

*[Handwritten signature]*



## *Secretaría*

- Ver al dorso
- Para su información
- Notas
- Para mantenerle al día
- Expediente
- Dar Cuenta
- Registrar y Procesar

*Senado*  
DE PUERTO RICO

EL CAPITOLIO  
PO Box 9023431  
San Juan, Puerto Rico  
00902-3431

T: 787.722.3460  
787.722.4012  
F: 787.723.5413  
W: [www.senadopr.us](http://www.senadopr.us)

## REFERIDO A:

### COMISIONES PERMANENTES

---

- Hacienda
- Gobierno
- Seguridad Pública y Judicatura
- Salud
- Educación y Asuntos de la Familia
- Desarrollo Económico y Planificación
- Urbanismo e Infraestructura
- Jurídico Penal
- Jurídico Civil
- Agricultura
- Recursos Naturales y Ambientales
- Comercio y Cooperativismo
- Turismo y Cultura
- Trabajo, Asuntos del Veterano y Recursos Humanos
- Bienestar Social
- Asuntos Municipales
- Recreación y Deportes
- Banca, Asuntos del Consumidor y Corporaciones Públicas
- Desarrollo de la Región del Oeste
- Asuntos de la Mujer
- Asuntos Internos
- Reglas y Calendario
- Asuntos Federales
- De la Montaña
- Ética

### COMISIONES ESPECIALES

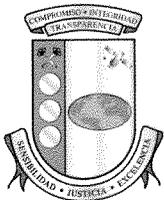
---

- Puerto de las Américas
- Derecho de Autodeterminación del Pueblo de Puerto Rico
- Sobre Reforma Gubernamental

### COMISIONES CONJUNTAS

---

- Informes Especiales del Contralor
- Donativos Legislativos de Puerto Rico
- Internado Córdova-Fernós
- Internado Pilar Barbosa
- Internado Ramos Comas
- Código Penal
- Revisión y Reforma del Código Civil
- Alianzas Público Privadas
- Auditoría Fiscal y Manejo Fondos Públicos
- Revisión Continua Código Penal y Reforma de las Leves



Estado Libre Asociado de Puerto Rico  
**Oficina del Contralor**

RECIBIDO SECRETARIA  
SAN JUAN DE P.R.

2012 APR 10 AM 8:57

Yesmín M. Valdivieso  
Contralora

3 de abril de 2012

**A LA MANO**

**PRIVILEGIADA Y CONFIDENCIAL**

Hon. Thomas Rivera Schatz  
Presidente  
Senado de Puerto Rico  
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copias de los informes de auditoría *TI-12-10* y *TI-12-11* de la División de Informática de la Oficina del Comisionado de Asuntos Municipales y de la Oficina de Sistemas de Información, Computación y Comunicación de la Universidad de Puerto Rico en Humacao, respectivamente, aprobados por esta Oficina el 26 de marzo de 2012. Publicaremos dichos informes en nuestra página en Internet: <http://www.ocpr.gov.pr> para conocimiento de los medios de comunicación y de otras partes interesadas.

Estamos a sus órdenes para ofrecerle cualquier información adicional que estime necesaria.

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

Cordialmente,

  
Yesmín M. Valdivieso

Anejos

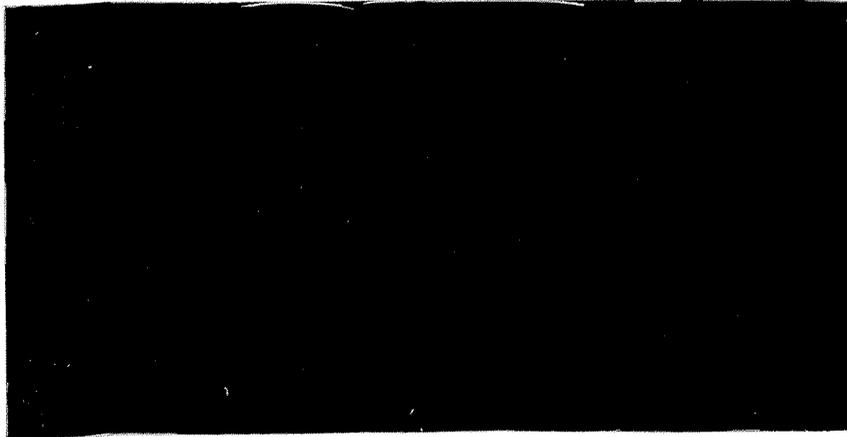
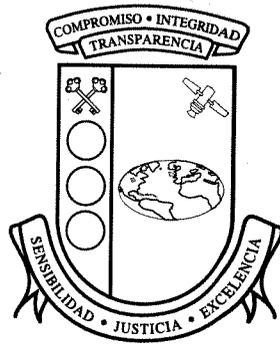
2012 APR -9 AM 2:22

RECEIVED  
SECRETARIA  
SAN JUAN DE P.R.

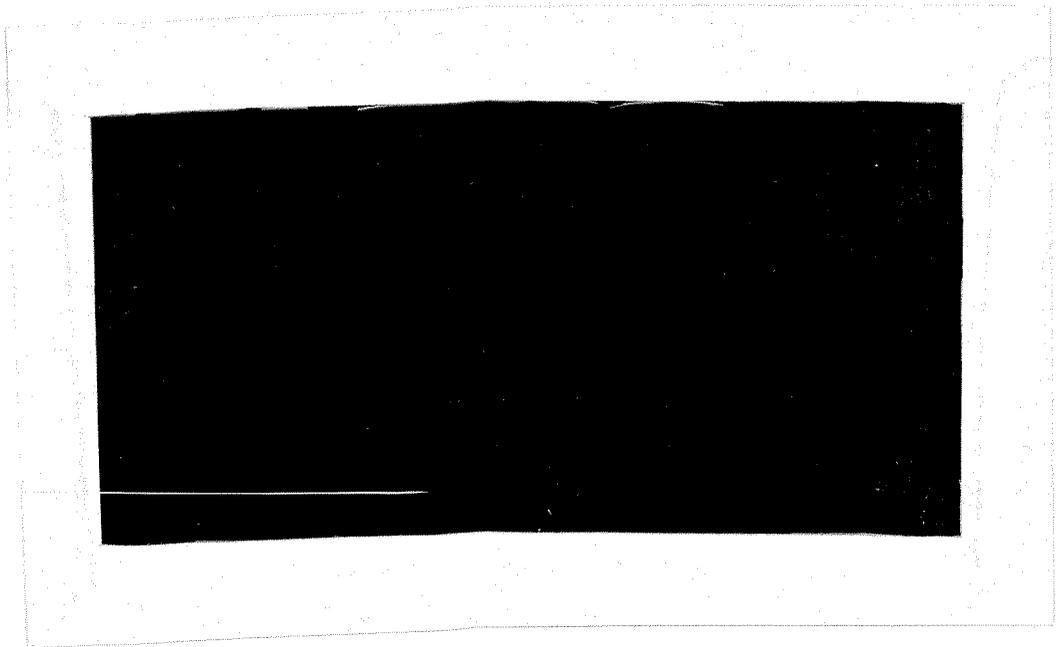
PO BOX 366069 SAN JUAN PUERTO RICO 00936-6069  
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136  
TEL. (787) 754-3030 FAX (787) 751-6768  
E-MAIL: [ocpr@ocpr.gov.pr](mailto:ocpr@ocpr.gov.pr) INTERNET: <http://www.ocpr.gov.pr>

PO17756





*Estado Libre Asociado de Puerto Rico*  
*Oficina del Contralor*  
*San Juan, Puerto Rico*



**INFORME DE AUDITORÍA TI-12-10**

26 de marzo de 2012

**Oficina del Comisionado de Asuntos Municipales**

**División de Informática**

(Unidad 5374 - Auditoría 13359)

Período auditado: 9 de septiembre de 2009 al 28 de mayo de 2010



## CONTENIDO

	<b>Página</b>
<b>ALCANCE Y METODOLOGÍA .....</b>	<b>2</b>
<b>OBJETIVOS DE LA AUDITORÍA .....</b>	<b>2</b>
<b>INFORMACIÓN SOBRE LA UNIDAD AUDITADA .....</b>	<b>3</b>
<b>COMUNICACIÓN CON LA GERENCIA .....</b>	<b>4</b>
<b>OPINIÓN Y HALLAZGOS.....</b>	<b>4</b>
1 - Falta de un informe de avalúo de riesgos de los sistemas de información computadorizados .....	5
2 - Deficiencias relacionadas con el Manual de Gestión de Seguridad de la Información (MGSI) sobre aspectos de seguridad.....	6
3 - Deficiencias relacionadas con el <i>OCAM Disaster Recovery Guide</i> , y falta de pruebas o simulacros para comprobar su efectividad, y falta de un centro alternativo para la recuperación de las operaciones computadorizadas .....	8
4 - Falta de documentación sobre la justificación y la autorización de las cuentas de acceso con privilegios de administrador de los sistemas operativos.....	12
5 - Deficiencias relacionadas con los controles para la preparación, el manejo y la identificación de los respaldos de información de la OCAM .....	14
<b>RECOMENDACIONES .....</b>	<b>16</b>
<b>AGRADECIMIENTO.....</b>	<b>18</b>
<b>ANEJO - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DEL 9 DE         SEPTIEMBRE DE 2009 AL 28 DE MAYO DE 2010 .....</b>	<b>19</b>

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

26 de marzo de 2012

Al Gobernador, al Presidente del Senado  
y a la Presidenta de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la División de Informática (DI) de la Oficina del Comisionado de Asuntos Municipales (OCAM) para determinar si se hicieron de acuerdo con las normas generalmente aceptadas en este campo y si el sistema de control interno establecido para el procesamiento de las transacciones era adecuado. Efectuamos 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.

---

**ALCANCE Y  
METODOLOGÍA**

La auditoría cubrió del 9 de septiembre de 2009 al 28 de mayo de 2010. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas, inspecciones físicas, examen y análisis de informes y de documentos generados por la unidad auditada, pruebas y análisis de procedimientos de control interno y de otros procesos, y confirmaciones de información pertinente.

---

**OBJETIVOS DE LA  
AUDITORÍA**

Este *Informe* contiene cinco hallazgos sobre el resultado del examen que realizamos de la administración de la seguridad y la continuidad de servicio de la OCAM. El mismo está disponible en nuestra página en Internet: <http://www.ocpr.gov.pr>.

**INFORMACIÓN SOBRE  
LA UNIDAD AUDITADA**

La OCAM se creó mediante la *Ley 81-1991, Ley de Municipios Autónomos del Estado Libre Asociado de Puerto Rico*, según enmendada. Esta *Ley* derogó la *Ley Núm. 18 del 9 de agosto de 1974, Ley de la Administración de Servicios Municipales*. Con la *Ley 81-1991* se le asigna a la OCAM, entre otras funciones dispuestas por esta *Ley*, la responsabilidad principal de asesorar y aprobar reglamentación para los municipios con el propósito de asegurar la aplicación de los procedimientos de contabilidad generalmente aceptados.

La OCAM está dirigida por un Comisionado, nombrado por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico. Para llevar a cabo sus operaciones, la OCAM cuenta con una estructura organizacional compuesta por la Oficina de Asesoramiento Legal, la Oficina de Auditoría Interna y el Área de Administración. Esta última es dirigida por un Comisionado Auxiliar que vela por el funcionamiento de cinco divisiones. Estas son: Recursos Humanos, Finanzas, Servicios Generales, Presupuesto y Planificación, y DI.

Por otra parte, la OCAM cuenta con las siguientes áreas programáticas: Asesoramiento, Reglamentación e Intervención Fiscal, Sistemas de Información<sup>1</sup>, Programas Federales, Códigos de Orden Público, Organizaciones Comunitarias y Bases de Fe, y Programa de Justicia Juvenil<sup>2</sup>.

La DI la dirige un Ayudante Especial que tiene a su cargo la administración de la red de comunicaciones (red) de la OCAM. Esta red consiste de 7 servidores.

---

<sup>1</sup> Esta área tiene la responsabilidad principal de proveer el asesoramiento técnico para la utilización del Sistema de Contabilidad Uniforme Mecanizado (SUCM) diseñado por la OCAM o para la instalación de nuevos sistemas adquiridos o desarrollados por los municipios. Además, el Área de Sistemas de Información es la responsable de asegurarse de que los municipios cumplan con los requisitos establecidos por el Comisionado.

<sup>2</sup> El Área de Códigos de Orden Público fue adscrita a la OCAM por virtud de la *Ley 169-2005*. El Boletín Núm. OE-2005-32 del 19 de mayo de 2005 adscribió a la OCAM el Área de Organizaciones Comunitarias y Bases de Fe, y el 2 de marzo de 2006 le fue adscrita el Programa de Justicia Juvenil.

El **ANEJO** contiene una relación de los funcionarios principales de la OCAM que actuaron del 9 de septiembre de 2009 al 28 de mayo de 2010.

Los gastos de operación de la DI se sufragan del presupuesto de la OCAM, que para el año fiscal 2009-10 ascendió a \$4,415,114.

También cuenta con una página en Internet a la cual se puede acceder mediante la siguiente dirección: <http://www.ocam.gobierno.pr>. Esta página provee información acerca de la entidad y de los servicios que presta.

---

## COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al entonces Comisionado, Sr. Omar Negrón Judice, por carta de nuestros auditores, del 1 de junio de 2010. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

El 25 de junio de 2010, el entonces Comisionado remitió sus comentarios a los **hallazgos** incluidos en la carta de nuestros auditores. Sus comentarios fueron considerados en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al entonces Comisionado para comentarios, por carta del 31 de mayo de 2011.

El entonces Comisionado contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 1 de julio de 2011. Sus comentarios fueron considerados en la redacción final de este *Informe*; y se incluyen en la sección titulada **Opinión y Hallazgos**.

---

## OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la DI en lo que concierne a los controles internos establecidos para la administración del programa de seguridad y la continuidad del servicio no se realizaron conforme a las normas generalmente aceptadas en este campo. A continuación se comentan los **hallazgos del 1 al 5**.

## **Hallazgo 1 - Falta de un informe de avalúo de riesgos de los sistemas de información computadorizados**

### **Situación**

a. Un avalúo de riesgos de los sistemas de información computadorizados es un método para identificar las vulnerabilidades y las amenazas a los recursos de dichos sistemas. Mediante este se identifican los posibles daños para determinar dónde implantar las medidas de seguridad para proteger dichos recursos, de manera que no se afecten adversamente las operaciones. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.
- Identificar las vulnerabilidades y las amenazas de los recursos de sistemas de información.
- Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad gubernamental.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 25 de marzo de 2010, en la OCAM no se había preparado por escrito un informe de avalúo de riesgos de los sistemas de información computadorizados.

### **Criterio**

Esta situación es contraria a lo establecido en la *Política Núm. TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipo 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.

**Efectos**

La situación comentada impidió a la OCAM estimar el impacto que los elementos de riesgo tendrían sobre las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información. [Véase el Hallazgo 2] 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. [Véase el Hallazgo 3]

**Causa**

La situación comentada se atribuye a que el Comisionado no había promulgado una directriz para la preparación y la documentación del avalúo de riesgos de los sistemas de información de la OCAM, según lo establecido en la *Carta Circular Núm. 77-05*.

**Comentarios de la Gerencia**

En la carta del entonces Comisionado, este nos indicó, entre otras cosas, lo siguiente:

En este momento nos encontramos evaluando la información y requerimientos necesarios para la preparación del informe.

**Véase la Recomendación 1.****Hallazgo 2 - Deficiencias relacionadas con el Manual de Gestión de Seguridad de la Información (MGSI) sobre aspectos de seguridad****Situación**

- a. Al 18 de mayo de 2010, la OCAM contaba con el *Manual de Gestión de Seguridad de la Información* (MGSI)<sup>3</sup> como plan de seguridad. El MGSI fue preparado en noviembre de 2004, a un costo de \$16,000, por una compañía<sup>4</sup> contratada por la OCAM. En este se establecían las políticas y los procedimientos sobre aspectos de la seguridad que la OCAM debía considerar.

---

<sup>3</sup> El MGSI se revisó y aprobó el 30 de junio de 2011. Esta revisión contempló asignar responsabilidades, establecer un programa de adiestramiento, y establecer controles administrativos, técnicos y físicos relacionados con los sistemas de información computadorizados de la OCAM.

<sup>4</sup> El nombre de la compañía se incluyó en el borrador de los hallazgos del *Informe* remitido al entonces Comisionado para comentarios.

El examen del MGSÍ revisado y aprobado reveló que este carecía de la siguiente información, que debe ser parte esencial de un plan de seguridad:

- La documentación de la validación de las normas de seguridad<sup>5</sup>
- La evidencia de un análisis de riesgos actualizado, que sea la base de las determinaciones sobre la seguridad y la continuidad de las operaciones. [Véase el Hallazgo 1]

Una situación similar fue comentada en el informe *OCAM-09-01* del 15 de noviembre de 2008, emitido por la Oficina de Auditoría Interna de la OCAM.

#### **Criterio**

Esta situación es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*.

#### **Efecto**

La situación comentada podría provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos.

#### **Causa**

La situación comentada se atribuye a que el Comisionado no se aseguró de que se efectuara el informe de avalúo de riesgos previo a la revisión y a la aprobación del MGSÍ. Tampoco se aseguró de incluir en el mencionado documento la validación de las normas establecidas.

#### **Comentarios de la Gerencia**

En la carta del entonces Comisionado, este nos indicó, entre otras cosas, lo siguiente:

Se incluye el Manual de Gestión de Seguridad de la Información aprobado por el Comisionado en junio de 2011.

---

<sup>5</sup> La validación de las normas de seguridad se efectúa mediante las pruebas de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el avalúo de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

Consideramos las alegaciones del Comisionado, pero determinamos que el **Hallazgo** prevalece. Esto, porque el MGSÍ incluido en la carta del Comisionado carecía de la documentación sobre la validación de las normas de seguridad y la evidencia de un análisis de riesgos actualizado, que sea la base para las determinaciones sobre la seguridad y la continuidad de las operaciones.

**Véase la Recomendación 2.a.**

**Hallazgo 3 - Deficiencias relacionadas con el *OCAM Disaster Recovery Guide*, y falta de pruebas o simulacros para comprobar su efectividad, y falta de un centro alternativo para la recuperación de las operaciones computadorizadas**

**Situaciones**

- a. Al 9 de septiembre de 2009, la OCAM contaba con el *OCAM Disaster Recovery Operation Guide* (Guía) como plan de continuidad de negocio. El mismo fue preparado en diciembre de 2004, a un costo de \$10,000, por una compañía<sup>6</sup> contratada para preparar un plan para el manejo de desastres y un plan de contingencias.

El examen de la Guía, reveló las siguientes deficiencias:

- 1) Como plan de continuidad de negocio, carecía de los planes específicos, completos y actualizados de la DI. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la DI, en caso de riesgos como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros. En su lugar, la Guía consistía de instrucciones para operar, configurar y monitorear el directorio<sup>7</sup> de los servicios provistos para los servidores de la OCAM.

---

<sup>6</sup> Véase la nota al calce 4.

<sup>7</sup> Mediante este directorio se permite el acceso a la información y a los recursos de la red a los administradores y usuarios autorizados a través de un proceso de autenticación.

- 2) Como plan de contingencia, no incluía los siguientes requisitos que son parte esencial al atender las situaciones de emergencia:
- El nombre del encargado de activar el plan y del personal de reserva, de manera que pueda ser activado sin depender de individuos específicos
  - La identificación de los integrantes de los grupos de recuperación y la responsabilidad asignada a cada uno
  - Una lista de los números de teléfonos de los miembros de cada grupo de recuperación
  - Un plan general de acción identificado por grupos y tareas de forma secuencial
  - El inventario de los equipos, los sistemas operativos, las aplicaciones y los archivos críticos de la OCAM
  - El detalle de la configuración de los sistemas utilizados en la DI y los requeridos para el centro de información alternativo
  - El itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos
  - Una lista de los proveedores principales, que incluya el número de teléfono y el nombre del personal de enlace con la OCAM
  - Los procedimientos para efectuar pruebas en el centro alternativo
  - Una hoja de cotejo para verificar los daños ocasionados por la contingencia.
- b. Al 6 de abril de 2010, la OCAM no había realizado pruebas o simulacros que certificaran la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afectan su funcionamiento.

- c. Al 21 de mayo de 2010, la OCAM no contaba con un centro alternativo para restaurar sus operaciones críticas computadorizadas en caso de emergencia. Tampoco había formalizado acuerdos con otra entidad para establecer un centro alternativo en las instalaciones de esta.

### **Criterios**

La situación comentada en el **apartado a.1)** es contraria a lo establecido en las políticas núms. *TIG-003* y *TIG-004, Servicios de Tecnología* de la *Carta Circular Núm. 77-05*.

Las mejores prácticas en el campo de la tecnología utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que como parte del *Plan de Continuidad de Negocios* se deberá preparar un *Plan de Contingencias*. Este es una guía que asegura la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afectan su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la entidad y deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del centro de cómputos o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. **[Apartado a.2)]** Además, se deben efectuar pruebas o simulacros, por lo menos una vez al año, para comprobar la efectividad de los planes. **[Apartado b.]**

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. 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 c.]**

- Una entidad pública o privada de similar configuración y tamaño
- Una compañía dedicada a servicios de restauración

- Un centro alternativo de la propia entidad.

### **Efectos**

Las situaciones comentadas en los **apartados a. y b.** pueden 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, e interrupciones prolongadas de los servicios ofrecidos a los usuarios de la OCAM.

La situación comentada en el **apartado c.** podría afectar las funciones de la OCAM y los servicios de la DI, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la DI.

### **Causas**

Las situaciones comentadas en el **apartado a.** se atribuyen a la falta de un avalúo de riesgos de los sistemas de información computadorizados de la OCAM (**Véase el Hallazgo 1**) que sirviera de base para la preparación y la revisión del plan de continuidad de negocios. También denotan que el Comisionado no había impartido instrucciones al Ayudante Especial de la DI para que se asegurara de considerar los aspectos que se indican en el **apartado a.** de este **Hallazgo**.

La situación comentada en el **apartado b.** se atribuye a que el Ayudante Especial de la DI no había realizado las gestiones para que se prepararan para la aprobación del Comisionado los procedimientos escritos para efectuar las pruebas y corroborar que las operaciones computadorizadas de la OCAM pueden ser restauradas.

La situación comentada en el **apartado c.** se atribuye a que el Ayudante Especial de la DI no había coordinado la identificación de un lugar disponible y adecuado como centro alternativo para restaurar las operaciones críticas computadorizadas de la DI.

### **Comentarios de la Gerencia**

En la carta del entonces Comisionado, este nos indicó, entre otras cosas, lo siguiente:

Se incluye el *OCAM Disaster Recovery Operation Guide* aprobado por el Comisionado. **[Apartado a.]**

Estamos coordinando un simulacro para finales de agosto de 2011. **[Apartado b.]**

En este momento nuestro centro alternativo de recuperación está localizado en las facilidades de [...]. En ese lugar se pueden restablecer las operaciones de la DI ya que nuestra oficina realiza un *backup* diario para poder recuperar la data de surgir una emergencia. *[sic]* **[Apartado c.]**

Consideramos las alegaciones del entonces Comisionado, pero determinamos que los apartados a. y c. del Hallazgo prevalecen. El *OCAM Disaster Recovery Operation Guide* no incluye los elementos indicados y no enviaron evidencia de que en el lugar externo se puedan restaurar las operaciones de la DI.

**Véanse las recomendaciones de la 2.b. a la d., y 3.**

### **Hallazgo 4 - Falta de documentación sobre la justificación y la autorización de las cuentas de acceso con privilegios de administrador de los sistemas operativos**

#### **Situación**

- a. Al 25 de marzo de 2010, el Ayudante Especial de la DI no proveyó a nuestros auditores los documentos justificantes para autorizar el acceso a 12 cuentas de acceso activas con privilegios de administrador de los sistemas operativos. Estas cuentas eran solicitadas mediante llamadas telefónicas, peticiones verbales o correos electrónicos, de los cuales no se conservaba documentación. Una cuenta como esta tiene amplios privilegios que permiten, entre otras cosas, realizar cambios a la configuración del sistema, instalar programas y equipos, acceder a todos los archivos de la computadora y realizar cambios a las cuentas de otros usuarios.

**Criterio**

Esta situación es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*.

**Efectos**

La situación comentada impide mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y los privilegios a los usuarios. También propicia que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, puede propiciar la comisión de errores e irregularidades, sin que puedan ser detectados a tiempo para fijar responsabilidades.

**Causa**

La situación comentada se atribuye a que el Comisionado Auxiliar del Área de Administración no le requirió al Ayudante Especial de la DI que desarrollara y remitiera, para la consideración y aprobación del Comisionado, un procedimiento para la creación, el mantenimiento y el control de las cuentas de acceso. Este debía incluir, entre otras cosas, la utilización y el control de un formulario para la solicitud, la creación, la aprobación y la cancelación de las cuentas de acceso de los usuarios, y para la justificación y la autorización de las cuentas de acceso con privilegios de administrador de los sistemas operativos.

**Comentarios de la Gerencia**

En la carta del entonces Comisionado, este nos indicó, entre otras cosas, los siguiente:

Se creó un formulario para fines de documentar los accesos y modificaciones a los sistemas de información de la red de la OCAM.

Consideramos las alegaciones del entonces Comisionado, pero determinamos que el **Hallazgo** prevalece porque no enviaron evidencia de la acción tomada con relación a las 12 cuentas con privilegios de administrador de los sistemas operativos.

**Véase la Recomendación 2.e. y f.**

### **Hallazgo 5 - Deficiencias relacionadas con los controles para la preparación, el manejo y la identificación de los respaldos de información de la OCAM**

#### **Situaciones**

- a. El 2 de agosto de 2007, la OCAM formalizó un acuerdo por tres años con una compañía<sup>8</sup> para obtener servicios de Internet, tecnología VoIP<sup>9</sup> y almacenaje de datos. Como parte del acuerdo, la OCAM ubicó un servidor<sup>10</sup> en la instalación física de la compañía. Esto, con el propósito de mantener un respaldo externo de los datos que almacena el servidor principal<sup>10</sup> de la OCAM. Además, mantenía un contrato con una compañía<sup>11</sup> para el almacenamiento de las cintas de respaldo.

El examen del proceso de preparación, manejo e identificación de los respaldos, reveló las siguientes deficiencias:

- 1) Al 13 de mayo de 2010, el servidor<sup>10</sup> ubicado en la instalación física de la compañía no recibía del servidor principal<sup>10</sup> el respaldo externo de las aplicaciones críticas de la OCAM, y de los datos procesados por estas.
- 2) Al 14 de mayo de 2010, las etiquetas utilizadas para identificar las cintas de respaldo carecían de la siguiente información:
  - La descripción clara de los archivos respaldados
  - La identificación de la procedencia de los archivos
  - La fecha de actualización del respaldo.

En su lugar, las cintas solo se identificaban con un número secuencial.

---

<sup>8</sup> Véase la nota al calce 4.

<sup>9</sup> Esta es una tecnología que hace posible tener una conversación de voz a través de Internet en lugar de líneas de transmisión de voz dedicadas. También se conoce como telefonía IP, Internet telefónico o telefonía de banda amplia.

<sup>10</sup> El nombre del servidor se incluyó en el borrador de los **hallazgos** del *Informe* remitido al entonces Comisionado para comentarios.

<sup>11</sup> Véase la nota al calce 4.

### **Crterios**

Las situaciones comentadas en el **apartado a.1) y 2)** se apartan de lo establecido en la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05*. En consonancia con dicha política pública, es necesario, entre otras cosas, que la información esencial para las operaciones normales de la entidad, sea duplicada periódicamente y guardada en un lugar seguro fuera de los predios de la entidad. Esto, con el propósito de recuperar la mayor cantidad de información posible en caso de una emergencia o desastre. Además, las cintas de respaldo deben estar rotuladas con la información que permita su pronta localización.

La situación comentada en el **apartado a.2)** es contraria a lo establecido en la sección de Procedimientos de Copias de Resguardo del *Manual de Normas y Procedimientos Uso de Microcomputadoras de la OCAM*, aprobado en el 2000 por la Comisionada.

### **Efectos**

La situación comentada en el **apartado a.1)** pueden ocasionar que en casos de emergencias la OCAM no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

La situación comentada en el **apartado a.2)** podría dificultar la localización e identificación del contenido de las cintas de respaldos en caso de que se requiera reconstruir la información en forma efectiva.

### **Causa**

Las situaciones comentadas se debieron a la falta de un procedimiento detallado y aprobado por el Comisionado para la creación, la rotulación, las pruebas, el envío y el almacenamiento de las cintas de respaldos.

### **Comentarios de la Gerencia**

En la carta del entonces Comisionado, este nos indicó, entre otras cosas, lo siguiente:

Se realizó una reconfiguración de los respaldos realizados fuera de los predios de la oficina, el mismo incluye toda la información crítica de la agencia.

Dado que en la evidencia provista para examen de nuestros auditores no se incluyó como parte de la reconfiguración de los respaldos, la información de Finanzas y la correspondiente a la aplicación del sistema de la OCAM, consideramos las alegaciones del Comisionado, pero determinamos que el **Hallazgo** prevalece.

Véase la **Recomendación 2.g.**

## RECOMENDACIONES

### Al Comisionado de Asuntos Municipales

1. Asegurarse de que se realice el análisis de riesgos de los sistemas de información y se documente en un informe, según se establece en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* y se sugiere en las mejores prácticas en el campo de la tecnología. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. **[Hallazgo 1]**
2. Ejercer una supervisión eficaz sobre el Comisionado Auxiliar de Administración, para asegurarse de que el Ayudante Especial de la DI:
  - a. Revise el *MGSI* para que se incluyan los aspectos que surjan del informe de avalúo de riesgos, y lo remita para su aprobación. Una vez aprobado, prepare los procedimientos de prueba necesarios para validar la efectividad de los controles establecidos. **[Hallazgo 2]**
  - b. Prepare un plan de continuidad de negocios que cumpla con lo requerido en la *Política Núm. TIG-003*. Este plan debe ser remitido para la revisión y la aprobación del Comisionado. Una vez este sea aprobado, tomar 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 OCAM. Además, el plan debe ser distribuido a los funcionarios y a los empleados concernientes. **[Hallazgo 3-a.1)]**

- c. Revise el *OCAM Disaster Recovery Operation Guide* para que incluyan los aspectos comentados en el **Hallazgo 3-a.2)** y lo remita para la aprobación del Comisionado.
  - d. Prepare los procedimientos de prueba o simulacros necesarios para verificar que las operaciones computarizadas de la OCAM pueden ser restauradas y lo remita para la aprobación del Comisionado. Una vez este sea aprobado, efectúe las pruebas correspondientes, por lo menos una vez al año, y mantenga la documentación de las estrategias utilizadas y de los resultados de las pruebas. **[Hallazgo 3-b.]**
  - e. Prepare los procedimientos para la solicitud, la aprobación, la creación, la modificación y la cancelación de las cuentas de acceso de los usuarios de los sistemas de información computarizados, y para la justificación y la autorización de las cuentas de acceso con privilegios de administrador de los sistemas operativos y los remita para la aprobación del Comisionado. **[Hallazgo 4]**
  - f. Evalúe los deberes y las responsabilidades de los usuarios que tienen cuentas de acceso con privilegios de administrador de los sistemas operativos. Una vez realizada la evaluación, documente la justificación y la autorización de los privilegios otorgados. **[Hallazgo 4]**
  - g. Revise las normas y los procedimientos para la preparación, el manejo y la identificación del respaldo de las aplicaciones y los datos críticos de la OCAM, para que se corrijan y no se repitan las situaciones comentadas en el **Hallazgo 5.**
3. Formalizar un acuerdo escrito con otra entidad que acepte la utilización de sus equipos en caso de desastres o emergencias en la OCAM, o considerar establecer su propio centro alternativo en alguna instalación que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la DI. **[Hallazgo 3-c.]**

**AGRADECIMIENTO**

A los funcionarios y a los empleados de la OCAM, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Por:

*Oficina del Contralor*  
*José María Maldonado*

## ANEJO

OFICINA DEL COMISIONADO DE ASUNTOS MUNICIPALES  
DIVISIÓN DE INFORMÁTICA  
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD  
DEL 9 DE SEPTIEMBRE DE 2009 AL 28 DE MAYO DE 2010

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Omar E. Negrón Judice	Comisionado	9 sep. 09	28 m. 10
Sr. Juan C. Cruz Rodríguez	Comisionado Auxiliar de Administración	9 sep. 09	28 m. 10
Sr. Javier Castro Badillo	Ayudante Especial encargado de la División de Informática	9 sep. 09	28 m. 10
Sr. Ángel Delgado Rivera	Director de Finanzas	9 sep. 09	28 m. 10
Sr. José Velázquez Ruiz	Comisionado Auxiliar de Reglamentación e Intervención	9 sep. 09	28 m. 10
Sra. Máver Rivas Muñoz	Directora de Recursos Humanos	21 dic. 09	28 m. 10
Vacante	Director de Recursos Humanos <sup>12</sup>	9 sep. 09	20 dic. 09

---

<sup>12</sup> El Sr. Juan C. Cruz Rodríguez, Comisionado Auxiliar de Administración, ejercía las funciones de Director de Recursos Humanos.

---

**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, extensión 2124, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico [Querellas@ocpr.gov.pr](mailto:Querellas@ocpr.gov.pr) o a través de 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.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet en 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) 294-0625 o (787) 200-7253, extensión 536.

---

**INFORMACIÓN DE  
CONTACTO***Dirección física:*

105 Avenida Ponce de León  
Hato Rey, Puerto Rico  
Teléfono: (787) 754-3030  
Fax: (787) 751-6768

*Internet:*

<http://www.ocpr.gov.pr>

*Correo electrónico:*

[ocpr@ocpr.gov.pr](mailto:ocpr@ocpr.gov.pr)

*Dirección postal:*

PO Box 366069  
San Juan, Puerto Rico 00936-6069



