

# Mejores Prácticas de Seguridad para Pagos Manuales y Electrónicos

Las transacciones bancarias hoy están más digitalizadas que nunca. A pesar de la creciente tendencia hacia los pagos electrónicos y los medios que estos ofrecen para gestionar pagos a proveedores de manera más eficiente, a veces es necesario transferir fondos de manera manual. A continuación veremos algunos de los riesgos de fraude asociados a ambos métodos de pago junto con algunas de las mejores prácticas para estar protegidos contra ellos.

## Pagos Manuales

### ¿Cuáles son los riesgos?

Se considera que los pagos iniciados manualmente conllevan mayores riesgos que las transferencias electrónicas. Estos implican un riesgo de fraude inherente a la intervención manual necesaria para llevar a cabo la transacción. Los pagos manuales incluyen los siguientes riesgos asociados:

- Son fáciles de falsificar, especialmente con las aplicaciones de escritorio actuales que permiten que cualquiera con una computadora pueda imprimir cheques, logos de las compañías y demás.
- Las firmas son fácilmente falsificadas. Las firmas de los signatarios autorizados de las empresas se pueden obtener fácilmente interceptando cheques o documentación de la empresa en el correo.
- Son fáciles de interceptar. Los múltiples puntos de vulnerabilidad las hacen fáciles de enmendar. Las transacciones en papel pueden ser interceptadas en camino hacia el banco donde los detalles del beneficiario pueden ser capturados y alterados para redirigir los fondos hacia cuentas fraudulentas pertenecientes a terceros.

- Las demoras en la conciliación de cuentas favorecen la detección tardía de cualquier fraude así como el riesgo de fraude interno. La instrucción de una transacción manual apócrifa en papel puede ser fabricada por una fuente interna y ubicada en una partida diaria de solicitudes de transacciones para redirigir fondos hacia una cuenta externa fraudulenta.
- Los pagos manuales a menudo pueden ser iniciados sin pasar por procesos de control.
- Generalmente no pueden ser completadas de manera remota, lo que lleva a buscar soluciones alternativas excepcionales como ser cheques y documentos pre-firmados que crean mayores riesgos innecesarios.

### ¿Cómo combatirlos?

Si es absolutamente necesario hacer pagos manuales, hay una serie de medidas que Usted puede tomar en cuenta para protegerse del fraude.

- Si Usted hace pagos a un proveedor en particular regularmente, puede configurar una instrucción de liquidación estándar que sea correctamente autenticada. Una vez que esto esté configurado, todos los pagos deben ser hechos hacia esa cuenta únicamente.

- No acepte enmiendas sin la autenticación apropiada. Por ejemplo, una solicitud para enmendar los detalles de una cuenta bancaria de un proveedor debe ser verificada con un proceso de devolución de llamada, hacia un contacto designado por el proveedor, utilizando un número de teléfono adecuadamente autenticado y brindado de manera independiente.
- Las solicitudes de transferencia manual deben ser ejecutadas con niveles adicionales de aprobación.
- Se deben utilizar siempre formularios pre-establecidos, que permitan su verificación y que no difieran a los utilizados para transmisiones previas.
- Los procesos internos pueden ser implementados sistemáticamente. Los límites de privilegios y autorizaciones pueden establecerse según el riesgo.
- Permiten el acceso remoto. Las transacciones pueden ser llevadas a cabo sin la necesidad de contingencias de alto riesgo o procesos excepcionales si el personal clave está fuera de la oficina.

### ¿Existen riesgos?

A pesar de tener mayor seguridad, los pagos electrónicos no están libres de riesgos. Por ejemplo, ya sea intencionalmente o no, las contraseñas pueden estar comprometidas. Esto puede suceder si se comparten las contraseñas o se registran en lugares inseguros. También existe el riesgo de connivencia que involucra dos partes o empleados trabajando en conjunto para comprometer la integridad del pago. Por lo tanto algunas mejores prácticas para reducir los riesgos de los pagos electrónicos incluyen las siguientes:

## Pagos Electrónicos

### ¿Por qué son seguros?

Los pagos electrónicos son considerados más seguros por una serie de razones, que incluyen:

- Son seguros y cifrados; pueden ser protegidos con un código de un único uso (OTP - por sus siglas en inglés) y con autorizaciones y aprobaciones de múltiples niveles.
- Se realizan velozmente y no tienen riesgos de ser interceptados: las solicitudes de transferencia de fondos están cifradas de forma segura.
- Las firmas no pueden ser falsificadas. Los privilegios y autorizaciones están avalados por un OTP seguro y aprobaciones de múltiples niveles.
- Se hace una conciliación inmediata y automatizada. Las cuentas pueden ser verificadas y conciliadas en tiempo real, lo que permite la detección de anomalías de manera oportuna.
- Asegúrese que las Safeword Cards y PINs sean guardadas siempre de manera separada.
- No permita que las contraseñas sean compartidas o comprometidas.
- Involucre solamente a empleados con niveles de autorización apropiados.
- Haga que todas sus transacciones sean aprobadas por lo menos por un doble control, por ejemplo, imponga la lógica maker-checker.
- Establezca la prueba o conciliación oportuna de cuentas de tal manera que sean identificadas rápidamente.
- Asegúrese que las transacciones de alto valor requieran de múltiples aprobadores siempre.

Treasury and Trade Solutions  
[citi.com/treasuryandtradesolutions](https://citi.com/treasuryandtradesolutions)

© 2016 Citibank, N.A. Todos los derechos reservados. Citi y Citi y Arc Design son marcas de servicio de Citigroup Inc., utilizadas y registradas en todo el mundo. La información y los materiales contenidos en estas páginas, y los términos, condiciones y descripciones que aparecen, están sujetos a cambios. No todos los productos y servicios están disponibles en todas las áreas geográficas. Su elegibilidad para ciertos productos y servicios está sujeta a la determinación final por parte de Citi y/o sus filiales. Cualquier uso no autorizado, la duplicación o la divulgación están prohibidos por ley y puede resultar en un proceso legal. Citibank, NA está constituida con responsabilidad limitada en virtud de la Ley del Banco Nacional de los EE.UU. y tiene su domicilio social en 399 Park Avenue, Nueva York, NY 10043, EE.UU. Citibank, N.A. filial Londres se ha registrado en el Reino Unido en Citigroup Centre, Canary Square, Canary Wharf, Londres E14 5LB, bajo el número BR001018, y está autorizada y regulada por la Oficina del Contralor de la moneda (EE.UU.) y autorizada por el Organismo de de Regulación Prudencial. Sujeta a la regulación de la Autoridad de Conducta Financiera y regulación limitada por el Organismo de Regulación Prudencial. Los detalles sobre el alcance de nuestra regulación por parte del Organismo de Regulación Prudencial están disponibles a solicitud. Número de IVA GB 429 6256 29. En última instancia es propiedad de Citi Inc., Nueva York, EE.UU.

