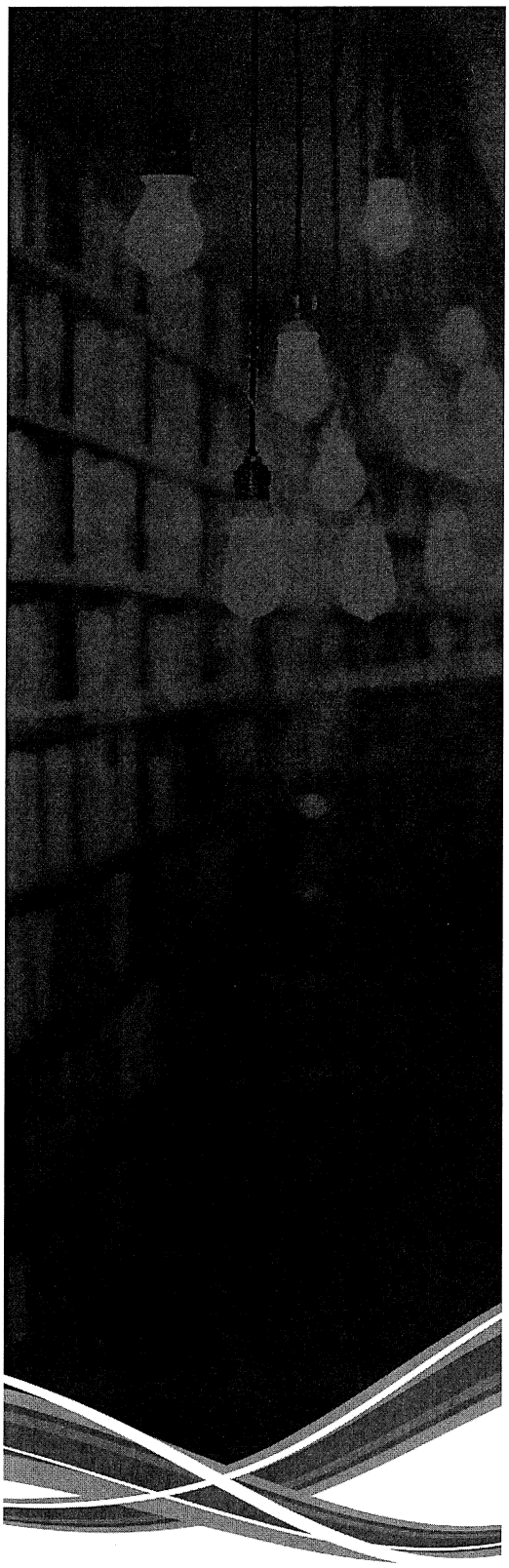

INFORME DE EXAMEN

OIG-E-22-005

DEPARTAMENTO DE DESARROLLO ECONÓMICO Y COMERCIO (DDEC)

COMPAÑÍA DE TURISMO

12 de octubre de 2021

OIG

OFICINA DE LA INSPECTORA GENERAL

GOBIERNO DE PUERTO RICO

TABLA DE CONTENIDO

PÁGINA

RESUMEN EJECUTIVO

La Oficina del Inspector General de Puerto Rico (OIG), realizó un examen de controles internos en la Oficina de Finanzas e Informática de la Compañía de Turismo del Departamento de Desarrollo Económico y Comercio del Gobierno de Puerto Rico (Oficina). El propósito de dicha intervención era corroborar que los procesos llevados a cabo al realizar transferencias electrónicas utilizando la Red *Automated Clearing House* (Red ACH)[1], se realizaran conforme a las leyes y reglamentos aplicables.

Las entidades gubernamentales utilizan las transferencias electrónicas en los procesos de cobro o pago. Incluyendo el depósito directo de cheques de pago de nómina y el débito mensual de pagos habituales.

El examen realizado detectó las siguientes deficiencias:

a. La autorización de pago mediante transferencia electrónica no mantiene datos de forma precisa, que provea evidencia de la titularidad, de la cuenta de banco, del empleado o suplidor.

b. Falta de aprobación y de disposiciones específicas en las Normas y Procedimientos para Transferencias Electrónicas. El procedimiento no está aprobado por la directora ejecutiva o la junta de directores de la Oficina, según requerido.

c. Falta de acuerdos de confidencialidad y seguridad y de adiestramiento a los empleados sobre las normas y procedimientos en la seguridad de información.

d. Deficiencias relacionadas con las solicitudes de acceso de los usuarios a las aplicaciones de la Oficina y la falta de revisiones periódica de los accesos y roles de los usuarios en los sistemas.

La evaluación realizada a los documentos, y la información recopilada durante el examen, reflejó que la Oficina cumplió parcialmente con las leyes y reglamentos aplicables a los procesos de transferencias electrónicas. Las deficiencias encontradas, podrían incidir en la ocurrencia de errores que conlleven la pérdida de fondos públicos. Por lo cual, se acompañan diferentes recomendaciones, las cuales deben ser implementadas por la entidad intervenida en aras de fortalecer los controles internos y asegurar la sana administración pública.

La OIG está comprometida en fomentar los más óptimos niveles de integridad, honestidad, transparencia, efectividad y eficiencia en el servicio público. De igual forma rechaza todo acto, conducta o indicio de corrupción por parte de funcionarios o empleados públicos que inflija sobre la credibilidad del Gobierno de Puerto Rico y sus entidades.

[1] Transferencia Electrónica ACH — es una transferencia de fondos entre instituciones bancarias procesadas a través de la red *Automated Clearing House*.

De usted conocer sobre actos que podrían poner el peligro el buen uso de fondos públicos, así como actos que podrían constituir corrupción, puede comunicarse con la línea confidencial de la OIG al 787-679-7979 o a través del correo electrónico informa@oig.pr.gov.

El presente informe se hace público conforme con lo establecido en la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (Ley Núm. 15-2017) y otras normativas aplicables.

INFORMACIÓN SOBRE LA ENTIDAD EXAMINADA

La Oficina fue creada por virtud de la Ley Núm. 10 del 18 de junio de 1970, según enmendada, conocida como *Ley de la Oficina de Turismo del Departamento Económico y Comercio del Gobierno de Puerto Rico* con el propósito de promover, desarrollar y mejorar la industria turística de Puerto Rico. La Oficina es administrada por un director ejecutivo que es nombrado por el gobernador, con el consejo y consentimiento del Senado de Puerto Rico, y se desempeñará en el cargo hasta que su sucesor sea nombrado y tome posesión del mismo. El director ejecutivo de la Oficina responderá directamente al secretario del Departamento de Desarrollo Económico y Comercio (DDEC). Además, el director ejecutivo contará con un Consejo Asesor, con miembros compuesto por representantes del sector turístico quienes no cobrarán salario, compensación o dietas por su participación en el referido consejo. Dicho Consejo Asesor aconsejará al director ejecutivo en cualquier materia que le sea referida, incluyendo, pero sin limitarse al Programa de Préstamos y Garantías de Préstamos a Empresas de Interés Turístico en Puerto Rico y el Fondo para el Desarrollo de la Industria Turística de Puerto Rico.

Desde la última enmienda a la Ley Núm. 10 por la Ley Núm. 141-2018, *Ley de Ejecución del Plan de Reorganización del Departamento de Desarrollo Económico y Comercio de 2018*, la cual designó a la Compañía de Turismo de Puerto Rico como una entidad operacional del DDEC; esta Oficina se mantiene como una corporación pública adscrita al mismo. Esto, hasta tanto el secretario del Departamento de Desarrollo Económico y Comercio (DDEC) presente una certificación al gobernador y a la Asamblea Legislativa, en la que indique que el proceso de transición correspondiente fue completado. En ese momento, la Oficina pasará a ser una entidad consolidada del DDEC. Al finalizar el examen, dicho proceso no había finalizado, por lo que la Oficina continuaba adscrita al DDEC como una entidad operacional.

BASE LEGAL

El presente informe se emite en virtud de los Artículos 7, 8 y 9 de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico*.

OBJETIVOS

El examen estuvo dirigido a evaluar si los controles establecidos relacionados a las transferencias electrónicas de red ACH por parte de la Oficina de Contabilidad, Oficina de Finanzas y Oficina de Tecnología de Información, cumplen con las disposiciones de la Ley Núm. 103-2006, según enmendada, conocida como *Ley para la Reforma Fiscal de 2006*, el *Reglamento para Usuarios que Manejan Sistemas de Tecnología de Información* aprobado el 14 de septiembre de 2010 y la Carta Circular OC-19-15, *Aspectos a Considerar en el Proceso y Control de las Transferencias Electrónicas por la Red Automated Clearing House (red ACH),* emitida el 28 de junio de 2019 por el entonces Contralor de la Oficina del Contralor de Puerto Rico.

ALCANCE Y METODOLOGÍA DEL EXAMEN

El examen cubrió del 1 de noviembre de 2019 al 30 de abril de 2020, estuvo dirigido a determinar, si los controles internos utilizados en las Oficinas de Finanzas e Informática de la Oficina estaban acorde con las leyes y reglamentos aplicables, al momento de realizar transferencias electrónicas.

Para realizar la intervención se utilizó la siguiente metodología:

1. Estudio de reglamentos aplicables
2. Análisis de documentos e información
3. Selección de muestra de transferencias electrónicas y análisis de sus justificantes, durante el período de intervención.
4. Pruebas de control interno
5. Entrevistas a empleados.

En algunos aspectos se examinaron transferencias, documentos y operaciones de fechas anteriores y posteriores.

HALLAZGOS

A continuación, detallamos los hallazgos relacionados con las situaciones detectadas durante el transcurso del presente examen.

Hallazgo 1 – Deficiencias en el documento de autorización de pago mediante transferencias electrónicas

Situación

La Oficina autorizó el 10 de abril de 2015 a la división de contabilidad el uso del *Formulario Pago por Transferencia Electrónica/Electronic Transfer Payments (Formulario)*. Esto con el propósito

de establecer medidas de control interno que evidencien la autorización de las transferencias electrónica ACH realizadas utilizando la *red Automated Clearing House (red ACH)*.

El examen realizado a 385 formularios de pago por transferencias electrónicas reveló lo siguiente:

a. El 100% de los formularios no contenía lo siguiente:

    1. Una codificación, lo que no permite identificar cual es el formulario oficial o el más reciente.

    2. Un apartado o renglón que permita al director auxiliar de contabilidad o su representante autorizado, aprobar la transferencia mediante su nombre, firma y fecha de aprobación.

    3. Un apartado con la información de empleado o suplidor que contenga lo siguiente:

        - Que se identifique si el pago era realizado a un empleado o a un suplidor. Los 60 formularios de suplidores fueron identificados por el nombre que colocaron en el apartado de beneficiario.

        - Números de teléfono o correo electrónico para poder contactar al empleado o suplidores.

        - Un apartado para indicar persona contacto o representante en el caso de suplidores.

    4. Un apartado para indicar el tipo de pago que se realiza. Por ejemplo, si es: servicios, dietas, nómina, rembolso de gastos, u otros.

b. No se requiere evidencia o documentación que asegure, que el empleado o el proveedor es el titular de la cuenta bancaria.

c. En los 325 formularios completados por los empleados de la Oficina se detectaron las siguientes deficiencias:

    - Cincuenticuatro (54) formularios no proveen un renglón para la firma y fecha de completado.

    - Veintiocho (28) formularios contenían solo la autorización del empleado, estas no reflejan la ruta y cuenta del banco. Tampoco se encontró evidencia de la titularidad de la cuenta bancaria.

    - Veinticinco (25) empleados tenían al menos 2 formularios de pagos completados con diferentes tipos de cuentas. No se observó que fueran cancelados o anulados aquellos formularios que sustituían al anterior por cambios de cuentas bancarias.

- Seis (6) formularios indicaban en el apartado del nombre del beneficiario una letra S y unos números, en lugar del nombre del empleado.

- Cuatro (4) formularios presentaban información con diferentes cuentas bancarias, anotadas en notas adhesivas (conocidas como *post-it)*. El empleado no actualizó el formulario con la información final.

Criterio

Las situaciones comentadas son contrarias al artículo 20 de Ley Núm. 103-2006, según enmendada, conocida como *Ley para la Reforma Fiscal de 2006*, que establece lo siguiente:

> *Artículo 20. - Legalidad y Exactitud de Gastos, Responsabilidad*
>
> *El secretario, director, administrador o jefe de agencia y/o los funcionarios y empleados en que éste delegue y/o cualquier representante autorizado del mismo o de la agencia correspondiente, serán responsables de la legalidad, exactitud, propiedad, necesidad y corrección de todos los gastos que se autoricen para el pago de cualquier concepto. A estos fines, deberán producir y someter todos los informes que requieren las leyes, reglamentos, procedimientos y normas aplicables, dentro del término establecido para los mismos...*

Además, en el inciso b. de la Carta Circular OC-19-15 de 28 de junio de 2019 emitida por la Oficina del Contralor de Puerto Rico, titulada *Aspectos a considerar en el proceso y control de las transferencias electrónicas por la red Automated Clearing House (red ACH)*, establece lo siguiente:

> *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:*
>
> *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 a 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 ahorros); 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 notificación 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 o del pago.

Efecto

Lo comentado impide mantener una administración y control adecuado sobre los desembolsos, lo que propicia el ambiente para la comisión de errores e irregularidades. El no mantener un formulario regulado y que contenga datos precisos del empleado o suplidor puede ocasionar el que se ejecute un pago indebido.

Causa

La situación comentada se atribuye a que el director de Asuntos Fiscales y demás funcionarios responsables de los desembolsos, mediante transferencias electrónicas, se apartaron de las disposiciones citadas, en la Carta Circular OC-19-15, al no reglamentar el proceso de dichas transferencias. Además, el no aprobar y establecer disposiciones específicas en las normas y procedimientos para transferencias electrónicas, causa que no se defina un formulario que contenga información precisa y confiable.

Ver recomendaciones 1, 2 y 4 a la 5.

Hallazgo 2 – Deficiencias en los procesos y controles establecidos para las transferencias electrónicas

Situación

Los avances tecnológicos y la política pública establecida de que todo desembolso de fondos públicos se realice mediante métodos electrónicos, hace meritorio que todo funcionario a cargo de estos procesos se mantenga a la vanguardia y se capacite continuamente en el tema de referencia. De igual forma, es necesario establecer y mantener unos controles efectivos para el monitoreo de las cuentas.

La información provista y evaluada respecto a los procesos y controles establecidos por la Oficina reveló que:

a. No se estableció un acuerdo escrito con la institución financiera, donde mantiene sus cuentas, en el cual acepten regirse por las normas de ACH.

b. No se ofrecieron adiestramientos a los empleados encargados del área de Contabilidad de la Oficina sobre las normas y seguridad de las transferencias electrónicas.

c. No se asignó o nombró un funcionario o empleado ajeno al proceso de aprobación de transferencia a través de la red ACH, para monitorear y dar seguimiento a las alertas del sistema.

Criterio

En los incisos a y d de la Carta Circular OC-19-15 de 28 de junio de 2019 emitida por la Oficina del Contralor de Puerto Rico, *Aspectos a considerar en el proceso y control de las transferencias electrónicas por la red Automated Clearing House (*red ACH), establece lo siguiente:

> *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:*
>
> *Formalizar un acuerdo escrito con la institución financiera donde mantiene sus cuentas, en cual aceptan regirse por las normas establecidas en la red ACH. ...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 asegurarse de gestionar adiestramiento, 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.*
>
> *Designar un funcionario o empleado, ajeno al proceso y a la aprobación de las transferencias electrónicas por la red ACH, para monitorear las cuentas del banco y estar atento a cualquier alerta. Esta persona, además, debe tener acceso a los reportes de la aplicación.*

Además, la situación comentada en el **apartado b.** es contraria al apartado H de la Política ATI-003, *Seguridad de los Sistemas de Información*, de la Carta Circular 140-16, aprobada por el director de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016 que establece:

> *H. Adiestramientos*
>
> *Cada agencia es responsable de proveer adiestramientos al personal para que estén al tanto de los controles de seguridad y los beneficios correspondientes.*
>
> *El personal de sistemas de información y telecomunicación deberá estar adiestrado y mantenerse actualizado sobre los aspectos de seguridad de su área.*
>
> *Se deben proveer mecanismos para capacitar a todos los empleados periódicamente.*

Efecto

Lo comentado impide a la Oficina contar con controles internos de los procesos relacionados a las transferencias ACH, que se realicen de forma correcta y confiable. Además, impide responder

eficientemente al momento de reconocer o detectar situaciones que sean adversas para los recursos económicos de la Oficina.

Causa

La situación comentada obedece, a que el director ejecutivo no formalizó un acuerdo escrito con el banco donde se estableciera los aspectos a considerar y control de las transferencias conforme lo indica la Carta Circular OC-19-15 emitida por la OCPR y Carta Circular Carta Circular 140-16 emitida por OGP.

Ver recomendaciones 1, 2, 6 a la 7.

Hallazgo 3 – Falta de aprobación y de disposiciones específicas en las Normas y Procedimientos para Transferencias Electrónicas

Situación

El 16 de junio de 2020 el principal oficial financiero de la Oficina, estableció el procedimiento interno, *Normas y Procedimientos para Transferencias Electrónicas*. Este tiene el propósito de enmendar el *Artículo 10, Inciso A del Manual de Contabilidad – Procedimiento de Cuentas por Pagar,* para establecer normas y procedimientos para el pago a proveedores por compras de bienes y servicios adquiridos por la Oficina, reembolsos de gastos a empleados, reclamaciones, estipendios y créditos a ejecutar mediante pago por transferencias electrónicas.

De la evaluación realizada se detectaron las siguientes situaciones:

a. El procedimiento interno establecido no está aprobado por la directora ejecutiva o la junta de directores de la Oficina según corresponde, lo que se hace necesario ya que enmienda un procedimiento que si estaba debidamente aprobado.

b. Este procedimiento interno, refleja las siguientes deficiencias:

    1. Los procesos indicados no incluyen los realizados con el banco referente a las transacciones ACH:

        - No establece las autorizaciones requeridas para evidenciar el nombre y cuenta de banco indicado en el formulario *Pagos Por Transferencias Electrónicas/Electronic Transfer Payments*.

        - No establece los niveles de autorización del personal autorizado para crear y aprobar las transferencias ACH ni de los funcionarios autorizados para asignar las cuentas de acceso al banco.

    2. No establece revisión periódica de 6 meses o anualmente de las funciones y responsabilidades de cada funcionario y de los controles de acceso.

3. Hace referencia, pero no incluye el formulario enmendado de Pagos por transferencias electrónicas/*Electronic transfer Payments*.

Criterio

En los Artículo 4 (h) de la Ley Núm. 10 de 18 de junio de 1970, según enmendada, conocida como *Ley de la Oficina de Turismo del Departamento Económico y Comercio del Gobierno de Puerto Rico,* establece lo siguiente:

> *Artículo 4. - [Derechos, Deberes y Poderes] (23 L.P.R.A. § 671d)*
>
> *Para llevar a cabo los propósitos la Oficina de Turismo del Departamento de Desarrollo Económico y Comercio tendrá y podrá ejercer los derechos, deberes y poderes que sean necesarios o convenientes para promover, desarrollar y mejorar la industria turística, incluyendo, pero sin intención de limitar, los siguientes: ...*
>
> *...(h) Establecer las reglas y normas necesarias para la conducción de los procedimientos administrativos, tanto de reglamentación como de adjudicación que celebre conforme a la Ley 38-2017, según enmendada.*

Las situaciones comentadas en el **apartado b**. no cumplen con lo establecido en los incisos b y c de la Carta Circular OC-19-15, *Aspectos a considerar en el proceso y control de las transferencias electrónicas por la red Automated Clearing House (*red ACH) emitida el 28 de junio de 2019 por la Oficina del Contralor de Puerto Rico que establecen:

> *Solicitar y obtener el consentimiento por escrito de empleados y suplidores, en el cual se establezca que toda transacción de pagos 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, reembolso de gastos, entre otros); el detalle de la cuenta, incluidos el número y el tipo de cuenta (cheque 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 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, con anticipación, sobre los cambios en la fecha o el importe del depósito directo o del pago.*
>
> *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.*

Efecto

La situación comentada impide estandarizar, adecuadamente, el proceso para el desarrollo y fortalecimiento de los controles internos. Además, no permite a la gerencia disponer de procesos que permitan realizar su labor en concordancia con las políticas establecidas por el gobierno, como parte de los retos por los avances tecnológicos y la política pública establecida.

Causa

Las situaciones mencionadas obedecen a que el principal oficial financiero no siguió el debido proceso de aprobación e implementación de los procedimientos de la Oficina. El propósito de mantener normas y procedimientos actualizados sirve de apoyo en el desarrollo de las operaciones, que en forma cotidiana se realizan en la Oficina, además, de fortalecer el control interno.

Ver recomendaciones 1, 2 y 8 a la 9.

Hallazgo 4 – Falta de acuerdos de confidencialidad y seguridad y de adiestramientos a los empleados sobre las normas y procedimientos de la seguridad de la información

Situación

a. De la información recibida y evaluada se encontró que la Oficina no cuenta con Acuerdos de Confidencialidad y Seguridad de Información y Protección de Equipos, firmado por el empleado y de empleados de otras agencias en asignación administrativa, que detalle los deberes y responsabilidades del usuario en el uso de los sistemas de tecnología de información y en cuanto a la protección de los equipos con los que cuenta la Oficina.

   En adición, el director auxiliar de Sistemas de Tecnología, presentó como evidencia la *Forma 240.03* llamada como *Certificación de Orientación y Entrega de Documentos a Empleados de Nuevo Nombramiento,* formulario tipo *checklist.* No obstante, este documento no es un acuerdo de confidencialidad ya que este es un formulario de orientación a empleados de nuevo ingreso, en el mismo certifican haber recibido las políticas de la Oficina.

b. El Reglamento para Usuarios que Manejan Sistemas de Tecnología de Información, aprobado el 14 de septiembre de 2010, tiene el propósito de establecer las políticas, normas, guías y controles para la administración y el manejo de los sistemas de tecnología de información de Turismo.

   El referido reglamento establece en sus definiciones el Concienciar (*Awareness*) como un programa de orientación el cual se ofrece periódicamente a todos los usuarios en todos los niveles. En este programa se resalta la importancia de mantener medidas de control adecuadas al utilizar la información. También se discute la política pública sobre Seguridad de Información y las reglamentaciones que exigen estos controles, así como el efecto que

tendrá el no cumplir con ellos. No obstante, no se establece en el reglamento como se estará implementando el programa ni las personas encargadas del mismo.

De la evaluación realizada no se encontró evidencia sobre la existencia de un programa para concienciar. Según expresado por el director de la Oficina de Tecnología de Información, un representante oficial de recursos humanos solicita la cumplimentación de la Forma 240.03 *Certificación de Orientación y Entrega de Documentos a Empleados de Nuevo Nombramiento*, donde el empleado certifica que ha recibido las políticas de la Oficina, la orientación correspondiente a los beneficios y las demás orientaciones mencionadas en la Forma 240.03.

Criterio

En los artículos 7.1 y 7.2 Inciso B del *Reglamento para Usuarios que Manejan Sistemas de Tecnología de Información V3.0,* aprobado el 14 de septiembre de 2020, por el presidente de la junta establece lo siguiente:

> *Sección 7.1 - Acuerdo de Confidencialidad y Seguridad*
>
> *Todo usuario tiene que suscribir un Acuerdo de Confidencialidad y Seguridad de Información y Protección de Equipos que detalla los deberes y responsabilidades del usuario en el uso de los sistemas de Tecnología de Información y en cuanto a la protección de los equipos que para tales fines cuenta la Compañía.*
>
> *El departamento de Recursos Humanos será responsable de custodiar y mantener en archivo los acuerdo firmados por los empleados de la Compañía y de empleados de otras agencias en asignación administrativa. Como parte de la orientación de nuevos empleados, el representante oficial de Recursos Humanos le proveerá copia de este reglamento y le proveerá el Acuerdo para que se suscriban en el mismo en o antes de que comiencen las labores.*
>
> *No se podrá hacer usos de los Sistemas de Tecnología de Información y equipos de la Compañía sin haber recibido una orientación en torno a las normas, políticas y reglamentos de la Compañía que rigen el uso de sus sistemas de Tecnología de Información.*
>
> *Articulo 7.2 - Responsabilidades de la Oficina de Tecnología de Información en cuanto a la administración e implementación de las políticas y normas contenidas en el presente Reglamento.*
>
> *B. Velará y orientará a los usuarios de Sistemas de Tecnología de Información de las normas de seguridad, confidencialidad y protección de equipos que implica tal uso.*

Además, el **apartado b.** es contrario al apartado H de la Políticas ATI-003, *Seguridad de los Sistemas de Información*, de la Carta Circular 140-16, aprobada por el director de la Oficina de Gerencia y Presupuesto el 7 de noviembre de 2016 que establece:

> *H. Adiestramientos*
>
> *Cada agencia es responsable de proveer adiestramientos al personal para que estén al tanto de los controles de seguridad y los beneficios correspondientes.*
>
> *El personal de sistemas de información y telecomunicación deberá estar adiestrado y mantenerse actualizado sobre los aspectos de seguridad de su área.*
>
> *Se deben proveer mecanismos para capacitar a todos los empleados periódicamente.*

Efecto

Lo comentado puede propiciar el mal uso o manejo de la información confidencial, en caso de que la Oficina sufra algún menoscabo, esta no podrá presentar un contrato firmado que atestigüe la relación que se estableció con el empleado de la Oficina y los empleados de otras agencias. Asimismo, el no mantener, periódicamente, un programa de orientación a todos los usuarios en todos los niveles, impide mantener medidas de control adecuadas al utilizar la información.

Causa

La situación comentada obedece a que el director de la Oficina de Tecnología de Información no cumplió con lo que establece la Sección 7.1 – Acuerdo de Confidencialidad y Seguridad y el apartado H de la Políticas ATI-003, Seguridad de los Sistemas de Información, de la Carta Circular 140-16, aprobada por el director de la Oficina de Gerencia y Presupuesto.

Ver recomendaciones 1, 3 y 10 a la 11.

Hallazgo 5 – Deficiencias relacionadas con las solicitudes de acceso de los usuarios a las aplicaciones de la Oficina

Situación

La reglamentación para los sistemas de tecnología establece que el nivel de acceso de cada empleado deberá ser solicitado por el director del área, división u oficina mediante la cumplimentación de la Forma 340.17 *Solicitud de Acceso a Servicios de la Red Informática*. La Oficina de Tecnología de Información procesará las solicitudes cuando estén debidamente autorizadas y a su vez podrá denegar el nivel de acceso solicitado si entiende que este no corresponde, según los deberes del puesto que ocupa el empleado.

Se examinaron 35 solicitudes de acceso a los servicios de la red informática de los empleados de contabilidad y finanzas y la evaluación reflejó las siguientes deficiencias:

a. La Forma de Solicitud de Acceso no contenía lo siguiente:

   - Un apartado para la cancelación de mismo.
   - Un apartado para indicar el nivel de acceso, rol o privilegio. Por ejemplo: crear, actualizar, eliminar o leer.

b. Para 6 empleados no se actualizó la Forma de Solicitud de Acceso conforme a los deberes, funciones y responsabilidades del puesto. En la Forma se indica un puesto que no coincide con el que actualmente ocupa.

c. En 20 formularios no se indican los roles o privilegios otorgados a los usuarios de acceso a programas contables y financieros**.**

d. En 4 formularios no se indican los accesos a otorgar. El formulario establecía lo siguiente: *favor de asignar los mismos accesos de Empleado A de la Oficina.*

e. En 19 formularios no tenían todas las debidas autorizaciones y fueron procesadas:

   - Catorce (14) no tenían la firma del director de sistemas de información.
   - Uno (1) no tenía la firma del director de recursos humanos y el director de sistemas de información.
   - Uno (1) no tenía la firma del director del área y el director de sistemas de información.
   - Dos (2) no tenían la firma del director del Área.
   - Una (1) sólo tenía la firma del empleado.

f. En 12 solicitudes de acceso se utilizó el formulario incorrecto. Conforme a la reglamentación establecida la forma para HR SENSE debe ser 340.17C y para Oracle 340.17A.

g. El director de Sistemas de Información no ha realizado una revisión periódica de los accesos de la Oficina en conjunto con la gerencia de las áreas aplicables. Esta debe ser verificada una vez al año para asegurarse que los accesos son correctos y están vigentes.

Una situación similar fue señalada por la Oficina del Contralor en su informe TI-20-01 del 18 de julio de 2019.

Criterio

En los artículos 6, Inciso T, 7, Sección 7.2, Inciso C y K, Sección 7.3, Inciso C y 8, Sección 8.1 del *Reglamento para Usuarios que Manejan Sistemas de Tecnología de Información V3.0,* aprobado el 14 de septiembre de 2010, establece que:

> *Artículo 6. - Definiciones*
>
> *T. Nivel de Seguridad de Acceso – Es el tipo de acceso que el usuario podrá tener a los recursos. Los niveles de acceso más utilizados son: LEER, ACTUALIZAR, CREAR, ELIMINAR.*
>
> *Artículo 7. - Política para la administración y manejo de los sistemas de tecnología de información*
>
> *La política para la administración y manejo de los sistemas de Tecnología de Información es que cada usuario haga un uso adecuado de los mismos observando en todo momento las normas aplicables para el manejo de tales sistemas y de sus equipos.*
>
> *Sección 7.2 - Responsabilidad de la Oficina Tecnología de Información en cuanto a la administración e implementación de las políticas y normas contenidas en el presente Reglamento.*
>
> *La Oficina de Tecnología de Información tendrá las siguientes responsabilidades en torno a la implementación y aplicación de las normas contenidas en este Reglamento:*
>
> *C. Tendrá a su cargo la administración de todo lo relativo al acceso a los sistemas de Tecnología de Información incluyendo crear la identificación del usuario y la contraseña.*
>
> *K. Coordinar una revisión periódica de los accesos a los sistemas de la Compañía en conjunto con la gerencia de las áreas aplicables. De esta forma se asegura que los accesos son correctos y vigentes.*
>
> *Sección 7.3 - Políticas dirigidas a salvaguardar la Seguridad de Información*
>
> *C. Revisión Periódica de Accesos*
>
> *Al menos una vez al año se hará revisión de los privilegios de acceso aplicable a todos los usuarios de sistemas. Esta revisión será hecha por los directores de las áreas a las cuales pertenecen los usuarios, de manera que certifiquen que los accesos que tienen siguen vigentes y de acuerdo a los controles que deben estar establecidos por las áreas para evitar conflictos de responsabilidades.*
>
> *Artículo 8 - Solicitud de Acceso y Manejo a los Sistemas de Información*

Sección 8.1 – Acceso

El acceso a los sistemas de información de la Compañía se determinará en atención a las funciones, deberes o responsabilidades del puesto que se ocupa.

El director de Área, División u Oficina determinará en primera instancia el nivel de acceso necesario para que el empleado pueda realizar efectivamente tales deberes o responsabilidades. Para ello, el director del Área, División u Oficina en que se desempeña el potencial usuario cumplimentarán el formulario "Solicitud de Acceso a Servicios de la Red Informática" Forma 340.17 y autorizará tal acceso y enviará el formulario aprobado a la División de Sistemas de Información. De necesitar acceso al Sistema de Oracle tiene que además llenar la Forma 340.17 A. De necesitar acceso al Sistema SATT, debe llenar la Forma 340.17B. Si requiere acceso al Sistema de HR Sense debe llenar la Forma 340. 17C.

La Oficina de Tecnología de Información podrá procesar las peticiones de acceso solo cuando estas están debidamente autorizadas. No se podrán procesar accesos sin la debida documentación. Además, la Oficina de Tecnología de Información podrá denegar el nivel de acceso solicitado al empleado en aquellos casos que, después de verificar, entienda que tal nivel no corresponda según la posición o el puesto del empleado.

Además, el apartado E, Inciso 2, 3 y 6 de la Políticas ATI-003, *Seguridad de los Sistemas de Información*, de la Carta Circular 140-16, establece los siguiente:

Apartado E. Controles Generales

2. La seguridad de la información deberá ser parte integral del diseño de cualquier programa de aplicación que se adquiera o desarrolle la agencia para facilitar las operaciones de la agencia y/o mejorar el servicio a los ciudadanos.

3. La información y los programas de aplicación en las operaciones de la agencia deberán tener controles de accesos para su utilización de tal manera que solamente el personal autorizado pueda ver los datos o acceder a las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.

6. Los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.

Efecto

El no contar con una revisión periódica de los accesos y roles de los usuarios en los sistemas, puede propiciar que empleados, transferidos a otras áreas dentro de la Oficina, continúen manteniendo accesos a información a la que no esten autorizados. Además, no permite mantener un control

correcto y válido del acceso establecido a los usuarios conforme los roles y deberes a los que fueron asignados y autorizados por los funcionarios de las áreas correspondientes.

Causa

Las situaciones comentadas obedecen a que el director de Sistemas de Información y demás funcionarios responsables a cargo de la seguridad en los sistemas de la Oficina no cumplieron con lo establecido en el Reglamento y Políticas ATI-003, Seguridad de los Sistemas de Información, de la Carta Circular Núm. 140-16.

Ver recomendaciones 1, 3 y 12 a la 15.

COMUNICACIÓN GERENCIAL

El borrador de los hallazgos de este examen se sometió para comentarios mediante cartas del 15 y 27 de abril de 2021 al director ejecutivo interino de la Oficina y al secretario del Departamento de Desarrollo Económico y Comercio (DDEC). A pesar de los trámites por obtener dicha comunicación no se recibió respuesta alguna.

La OIG está comprometida con velar que las recomendaciones sean debidamente cumplimentadas e implantadas y continuará trabajando con la Oficina en aras de continuar promoviendo una sana administración.

RECOMENDACIONES

Al secretario del DDEC

1. Asegurarse que el director ejecutivo cumpla con las recomendaciones de la 2 a la 15 de este informe. **(Ver Hallazgos 1 al 5)**

Al director ejecutivo de la Oficina

2. Asegurarse que el principal oficial financiero cumpla con las recomendaciones de la 4 a la 9 de este informe. **(Ver Hallazgos 1 al 3)**

3. Asegurarse que el director de recursos humanos y administración se asegure que el director de sistemas de información cumpla con las recomendaciones de la 10 a la 15 de este informe. **(Ver Hallazgos 4 y 5)**

Al oficial principal financiero

4. Evaluar las deficiencias señaladas en el **Hallazgo 1** y hacer los ajustes y correcciones al formulario de pago por transferencia electrónica.

5. Requerir a los empleados y proveedores que sometan certificación de la cuenta de banco que valide la información bancaria indicada en el formulario. **(Ver Hallazgo 1)**

6. Impartir instrucciones para que se provea adiestramientos, operativos y de seguridad a los empleados de contabilidad y finanzas. **(Ver Hallazgo 2)**

7. Designar a un empleado, ajeno al proceso de las transferencias electrónicas, para monitorear las cuentas del banco y alertas. **(Ver Hallazgo 2)**

8. Evaluar las deficiencias señaladas al procedimiento interno e incorporarlas a este, de forma que contemple los procesos de las transferencias electrónicas que se realizan con el banco. **(Ver Hallazgos 3)**

9. Requerir que se remita para su revisión y se someta para la aprobación del director ejecutivo y el secretario las normas y procedimientos para transferencias electrónicas. **(Ver Hallazgo 3)**

Al director de sistemas de información

10. Orientar al personal de sistemas de información sobre la necesidad de cumplir con las responsabilidades establecidas en los procedimientos y normativas aplicables a su área. **(Ver Hallazgo 4)**

11. Revisar los procedimientos y normativas establecidas y atemperarlos a los procesos actuales de la Oficina. **(Ver Hallazgo 4)**

12. Coordinar con los directores de las áreas para realizar una revisión de los privilegios de acceso aplicable a todos los usuarios de sistemas. Además, mantener documentación de la revisión efectuada. **(Ver Hallazgo 5)**

13. Mantener una copia de las Formas 340.17 más reciente, debidamente aprobadas por los funcionarios correspondientes, y velar porque se describan los roles asignados. De existir más de una forma se deberá evaluar si los privilegios o accesos otorgados son los correctos y siguen vigentes. **(Ver Hallazgo 5)**

14. Mantener un proceso y registro de todos los privilegios asignados. No otorgar privilegios hasta que el proceso de autorización haya concluido. **(Ver Hallazgo 5)**

15. Evaluar la Forma 340.17 para añadir una sección donde se indique el rol o privilegio otorgado: leer, consultar, eliminar, ingresar, entre otros. **(Ver Hallazgo 5)**

CONCLUSIÓN

La evaluación realizada a los documentos, y la información recopilada durante el examen, reflejó que la Oficina cumplió parcialmente con las leyes y reglamentos aplicables a los procesos de transferencias electrónicas. Las deficiencias encontradas respecto a los controles internos,

impiden la eficacia en el cumplimiento con reglamentación y leyes relacionadas con los desembolsos y recaudos generados a través de transferencias electrónicas. A su vez, estos podrían incidir en la ocurrencia de errores que podrían conllevar la pérdida de fondos públicos.

Conforme a lo establecido en el Artículo 17 de la Ley Núm. 15-2017, *supra*, la OIG se remite el presente informe a la autoridad nominadora para que tome las medidas correctivas que estime pertinentes ante el incumplimiento de procedimientos internos por parte de sus empleados y remita a la OIG las acciones tomadas para garantizar el fiel cumplimiento de las leyes y reglamentos aplicables. El incumplimiento de lo requerido podría representar la imposición de acciones correctivas o disciplinarias.

APROBACIÓN

El presente informe es aprobado en virtud de los poderes conferidos por la Ley Núm. 15-2017, antes citada. Será responsabilidad de los funcionarios, empleados o cuerpo rector del gobierno de cada entidad, observar y procurar por que se cumpla cabalmente con la política pública. De la misma manera, establecer los controles y mecanismos adecuados para garantizar su cumplimiento. Será el deber, además, de cada uno de estos y de los demás funcionarios y servidores públicos, el poner en vigor las normas, prácticas y estándares que promulgue la OIG, así como de las recomendaciones, medidas y planes de acción correctiva que surjan de las evaluaciones.

Hoy, 12 de octubre de 2021, en San Juan, Puerto Rico.

Ivelisse Torres Rivera
Inspectora General

INFORMACIÓN GENERAL

Misión

Consolidar los recursos y esfuerzos del Gobierno de Puerto Rico, para promover una sana administración pública y mediante una preintervención efectiva, el óptimo funcionamiento de sus instituciones.

Visión

Servir como entidad gubernamental reconocida a nivel local e internacional y lograr a través de auditorías internas y acciones preventivas, el funcionamiento efectivo y eficiente de los fondos y de la propiedad pública del Gobierno de Puerto Rico.

Línea de Consultas

La Oficina del Inspector General tiene el compromiso de promover una sana administración pública. Por lo que, cualquier persona que tenga información sobre un acto irregular o falta de controles internos en las operaciones de la rama ejecutiva, puede comunicarse a la OIG a través de:

- Línea de Consultas: 787-679-7979
- Correo Electrónico: informa@oig.pr.gov

Contactos


PO Box 191733 San Juan, Puerto Rico 00919-1733


Ave Arterial Hostos 249 Esquina Chardón Edificio ACAA Piso 7, San Juan, Puerto Rico


787-679-7997


consultas@oig.pr.gov


www.oig.pr.gov