INFORME DE AUDITORÍA TI-18-09

4 de mayo de 2018

Junta de Planificación de Puerto Rico

Programa de Sistemas de Información

(Unidad 5347 - Auditoría 14127)

Período auditado: 31 de mayo de 2016 al 13 de junio de 2017

CONTENIDO

Página

OBJETIVO DE AUDITORÍA **2**

CONTENIDO DEL INFORME **2**

ALCANCE Y METODOLOGÍA **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **6**

CONTROL INTERNO **7**

OPINIÓN Y HALLAZGOS **7**

1 - Falta de un informe de análisis de riesgos y de un análisis de impacto de negocio sobre los sistemas de información 8

2 - Falta de un plan de continuidad de negocios y de un centro alterno para restaurar las operaciones críticas computadorizadas 10

3 - Falta de respaldos periódicos de la información computadorizada, y deficiencias relacionadas con el almacenamiento de respaldos y documentación en la compañía externa 12

4 - Falta de segregación de las funciones realizadas por un programador de sistemas electrónicos I 15

RECOMENDACIONES **17**

APROBACIÓN **19**

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE PLANIFICACIÓN DURANTE EL PERÍODO AUDITADO **20**

ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **21**

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

4 de mayo de 2018

Al Gobernador, 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 las operaciones del Programa de Sistemas de Información (Programa) de la Junta de Planificación de Puerto Rico (Junta). 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.*

OBJETIVO DE AUDITORÍA

Determinar si las operaciones del Programa, en lo que concierne a los controles para la administración de la seguridad, el acceso lógico, la continuidad del servicio, la segregación de deberes y los equipos computadorizados, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

Este *Informe* contiene cuatro hallazgos sobre el resultado del examen que realizamos de las áreas indicadas en la sección anterior. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 31 de mayo de 2016 al 13 de junio de 2017. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico. Estas normas requieren que planifiquemos y realicemos la auditoría para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestros hallazgos y opinión. En consecuencia, realizamos las pruebas que consideramos necesarias, a base

de muestras y de acuerdo con las circunstancias, según nuestro objetivo de auditoría. Realizamos pruebas tales como: entrevistas; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno, y de otros procesos; y confirmaciones de información pertinente.

En relación con el objetivo de la auditoría, consideramos que la evidencia obtenida proporciona una base razonable para nuestros hallazgos y opinión.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Junta fue creada en virtud de la *Ley Núm. 75 del 24 de junio de 1975, Ley Orgánica de la Junta de Planificación de Puerto Rico*, según enmendada, y está adscrita a la Oficina del Gobernador.

La Junta se compone de siete miembros asociados, los cuales son nombrados por el Gobernador de Puerto Rico, con el consejo y consentimiento del Senado de Puerto Rico. El Gobernador designa a un miembro de la Junta como presidente para dirigir la misma. Además, puede nombrar hasta tres miembros alternos para que puedan formar parte de una sala[1] cuando el presidente así lo determine; para que sustituyan a los asociados en los casos de vacantes, enfermedades, licencias con o sin sueldo, vacaciones, ausencias temporeras o inhabilidad de cualquiera de estos; para que realicen las funciones o encomiendas que el presidente estime necesarias asignarles para lograr los propósitos de esta ley; o para llevar a cabo cualquier función asignada por este o por cualquier otra ley.

El propósito general de la Junta es guiar el desarrollo integral de Puerto Rico de modo coordinado, adecuado y económico. El desarrollo debe estar de acuerdo con las necesidades sociales actuales y futuras, y los recursos humanos, ambientales, físicos y económicos. Además, debe fomentar, en la mejor forma, la salud, la seguridad, el orden, la convivencia, la prosperidad, la defensa, la cultura, la solidez económica

[1] Lugar en el que se celebran las reuniones convocadas por el presidente. Cada una de las salas de la Junta funciona y adjudica asuntos independientemente.

y el bienestar general de sus habitantes. También debe fomentar la eficiencia, la economía y el bienestar social en el proceso de desarrollo, en la distribución de población, en el uso de las tierras y otros recursos naturales, y en las mejoras públicas que tiendan a crear condiciones favorables para que la sociedad pueda desarrollarse integralmente.

La *Ley 161-2009, Ley para la Reforma del Proceso de Permisos de Puerto Rico*, según enmendada, creó la Oficina de Gerencia de Permisos (OGPe)[2], adscrita a la Junta[3]. Esta *Ley* transfirió a la OGPe las funciones de la Junta relacionadas con las consultas de ubicación y cambios de clasificación de terrenos. Esto ocasionó que la Junta perdiera su mayor fuente de ingresos propios, provenientes del cobro que realizaba al público por dichas consultas.

A la fecha de nuestra auditoría, la estructura organizacional de la Junta estaba integrada por la Oficina del Presidente; las oficinas de Asuntos Legales, Auditoría Interna y Secretaría; el Consejo Estatal sobre Deficiencias en el Desarrollo (CEDD)[4]; el Centro de Servicios Compartidos; y los programas de Planificación Física, y Planificación Económica y Social. Los programas estaban compuestos, a su vez, de subprogramas u oficinas. Los directores de cada uno de los programas respondían al director ejecutivo auxiliar de la Junta, quien, a su vez, responde al presidente.

El Programa se compone de los subprogramas de Análisis y Programación, Operaciones Computadorizadas y Sistemas de Información Geográfica[5].

---

[2] Anterior Administración de Reglamentos y Permisos (ARPE).

[3] La *Ley 161-2009* también creó la Junta Revisora de Permisos y Usos de Terrenos (Junta Revisora), y la Oficina del Inspector General de Permisos (OIGPe). Posteriormente, esta *Ley* fue enmendada por la *Ley 151-2013*, la cual, entre otras cosas, eliminó la Junta Revisora y la OIGPe y reasignó las responsabilidades de la OGPe.

[4] Organismo gubernamental asignado administrativamente a la Junta que se rige por la *Ley Pública Federal 106-402*, según enmendada en el 2000, y la *Orden Ejecutiva OE-1997-25*.

[5] Este sirve como centro de información de data geográfica para el Gobierno y la ciudadanía en general conforme a la *Ley 398-2000, Ley para crear el Comité Coordinador para la Adquisición y Acceso a Información Geográfica de Puerto Rico*. Esta *Ley* creó el *Sistema de Información Geográfica* como un sistema central digital de información geográfica integrada y de mapas que interrelaciona diferentes bancos de información y sirve como depositario de toda información geográfica adquirida, comprada o producida por cualquier organismo gubernamental.

Es dirigido por un director de sistemas de información y cuenta con 1 director de negociado y 1 director de negociado interino, quienes están a cargo de dirigir el subprograma de Operaciones Computadorizadas y de Sistemas de Información Geográfica, respectivamente. También cuenta con 5 operadores de equipos electrónico de procesar datos, 4 programadores de sistemas electrónicos, 1 administrador de base de datos, 3 analistas de base geográfica de datos, 1 coordinador de servicio al usuario, 1 auxiliar de analista de base geográfica de datos, 1 auxiliar administrativo I, 2 analistas de base geográfica de datos II y 1 especialista en servicios técnicos para computadoras.

La infraestructura tecnológica de la Junta consiste en una red virtual de área local (VLAN, por sus siglas en inglés) para las operaciones en su edificio principal[6], y una red de área amplia (WAN, por sus siglas en inglés) para la comunicación con el CEDD y las cuatro oficinas regionales que comparte con la OGPe. Estas oficinas están localizadas en Aguadilla, Hatillo, Humacao, y Ponce. La red de comunicación de la Junta está compuesta por 20 servidores físicos y 31 virtuales, 305 computadoras de escritorio (*desktops*) y 60 computadoras portátiles (*laptops*).

Los recursos para financiar las actividades operacionales de la Junta provienen principalmente de resoluciones conjuntas del presupuesto general, de asignaciones especiales, de fondos especiales estatales y de fondos federales. Para los años fiscales del 2014-15 al 2016-17, el presupuesto de la Junta ascendió a $18,375,000, $15,266,000 y $14,464,000, respectivamente. Los gastos operacionales del Programa se sufragaron del presupuesto asignado de $1,192,000 en los años fiscales 2014-15 y 2015-16; y de $1,172,000 en el 2016-17.

Los **anejos 1 y 2** contienen una relación de los miembros y los funcionarios principales que actuaron durante el período auditado.

[6] La Oficina de Gerencia y Presupuesto provee el servicio de Internet a la Autoridad de Edificios Públicos, y esta se encarga de distribuirla al resto de las agencias que están localizadas en el edificio.

La Junta cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.jp.gobierno.pr. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* y otras situaciones determinadas durante la auditoría, fueron remitidas a la Sra. María del C. Gordillo Pérez, presidenta, mediante carta de nuestros auditores del 6 de julio de 2017. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante carta del 14 de julio de 2017, la señora Gordillo Pérez contestó la carta de nuestros auditores. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

Mediante carta del 8 de marzo de 2018, se remitió, para comentarios, el borrador de este *Informe*, que incluía 5 hallazgos, a la presidenta; y el borrador de los cinco hallazgos al Sr. Luis García Pelatti, expresidente.

El expresidente contestó el 23 de marzo e indicó lo siguiente:

> Mis comentarios, son de carácter general, y se enfocan en reconocer la frustración, de que dos de los hallazgos se deben a desconocimiento por parte de los directores y los otros se relacionan a la falta de fondos y recursos. Así que es importante que la Oficina del Contralor, continue sus trabajos, difundiendo los problemas que se están generando en la administración pública, ante la falta de fondos en las agencias, que están limitando la capacidad de proveer adiestramientos y capacitaciones de los empleados. [*sic*]
>
> Por otro lado, siento que parte de estos hallazgos, muestra la ausencia de continuidad en ciertas Oficinas, Programas o Áreas de las agencias, debido a que son empleados de confianza. [*sic*]
>
> Es necesario limitar las posiciones de confianza, pero por supuesto, con un sistema de contratación por oposición o examen acreditado, que permita dar continuidad. […] [*sic*]

La presidenta contestó mediante carta del 26 de marzo y, luego de evaluar sus comentarios, determinamos no incluir en este *Informe* uno de los hallazgos remitidos. En los **hallazgos** incluidos en este *Informe* se consideraron algunos de sus comentarios.

CONTROL INTERNO

La gerencia de la Junta 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 este *Informe*. 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 de la Junta.

En los **hallazgos** de este *Informe* se comentan las deficiencias de controles internos significativas, dentro del contexto del objetivo de nuestra auditoría, identificadas 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 del Programa de la Junta, 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 4** que se comentan a continuación.

Hallazgo 1 - Falta de un informe de análisis de riesgos y de un análisis de impacto de negocio sobre los sistemas de información

Situaciones

a. El análisis de riesgos es un proceso mediante el cual se identifican los activos de los sistemas de información computadorizados existentes en una entidad, sus vulnerabilidades y las amenazas a las que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas. Esto, con el fin de determinar las medidas de seguridad y los controles adecuados a ser implementados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo, y proteger dichos activos, de manera que no se afecten adversamente las operaciones de la entidad. Mediante este proceso, se asegura que las medidas de seguridad y los controles a ser implementados sean costo-efectivos, pertinentes a las operaciones de la entidad y que respondan a las posibles amenazas identificadas.

   Al 16 de agosto de 2016, en la Junta no se había preparado un informe del análisis de riesgos de los sistemas de información computadorizados.

b. El análisis de impacto de negocio tiene como objetivo cuantificar y calificar el impacto de negocio por la pérdida o la interrupción de las operaciones, y de las vulnerabilidades y amenazas que fueron identificadas y clasificadas en el análisis de riesgos. Además, debe proveer información para determinar las estrategias de recuperación más apropiadas. Al 16 de agosto de 2016, en la Junta no se había realizado un análisis de impacto de negocio sobre los sistemas de información computadorizados.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 77-05, Normas sobre la Adquisición e Implantación de*

los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales, aprobada el 8 de diciembre de 2004 por la directora de la Oficina de Gerencia y Presupuesto (OGP); y en la *Política TIG-015, Programa de Continuidad Gubernamental*, aprobada el 22 de septiembre de 2011 por el director de la OGP[7].

Efectos

Las situaciones comentadas impiden a la Junta estimar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y de pérdida de información.

Además, dificultan 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 de la Junta, en caso de alguna eventualidad. **[Véase el Hallazgo 2-a.]**

Causa

Las situaciones comentadas se debieron principalmente al desconocimiento del director de sistemas de información sobre la importancia de preparar los análisis de riesgos y de impacto de negocio, y de los requerimientos específicos para la preparación de estos informes.

Comentarios de la Gerencia

La presidenta indicó lo siguiente:

> Dirigidos a establecer el nivel de vulnerabilidad ante la exposición de riesgos y la efectividad de los controles existentes, estamos trabajando en la redacción de un Informe de Análisis de Riesgos y de un Análisis de Impacto de Negocio. Hemos establecido medidas para evitar que estos riesgos se materialicen causando mayores problemas. [*sic*]

Véase la Recomendación 1.

---

[7] La *Carta Circular 77-05* y la *Política TIG-015* fueron derogadas por 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 OGP. Esta contiene disposiciones similares a las de la *Carta Circular* y *Política* derogadas.

Hallazgo 2 - Falta de un plan de continuidad de negocios y de un centro alterno para restaurar las operaciones críticas computadorizadas

Situaciones

a. Al 13 de julio de 2016, la Junta carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de los sistemas de información computadorizados. Esto era necesario para lograr el pronto funcionamiento de dichos sistemas y restaurar las operaciones de la Junta, en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, o desastres naturales, entre otros.

b. Al 6 de junio de 2017, la Junta no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en casos de emergencia.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05* y en la *Política TIG-015*.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del plan de continuidad de negocios, deben existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la agencia, podrían ser los siguientes: **[Apartado b.]**

- Una entidad pública o privada de similar configuración y tamaño.
- Una compañía dedicada a servicios de restauración.
- Un centro alterno de la propia entidad.

Efectos

La situación comentada en el **apartado a.** podría 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 ofrecidos a los usuarios de la de la Junta y la OGPe.

La situación comentada en el **apartado b.** podría afectar las operaciones de la Junta y los servicios de la OGPe, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o evento que afectara su funcionamiento. Esto, a su vez, podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales, y afectar las funciones de la Junta y sus sistemas de información computadorizados.

Causas

La situación comentada en el **apartado a.** se atribuye a que la Junta se atrasó en el proceso de revisión, actualización y validación de las políticas y los procedimientos administrativos y operacionales. Esto, debido a la restricción de acceso a las oficinas en la torre norte del Centro Gubernamental Minillas, por un problema de contaminación de asbesto; y la reducción en la cantidad de empleados públicos y del presupuesto operacional que han impactado adversamente a las agencias públicas.

La situación comentada en el **apartado b.** se atribuye a que el director de sistemas de información se encontraba en negociaciones con la OGP para la creación de un centro alterno, a través del servicio de *Microsoft Azure*[8].

Comentarios de la Gerencia

La presidenta indicó lo siguiente:

> A falta de un plan de continuidad de negocios, identificamos aquellas tareas y servicios que brinda la agencia, que pueden realizarse utilizando el sistema *Office 365*. A tales efectos, implementamos la JP-OA-2017-03, orden administrativa que establece el Programa de Red Inalámbrica (PRIN), el cual permite a los empleados laborar en cualquier lugar, incluso desde el hogar.

[8] Servicio en la nube utilizada para crear, implementar y administrar aplicaciones a través de una red global. Este servicio lo ofrece OGP a las entidades gubernamentales.

> De esta forma podemos dar continuidad de servicios sin la agencia afectarse. Además, estamos en el proceso de la redacción del Plan de Continuidad de Negocios, tomando en consideración las recomendaciones de los Directores de cada Programa u Oficina y el sistema PRIN, formará parte del mismo. [*sic*] **[Apartado a.]**
>
> Respecto al centro alterno para restaurar las operaciones críticas computadorizadas, estamos coordinando con el soporte de la Oficina de Gerencia y Presupuesto (OGP), un espacio en la nube para hacer pruebas de recuperación y restauración de sistemas. **[Apartado b.]**

Véanse las recomendaciones 2.a. y 3.

Hallazgo 3 - Falta de respaldos periódicos de la información computadorizada, y deficiencias relacionadas con el almacenamiento de respaldos y documentación en la compañía externa

Situaciones

a. Al 13 de junio de 2017, la operadora de equipo computadorizado del Subprograma de Operaciones Computadorizadas era la encargada de realizar los respaldos de los sistemas de información computadorizados. La operadora preparaba, entre otros, los siguientes respaldos:

- *Full Unix* - Se realizaba los sábados y contenía información relacionada con el sistema Oracle, que incluía las bases de datos de Radicación de Casos y del sistema ECON[9].
- *Full CMS* - Se realizaba de lunes a viernes y contenía información de la configuración de la aplicación utilizada para realizar los respaldos *(Domain Controller del Data Protector)*.
- *Full Usuario* - Se realizaba los sábados y contenía información del registro diario de asistencia de los empleados, de documentos preparados y de las aplicaciones de la Junta, entre otros.

[9] Sistema compuesto por distintos módulos para apoyar la gestión de análisis económico en sus distintas facetas, tales como: producto bruto, empleo, comercio exterior, permisos de construcción, indicadores económicos, estadísticas municipales y seguridad de empleo.

- *Full SQL* - Se realizaba los sábados y contenía información de programas, configuraciones y bases de datos de la Junta.
- *Full SPS* - Se realizaba los sábados y contenía información de varios servidores, incluido el servidor principal de la Junta.

Examinamos una lista de respaldos entregada el 23 de enero de 2017 por la operadora. Esta incluía el detalle de los respaldos de los servidores, efectuados entre octubre y diciembre de 2016. Del examen efectuado encontramos que en la Junta no se realizaron respaldos periódicos de la información computadorizada, según se indica:

1) El respaldo *Full Unix* no se preparó para 7 de los 14 sábados incluidos en el período evaluado.

2) El respaldo *Full CMS* no se preparó para 11 de los 65 días incluidos en el período evaluado.

3) El respaldo *Full Usuario* no se preparó para 8 de los 14 sábados incluidos en el período evaluado.

4) Los respaldos *Full SQL* y *Full SPS* no se prepararon para 10 de los 14 sábados incluidos en el período evaluado.

b. La Junta tenía arrendado un archivo de seguridad de seis gavetas a una compañía externa, para el almacenamiento de las cintas de respaldo. Para este servicio, en la Junta se prepararon dos órdenes de compra, en julio de 2015 y de 2016, por $3,750 cada una. El examen realizado reveló que, del 1 de julio de 2015 al 5 de mayo de 2017, no se enviaron los respaldos de información mensuales a la compañía externa. En dicho archivo tampoco se mantenía una copia del *Plan de Contingencia*, la documentación de los sistemas y las aplicaciones, las configuraciones, los diagramas, las contraseñas y el inventario de los equipos.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el inciso II.A. y C. del *Procedimiento para el Negocio de Operaciones* del *Manual de Procedimientos*, aprobado el 3 de diciembre de 2003 por el presidente de la Junta. En este se establece que:

- Toda la información debe estar almacenada en respaldos y en lugares seguros para que; cuando surja cualquier eventualidad, ya sea desastre natural, fuego, sabotaje, o problemas de equipo; se pueda recuperar o procesar sin ningún problema. **[Inciso II.A.] [Apartado a.]**

- Se debe almacenar una copia en un lugar seguro fuera de la agencia para que, cuando surja una emergencia, se pueda procesar todo sin ningún problema. **[Inciso II.C.] [Apartado b.]**

Además, lo comentado en el **apartado b.** es contrario a lo establecido en Artículo 6 del *Plan de Contingencia*, aprobado el 23 de marzo de 2017 por la presidenta de la Junta. En este se indica que en la bóveda de seguridad se mantiene una copia de las configuraciones, los diagramas, las contraseñas y el inventario de los equipos.

Las situaciones comentadas también son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

Efectos

Las situaciones comentadas podrían ocasionar que, en caso de emergencia, la Junta no pueda disponer de los respaldos de información necesarios y de la documentación importante para mantener la continuidad de las operaciones. Además, la situación comentada en el **apartado a.**, podría ocasionar la pérdida permanente de información importante, sin la posibilidad de recuperarla, lo que afectaría adversamente las operaciones de la Junta.

Además, como resultado de la situación comentada en el **apartado b.**, la Junta no obtuvo el beneficio máximo de los $7,500 pagados a la compañía externa por el arrendamiento del archivo de seguridad.

Causas

La situación comentada en el **apartado a.** se atribuye, en parte, a que la Junta no contaba con los fondos suficientes para contratar otro recurso que colaborara con la encargada de realizar los respaldos.

Las situaciones comentadas en el **apartado b.** se atribuyen a que en el *Procedimiento para el Negocio de Operaciones* del *Manual de Procedimientos* no se establecen las responsabilidades de la encargada de realizar los respaldos de información, con respecto a la frecuencia con que se deben trasladar los mismos a la bóveda externa, y al almacenamiento de la documentación de los sistemas, las aplicaciones, los diagramas, las contraseñas y el inventario de los equipos en dicho lugar.

Comentarios de la Gerencia

La presidenta indicó lo siguiente:

> Actualmente, trabajamos con la automatización de resguardos para asegurarnos que la interacción con los equipos, sea solo en casos de fallas. Las actualizaciones al servidor, ayudarán a seguir los procedimientos de resguardo con mayor eficiencia. [*sic*] **[Apartado a.]**
>
> Las deficiencias relacionadas con el almacenamiento de respaldos y documentación en la compañía, se trabajarán realizando visitas semanales a la bóveda. Mensualmente, el Director del Programa de Sistemas de Información (PSI) y el Director de Operaciones verificarán resguardos y registros, según lo indica el Manual de Procedimientos […]. Se realizará el inventario de cintas dirigido a duplicar las mismas para mantenerlas tanto en bóveda interna, como externa. […] [*sic*] **[Apartado b.]**

Véase la Recomendación 2 de la b. a la e.

Hallazgo 4 - Falta de segregación de las funciones realizadas por un programador de sistemas electrónicos I

Situación

a. Un programador de sistemas electrónicos I de la Junta, como parte de las funciones de su puesto, era responsable de, entre otras cosas, colaborar en el desarrollo de la lógica, la corrección, la prueba y el mantenimiento de programas; preparar data de prueba para programas de naturaleza sencilla; revisar programas existentes para corregir errores; y analizar y estudiar la definición de los programas que se le

asignan. Además, realizaba el proceso completo de migración, los cambios y las pruebas, y los llevaba a producción. Las funciones realizadas como programador y las adicionales resultan incompatibles y conflictivas al ser realizadas por una misma persona. Esta situación se agrava al no existir un control alterno de supervisión por parte del director de sistemas de información, como un registro automático (*log*) de las modificaciones realizadas por el programador; y de documentación de las migraciones realizadas.

Criterio

Esta situación es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que las entidades gubernamentales deberán implementar controles adecuados en sus sistemas de información computadorizados para garantizar la confidencialidad, integridad y disponibilidad de la información. Conforme a dicha *Política*, y como norma de sana administración, es necesario que se segreguen las funciones relacionadas con las operaciones de los sistemas de información de la entidad o se establezca la supervisión necesaria como control compensatorio. El objetivo primordial de dichas medidas de control es disminuir la probabilidad de que se cometan errores o irregularidades y que no se detecten a tiempo.

Efecto

La situación comentada podría propiciar que se realizaran cambios a la programación sin la autorización requerida.

Causa

La situación comentada se debía a la falta de personal, adiestramientos y recursos existente en el Programa.

Comentarios de la Gerencia

La presidenta indicó las medidas que están en proceso para corregir la situación comentada en el **Hallazgo**.

Véase la Recomendación 2.f.

RECOMENDACIONES

A la Presidenta de la Junta de Planificación

1. Asegurarse de que se realicen los análisis de riesgos de los sistemas de información computadorizados y de impacto de negocios, según se establecen en las políticas *ATI-003, Seguridad de los Sistemas de Información*, y *ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular Núm. 140-16*. Los mismos deben ser remitidos para revisión y aprobación de la Junta. Una vez aprobados, ver que los mismos se revisen cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica de la Junta, para asegurarse de que se mantengan actualizados. **[Hallazgo 1]**

2. Ejercer una supervisión efectiva sobre el director de sistemas de información, para asegurarse de que:

    a. Se prepare y remita para su aprobación un plan de continuidad de negocios que incluya los planes específicos, completos y actualizados del Programa. Una vez este documento sea aprobado, tome las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la Junta. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 2-a.]**

    b. La persona encargada de realizar los respaldos prepare copias recurrentes de la información contenida en los servidores, y almacene una de estas en el archivo arrendado a la compañía externa, o en algún otro lugar seguro fuera de los predios de la Junta. **[Hallazgo 3-a.]**

    c. Se evalúe la necesidad y realicen las gestiones para identificar un recurso interno que colabore con la encargada de realizar los respaldos, para asegurar la preparación de los mismos. **[Hallazgo 3-a.]**

d. Se revise y actualice el *Procedimiento para el Negocio de Operaciones* del *Manual de Procedimientos*, para asegurarse de que se establezcan las responsabilidades de la encargada de realizar los respaldos de información, con respecto a la frecuencia con que se deben trasladar los mismos a la bóveda externa, y al almacenamiento de la documentación de los sistemas, las aplicaciones, los diagramas, las contraseñas y el inventario de los equipos en dicho lugar. **[Hallazgo 3-b.]**

e. Cumpla con lo establecido en el *Plan de Contingencia* con respecto al almacenamiento de la documentación de los sistemas, las aplicaciones, los diagramas, las contraseñas y el inventario de los equipos en un lugar externo a la Junta. **[Hallazgo 3-b.]**

f. Evalúe la situación comentada en el **Hallazgo 4** y se asegure de establecer una segregación adecuada de las funciones realizadas por el programador de sistemas electrónicos I. De no contar con los recursos necesarios, establecer los controles compensatorios, tales como: la supervisión, la utilización y revisión de registros de auditorías, y la documentación de las migraciones efectuadas; que permitan mitigar el riesgo resultante de la falta de segregación de funciones.

3. Formalizar un acuerdo escrito que incluya los términos y las condiciones, bajo las cuales la Junta utilizará los servicios de recuperación y restauración de los sistemas negociados, en coordinación con la OGP, para el uso de la nube. **[Hallazgo 2-b.]**

APROBACIÓN

A los funcionarios y a los empleados de la Junta de Planificación de Puerto Rico, 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 1

JUNTA DE PLANIFICACIÓN DE PUERTO RICO
PROGRAMA DE SISTEMAS DE INFORMACIÓN

MIEMBROS PRINCIPALES DE LA JUNTA DE PLANIFICACIÓN DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sra. María del C. Gordillo Pérez	Presidenta	2 ene. 17	13 jun. 17
Sr. Luis García Pelatti	Presidente	31 may. 16	31 dic. 16
Sra. Eileen Poueymirou Yunqué	Miembro Asociado	12 ene. 17	13 jun. 17
Sr. José L. Valenzuela Vega	"	11 ene. 17	13 jun. 17
Sra. Rebecca Rivera Torres	"	10 ene. 17	13 jun. 17
Sr. Juan C. Santiago Colón	"	31 may. 16	31 dic. 16
Sra. Sylvia Rivera Díaz	"	31 may. 16	31 dic. 16
Sr. Pedro Cardona Puig	"	31 may. 16	31 dic. 16

ANEJO 2

JUNTA DE PLANIFICACIÓN DE PUERTO RICO
PROGRAMA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sra. María del C. Gordillo Pérez	Presidenta	2 ene. 17	13 jun. 17
Sr. Luis García Pelatti	Presidente	31 may. 16	31 dic. 16
Sra. Ana Corrada Marqués	Directora Ejecutiva Auxiliar	27 ene. 17	13 jun. 17
Vacante	"	16 dic. 16	26 ene. 17
Sr. Ángel L. Valle Valle	Director Ejecutivo Auxiliar	31 may. 16	15 dic. 16
Sr. Andrés Ruiz Rodríguez	Director de Presupuesto y Finanzas	31 may. 16	13 jun. 17
Sra. Jocelyn Castro Nieves	Directora de Recursos Humanos y Relaciones Laborables	19 ene. 17	13 jun. 17
Sra. Aurie D. Roqué Rodríguez	"	1 ago. 16	31 dic. 16
Sra. Carmen D. Rosario Morales	"	31 may. 16	31 jul. 16
Sr. Carlos Llanos Vázquez	Director de Sistemas de Información	1 feb. 17	13 jun. 17
Sr. Carlos R. Castillo Domena	Director Interino de Sistemas de Información	3 ene. 17	31 ene. 17
Sr. Daniel Díaz Torres	"	22 nov. 16	2 ene. 17
Sr. Yojan Rosado Portalatín	Director de Sistemas de Información	16 oct. 16	21 nov. 16
Sra. Yamira Valles Nevárez	Directora de Sistemas de Información	31 may. 16	15 oct. 16
Sr. Carlos R. Castillo Domena	Director de Administración Interna	19 ene. 17	13 jun. 17

Continuación **ANEJO 2**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	**HASTA**
Vacante	Director Interino de Administración Interna	16 dic. 16	18 ene. 17
Sr. Ángel I. Valle Valle	"	16 oct. 16	15 dic. 16
Sra. Carmen D. Rosario Morales	Directora de Administración Interna	31 may. 16	15 oct. 16

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-08-32* del 27 de junio de 2008, 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