Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Derogada por la Carta Circular OC-23-15 del 24 de octubre de 2022.

Yesmín M. Valdivieso
Contralora

Carta Circular
OC-19-15

Año Fiscal 2018-2019
28 de junio de 2019

Gobernador; presidentes del Senado de Puerto Rico y de la Cámara de Representantes; senadores; representantes; secretarios de Gobierno; directores de organismos y de dependencias de las tres Ramas del Gobierno del Estado Libre Asociado de Puerto Rico; alcaldes; presidentes de legislaturas municipales, de corporaciones municipales y de juntas directivas; directores de consorcios municipales y de finanzas; y auditores internos[1]

Asunto: **Aspectos a considerar en el proceso y el control de las transferencias electrónicas por la red *Automated Clearing House* (red ACH)[2]**

Estimados señores y señoras:

Los avances tecnológicos han transformado la manera tradicional en que se llevan a cabo los procesos en las entidades gubernamentales. El Gobierno de Puerto Rico, alineado con esta era informática, estableció la política pública de que todo desembolso de fondos públicos se realice mediante métodos electrónicos[3]. Como resultado, las entidades gubernamentales han incorporado en sus operaciones y en los servicios que ofrecen una alternativa que le permite hacer todos los procesos de cobro o pago[4], electrónicamente, a través de la red ACH.

---

[1] Las normas de la Oficina prohíben el discrimen por cualquier motivo prohibido por ley. Para propósitos de esta *Carta Circular* se debe entender que todo término utilizado para referirse a una persona o puesto es sin alusión a géneros.

[2] Es un sistema de transferencia electrónica de fondos administrado por la *National Automated Clearing House Association* (NACHA). Esta asociación rige las operaciones que se llevan a cabo mediante la red.

[3] Artículo 20 de la *Ley 103-2006, Ley para la Reforma Fiscal del Gobierno del Estado Libre Asociado de Puerto Rico de 2006*, según enmendada.

[4] Incluye el depósito directo de cheques de pago de nómina y el débito mensual de pagos, tales como: agua, luz y teléfono. Además, comprende el pago a contratistas y suplidores por servicios prestados o bienes recibidos y el recibo de pagos por concepto de patentes y del impuesto sobre ventas y uso (IVU), entre otros.

PO BOX 366069 SAN JUAN PUERTO RICO 00936-6069
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136
TEL. (787) 754-3030 FAX (787) 751-6768
E-MAIL: ocpr@ocpr.gov.pr INTERNET: www.ocpr.gov.pr
www.facebook.com/ocpronline www.twitter.com/ocpronline

Derogada por la Carta Circular OC-23-15 del 24 de octubre de 2022

El uso de la red ACH conlleva unos riesgos inherentes asociados a la transferencia electrónica, por la sensibilidad de la información que se transmite, lo que requiere una estructura de control interno que permita mitigar los mismos. La Oficina del Contralor de Puerto Rico, ante el aumento en la utilización de este mecanismo, emite esta *Carta Circular* para orientar a los funcionarios y los empleados de las entidades sobre los controles que deben tener para salvaguardar los fondos públicos que se remiten por medio de transferencias electrónicas, ya sea para el pago directo de la nómina o por bienes y servicios prestados por suplidores del gobierno.

Los funcionarios principales de las entidades que utilicen la red ACH para efectuar pagos y el personal designado para trabajar con el proceso de las transferencias electrónicas, entre otras cosas, deben considerar los siguientes aspectos:

a. Formalizar un acuerdo escrito con la institución financiera donde mantienen sus cuentas, en el cual aceptan regirse por las normas establecidas en la red ACH. Este acuerdo debe ser completado en todas sus partes y estar firmado por el funcionario principal de la entidad gubernamental o su representante autorizado. La entidad debe mantener una copia del acuerdo en sus registros. El funcionario principal de la entidad debe aprobar la suscripción a la red ACH. Algunos de los asuntos que debe atender el acuerdo son:

    - La entidad debe requerir a la institución financiera que no se expidan tarjetas de débito de la cuenta, las cuales permitan el retiro de efectivo en cajeros automáticos (ATM, por sus siglas en inglés) o realizar transacciones de compra, ya sea en Internet o en establecimientos comerciales.

    - El funcionario principal de la entidad debe autorizar, por lo menos, a dos funcionarios o empleados para que se encarguen de contratar los servicios con el banco.

    - Se debe designar personal alterno, en caso de que la persona responsable de originar las transacciones se ausente de forma prolongada, ya sea por enfermedad, vacaciones o cualquier otra circunstancia. La persona designada como principal debe tomar vacaciones, al menos, una vez al año.

    - La entidad debe asegurarse de gestionar adiestramientos, operativos y de seguridad, sobre el funcionamiento de la red ACH. Además, es responsable de obtener el apoyo técnico que sea necesario para proveer asistencia a los usuarios.

    - Los firmantes en la cuenta no pueden solicitar préstamos o cualquier otro crédito utilizando como garantía los fondos de la entidad.

b. Solicitar y obtener el consentimiento por escrito de empleados y suplidores, en el cual se establezca que toda transacción de pago se realiza mediante transferencia electrónica. La autorización debe incluir información relacionada con: el beneficiario; el tipo de pago que se autoriza realizar (nómina, dieta y millaje, rembolso de gastos, entre otros); el detalle de la cuenta, incluidos el número y el tipo de cuenta (cheques o ahorro); y el número de ruta y tránsito de la institución financiera. El documento de autorización debe estar firmado por el empleado o proveedor y vigente al momento de enviar las transacciones por la red ACH. Además, mediante identificación o presentación de la evidencia,

asegurarse de que el empleado o proveedor es titular de la cuenta bancaria. El documento debe permanecer en los registros de la entidad y se le debe proveer copia al beneficiario. También la entidad debe generar una notificación para informar al empleado o proveedor cada vez que se le hace una transferencia electrónica. De igual forma, debe notificar al beneficiario, con anticipación, sobre los cambios en la fecha o el importe del depósito directo o del pago.

c. Establecer una adecuada segregación de deberes entre los funcionarios y empleados de la entidad que participan en el proceso de las transferencias electrónicas por la red ACH. Los controles que se establezcan deben asegurar que la persona que genera las transacciones sea distinta a la persona que revisa y aprueba las mismas. Por lo general, esta última posee un mayor nivel de autoridad en la estructura organizacional.

d. Designar un funcionario o empleado, ajeno al proceso y a la aprobación de las trasferencias electrónicas por la red ACH, para monitorear las cuentas de banco y estar atento a cualquier alerta. Esta persona, además, debe tener acceso a los reportes de la aplicación.

e. Mantener, para sus registros, una copia de los documentos justificantes de las transferencias por el período de conservación, conforme a la reglamentación aplicable.

f. Registrar la transferencia electrónica con la fecha e importe de la transacción, la cuenta utilizada y el número de referencia asignado en el sistema de contabilidad de la entidad.

g. Atender las notificaciones de cambio[5] dentro del tiempo establecido, ya sea por NACHA o por la institución financiera.

h. Inactivar, inmediatamente, aquellos funcionarios o empleados de la entidad que cesan en sus funciones, ya sea por licencia sin sueldo, renuncia o muerte.

i. La función de auditoría de la entidad, establecida internamente o mediante legislación, debe considerar dentro de su plan de auditorías la evaluación de las transferencias electrónicas que se realizan por la red ACH.

Derogada por la Carta Circular OC-23-15 del 24 de octubre de 2022

[5] Es una entrada no monetaria que remite la institución financiera a la entidad gubernamental para identificar información incorrecta contenida dentro de una transferencia por la red ACH y también proporcionar los datos correctos en el formato preciso para ser utilizado en futuras transacciones. Algunas de las razones para que la institución financiera emita una notificación de cambio son: errores en el número de cuenta o de ruta; información incorrecta en el nombre del empleado o del proveedor; y código de transacción equivocada.

j. Observar las políticas y los procedimientos de seguridad en los sistemas[6], respecto a lo siguiente:

- La configuración de los usuarios se debe realizar conforme a los niveles de autorización requeridos para efectuar las trasferencias electrónicas por la red ACH. También se deben establecer los privilegios que tienen los usuarios, tales como: generar archivos de pago, solicitar suspensión de pago (*stop payment*) y transferencia electrónica.

- Los usuarios deben utilizar contraseñas que incluyan una combinación de números, letras (mayúsculas y minúsculas) y caracteres especiales, según el sistema lo permita; y, por lo menos, ocho caracteres. También se le debe requerir a los usuarios que cambien sus contraseñas, como mínimo, cada seis meses.

- Se tomen las medidas adecuadas para garantizar que todas las identificaciones de usuario, las contraseñas y la información de los métodos de autenticación emitidos a sus empleados están protegidos y se mantienen confidenciales. Además, el personal que trabaje con las trasferencias electrónicas debe comprender la necesidad de la seguridad del usuario, los controles relacionados con las contraseñas y la separación de tareas.

- Las comunicaciones relacionadas con las transferencias electrónicas que se realizan por la red ACH, deben estar encriptadas.

- Los equipos computadorizados deben tener instaladas aplicaciones para la prevención y detección de programas no deseados, tales como virus, *spyware*, *malware* y *adware*. Además, deben mantener el sistema con las últimas actualizaciones de estas aplicaciones. También el sistema debe tener un *firewall* para proteger la conexión de internet[7].

- La entidad debe fijar múltiples factores de autenticación[8] para corroborar la identidad de las personas que originan la transferencia y asegurar que el usuario es quien dice ser. Esta medida de seguridad, además de limitar el acceso a los datos y las aplicaciones, permite verificar la legitimidad de una transacción.

Derogada por la Carta Circular OC-23-15 del 24 de octubre de 2022

---

[6] La *Política Núm. ATI-003, Seguridad de los Sistemas de Información*, del 7 de noviembre de 2016, establece las directrices generales relacionadas con las políticas de seguridad que deben seguir las agencias adscritas a la Rama Ejecutiva del Estado Libre Asociado de Puerto Rico.

[7] Según requerido por la *Política Núm. ATI-014, Manejo de Firewalls*, del 7 de noviembre de 2016.

[8] Se refiere al mecanismo de seguridad por el cual las personas se autentican a través de más de un procedimiento de seguridad y validación requerido. La autenticación multifactorial se construye a partir de una combinación de dos o más credenciales independientes, relacionadas con la validación física (deslizar una tarjeta o colocar un *token* de seguridad); lógica (usar una contraseña, un PIN o una pregunta de seguridad); y biométrica (escanear una huella dactilar).

- La entidad se debe asegurar de que la opción de alertas del sistema esté activada. Esto permite que la entidad monitoree las entradas y salidas en la aplicación mediante la cual se genera la transferencia electrónica y pueda identificar cualquier actividad sospechosa. El acceso a las alertas que emita el sistema debe estar restringido al personal de auditoría interna de la entidad u otro personal ajeno al proceso y la aprobación de las transferencias electrónicas por la red ACH.

Cualquier información adicional pueden comunicarse con la Oficina Anticorrupción y Relaciones Externas al (787) 754-3030, extensiones 5700, 5702 y 5703.

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,

Yesmín M. Valdivieso

Derogada por la Carta Circular OC-23-15 del 24 de octubre de 2022.