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 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 Leyes

#863

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

17 de junio 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-13-20* de la Oficina de Sistemas de Información de la Oficina de Asuntos de la Juventud, adscrita a la Oficina del Gobernador, aprobado por esta Oficina el 5 de junio 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

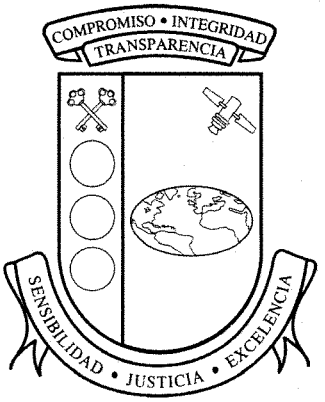
Anejo

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

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

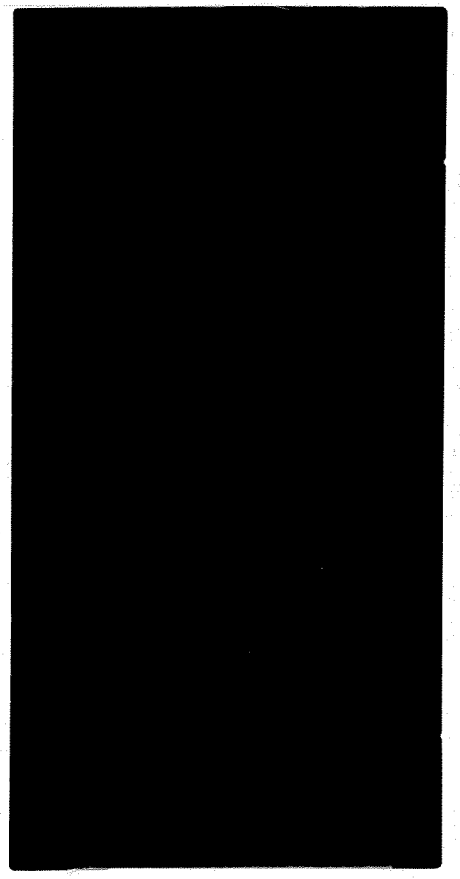
629

#863



[redacted]

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



INFORME DE AUDITORÍA TI-13-20

5 de junio de 2013

Oficina del Gobernador

Oficina de Asuntos de la Juventud

Oficina de Sistemas de Información

(Unidad 5372 - Auditoría 13545)

Período auditado: 29 de noviembre de 2010 al 15 de junio 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 4

1 - Falta de estudio de viabilidad, de solicitud de propuestas por escrito y de información en el Plan Anual de Administración de Recursos Tecnológicos para el otorgamiento de un contrato para la implantación de un sistema financiero y de sistemas computadorizados para los programas de Juvempleo y Sorteo de Viajes Estudiantiles, y otra deficiencia relacionada 5

2 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados 9

3 - Falta de un plan de seguridad 11

4 - Deficiencias relacionadas con el Plan de Contingencias, y falta de pruebas o simulacros para certificar la efectividad del Plan, de almacenamiento de los respaldos y de documentación fuera de la OAJ, y de un centro alterno de recuperación de los sistemas de información 12

5 - Falta de un registro de programas instalados en los servidores y en las computadoras portátiles, y de documentación para la implantación y las actualizaciones de la red y del sistema operativo 16

6 - Falta de producción de un registro de auditoría sobre las transacciones registradas en la aplicación Programa Sorteo Viajes Estudiantiles y deficiencia relacionada con la documentación de dicha aplicación 18

7 - Falta de un formulario para la creación, la modificación y la cancelación de las cuentas de acceso 20

8 - Falta de activación de las políticas de auditoría en el servidor principal de la OAJ 21

9 - Falta de un programa para divulgar al personal las normas y los procedimientos de seguridad de la información 23

RECOMENDACIONES 25

AGRADECIMIENTO 28

ANEJO - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO 29

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

5 de junio 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 Sistemas de Información (OSI) de la Oficina de Asuntos de la Juventud (OAJ), adscrita a la Oficina del Gobernador, para determinar si las mismas se efectuaron 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 29 de noviembre de 2010 al 15 de junio 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 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 confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este *Informe* contiene nueve hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, la configuración de los sistemas de información, el control de acceso lógico y físico, la continuidad del servicio, el desarrollo

y el control de los cambios de las aplicaciones, y la evaluación de los contratos de servicios profesionales. El *Informe* está disponible en nuestra página en Internet: http://www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La OAJ fue creada en virtud de la *Ley Núm. 34 del 13 de julio de 1978, Ley de la Oficina de Asuntos de la Juventud*, según enmendada[1] y está adscrita a la Oficina del Gobernador.

Las operaciones de la OAJ son administradas por un Director Ejecutivo nombrado por el Gobernador de Puerto Rico, con el consejo y el consentimiento del Senado de Puerto Rico. Esta es responsable, entre otras cosas, de implantar las siguientes funciones y encomiendas establecidas en la *Ley Núm. 34*, tales como: preparar con prioridad y en coordinación con las agencias de gobierno concernientes, organizaciones y sector privado, un programa eficaz para proveerle trabajo y otras oportunidades de desarrollo a los jóvenes desempleados entre las edades de 16 a 29 años; y establecer, con la participación y en coordinación con el Departamento del Trabajo y Recursos Humanos, mecanismos para la selección y el referimiento de jóvenes para empleo, en el sector público o en el sector privado. Además, esta es responsable de examinar los programas gubernamentales para determinar el impacto y la efectividad de los mismos en la atención y la solución de los problemas de la juventud, y recomendar acciones correctivas; desarrollar actividades, participar en foros, y establecer mecanismos y procedimientos para garantizar los derechos de la juventud y lograr su participación plena en la vida de nuestro Pueblo; promover el establecimiento de organizaciones juveniles; y ofrecer incentivos, ayuda y estímulo a los jóvenes directamente y a las entidades privadas que presten servicios a la juventud, y promover el desarrollo de las mismas.

A la fecha de nuestra auditoría, la OSI contaba con un Director de Programa que fungía como Director de la OSI y un Auxiliar de Sistemas de Información.

[1] Mediante la *Ley 85-2005* que enmendó la *Ley Núm. 34*, se eliminó el Consejo Asesor. Las funciones y los poderes que tenía el Consejo Asesor fueron asignadas a la OAJ y a su Director Ejecutivo.

Los gastos operacionales de la OSI eran sufragados del presupuesto operacional de la OAJ, que para los años fiscales 2008-09, 2009-10 y 2010-11 ascendió a $11,711,000, $9,195,000 y $7,229,000, respectivamente.

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

La OAJ cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.oaj.pr.gov. 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 Sr. Héctor O'Neill Rosa, entonces Director Ejecutivo de la OAJ, mediante cartas de nuestros auditores, del 10 de junio y del 12 de julio de 2011. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

El entonces Director Ejecutivo de la OAJ no contestó las cartas de nuestros auditores ni la carta de seguimiento del 15 de julio de 2011.

El borrador de los **hallazgos** de este *Informe* se remitió al entonces Director Ejecutivo de la OAJ para comentarios, por carta del 27 de noviembre de 2012.

El 7 de diciembre de 2012 la Lcda. Yomarie Cardona Cosme, entones Subdirectora Ejecutiva de la OAJ, solicitó una prórroga para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. El 10 de diciembre de 2012 le concedimos la prórroga al entones Director Ejecutivo hasta el 8 de enero de 2013.

El entonces Director Ejecutivo de la OAJ contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 21 de diciembre de 2012. 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 revelaron que las operaciones de la OSI en lo que concierne a los controles internos establecidos para la administración del

programa de seguridad, la configuración de los sistemas de información, el control de acceso lógico y físico, la segregación de deberes, la continuidad del servicio, el desarrollo y el control de los cambios de las aplicaciones, la evaluación de los contratos de servicios profesionales y consultivos y la participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 9** que se comentan a continuación.

Hallazgo 1 - Falta de estudio de viabilidad, de solicitud de propuestas por escrito y de información en el Plan Anual de Administración de Recursos Tecnológicos para el otorgamiento de un contrato para la implantación de un sistema financiero y de sistemas computadorizados para los programas de Juvempleo y Sorteo de Viajes Estudiantiles, y otra deficiencia relacionada

Situaciones

a. El 18 de junio de 2010 la OAJ otorgó el Contrato 2010-000041 por $344,081 a una compañía para el desarrollo, la implantación, el adiestramiento y el uso de sistemas computadorizados para los programas de Juvempleo y Sorteo de Viajes Estudiantiles, y un sistema financiero. El contrato tenía vigencia del 18 de junio al 31 de diciembre de 2010. El 29 de diciembre de 2010 y el 28 de febrero de 2011 la OAJ efectuó dos enmiendas a dicho Contrato para extender la vigencia hasta el 28 de febrero y el 30 de mayo de 2011. En el contrato se estimaron 1,912 horas distribuidas por fases para los sistemas computadorizados y 1,156 horas para el sistema financiero.

   El examen realizado del otorgamiento, la administración y los desembolsos del Contrato reveló lo siguiente:

   1) La OAJ no preparó un estudio de viabilidad en el que se evaluaran los beneficios y los costos asociados a cada una de las soluciones potenciales, así como el rendimiento en la inversión de cada solución.

2) La OAJ no preparó una solicitud de propuestas por escrito con especificaciones claras y detalladas de los servicios a ser contratados. El Director Ejecutivo y el Subdirector de la OAJ le solicitaron verbalmente propuestas a tres compañías. El Director Ejecutivo nos certificó que las propuestas fueron evaluadas por un grupo de trabajo compuesto por este, el entonces Subdirector de Área y el Director de la OSI. No se nos suministró evidencia de la evaluación de las propuestas que realizó este grupo de trabajo.

3) La OAJ no incluyó la información sobre la adquisición y la implantación de los mencionados sistemas en el *Plan Anual de Administración de Recursos Tecnológicos (PAART)*, preparado para el año fiscal 2009-10, y remitido para evaluación a la Oficina de Gerencia y Presupuesto (OGP). Además, el 2 de febrero de 2011 el Director de la OSI nos certificó que no preparó el *PAART* correspondiente al año fiscal 2010-11.

4) De junio de 2010 a junio de 2011, la Compañía presentó 10 facturas, con sus correspondientes informes, de los servicios rendidos relacionados con los sistemas para los programas de Juvempleo y Sorteo de Viajes Estudiantiles. En cada factura se incluía el total de horas trabajadas por empleado y el importe total, y en los informes se indicaba la descripción de las tareas realizadas por cada empleado, la fecha en que se realizaron y las horas invertidas. Sin embargo, en ninguno de los documentos se especificaba a qué fase pertenecían las horas facturadas, según el desglose establecido en el Contrato.

Criterios

Las mejores prácticas utilizadas para la adquisición de sistemas de información computadorizados sugieren que antes de contratar o de invertir recursos para el desarrollo de proyectos de sistemas de información es necesario realizar un estudio de viabilidad para determinar si la inversión propuesta en el desarrollo o adquisición está de acuerdo con las metas y los objetivos de la entidad. La documentación

desarrollada durante el transcurso del estudio se utilizará para preparar las especificaciones de los sistemas y la solicitud de propuestas. **[Apartado a.1) y 2)]**

La falta de evidencia de la evaluación de las propuestas se aparta de lo establecido en el *Reglamento 23, Para la Conservación de Documentos de Naturaleza Fiscal o Necesarios para el Examen y Comprobación de Cuentas y Operaciones Fiscales*, aprobado el 15 de agosto de 1988 por el Secretario de Hacienda y en el Artículo 18 del *Reglamento 4284, Reglamento para la Administración de Documentos Públicos en la Rama Ejecutiva*, emitido el 19 de julio de 1990 por el Administrador de Servicios Generales, según enmendados.

La situación comentada en el **apartado a.3)** es contraria a lo establecido en la *Política TIG-001, Plan Anual de Administración de Recursos Tecnológicos, PAART* 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 OGP.

La situación comentada en el **apartado a.4)** se aparta de lo establecido en el Artículo 2(g) de la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada, y en la Sexta Cláusula del Contrato 2010-000041. En dicha cláusula se establece que la cuantía máxima a pagar al contratista no excederá de $344,081 durante la vigencia del Contrato los cuales serán pagados conforme a la distribución de fases incluida en el mismo.

Efectos

Las situaciones comentadas en el **apartado a. del 1) al 3)** impidieron a la OAJ identificar todos los requerimientos y las especificaciones para el desarrollo de sistemas que automatizaran sus operaciones. Además, propiciaron que no se establecieran criterios para evaluar distintos sistemas de mecanización y automatización, y, a su vez, promover una libre competencia entre proveedores potenciales de soluciones similares para así

obtener mejores precios. También impidió a la OAJ obtener el asesoramiento y la aprobación de la OGP para este proyecto previo al otorgamiento del mencionado Contrato.

La situación comentada en el **apartado a.4)** impidió a la OAJ mantener un control efectivo sobre los servicios contratados y del tiempo para culminar cada fase establecida en el Contrato. Además, impidió a nuestros auditores verificar la corrección de los pagos efectuados.

Causas

Las situaciones comentadas en el **apartado a. del 1) al 3)** se atribuyen a que el Director Ejecutivo no cumplió con las disposiciones reglamentarias ni tomó las medidas necesarias para proteger adecuadamente los mejores intereses de la OAJ.

La situación comentada en el **apartado a.4)** se atribuye a la falta de planificación y de supervisión adecuada en la administración del Contrato.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este indicó, entre otras cosas, lo siguiente:

> [...] al momento de solicitar las propuestas a los tres proveedores de servicio, como requiere la Ley, la Agencia contaba con las especificaciones y requerimientos para la adquisición del nuevo sistema. [*sic*] **[Apartado a.1)]**
>
> Conforme a las especificaciones establecidas se evaluaron las propuestas por el Director de la OSI, el Subdirector de área y el Director Ejecutivo. [*sic*] **[Apartado a.2)]**
>
> [...] aunque no se incluyó en el Plan Anual (PAART) [...] esta acción se le comunicó a la OGP antes de comenzar todo el proceso. **[Apartado a.3)]**
>
> El proceso de implementar el nuevo sistema para los Programas de Juvempleo y Sorteo de Viajes Estudiantiles fue uno rigurosamente revisado por los funcionarios de la Agencia a los fines de que se cumpliera con las especificaciones requeridas y establecidas en el contrato. Dichos informes fueron validados por los funcionarios a cargo de revisar la implantación del nuevo sistema y los mismos eran bien detallados. **[Apartado a.4)]**

Consideramos las alegaciones del entonces Director Ejecutivo, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que en la contestación no suministró evidencia de las especificaciones y los requerimientos para los sistemas computadorizados ni de la evaluación que realizaron de las propuestas remitidas por las compañías. Tampoco incluyeron evidencia de la comunicación que tuvieron con la OGP sobre la adquisición y la implantación de los mencionados sistemas. Además, con respecto al **apartado a.4)**, no suministraron documentos adicionales a los examinados durante nuestro examen.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados

Situación

a. Un análisis de riesgos de los sistemas de información 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 que 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.

> Al 2 de febrero de 2011, en la OAJ no se había preparado un informe escrito de análisis de riesgos de los sistemas de información computadorizados.

Criterio

Esta situación es contraria a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular 77-05*.

Efectos

La situación comentada impide a la OAJ estimar el impacto que los elementos de riesgos 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. Además, impide el desarrollo de 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 OAJ en caso de que surja alguna eventualidad.

Causa

La situación comentada se atribuye a que el Director Ejecutivo en funciones de la OAJ no había promulgado una directriz para la preparación del análisis de riesgos de los sistemas de información, como se establece en la *Carta Circular 77-05*.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este nos indicó, lo siguiente:

> Se le impartieron instrucciones al Director de la OSI a los fines de preparar un análisis de riesgos de los sistemas de información a tono con lo establecido en la Carta Circular Núm. 77-05.

Véase la Recomendación 3.

Hallazgo 3 - Falta de un plan de seguridad

Situación

a. Al 7 de febrero de 2011, la OAJ no tenía un plan de seguridad aprobado por el Director Ejecutivo, que incluyera, entre otras cosas, disposiciones en cuanto a:

- La documentación de la validación de las normas de seguridad[2]
- La evidencia de un análisis de riesgos actualizado, que sea la base del plan de seguridad
- La responsabilidad de la gerencia y de los demás componentes de la unidad
- 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)
- La documentación de la interconexión de los sistemas.

Criterio

La situación comentada se aparta de lo establecido en la *Política TIG-003* de la *Carta Circular 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.

---

[2] La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las 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.

Causa

La situación comentada se atribuye a que el Director Ejecutivo en funciones no había promulgado una directriz para la preparación de un plan de seguridad, basado en un análisis de riesgos de los sistemas de información, y la implantación y la actualización continua del mismo.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este nos indicó, lo siguiente:

> Se comenzó a trabajar con el Plan de Seguridad a tono con la Política Núm. TIG-003 de la Carta Circular Núm. 77-05.

Véase la Recomendación 4.

Hallazgo 4 - Deficiencias relacionadas con el Plan de Contingencias, y falta de pruebas o simulacros para certificar la efectividad del Plan, de almacenamiento de los respaldos y de documentación fuera de la OAJ, y de un centro alterno de recuperación de los sistemas de información

Situaciones

a. El *Plan de Contingencia y Recuperación de Desastres* (*Plan*), aprobado el 30 de septiembre de 2008 por el Director Ejecutivo y la Directora de la OSI, no incluía los siguientes requisitos para atender situaciones de emergencia:

   - Los procedimientos a seguir cuando el cuarto de los servidores no puede recibir ni transmitir información
   - Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar
   - Una hoja de cotejo para verificar los daños ocasionados por la contingencia
   - Una lista de los proveedores principales, que incluya el número de teléfono y el nombre del personal de enlace con la entidad.

b. Al 23 de febrero de 2011, el *Plan* incluía la siguiente información que no estaba actualizada:

   - La localización de la OAJ

- El nombre del Director Ejecutivo, el cual era el encargado de activar el *Plan*
- La lista de los miembros de cada grupo de recuperación con sus números de teléfono
- El inventario de los equipos, de los sistemas operativos y de las aplicaciones
- El diagrama esquemático y las especificaciones de la red de la OAJ
- El detalle de la configuración de los equipos críticos (equipos de comunicaciones y servidores) y del contenido de los respaldos, así como los nombres de librerías y de los archivos
- La lista de los usuarios de la OAJ.

c. La OSI no había efectuado pruebas o simulacros para certificar la efectividad del *Plan*.

d. No se mantenía una copia del *Plan*, de los respaldos (*backups*) diarios y mensuales de la información de los sistemas computadorizados, ni de la documentación de las configuraciones de los sistemas, de las aplicaciones y de los programas críticos, en un lugar seguro fuera de las instalaciones de la OAJ.

e. La OAJ no contaba con un centro alterno para restaurar sus operaciones críticas computadorizadas en caso de emergencia. Tampoco había formalizado acuerdos escritos con otra entidad para establecer un centro alterno en las instalaciones de esta.

Situaciones similares a las indicadas en los **apartados b. y e.** se comentaron en el *Informe de Auditoría CPED-96-16* del 30 de junio de 1996.

Criterios

Las mejores prácticas en el campo de la tecnología de información 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 prepare 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 que afectan su funcionamiento. El mismo deberá revisarse periódicamente y estar aprobado por el funcionario de máxima autoridad de la entidad, y deberá incluir todos los procesos necesarios para recuperar cualquier segmento de las operaciones computadorizadas o, si fuera necesario, relocalizar dichas operaciones en el menor tiempo posible y de la forma más ordenada y confiable. **[Apartados a. y b.]** Además, se deberán efectuar pruebas o simulacros, por lo menos una vez al año, para comprobar la efectividad del *Plan*. **[Apartado c.]**

Como norma de sana administración y de control interno, se requiere que las entidades gubernamentales mantengan una copia actualizada del *Plan* y de la documentación de las configuraciones de los sistemas, de las aplicaciones y de los programas críticos, en un lugar seguro fuera del edificio donde radica el centro. Esto es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado. **[Apartado d.]**

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 con otras entidades 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 e.]**

- 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

Las situaciones comentadas en los **apartados del a. al c.** podrían propiciar la improvisación y, que en casos de emergencia, se tomen medidas

inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos y de interrupciones prolongadas de los servicios a los usuarios de la OAJ.

La situación comentada en el **apartado d.** podría ocasionar que, de ocurrir una emergencia que impida entrar a las instalaciones de la OAJ, el encargado de activar el *Plan* no pueda disponer de la documentación y de los respaldos de información necesarios para iniciar el proceso de reconstrucción de archivos y programas, y el restablecimiento y la continuidad de las operaciones computadorizadas en un tiempo razonable.

La situación comentada en el **apartado e.** podría afectar las funciones de la OAJ y los servicios de la OSI, 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 OSI.

Causas

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a la falta de un análisis de riesgos de los sistemas de información computadorizados de la OAJ que sirviera de base para la preparación y la revisión del *Plan*. **[Hallazgo 2]**

La situación comentada en el **apartado c.** se atribuye a que el Director Ejecutivo no veló ni le requirió al Director de la OSI que efectuara las pruebas al *Plan* para asegurarse de que este era funcional y consideraba las necesidades y los riesgos de la OAJ.

La situación comentada en el **apartado d.** se debía a que el Director de la OSI no había efectuado las gestiones necesarias para mantener copia del *Plan*, de los respaldos (*backups*) diarios y mensuales de la información de los sistemas computadorizados, y de la documentación de las configuraciones de los sistemas, de las aplicaciones y de los programas críticos, en un lugar seguro fuera de los predios de la OAJ.

La situación comentada en el **apartado e.** se atribuye a que el Director Ejecutivo en funciones de la OAJ no había coordinado con el Director de

la OSI la identificación de un lugar disponible y adecuado como centro alterno para restaurar las operaciones computadorizadas críticas de la OAJ en casos de emergencias.

Comentarios de la Gerencia

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

> Se impartieron instrucciones a los fines de incluir sus recomendaciones en el Plan de Contingencia y Recuperación de Desastres. **[Apartado a.]**
>
> Se impartieron instrucciones a los fines de actualizar la información requerida en el Plan. **[Apartado b.]**
>
> Se comenzaron a realizar las pruebas y/o simulacros requeridos por el Plan. [*sic*] **[Apartado c.]**
>
> Se comenzaron a evaluar alternativas viables para la Agencia a los fines de mantener los resguardos en un lugar seguro fuera de la misma. [*sic*] **[Apartado d.]**
>
> Se comenzó con la evaluación de alternativas viables para establecer el centro alterno. **[Apartado e.]**

Véanse las recomendaciones 5 de la a. a la c., y 6.

Hallazgo 5 - Falta de un registro de programas instalados en los servidores y en las computadoras portátiles, y de documentación para la implantación y las actualizaciones de la red y del sistema operativo

Situaciones

a. Al 23 de febrero de 2011, en la OSI no se mantenía un registro de los programas adquiridos e instalados en los servidores y en las computadoras portátiles de la OAJ que incluyera, entre otras cosas, lo siguiente:

   - El número de licencia de los programas instalados
   - El nombre del usuario
   - El número de propiedad y la descripción de la computadora donde estaban instalados los programas
   - El costo de los programas.

b. Al 2 de febrero de 2011, en la OSI no se mantenía la documentación sobre la implantación y las actualizaciones de la red y del sistema operativo.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en la *Política TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de la *Carta Circular 77-05*. En consonancia con dicha *Política*, el registro de los programas debe contener lo siguiente: el número de la licencia, el nombre del proveedor, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el equipo donde está instalado (número de propiedad o de serie), la ubicación física de la licencia, los disquetes y los manuales, el nombre del usuario, el número de propiedad asignado, la lista de inventario (licencia, disquetes, manuales, equipo) y el costo.

La situación comentada en el **apartado b.** se aparta de lo establecido en la *Política TIG-011, Mejores Prácticas de Infraestructura Tecnológica* de la *Carta Circular 77-05*.

Efectos

La situación comentada en el **apartado a.** impide ejercer un control eficaz de los programas y de las licencias de estos. Además, propicia la instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para la OAJ. También dificulta nuestra gestión fiscalizadora.

La situación comentada en el **apartado b.** impide a la OAJ controlar, administrar y efectuar un mantenimiento rápido, eficiente y efectivo de los equipos que componen su red. Además, dificulta atender los problemas de conexión en un tiempo razonable y efectuar una planificación efectiva para realizar mejoras a la red, según el crecimiento de sus sistemas.

Causas

La situación comentada en el **apartado a.** se debía a que el Director de la OSI no había tomado las medidas necesarias para mantener un registro y un control adecuado de los programas adquiridos e instalados en los servidores y en las computadoras portátiles de la OAJ.

La situación comentada en el **apartado b.** se atribuye a que el Director de la OSI no preparó la documentación de implantación y de las actualizaciones de la red y del sistema operativo.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este nos indicó, lo siguiente:

> Se le impartió instrucciones al Director de la OSI a los fines de preparar y mantener un registro de los programas adquiridos e instalados en los servidores y en las computadoras portátiles. [*sic*] **[Apartado a.]**
>
> Se le impartió instrucciones al Director de la OSI a los fines de preparar la documentación de implantación y actualizaciones de la red y el sistema operativo. [*sic*] **[Apartado b.]**

Véase la Recomendación 5.d. y e.1).

Hallazgo 6 - Falta de producción de un registro de auditoría sobre las transacciones registradas en la aplicación Programa Sorteo Viajes Estudiantiles y deficiencia relacionada con la documentación de dicha aplicación

Situaciones

a. El Programa Sorteo de Viajes Estudiantiles fue creado en virtud de la *Ley Núm. 32 del 23 de junio de 1985*. Dicho programa le ofrece a estudiantes de escuela superior la oportunidad de viajar dentro y fuera de Puerto Rico, con el propósito de ampliar sus horizontes, conocimiento cultural, económico, político y social, y, a su vez, servir de embajadores de nuestras manifestaciones culturales. La OAJ desarrolló la aplicación Programa Sorteo Viajes Estudiantiles (Aplicación) para computadorizar los siguientes procesos relacionados con el registro y el control del sorteo: el almacenamiento de la información de los participantes en una base de datos, la

corrección de los datos de los participantes y los viajeros, el registro de los bolos del sorteo que resultaron ganadores, y el mantenimiento de un registro histórico de los ganadores, entre otros.

El examen realizado reveló que, al 23 de febrero de 2011, no se producía un registro de auditoría de las transacciones realizadas en la Aplicación que permitiera efectuar revisiones periódicas para propósitos de control.

b. La documentación de la Aplicación mantenida en la OSI de la OAJ incluía lo siguiente:

- *Programa Sorteo Viajes Estudiantiles - Manual Técnico*
- *Programa Sorteo Viajes Estudiantiles - Manual de Usuario*

El examen de la documentación efectuado el 23 de febrero de 2011, reveló que esta no contenía el diagrama de flujo sobre el procesamiento de los datos ni el diccionario de datos.

Una situación similar se comentó en el *Informe de Auditoría CPED-96-16*.

Criterios

La situación comentada en el **apartado a.** se aparta de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

La situación comentada en el **apartado b.** es contraria a lo establecido en la *Política TIG-011* de la *Carta Circular 77-05*. Esta política se instrumenta, en parte, mediante el desarrollo y la actualización de la documentación de los sistemas.

Efectos

La situación comentada en el **apartado a.** priva a los supervisores y auditores de una herramienta necesaria para detectar el uso indebido de la Aplicación o la alteración de datos en los registros de estudiantes. Además, dificulta fijar responsabilidades en los casos que procedan.

La situación comentada en el **apartado b.** podría ocasionar dificultades a los técnicos, usuarios, auditores y consultores externos para entender el funcionamiento de los procesos y los controles de la Aplicación. Además, podría ocasionar que el personal de la OSI utilizara su propio criterio para realizar los trabajos relacionados con el mantenimiento de la Aplicación; y la comisión de faltas, errores e irregularidades durante el registro de la información, y el procesamiento y la salida de los datos.

Causas

La situación comentada en el **apartado a.** se debía a que el Director de la OSI no había efectuado gestiones para mejorar el diseño del módulo de seguridad de la Aplicación que incluyera el registro de auditoría.

La situación comentada en el **apartado b.** se debía a que el Director de la OSI no había implantado las medidas para que la documentación de la Aplicación se mantuviera completa y actualizada.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este nos indicó, lo siguiente:

> Se impartió instrucciones al Director de la OSI a los fines de que las situaciones comentadas en los apartados a y b no se repitan. [*sic*]

Véase la Recomendación 5.e.2) y f.

Hallazgo 7 - Falta de un formulario para la creación, la modificación y la cancelación de las cuentas de acceso

Situación

a. La OAJ no había establecido un formulario para la solicitud, la aprobación, la creación, la modificación y la cancelación de las cuentas de acceso de los usuarios para acceder a la red de la OAJ, a las aplicaciones, al correo electrónico y a Internet. Las solicitudes se realizaban mediante comunicación verbal o por correo electrónico al Director de la OSI.

Criterio

La situación comentada se aparta de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

Efectos

La situación comentada impide mantener la evidencia requerida de las autorizaciones para otorgar, modificar o cancelar los accesos y los privilegios a los usuarios. Esto puede dificultar que se fijen responsabilidades por el uso indebido de los sistemas computadorizados. Además, puede afectar la integridad de la información registrada en estos.

Causa

Esta situación se debía a que el Director Ejecutivo no le había requerido al Director de la OSI que desarrollara y remitiera para su aprobación las normas y los procedimientos para la administración y el control de las cuentas de acceso a la red de la OAJ, al correo electrónico y a Internet, que incluyeran, entre otras cosas, las directrices para 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 para acceder a estos.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este nos indicó, lo siguiente:

> Se instruyó al Director de la OSI a que prepare y establezca un formulario para la solicitud, aprobación, creación, modificación y cancelación de las cuentas de acceso de los usuarios para acceder a la red de la OAJ. [*sic*]

Véase la Recomendación 5.g.

Hallazgo 8 - Falta de activación de las políticas de auditoría en el servidor principal de la OAJ

Situación

a. El sistema operativo del servidor principal[3] proveía las opciones para configurar la política de auditoría (*Audit Policy*) que permitía producir registros sobre los eventos relacionados con los accesos a los sistemas de información y los cambios en las políticas de seguridad establecidas. El examen efectuado el 14 de febrero de 2011 reveló que el Director de la OSI no había evaluado la política de auditoría

[3] El nombre del servidor se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al entonces Director Ejecutivo para comentarios.

provista por el sistema para determinar la necesidad de activar aquellas opciones que producen registros cuando ocurren los siguientes eventos:

- Las solicitudes al servidor para validar una cuenta de usuario (*Audit account logon events*)
- La creación, la modificación, o la eliminación de una cuenta o grupo de usuarios, el cambio de nombre o contraseña y la activación o desactivación de una cuenta o grupo de usuarios (*Audit account management*)
- El acceso a un objeto del *Active Directory* (*Audit directory service access*)
- La conexión o desconexión de una cuenta de acceso a una computadora conectada a la red (*Audit logon events*)
- Los accesos a los archivos, a los fólders y a las impresoras (*Audit object access*)
- Los cambios efectuados a las opciones de seguridad, a los privilegios de usuarios y a las políticas de auditoría (*Audit policy change*)
- El uso de los privilegios de los usuarios (*Audit priviledge use*)
- Las acciones ejecutadas por algún programa (*Audit process tracking*)
- El apagado, el reinicio de la computadora, y los eventos que afectan al sistema de seguridad (*Audit system events*).

Criterio

La situación comentada es contraria a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. Esta norma se instrumenta, en parte, mediante la activación de las opciones para registrar los eventos de seguridad, de las aplicaciones y del sistema.

Efectos

Las situaciones comentadas impiden la detección temprana de errores críticos o problemas con los servidores, que permitan tomar de inmediato las medidas preventivas y correctivas necesarias. Además, privan a la gerencia de las herramientas necesarias para supervisar eficientemente los trabajos realizados por los usuarios, y detectar el acceso y el uso indebido de los sistemas computadorizados.

Causa

Las situaciones comentadas se debían, en parte, a que el Director Ejecutivo en funciones no se había asegurado de que el Director de la OSI evaluara las opciones de seguridad disponibles en los sistemas operativos, para que active las opciones de seguridad necesarias para mitigar los riesgos y las amenazas existentes.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este nos indicó, lo siguiente:

> Se le impartieron instrucciones al Director de la OSI y al Auditor Interno a los fines de evaluar periódicamente la política de auditoría provista por el sistema operativo. [*sic*]

Véase la Recomendación 5.h.

Hallazgo 9 - Falta de un programa para divulgar al personal las normas y los procedimientos de seguridad de la información

Situación

a. Al 2 de febrero de 2011, la OAJ no contaba con un programa para divulgar al personal las normas y los procedimientos de seguridad de la información (*security awareness*). Mediante este se orienta a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la agencia y se dan a conocer la reglamentación y la política pública relacionadas con la seguridad de la misma.

Criterio

Las mejores prácticas en el campo de la tecnología de información requieren que cada entidad gubernamental establezca e implante un programa para la divulgación de las normas y los procedimientos de

seguridad de información a todos sus funcionarios y empleados. Un programa bien diseñado para la divulgación de las normas y los procedimientos de seguridad debe estar, primeramente, encaminado a crear conciencia de los riesgos a los cuales están expuestos los sistemas de información, y luego a desarrollar actitudes prácticas en los funcionarios y los empleados de una organización con el fin de promover la protección de los activos físicos y los de la información. La concienciación de los riesgos y las salvaguardas disponibles son las primeras líneas de defensa que se utilizan en la seguridad de los sistemas de información y de las redes de comunicación gubernamentales.

Efectos

La situación comentada podría ocasionar el incumplimiento de las normas de seguridad con los consiguientes efectos adversos en cuanto a la protección de la información. Esto, a su vez, podría afectar la integridad, la disponibilidad y la confiabilidad de la información procesada por los usuarios.

Causa

La situación comentada se atribuye a que el Director Ejecutivo en funciones no le requirió a la Directora de Recursos Humanos que implantara un programa de capacitación sobre lo establecido en las normas y los procedimientos de seguridad de la información para orientar a todos los empleados de la OAJ.

Comentarios de la Gerencia

En la carta del entonces Director Ejecutivo, este nos indicó, lo siguiente:

> Se impartieron instrucciones a los fines de preparar el programa sobre las normas y procedimientos de seguridad de la información [...]. [*sic*]

Véase la Recomendación 7.

RECOMENDACIONES

Al Director Ejecutivo de la Oficina de Asuntos de la Juventud

1. Asegurarse de que para futuros proyectos para el desarrollo e implantación de sistemas computadorizados se preparen, previo al otorgamiento de un contrato:

   a. Estudios de viabilidad que permitan definir los requisitos de los usuarios y evaluar los beneficios y costos asociados a cada una de las soluciones identificadas para satisfacer estos requisitos. **[Hallazgo 1-a.1)]**

   b. Solicitudes de propuestas que permitan evaluar el alcance y el costo de los servicios ofrecidos por los posibles contratistas antes de otorgar los contratos, y así obtener los mejores precios y condiciones. **[Hallazgo 1-a.2)]**

   c. El *Plan Anual de Administración de Recursos Tecnológicos (PAART)* para cumplir con la *Política TIG-001* de la *Carta Circular 77-05*, y que el mismo sea remitido para evaluación a la Oficina de Gerencia y Presupuesto. **[Hallazgo 1-a.3)]**

2. Ejercer una supervisión eficaz sobre el Director de Finanzas para que se asegure de que los encargados de certificar los servicios y las facturas de los contratos verifiquen que los contratistas cumplan con lo estipulado en los contratos y que la documentación incluya toda la información necesaria para fiscalizar los pagos. **[Hallazgo 1-a.4)]**

3. Asegurarse de que se realice, si aún no se ha hecho, y se documente el análisis de riesgos, según se establece en la *Política TIG-003* de la *Carta Circular 77-05*. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. **[Hallazgo 2]**

4. Realizar las gestiones necesarias para que la OAJ cuente con un *Plan de Seguridad* que incluya los criterios descritos en el **Hallazgo 3**.

Además, se asegure 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 Programa de la OSI para asegurarse de que:

   a. Revise el *Plan de Contingencia y Recuperación de Desastres* para que incluya y actualice los aspectos comentados en el **Hallazgo 4-a. y b.** y lo remita para aprobación.

   b. Prepare los procedimientos de prueba o simulacros necesarios para verificar la efectividad del *Plan de Contingencia y Recuperación de Desastres* y los remita para aprobación. Además, de efectuar pruebas o simulacros del *Plan*, por los menos, dos veces al año y mantenga la documentación de las estrategias utilizadas y los resultados de las pruebas. **[Hallazgo 4-c.]**

   c. Realice las gestiones necesarias para identificar un lugar seguro y adecuado fuera de los predios de la OAJ para guardar una copia del *Plan de Contingencia y Recuperación de Desastres* aprobado, copias de los respaldos diarios y mensuales de la información de los sistemas computadorizados y de la documentación de las configuraciones de los sistemas, de las aplicaciones y de los programas críticos. **[Hallazgo 4-d.]**

   d. Mantenga un registro de los programas adquiridos e instalados en los servidores y en las computadoras portátiles de la OAJ que contenga, entre otra información, el número de licencia y el costo de los programas instalados, el nombre del usuario, el número de propiedad y la descripción de la computadora donde están instalados los mismos. Esto, con el fin de mantener un inventario de los programas y prevenir la instalación de programas no autorizados. **[Hallazgo 5-a.]**

e. Realice las gestiones necesarias para que:

1) Se prepare la documentación de implementación y actualización de la red y del sistema operativo, y documenten todos los cambios realizados a la misma. **[Hallazgo 5-b.]**

2) Se incluya un registro de auditoría en el módulo de seguridad de la Aplicación para que permita efectuar revisiones periódicas sobre transacciones registradas. **[Hallazgo 6-a.]**

f. Establezca las medidas necesarias para que la documentación de la aplicación Programa Sorteo Viajes Estudiantiles, o de cualquier sistema utilizado, se mantenga completa y actualizada. **[Hallazgo 6-b.]**

g. Prepare y remita para aprobación los procedimientos para la administración y el control de las cuentas de acceso a la red de la OAJ, a las aplicaciones, al correo electrónico y a Internet. En estos se deben establecer las directrices para la utilización y el control de un formulario para la solicitud, la aprobación, la creación, la modificación y la cancelación de las cuentas de acceso de los usuarios. **[Hallazgo 7]**

h. Evalúe las opciones de seguridad disponibles en los sistemas de seguridad de los sistemas operativos y establezca las medidas necesarias para mitigar los riesgos y las amenazas existentes. **[Hallazgo 8]**

6. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus respectivos equipos en casos de desastres o emergencia en la OAJ, o considerar establecer su propio centro alterno en alguna instalación que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. **[Hallazgo 4-e.]**

7. Ejercer una supervisión eficaz sobre la Directora de Recursos Humanos para asegurarse de que establezca un programa de capacitación para orientar a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la agencia y dar a conocer las reglamentaciones y las políticas relacionadas con la seguridad de la información. **[Hallazgo 9]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yesmín M. Valdivieso

ANEJO

OFICINA DEL GOBERNADOR
OFICINA DE ASUNTOS DE LA JUVENTUD
OFICINA DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Héctor O'Neill Rosa	Director Ejecutivo	29 nov. 10	15 jun. 11
Sr. Rolando Meléndez Martínez	Subdirector	29 nov. 10	15 jun. 11
Sra. Marielis Rivera Cosme	Directora de Área[4]	1 abr. 11	15 jun. 11
Sra. Marisel Félix Ortiz	Directora de Recursos Humanos	29 nov. 10	15 jun. 11
Sr. Miguel Borges Guevara	Director de la Oficina de Sistemas de Información	29 nov. 10	15 jun. 11
Sr. Carlos J. Aja Rivera	Director de Finanzas	29 nov. 10	15 jun. 11
Sr. Elvin Rivera Mora	Director del Área Auxiliar de Servicios	29 nov. 10	15 jun. 11
Sr. Héctor Vázquez García	Auditor Interno	29 nov. 10	15 jun. 11
Sr. Luis Rodríguez Díaz	Director de Relaciones Públicas	29 nov. 10	15 jun. 11

[4] El puesto de Director de Área fue aprobado el 15 de febrero de 2011 por la OGP.

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 1106, 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) 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:

http://www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr