# Secretaría

## Lcda. Tania Barbarossa Ortiz

- ☐ Ver al dorso
- ☐ Para su información
- ☐ Notas
- ☐ Para mantenerle al día
- ☐ Expediente
- ☑ Dar Cuenta
- ☐ Registrar y Procesar
- ☐ Archivar
- ☐ Preparar Carta

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

# 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 Públic
- ☐ 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 R
- ☐ 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 Leye

#860

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

**Yesmín M. Valdivieso**
*Contralora*

RECIBIDO
SECRETARIA
SENADO P.R.
2013 AUG -1 AM 9:58

8 de marzo de 2013

**A LA MANO**

**PRIVILEGIADA Y CONFIDENCIAL**

Hon. Eduardo A. Bhatia Gautier
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-13-17* de la Oficina de Gerencia de Sistemas de Información del Centro de Recaudación de Ingresos Municipales, aprobado por esta Oficina el 22 de febrero de 2013. Publicaremos dicho *Informe* 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

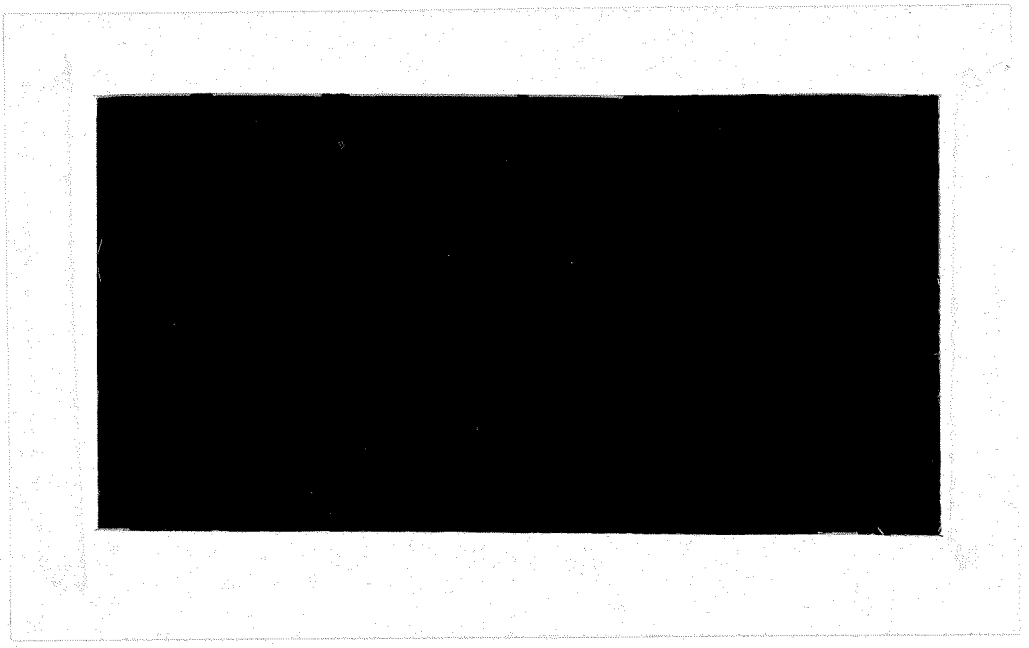
Anejo

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

#860

[redacted]

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



**INFORME DE AUDITORÍA TI-13-17**

22 de febrero de 2013

**Centro de Recaudación de Ingresos Municipales**

**Oficina de Gerencia de Sistemas de Informática**

(Unidad 5194 - Auditoría 13540)

Período auditado: 17 de noviembre de 2010 al 13 de mayo de 2011

## CONTENIDO

Página

**ALCANCE Y METODOLOGÍA** ..... **2**

**CONTENIDO DEL INFORME** ..... **2**

**INFORMACIÓN SOBRE LA UNIDAD AUDITADA** ..... **3**

**COMUNICACIÓN CON LA GERENCIA** ..... **4**

**OPINIÓN Y HALLAZGOS** ..... **5**

1 - Cuentas para acceder a Internet utilizadas para fines ajenos a la gestión pública ..... 5

2 - Deficiencias en la Evaluación de Riesgos y en la Evaluación de Riesgo y Actividades de Control Área de Sistemas de Información, y falta de un plan de seguridad y de acuerdos de confidencialidad ..... 8

3 - Falta de un plan de continuidad de negocios y de un centro alterno para la recuperación de los sistemas de información ..... 12

4 - Deficiencias en los parámetros de contraseñas y en el proceso de eliminar las cuentas de acceso de los exempleados ..... 15

5 - Falta de normas y de procedimientos para reglamentar las operaciones de la OGSI ..... 17

6 - Falta de diagramas esquemáticos de las oficinas regionales ..... 19

**RECOMENDACIONES** ..... **20**

**AGRADECIMIENTO** ..... **22**

**ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE GOBIERNO DURANTE EL PERÍODO AUDITADO** ..... **23**

**ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO** ..... **24**

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

22 de febrero de 2013

Al Gobernador, y a los presidentes del Senado
y de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la Oficina de Gerencia de Sistemas de Informática (OGSI) del Centro de Recaudación de Ingresos Municipales (CRIM) 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. 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.

**ALCANCE Y METODOLOGÍA**

La auditoría cubrió del 17 de noviembre de 2010 al 13 de mayo de 2011. En algunos aspectos examinamos transacciones de fechas anteriores. 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. 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; pruebas y análisis de procedimientos de control interno; y confirmaciones de cuentas y de otra información pertinente.

**CONTENIDO DEL INFORME**

Este es el primer informe y contiene seis hallazgos sobre el resultado del examen que realizamos de los controles relacionados con la administración del programa de seguridad, el acceso lógico, la continuidad del servicio y la red de comunicaciones. El mismo está disponible en nuestra página en Internet: http://www.ocpr.gov.pr.

**INFORMACIÓN SOBRE LA UNIDAD AUDITADA**

El CRIM es una entidad municipal independiente de las demás agencias del Gobierno. Este se creó en virtud de la *Ley 80-1991, Ley del Centro de Recaudación de Ingresos Municipales*, según enmendada, con el propósito de recaudar, recibir y distribuir los fondos públicos que corresponden a los municipios.

Mediante la *Ley 83-1991, Ley de Contribución Municipal sobre la Propiedad de 1991*, según enmendada, se confirieron al CRIM los poderes y las facultades para realizar todas las operaciones relacionadas con la tasación, la imposición, la notificación, la determinación y el cobro de las contribuciones sobre la propiedad; y con las exoneraciones y las exenciones concedidas por ley. Además, se le transfirieron aquellos poderes referentes a la contribución sobre la propiedad mueble e inmueble, anteriormente asignados al Secretario de Hacienda.

Los poderes del CRIM son ejercidos por una Junta de Gobierno compuesta por nueve miembros. Siete de estos son alcaldes en representación de todos los municipios de Puerto Rico, y los otros dos son el Presidente del Banco Gubernamental de Fomento para Puerto Rico y el Comisionado de Asuntos Municipales. Las funciones administrativas del CRIM son ejercidas por un Director Ejecutivo nombrado por la Junta de Gobierno.

A la fecha de nuestra auditoría, la OGSI tenía en operación una red de comunicaciones de área amplia[1] (*WAN*, por sus siglas en inglés). Dicha red permite el acceso a los sistemas de información computadorizados de los usuarios de la Oficina Central y de las nueve oficinas regionales.

Los recursos para financiar las actividades operacionales de la OGSI provienen de los ingresos que genera el CRIM. El presupuesto del CRIM

[1] Es una red de comunicación que se conecta con diferentes lugares remotos que puede incluir desde distancias cortas, como por ejemplo un piso o un edificio, hasta transmisiones extremadamente largas que abarcan una región grande o varios países.

en el año fiscal 2009-10 ascendió a $40,081,055. Este presupuesto procede de los fondos operacionales, de mejoras permanentes y de catastro digital.

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

El CRIM cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.crimpr.net. 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 a la Lcda. Gloria E. Santos Rosario, CPA, Directora Ejecutiva, mediante carta de nuestros auditores del 30 de agosto de 2011. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante carta del 16 de septiembre de 2011, la Directora Ejecutiva remitió sus comentarios a los **hallazgos** incluidos en la carta de nuestros auditores. Sus comentarios fueron considerados al redactar el borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió a la Directora Ejecutiva para comentarios, por carta del 29 de noviembre de 2012. En este se indicaron datos específicos, tales como: nombres, cuentas de acceso y localizaciones, que por seguridad no se incluyen en este *Informe*. El 10 de diciembre de 2012 la CPA Gricelis Acevedo Román, Directora de Auditoría Interna del CRIM, solicitó una prórroga para remitir los comentarios de la Directora Ejecutiva. El mismo día le concedimos la prórroga a la Directora Ejecutiva para remitir sus comentarios hasta el 21 de diciembre de 2012.

La Directora Ejecutiva contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 10 de enero de 2013. Sus comentarios se consideraron en la redacción final de este *Informe*, y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

**OPINIÓN Y HALLAZGOS**

Las pruebas efectuadas revelaron que las operaciones de la OGSI, en lo que concierne a los controles establecidos para la administración del programa de seguridad, el acceso lógico, la continuidad del servicio y la red de comunicaciones se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 6** que se comentan a continuación.

**Hallazgo 1 - Cuentas para acceder a Internet utilizadas para fines ajenos a la gestión pública**

**Situación**

a. El CRIM mantenía en un servidor una aplicación que permitía el acceso a Internet a los usuarios autorizados y, además, filtraba y monitoreaba el uso del mismo. La aplicación generaba un archivo diariamente con el registro de todas las direcciones en Internet (*web logs*) que fueron accedidas por las cuentas de los usuarios. El examen del registro de direcciones en Internet visitadas por los usuarios y registradas en el servidor el 22 de febrero de 2011, reveló que de un total de 114 cuentas que accedieron a Internet ese día, 54 fueron utilizadas para examinar páginas en Internet con contenido ajeno a la gestión pública.

**Criterios**

La situación comentada es contraria a lo establecido en:

- La Sección 9 del Artículo VI de la Constitución en la que se establece que sólo se dispondrá de las propiedades y de los fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado y en todo caso por autoridad de ley.

- El Artículo 3.2(c) de la *Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, según enmendada[2], en el que se dispone, entre otras cosas, que

[2] Esta *Ley* fue derogada por la *Ley 1-2012, Ley de Ética Gubernamental de Puerto Rico de 2011*, la cual en el Artículo 4.2(b) contiene disposiciones similares.

ningún funcionario o empleado público utilizará propiedad pública para obtener directa o indirectamente ventajas, beneficios o privilegios que no estén permitidos por ley.

- Las *Normas para el Uso, Administración y Seguridad de los Sistemas Electrónicos* (*Normas de los Sistemas Electrónicos*), aprobadas el 28 de mayo de 2003 por la Junta de Gobierno y el Director Ejecutivo del CRIM, en las que se establece, entre otras cosas, que se prohíbe el uso de los sistemas de microcomputadoras y comunicaciones para propósitos personales, de recreo, y de manejo de un negocio o asunto privado de un usuario. Además, se establece que el usuario no podrá utilizar los recursos electrónicos del CRIM para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a sus funciones.

**Efectos**

El uso de las cuentas para acceder a páginas en Internet ajenas al fin público es contrario al interés público y desvirtúa el propósito para el cual fue asignado dicho privilegio. Además, provee al funcionario o empleado que indebidamente las utiliza, ventajas, beneficios y privilegios que no están permitidos por ley. También expone a los equipos y a la información sensitiva almacenada en los sistemas a riesgos innecesarios como son la propagación de virus, *spyware*[3],

[3] Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

*phishing*[4], *spoofing*[5], *spamming*[6] y ataques de negación de servicios[7], entre otros, que pudieran afectar la continuidad de las operaciones del CRIM, sin que se puedan fijar responsabilidades.

**Causas**

La situación comentada se debía, en parte, a la falta de:

- Orientaciones periódicas a los usuarios de los sistemas de información computadorizados sobre las leyes y las normas que reglamentan el uso y el manejo de las cuentas para acceder a Internet
- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento de las normas establecidas para el uso oficial de las cuentas para acceder a Internet
- Evaluaciones periódicas para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado a acceder a Internet. Esto, para que el encargado de administrar la red limite el acceso a las páginas autorizadas.

**Comentarios de la Gerencia**

En la carta de la Directora Ejecutiva, esta nos indicó, entre otras cosas, lo siguiente:

> [...] estaremos creando/redactando un documento oficial, que será firmado por el empleado detallando las políticas específicas del uso de Internet y las consecuencias de su mal uso. El mismo será parte integral del Manual del Empleado. Además se estará monitoreando preventivamente el uso adecuado de las cuentas de acceso y enviando comunicaciones periódicamente como

---

[4] Es un tipo de ataque de correo electrónico que trata de convencer a un usuario de que el originador es auténtico, pero con la intención de obtener información.

[5] Es un ataque activo en el que el intruso presenta una identidad que no es la identidad original. En este ataque, el propósito es obtener acceso a los datos sensitivos o a los recursos de los sistemas de información computadorizados a los que no se permite el acceso bajo la identidad original.

[6] Es el envío de correspondencia electrónica a cientos o a miles de usuarios.

[7] Ocurren cuando una computadora conectada a Internet es inundada con datos y solicitudes que deben ser atendidas. La computadora se dedica exclusivamente a atender estos mensajes y queda imposibilitada de realizar otras actividades.

> orientación. [...] Se establecerá un proceso de revisión periódica de los logs del Proxy/ISA para asegurar que no se estén accediendo páginas o "sites" no aprobados por el CRIM. [*sic*]

**Véanse las recomendaciones 1, y 2.a.1) y 2).**

**Hallazgo 2 - Deficiencias en la Evaluación de Riesgos y en la Evaluación de Riesgo y Actividades de Control Área de Sistemas de Información, y falta de un plan de seguridad y de acuerdos de confidencialidad**

**Situaciones**

a. Un análisis 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, 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 y pertinentes a las operaciones de la entidad gubernamental, y respondan a las posibles amenazas identificadas. El análisis 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.

   El 17 de noviembre de 2010 nos suministraron para examen la *Evaluación de Riesgos* y la *Evaluación de Riesgo y Actividades de Control Área de Sistemas de Información*. Estas evaluaciones consistían de unas tablas que incluían actividades de control, comentarios, objetivos, factores de riesgos, y conclusión, entre otros. El examen de estas evaluaciones de riesgos reveló que las

mismas carecían de un inventario de todos los activos de sistemas de información que detallara los equipos, programas y datos; y su valoración y clasificación de acuerdo con la misión y los servicios del CRIM. Además, no tenían la fecha de preparación ni los nombres y las firmas de los funcionarios que los prepararon y los aprobaron.

b. Al 7 de abril de 2011, el CRIM no tenía un plan de seguridad aprobado por la Directora Ejecutiva que incluyera, entre otras cosas, disposiciones en cuanto a:

- La documentación de la validación de las normas de seguridad[8]
- La evidencia de un análisis de riesgo actualizado, como base del plan de seguridad
- La responsabilidad de la gerencia, los oficiales de seguridad y de los demás componentes de la unidad, tales como, los dueños y los usuarios de los recursos de información, el personal administrativo del CRIM, el personal a cargo del procesamiento de los datos y los administradores de seguridad, entre otros
- Un programa de adiestramiento especializado al equipo clave de seguridad
- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, contratistas y usuarios, y que permita mantener los conocimientos actualizados
- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros).

---

[8] La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y vulnerabilidades detectadas en el análisis de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

c. Al 15 de abril de 2011, el CRIM no había establecido acuerdos de confidencialidad escritos con los empleados de la OGSI antes de exponerlos a información confidencial. Además, en el examen de 21 contratos de servicios para la OGSI, encontramos que 18 (86%) no contenían una cláusula sobre acuerdos de confidencialidad.

**Criterios**

Las mejores prácticas en el campo de la tecnología de información sugieren que cada entidad debe implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Para esto, deberá realizar un análisis de riesgos que incluya, al menos: **[Apartado a.]**

- Un inventario de activos de sistemas de información que incluya el equipo, los programas y los datos. Todos los activos deberán ser clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.

- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido a los datos, entre otras), junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

Además, las mejores prácticas en el campo de la tecnología de información sugieren que:

- Las entidades deben mantener un plan escrito que describa claramente el programa de seguridad y los procedimientos relacionados con este. Los mismos deben considerar los sistemas y las instalaciones principales, e identificar los deberes de los

dueños y de los usuarios de los sistemas de información de la entidad, y de los empleados responsables de velar por la seguridad de dichos sistemas. **[Apartado b.]**

- Las entidades deben establecer controles en el reclutamiento del personal de sistemas de información, especialmente para el área de seguridad, que requieran como medida de protección que este firme acuerdos de confidencialidad antes de exponerlo a información confidencial. Estos acuerdos deberán establecer, por escrito, las pautas a seguir para el manejo de la información confidencial, los límites establecidos para su divulgación y uso, y las obligaciones de las partes concernientes. **[Apartado c.]**

**Efectos**

La situación comentada en el **apartado a.** impide al CRIM estimar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de este, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

La situación comentada en el **apartado b.** 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.

La situación comentada en el **apartado c.** dificulta fijar responsabilidad a los empleados que trabajan con la información confidencial cuando la misma es divulgada. Además, puede dar lugar al uso indebido de la información privilegiada, lo que resultaría en otras consecuencias adversas para el CRIM.

**Causas**

La situación comentada en el **apartado a.** se atribuye a que en la *Evaluación de Riesgos* y en la *Evaluación de Riesgo y Actividades de Control Área de Sistemas de Información* del CRIM no se habían considerado todos los aspectos necesarios para la preparación de un análisis de riesgos. Además, estas evaluaciones no se habían remitido a la Directora Ejecutiva para revisión y aprobación.

La situación comentada en el **apartado b.** se atribuye a que la Directora Ejecutiva no había promulgado una directriz para el desarrollo, la implantación y la actualización continua del plan de seguridad.

La situación comentada en el **apartado c.** se atribuye, principalmente, a que en la Oficina de Recursos Humanos entendían que la confidencialidad de la información estaba considerada en las *Normas de los Sistemas Electrónicos*.

**Comentarios de la Gerencia**

En la carta de la Directora Ejecutiva, esta nos indicó, entre otras cosas, lo siguiente:

> [...] El área de Administración es el custodio de la valorización del inventario del equipo de computadoras del CRIM. La misma es aceptada y certificada por la OGSI. Al momento de esta auditoría, no contábamos con un inventario actualizado. Estaremos verificando y actualizando dicho inventario, para el análisis de riesgos correspondiente. La agencia estará considerando hacer contratación externa para llevar a cabo un Análisis de Riesgos de Tecnologías de Información. Para este análisis se estará considerando las guías publicadas por ISACA y por el Instituto de Auditores Internos. [*sic*] **[Apartado a.]**
>
> [...] aunque existe un borrador que recoge los diferentes puntos a establecerse en dicho plan, el mismo nunca fue certificado. Se estará trabajando con su actualización para ponerlo en función. **[Apartado b.]**
>
> [...] se ha creado un documento de confidencialidad el cual se integrará al Manual del Empleado y tendrá que ser firmado como aceptación. **[Apartado c.]**

**Véanse las recomendaciones 1 y de la 3 a la 5.a.**

**Hallazgo 3 - Falta de un plan de continuidad de negocios y de un centro alterno para la recuperación de los sistemas de información**

**Situaciones**

a. Al 18 de marzo de 2011, el CRIM carecía de un plan de continuidad de negocios aprobado que incluyera los planes específicos, completos y actualizados de la OGSI. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información

computadorizados y restaurar las operaciones de la OGSI en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, desastres naturales, entre otros.

Esta situación fue comentada por los auditores externos en su *Assessment of IT Organization and the Hansen Tax Management System* emitido el 22 de febrero de 2010.

b. El CRIM no contaba con un centro alterno de los sistemas de información para restaurar las operaciones críticas computadorizadas en casos de emergencias. Tampoco había formalizado acuerdos con otra entidad para establecer un centro alterno en las instalaciones de esta.

**Criterios**

Las mejores prácticas en el campo de la tecnología de información sugieren que:

- Las entidades deben desarrollar un Plan de Continuidad de Negocios que incluya un Plan para la Recuperación de Desastres y un Plan para la Continuidad de las Operaciones. **[Apartado a.]**

- Las dependencias y entidades gubernamentales deben garantizar el buen uso, el manejo, la integridad, la exactitud y la preservación de la información del Gobierno y protegerla contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental. Dicha medida se instrumenta, en parte, mediante el establecimiento de un centro alterno propio o mediante convenio con otra entidad donde se estipule la necesidad y los servicios requeridos para atender la emergencia. **[Apartado b.]**

**Efectos**

La situación comentada en el **apartado a.** puede propiciar la improvisación, y que en casos de emergencias 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 del CRIM. Además,

se podría atrasar el proceso de reconstrucción de archivos y programas, y el pronto restablecimiento y la continuidad de las operaciones normales de los sistemas de información del CRIM.

La situación comentada en el **apartado b.** podría afectar las funciones de la OGSI y los servicios del CRIM, 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 OGSI y el CRIM.

**Causas**

La situación comentada en el **apartado a.** se atribuye, en parte, a que la Directora Ejecutiva no había impartido una directriz para la preparación de un plan de continuidad de negocios, que incluyera un plan para la recuperación de desastres y un plan para la continuidad de las operaciones.

La situación comentada en el **apartado b.** se atribuye a que el Director de Sistemas de Información no había efectuado las gestiones para habilitar, con la infraestructura y los equipos necesarios, las instalaciones identificadas por el CRIM como un lugar para restaurar las operaciones críticas.

**Comentarios de la Gerencia**

En la carta de la Directora Ejecutiva, esta nos indicó, entre otras cosas, lo siguiente:

> [...] se ha analizado la viabilidad de establecer un plan de Continuidad de Negocios para la Oficina de Gerencia de Sistemas de Informática del CRIM. [...] Se debe evaluar y trabajar sobre al menos diez (10) puntos críticos ("Business Impact Analysis") para asegurar la continuidad operativa del CRIM y llevar a cabo todas las pruebas. Sin embargo, dado el tema de costo (presupuesto) que ésto conlleva, y el hecho de que era necesario primero crear la infraestructura para dar apoyo a la recuperación y continuidad de negocios, éste plan no se ha llevado a cabo. Se retomará éste tema, tan pronto terminemos el Proyecto de Virtualización. [*sic*] **[Apartado a.]**
>
> [...] se identificó y asignó un espacio en la Región de [...] donde será establecido el centro alterno para la restauración de

> las operaciones. Ya se adjudicó la subasta para la adquisición de los equipos necesarios (Proyecto Virtualización) y se comenzaron a realizar los trabajos relacionados los cuales se esperan estén culminados para el primer trimestre de 2013. [...] [*sic*] **[Apartado b.]**

**Véanse las recomendaciones 1, 2.b. y 6.**

**Hallazgo 4 - Deficiencias en los parámetros de contraseñas y en el proceso de eliminar las cuentas de acceso de los exempleados**

**Situaciones**

a. El examen efectuado el 17 de febrero de 2011 sobre los parámetros de contraseñas definidos en el sistema operativo del servidor principal de la red de comunicaciones del CRIM, reveló que no se habían configurado las políticas de contraseña (*Password Policy*) para establecer lo siguiente:

   1) El mínimo de caracteres requeridos para la utilización de las contraseñas (*Minimum Password Length*)

   2) El mínimo de días para que el sistema le permita al usuario cambiar la contraseña nuevamente (*Minimum Password Age*)

   3) La cantidad de veces en que la contraseña podía ser reutilizada (*Enforce Password History*)

   4) La cantidad de intentos de acceso sin éxito a los recursos de la red para que el sistema deshabilitara automáticamente las cuentas de acceso (*No account lockout*)

   5) El tiempo de acceso a la red para todas las cuentas de acceso, de acuerdo con las funciones de cada usuario (*Do not force logoff when logon hours expire*). El sistema les permitía a los usuarios tener acceso los 7 días de la semana y las 24 horas del día.

b. Al 15 de abril de 2011, permanecían activas las cuentas de acceso para acceder los sistemas del CRIM de dos exempleadas, quienes cesaron en sus funciones el 12 de noviembre de 2010 y el 28 de febrero de 2011. El tiempo transcurrido posterior a la fecha del cese de funciones de estas empleadas era 43 y 151 días.

**Criterios**

Las mejores prácticas en el campo de la tecnología de información sugieren que las entidades deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Además, sugieren que cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de tal manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Esto se instrumenta, en parte, mediante lo siguiente:

- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos.
- La notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones por motivo de renuncia, separación o traslado, para la cancelación de su cuenta de acceso.

**Efectos**

Las situaciones comentadas propician que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de esta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

**Causas**

Las situaciones comentadas en el **apartado a.** se debían, en parte, a que los funcionarios que hacían las funciones de administrador de red, no habían puesto en vigor todas las opciones de seguridad de acceso lógico que proveen los sistemas operativos ni había establecido controles para el mantenimiento de las cuentas de acceso a la red.

La situación comentada en el **apartado b.** se atribuye a la falta de comunicación efectiva entre la Oficina de Recursos Humanos y la OGSI,

para informar el cese de labores de los usuarios de los sistemas de información, de modo que sus cuentas de acceso fueran canceladas.

**Comentarios de la Gerencia**

En la carta de la Directora Ejecutiva, esta nos indicó, entre otras cosas, lo siguiente:

> [...] se repasarán las opciones de seguridad. También se está desarrollando un procedimiento para cubrir este hallazgo. El mismo tendrá la nomenclatura que debe ser utilizada para la asignación de contraseñas. Las mismas deben ser actualizadas por el usuario en un tiempo especificado y el cual será verificado por el personal de OGSI. [...] **[Apartado a.]**
>
> [...] reforzaremos la comunicación con Recursos Humanos para asegurarnos de recibir notificaciones del cese de un usuario en sus funciones para la cancelación de su cuenta de acceso, el mismo día que sea efectiva su renuncia. Se establecerá un proceso de revisión de los acceso de usuarios y de usuarios terminados, para confirmar que sean los adecuados y correctos. Esta revisión se llevará a cabo dos veces al año. **[Apartado b.]**

**Véanse las recomendaciones 1, 2.a.3) y 5.b.**

**Hallazgo 5 - Falta de normas y de procedimientos para reglamentar las operaciones de la OGSI**

**Situación**

a. Al 18 de marzo de 2011, no se habían promulgado las normas ni los procedimientos necesarios para reglamentar los siguientes procesos:

- El desarrollo o la adquisición de las aplicaciones
- La instalación y la configuración de la red de comunicaciones
- La creación y el mantenimiento de la información divulgada en la página electrónica
- La disposición de información sensitiva y de programas antes de transferir o disponer de los equipos computadorizados y de los medios de almacenamiento de información.

**Criterio**

Las mejores prácticas en el campo de la tecnología de información sugieren que se deben establecer por escrito normas, procedimientos y

políticas de control interno eficaces que reglamenten las operaciones computadorizadas y que estén aprobados por la alta gerencia. Mediante los mismos, se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en caso de renuncias o ausencias del personal de mayor experiencia, y facilita la labor de adiestramiento.

**Efectos**

La situación comentada podría ocasionar que las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias. Además, podría exponer al personal de la OGSI, a los equipos y a la información a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

**Causa**

La situación comentada obedece, principalmente, a que la Directora Ejecutiva no había requerido al Director de Sistemas de Información que desarrollara y remitiera para su consideración y aprobación, las normas y los procedimientos necesarios para reglamentar los procesos que se comentan.

**Comentarios de la Gerencia**

En la carta de la Directora Ejecutiva, esta nos indicó, entre otras cosas, lo siguiente:

> Se están desarrollado procedimientos y documentos acordes (y repasando aquellos documentos existentes), para los puntos detallados en este hallazgo. También se estarán incluyendo aquellos que surjan a causa del proceso de virtualización. Los mismos pasarán por la revisión y evaluación de Auditoría Interna. Al finalizar ésta tarea, OGSI contará con las guías para establecer los controles adecuados y necesarios, para una eficiente y adecuada administración de los sistemas. [*sic*]

**Véanse las recomendaciones 1 y 2.c.**

**Hallazgo 6 - Falta de diagramas esquemáticos de las oficinas regionales**

**Situación**

a. Al 6 de mayo de 2010, la OGSI no contaba con los diagramas esquemáticos aprobados donde se incluyeran los equipos que componen la infraestructura de la red de comunicaciones de las oficinas regionales del CRIM.

**Criterio**

Las mejores prácticas en el campo de tecnología de información sugieren que las entidades adquieran, desarrollen e implanten una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientemente. Además, incluyen como práctica que el diseño de la red debe estar documentado con diagramas esquemáticos de las redes.

**Efectos**

La situación comentada impide al CRIM tener una comprensión clara y precisa sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento a la misma. Además, dificulta la atención de problemas en un tiempo razonable y que se planifiquen efectivamente las mejoras a la red.

**Causa**

La situación comentada se debía, en parte, a que el Director de Sistemas de Información entendía que los planos de planta de las oficinas regionales del CRIM eran diagramas esquemáticos.

**Comentarios de la Gerencia**

En la carta de la Directora Ejecutiva, esta nos indicó, entre otras cosas, lo siguiente:

> A pesar de que se hizo entrega de diagramas para la Oficina Central y las diferentes Oficinas Regionales con los planos de ubicación de la infraestructura, los mismos no cumplían con las especificaciones sobre esquemas. Por lo cual se estará

coordinando para preparar los diagramas esquemáticos de todas las oficinas del CRIM, una vez culminado el proceso de virtualización. [*sic*]

**Véanse las recomendaciones 1 y 2.d.**

**RECOMENDACIONES**

**A la Junta de Gobierno del Centro de Recaudación de Ingresos Municipales**

1. Ver que la Directora Ejecutiva cumpla con las **recomendaciones de la 2 a la 6** de este *Informe*. **[Hallazgos del 1 al 6]**

**A la Directora Ejecutiva del Centro de Recaudación de Ingresos Municipales**

2. Ejercer una supervisión efectiva sobre el Director de Sistemas de Información para asegurarse de que:

   a. Imparta instrucciones al personal que realiza las funciones de administrador de la red, para que:

      1) Realice inspecciones periódicas para verificar el uso adecuado de las cuentas de acceso a Internet. **[Hallazgo 1]**

      2) Limite el acceso a las páginas electrónicas para que sólo se pueda acceder aquellas que son necesarias para cumplir con los deberes y las responsabilidades del personal autorizado. **[Hallazgo 1]**

      3) Configure los parámetros de contraseñas que provee el sistema operativo para:

         a) Requerir un mínimo de caracteres para la utilización de las contraseñas. **[Hallazgo 4-a.1)]**

         b) Requerir un mínimo de días para que el sistema le permita al usuario cambiar la contraseña nuevamente. **[Hallazgo 4-a.2)]**

         c) Restringir que los usuarios puedan repetir las últimas cinco contraseñas utilizadas previamente. **[Hallazgo 4-a.3)]**

d) Desconectar automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la red. **[Hallazgo 4-a.4)]**

e) Restringir el horario de acceso a los recursos de la red, según las funciones y las responsabilidades de cada usuario, y activar la opción para desconectar automáticamente las cuentas de acceso cuando estas son utilizadas para acceder a los recursos de la red fuera del horario de acceso autorizado. **[Hallazgo 4-a.5)]**

b. Realice las gestiones para habilitar, con la infraestructura y los equipos necesarios, las instalaciones identificadas por el CRIM para utilizarse como centro alterno. **[Hallazgo 3-b.]**

c. Prepare y remita para su aprobación las normas y los procedimientos necesarios para reglamentar los procesos de sistemas de información comentados en el **Hallazgo 5**. Una vez aprobados, se asegure de que se mantengan actualizados y se cumpla con los mismos.

d. Remita para su aprobación los diagramas esquemáticos en los que se incluyan los equipos que componen la infraestructura de la red de comunicaciones, incluidos los asignados a las oficinas regionales del CRIM. **[Hallazgo 6]**

3. Asegurarse de que se realice y se documente el análisis de riesgos de los sistemas de información computadorizados, según se sugiere en las mejores prácticas en el campo de la tecnología de información. El informe producto de este análisis de riesgos debe ser remitido para su revisión y aprobación. **[Hallazgo 2-a.]**

4. Realizar las gestiones necesarias para que el CRIM cuente con un plan de seguridad que incluya los criterios descritos en el

**Hallazgo 2-b.** Además, asegurarse de que se realicen pruebas periódicas al plan de seguridad, y que el mismo se divulgue a los empleados y a los funcionarios.

5. Ejercer una supervisión eficaz sobre el Director de Recursos Humanos para asegurarse de que:

   a. Se preparen acuerdos de confidencialidad escritos, dirigidos a los empleados y a los contratistas que trabajan con datos confidenciales y activos sensitivos. Estos acuerdos deben establecer el período de no divulgación posterior a la fecha de terminación del empleo. **[Hallazgo 2-c.]**

   b. Se informe prontamente a la OGSI el cese de los empleados para la cancelación de sus cuentas de acceso. **[Hallazgo 4-b.]**

6. Realizar las gestiones para asegurarse de que se prepare un plan de continuidad de negocios, que incluya un plan para la recuperación de desastres y un plan para la continuidad de las operaciones. Este plan debe ser remitido para su revisión y aprobación. 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 del CRIM. Además, asegurarse de que sea distribuido a los funcionarios y empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 3-a.]**

**AGRADECIMIENTO**

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

Oficina del Contralor

Por: Yazmín M. Valdivieso

**ANEJO 1**

CENTRO DE RECAUDACIÓN DE INGRESOS MUNICIPALES
OFICINA DE GERENCIA DE SISTEMAS DE INFORMACIÓN
**MIEMBROS PRINCIPALES DE LA JUNTA DE GOBIERNO**
**DURANTE EL PERÍODO AUDITADO**

| NOMBRE | CARGO O PUESTO | PERÍODO | |
|---|---|---|---|
| | | DESDE | HASTA |
| Hon. Javier D. Jiménez Pérez | Presidente | 17 nov. 10 | 13 may. 11 |
| Hon. Jesús E. Colón Berlingeri | Vicepresidente | 17 nov. 10 | 13 may. 11 |
| Sr. Roberto Hernández Vélez | Secretario | 17 nov. 10 | 13 may. 11 |

**ANEJO 2**

CENTRO DE RECAUDACIÓN DE INGRESOS MUNICIPALES
OFICINA DE GERENCIA DE SISTEMAS DE INFORMACIÓN
**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD**
**DURANTE EL PERÍODO AUDITADO**

| NOMBRE | CARGO O PUESTO | PERÍODO | |
|---|---|---|---|
| | | DESDE | HASTA |
| Lcda. Gloria E. Santos Rosado, CPA | Directora Ejecutiva | 17 nov. 10 | 13 may. 11 |
| Sr. Gustavo A. Freyre Conde | Subdirector Ejecutivo de Operaciones | 17 nov. 10 | 13 may. 11 |
| Sr. Raúl A. Cruz Franqui | Director de Sistemas de Información | 17 nov. 10 | 13 may. 11 |
| Lcdo. Eliezer Ramos Parés | Director de Recursos Humanos | 17 nov. 10 | 13 may. 11 |
| Sr. Edwin M. Quiles Méndez | Director de Servicios Administrativos | 17 nov. 10 | 13 may. 11 |
| CPA Gricelis Acevedo Román | Directora de Auditoría Interna | 17 nov. 10 | 13 may. 11 |

## 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 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.

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) 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

*Dirección postal:*

PO Box 366069

San Juan, Puerto Rico 00936-6069

*Internet:*

http://www.ocpr.gov.pr

*Correo electrónico:*

ocpr@ocpr.gov.pr