1

Madeline Dimo

SENADO PUERTO RICO

Secretaría

MANUEL A. TORRES NIEVES
SECRETARIO DEL SENADO

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

Senado
DE PUERTO RICO

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

T: 787.722.3460
787.722.4012
F: 787.723.5413
E: mantorres@senadopr.us
W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

- ☐ Hacienda
- ☐ Gobiemo
- ☐ Seguridad Pública y Judicatura
- ☐ Salud
- ☐ Educación y Asuntos de la Familia
- ☐ Desarrollo Eonómico 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 de la Montaña
- ☐ Asuntos de la Mujer
- ☐ Asuntos Internos
- ☐ Reglas y Calendario
- ☐ Asuntos Federales
- ☐ Ética

COMISIONES ESPECIALES

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

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

INFORME DE AUDITORÍA TI-10-06

1 de octubre de 2009

DEPARTAMENTO DE RECREACIÓN Y DEPORTES

OFICINA DE SISTEMAS DE INFORMACIÓN

(Unidad 5030 - Auditoría 13017)

Período auditado: 1 de junio de 2007 al 27 de mayo de 2008

CONTENIDO

Página

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

RESPONSABILIDAD DE LA GERENCIA **5**

ALCANCE Y METODOLOGÍA **6**

OPINIÓN **6**

RECOMENDACIONES **7**

AL SECRETARIO DE RECREACIÓN Y DEPORTES 7

CARTAS A LA GERENCIA **12**

COMENTARIOS DE LA GERENCIA **12**

AGRADECIMIENTO **12**

RELACIÓN DETALLADA DE HALLAZGOS **13**

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO 13

HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DE RECREACIÓN Y DEPORTES 14

1 - Computadoras y cuentas para acceder a Internet y al correo electrónico utilizadas para fines ajenos a la gestión pública, y falta de actualización de las definiciones del programa antivirus instalado en las computadoras 14

2 - Falta de un Informe de Avalúo de Riesgos sobre los sistemas de información 19

3 - Falta de un Plan de Seguridad, de acuerdos de confidencialidad y de un procedimiento para el manejo de incidentes de seguridad sobre los sistemas de información 21

4 - Falta de un Plan de Continuidad de las Operaciones, de acuerdos escritos para mantener un centro alterno y de una fuente de energía alterna 24

5 - Deficiencias en los parámetros de seguridad de los servidores del Departamento para controlar las cuentas de acceso a los recursos de la Red 26

6 - Falta de revisiones periódicas a los registros de eventos producidos en el servidor principal 30

7 - Deficiencias relacionadas con la configuración y la estructura de acceso a la Red, y con la documentación de la estructura de la Red del Departamento 32

8 - Falta de normas y de procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados del Departamento 34

9 - Falta de controles sobre los equipos computadorizados 36

10 - Falta de un registro de programas instalados en cada computadora 37

11 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información 38

ANEJO - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO 41

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

1 de octubre de 2009

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) del Departamento de Recreación y Deportes (Departamento) para determinar si se hicieron de acuerdo con las normas generalmente aceptadas en este campo y si el sistema de control interno establecido para el procesamiento de las transacciones era adecuado. Efectuamos la misma a base de la facultad que se nos confiere en la **Sección 22 del Artículo III de la Constitución del Estado Libre Asociado de Puerto Rico** y en la **Ley Núm. 9 del 24 de julio de 1952**, según enmendada.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Departamento fue creado por la **Ley Núm. 8 del 8 de enero de 2004**[1], **Ley Orgánica del Departamento de Recreación y Deportes**, según enmendada. Su función principal es ofrecer a la ciudadanía alternativas saludables para el buen uso de su tiempo libre, administrar los programas de recreación y deportes de manera ágil y proactiva, en coordinación con los municipios y las organizaciones comunitarias para lograr una mayor participación de todos los sectores de la sociedad.

El Departamento es administrado por un Secretario nombrado por el Gobernador de Puerto Rico, con el consejo y consentimiento del Senado. Para realizar sus funciones, el Departamento está organizado en las siguientes secretarías auxiliares: Administración,

[1] Dicha **Ley** derogó la **Ley Núm. 126 del 13 de junio de 1980**, según enmendada.

Recursos Humanos y Relaciones Laborales, Infraestructura Física, Recreación y Deportes, y el Deporte de Alto Rendimiento. Además, cuenta con 5 oficinas administrativas a nivel central (Asesoramiento Legal, Auditoría Interna, Prensa y Comunicaciones, Presupuesto y Planificación, y Sistemas de Información), 10 oficinas regionales y 4 comisiones[2]. También cuenta con el Consejo Nacional para la Vinculación del Deporte, Recreación y la Educación Física; la Comisión de Seguridad en la Recreación y el Deporte; la Comisión de Deporte Profesional; y el Instituto Puertorriqueño para el Desarrollo del Deporte y la Recreación, adscritos a la Oficina del Secretario.

A la fecha de nuestra auditoría, la OSI del Departamento tenía una red de comunicaciones de área local (Red) compuesta por 10 servidores. El Departamento tenía 421 computadoras con sus respectivos equipos periferales, de las cuales 271 estaban conectadas a la Red. Además, la Red era utilizada para el acceso a Internet y al correo electrónico.

La OSI se componía de un Oficial Principal de Informática (OPI), un Director Auxiliar en Sistemas de Información, un Administrador de Redes, un Técnico en Programación y Conservación de Sistemas y Equipo de Información Electrónica II, y un Técnico en Programación y Conservación de Sistemas y Equipo de Información Electrónica I.

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

El presupuesto asignado al Departamento para el año fiscal 2006-07 fue de $58,256,000. Este se compone de $41,356,000 con cargo a la Resolución Conjunta del Presupuesto General y de $16,900,000 de Asignaciones Especiales.

---

[2] Comisiones de: Asuntos Gallísticos, Boxeo Profesional, Deportes Profesionales, y Seguridad en la Recreación y el Deporte.

Al 27 de marzo de 2008 estaban pendientes de resolución por los tribunales 11 demandas civiles presentadas contra el Departamento por $1,467,371. De este importe, $606,000 eran por daños y perjuicios, $761,371 eran por cobro de dinero y $100,000 por otras situaciones.

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

RESPONSABILIDAD DE LA GERENCIA

La gerencia de todo organismo gubernamental debe considerar los siguientes **Diez Principios para Lograr una Administración Pública de Excelencia**. Éstos se rigen por principios de calidad y por los valores institucionales:

1. Adoptar normas y procedimientos escritos que contengan controles internos de administración y de contabilidad eficaces, y observar que se cumpla con los mismos.
2. Mantener una oficina de auditoría interna competente.
3. Cumplir con los requisitos impuestos por las agencias reguladoras.
4. Adoptar un plan estratégico para las operaciones.
5. Mantener el control presupuestario.
6. Mantenerse al día con los avances tecnológicos.
7. Mantener sistemas adecuados de archivo y de control de documentos.
8. Cumplir con el **Plan de Acción Correctiva** de la Oficina del Contralor de Puerto Rico, y atender las recomendaciones de los auditores externos.
9. Mantener un sistema adecuado de administración de personal que incluya la evaluación del desempeño, y un programa de educación continua para todo el personal.
10. Cumplir con la **Ley de Ética Gubernamental**, lo cual incluye divulgar sus disposiciones a todo el personal.

El 27 de junio de 2008, mediante la **Carta Circular OC-08-32**, divulgamos la revisión de los mencionados diez principios establecidos en nuestra **Carta Circular OC-98-09 del 14 de abril de 1998**. Ambas **cartas circulares** se pueden acceder a través de nuestra página de Internet: http://www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de junio de 2007 al 27 de mayo de 2008. 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.

Para efectuar la auditoría utilizamos la siguiente metodología:

- Entrevistas a funcionarios, a empleados y a particulares
- Inspecciones físicas
- Examen y análisis de informes y de documentos generados por la unidad auditada
- Análisis de información suministrada por fuentes externas
- Pruebas y análisis de procedimientos de control interno y de otros procesos
- Confirmaciones de información pertinente

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne a la planificación y la administración del programa de seguridad para el área de sistemas de información, la evaluación de los controles de acceso, la continuidad del servicio y el uso de las computadoras, el correo electrónico e Internet no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 11** de este **Informe**, clasificados como principales.

En la parte de este **Informe** titulada **RELACIÓN DETALLADA DE HALLAZGOS** se comentan los referidos **hallazgos**.

RECOMENDACIONES

AL SECRETARIO DE RECREACIÓN Y DEPORTES

1. Ejercer una supervisión efectiva sobre el OPI para asegurarse de que:

   a. Colabore con la persona encargada de ofrecer los adiestramientos durante las orientaciones a los funcionarios y a los empleados del Departamento sobre las normas establecidas en el **Reglamento Interno sobre el Uso de Computadoras del Departamento de Recreación y Deportes**, aprobado el 20 de enero de 2009 por el Secretario, y en otras leyes y políticas aplicables sobre el uso oficial de las computadoras, de las cuentas para acceder a Internet y al sistema de correo electrónico. Además, velar por que se conserve evidencia de dichas orientaciones. **[Hallazgo del 1-a.1) al 3) y b.]**

   b. Realice las inspecciones periódicas necesarias para verificar el uso oficial de las computadoras, de las cuentas para acceder a Internet y al sistema de correo electrónico. **[Hallazgo del 1-a.1) al 3) y b.]**

   c. El Administrador de Redes:

      1) Identifique las computadoras que tienen problemas con las actualizaciones del programa de antivirus y se establezca un plan para asegurarse de que el archivo de definiciones de virus de las mismas se actualice mediante un proceso alterno automatizado o manual. **[Hallazgo 1-a.4)]**

      2) Limite el acceso a Internet para que el personal autorizado sólo pueda acceder las páginas electrónicas que son necesarias para cumplir con sus deberes y responsabilidades, según el análisis realizado por la gerencia. **[Hallazgo 1-b.]**

      3) Efectúe las modificaciones en los parámetros de seguridad del sistema operativo para:

         a) Establecer un mínimo de, al menos, seis caracteres para la utilización de las contraseñas. **[Hallazgo 5-a.1)a)]**

b) Requerir un mínimo de 10 días antes de que el sistema permita al usuario cambiar la contraseña nuevamente. **[Hallazgo 5-a.1)b)]**

c) Restringir que los usuarios puedan repetir las últimas cinco contraseñas utilizadas previamente. **[Hallazgo 5-a.1)c)]**

d) Desconectar automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la Red. **[Hallazgo 5-a.1)d) y e)]**

4) Active las políticas de auditoría (*Audit Policy*) que provee el sistema operativo, de manera que se realicen revisiones continuas de las actividades del sistema. **[Hallazgo 5-a.2)]**

5) Active la opción en el servidor de correo electrónico que le permite producir un archivo sobre todas las cuentas de correo electrónico que han enviado y recibido mensajes de correo electrónico de fuentes externas. Esto, para que le permita, entre otras cosas, hacer revisiones periódicas sobre la efectividad de los controles establecidos y los usuarios autorizados para enviar y recibir mensajes de correo electrónico de fuentes externas. **[Hallazgo 5-a.3)]**

6) Restrinja los derechos y los privilegios para que solamente el personal clave del Departamento pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis realizado por la gerencia. **[Hallazgo 5-a.3)]**

7) Establezca un máximo de 90 días para cambiar la contraseña en la cuenta de acceso con privilegios de administrador. **[Hallazgo 5-b.1)]**

8) Revise periódicamente el registro de eventos que produce el servidor principal y los intentos de acceso a la Red del Departamento y, de ser necesario, tome de inmediato las medidas preventivas y correctivas correspondientes. **[Hallazgo 6]**

d. Prepare y someta para aprobación:

1) El **Plan de Seguridad** en el que se establezcan los proyectos, las tareas y las actividades requeridos para proteger al personal y a los activos del sistema de información. **[Hallazgo 3-a.]**

2) Las normas y los procedimientos para establecer acuerdos de confidencialidad con los funcionarios, los empleados y los consultores del Departamento. **[Hallazgo 3-b.]**

3) El procedimiento para el manejo de incidentes no esperados. Como parte del procedimiento, se debe requerir que se documenten todos los incidentes y cómo se resolvieron, de manera que cuando se repitan los mismos, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información y la continuidad de las operaciones. **[Hallazgo 3-c.]**

4) El **Plan de Continuidad de Negocios**, que incluya un **Plan para la Recuperación de Desastres** y un **Plan para la Continuidad de las Operaciones**. Una vez éste 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 Departamento. Además, asegurarse de que sea distribuido a los funcionarios y los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 4-a.]**

5) Las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el **Hallazgo 8**.

e. Se eliminen prontamente las cuentas de acceso de los empleados que cesaron en sus funciones y vea que, en lo sucesivo, las cuentas se eliminen en el momento en que el empleado cesa. Esto, de manera que se corrija y no se repita la situación comentada en el **Hallazgo 5-b.2)**.

f. Establezca una configuración que incluya una Zona Desmilitarizada (*DMZ,* por sus siglas en inglés)[3] que limite el acceso desde Internet a los servidores de la Red del Departamento y viceversa. Esto es necesario para proteger la Red de ataques cibernéticos y para evitar que personas externas y no autorizadas puedan acceder a ésta y comprometer la seguridad de sus sistemas. **[Hallazgo 7-a.]**

g. Actualice el diagrama de las instalaciones y las configuraciones de la Red del Departamento, dentro de un término razonable, para que incluya la información descrita en el **Hallazgo 7-b.**

h. Mantenga un registro de los programas adquiridos e instalados en las computadoras del Departamento que contenga, entre otra información, el número de la 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 10]**

2. Realizar un análisis para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado para acceder a Internet. Luego de efectuado el análisis, someter la lista de las páginas autorizadas a la OSI. **[Hallazgo 1-b.]**

3. Asegurarse de que se realice y se documente el análisis de riesgos, según se establece en la **Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipo y Programas de Información Tecnológica para los Organismos Gubernamentales**, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto, y según se sugiere en las mejores prácticas del campo de la

---

[3] En seguridad informática, una zona desmilitarizada (*DMZ*, por sus siglas en inglés) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una *DMZ* es que las conexiones desde la red interna y la externa a la *DMZ* estén permitidas, mientras que las conexiones desde la *DMZ* sólo se permitan a la red externa. La *DMZ* se utiliza para ubicar servidores que son necesarios que sean accedidos desde fuera, como servidores de *E-mail*, *Web* y *DNS* (*Domain Name Service*).

tecnología. El informe, producto de este análisis de riesgos, debe ser sometido para su revisión y aprobación. **[Hallazgo 2]**

4. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus equipos en caso de desastres o emergencias en el Departamento, o considerar establecer su propio centro alterno en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. **[Hallazgo 4-b.]**

5. Proveer a la OSI una fuente de energía alterna, de forma que se garantice la continuidad de las operaciones y los servicios de la red de comunicaciones para cuando ocurra una falla prolongada de energía eléctrica. **[Hallazgo 4-c.]**

6. Realizar un análisis para determinar el personal clave del Departamento que requiera tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. Luego de efectuado el análisis, someter la lista del personal clave a la OSI. **[Hallazgo 5-a.3)]**

7. Ver que la Secretaria Auxiliar de Recursos Humanos y Relaciones Laborales, en coordinación con el OPI, establezca un procedimiento para que se notifique a tiempo a la OSI el cese de un usuario en sus funciones para la cancelación de su cuenta de acceso. **[Hallazgo 5-b.2)]**

8. Ver que el Secretario Auxiliar de Administración se asegure de que el Encargado de la Propiedad cumpla con la **Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico**, según enmendada, y con el **Reglamento Núm. 11, Normas Básicas para el Control y la Contabilidad de los Activos Fijos**, aprobado el 29 de diciembre de 2005 por el Secretario de Hacienda, relacionado con la custodia y el control de la propiedad. **[Hallazgo 9]**

9. Asegurarse de que el Director de la Oficina de Auditoría Interna: **[Hallazgo 11]**

    a. Establezca un programa de adiestramiento continuo para capacitar a los auditores internos del Departamento en las técnicas de auditoría de sistemas de información computadorizados.

b. Realice las gestiones necesarias para que se examinen periódicamente los controles y las operaciones de los sistemas de información computadorizados del Departamento.

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este **Informe** se sometió para comentarios al Secretario de Recreación y Deportes, Hon. Henry Neumann Zayas (Secretario), y al ex Secretario de Recreación y Deportes, Dr. David E. Bernier Rivera (ex Secretario), en cartas del 5 de mayo de 2009.

COMENTARIOS DE LA GERENCIA

El Secretario contestó el borrador de los **hallazgos** de este **Informe** mediante carta del 1 de junio de 2009. El ex Secretario contestó el borrador de los **hallazgos** de este **Informe** mediante carta del 4 de junio de 2009. Los comentarios del Secretario y del ex Secretario fueron considerados en la redacción final del **Informe**. Algunas de sus observaciones se incluyen en la parte de este **Informe** titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DE RECREACIÓN Y DEPORTES.

AGRADECIMIENTO

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

Oficina del Contralor

Por:

RELACIÓN DETALLADA DE HALLAZGOS

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO

En nuestros informes de auditoría se incluyen los hallazgos significativos determinados por las pruebas realizadas. Éstos se clasifican como principales o secundarios. Los principales incluyen desviaciones de disposiciones sobre las operaciones de la unidad auditada que tienen un efecto material, tanto en el aspecto cuantitativo como en el cualitativo. Los secundarios son los que consisten en faltas o errores que no han tenido consecuencias graves.

Los hallazgos del informe se presentan según los atributos establecidos conforme a las normas de redacción de informes de nuestra Oficina. El propósito es facilitar al lector una mejor comprensión de la información ofrecida. Cada uno de ellos consta de las siguientes partes:

Situación - Los hechos encontrados en la auditoría indicativos de que no se cumplió con uno o más criterios.

Criterio - El marco de referencia para evaluar la situación. Es principalmente una ley, reglamento, carta circular, memorando, procedimiento, norma de control interno, norma de sana administración, principio de contabilidad generalmente aceptado, opinión de un experto o juicio del auditor.

Efecto - Lo que significa, real o potencialmente, no cumplir con el criterio.

Causa - La razón fundamental por la cual ocurrió la situación.

Al final de cada hallazgo se hace referencia a las recomendaciones que se incluyen en el informe para que se tomen las medidas necesarias sobre los errores, irregularidades o actos ilegales señalados.

En la sección sobre los **COMENTARIOS DE LA GERENCIA** se indica si el funcionario principal y los ex funcionarios de la unidad auditada efectuaron comentarios sobre los hallazgos incluidos en el borrador del informe que les envía nuestra Oficina. Dichos comentarios se consideran al revisar el borrador del informe y se incluyen al final del hallazgo

correspondiente en la sección de HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DE RECREACIÓN Y DEPORTES, de forma objetiva y conforme a las normas de nuestra Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, éste prevalece y se añade al final del mismo la siguiente aseveración: Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DE RECREACIÓN Y DEPORTES

Los **hallazgos** de este **Informe** se clasifican como principales.

Hallazgo 1 - Computadoras y cuentas para acceder a Internet y al correo electrónico utilizadas para fines ajenos a la gestión pública, y falta de actualización de las definiciones del programa antivirus instalado en las computadoras

a. Al 8 de agosto de 2007 el Departamento tenía 381 computadoras. El examen realizado del 9 de enero al 11 de marzo de 2008 sobre el uso de 16 computadoras reveló las siguientes faltas de control:

1) Ocho computadoras[4] contenían archivos ajenos a la gestión pública.

2) Cinco computadoras[4] se utilizaron para examinar páginas de Internet con contenidos ajenos a la gestión pública.

3) Ocho computadoras[4] se utilizaron para recibir y enviar mensajes de correo electrónico con contenido ajeno a la gestión pública.

4) Siete computadoras[4] no tenían actualizadas las definiciones[5] (*virus definitions file*) del programa antivirus.

---

[4] Una relación de las computadoras se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al Secretario y al ex Secretario de Recreación y Deportes.

[5] Archivos que contienen información sobre las características y el comportamiento de los virus que afectan los sistemas computadorizados.

b. Al 9 de noviembre de 2007 el Departamento mantenía un servidor[6] que permitía acceso a Internet a los usuarios autorizados. A dicha fecha el Departamento tenía 129 cuentas para acceder a Internet. El servidor producía diariamente un archivo en el cual se registraban todas las páginas de direcciones de Internet que fueron accedidas por las cuentas de usuarios. El examen del registro de direcciones de Internet visitadas por los usuarios y registradas en el servidor del 26 al 30 de noviembre de 2007 reveló que 31 cuentas de acceso de usuarios[7] se utilizaron para acceder páginas de Internet con contenidos ajenos a la gestión pública[8].

En la **Sección 9 del Artículo VI de la Constitución del Estado Libre Asociado de Puerto Rico** 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.

En 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, se dispone, entre otras cosas, que ningún funcionario o empleado público utilizará propiedad pública para obtener directa o indirectamente ventajas, beneficios o privilegios que no estén permitidos por ley.

En el **Artículo 6, Titularidad y Derechos, del Reglamento sobre Uso de Computadoras del Departamento de Recreación y Deportes**, aprobado el 3 de octubre de 2007 por el Secretario de Recreación y Deportes, se establece que las computadoras, los servicios asociados internos y externos, el sistema de correspondencia electrónica (*e-mail*), la red

---

[6] El nombre del servidor se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al Secretario y al ex Secretario de Recreación y Deportes.

[7] La relación de las cuentas de acceso de los usuarios se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al Secretario y al ex Secretario de Recreación y Deportes.

[8] Dicha información se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al Secretario y al ex Secretario de Recreación y Deportes.

interna, el acceso a Internet, y los documentos y programas que existen en la misma, son propiedad del Departamento y sólo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones o poderes de éste.

Además, en el **inciso b. del Artículo 9, Políticas Sobre Uso de Internet y Correo Electrónico**, de dicho **Reglamento** se establece que se prohíbe el uso de los sistemas de información y comunicaciones (Internet y/o correo electrónico) para manejo de negocios o asuntos privados del usuario o para la utilización y el envío de mensajes en cadena. De igual forma, el usuario no podrá utilizar el recurso electrónico para tener acceso a juegos, concursos, encuestas, páginas de entretenimiento o cualquier otro servicio ajeno a sus funciones.

En la **Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico, de la Carta Circular Núm. 77-05** se establece que:

- Los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos son propiedad del Estado Libre Asociado de Puerto Rico, por lo que sólo pueden utilizarse para fines estrictamente oficiales y legales.

- Los sistemas de comunicación y el acceso a Internet son propiedad de la entidad gubernamental y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la entidad y nunca con fines no oficiales o para actividades personales o con fines de lucro.

- El correo electrónico podrá utilizarse únicamente para propósitos oficiales relativos a las funciones de la agencia. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro o en menoscabo de la imagen de la entidad gubernamental o sus empleados.

- Cada entidad gubernamental será responsable de verificar que el correo electrónico e Internet funcionen adecuadamente. También se asegurarán de que la información contenida en dichos sistemas esté protegida de accesos no autorizados. La agencia utilizará sistemas de protección contra virus y sistemas de protección contra accesos no autorizados (*firewall*).

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política pública que las agencias deberán instalar controles automáticos para la prevención y detección de programas no deseados, tales como: virus, *spyware*[9], *adware*[10] y *updates* automáticos. Esto implica que, como norma de sana administración, dichos programas deberán estar actualizados, de manera que los mismos puedan detectar y eliminar nuevas amenazas.

El uso de las computadoras y de las cuentas para acceder a Internet y al correo electrónico, pertenecientes al Departamento, para procesar documentos y examinar archivos de carácter privado, es contrario al interés público y desvirtúa los propósitos para los cuales fueron adquiridos. Además, provee al funcionario o empleado que indebidamente los utiliza unas ventajas, beneficios y privilegios que no están permitidos por ley. También los archivos ajenos a la gestión pública ocupan espacio y capacidad en los sistemas de información lo que afecta el rendimiento de los mismos para los propósitos oficiales del Departamento. **[Apartados del a.1) al 3) y b.]**

La falta de actualización en las definiciones del programa antivirus puede impedir la prevención y la detección de programas no deseados y permitir que éstos puedan propagarse a los sistemas de información, lo que afectaría la integridad, la confidencialidad y la disponibilidad de los sistemas de información del Departamento. **[Apartado a.4)]**

---

[9] 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.

[10] Programa que se instala inadvertidamente en una computadora y su principal propósito es desplegar ante el usuario anuncios y propaganda.

Las situaciones comentadas en los **apartados del a.1) al 3) y b.** se debían, en parte, a la falta de:

- Orientaciones periódicas a todos los usuarios de los equipos computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso de las computadoras, del correo electrónico e Internet.

- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento por los usuarios de las normas establecidas para el uso oficial de las computadoras, el correo electrónico y las cuentas para acceder a Internet.

- Análisis 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 Administrador de Redes limite el acceso sólo a las páginas autorizadas.

La situación comentada en el **Apartado a.4)** se debía a que el OPI no le requirió al Administrador de Redes que estableciera, para su consideración y aprobación, un proceso alterno automatizado o manual para las computadoras que confrontan problemas de actualización de las definiciones del programa de antivirus. Esto, para asegurarse de que dichas computadoras estén debidamente protegidas con la instalación de la última versión disponible de las definiciones del programa de antivirus.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas o que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

El ex Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Véanse las recomendaciones de la 1.a. a la c.2) y 2.

Hallazgo 2 - Falta de un Informe de Avalúo de Riesgos sobre los sistemas de información

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 21 de agosto de 2007 el Departamento no había realizado un avalúo de riesgos sobre los sistemas de información.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** 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.

Las mejores prácticas en el campo de la tecnología de información sugieren que se establezcan normas y procedimientos escritos para garantizar la integridad, la confidencialidad y la disponibilidad de los sistemas críticos, de modo que se garantice la continuidad de las operaciones en la eventualidad de que sucesos inesperados ocurran. Esto implica, entre otras cosas, que el Departamento desarrolle e implante un programa de avalúo y administración de riesgos para proteger y clasificar los mismos en términos de criticidad y sensitividad. Luego de la identificación y clasificación de los activos y recursos, se identifican los elementos de riesgos que podrían afectar los mismos, específicamente los sistemas de información, para entonces determinar la probabilidad de que las amenazas o los eventos ocurran y el impacto que tendrían en las operaciones.

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 del Departamento en caso de que surja alguna eventualidad. **[Véase el Hallazgo 4-a.]**

La situación comentada se atribuye a que los funcionarios del Departamento no se percataron de la importancia de la información que se recopila diariamente en el Departamento y de los riesgos que podrían afectar la confidencialidad, la integridad, la disponibilidad y el uso efectivo de la misma. Además, a que el Secretario no había

promulgado una directriz para la preparación del avalúo de riesgos de los sistemas de información, según lo establecido en la **Carta Circular Núm. 77-05**.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas o que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

El ex Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 3.

Hallazgo 3 - Falta de un Plan de Seguridad, de acuerdos de confidencialidad y de un procedimiento para el manejo de incidentes de seguridad sobre los sistemas de información

a. Al 21 de agosto de 2007 el Departamento 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[11]
- La evidencia de un análisis de riesgos actualizado, como 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 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)

[11] 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 probar la efectividad del **Plan de Seguridad**.

- La documentación de la interconexión de los sistemas.

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. 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 para que se actualicen los conocimientos 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.

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

- Pérdidas de vidas humanas

- 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.

La situación comentada se atribuye a que el Secretario no había promulgado una directriz para la preparación del **Plan de Seguridad**.

b. Al 3 de octubre de 2007 el Departamento no había establecido acuerdos de confidencialidad con los empleados ni con los contratistas antes de exponerlos a información confidencial u otros activos sensitivos.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece, entre otras cosas, que las agencias o departamentos establecerán controles en el reclutamiento del personal de sistemas de información, especialmente para el área de seguridad que requieran que éste firme acuerdos de no divulgación o confidencialidad antes de exponerlo a información confidencial u otros activos sensitivos como los programas y los equipos.

La situación comentada podría dar lugar al uso indebido de información privilegiada y a que de esto ocurrir se dificulte fijar responsabilidades. Esto, a su vez, resultaría en otras consecuencias adversas para el Departamento.

c. Al 6 de noviembre de 2007 la OSI no tenía un procedimiento para el manejo de incidentes donde se estableciera, entre otras cosas, una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece, entre otras cosas, que las agencias tendrán la responsabilidad de desarrollar procedimientos para detectar, informar y responder a incidentes de seguridad incluidos los límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta. Además, se establece que todos los empleados y los contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.

La situación comentada le impide a la OSI tener un control eficaz y documentado sobre el manejo de incidentes. Además, puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

Las situaciones comentadas en los **apartados b. y c.** obedecen, principalmente, a que el Secretario no le había requerido al OPI que desarrollara y sometiera para su consideración y aprobación las normas y los procedimientos escritos necesarios para establecer acuerdos de confidencialidad escritos y para el manejo de incidentes.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas o que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación de la 1.d.1) a la 3).

Hallazgo 4 - Falta de un Plan de Continuidad de las Operaciones, de acuerdos escritos para mantener un centro alterno y de una fuente de energía alterna

a. Al 6 de noviembre de 2007 el Departamento carecía de un **Plan de Continuidad de Negocios** que incluyera los planes específicos, completos y actualizados de la OSI. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la OSI en caso de riesgos como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros.

   En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que las agencias deberán 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**.

   La situación comentada podría propiciar la improvisación, y que en casos de emergencia se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, e interrupciones prolongadas de los servicios a los usuarios del Departamento.

   La situación comentada se atribuye a que el Secretario no le había requerido al OPI que efectuara un avalúo de riesgo sobre los sistemas de información **[Véase el Hallazgo 2]** que sirviera de base para el desarrollo, la aprobación y la implantación de un **Plan de Continuidad de Negocios**. Éste debe contener un **Plan para la Continuidad de las Operaciones** y un **Plan para la Recuperación de Desastres**, con el fin de que sirvan como herramientas para responder ante cualquier incidente o desastre que ocurra.

b. Al 30 de octubre de 2007 el Departamento no había formalizado acuerdos con otra entidad para establecer, en las instalaciones de ésta, un centro alterno de sistemas de información que permita restaurar las operaciones computadorizadas en casos de emergencia.

Como norma generalmente aceptada en el campo de la informática se requiere que como parte integral del **Plan de Continuidad de Negocio** deben existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. Debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la agencia, podrían ser los siguientes:

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

La situación comentada podría afectar las funciones del Departamento y los servicios de la OSI, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o de un 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.

La situación comentada se debía a que el OPI no había coordinado la identificación de un lugar disponible y adecuado como centro alterno para formalizar los acuerdos escritos necesarios para utilizar el mismo para la recuperación de información en caso de desastre o de alguna emergencia.

c. Al 25 de octubre de 2007 no se había instalado una fuente de energía alterna que asegurara la continuidad de las operaciones de la OSI en caso de fallas prolongadas en el servicio de energía eléctrica.

Las mejores prácticas en el campo de la tecnología de información sugieren que en las instalaciones de sistemas de información se deben mantener fuentes de energía alternas que garanticen la continuidad de las operaciones ante la ausencia de electricidad durante períodos prolongados.

La situación comentada podría ocasionar que se afecten los usuarios y la prestación de los servicios que brinda el Departamento de surgir interrupciones prolongadas en el servicio eléctrico.

La situación comentada se atribuye a que en el Departamento no se había considerado la posibilidad de adquirir una fuente de energía alterna para la OSI.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas o que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

El ex Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Véanse las recomendaciones 1.d.4), 4 y 5.

Hallazgo 5 - Deficiencias en los parámetros de seguridad de los servidores del Departamento para controlar las cuentas de acceso a los recursos de la Red

a. En noviembre de 2007 la OSI tenía en operación 10 servidores. El examen efectuado sobre los parámetros de control de acceso y de seguridad definidos en el sistema operativo de 9 servidores[12] del Departamento reveló las siguientes deficiencias en la utilización de las opciones que permiten controlar la seguridad local de las cuentas de los usuarios:

1) En la pantalla *Account Policies* de los 9 servidores[12] existían deficiencias en la activación de las políticas relacionadas con las cuentas de acceso, según se indica:

a) No se había definido el mínimo de caracteres requeridos para establecer las contraseñas de las cuentas de acceso de los usuarios (*Minimum Password Lenght*).

[12] La relación de los servidores se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al Secretario y al ex Secretario de Recreación y Deportes.

b) No se requería un mínimo de 10 días para que el sistema le permitiera al usuario cambiar la contraseña nuevamente (*Minimum Password Age*).

c) No se requería un mínimo de cinco contraseñas diferentes antes de volver a utilizar la misma (*Enforce Password History*).

d) Luego de tres intentos de acceder a los recursos de la Red sin éxito, la cuenta de acceso se desactivaba sólo por media hora (*Account Lockout Duration*).

e) Se había definido media hora en la instrucción para reiniciar el conteo de intentos para acceder a los recursos de la Red sin éxito (*Reset account lockout counter alter*).

2) En dos servidores[12] no se había activado la política de auditoría (*Audit Policy*) para que el sistema produzca un registro cuando ocurran los siguientes eventos:

- El encendido y apagado de la computadora (*Restart and Shutdown*)
- El acceso a archivos y objetos (*File/Object Access*)
- El seguimiento de los procesos (*Process Tracking*)
- Los cambios a las políticas de seguridad (*Security Policy Changes*)
- La administración de usuarios o grupos (*User/Group Management*)
- El acceso al directorio de servicio (*Directory Service Access*)

3) En el servidor que proveía el servicio de correo electrónico no se había activado la opción *Message Tracking*. Dicha opción permite producir un informe para identificar los usuarios que han enviado o recibido mensajes de correo electrónico mediante la Red. Además, los usuarios podían recibir y enviar mensajes de correo electrónico de fuentes externas al Departamento sin restricción.

b. El examen efectuado el 9 de noviembre de 2007 al servidor principal reveló que:

1) La contraseña de la cuenta de acceso con privilegios de administrador no se había cambiado en 611 días.

2) No se habían eliminado del servidor principal cinco cuentas de ex empleados que cesaron sus funciones del 1 de enero al 30 de septiembre de 2007.

En el **Inciso 2 del Artículo 8, Medidas de Seguridad, del Reglamento sobre Uso de Computadoras del Departamento de Recreación y Deportes**, se establece que las contraseñas deberán mantenerse en estricta confidencialidad y que el usuario deberá cambiarlas cada 90 días, o cuando sea necesario. Además, se establece que las contraseñas deberán contar con seis caracteres de longitud como mínimo y que no podrán ser igual a las últimas cinco que haya tenido el usuario.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política pública que las entidades gubernamentales 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. También se establece que si existe la necesidad de acceder a la Red desde afuera de las instalaciones de la agencia (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación mediante Internet), deberán existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información. Además, se establece 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. 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. Esta norma 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 asignación de códigos y contraseñas de autorización únicas y confidenciales para cada usuario que garantice un nivel óptimo de seguridad en los sistemas computadorizados

- La notificación inmediata al encargado de la seguridad de datos del cese de un usuario en sus funciones por motivo de renuncia, separación o traslado para la cancelación de su cuenta de acceso

- Renovación periódica de la contraseña de cada usuario, según las necesidades de la agencia y los procedimientos establecidos.

En la **Política Núm. TIG-008 de la Carta Circular Núm. 77-05** se establece que cada agencia será responsable de establecer las normas mediante las cuales se asignan las cuentas de acceso y las contraseñas, los controles de acceso al servidor y los sistemas para auditar el uso del sistema, la integridad y la seguridad de los datos y las comunicaciones enviadas.

Las situaciones comentadas en los **apartados a.1) y b.** propician que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de ésta. 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.

La situación comentada en el **Apartado a.2)** impide al Departamento mantener un registro de los eventos inusuales o problemas ocurridos en la Red que le permitiera al Administrador de Redes tomar a tiempo las medidas correctivas o preventivas necesarias.

La situación comentada en el **Apartado a.3)** impide al Departamento mantener un control efectivo de los mensajes de correo electrónico que se reciben y se envían de fuentes externas.

Las situaciones comentadas en los **apartados a. y b.1)** se debían a que el OPI no se había asegurado de que se activaran las opciones de seguridad de acceso lógico que provee el sistema operativo y la opción *Message Tracking*. Además, a la falta de análisis para

determinar los funcionarios y los empleados a quienes debían otorgarse los privilegios para recibir y enviar mensajes de correo electrónico de fuentes externas, de acuerdo con las necesidades del Departamento y con los deberes y las responsabilidades de sus puestos. Esto, para que el encargado de administrar la Red configure las cuentas de los usuarios.

La situación comentada en el **Apartado b.2)** se debe a que no existían procedimientos escritos que les requirieran a los empleados de la Secretaría Auxiliar de Recursos Humanos y Relaciones Laborales informarle a la OPI el cese de un usuario en sus funciones por motivo de renuncia, separación o traslado para proceder con la cancelación de su cuenta de acceso.

El Secretario informó en la carta que nos envió, entre otras cosas, que en los servidores que no son *domain controllers* sólo estaban activadas las cuentas de servicio y la del administrador local. **[Apartado a.1)]** Además, informó las medidas implantadas y las que se proponía implantar para corregir las situaciones comentadas en los **apartados a.2) y 3), y b.**

El ex Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Consideramos las alegaciones del Secretario respecto al **Apartado a.1)**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones de la 1.c.3) a la 7) y e., 6 y 7.

Hallazgo 6 - Falta de revisiones periódicas a los registros de eventos producidos en el servidor principal

a. Al 1 de noviembre de 2007 el Administrador de Redes no efectuaba revisiones periódicas del registro de eventos (*Log File*) de las aplicaciones de sistemas que produce el servidor principal, ni de los intentos de acceso a la Red. Esto era necesario para conocer las posibles violaciones de seguridad que pudieran ocurrir en los sistemas de información de la Red y tomar prontamente las medidas preventivas y correctivas necesarias.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política pública que las entidades gubernamentales 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, se establece que será responsabilidad de cada agencia 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. Esta norma se instrumenta, en parte, mediante la revisión continua por el personal técnico especializado de los informes en los que se registran todos los eventos de seguridad de la Red.

La situación comentada impide la detección temprana de intentos no autorizados, errores críticos o problemas con los servidores y con la Red lo que no permite tomar de inmediato las medidas preventivas y correctivas necesarias. Además, priva al Departamento de las herramientas necesarias para supervisar eficazmente los trabajos realizados por los usuarios, y detectar el acceso y uso indebido de los sistemas computadorizados.

La situación comentada se atribuye a que el OPI no se había asegurado de que el Administrador de Redes examinara periódicamente el registro de eventos que produce el servidor principal y los intentos de acceso a la Red.

El Secretario, en la carta que nos envió informó, entre otras cosas, que:

> La Oficina de Sistemas de Información revisa periódicamente el registro de eventos (Log File) de las aplicaciones de sistema que produce el servidor principal y los accesos a la Red. Sin embargo, no existía un proceso de documentación que valide dicho proceso. Impartiremos instrucciones para que se documente el proceso de revisión de registro de eventos adecuadamente.

El ex Secretario, en la carta que nos envió informó, entre otras cosas, que:

> La información provista por los funcionarios encargados del sistema de información del Departamento refleja que se cumplía cabalmente con las revisiones a los registros de eventos. Evidencia de que dicha revisiones se realizaban, son las cartas circulares impartiendo instrucciones sobre el adecuado uso de los sistemas y las amonestaciones

por deficiencias en la utilización de los sistemas en violación de la reglamentación establecida por el Departamento (*sic*). Este trabajo era realizado por la OSI del Departamento.

Consideramos las alegaciones del ex Secretario, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.c.8).

Hallazgo 7 - Deficiencias relacionadas con la configuración y la estructura de acceso a la Red, y con la documentación de la estructura de la Red del Departamento

a. El examen realizado el 1 de noviembre de 2007 a la configuración y a la estructura de seguridad establecida para acceder a la Red del Departamento a través de Internet, reveló que no se había establecido como medida de seguridad una Zona Desmilitarizada. Esto, para brindar a la Red interna del Departamento una protección que minimice los riesgos de que la información sea accedida de forma no autorizada.

b. La documentación de la estructura de la Red del Departamento suministrada para examen durante nuestra auditoría no contenía la siguiente información:

- El detalle de las computadoras y los servidores conectados a la Red, con sus respectivas identificaciones y localizaciones
- La ubicación de todos los cuartos de distribución del cableado
- La descripción del equipo de comunicación ubicado en los cuartos de distribución del cableado de los diferentes pisos del Departamento
- La instalación y la configuración del sistema operativo de cada computador principal

- La instalación y la configuración de los *switches*[13], del *firewall*[14] y de los *routers*[15]

- La aprobación por la alta gerencia.

En la **Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular 77-05** se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar e implantar 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.

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 de 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.

La situación comentada en el **Apartado a.** propicia que personas no autorizadas puedan lograr acceso mediante Internet a información confidencial y, a la vez, comprometan la seguridad de los equipos de la Red por el uso indebido de ésta.

La situación comentada en el **Apartado b.** impide al Departamento tener una comprensión clara y precisa de los componentes de la Red y dificulta mantener un control eficiente y

---

[13] Dispositivos de comunicación central que conectan dos o más segmentos de red y permiten que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

[14] Sistema que se coloca entre una red de comunicaciones e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad y autentificación, entre otros.

[15] Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza a base de la información de nivel de red y tablas de direccionamiento.

efectivo en la administración y el mantenimiento a la misma. Además, dificulta la atención de problemas de conexión en un tiempo razonable y que se planifique efectivamente las mejoras a la Red, según el crecimiento de sus sistemas.

La situación comentada en el **Apartado a.** se debía, en parte, a que el OPI no había ejercido una supervisión eficaz sobre el Administrador de Redes para que configurara la Red del Departamento con los criterios básicos de una estructura de seguridad.

La situación comentada en el **Apartado b.** se atribuye a que el OPI no había establecido los controles para documentar adecuadamente la Red.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas o que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

El ex Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 1.f. y g.

Hallazgo 8 - Falta de normas y de procedimientos escritos para la administración y la seguridad de los sistemas de información computadorizados del Departamento

a. Al 21 de agosto de 2007 el Departamento no había promulgado normas y procedimientos escritos necesarios para reglamentar los siguientes procesos de la OSI:

- El mantenimiento a los equipos computadorizados y la administración de problemas y cambios para prevenir interrupciones no esperadas
- La preparación, la identificación, la protección y los períodos de retención de los respaldos (*backups*) de información
- Los criterios de clasificación de los recursos de tecnología de información
- La administración y el control del acceso lógico a los sistemas de información

- La prevención y la detección de los accesos no autorizados
- La administración de la seguridad y el control de acceso físico a la OSI y al equipo de sistemas de información
- La disposición de información sensitiva y de programas, antes de transferir o disponer de un equipo o de un medio de almacenamiento de información.

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. Será responsabilidad de cada entidad gubernamental desarrollar normas específicas que consideren las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. 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 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 casos de renuncias o ausencias del personal de mayor experiencia y facilitan la labor de adiestramiento.

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

La situación comentada se atribuye a que el OPI no había preparado y sometido para la aprobación del Secretario, las normas y los procedimientos que debían regir las operaciones de la OSI.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

El ex Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 1.d.5).

Hallazgo 9 - Falta de controles sobre los equipos computadorizados

a. El examen realizado del 9 de enero al 19 de marzo de 2008 sobre el uso de 26 computadoras del inventario de equipo computadorizado del Departamento reveló las siguientes faltas de control:

1) En 7 de éstas (27 por ciento) existían discrepancias en cuanto a la localización física y la indicada en el inventario de equipo computadorizado, según se indica:

NÚMERO DE PROPIEDAD	LOCALIZACIÓN SEGÚN INVENTARIO	LOCALIZACIÓN FÍSICA
36340	Región de Caguas	Almacén de Propiedad
38886	Secretaría Auxiliar para el Deporte de Alto Rendimiento	"
40510	Oficina de Sistemas de Información	Región de Guayama
40654	División de Finanzas	Almacén de Propiedad
41778	Oficina del Secretario	Oficina de Asuntos Gallísticos
41979	Oficina de Sistemas de Información	Región de Arecibo
41989	Secretaría Auxiliar de Recursos Humanos y Relaciones Laborales	Región de Ponce

2) Tres computadoras (12 por ciento) identificadas con los números de propiedad 36317, 36325 y 36356 no fueron localizadas para examen.

En la **Ley Núm. 230** se establece como política pública que la custodia, el cuidado y el control físico de la propiedad pública será responsabilidad del jefe de la propia dependencia o entidad corporativa o su representante autorizado.

En el **Reglamento Núm. 11** se establecen las normas básicas relacionadas con el recibo, la custodia, el control y la contabilidad de los activos fijos que adquieran las agencias que tienen sus fondos bajo la custodia del Secretario de Hacienda. En el **Artículo VI-A-3** de dicho **Reglamento** se establece, entre otras cosas, que el Encargado de la Propiedad será responsable de mantener al día todos los expedientes relacionados con el activo fijo.

Las situaciones comentadas impiden mantener un control adecuado sobre la propiedad y pueden propiciar el uso indebido o la pérdida de la misma, sin que se pueda detectar a tiempo para fijar responsabilidades. Además, dificultan la identificación y la localización de los equipos y le resta confiabilidad a la información existente en el sistema de inventario. También dificultan nuestra gestión fiscalizadora.

Las situaciones comentadas se debían a que el Encargado de la Propiedad no cumplió con la reglamentación establecida.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas o que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

El ex Secretario informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 8.

Hallazgo 10 - Falta de un registro de programas instalados en cada computadora

a. Al 31 de marzo de 2008 la OSI no mantenía un registro de los programas adquiridos e instalados en cada computadora que incluyera, entre otras cosas, 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 y el costo de los mismos.

En la **Política TIG-008 de la Carta Circular Núm. 77-05** se establece que los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas agencias y sólo pueden utilizarse para fines estrictamente oficiales y legales. Además, los programas y los recursos utilizados en los sistemas de información de las entidades gubernamentales deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas sólo podrán ser instalados por el personal autorizado. Además, no podrán instalarse programas sin la autorización previa del Departamento de Sistemas de Información, aunque sean programas libre de costo.

No cumplir con la disposición mencionada impide ejercer un control eficaz de los programas y las licencias correspondientes. 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 Departamento. También dificulta nuestra gestión fiscalizadora.

La situación comentada se debía a que el OPI no había tomado las medidas necesarias para mantener un registro y un control adecuado de los programas adquiridos e instalados en las computadoras del Departamento.

El Secretario informó en la carta que nos envió, entre otras cosas, las medidas que se proponía implantar para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 1.h.

Hallazgo 11 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información

a. Al 29 de agosto de 2007 la Oficina de Auditoría Interna del Departamento no había efectuado auditorías de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados.

En las 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 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 al gobierno, las operaciones y los 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.

La falta de fiscalización y de recomendaciones sobre los procedimientos, los controles 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.

Esta situación se debía a que la Oficina de Auditoría Interna del Departamento no contaba con personal suficiente y adiestrado en el área de auditoría de sistemas de información.

El Secretario informó en la carta que nos envió, entre otras cosas, que actualmente la Oficina de Auditoría Interna realiza monitorías sobre el uso y el control de los sistemas de

información junto con personal de la OSI. Además, esa oficina ha integrado cursos de informática en su plan de adiestramientos con el propósito de capacitar a su personal y poder participar activamente en la evaluación de todos los controles relacionados con dicha área.

Véase la Recomendación 9.

ANEJO

DEPARTAMENTO DE RECREACIÓN Y DEPORTES

OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Dr. David E. Bernier Rivera	Secretario	1 jun. 07	27 may. 08
Sra. Luz M. Molinari García	Subsecretaria	1 jun. 07	27 may. 08
Sr. Javier Rodríguez Rivera	Secretario Auxiliar de Administración	1 jun. 07	27 may. 08
Lic. Jennifer Rodríguez Collazo	Secretaria Auxiliar de Recursos Humanos y Relaciones Labores	1 jun. 07	27 may. 08
Sr. Martín Rafaelle Ayala	Oficial Principal de Informática	1 jun. 07	27 may. 08
Sra. María C. Ortiz Navarro	Directora de Finanzas	1 jun. 07	27 may. 08
Sra. Hilda Sánchez Ríos	Directora Auxiliar de Auditoría Interna	1 jun. 07	27 may. 08