de las instrucciones enviadas en el Formulario de Lista de Beneficiarios Predefinidos, una vez que se hayan establecido inicialmente. El candidato de devolución de llamada y el iniciador no pueden ser el mismo. La confirmación por teléfono puede ser grabada por Citi.
4. Citi procesa las instrucciones manuales una vez que determina que todas las verificaciones son exitosas.

El procesamiento de la instrucción está sujeto a los procedimientos y las condiciones internas de Citi dado que existen canales electrónicos alternativos para realizar dicha instrucción.

Actualizaciones a las Autorizaciones

Si la información provista en GMTA cambia, el Cliente debe enviar un nuevo formulario de GMTA que reemplaza el formulario anterior. Los cambios para los cuales Citi debe ser informado incluyen, pero no están limitados a:

- Cambios personales
- Cambios en el nombre de una persona (p. ej., debido a cambios en el estado civil)
- Nuevos números de teléfono (p. ej., nuevo número de teléfono, nuevo código de área o nuevo código de ciudad)
- Nuevo número de cuenta

Ni un formulario de GMTA que detalle solo la actualización, ni una carta o cualquier otra forma de documento serán aceptados. Esto es necesario para asegurar la integridad operacional del proceso de comunicación manual.

Eliminaciones de Autorizaciones

El Cliente deberá enviar los nombres del(los) candidato(s) que se eliminarán del formulario de GMTA en una carta con membrete de la empresa y firmados por signatarios autorizados según la Resolución del Consejo del Cliente o equivalente. De nuevo, en interés de la integridad operacional, Citi solicitará un nuevo formulario de GMTA que sustituirá a todos los formularios GMTA anteriores si hay varias eliminaciones de firmas.

V. Servicios de Información: Agregación de Datos en Infopool

A. Servicio de Consolidación

Infopool es una interfaz única para cuentas con Citi y otros bancos. El Servicio de Infopool permite la supervisión diaria de saldos y transacciones de cuentas mantenidas en diferentes bancos, países y monedas. Por lo tanto, los Servicios de Infopool consisten en consolidar la información en las cuentas bancarias del Cliente y las de sus subsidiarias en los libros de Citi, los bancos de Citigroup y/o en los libros de otros bancos (en adelante, Terceros), a través del sistema de banca electrónica CitiDirect BE®.

Citi solo consolidará la información de las cuentas indicadas por el Cliente en el formulario de activación, sin hacer ajustes a la información proporcionada 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.

El Cliente tiene y retiene todos los derechos, títulos e intereses en la información de las cuentas y le permite a Citi consolidar dicha información de cuenta para realizar consultas. Dada la provisión del servicio, Citi solo consolidará la información en las cuentas establecidas por el Cliente, sin ajustar la información provista por el emisor.

El Cliente entiende que Infopool es un servicio global, pero algunos países tienen leyes de protección de datos personales que limitan la compilación, divulgación, procesamiento o transferencia de datos personales y la información de la cuenta puede incluir datos personales sujetos a las leyes de datos personales de uno o más países.

B. Procedimiento

1. El Cliente garantiza que, para cada cuenta, independientemente de la identidad del titular de la cuenta, el Cliente tiene el derecho y está legalmente autorizado para acceder a la información de la cuenta. Asimismo, el titular de la cuenta autoriza a Citi a consolidar dicha información.

2. Para la implementación del servicio de Agregación de Datos (Infopool), el Cliente enviará el Formulario de solicitud de informe de cuenta y confirmará la presentación de la Carta de Muestra de Infopool al Grupo Citi y/o a Bancos Terceros en cuyos libros se mantienen las cuentas a consolidar mediante este servicio.

3. Los usuarios de Infopool serán aquellos definidos por el Cliente en los formularios de solicitud de CitiDirect BE® con el perfil habilitado para consultas.

VI. Procedimientos de Seguridad Consolidados TTS

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

- CitiDirect BE® (incluida la administración electrónica de cuentas bancarias ("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 canales de conectividad variará en los mercados locales. Estos Procedimientos pueden actualizarse y notificarse al Cliente por medios electrónicos o de otro modo de vez en cuando. El uso continuo por parte del Cliente de cualquiera de los servicios o canales de conectividad mencionados anteriormente después de ser informado de los Procedimientos actualizados (que pueden incluir, entre otros, la publicación de Procedimientos actualizados en CitiDirect BE®, en conexión con el servicio o canal de conectividad) constituirá la aceptación del Cliente de dichos Procedimientos actualizados. Estos Procedimientos se deben leer junto con MAST, dado que dicho MAST se puede modificar periódicamente. Los términos en mayúscula no definidos de otra manera en este documento tendrán los significados que se les atribuyen en MAST.

A. Funciones y Responsabilidades del Usuario administrador*

Para las aplicaciones accesibles en CitiDirect BE®, el Banco requiere de dos individuos separados para introducir y autorizar las instrucciones; por lo tanto, se requieren un mínimo de dos Gerentes de Seguridad. Dos usuarios administradores, actuando en conjunto, pueden dar instrucciones y/o confirmaciones a través de los canales de conectividad en relación con cualquier función del Usuario administrador o en relación con la facilitación de nuestra comunicación a través de Internet. Cualquiera de estas Comunicaciones, cuando sea autorizada por dos Gerentes de Seguridad, deberá ser aceptada y ejecutada por el Banco. El Banco recomienda la designación de al menos tres Gerentes de Seguridad para garantizar un respaldo adecuado. El Cliente deberá designar a sus Gerentes de Seguridad en el Formulario de Incorporación de Canales TTS. Un Usuario administrador del Cliente también puede actuar como el Usuario administrador de una entidad externa (por ejemplo, un afiliado del Cliente) y ejercer todos los derechos relacionados con este (incluida la designación de los usuarios para la(s) Cuenta(s) de esa entidad externa), sin ninguna designación adicional, si esa entidad externa ejecuta un formulario de Autoridad de Acceso Universal (o cualquier otra forma de autorización aceptable para el banco) que otorga al Cliente acceso a su(s) Cuenta(s). Esto solo se aplica en relación con la(s) cuenta(s) cubierta(s) bajo la autorización pertinente.

*Las Funciones y Responsabilidades del Usuario administrador pueden estar prohibidas en ciertos mercados locales. Por favor, póngase en contacto con su representante de Atención al cliente para obtener más información.

La función del Usuario administrador incluye, pero no está limitada a:

1. Establecer y mantener el acceso y los derechos de los usuarios (incluidos los propios Gerentes de Seguridad), incluidas actividades tales como:

    a. creación, eliminación o modificación de Perfiles de Usuario (incluidos los Perfiles de Usuario administrador) y derechos de titularidad (tenga en cuenta que el nombre de usuario debe alinearse con los documentos de identificación de apoyo)

    b. creación de perfiles de acceso que definen las funciones y los datos disponibles para varios usuarios; y

    c. habilitar y deshabilitar las credenciales de inicio de sesión del usuario.

2. Crear y modificar entradas en bibliotecas mantenidas por el Cliente (como pagos preformateados y bibliotecas beneficiarias) y autorizar a otros usuarios a hacer lo mismo

3. Modificar los flujos de autorización de pago.

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

5. Notificar al Banco si hay alguna razón para sospechar que la seguridad se ha visto comprometida.

Los Gerentes de Seguridad también asignan límites de transacción a los usuarios de los productos del Banco a los que el Cliente tiene acceso. Estos límites no son supervisados ni validados por el Banco; El Cliente debe supervisar estos límites para garantizar el cumplimiento de las políticas y requisitos internos del Cliente, incluidos, entre otros, los establecidos por la Junta Directiva del Cliente o su equivalente.

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. Tenga en cuenta que la disponibilidad de los métodos de autenticación descritos a continuación varía en función de los mercados locales.

Los Gerentes 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 periódicamente, 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 Identificación de Usuario:

Método de Autentificación	**Descripción**
Token: Respuesta al Reto	Ya sea un (i) soft token basado en aplicaciones móviles (por ejemplo, MobilePASS) o (ii) un token físico (por ejemplo, SafeWord Card, Vasco) que en cada caso se utiliza para generar una contraseña dinámica después de autenticarse con un pin de 4 dígitos. Al acceder a CitiDirect BE, el sistema genera un reto y el token utilizado genera una clave de acceso de respuesta que ingresa al sistema.
Token: Contraseña de Un Solo Uso	Ya sea un (i) soft token basado en la aplicación móvil (por ejemplo, MobilePASS) o (ii) un token físico (por ejemplo, SafeWord Card, Vasco) que se utiliza para generar una contraseña dinámica después de autenticarse con un pin de 4 dígitos. Esta contraseña dinámica se ingresa al sistema para obtener acceso.
Código SMS de Un Solo Uso	Se entrega una contraseña dinámica 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.
Código de Voz de Una Sola Vez	Se entrega una contraseña dinámica a un usuario a través de una llamada de voz automatizada, después de lo cual el usuario ingresa la contraseña dinámica y una contraseña segura para obtener acceso al sistema
Autenticación MultiFactor	Se genera una contraseña dinámica a través de una tarjeta SafeWord o un token MobilePASS, 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 Clave y un PIN correspondiente, y pueden ser emitidos por IdenTrust, SWIFT (3SKey) u otros proveedores acordados.
Contraseña 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 manera que se puede ver la información y no se habilitan las capacidades de transacción.
Respuesta de Voz Interactiva ("IVR") y correo electrónico	A los usuarios que se comuniquen con el banco se les pedirá que ingresen un número de PIN o proporcionen otra información para validar el acceso autorizado por teléfono o por correo electrónico.
Fax:	La correspondencia recibida por el Banco, excluyendo las solicitudes MIFT, se realizará una verificación de firmas basada en la información contenida en la tabla de firmas del cliente.
MTLS	La Seguridad de Capa de Transporte Obligatoria (MTLS) crea una conexión de correo electrónico segura y privada entre Citi y la parte externa. Un correo electrónico transmitido enviado utilizando este canal se envía a través de Internet a través de un túnel TLS cifrado creado por la conexión.
PDF Seguro	Los correos electrónicos encriptados se envían a un buzón de correo normal como un Documento PDF que se abre ingresando una contraseña privada, tanto el cuerpo del mensaje como los archivos adjuntos 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 para Iniciar sesión en CitiDirect BE®:
https://portal.citidirect.com/portalservices/forms/loginHelp.pser

Para CitiConnect®:

- Si el Cliente elige usar una conexión de Internet pública para conectarse a Citi, incluyendo HTTPS, FTP seguro y FTP, el Banco y el Cliente intercambiarán certificados de seguridad para garantizar que tanto el canal de comunicación como los mensajes intercambiados estén totalmente encriptados y protegidos. El Banco solo aceptará las comunicaciones que se originen en el enlace de comunicación segura del Cliente utilizando los certificados de seguridad intercambiados, y viceversa, y el Banco solo transmitirá Comunicaciones al enlace de comunicaciones del Cliente utilizando los certificados de seguridad intercambiados.

- Si el Cliente elige usar CitiConnect a través de SWIFT, entonces para cualquier orden de pago e instrucciones que involucren a SWIFT, incluida la modificación o cancelación de dichas órdenes, los Procedimientos que se utilizarán para autenticar que una orden de pago o instrucción fue emitida y autorizada por el Cliente será el indicado en la Documentación Contractual de SWIFT (según dicho término esté definido por SWIFT y pueda ser enmendado o complementado oportunamente), que incluye, entre otros, sus Términos y Condiciones Generales y la Descripción del Servicio FIN o como se establece 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 al Banco se deben proporcionar en el formato y 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 las Comunicaciones entre el Cliente y el Banco. El Banco solo aceptará Comunicaciones que se originen en la dirección IP designada del Cliente, y viceversa, y el Banco solo transmitirá Comunicaciones a la dirección IP designada del Cliente, y viceversa.

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

El Banco requiere:

- La protección del Cliente de los Métodos de Autenticación incluyendo cualquier credencial de inicio de sesión y/o certificados de seguridad asociados con los Métodos de Autenticación (colectivamente, las "Credenciales") y asegurando que el acceso a 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 todas las medidas 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 las personas (y sus credenciales correspondientes) sean identificadas como conformes con los requisitos de legislación ALD 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 entidad o proveedor de servicios externo (incluido, entre otros, cualquier proveedor de nómina de terceros) designado por el Cliente para tener acceso a las Credenciales del Cliente (dicha tercera entidad o el proveedor del servicio se denominará en este documento "Tercero Autorizado") con el fin de acceder y utilizar CitiConnect 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 adopte, todos los pasos razonables para proteger las Credenciales de ser divulgadas a cualquier persona de

Tercera Parte No Autorizada. El Banco está autorizado para actuar en 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 estará transmitiendo datos y de otra manera intercambiando Comunicaciones 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 cifrados líderes en la industria (según lo determine 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 un acceso o uso indebido 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 deberá notificar al Banco de inmediato tal ocurrencia. En caso de acceso o uso indebido por parte de una persona autorizada, el Cliente debe tomar medidas inmediatas para rescindir el acceso y el uso por parte de esa persona autorizada de los servicios o canales de conectividad del Banco.

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

VII. Conclusión

Gracias por elegir Citi Treasury and Trade Solutions (TTS) para sus necesidades de administración de efectivo. No dude en ponerse en contacto con su gerente de relaciones de Citi si tiene preguntas adicionales sobre los servicios de TTS.

VIII. Otras Consideraciones

A. Tarifas por Servicios

Las transacciones del Cliente pueden estar sujetas a tarifas. El cronograma de las tarifas que Citi cobra por la prestación de sus servicios está disponible en: https://www.citibank.co.cr/bancaCorporativa/Avatar/banca-corporativa/cash-management/tarifario-productos-cash-management/ tarifario.htm.

Las tarifas pueden modificarse periódicamente a discreción del Banco y se debitarán automáticamente, en concordancia con los servicios prestados por el Banco, desde cualquiera de las cuentas del Cliente.

B. CitiService y Contactos

CitiService proporciona soporte al cliente y acceso a información sobre cuentas bancarias y otros productos y servicios proporcionados por el Banco. CitiService también es el medio por el cual los clientes pueden enviar solicitudes, quejas y reclamaciones en relación con este.

Las personas autorizadas que se comuniquen con CitiService por cualquiera de los canales habilitados para este fin, ya sea que: por teléfono, correo electrónico u otros canales, se les pedirá que se identifiquen con el nombre de usuario y la contraseña previamente emitidos por CitiService.

El Banco no puede proporcionar información a las personas que se comuniquen con CitiService, de acuerdo con los procedimientos de seguridad interna, si su nombre de usuario y contraseña no coinciden o si el Banco no está seguro de que la persona que accedió al canal sea una persona autorizada.

Los administradores con acceso a CitiService pueden enviar solicitudes por correo electrónico para agregar, modificar o eliminar usuarios y autorizarlos para ver información o realizar solicitudes de CitiService. El cliente debe informar al banco cuando haya algún cambio relacionado con los usuarios autorizados.

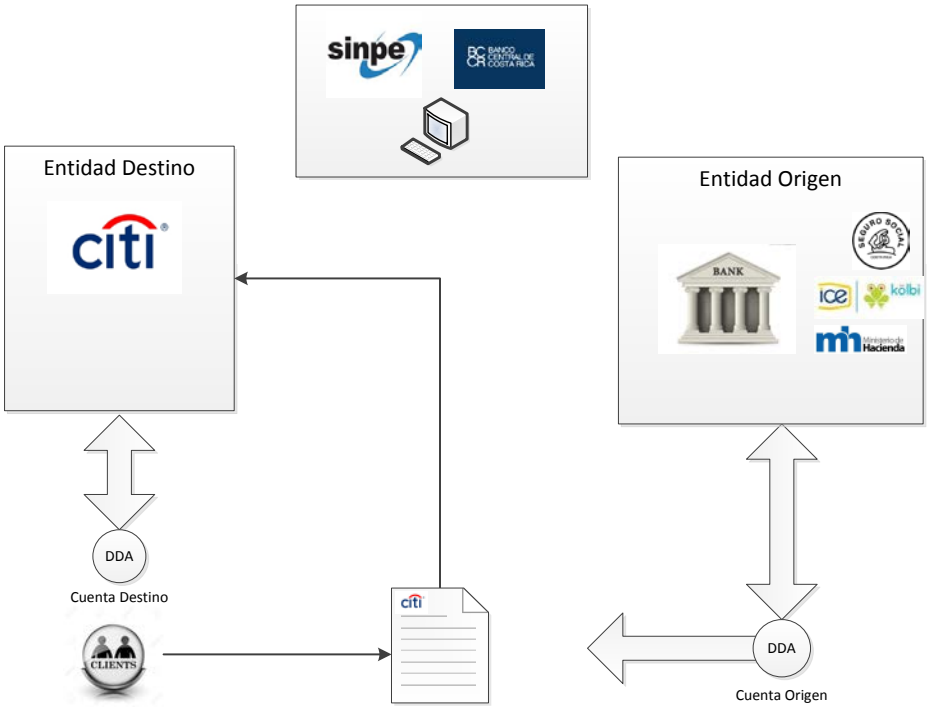
Información de Contacto de CitiService:
Tel: (506) 2201-0888
Fax: (506) 2201-8311
E-mail: citiservicecostarica@citi.com.

Las instrucciones enviadas a través de documentos físicos originales deben enviarse a la siguiente dirección:

Sucursal Corporativa
Centro Corporativo Plaza Tempo
Al lado de Pricesmart San Rafael de Escazu, Edificio B, Piso 5.
Tel: (506) 2201-0800

Sitio web de Banco CMB (Costa Rica) S.A.: https://www.citibank.com/icg/sa/latam/costa-rica/

C. Diagrama de Flujo del Procedimiento de las Órdenes de Débito Directo



Orden de domiciliación Citi (ADA)

Cash Management User Guide

Banco CMB (Costa Rica) S.A.

Treasury and Trade Solutions

citi®

Table of Contents

I. Introduction

Thank you for choosing the solutions of Citi Treasury and Trade Solutions (TTS) for your cash management business needs. The objective of this User Guide is to provide Customers with detailed information on the services available to them. In this guide, Citi Costa Rica, Banco CMB (Costa Rica), which is the subsidiary of Citi in Costa Rica, and Bank may be used interchangeably. This guide can be updated from time to time and the most up-to-date version is available on the Bank's official website. A direct link to the site is included in Section VIII of this guide.

II. Payment Services

A. Types of Payment Services

- Book-to-book Transfers: Electronic funds transfers from a current account in Citi Costa Rica to another current account at Citi Costa Rica.
- Real Time SINPE (RTGS) Transfers: Also known as TEF; electronic transfer of funds with debit in real time through the SINPE (Sistema Nacional de Pagos Electrónicos), the national system of electronic payments.
- Automated Clearing House (ACH) SINPE Credit Transfers: Also known as Payment Default, are electronic interbank funds transfers through SINPE.
- Checks: Negotiable paper-based instruments that can be passed from one person or entity to another and exchanged for money. A check unconditionally instructs a bank to pay a specific amount in a specific currency to a specified person, or to "cash" upon presentment. Checks may be presented for deposit in the Customer's account via a Citi teller or at a network extension. The Bank, at the request of the Customer, will issue books of preprinted checks that allow the Customer to make payments to beneficiaries. Checkbooks will be delivered to the address indicated by the Customer in the request. Checkbooks will be enabled in the Bank's system 24 hours after receipt by the Customer.
- Cross-border Funds Transfers: Allow customers to transfer funds to accounts in other countries in different currencies. The process may involve the use of correspondent banks or other intermediaries and may be subject to additional charges.
- Direct Debits: A means of collecting monies owed by a payer, where the beneficiary (originator) generates the initiating transaction to be processed by the payer's bank against the payer's account. Direct debits are subject to the payer's authorization (if different than originator) and typically used for recurring payments, such as credit card and utility bills, where the payment amounts vary from one payment to another.

B. Sending a Payment

5. The Customer sends a payment instruction to Citi, with the minimum data required by SINPE and indicated in the standard format of interbank payments, which are provided by the Bank to the Customer when the payment service is implemented. Instructions can be sent through:
    - The Bank's electronic channels, including CitiDirect BE® and CitiConnect®,
    - A SWIFT interface
    - A manual request (see Section IV for details on the manual transactions)

    The processing of transactions is subject to specific cut-off times.

The Bank is not obligated to overdraw the Customer's account to comply with the payment instructions unless the Customer has an overdraft previously approved by the Bank. In the event the account is overdrawn, the Customer may be subject to additional charges.

6. Citi forwards the instructions to the relevant payment system for further processing.
7. The payment system forwards the instructions to the beneficiary bank based on the locally defined clearing cycle.
8. The beneficiary bank credits the beneficiary's account as determined by the cycle and type of clearing of the requested service.

   In the event that the information in the payment instruction is incorrect, the payment will be rejected by the SINPE. Citi will return the funds in real time and credit the Customer's current account. The Customer can view, via CitiDirect BE®, the status of SINPE (RTGS) payments in real time. Credit transfers and Automated Clearing House (ACH) SINPE payment details are available via CitiDirect BE® after 10 a.m. of the payment value date.

   From the date of dispatch of the payment by Citi, any delay will depend exclusively on SINPE's operation and the location of the recipient's bank account.

C. PayLink® Manager's Checks

The Customer can request, by instructing the Bank through authorized electronic channels, the issuance of a PayLink® Manager's Check payable to a beneficiary to be withdrawn at a Citi branch or sent to the Customer's offices. The bank will issue the PayLink® manager's check according to the Customer's instruction. Citi manager checks are crossed indicating "|BANK|" or the name of the Bank, for which the money should be paid through a bank only by the deposit of a check or money in Customer's checking account. The officers of the Bank whose signatures appear on the check are not responsible for the content of the check or its use.

In general, a check is a document that the Bank issues with the resources that the Customer has in the bank in your checking account.

For the Bank to issue a check or money order, the Customer must have resources in its account with the Bank or an overdraft previously approved by the Bank.

Issuance and Processing of PayLink® Manager's Checks

4. The Customer instructs the bank to issue the PayLink® check(s) through the agreed electronic channel and the process defined by the administrator of the Customer's electronic platform.
5. Citi debits the funds from the Customer's account and prints the check(s) with a facsimile signature of the Bank's officer(s) and crosses the check(s).
6. Citi delivers the checks per one of the following options, which must be included in the Customer's instruction:

   - Delivery to the offices of the Customer and person(s) authorized to receive checks

- Delivery to the corporate branch of Citi for pickup by the beneficiary or other person(s) previously authorized by the Customer

At the time of pickup, the authorized person must provide an official identification document. In the event the authorized person refuses to present identification, Citi will not deliver the checks.

If a check is not picked up within 60 calendar days following the date of issuance, the Bank shall return it to the Customer.

6. Checks are deposited by the beneficiary and the receiving bank submits them to Citi per SINPE's local agreements.

7. Citi will not make a payment if it considers a check to be altered, forged or stolen, or at the request of a competent authority.

   The Customer may request that the Bank stop payment on a check in accordance with Bank procedures by submitting a written request signed by the legal representative of the Customer indicating the serial number of the check, the date of issuance, the name of the recipient (if available) and the amount, and a Certificate of Power of Attorney for the authorized representative. In addition, the original check should be submitted for its annulment.

   In the event of loss or theft of a manager's check issued by the Bank, the check will be replaced by the Bank at the request of the Customer, prior performance of a guarantee for the term of the statute of limitations for the lost certificate to the satisfaction of the Bank. This bank guarantee should cover the amount of the check(s). The Customer shall submit to the Bank a written request signed by the Customer's legal representative along with a Certification of Power of Attorney. In addition, the Customer must publish a notice of the lost check three consecutive times in a newspaper of national circulation and in the Official Gazette. The Bank shall replace the check(s) fifteen (15) days after the last publication date.

   The period of validity of a PayLink® check is determined by applicable laws and banking practices. If a PayLink® check is not presented for payment on or before the prescription deadline, the Bank will not pay the check subject to applicable banking laws and practices.

   The Customer will be informed through CitiService in case of any problem with the check(s).

D. Revocation and Suspension of Payments

All payment instructions confirmed by the Customer and accepted by the Bank are and shall be final and irrevocable. The Bank shall not incur any liability with the Customer or third parties with respect to this, regardless of whether or not payment has been made.

The Customer has the option to send a payment cancel order to the Bank through the CitiDirect BE® or via a written request that follows the Bank's instructions for suspensions of payment in accordance with the applicable laws and business practices.

E. Receive Direct Debits (Payments)

Citi, as the Customer's paying Bank or destination entity, supports incoming direct debit mandates received from other financial institutions via SINPE. They include:

- Real-time Debits: An entity sends a direct debit to the account of Citi to credit an account in another bank in Costa Rica or an authorized third party (i.e. taxes and utilities charges).
- Direct Debits: An entity sends a direct debit order to debit the Citi account to credit an account in another bank in Costa Rica or an authorized third party (i.e. taxes and utilities charges). These transactions will be processed the same day until 10 p.m.

SINPE direct debits are subject to the payer's authorization and, as such, the Customer must approve and submit a Direct Debit Order (ADA) to the Bank to ensure that the account is configured to enable direct debits from it.

Direct Debit Process

3. In accordance with the direct debit authorization (ADA), Citi processes the instruction and debits the Customer's account according to SINPE's procedures for direct debits.
4. Citi communicates to the collecting financial institution via SINPE for positive or negative (rejections and returns) acknowledgements. In the event that there are insufficient funds in the Customer's account, Citi will not process the payment by direct debit and will return the status of "failed".

The procedure for authorizing debits from a third party is as follows:

4. The Customer signs a direct debit order (ADA) authorizing a third party account to debit the Citi account of the Customer to make the respective payments of the Customer's obligations.
5. The Customer presents to Citi the ADA in original and two copies signed according to the requirements in force.
6. Citi enables the direct debit on its systems within 24 hours, when the Customer's account may be debited by the authorized direct debit originator.

F. Schedule of Payments

The following table details the cut-off times and value dates of different payment types:

Payment Type	Cut-off Time	Value Date
Internal Transfers	6:00 p.m.	T+0 (Same day)
Real Time SINPE (RTGS) Transfers	2:00 p.m.	Real Time
Automated Credit Transfers of the SINPE Clearing House (ACH)	6:00 p.m.	T+1 (Next business day)
Direct Debits	6:00 p.m.	T+1 (Next business day)
Real Time Direct Debits	2:00 p.m.	Real Time
PayLink® Manager's Checks	6:00 p.m.	T+2. (Two business days)

III. Receivables Services

A. Receiving a Payment

- The clearing house forwards the instruction to Citi based on the locally defined clearing cycle.
- Citi credits the account of the Customer. Any rejections or returns by Citi will be credited back to the payer account. The reason for the return is communicated to the payer.

For any payments rejected or returned by Citi, the clearing house or the beneficiary bank, returns the funds to the account of the payer. The reason for the return is communicated to the payer.

B. Direct Debit Collections

A direct debit collection is a financial transaction originated electronically by the Customer instructing the bank to withdraw funds from the bank account of a payer (third party).

Direct Debit Orders

A direct debit orders constitute authorization to the Bank for a third party to debit the current account of the Customer. Duly signed orders must be submitted by each of the Customer's paying agencies to have the proper legal value.

The Citi Direct Debit Order may be downloaded directly from the Citi website under the Direct Debit section or may be designed by the Customer in accordance with the minimum requirements established by the rules and procedures of the Central Bank of Costa Rica, known as the "standardization of the physical order of Direct Debit for Direct Debits".

Direct debit orders received after 6:00 p.m. will be processed on the next business day.

At a minimum, the direct debit order must contain:

- The Customer account number to which the debit is made
- The service under which the account is being debited
- The signature of the account holder, which must be registered in conjunction with his or her identity card number
- Maximum amount authorized to debit and maximum date to debit funds.

This is an agreement between the Customer and the collector in the originating entity. Citi serves only as a channel of a complaint to the SINPE.

Direct Debit Collection Process

4. To collect funds by direct debit, the Customer (beneficiary) issues a direct debit instruction through the CitiDirect BE® electronic banking system.

5. The Customer must submit to Citi direct debit orders duly signed by each of the Customer's paying agencies so that Citi can communicate transactions to the payers' banks.

6. Once a payment transaction is authorized, the payment is sent for processing. The transaction may be executed in real time or at the end of the day via the SINPE, according to the option selected by the Customer.

If a direct debit is not processed successfully through the clearing house, the Customer can view the status of the transaction and the reason for the rejection through CitiDirect BE®. The most common causes of rejection are:

6. The paying bank has not effectively authorized the collector on its system

7. Invalid, non-existent, or closed account

8. Invalid information

9. Accounts has insufficient or no funds

10. Communication problems with the paying entity

The Customer should contact CitiService with any questions related to rejected direct debit transactions.

C. Deposit of Checks and Cash

Citi Accounts in Costa Rica can receive deposits of checks and/or cash through the following options:

3. At the Citi Corporate Branch: Corporate Center Plaza Tempo, next to San Rafael de Escazu, Lobby B, Floor 5.

4. At our network extension (trading partner) collecting agencies

Information related to these services is available through CitiDirect BE®.

Collection by Network Extension

Collection services are offered according to the location, policies, dates and times applicable to each collection point.

The collection service will accept cash payments in US dollars and colones (up to $9,999 or colones equivalent) and checks of any institution of the national banking system. International checks are not accepted under this mode of payment.

Cash collections made through the collection points between Monday and Thursday (inclusive) will be available in the appropriate account on the next business day. Collections made on Friday will be credited on the following Monday. Collections carried out on Saturdays, Sundays or public holidays shall be credited on Tuesday or the next business day. Collected checks will be cleared and settled according to processes established by the Central Bank of Costa Rica.

D. Central Payments

Central Payments is a web-based platform that allows Citi customers to publish pending invoices and accounts receivable to their respective customers, who can access them through customized and individual passwords.

The Customer's debtors can also customize their payment type or complete the payment through the Central Payments platform. With this option, the Customer received detailed information for automated reconciliation processes, reducing and even eliminating operative and manual processes.

Granting Access to Customers

Through the secure file sharing capabilities of CitiDirect BE®, the Customer will provide to the Bank the list of its customers and instructions to grant them access to Central Payment platform.

Accounts Receivable Upload

The Customer will transmit to the Bank via CitiDirect BE® the amount to be paid by each Central Payments user. As a contingency method, the Customer can manually upload the file with this information in Central Payments.

Files shared with the Bank between 8:00 a.m. and 6:00 p.m. on business days will be processed the same day and it will update the debt base during the batch process. If the file is received on the weekend, a holiday, or after cut-off time it will be processed the next day. The client can update the debt information through these files. Each file supersedes the previous information.

Advising a Payment in the Platform

All users with access to Central Payments will be able to consult their commercial outstanding payments, choose the invoices to be paid, and print deposit slips with their debt information.

Such invoices can be paid through these types of transactions:

- SINPE transfers
- Book-to-book transfers
- Direct debits (through Central Payments On-line)
- Deposit in Citi branches
- Deposit in branches of other banks (if the Citi Customer holds an account in other banks).
- Any other means that in the future will be approved.

The Bank will inform the Customer of payments that it receives via Central Payments.

IV. Manual Initiation of Instructions

Citi offers its Customers the ability to initiate manual instructions or Manually Initiated Funds Transfer (MIFT) in the event of a contingency or other scenarios that may involve a manual instruction, including amendment, recall or cancellation of previous instructions.

To enable this capability, the Customer should complete the Global Manual Transaction Authorization (GMTA) form, which supplements the Master Account and Service Terms (MAST), and any other applicable account terms and conditions. The GMTA form should be signed by authorized signatories as listed in the Customer's Board Resolution or equivalent.

The GMTA form identifies those individuals who are authorized to initiate and confirm instructions by manual means, on behalf of the Customer.

Customers who do not provide a GMTA form to Citi, and therefore do not have MIFT payment capability, understand that manual means of communication will not be available to them in the event they are required for contingency or other applicable scenarios that may involve manual instructions.

Additionally, Citi shares concern about operational risk related to sending physical letters to Citi offices, enabling Customers to send manual instructions via CitiDirect BE® as scanned images. To enable this capability, the Customer should request the Manual Payments solution package in CitiDirect BE® Activation Form, where it should indicate which CitiDirect BE® users will be granted this profile and how they can send manual instructions.

Manual Payments through CitiDirect BE® (Pagos Manuales Virtuales)

5. The Virtual Manual Payments service allows the Customer to enter, see, and authorize instructions via images (letters) through the CitiDirect BE®, CitiDirect BE® Mobile, and CitiDirect BE® Tablet Electronic Banking system, using a secure transmission channel and following the current authentication processes (use of the Safeword Card/MobilePASS) as means of accessing and authenticating the users and processing (with preparer and approver levels previously requested and authorized by the Customer).

6. The sending of instructions through the Virtual Manual Payments service is limited to the transactions that the Bank defines for this purpose.

7. Instruction images entered in the Virtual Manual Payments service should be previously signed by the Customer's authorized representatives and will follow the procedure established in the signature validation account contract.

8. The images can only be processed in two format types: PDF and JPG

Notes for Completing the GMTA Form

1. The manual instruction can be sent to Citi via either one of the following communication modes. Please select the option(s) you want to activate in the GMTA form:
   - Letter
   - Fax
   - CitiDirect BE®

2. The initiators can be made available only with Option 1 in the GMTA form.

3. Please provide at least two call-back nominees. Citi recommends that the nominees be located in the same time zone as the country where the Customer's Account is located.

4. When completing the GMTA form, the Customer should list all account numbers that are to be enabled for manual processing on the GMTA Account Information Schedule.

Processing MIFT Instructions

In the event that the Customer requires Citi to process a MIFT instruction:

5. The Customer sends a manual instruction, duly signed, to Citi via the selected communication mode. For movement of funds from the Customer's Account, Citi recommends using the Citi standard manual payment form.

6. Upon receipt of the manual instruction, Citi carries out its internal verification, including but not limited to, reviewing for completeness of the required processing details and verifying the initiators' signature(s) against those provided in the Signature Card. The Customer should take care when completing the Citi standard form for manual payment as it may be rejected if it contains erasures/white-outs.

7. Citi may conduct an additional control by calling back the nominees included in the GMTA form, with the exception of instructions submitted in the Pre-Defined Beneficiary List Form, once they are initially set up. The call-back nominee and the initiator cannot be the same. Confirmation by telephone may be recorded by Citi.

8. Citi processes the manual instruction once Citi determines that all the verifications are successful.

The processing of the instruction is subject to Citi's internal procedures and conditions given that there are alternative electronic channels to perform such instruction.

Updates to Authorizations

If information provided in the GMTA changes, the Customer should submit a new GMTA form which supersedes the previous form. Changes for which Citi should be informed include, but are not limited to:

- Personnel changes
- Changes to a person's name (e.g., due to change in marital status)
- New telephone numbers (e.g., new phone number, new area code, or new city code)
- New account number

Neither a GMTA form detailing just the updated alone, nor a letter or any other form of document will be accepted. This is necessary to assure the operational integrity of the manual communication process.

Deletions to Authorizations

The Customer should submit the name(s) of the nominee(s) to be removed from the GMTA form in a letter on company letterhead and signed by authorized signatories as per the Customer's Board Resolution or equivalent. Again, in the interest of operational integrity, Citi will request a new GMTA form that will supersede all the previous GMTA forms if there are several signature deletions.

V. Information Services: Data Aggregation-Infopool

A. Consolidation Service

Infopool is a single interface to accounts with Citi and third-party banks. The Infopool Service allows daily monitoring of balances and transaction of accounts maintained in different banks across borders and currencies. Thus, Infopool Services consists of consolidating the information on the Customer's bank accounts and those of its subsidiaries on the books of Citi, Citigroup banks and/or on the books of other banks (hereinafter Third Parties), through the CitiDirect BE® electronic banking system.

Citi will only consolidate the information for the accounts indicated by the Customer on the activation form, without making adjustments to the information provided by its issuer and, as such, Citi is not responsible for the content or preciseness of the information on the accounts.

The Customer will authorize Group or Third Party service provider banks to provide to Citi the account information, including personal data. It likewise authorizes Citi to receive this information and to process it.

The Customer has and retains all the rights, titles and interests in the accounts information and permits Citi to consolidate such account information for querying. Given the provision of the service, Citi will only consolidate the information on accounts established by the Customer, without adjusting the information provided by the issuer.

The Customer understands that Infopool is a global service, but some countries have personal data protection laws that limit the compilation, disclosure, processing or transfer of personal data and the account information may include personal data subject to the personal data laws of one or more countries.

B. Procedure

4. The Customer warrants that for each account, regardless of the identity of the account holder, the Customer has the right and is legally authorized to access the account information. Likewise, the account holder authorizes Citi to consolidate such information.

5. For the implementation of the Data Aggregation (Infopool) service the Customer will submit the Account Reporting Request Form and confirm the submittal of the Infopool Sample Letter to the Citi Group and/or Third Party banks on whose books the accounts to be consolidated using this service are held.

6. Infopool users will be those defined by the Customer on the CitiDirect BE® application forms with the profile enabled for queries.

VI. TTS Consolidated Security Procedures

As referenced in the Communications section of the Master Account and Service Terms (or other applicable account terms and conditions) ("MAST") that has been entered into between the Customer and the Bank the following is a description of the security procedures ("Procedures") used by Citi Treasury and Trade Solutions in connection with the following Services or connectivity channels.

- CitiDirect BE® (including Electronic Bank Account Management ("eBAM")), TreasuryVision®, and WorldLink®)
- Interactive Voice Response ("IVR")
- Email/fax with the Bank excluding Manually Initiated Funds Transfer (MIFT)
- CitiConnect®
- Other local electronic connectivity channels

Availability of the Services or connectivity channels will vary across local markets. These Procedures may be updated and advised to the Customer by electronic means or otherwise from time to time. Customer's continued use of any of the above noted services or connectivity channels after being advised of updated Procedures (which may include, but is not limited to, the posting of updated Procedures on CitiDirect BE®, in connection with the service or connectivity channel) shall constitute Customer's acceptance of such updated Procedures. These Procedures are to be read together with the MAST as such MAST may be amended from time to time. Capitalized terms not otherwise defined herein shall have the meanings ascribed to them in the MAST.

A. Security Manager Roles and Responsibilities*

For the applications accessible in CitiDirect BE®, the Bank requires two 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 our communication via the Internet. Any such Communications, when authorized by two Security Managers, will be accepted and acted on by the Bank. The Bank recommends the designation of at least three Security Managers to ensure adequate backup. The Customer shall designate its 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.

* Security Manager Roles and Responsibilities may be prohibited in certain local markets. Please contact your Customer Service representative for further information.

The Security Manager function includes, but is not limited to:

2. Establishing and maintaining the access and entitlements of users (including the Security Managers themselves), including activities such as:

    d. creating, deleting or modifying User Profiles (including Security Manager Profiles) and entitlement rights (please note that user name should align with supporting identification documents)

    e. building access profiles that define the functions and data available to various users; and

    f. enabling and disabling user log-on credentials.

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

7. Modifying payment authorization flows.

8. Allocating dynamic password credentials or other system access credentials or passwords to the Customer's users

9. Notifying the Bank if there is any reason to suspect that security has been compromised.

Security Managers also assign transaction limits to users for those Bank products to which the Customer has access. These limits are not monitored or validated by the Bank; Customer should monitor these limits to ensure in compliance with Customer's internal policies and requirements, including but not limited to, those established by Customer's Board of Directors or equivalent.

B. Authentication Methods

The 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 typically through mechanisms such as User ID / password pairs, digital certificates, and security tokens (deployed via hardware or software) which generate a dynamic password used to access the services or connectivity channels each time the Customer or a user logs in or authenticates themselves. Please note that availability of the Authentication Methods described below varies based on local markets.

Security Managers and all users who want to (a) initiate or approve transactions (and whose User Profile permits them to do so) and/or (b) access the systems in accordance with entitlements should use the available Authentication Methods (which may be updated from time to time as described above).

The following Authentication Methods are available to access the above-noted services or connectivity channels in combination with a User ID:

Authentication Method	**Description**
Token: Challenge Response	Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which in each case is used to generate a dynamic password after authenticating with a 4 digit pin. When accessing CitiDirect BE, the system generates a challenge, and a response passcode is generated by the utilized token and entered into the system.
Token: One-Time Password	Either a (i) mobile application based soft token (e.g. MobilePASS) or (ii) physical token (e.g. SafeWord Card, Vasco) which is used to generate a dynamic

	password after authenticating with a 4 digit pin. This dynamic password is entered into the system to gain access.
SMS One-Time Code	A dynamic password is delivered to a user via SMS, after which the user enters the dynamic password and a secure password to gain access to the system
Voice One-Time Code	A dynamic password is delivered to a user via an automated voice call, after which the user enters the dynamic password and a secure password to gain access to the system
MultiFactor Authentication	A dynamic password is generated via a SafeWord Card or MobilePASS token, after which such dynamic password is entered along with a secure password to gain access to the system.
Digital Certificates	A Digital Certificate issued by an approved certificate authority which is used for authentication. Digital Certificates utilize a Key Storage Mechanism and a corresponding PIN, and may be issued by IdenTrust, SWIFT (3SKey) or other agreed-upon providers.
Secure Password	A user enters their secure password to access the system. A Secure Password typically limits a user's capabilities on the system, such that information can be viewed and no transaction capabilities are enabled.
Interactive Voice Response ("IVR") & email	Users contacting the bank will be prompted to enter a PIN number or provide other information to validate authorized access over the phone or over email.
Fax	Correspondence received by the Bank, excluding MIFT requests, will be signature verified based on the information that is contained in the Customer's board resolution.
MTLS	Mandatory Transport Layer Security (MTLS) creates a secure, private email connection between Citi and the external party. An email transmitted sent using this channel is sent over the Internet through an encrypted TLS tunnel created by the connection.
Secure PDF	Encrypted emails are delivered to a regular mailbox as a PDF Document that is opened by entering a private password, both the message body and any attached files are encrypted. A private password can be set up upon receipt of the first Secure Email received.

To learn more about any of these Authentication Methods, please refer to the Login Help page on CitiDirect BE®: https://portal.citidirect.com/portalservices/forms/loginHelp.pser

For CitiConnect®:

- If the Customer chooses to use a public Internet connection to connect to Citi, including HTTPS, secure FTP, and FTPs, the Bank and the Customer will exchange security certificates to ensure both the communication channel and the messages exchanged are fully encrypted and protected. The Bank will only accept Communications originating from the Customer's secured communication gateway using the exchanged security certificates, and vice versa, and the Bank will only transmit Communications to the Customer's communication gateway using the exchanged security certificates.

- If the Customer chooses to use CitiConnect via SWIFT, then for any payment orders and instructions involving SWIFT, including amending or cancelling such orders, the Procedures that will be used to authenticate that a payment order or instruction is that of the Customer and authorized by the Customer shall be those as provided for in the SWIFT Contractual Documentation (as such term is defined by SWIFT and as may be 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 any other terms and conditions that may be established by SWIFT. The Bank is not responsible for any errors or delays in the SWIFT system. Communications to the Bank are to be provided in the format and type required and specified by SWIFT.

- If using a VPN, both the Customer and the Bank will designate a single IP address from which Communications between the Customer and Bank will be sent and/or received. 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.

- The Customer and the Bank may also use a Hardware Security Module Authentication to accompany VPN Authentication. This requires the Bank and the Customer each to install a device on the servers designated for Communications between the Bank and the Customer.

The Bank requires:

- Customer's safeguarding of the Authentication Methods including any log-on credentials and/or security certificates associated with the Authentication Methods (collectively, the "Credentials") and ensuring that access to and distribution of the Credentials are limited only to authorized persons of the Customer. The Authentication Methods and associated Credentials are the methods by which the Bank verifies the origin of Communications issued by the Customer to the Bank.

- The Customer should take all reasonable steps to protect the Credentials. Accordingly, the Bank strongly recommends that the Customer does not share the Credentials with any third party.

Certain jurisdictions may require individuals (and their corresponding credentials) to be identified as compliant with applicable AML legislation requirements before granting access to perform certain functions.

The Bank understands that the Customer may, in some cases, wish to share the Customer's Credentials with a third party entity or service provider (including without limitation any third party payroll provider) designated by the Customer to have access to the Customer's Credentials (such third party entity or service provider shall be referred to herein as an "Authorized Third Party") for the purpose of accessing and utilizing CitiConnect on the Customer's behalf. In the event that the Customer elects to share its Credentials with an Authorized Third Party, the Bank strongly recommends that the Customer takes, and ensure that any Authorized Third Party takes, all reasonable steps to protect the Credentials from being disclosed to any non-Authorized Third Party personnel. The Bank is authorized to act upon any Communication that it receives from an Authorized Third Party on behalf of the Customer in compliance with these Procedures.

C. Data Integrity and Secured Communications

- The Customer will be transmitting data to and otherwise exchanging Communications with the Bank, utilizing the Internet, email and/or fax, which are not necessarily secure communication and delivery systems. 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 transit.

- If the Customer suspects or becomes aware of, a technical failure or any improper access to or use of the Bank's services, connectivity channels or the 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 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.

- If the Customer utilizes file formatting, 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 Citi, then the Customer will use such software solely for the purpose for which it has been installed.

VII. Conclusion

Thank you for choosing Citi Treasury and Trade Solutions (TTS) for your cash management needs. Please feel free to contact your Citi relationship manager with any additional questions you have regarding TTS services.

VIII. Other Considerations

A. Fees for Services

The Customer's transactions may be subject to fees. A schedule of the fees that Citi charges for the provision of its services are available at: https://www.citibank.co.cr/bancaCorporativa/Avatar/banca-corporativa/cash-management/tarifario-productos-cash-management/tarifario.htm.

Fees may be modified from time to time at the discretion of the Bank and will be debited automatically, in accordance with the services provided by the Bank, from any of the Customer's accounts.

B. CitiService and Contacts

CitiService provides customer support and access to information about bank accounts and other products and services provided by the Bank. CitiService also is the means by which customers can submit applications, complaints and claims in relation to the same.

Authorized persons who contact CitiService by any of the channels enabled for this purpose, whether via telephone, e-mail, or other channels, will be asked to identify themselves with the username and password previously issued by CitiService.

The Bank may not provide information to persons who contact CitiService, according to internal security procedures, if their username and password do not match or when the Bank is not sure that the person who accessed the channel is an authorized.

Administrators with access to CitiService may email requests to add, modify, or delete users and authorize them to view information or make CitiService requests. The Customer must inform the bank when there is any change related to authorized users.

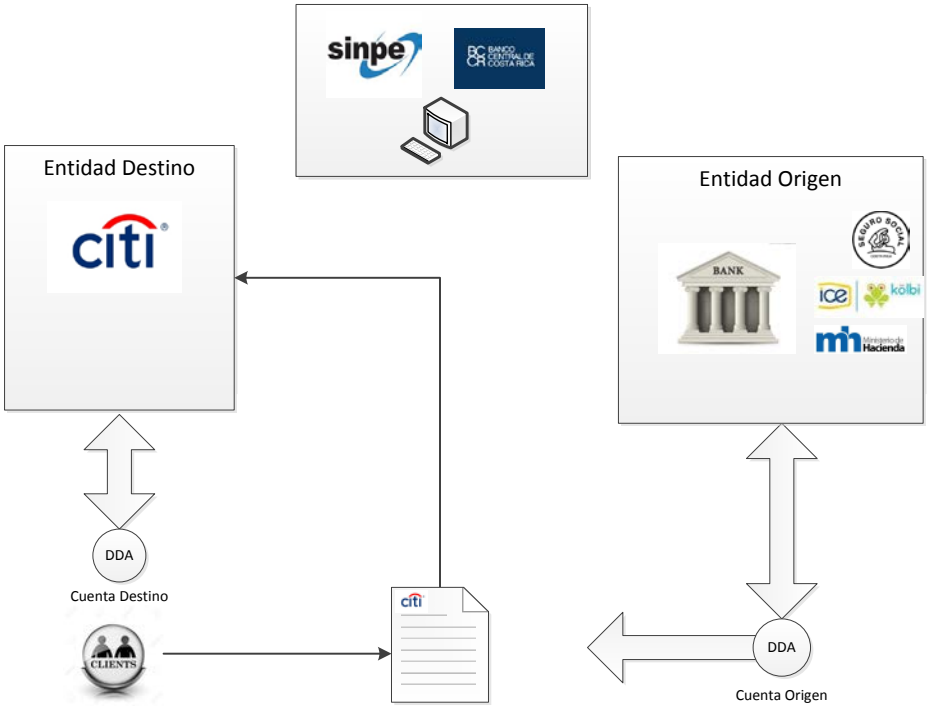
CitiService Contact Information:
Tel: (506) 2201-0888
Fax: (506) 2201-8311
E-mail: citiservicecostarica@citi.com.

Instructions sent via original physical documents must be sent to the following address:

Corporate Branch
Corporate Center Plaza Tempo
Next to Pricesmart San Rafael de Escazu, Lobby B, Floor 5
Tel: (506) 2201-0736

CMB Bank (Costa Rica) S.A website: https://www.citibank.com/icg/sa/latam/costa-rica/

Direct Debit Orders Procedure Flowchart



Orden de domiciliación Citi (ADA)