Estado Libre Asociado de Puerto Rico
Oficina del Contralor

BORRADOR
PARA DISCUSIÓN SOLAMENTE
PRIVILEGIADO Y CONFIDENCIAL

13 de diciembre de 2011

PRIVILEGIADA Y CONFIDENCIAL

Hon. Miguel Hernández Vivoni
Secretario
Departamento de la Vivienda
San Juan, Puerto Rico

Estimado señor Secretario:

RE: CG 5330 - 13615 - 01

Realizamos la auditoría de los Sistemas de Información Computadorizados del Departamento de la Vivienda (Departamento) en lo que concierne a la planificación y administración del programa de seguridad, la evaluación de los controles de acceso, la continuidad del servicio, la evaluación de los procedimientos relacionados con las operaciones de los sistemas de información y la participación de la Oficina de Auditoría Interna en la evaluación de la seguridad, los controles y las operaciones de los sistemas computadorizados de información del Departamento. Esta auditoría cubre el período del 31 de mayo de 2011 al 7 de septiembre de 2011. En el anejo se comentan detalladamente los hallazgos relacionados con estas operaciones. Estos contienen los resultados preliminares de nuestro examen, por lo que su contenido es exclusivamente para uso interno del Departamento y deberá mantenerse en absoluta confidencialidad.

El propósito de esta comunicación es obtener sus comentarios sobre los hallazgos e información referente a las medidas tomadas, para considerarlos antes de producir el borrador de informe. Agradeceremos que nos remita sus comentarios y la información pertinente no más tarde del 11 de enero de 2012.

Si usted interesa una reunión con el suscribiente para aclarar algún asunto sobre los hallazgos, le agradeceremos que nos lo notifique dentro de los próximos tres días. 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,

Erik J. Lebrón Matos
Auditor Senior
de Tecnología de Información

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

ANEJO 1

DEPARTAMENTO DE LA VIVIENDA
31 de mayo de 2011 al 30 marzo de 2012
13615

HALLAZGOS

Hallazgo 1 – Falta de un informe de Avalúo de Riesgos sobre los sistemas de información computadorizados

Situación

a. Un avalúo de riesgos es un método para identificar las vulnerabilidades y las amenazas a los recursos de sistemas de información. Además, evalúa los posibles daños para determinar dónde implantar las medidas de seguridad para poder alcanzar y cumplir con los objetivos de la entidad gubernamental. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo efectivas, relevantes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

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

Al 23 de junio de 2011, el Departamento no había realizado un avalúo de riesgos sobre los sistemas de información.

Criterio

En la *Política Núm. TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto se establece, entre otras cosas, que cada agencia deberá 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:

- Un inventario de activos de sistemas de información, incluidos 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 datos, entre otros) 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

Efecto

La situación comentada impide al Departamento evaluar el impacto que

los elementos de riesgos tendrían en las áreas y en los sistemas críticos de ésta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y 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 en caso de que surja alguna eventualidad.

Hallazgo 2 – Falta de un Plan de Seguridad

Situación

a. Al 13 de julio de 2011, la Oficina de Sistemas de Información (OSI) no tenía un Plan de Seguridad aprobado por el Secretario que incluyera, entre otras cosas, disposiciones relacionadas con:

- La documentación de la validación de las normas de seguridad[1].
- La evidencia de un análisis de riesgos actualizado, que sea la base del *Plan*.
- 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, personal de sistemas de información y usuarios, y que permita mantener los

[1] 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 **Avalúo de Riesgos**. Además, se valida mediante los resultados de los simulacros efectuados para probas la efectividad del **Plan de Seguridad**.

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

En la *Política Núm. TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular Núm. 77-05*, se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. También se establece que las entidades gubernamentales son responsables de:

- Proveer adiestramientos a toda la gerencia y a los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- Proveer adiestramientos al personal de sistemas de información y telecomunicaciones y de que se le transmitan conocimientos actualizados sobre los aspectos de seguridad de sus áreas. Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

Efecto

De ocurrir una emergencia, la falta de un Plan de Seguridad y de los correspondientes adiestramientos y simulacros podría dar lugar a:

- Pérdidas de vidas humana
- Daños a los equipos de sistemas de información, así como la pérdida

de datos importantes

- Atrasos en el proceso de reconstrucción de datos y programas, y en el restablecimiento y la continuidad de las operaciones normales y otras situaciones adversas.

Hallazgo 3 – Deficiencias en el *Plan de Manejo de Emergencia del Área de Sistemas de Información*, falta de acuerdos para mantener un centro alterno de recuperación de operaciones y falta de simulacros para comprobar la efectividad de los procedimientos de emergencias

Situación

a. El Departamento contaba con un *Plan de Manejo de Emergencia del Área de Sistemas de Información* (*Plan de Emergencia*), aprobado el 5 de septiembre de 2006 por el Secretario de la Vivienda, que incluía los procedimientos para la continuidad de las operaciones y la recuperación en caso de desastre. Nuestro examen de este *Plan de Emergencia* reveló que no incluía información actualizada sobre:

   - El programa utilizado por el Departamento para efectuar los respaldos de los sistemas de información (*Symantec Backup Exe 2010)*. En su lugar el *Plan de Emergencia* hacía referencia al programa *Veritas 8.6* el cual no era utilizado desde noviembre de 2008.

   - Ocho servidores virtuales (BACKUP_SERVER, WEBDV, DPTOANTIVIRUS, FILESERVER 05, SERVIO, SERVER 3, SQL SERVER, VSPHERE CENTER) que eran utilizados por la OSI del Departamento para almacenar las bases de datos preparadas en el Departamento, para actualizar el antivirus en las estaciones de trabajo, para controlar los servidores virtuales y para manejar el *Active Directory*, la aplicación de intranet (*Microsoft Share Point Portal Server*) y la aplicación de

PRIFAS-RHUM.

- El diagrama organizacional del Departamento.
- El personal autorizado para acceder a la bóveda externa. El *Plan de Emergencia* incluía un Especialista en Sistemas Electrónicos y un ex supervisor de Redes, los cuales no estaban autorizados.
- Un centro alterno ubicado en la Secretaría de Subsidio de Vivienda y Desarrollo Comunitario de la Avenida Las Lomas. Este centro alterno no estaba en funcionamiento a la fecha de nuestra auditoría, se utilizaba como almacén. **[Hallazgo 3.b]**

b. Al 13 de julio de 2011, la Oficina de Sistemas de Información del Departamento no contaba con un centro alterno de los sistemas de información para restaurar las operaciones críticas computarizadas en casos de emergencia. Tampoco había formalizado acuerdos con otra entidad para establecer un centro alterno en las instalaciones de ésta.

c. Al 20 de julio de 2011, la OSI no había efectuado las pruebas o simulacros que certificaran la efectividad del *Plan de Emergencia.*

Criterio

En el *Artículo 4* de la *Ley Núm. 97 del 10 de junio de 1972*, según enmendada, *Ley Orgánica del Departamento de la Vivienda*, se establecen los poderes y las facultades conferidas al Secretario entre las cuales se incluyen los siguientes:

- Planificar, dirigir y supervisar el funcionamiento del departamento y sus programas.
- Prescribir, derogar, y enmendar reglamentos para el funcionamiento del departamento.

En el *Plan de Emergencias* se establece que éste debe ser revisado y

actualizado continuamente tomando en cuenta los resultados y experiencias de cada una de las actividades de prueba. El itinerario de estas pruebas será preparado por el Oficial Principal de Informática de acuerdo con la frecuencia establecida en el mismo. **[Apartado a.]**

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:

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

[Apartado b.]

Además, sugieren se deben efectuar procedimientos para realizar pruebas o simulacros, por lo menos una vez al año, revisar del Plan anualmente o en un término menor, según las necesidades del Departamento y darlo a conocer a todo el personal que llevará a cabo los procesos del mismo. **[Apartado c.]**

Efecto

Las situaciones comentadas en los **apartados a. y 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 e interrupciones prolongadas de los servicios a los usuarios de la OSI. Además, podría

exponer al personal, a los equipos y a la información a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

La situación comentada en el **apartado b.** podría afectar las funciones de la OSI y los servicios del Departamento, 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, con los consiguientes efectos adversos para las operaciones del Departamento.

Hallazgo 4 – Deficiencias relacionadas con los controles ambientales del cuarto de servidores de la OSI y en los cuartos de distribución de cableado (*wiring closets*) del Departamento

a. La OSI contaba con dos cuartos continuos de servidores. En el primer cuarto se encontraba el *ISA Server*, un servidor para almacenar imágenes geográficas, un servidor para los resguardos, un *apliance* como *firewall* para manejar la seguridad interna y externa, un servidor *Catalyst 6500 CISCO* que maneja la data y el cuadro telefónico, y un servidor que controla las luces del edificio. En el segundo cuarto se encontraban los servidores virtuales, y los servidores físicos que manejan la aplicación *Emphasys Elite*. Además, se encontraba el servidor dedicado al control de las cámaras de seguridad y otro para el monitoreo de los accesos en los diferentes pisos del Departamento.

   El 20 de julio de 2011, examinamos los controles ambientales de los cuarto de servidores de la OSI y determinamos que los mismos no contaban con equipos para verificar de forma preventiva los niveles de humedad. El uso de los termómetros de humedad son recomendados para entre otras cosas identificar posibles problemas con el funcionamiento de los aires acondicionados.

b. El Departamento contaba con ocho cuartos de distribución de cableados, cinco de estos estaban ubicados en los pisos décimo, sexto, quinto, cuarto y sótano del edificio principal del Departamento y los restantes tres se encontraban ubicados en el edificio anexo, uno en la Secretaría Auxiliar de Recursos Humanos, uno en la Oficina Regional de San Juan y uno en la Oficina de Servicio al Cliente. El examen sobre la seguridad y el acceso físico existentes en los cuartos de distribución del cableado (*wiring closets*) en los que se mantenían los equipos de telecomunicaciones de la red del Departamento, reveló las siguientes deficiencias:

1) En todos los cuartos de distribución de cableado los cables de fibra óptica y energía eléctrica se encuentran expuestos o no están debidamente protegidos. Además, los equipos se encontraban cubiertos de polvo.

2) En los cuartos de distribución de cableado del cuarto y quinto piso se observó que la tubería sanitaria discurre sobre los equipos de la red de comunicación.

3) En el cuarto de distribución de cableado del cuarto piso se encontró partes residuales de equipo de oficina. Además, en el cuarto de cableado ubicado en la Oficina de Servicio al Cliente, se encontraron varias cajas de cartón.

4) En el cuarto de distribución de cableado ubicado en el sótano del edificio del Departamento se encontró equipo de limpieza.

5) El cuarto de distribución de cableado del sexto piso no había iluminación.

6) Los equipos de respaldo (*Battery Backup's*) de los equipos de comunicaciones estaban ubicados a nivel del piso en los cuartos

b. El Departamento contaba con ocho cuartos de distribución de cableados, cinco de estos estaban ubicados en los pisos décimo, sexto, quinto, cuarto y sótano del edificio principal del Departamento y los restantes tres se encontraban ubicados en el edificio anexo, uno en la Secretaría Auxiliar de Recursos Humanos, uno en la Oficina Regional de San Juan y uno en la Oficina de Servicio al Cliente. El examen sobre la seguridad y el acceso físico existentes en los cuartos de distribución del cableado (*wiring closets*) en los que se mantenían los equipos de telecomunicaciones de la red del Departamento, reveló las siguientes deficiencias:

1) En todos los cuartos de distribución de cableado los cables de fibra óptica y energía eléctrica se encuentran expuestos o no están debidamente protegidos. Además, los equipos se encontraban cubiertos de polvo.

2) En los cuartos de distribución de cableado del cuarto y quinto piso se observó que la tubería sanitaria discurre sobre los equipos de la red de comunicación.

3) En el cuarto de distribución de cableado del cuarto piso se encontró partes residuales de equipo de oficina. Además, en el cuarto de cableado ubicado en la Oficina de Servicio al Cliente, se encontraron varias cajas de cartón.

4) En el cuarto de distribución de cableado ubicado en el sótano del edificio del Departamento se encontró equipo de limpieza.

5) El cuarto de distribución de cableado del sexto piso no había iluminación.

6) Los equipos de respaldo (*Battery Backup's*) de los equipos de comunicaciones estaban ubicados a nivel del piso en los cuartos

- Se mantenga la documentación e identificación adecuada del cableado de conexión a la red, de forma que se puedan corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada. **[Apartado b.7)]**

En la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica* de la *Carta Circular Núm. 77-05,* se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar e implementar 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, incluye como política que el diseño de la Red debe estar documentado. **[Apartado b.7]**

Las mejores prácticas en el campo de la tecnología de información sugieren que, para mantener en funciones aceptables la red, es necesario establecer controles adecuados sobre los inventarios, la ubicación y las conexiones entre sus componentes. Esto se logra mediante la documentación detallada y actualizada de las conexiones que permita corregir a tiempo problemas de comunicación de la red y detectar cualquier conexión no autorizada. **[Apartado b.7)]**

Efecto

La situación comentada en los **apartados a. al b.1) al b.6)** podría tener como resultado el mal funcionamiento de los equipos, afectando considerablemente las operaciones diarias del Departamento, y resultaría en costos considerables para regresar a las operaciones normales. Además, la situación comentada en el **apartado b.7)** dificulta la atención de problemas de conexión en un tiempo razonable.

Hallazgo 5 – Cuentas de acceso activas de exempleados del Departamento

Situación

a. El examen efectuado sobre los controles de acceso al servidor configurado como *Primary Domain Controller* reveló que al 30 de julio de 2011, no se habían desactivado las cuentas de accesos de siete exempleados del Departamento. Estos exempleados habían cesado sus funciones entre 31 de enero de 2009 y el 31 de diciembre de 2010. [aromero, AWtorres, Druiz, Mcortes, lcolon, yogonzalez, yramos,]

Criterio

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establecen las directrices generales que permiten a las agencias establecer controles adecuados en sus sistemas de información computadorizados para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Además, establece que cada agencia deberá implantar controles para el manejo de la terminación de empleados, de manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto, deberán establecerse procedimientos que incluyan una comunicación efectiva entre el Área de Recursos Humanos, el área en que trabaja el empleado y el Área de Sistemas de Información. Estos procedimientos se instrumentan, en parte, mediante la notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones o de la modificación de las mismas para su acción correspondiente. **[Apartado a.]**

Efecto

La situación comentada en el **apartado a.** propicia que personas no autorizadas puedan lograr acceso a información confidencial mantenida en

los sistemas computadorizados, y hacer uso indebido de ésta. Además, propicia 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.

Hallazgo 6 – Falta de adiestramientos sobre el uso y la seguridad de los sistemas de información

a. El 1 de septiembre de 2011, la Directora Administrativa III del Área de Servicios al Empleado de la Secretaría Recursos Humanos y Servicios Auxiliares, nos certificó que desde el 16 de febrero de 2010 hasta el 19 de agosto del 2011, solamente 3 (0.69 por ciento) de 436 empleados con acceso a la red de comunicaciones del Departamento recibieron adiestramientos relacionados con el uso y la seguridad de los sistemas de información computadorizados. Estos adiestramientos son necesarios para asegurarse de que el personal esté capacitado para ejercer sus funciones y cumplir con sus responsabilidades relacionadas con el uso y la seguridad de los sistemas de información computadorizados.

Criterio

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece como política pública que las entidades gubernamentales son responsables de:

- Proveer adiestramientos a toda la gerencia y a los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen

Efecto

La falta de adiestramientos relacionados con el uso y la seguridad de los sistemas de información computadorizados podría ocasionar efectos adversos en cuanto a la utilización y protección de la información y del equipo. Esto, a su vez, podría afectar la integridad, la disponibilidad y la confiabilidad de la información manejada por los usuarios.

Hallazgo 7 – Falta de procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados del Departamento, para el trámite de renuncias, separación o destitución de los empleados, y deficiencias en las *Normas Sobre el Uso de los Sistemas Electrónicos*

a. Al 6 de septiembre de 2011, el Departamento contaba con las siguientes normas y procedimientos para la administración y seguridad de los sistemas de información computadorizados.

- El manual *Normas Sobre el Uso de los Sistemas de Electrónicos del Departamento de la Vivienda,* aprobado el 12 de mayo de 2010 por el Secretario de la Vivienda
- El *Plan de Emergencia.*

Nuestro examen sobre la reglamentación del Departamento reveló las siguientes deficiencias:

1) No se habían promulgado las normas ni los procedimientos escritos necesarios para reglamentar los siguientes procesos relacionados con la administración y la seguridad de los sistemas computadorizados:

- Los controles de acceso físico a los sistemas de información computadorizados.
- El establecimiento de un itinerario para el mantenimiento

preventivo del equipo de acuerdo a las especificaciones del proveedor.

- La solicitud, la aprobación, la creación, la otorgación de niveles de acceso, la modificación y la cancelación de las cuentas de los usuarios de los sistemas de información.
- El desarrollo de nuevas aplicaciones y el control de cambios a las existentes.
- La identificación y documentación de incidentes no esperados en las aplicaciones críticas del Departamento.
- El monitoreo del funcionamiento de la aplicación crítica del Departamento (*Emphasys Elite*).
- El monitoreo de la utilización del correo electrónico.
- El monitoreo de los accesos y el uso del Internet.
- La detección de accesos no autorizados a los sistemas de información del Departamento.

2) Al 12 de agosto de 2011, la Secretaría Auxiliar de Recursos Humanos no contaba con un procedimiento para informar a la OSI sobre los trámites de renuncias, separación o destitución de los empleados del Departamento con el fin de eliminar los accesos otorgados a los exempleados.

b. El manual *Normas Sobre el Uso de los Sistemas Electrónicos,* carecía de las siguientes disposiciones:

- La prohibición de utilizar o publicar material que viole los derechos de autor.
- El establecer que el Departamento se reserva el derecho de

radicar acusaciones criminales por las actuaciones que constituyan delito federal o estatal aunque no estén expresamente prohibidas por estas condiciones de uso de los equipos de computadoras.

Criterio

En el *Artículo 4* de la *Ley Núm. 97* se establecen los poderes y las facultades conferidas al Secretario entre las cuales se incluyen los siguientes:

- Planificar, dirigir y supervisar el funcionamiento del departamento y sus programas
- Prescribir, derogar y enmendar reglamentos para el funcionamiento del departamento

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. **[Apartado a. y b.]** Además, deberán existir procesos que permitan monitorear las actividades de los usuarios en aquellos activos que así lo ameriten **[Apartado a.]**.También, establece que deberán establecerse 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. Para esto deberán establecerse procedimientos que incluyan una comunicación efectiva entre el Área de Recursos Humanos, el área en que trabaja el empleado y el Área de Sistemas de Información. **[Apartado a.2)]**

En la *Política Núm. TIG-008* de la *Carta Circular Núm. 77-05* se dispone que cada agencia deberá establecer políticas necesarias para garantizar el

uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que éstos proveen. Esto implica que, como norma de sana administración, se deben establecer por escrito políticas, normas y procedimientos 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, contribuye a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia y facilitan la labor de adiestramiento. **[Apartado a. y b.]**

Efecto

La situación comentada en el **apartado a.1)** priva al Departamento de herramientas para llevar a cabo medidas disciplinarias de personal en casos de violación a las leyes relacionadas con el derecho de autor y otras aplicables al uso de los equipos computadorizados.

La situación comentada en el **apartado a.2)** ocasionó que la OSI no desactivara las siete cuentas de exempleados comentadas en el **Hallazgo 5-a.**

La situación comentada en el **apartado b.** pudiese exponer al Departamento a riesgos de seguridad innecesarios. El no establecer procedimientos uniformes que aseguren que tanto el acceso físico como el lógico del personal que no labora en el Departamento sea removido con prontitud, podría permitir que se realicen transacciones o modificaciones de datos sensitivos no autorizados. Además, no permite establecer responsabilidades al momento de asegurar que la gerencia de las diferentes áreas reciba rápidamente la información sobre los movimientos de los empleados.

Hallazgo 8 – Falta de participación de la Oficina de Auditoría Interna en la evaluación de la seguridad, los controles y las operaciones de los sistemas computadorizados de información del Departamento

Situación

a. Al 25 de agosto de 2010, el Departamento contaba con la Oficina de Auditoría Interna, compuesta por: el Director, el Subdirector y un Auditor II. A partir del 1 de octubre de 2011, los auditores internos que pertenecían al Departamento comenzaron a reportarse a la Oficina del Inspector General[2], sin embargo, permanecían ubicados físicamente en las facilidades de la Oficina de Auditoría Interna del Departamento. Nuestro examen de los informes de auditoría publicados del 19 de septiembre de 2008 al 25 de agosto de 2011 por la Oficina de Auditoria Interna del Departamento[3] y entrevista al Director de la Oficina de Auditoría Interna reveló que no se habían efectuado auditorías de los controles y las operaciones de los sistemas de información, ni de la seguridad o de los procesos que se llevan a cabo utilizando la aplicación más importante del Departamento.

Criterio

En la normas para la práctica profesional de la auditoría interna se establece, entre otras cosas, que la actividad de auditoría interna debe asistir a la organización mediante la identificación y la evaluación de las

---

[2] En el *Artículo 4* de la *Ley Núm. 42 del 16 de abril de 2010, Ley del Inspector General del Gobierno de Puerto Rico*, se creó la Oficina del Inspector General del Gobierno de Puerto Rico para coordinar y ampliar los esfuerzos gubernamentales para promover la integridad y la eficiencia, y detectar y prevenir fraude, malversación y abuso en el uso de los fondos públicos estatales y federales. Además, se estableció que dicha oficina absorbería las funciones, recursos y personal del Área de Auditoría de la Oficina de Gerencia y Presupuesto (OGP) y este personal sería reforzado sería reforzado con personal de las oficinas de auditoría interna de las agencias, departamentos y entidades gubernamentales, quienes le responderían directamente a dicha Oficina.

[3] El 5 de junio de 2009, se publicó el Informe de Auditoría DV-07-16 sin embargo, el período del mismo son los años fiscales 2006-2007 y 2007-2008 y no cubrió la aplicación *Emphasys Elite*.

exposiciones de los riesgos y contribuir al mejoramiento de los sistemas de gestión de riesgos y control. También se establece que la actividad de auditoría interna debe evaluar las exposiciones de riesgo referidas a gobierno, operaciones y sistemas de información con relación a lo siguiente:

- Confiabilidad e integridad de la información financiera y operativa
- Eficacia y eficiencia de las operaciones
- Protección de activos
- Cumplimiento de las leyes, los reglamentos y los contratos.

Efecto

La falta de fiscalización y de recomendaciones sobre los procedimientos, los controles, el uso y el funcionamiento de los sistemas de información computadorizados, por parte de los auditores internos, puede propiciar que se cometan errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades. También priva a la gerencia de información necesaria sobre el funcionamiento de los sistemas, los controles y demás operaciones del Departamento. Además, existe la posibilidad de que en los sistemas de información no se incluyan los controles básicos necesarios para evitar incurrir en errores, irregularidades y otras situaciones adversas.