INFORME DE AUDITORÍA TI-20-03

21 de octubre de 2019

Departamento de Desarrollo Económico y Comercio

Oficina de Sistemas de Información

(Unidad 5240 - Auditoría 14247)

Período auditado: 22 de enero al 15 de octubre de 2018

CONTENIDO

Página

Estado Libre Asociado de Puerto Rico
OFICINA DEL CONTRALOR
San Juan, Puerto Rico

21 de octubre de 2019

A la Gobernadora, y a los presidentes del Senado de
Puerto Rico y de la Cámara de Representantes

Incluimos los resultados de la auditoría de tecnología de información que realizamos de la Oficina de Sistemas de Información (OSI) del Departamento de Desarrollo Económico y Comercio (Departamento). Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico, y en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada; y en cumplimiento de nuestro *Plan Anual de Auditorías.*

OBJETIVOS DE AUDITORÍA

Objetivo general

Determinar si las operaciones de la OSI y de los sistemas de información computadorizados del Departamento se realizaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

1. Determinar si las operaciones de la OSI; en lo que concierne a los controles internos relacionados con la administración de la seguridad, el acceso lógico y la continuidad del servicio; se efectuaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

2. Determinar si los errores de configuración y procesamiento identificados por el Departamento durante la implementación del sistema de asistencia Kronos fueron corregidos.

CONTENIDO DEL INFORME

Este *Informe* contiene tres hallazgos del resultado del examen que realizamos de los objetivos indicados. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 22 de enero al 15 de octubre de 2018. En algunos aspectos examinamos transacciones anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de la auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas tales como: entrevistas a funcionarios y empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada o por fuentes externas; y pruebas y análisis de procedimientos de control interno y de otros procesos.

Al realizar esta auditoría utilizamos las políticas establecidas en la *Carta Circular 140-16*, *Normas Generales Sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016 por el director de la Oficina de Gerencia y Presupuesto. Para el área que no estaba considerada en dichas políticas **[Hallazgo 3]**, utilizamos como mejor práctica las guías establecidas en el *Federal Information System Controls Audit Manual* (*FISCAM*)[1], emitido por el GAO. Esto, porque, aunque al Departamento no se le requiere cumplir con dichas guías, entendemos que estas

[1] El *FISCAM* utiliza las guías emitidas por el *National Institute of Standards and Technology (NIST)*.

representan las mejores prácticas en el campo de la tecnología de información, al examinar los sistemas computadorizados de las entidades gubernamentales.

Consideramos que la evidencia obtenida proporciona una base razonable para nuestra opinión y hallazgos.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Departamento se creó por virtud del *Plan de Reorganización 4 del 22 de junio de 1994*[2] (*Plan de Reorganización 4*). Su misión es implementar y supervisar la ejecución de la política pública sobre el desarrollo de Puerto Rico en los sectores empresariales de manufactura, comercio, turismo, cine, servicios y cooperativismo. Además, el Departamento constituye el organismo de gobierno a cargo de propiciar el desarrollo de una economía privada, estable y autosostenida con una visión hacia el futuro que toma en consideración la globalización de la economía y la constitución de bloques económicos regionales.

Mediante la *Ley 141-2018, Ley de Ejecución del Plan de Reorganización del Departamento de Desarrollo Económico y Comercio de 2018*, se otorga al secretario de Desarrollo Económico y Comercio las facultades y poderes necesarios para implementar, con las enmiendas incluidas mediante esta *Ley*, el *Plan de Reorganización 7*[3] aprobado por la Asamblea Legislativa el 9 de abril de 2018; y ordena las enmiendas y derogaciones de leyes y del *Plan de Reorganización 4*, que son necesarias para lograr esta reorganización.

[2] Aprobado por el Gobernador del Estado Libre Asociado de Puerto Rico de acuerdo con la *Ley de Reorganización Ejecutiva de 1993*. El Departamento quedó constituido por la Compañía de Fomento Industrial de Puerto Rico, la Compañía de Turismo de Puerto Rico, la Corporación de Desarrollo Hotelero de Puerto Rico, la Administración de Fomento Comercial, la Administración de Fomento Económico, la Corporación para el Desarrollo del Cine, la Administración de Fomento Cooperativo, la Oficina del Inspector de Cooperativas, la Administración de Terrenos, y la Administración de la Industria y el Deporte Hípico. El *Plan de Reorganización 4* fue enmendado por las leyes *151-1994*, *508-2004* y *171-2014*.

[3] El *Plan de Reorganización 7* fue aprobado al amparo de la *Ley 122-2017, Ley del Nuevo Gobierno de Puerto Rico*. Este plan tiene como objetivo lograr una estructura que responda a las exigencias fiscales y del mercado.

El Artículo 5 de la *Ley 141-2018* establece que el Departamento estará constituido por los siguientes componentes:

- Entidades consolidadas que incluyen a la Oficina de Exención Contributiva Industrial, la Oficina Estatal de Política Pública Energética, la Corporación del Centro Regional y la Oficina de Gerencia de Permisos.
- Entidades operacionales que incluyen a la Compañía de Comercio y Exportación y la Compañía de Turismo. Estas entidades se mantienen como corporaciones públicas adscritas, hasta tanto el secretario certifique al Gobernador y la Asamblea Legislativa que se cumplió con el proceso de transición correspondiente. Una vez certificado el proceso, estas pasarán a ser entidades consolidadas.
- Entidades adscritas al Departamento que incluyen a la Autoridad para el Redesarrollo de los Terrenos y Facilidades de la Estación Naval Roosevelt Roads, la Compañía de Fomento Industrial (Fomento) y la Junta de Planificación.

El Departamento es dirigido por un secretario nombrado por el Gobernador con el consejo y consentimiento del Senado de Puerto Rico, quien es el responsable de cumplir con su ley habilitadora, las normas y los procedimientos aplicables. Al 13 de febrero de 2018, la estructura organizacional del Departamento estaba compuesta por: las secretarías auxiliares de Administración, Estrategia e Innovación, Iniciativas de Desarrollo Económico, Internacionalización y Asuntos Comerciales y Programas de Desarrollo Económico.

A la fecha de nuestra auditoría, la OSI respondía a la Secretaría Auxiliar de Administración. Como medida para establecer economías requeridas por la *Ley 3-2017, Ley para Atender la Crisis Económica, Fiscal y Presupuestaria para Garantizar el Funcionamiento del Gobierno de Puerto Rico y enmienda el Código de Rentas Internas del 1994, según enmendado*, el secretario había designado al director de sistemas de información de la Oficina de Tecnología de Informática de Fomento para que dirigiera también a la OSI. Además, la OSI contaba con 1 gerente de

sistemas de información, 1 especialista en sistemas de información, 1 auxiliar de sistemas de información, 1 programadora analista y 3 asistentes de servicios al usuario. El personal de la OSI administraba la red de área local (LAN, por sus siglas en inglés), proveía apoyo técnico a los usuarios, y otorgaba los accesos a la red, a Internet y a los sistemas del Departamento.

El Departamento cuenta con 9 servidores, 164 computadoras de escritorio, 60 computadoras portátiles, 2 tabletas, 6 *switches*[4] y 1 *router*[5]. Además, cuenta con el programa Juvempleo para mantener un expediente electrónico de las propuestas de empleo de los patronos participantes del Programa de Desarrollo de la Juventud (Programa de la Juventud)[6]; el Sistema Integrado para la Administración de Clientes (SIAC), para mantener un registro de los datos relacionados con los participantes y los servicios que se les proveen en las áreas locales del Programa de Desarrollo y Adiestramiento de la Fuerza Laboral de Puerto Rico (Programa de la Fuerza Laboral)[7]; el sistema financiero Micro Information Products Fund Accounting (MIP); el sistema Kronos para el registro de la asistencia de los empleados; el sistema FAS GOV para el manejo del inventario y de los activos fijos; y con servicios de alojamiento en la nube[8] (*hosting*). Mediante estos, la OSI ofrece los servicios de los sistemas de información computadorizados a las distintas áreas del Departamento, así

[4] Dispositivo de comunicación central que conecta dos o más segmentos de red, y permite que ocurran transmisiones simultáneas sin afectar el ancho de banda de la red para una comunicación más eficiente.

[5] Dispositivos que distribuyen tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza a base de la información de nivel de red y las tablas de direccionamiento.

[6] Incorporó las funciones de la entonces Oficina de Asuntos de la Juventud.

[7] Incorporó las funciones de la entonces Administración de Derecho Laboral.

[8] Se refiere al uso de la tecnología de informática en la nube (*cloud computing*), en la que solamente una organización tiene acceso a los recursos que se utilizan para implementarla. La tecnología de informática en la nube permite ofrecer servicios a través de una red, que usualmente es Internet.

como a las 15 áreas locales del Programa de la Fuerza Laboral[9]. También cuenta con infraestructura tecnológica y espacios en servidores para almacenamiento de información (*file server*) provisto por Fomento. Esto, debido a que en su origen el Departamento no contaba con infraestructura de sistemas de información y Fomento le proveía la misma.

El presupuesto asignado al Departamento proviene de la resolución conjunta del Fondo General del Estado Libre Asociado de Puerto Rico, de fondos federales e ingresos propios. El presupuesto aprobado del Departamento, para los años fiscales del 2015-16 al 2017-18, ascendió a $85,248,000, $79,002,000 y $90,715,000, respectivamente.

La OSI no cuenta con un presupuesto propio. Sus gastos operacionales son sufragados del presupuesto general de los gastos preparado por programas del Departamento.

El **ANEJO** contiene una relación de los funcionarios principales que actuaron durante el período auditado.

El Departamento cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.ddec.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones determinadas durante la auditoría fueron remitidas al Hon. Manuel Laboy Rivera, secretario de Desarrollo Económico y Comercio, mediante cartas del 29 de mayo, el 26 de septiembre, y el 6 de noviembre de 2018. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

El secretario contestó las cartas de nuestros auditores el 12 de junio, el 10 de octubre y el 28 de noviembre de 2018, respectivamente. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

[9] Bayamón-Comerío, Caguas-Guayama, Carolina, Guaynabo-Toa Baja, La Montaña, Mayagüez-Las Marías, Noreste, Noroeste, Norte Central-Arecibo, Norte Central-Manatí/Dorado, Ponce, San Juan, Sureste, Suroeste y Sur Central.

El borrador de este *Informe* se remitió para comentarios del secretario por carta del 20 de septiembre de 2019. Este contestó mediante carta del 7 de octubre, y algunos de sus comentarios se incluyen en la sección **OPINIÓN Y HALLAZGOS**.

CONTROL INTERNO

La gerencia del Departamento es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera
- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para los objetivos de esta auditoría. Utilizamos dicha evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias, pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno del Departamento.

En los **hallazgos** de este *Informe* se comentan deficiencias de control interno significativas, dentro del contexto de los objetivos de nuestra auditoría, identificados a base del trabajo realizado.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con los objetivos de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la OSI del Departamento, en lo que concierne a los

controles objeto de este *Informe*, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos del 1 al 3** que se comentan a continuación.

Hallazgo 1 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados y de un procedimiento para el manejo de incidentes de seguridad

Situaciones

a. Un análisis de riesgos es un proceso mediante el cual se identifican los activos de sistemas de información, sus vulnerabilidades y las amenazas a las que están expuestos. Además, se establecen medidas de seguridad y controles adecuados para evitar o disminuir los riesgos y proteger los activos. Toda entidad gubernamental debe realizar un análisis de riesgos, al menos, cada 24 meses o luego de un cambio significativo en la infraestructura operacional.

   Al 8 de mayo de 2018, el Departamento no contaba con un análisis de riesgos que considerara todas sus áreas y programas, y sus sistemas de información computadorizados. A dicha fecha, contaba con el *Information Technology Risk Assessment Report for the Workforce Development Program of the Department of Economic Development and Commerce of Puerto Rico* (*WDP Risk Assessment*) preparado el 29 noviembre de 2017, pero este solo consideraba los sistemas principales del Programa de la Fuerza Laboral.

b. Las agencias deben desarrollar procedimientos para identificar, informar y responder a incidentes de seguridad, incluidos aquellos que causen interrupción en la prestación de sus servicios. Estos procedimientos deberán identificar el personal asignado para responder a los incidentes de seguridad e incluir los límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta.

   Al 22 de mayo de 2018, el Departamento no contaba con un procedimiento o plan para el manejo de incidentes de seguridad relacionados con sus sistemas de información computadorizados.

Criterios

Lo comentado es contrario a lo establecido en las secciones A. y F. de la *Política ATI-003, Seguridad de los Sistemas de Información*, y en las secciones C. y E. de la *Política ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*.

Efectos

La situación comentada en el **apartado a.** impide al Departamento estimar el impacto que los elementos de riesgos tendrían sobre los sistemas de información principales utilizados en sus áreas y programas, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. Además, dificulta desarrollar un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones del Departamento, en caso de que surja alguna eventualidad. **[Hallazgo 2]**

Lo comentado en el **apartado b.** puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno. Además, impide al Departamento tener un control documentado sobre el manejo de incidentes.

Causas

El secretario auxiliar de administración indicó, mediante una certificación emitida el 22 de mayo de 2018, que la situación comentada en el **apartado a.** se debía a que el Departamento se encontraba en un proceso de reorganización que conllevaba cambios a los sistemas de información y determinaron prudente limitar los costos relacionados con la evaluación de los riesgos. Esto, para atender solamente las recomendaciones incluidas en el *Informe de Auditoría TI-15-02* realizado por nuestra Oficina a la entonces Administración de Derecho Laboral, cuyas funciones fueron incorporadas al Programa de la Fuerza Laboral.

La situación comentada en el **apartado b.** se debía a que el Departamento se encontraba en el proceso actualizar su reglamentación de acuerdo con

su nueva estructura organizacional. Además, tenían bajo evaluación una plataforma que les permitiera mantener un registro de todas las situaciones ocurridas en los sistemas de información del Departamento.

Comentarios de la Gerencia

El secretario nos indicó, entre otras cosas, lo siguiente:

> El Departamento de Desarrollo Económico y Comercio se encuentra en un proceso de reorganización […] Este proceso viene acompañado de la integración de nueva infraestructura tecnológica, sistemas, aplicaciones y servicios que deben ser integrados en nuestros servicios. El Departamento una vez completado el proceso de integración de toda esta nueva infraestructura, sistemas y servicios, tiene como objetivo desarrollar un análisis de riesgo donde estén contenidos todos los nuevos servicios. [*sic*] **[Apartado a.]**
>
> […] reconociendo la importancia de tener un procedimiento para el manejo de incidentes, el pasado mes de agosto la Oficina de Sistemas de Información, implementó un nuevo procedimiento para el manejo de incidentes, mediante un sistema electrónico. Este sistema, además de mantener un registro de los incidentes de seguridad en los sistemas, permite tener un registro de todas las solicitudes de servicio de nuestros usuarios, el personal de la Oficina de Sistemas de Información que atiende el incidente, la resolución y el tiempo que tomó atenderlo. [*sic*] **[Apartado b.]**

Consideramos las alegaciones del secretario relacionadas con el **apartado b.** pero el hallazgo prevalece. Sin embargo, la evidencia presentada no incluía la metodología utilizada por el Departamento para identificar y reaccionar a los incidentes de seguridad ni el personal asignado al equipo de respuesta. El sistema electrónico es una herramienta complementaria para mantener la documentación de los incidentes ocurridos y las acciones realizadas que, de ser necesario, pueden ser utilizadas de referencia para incidentes futuros.

Véanse las recomendaciones 1 y 2.a.

Hallazgo 2 - Falta de un plan de continuidad de negocios

Situación

a. Las agencias deben desarrollar un plan de continuidad de negocios que incluya un plan de recuperación de desastres y un plan de continuidad de las operaciones basado en un análisis de riesgo.

Estos planes deben establecer, entre otras cosas, las estrategias[10] de respuesta, recuperación, reanudación y restauración para todos los procesos principales de la agencia. Además, deberán ser actualizados cada vez que se incorpore un sistema o aplicación crítica en la agencia o cuando se realice un cambio significativo dentro de su infraestructura operacional.

Al 25 de julio de 2018, el Departamento carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de los sistemas de información computadorizados, incluidos los sistemas principales mantenidos en instalaciones remotas mediante servicios de alojamiento. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red de comunicación o desastres naturales, entre otros.

Criterios

La situación comentada es contraria a lo establecido en la Sección B.1 de la *Política ATI-003* y la Sección E. de la *ATI-015* de la *Carta Circular 140-16*.

Efecto

Lo comentado puede propiciar la improvisación y que en casos de emergencia se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, y de interrupciones prolongadas de los servicios a los usuarios de los sistemas de información del Departamento.

Causa

El subsecretario atribuyó la situación comentada a que el Departamento se encontraba en un proceso de reorganización que incluía la integración de varias entidades gubernamentales y corporaciones públicas. Como parte de

[10] Estas estrategias estarán basadas en los tiempos de recuperación y respaldo de sus procesos principales obtenidos en el *Informe de Análisis de Impacto*.

este, se evaluarán los procesos, la reglamentación y los planes existentes en cada componente para desarrollar la nueva reglamentación de los sistemas de información del Departamento.

Comentarios de la Gerencia

El secretario nos indicó, entre otras cosas, lo siguiente:

> […] durante las pasadas semanas la Oficina de Sistemas de Información se encontraba en el proceso de desarrollar el "Plan de Contingencia y Continuidad de Negocios […]. Actualmente se encuentra en el proceso de revisión para la firma. Una vez este proceso sea completado en los próximos días, dicho plan será implementado de forma inmediata. [*sic*]

Véase la Recomendación 2.b.

Hallazgo 3 - Falta de documentación de las solicitudes y autorizaciones para acceder a la red del Departamento

Situaciones

a. Las entidades gubernamentales deben implementar controles de acceso para la utilización de la información y los programas, de forma que estos sean accedidos solo por el personal autorizado. Entre estos controles se sugiere mantener la documentación de las solicitudes de acceso a los sistemas de información computadorizados.

   Al 24 de mayo de 2018, el Departamento contaba con 159 cuentas activas de acceso a su red. El gerente de sistemas de información, 1 asistente de servicio al usuario y el auxiliar de sistemas de información del Departamento creaban y efectuaban el mantenimiento de estas cuentas, y utilizaban un correo electrónico que enviaba la Oficina de Recursos Humanos del Departamento para documentar las solicitudes de acceso. Además, al 29 de mayo de 2018, en los servidores de Fomento se mantenían 46 cuentas de acceso activas de empleados del Departamento. Estas cuentas eran administradas por un técnico de redes y correo electrónico, 1 oficial de sistemas de información y 1 técnico de sistemas de

información de Fomento. Las solicitudes de acceso a la red de Fomento se deben documentar mediante el formulario *OTI-026, Solicitud para crear cuentas en la red, correo electrónico, servicio de Internet y otras aplicaciones*.

Solicitamos para examen la documentación para la creación y modificación de 20[11] de las 205 cuentas de acceso activas asignadas al personal del Departamento para acceder a su red y a la red de Fomento. En certificación del 11 de junio de 2018, el gerente de sistemas de información indicó que no contaba con documentación sobre la creación y modificación de las 10 cuentas localizadas en los servidores del Departamento.

Criterios

La situación comentada es contraria a lo establecido en la Sección E.3 de la *Política ATI-003* de la *Carta Circular 140-16* y el Capítulo 3.2, *Access Control*, del *FISCAM*.

Efectos

La situación comentada impide al Departamento mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y privilegios a los usuarios. Además, puede propiciar que personas no autorizadas logren acceso a información confidencial y hagan uso indebido de esta; y la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas, sin que puedan detectarse a tiempo para fijar responsabilidades.

Causa

La situación comentada se debía a que el Departamento se encontraba en un proceso de reorganización y no había completado la preparación del nuevo formulario para documentar las solicitudes de acceso y la actualización de la reglamentación existente para adaptarlas al nuevo ambiente operacional.

[11] Diez de las 159 cuentas localizadas en los servidores del Departamento y otras 10 de las 46 localizadas en los servidores de Fomento.

Comentarios de la Gerencia

El secretario nos indicó, entre otras cosas, lo siguiente:

> […] el pasado 1 de octubre, se completó el proceso de redacción del nuevo reglamento que regirá la administración de los sistemas de información del Departamento, titulado "Reglamento para la Administración de los Servicios de Sistemas de Información". Este reglamento establece las políticas, formularios y los procesos para la creación de cuentas de red, cuentas de correo electrónico, asignación de accesos, manejo correcto de los sistemas, responsabilidad de los usuarios, terminación de cuentas, entre otros procesos […]Luego del proceso de revisión que está programado para la próxima semana, se procederá con la firma para su implementación inmediata.

Véase la Recomendación 2.c.

RECOMENDACIONES

Al secretario de Desarrollo Económico y Comercio

1. Asegurase de que se realice y documente un análisis de riesgos que considere todos los sistemas de información computadorizados del Departamento, según se establece en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*, que esté de acuerdo con la estructura organizacional y ambiente operacional del Departamento. El análisis preparado debe ser remitido para su revisión y aprobación. Una vez aprobado, ver que se revise cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica del Departamento para asegurarse de que se mantenga actualizado. **[Hallazgo 1-a.]**

2. Ver que el director de sistemas de Información de Fomento, quien dirige las actividades de la OSI del Departamento, una vez se complete el proceso de reorganización:

    a. Prepare y remita para su aprobación un procedimiento o plan para el manejo de incidentes. Como parte de este, debe identificarse el personal asignado al equipo de respuesta, la

metodología básica para atender los incidentes y el tiempo mínimo y máximo de respuesta esperado. Además, asegurarse de que en el sistema electrónico adquirido se mantenga la documentación de los incidentes de seguridad ocurridos y la metodología utilizada para resolverlos. Esto, de manera que pueda ser utilizada de referencia cuando dichos incidentes se repitan, y estos se puedan resolver en el menor tiempo posible. **[Hallazgo 1-b.]**

b. Prepare un plan de continuidad de negocios que cumpla con lo requerido en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*, y que considere la nueva estructura organizacional y ambiente operacional del Departamento. Este plan debe ser remitido para su revisión y aprobación. Una vez sea aprobado, asegurarse de que se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios del Departamento. Además, asegurarse de que se distribuya a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar su efectividad. **[Hallazgo 2]**

c. Actualice y remita para su aprobación la reglamentación relacionada con la administración y la seguridad de los sistemas de información computadorizados. Además, asegurarse de que, como parte de esta, se establezca un proceso uniforme para la documentación de la creación, modificación y cancelación de las cuentas de acceso a los sistemas de información del Departamento. Una vez aprobado, actualizar la documentación de las cuentas de acceso. **[Hallazgo 3]**

APROBACIÓN

A los funcionarios y a los empleados del Departamento, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por:

ANEJO

DEPARTAMENTO DE DESAROLLO ECONÓMICO Y COMERCIO
OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Manuel Laboy Rivera	Secretario	22 ene. 18	15 oct. 18
Lcdo. Javier Rivera Aquino	Subsecretario	1 abr. 18	15 oct. 18
Lcdo. Ian Carlo Serna	Subsecretario Interino	22 ene. 18	30 mar. 18
Sr. Javier Rodríguez Aguiló	Director de la Oficina de Sistemas de Información[12]	2 feb. 18	15 oct. 18
Sr. Miguel Borges Guevara	Gerente de Sistemas de Información	22 ene. 18	15 oct. 18

[12] Ocupaba el puesto de director de tecnología de informática de Fomento y fue designado por el secretario como director de la Oficina de Sistemas de Información del Departamento.

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-18-19* del 27 de abril de 2018, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensiones 2801 o 2805, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos y el tipo de opinión del informe.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el administrador de documentos al (787) 754-3030, extensión 3400.

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr