INFORME DE AUDITORÍA TI-09-01

3 de julio de 2008

OFICINA DEL GOBERNADOR

OFICINA DE SISTEMAS DE INFORMACIÓN

(Unidad 5375 - Auditoría 12864)

Período auditado: 16 de febrero al 30 de junio de 2006

CONTENIDO

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

3 de julio de 2008

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) de la Oficina del Gobernador 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.

Determinamos emitir varios informes de dicha auditoría. Este es el primer informe y contiene el resultado de nuestro examen del plan de seguridad y avalúo de riesgo, los controles de seguridad física y administrativos, y la evaluación de la continuidad del servicio establecidos en la OSI.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Oficina del Gobernador tiene, entre otras, las siguientes funciones: dirigir y velar por la implantación de la política y del programa de gobierno; coordinar y supervisar la labor de las agencias y de los departamentos ejecutivos; asesorar y mantener informado al Gobernador y a los funcionarios de los organismos gubernamentales de la Rama Ejecutiva; y coordinar la labor del Gobernador con el Gobierno de los Estados Unidos. Para realizar sus funciones dicha

Oficina se componía de la Oficina del Gobernador Propia, la Oficina de la Primera Dama, la Secretaría de la Gobernación y otras 13 oficinas[1].

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

La OSI estaba adscrita a la Oficina de Administración y el Director de ésta le respondía directamente al Administrador de la Oficina del Gobernador. La OSI contaba, además, con un Subdirector, un Especialista en Sistemas de Información, un Analista en Sistemas de Información, un Técnico en Sistemas de Información y una Secretaria.

La Oficina del Gobernador cuenta con 10 servidores mediante los cuales se conectaban los equipos computadorizados ubicados en la Mansión Ejecutiva de La Fortaleza y en otros 8 edificios. Los sistemas computadorizados de la Oficina del Gobernador eran utilizados por 366 usuarios. También cuenta con una página de Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.fortaleza.gobierno.pr. Esta página provee información acerca de la entidad y de los servicios que presta.

Los gastos operacionales de la OSI eran sufragados del presupuesto operacional de la Oficina del Gobernador que para el año fiscal 2005-06 ascendió a $5,375,000.

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.

[1] Las oficinas de: (1) Justicia, Seguridad y Corrección; (2) Finanzas, Hacienda, Gerencia y Presupuesto; (3) Infraestructura, Transportación y Obras Públicas; (4) Cultura, Recreación, Deportes y Urbanismo; (5) Salud; (6) Planificación, Recursos Naturales y Calidad Ambiental; (7) Asuntos Legislativos; (8) Asuntos Federales; (9) Desarrollo Económico, Agricultura, Recursos Humanos y Trabajo; (10) Educación, Bienestar Social, Comunidades Especiales y Derechos Ciudadanos; (11) Asuntos Municipales y Vivienda; (12) Nombramientos Judiciales; y (13) Administración.

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 16 de febrero al 30 de junio de 2006. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias.

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

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne al plan de seguridad y avalúo de riesgo, los controles de seguridad física y administrativos, y la evaluación de la continuidad del servicio establecidos en la OSI no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 8**, clasificados principales.

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

RECOMENDACIONES

AL GOBERNADOR DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO

1. Tomar las medidas necesarias para asegurarse de que el Administrador de la Oficina del Gobernador cumpla con las **recomendaciones de la 3 a la 7** de este **Informe**. **[Hallazgos del 1 al 8]**

AL SECRETARIO DE JUSTICIA

2. Considerar la situación que se comenta en el **Hallazgo 1** de este **Informe** y tomar las medidas que correspondan. Además, tomar cualquier otra medida que considere de lugar respecto a los demás **hallazgos** de este **Informe**.

AL ADMINISTRADOR DE LA OFICINA DEL GOBERNADOR

3. Realizar las gestiones necesarias para enmendar el **Artículo 20: Fiscalización mediante Monitorías y Auditorías del Reglamento sobre Normas y procedimientos para el buen uso y manejo de los Sistemas Computadorizados de La Oficina del Gobernador (Reglamento)**, aprobado el 1 de febrero de 2006 por el Administrador de la Oficina del Gobernador, para que todos los equipos computadorizados de ésta estén accesibles para

examen por la Oficina del Contralor de Puerto Rico durante sus auditorías sobre el uso de los mismos y de los sistemas computadorizados. **[Hallazgo 1]**

4. Tomar las medidas necesarias para que se cumpla con lo establecido en 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, en lo concerniente a la seguridad de los sistemas de información, el análisis de riesgo y la continuidad de las operaciones. **[Hallazgos del 2 al 4]**

5. Ver que se cumpla con el **Reglamento** en lo concerniente a la seguridad física de los equipos computadorizados y las instalaciones del centro de cómputos principal y el alterno, el **Plan de Contingencias**, la cancelación de las cuentas de acceso cuando los usuarios cesan en sus funciones, el establecimiento de procedimientos internos, los adiestramientos sobre las normas de seguridad y la instalación de baterías para las computadoras de la Oficina del Gobernador. **[Hallazgos del 2 al 5, 7 y 8]**

6. Ejercer una supervisión eficaz del desempeño del Director de la OSI para asegurarse de que:

   a. Establezca los controles necesarios para que se corrijan las situaciones comentadas en los **hallazgos 2 y 3**, y se asegure de que las instalaciones de los equipos computadorizados sean ubicadas en lugares adecuados y seguros, y de que se protejan los equipos de las exposiciones ambientales.

   b. Revise el **Plan de Contingencias** y se asegure de que las medidas establecidas estén basadas en los riesgos y las vulnerabilidades incluidos en un informe de avalúo de riesgos que cumpla con lo requerido en la **Carta Circular Núm. 77-05**. **[Hallazgo 4-b.]**

   c. Adiestre al personal en cuanto al **Plan de Contingencias** y su responsabilidad cuando ocurra una emergencia; y vea que se efectúen simulacros para probar la efectividad de dicho **Plan**. **[Hallazgo 4-c.]**

d. Prepare las normas y los procedimientos necesarios para corregir las deficiencias comentadas en el **Hallazgo 5** y someta los mismos para su consideración y aprobación. Una vez aprobados, asegurarse de que se mantengan actualizados y se cumpla con éstos.

e. Mantenga un registro de los respaldos que le permita controlar y documentar adecuadamente la preparación de éstos y se asegure de que en las etiquetas utilizadas para identificar los cartuchos de respaldos se anote una descripción clara de los archivos respaldados, el nombre del servidor y la última fecha y hora de actualización de la información almacenada. **[Hallazgo 6]**

f. Elimine 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 7**.

g. Se asegure de que las computadoras estén conectadas a una batería para que, en caso de una falla del servicio de energía eléctrica, los usuarios puedan grabar los trabajos en proceso y apagar los equipos adecuadamente. **[Hallazgo 8-a.3)]**

7. Ver que la Directora de Recursos Humanos:

a. Notifique a tiempo al Director de la OSI el cese de un usuario en sus funciones para la cancelación de su cuenta de acceso. **[Hallazgo 7]**

b. Desarrolle y mantenga, en coordinación con el Director de la OSI, un programa continuo de adiestramientos al personal que incluya las orientaciones sobre las normas y los procedimientos relacionados con los sistemas de información computadorizados. **[Hallazgo 8-a.1) y 2)]**

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este **Informe** fue sometido para comentarios al Hon. Aníbal Acevedo Vilá, Gobernador del Estado Libre Asociado de Puerto Rico, en carta del 8 de febrero de 2008.

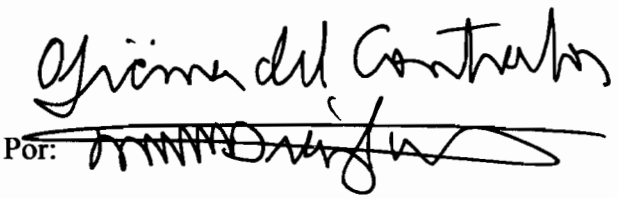
COMENTARIOS DE LA GERENCIA

El Sr. Kenneth Pérez Torres, Administrador Interino de la Oficina del Gobernador, sometió sus comentarios sobre el borrador de los **hallazgos** de este **Informe** en carta del 10 de marzo de 2008. Las observaciones sometidas por dicho funcionario fueron consideradas en la redacción final del informe. Algunas de las observaciones relacionadas con el **Hallazgo 1** se incluyen en la segunda parte de este **Informe** titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA OFICINA DEL GOBERNADOR. Relacionado con los **hallazgos del 2 al 8**, el Administrador Interino de la Oficina del Gobernador informó, entre otras cosas, que los mismos debían ser eliminados debido a que estaban protegidos por la doctrina del Privilegio Ejecutivo, de confidencialidad y de privilegio entre abogado y cliente. Además, informó que estos **hallazgos** se refieren a asuntos gerenciales y administrativos del sistema de información de la Oficina del Gobernador, los cuales nada tienen que ver con la función del Contralor de Puerto Rico de fiscalizar todos los ingresos, cuentas y desembolsos del Estado para determinar si se han hecho de acuerdo con la ley.

Diferimos de los comentarios del Administrador Interino de la Oficina del Gobernador porque las situaciones que se comentan en los **hallazgos del 2 al 8** tienen consecuencias fiscales que atañen a nuestra función fiscalizadora.

AGRADECIMIENTO

A los funcionarios y empleados de la Oficina del Gobernador les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

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 DE LA OFICINA DEL GOBERNADOR, 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 DE LA OFICINA DEL GOBERNADOR

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

Hallazgo 1 - Disposición reglamentaria que tiene el efecto de limitar el alcance en la selección de una muestra de la totalidad de los equipos computadorizados de la Oficina del Gobernador para los exámenes correspondientes

a. El **Reglamento sobre Normas y procedimientos para el buen uso y manejo de los Sistemas Computadorizados de La Oficina del Gobernador (Reglamento)** fue aprobado el 1 de febrero de 2006 por el Administrador de la Oficina del Gobernador. En el **Artículo 20: Fiscalización mediante Monitorías y Auditorías del Reglamento** se establece que:

> Los Sistemas Computadorizados adquiridos por la Oficina del Gobernador mediante compra, donación, confiscación, traspaso, permuta, cesión o por otros medios autorizados por ley así como la información desarrollada, transmitida o almacenada en estos sistemas, estarán accesibles para ser examinados y utilizados por personal autorizado de OSI o la Oficina del Contralor de Puerto Rico, excepto los sistemas del Gobernador, Asesores y Directores bajo la protección que le brinda el Privilegio del Ejecutivo y la información confidencial y el privilegio abogado-cliente.

Este **Artículo** está en contraposición con la **Sección 22 del Artículo III de la Constitución del Estado Libre Asociado de Puerto Rico**, el **Artículo 11 de la Ley Núm. 9 del 24 de julio de 1952**, según enmendada, y lo determinado por el Tribunal Supremo de Puerto Rico (Tribunal Supremo) en el caso **HMCA (PR) Inc. v. Colón Carlo, 133 D.P.R. 945, 964 (1993)** al limitar el alcance de nuestra auditoría de examinar el uso de las computadoras asignadas al Gobernador, sus asesores y directores.

En la **Sección 22 del Artículo III de la Constitución del Estado Libre Asociado de Puerto Rico** se autoriza al Contralor en el desempeño de sus deberes a tomar juramentos y declaraciones y a obligar, bajo apercibimiento de desacato, a la comparecencia de testigos y a la producción de libros, cartas, documentos, papeles, expedientes, y todos los demás objetos que sean necesarios para un completo conocimiento del asunto bajo investigación.

En el **Artículo Núm. 11 de la Ley Núm. 9** se dispone que los departamentos, agencias e instrumentalidades del Estado Libre Asociado de Puerto Rico y los municipios suministrarán al Contralor todos los documentos, expedientes e informes que éste solicite y darán acceso a los funcionarios y empleados de la Oficina del Contralor de Puerto Rico a todos sus archivos y documentos.

En el **Artículo 1 de la Ley Núm. 37 del 8 de enero de 2004** se establece que toda persona, funcionario público o privado, que voluntariamente retrasare, obstruyera o impidiera una auditoría o investigación que lleve a cabo la Oficina del Contralor de Puerto Rico, o cualquier funcionario designado por éste para llevar a cabo dicha gestión, cometerá delito grave y convicta que fuere, será sancionada con pena de reclusión por el término fijo de un (1) año, o pena fija de multa de $5,000, o ambas penas a discreción del Tribunal.

En el caso **López Vives v. Policía de Puerto Rico, 118 D.P.R. 219, 229 (1987)** el Tribunal Supremo estableció los criterios para determinar si procede un reclamo de confidencialidad por una entidad gubernamental. El mismo se configura cuando:

- Una ley así lo declara.
- La información está protegida por alguno de los privilegios evidenciarios que pueden invocar los ciudadanos.
- Revelar la información puede lesionar derechos de terceros.
- Se trate de la identidad de un confidente - **Regla 32 de Evidencia**.
- Sea información oficial conforme a la **Regla 31 de Evidencia**.

En el caso **HMCA (PR) Inc. v. Colón Carlo, 133 D.P.R. 945, 964 (1993)** el Tribunal Supremo determinó que:

> Es tarea germinal del Contralor determinar la legalidad de todas las cuentas, los ingresos y los desembolsos de propiedades y fondos públicos. Para la consecución de esta tarea nuestro ordenamiento le confiere un vasto poder para investigar. Según el preclaro imperativo constitucional, ese poder se extiende para requerir aquella evidencia testifical o documental que sea necesaria para el más cabal entendimiento de la materia bajo investigación. Por tanto, la autoridad del Contralor para requerir la producción de testimonio o documentos se determina según su pertinencia con su asunto legítimamente objeto de fiscalización...

Lo dispuesto en el **Artículo 20 del Reglamento** citado tiene el efecto de limitar el alcance en la selección de una muestra de la totalidad de los equipos computadorizados de la Oficina del Gobernador para los exámenes correspondientes[2].

La situación comentada se debía a que el **Artículo 20 del Reglamento** se había redactado basado en la protección que le brinda al Gobernador el privilegio del Ejecutivo y el privilegio de abogado-cliente. Esto, sin considerar, previo a su redacción, que el alcance de las auditorías de los sistemas de información computadorizados por parte de la Oficina del Contralor de Puerto Rico no va dirigida a evaluar la confidencialidad de las comunicaciones relacionadas con la implantación de la política pública del Gobernador, sino al uso de los equipos y sistemas computadorizados por la Oficina del Gobernador.

El Administrador Interino de la Oficina del Gobernador, en la carta que nos envió, informó lo siguiente:

> No cabe duda de que el Gobernador del Estado Libre Asociado de Puerto Rico y los Directores de sus oficinas pueden adoptar reglamentos para regular las actividades que se llevan a cabo en la Oficina del Gobernador. Dicha autorización surge de los poderes inherentes conferidos al Gobernador por virtud de la Sección 6 del Artículo IV de la Constitución del Estado Libre Asociado de Puerto Rico.

[2] Cualquier hallazgo relacionado con esta situación se incluirá en el próximo informe de esta auditoría.

> La doctrina del Privilegio Ejecutivo se refiere a la autoridad constitucional que tiene el Gobernador de no divulgar información confidencial bajo su poder, con la finalidad de que no se vea afectado el interés público y no se entorpezca la función ejecutiva constitucionalmente conferida por la Constitución.
>
> El sensitivo proceso de consultoría y de toma de decisiones inherente al descargue de las funciones constitucionales delegadas al Gobernador, sólo se puede cumplir efectivamente si se ejerce dentro de un manto de estricta confidencialidad. De ahí la necesidad de que todo el personal que realice estas funciones ejecutivas sea catalogado como personal de confianza...
>
> Los sistemas de información de los Asesores y Directores de la Oficina del Gobernador contienen información protegida por el privilegio de abogado-cliente. La norma de derecho de que todas las comunicaciones entre un cliente y su abogado son estrictamente confidenciales entre ellos y no pueden ser divulgadas a terceros, ni siquiera a los Tribunales de Justicia, es de aplicación en este caso.
>
> Los sistemas de información de la Oficina del Gobernador contienen información y comunicaciones sobre seguridad pública que debe mantenerse en estricta confidencialidad.

Consideramos las alegaciones del Administrador Interino, pero determinamos que el **Hallazgo** prevalece.

Véanse las recomendaciones de la 1 a la 3.

Hallazgo 2 - Falta de controles físicos y ambientales en el centro de cómputos principal y en el centro de cómputos alterno

a. Al 7 de marzo de 2006 la Oficina del Gobernador tenía un centro de cómputos principal y otro alterno. El examen efectuado entre el 7 de marzo y el 19 de mayo de 2006 de los controles ambientales[3] y físicos[4] en dichos centros de cómputos reveló que no se habían

[3] Controles diseñados para proteger las instalaciones y los equipos de eventos inesperados que ocurren naturalmente o son ocasionados por el hombre. Entre éstos, tormentas, erupciones volcánicas, huracanes, tornados, ataques terroristas, vandalismo, descargas eléctricas y fallas de equipo.

[4] Controles diseñados para proteger la organización y sus instalaciones contra accesos no autorizados por medio de sistemas de cerraduras, remoción de discos innecesarios y sistemas de protección del perímetro, entre otros.

establecido las condiciones de seguridad física[5] adecuadas para proteger los sistemas de información computadorizados de la Oficina del Gobernador, según se indica:

1) Relacionado con los controles ambientales:

   a) En el centro de cómputos principal no se restringía el consumo de alimentos para prevenir daños a los equipos computadorizados.

   b) Los paneles acústicos del techo del centro de cómputos principal tenían manchas de humedad que evidenciaban la existencia de filtraciones de agua en el área.

   c) El extintor portátil para combatir incendios, ubicado en el centro de cómputos alterno, no tenía el registro de inspecciones efectuadas para comprobar su funcionamiento.

2) Relacionado con los controles físicos:

   a) No se habían rotulado todos los puertos de los equipos de comunicaciones ubicados en el centro de cómputos principal y los cables conectados a éstos para identificar la ruta de conectividad. Además, los cables conectados a los equipos de comunicaciones de la Oficina del Gobernador y al *router*[6] de la Oficina de Gerencia y Presupuesto no se mantenían de forma organizada.

   b) Observamos que en el piso del centro de cómputos principal se mantenían varias cajas de cartón y equipo electrónico sin utilizar. Además, en el centro de cómputos alterno se mantenían varios equipos de comunicaciones encima de un archivo de

[5] Incluye los controles y procedimientos establecidos para proteger a las personas, la información, los equipos, los sistemas y las instalaciones al utilizar mecanismos de seguridad que incluyen el diseño y la ubicación de las instalaciones, los componentes ambientales, las medidas de respuesta de emergencia, el control de acceso, la detección de intrusos y la protección contra fuego y pérdida de energía.

[6] 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.

seguridad y en el piso un monitor y una caja de cartón que contenía cable y equipo periferal[7]. Esto denota falta de control de los equipos mantenidos en estos centros.

c) Se observó que la puerta que daba acceso al techo del edificio donde estaba localizado el centro de cómputos principal permanecía abierta. Dicha puerta estaba localizada en el pasillo que daba acceso a dicho centro.

d) En el centro de cómputos alterno se mantenía una fotocopiadora para uso de todos los empleados de la Oficina de Administración, lo que permitía el acceso de personal ajeno a las operaciones de la OSI.

Situaciones similares a las del **Apartado a.1)c) y 2)c)** fueron comentadas en el informe **Evaluación Sistemas de Información 2005, Diagnóstico y Recomendaciones**, emitido el 30 de junio de 2005 por una firma de consultores externos.

En la **Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05** se establece que el acceso a las facilidades de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas. En consonancia con dicha política pública, para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- Se controle adecuadamente el acceso de personas a dichas áreas.

- Se utilice equipo y tecnología adecuada para proteger los sistemas, tales como: detectores de humo, alarmas, sistemas de supresión de incendio, extintores portátiles inspeccionados anualmente, detectores de agua, sistemas de enfriamiento redundantes, sistemas alternos de electricidad, cerraduras y cámaras de seguridad.

- Se mantenga la temperatura y humedad requerida para el buen funcionamiento de los equipos.

[7] El equipo periferal es el equipo externo o interno que no es parte esencial de la computadora, la memoria y su microprocesador. Entre éstos se incluyen el *mouse*, teclado, monitor, impresora, unidades de disco externos (ZIP, CD y DVD) y escáner.

- Se establezcan las normas para prohibir consumir alimentos y mantener líquidos en estas instalaciones.

En el **Artículo 17: Instalación y Condiciones Ambientales para el Buen Funcionamiento de los Sistemas de Información Computadorizados del Reglamento** se establece que para garantizar el buen funcionamiento de los Sistemas de Información Computadorizados éstos deberán ser protegidos contra filtraciones, inundaciones y otras inclemencias del tiempo, incluida la exposición directa a la luz solar.

Además, en el **Artículo 18: Acceso a los Servidores en Sistemas en Redes del Reglamento** se establece que el acceso a los servidores debe estar restringido únicamente al administrador de la red y algún otro personal técnico que éste designe con la autorización del Director de la OSI. También se dispone que se deberán establecer procedimientos internos para el acceso a dicha área para cumplir con los parámetros de seguridad.

En la **Sección 1300.5**, **Extintores Portátiles para Combatir Incendios del Código para la Prevención de Incendios**, aprobado el 21 de junio de 1998 por el Jefe del Cuerpo de Bomberos de Puerto Rico se establece que, por lo menos, una vez al año los extintores deben ser examinados minuciosamente o recargados. Además, se debe fijar firmemente una tarjeta que indique cuándo y por quiénes fueron inspeccionados, recargados o reparados. También éstos deben ser inspeccionados por un técnico autorizado por el Cuerpo de Bomberos de Puerto Rico.

Las situaciones comentadas en el **Apartado a.1)** pueden propiciar daños a las instalaciones y los equipos, y provocar eventos de interrupción de servicios que afectarían la continuidad de las operaciones de los sistemas de información computadorizados de la Oficina del Gobernador. Además, pueden aumentar los costos de mantenimiento debido al deterioro prematuro de los equipos.

Las situaciones comentadas en el **Apartado a.2)a)** dificultaban la labor de mantenimiento que efectuaban los técnicos para resolver los problemas de comunicación e interrupciones de servicio, con los consiguientes efectos adversos como el retraso en las labores y el aumento en los costos relacionados.

Las situaciones comentadas en el **Apartado a.2)b) y c)** podían ocasionar la pérdida o el robo de equipo computadorizado e información de la Oficina del Gobernador.

Las situaciones comentadas en el **Apartado a.2)c) y d)** pueden propiciar que personas no autorizadas y ajenas a la OSI, por error o intención, causen daños al equipo o accedan indebidamente la información mantenida en los sistemas de información. Esto, a su vez, disminuye la confiabilidad de la información computadorizada, aumenta el riesgo de destrucción y divulgación indebida de información, dificulta la adjudicación de responsabilidades a las personas que cometan estos actos y afecta adversamente el funcionamiento de la Red y la continuidad de las operaciones.

Las situaciones comentadas se debían, en parte, a que el Director de la OSI no había tomado las medidas necesarias para que los equipos computadorizados estuvieran ubicados en lugares adecuados y seguros. Tampoco había cumplido con las normas citadas.

Véanse las recomendaciones 1 y de la 4 a la 6.a.

Hallazgo 3 - Falta de controles físicos y ambientales en las áreas donde estaban instalados los equipos de comunicaciones de la Red

a. El examen efectuado el 13 de marzo de 2006 de los controles ambientales y físicos de los equipos de comunicaciones de la Oficina del Gobernador[8] reveló que no se habían

[8] La localización de dichos equipos se incluyó en el borrador de los hallazgos del informe sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

preparado las condiciones de seguridad física adecuadas para proteger los sistemas de información computadorizados de la Oficina del Gobernador, según se indica:

1) Relacionado con los controles ambientales:

a) En la Oficina del Cuadro Telefónico se habían ubicado dos baterías encima del *switch*[9], lo que aumentaba la temperatura normal del equipo. Observamos que en esta área los cables conectados al *switch* no estaban protegidos con tubos o cubiertas y las conexiones de electricidad estaban instaladas en el techo de madera, lo que aumentaba el riesgo de incendio. Además, el extintor portátil para combatir incendios no se inspeccionaba desde julio de 2003.

b) En el Archivo Inactivo no se había instalado un acondicionador de aire mediante el cual se pudiera controlar la temperatura para la operación adecuada de los *switches*. Además, observamos que se había colocado un plástico sobre el gabinete de metal donde estaba instalado el equipo de comunicaciones. Esto, para protegerlo de daños que el agua, producto de filtraciones del techo, podía causar a los equipos.

c) En la Oficina de Fotografía no se había instalado un acondicionador de aire mediante el cual se pudiera controlar la temperatura para la operación adecuada de los *switches*. Además, observamos que en esta oficina se utilizaban productos químicos inflamables para el revelado de fotografías, lo que aumentaba el riesgo de incendios como consecuencia de las altas temperaturas.

d) El *switch* ubicado en la Oficina de Asuntos Federales estaba instalado sobre una batería que no le ofrecía estabilidad y podía afectar la temperatura normal del equipo. Observamos que el acondicionador de aire de dicha oficina se mantenía apagado, lo que podría afectar la temperatura para la operación adecuada del *switch*.

[9] Dispositivo de comunicación central que conecta dos o más segmentos de red y permite que ocurran transmisiones simultáneas, sin afectar el ancho de banda de la red para una comunicación más eficiente.

2) Relacionado con los controles físicos:

a) Los *hubs*[10] y *switches* estaban ubicados en áreas donde no se restringía el acceso de personal ajeno a las operaciones de la red, según se indica:

(1) Los *hubs* de la Oficina de Asuntos Legales, de la Oficina de Prensa y del Área del Retén se instalaron en estantes de metal abiertos y sin ninguna protección. Los *switches* de las oficinas de Asuntos Legislativos, de la Primera Dama, del Ayudante Administrativo y de Educación, del Archivo Inactivo y del Cuadro Telefónico también se instalaron en estantes de metal abiertos y sin ninguna protección.

(2) Un *switch* estaba instalado en un armario sin llave localizado en la Oficina del Ciudadano. Además, los cables conectados a este equipo se mantenían en el piso sin ser protegidos por tuberías o algún accesorio para la instalación segura de éstos. No se había restringido el acceso de los empleados o visitantes que podían interrumpir, de forma intencional o accidental, las conexiones o causar daños a los equipos.

(3) Un *switch* estaba localizado en un estante en el área de archivo de la Oficina de Asuntos Federales y otro estaba localizado en un estante en la Oficina de Servicios Generales donde se almacenaban accesorios de cocina y materiales y productos de limpieza que eran utilizados por los empleados asignados a esta oficina.

(4) Dos *hubs* estaban localizados en el piso de las dos oficinas de Desarrollo Económico (norte y sur). Uno de éstos se había caído detrás de un estante y el otro estaba al lado de una ventana abierta. Ambos equipos no estaban protegidos contra los daños que podían ser ocasionados por inundaciones, o la desconexión

[10] Dispositivo de comunicación que permite centralizar el cableado de una red.

de los cables que permitían la conexión entre las oficinas y los centros de cómputos.

(5) Un *hub* estaba instalado en el escritorio ubicado en la Cocina, sin protección y cubierto por varios materiales de oficina.

(6) Un *hub* ubicado en la oficina de Asuntos Legales y los *switches* ubicados en las oficinas de la Mansión Ejecutiva y del Ciudadano, y en el Cuadro Telefónico se habían instalado junto a los paneles telefónicos que eran accedidos por contratistas a cargo del mantenimiento de dicho servicio.

b) Los cables que se conectaban a los equipos de comunicaciones ubicados en las oficinas de la Primera Dama, de Prensa, de la Mansión Ejecutiva, del Ciudadano, de Desarrollo Económico y de Servicios Generales, en el Cuadro Telefónico, el Área del Retén y en la Cocina no habían sido rotulados. Ello es necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la Red en caso de interrupciones.

Situaciones similares a las del **Apartado a.2)a)** fueron comentadas en el informe **Evaluación Sistemas de Información 2005, Diagnóstico y Recomendaciones**.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que el acceso a las facilidades de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas. En consonancia con dicha política pública y para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- Se controle adecuadamente el acceso de personas a dichas áreas.

- Se utilice equipo y tecnología adecuada para proteger los sistemas, tales como: detectores de humo, alarmas, sistemas de supresión de incendio, extintores portátiles inspeccionados anualmente, detectores de agua, sistemas de enfriamiento redundantes, sistemas alternos de electricidad, cerraduras y cámaras de seguridad.

- No se utilice material y líquidos de limpieza inflamables en las instalaciones donde se ubica el equipo computadorizado.

- El alambrado se instale en paneles y conductos resistentes al fuego.

- Se mantengan la temperatura y humedad requeridas para el buen funcionamiento de los equipos computadorizados.

En el **Artículo 11: Protección de los Sistemas de Información Computadorizados del Reglamento** se establece que los sistemas de información computadorizados deben ser cuidados y utilizados correctamente para evitar daños y que los usuarios, funcionarios o empleados deberán, entre otras cosas, mantener el sistema que se le asigne limpio, en buenas condiciones y no deberán colocar objetos de ninguna clase encima de éstos.

En el **Artículo 17: Instalación y Condiciones Ambientales para el Buen Funcionamiento de los Sistemas de Información Computadorizados del Reglamento** se establece que para garantizar el buen funcionamiento de los Sistemas de Información Computadorizados éstos deberán:

- Ser ubicados en áreas seleccionadas cuidadosamente, que provean el espacio adecuado para todos los componentes del mismo. Además, el ambiente debe estar limpio, sin polvo, con suficiente ventilación y aire acondicionado.

- Ser instalados, de ser posible, lejos de ventanas y puertas.

- Ser protegidos contra filtraciones, inundaciones u otras inclemencias del tiempo, incluida la exposición directa a la luz solar.

- Estar fuera del alcance de intensos campos electromagnéticos producidos por dispositivos eléctricos como: acondicionadores de aire y ventiladores de gran tamaño.

En la **Sección 1300.5, Extintores Portátiles para Combatir Incendios del Código para la Prevención de Incendios** se establece que, por lo menos, una vez al año los extintores

deben ser examinados minuciosamente o recargados. Además, se debe fijar firmemente una tarjeta que indique cuándo y por quién fueron inspeccionados, recargados o reparados. También se establece que éstos deben ser inspeccionados por una persona que tenga una licencia, luego de probar ante el Cuerpo de Bomberos de Puerto Rico que está capacitado para realizar dicha tarea.

Las situaciones comentadas en el **Apartado a.1)** pueden propiciar daños a las instalaciones y los equipos, y provocar eventos de interrupción de servicios. Ello puede afectar la continuidad de las operaciones de los sistemas de información computadorizados de la Oficina del Gobernador. Además, pueden aumentar los costos de mantenimiento debido al deterioro prematuro de los equipos.

Las situaciones comentadas en el **Apartado a.2)a)** pueden propiciar que personas no autorizadas y ajenas a la OSI causen daños al equipo o accedan indebidamente la información mantenida en los sistemas de información. Esto, a su vez, disminuye la confiabilidad de la información computadorizada, aumenta el riesgo de destrucción y divulgación indebida de información, dificulta la adjudicación de responsabilidades a las personas que cometan estos actos y afecta adversamente el funcionamiento de la red y la continuidad de las operaciones. Además, puede ocasionar la pérdida o el robo de equipo computadorizado y de información de la Oficina del Gobernador.

La situación comentada en el **Apartado a.2)b)** dificultaba el trabajo de mantenimiento que efectuaban los técnicos para resolver los problemas de comunicación e interrupciones de servicio y aumentaba los costos relacionados con estos servicios.

Las situaciones comentadas se debían, en parte, a que el Director de la OSI no había tomado las medidas necesarias para que las instalaciones de equipos computadorizados estuvieran ubicadas en lugares adecuados y seguros. Tampoco había cumplido con las normas citadas.

Véanse las recomendaciones 1 y de la 4 a la 6.a.

Hallazgo 4 - Deficiencias en el Informe de Análisis, Manejo y Mitigación de Riesgos para la Oficina de Sistemas de Información de La Fortaleza y en el Plan de Contingencias

a. El examen del **Informe de Análisis, Manejo y Mitigación de Riesgos para la Oficina de Sistemas de Información de La Fortaleza (Informe)**, aprobado el 16 de marzo de 2006 por el Administrador de la Oficina del Gobernador, reveló las siguientes deficiencias:

1) No se incluyó la lista del inventario de los activos de sistemas de información. La misma debe contener la descripción de los equipos, programas y datos; su valoración y la clasificación de acuerdo con la misión y los servicios de la entidad.

2) No se incluyó información sobre las medidas de control establecidas para proteger cada uno de los activos de información ni se indicó si los controles existentes para mitigar el riesgo eran eficaces. En el **Informe** sólo se mencionaba, de forma general, cómo mitigar el riesgo.

3) No se completó el **Formulario de Identificación y Manejo de Riesgos** para la evaluación de los riesgos relacionados con fallas en las telecomunicaciones, daños a la información y programas, ataques maliciosos (propagación de virus electrónicos, accesos no autorizados y denegación de servicio, entre otros) y ataques mayores (artefactos explosivos y armas blancas y de fuego, entre otros).

4) Los por cientos de probabilidades de las amenazas presentados en los **formularios de Identificación y Manejo de Riesgos** que formaban parte del **Informe** no estaban sustentados por documentación, datos históricos o estudios realizados.

5) En los **formularios de Identificación y Manejo de Riesgos** no se indicó la persona asignada para dar mantenimiento a la **Hoja Matriz de Análisis y Evaluación de Riesgos** y responsable de informar los incidentes y dar seguimiento.

6) No se especificó el valor monetario del riesgo residual, luego de la implantación de los controles, que la Oficina del Gobernador estaba dispuesta a asumir o transferir a una compañía de seguros. Esto, basado en una comparación del valor del activo que podía

ser afectado por el riesgo residual, el beneficio de proteger el activo y el costo de la póliza de seguros.

b. El **Plan de Contingencia de la Oficina de Sistemas de Información (Plan de Contingencias)**, aprobado el 16 de marzo de 2006 por el Administrador de la Oficina del Gobernador, fue preparado el 10 de enero de 2006 por el Especialista en Sistemas de Información sin haberse aprobado el **Informe**, el cual contenía el resultado del avalúo de riesgo de los sistemas de información. El **Plan de Contingencias** no incluía los planes de acción para los riesgos de maremoto, interrupciones del acondicionador de aire, falta de acceso al edificio y al centro de cómputos, y hurto de equipo y de información. Éstos se habían incluido en el **Informe** como eventos importantes con entre un 25 y 75 por ciento de probabilidad de ocurrencia.

c. Al 20 de marzo de 2006 la Oficina del Gobernador no había efectuado simulacros del **Plan de Contingencias**, lo cual es necesario para probar su efectividad. Tampoco había adiestrado al personal en cuanto a las responsabilidades asignadas a éstos en una situación de interrupción o desastre.

Una situación similar a la del **Apartado c.** fue comentada en el informe **Evaluación Sistemas de Información 2005, Diagnóstico y Recomendaciones**.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece, como política pública, 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 o maliciosa. Además, se establece que se deberá realizar un análisis de riesgos que incluya:

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

- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido a los datos, entre 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.

Además, se establece que este análisis debe servir de base para desarrollar un **Plan de Continuidad de Negocios** que incluya un **Plan para Recuperación de Desastres** y un **Plan para la Continuidad de las Operaciones**.

En el **Artículo 19: Plan de Contingencias del Reglamento** se establece que para poder afrontar situaciones en las que se pueda afectar el funcionamiento del Sistema, que es parte de una red con servidores, los administradores de sistemas de información computadorizados deberán desarrollar, actualizar y practicar un **Plan de Respuestas de Emergencias y de Recuperación** o **Plan de Contingencias**. El **Plan** deberá garantizar la continuidad de la operación normal de los sistemas de información computadorizados cuando se presenten eventualidades inesperadas que afecten su funcionamiento.

En el **Plan de Contingencias** de la OSI se establece que uno de los objetivos relacionados con el **Plan** es adiestrar al personal en procedimientos de emergencia.

Las mejores prácticas utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados sugieren que:

- Como parte del proceso de administración de riesgos se deben identificar y clasificar los recursos de información, estudiar las amenazas y vulnerabilidades asociadas con cada recurso e identificar la probabilidad de que ocurran, para determinar el impacto de este riesgo. Posterior a esto se deben evaluar los controles existentes para desarrollar e implantar un **Plan de Seguridad** que permita reducir las vulnerabilidades hasta un nivel aceptable de riesgo y lograr un balance costo-efectivo entre los controles aplicados y las amenazas, las probabilidades y los riesgos identificados. Además, como parte del programa de administración de riesgo, se debe asignar la responsabilidad de desarrollar, implantar y dar seguimiento al **Plan de Administración de Riesgo**.

- Como parte del proceso de continuidad de operaciones los planes de contingencias deben ser ejecutados periódicamente en ejercicios de simulación, para determinar si éstos funcionan como se espera en situaciones de emergencia, y el personal asignado debe ser adiestrado sobre sus roles y responsabilidades en caso de ocurrir las mismas. Además, los resultados del ejercicio de simulación deben ser utilizados para efectuar los cambios necesarios al **Plan de Contingencias**, de forma que se garantice el funcionamiento adecuado de los centros alternos, que la información crítica y los programas puedan ser recuperados y que las capacidades de procesamiento de información puedan ser reanudadas prontamente.

La situación comentada en el **Apartado a.** impidió a la Oficina del Gobernador desarrollar e implantar un programa de seguridad adecuado y los controles necesarios para reducir los riesgos que afectan sus activos y operaciones en una base costo-efectiva.

La situación comentada en el **Apartado b.** impidió que la Oficina del Gobernador se asegurara de desarrollar un **Plan de Continuidad de Negocios** que incluyera estrategias apropiadas para recuperar las operaciones afectadas, a base de lo indicado en el informe de avalúo de riesgos.

La situación comentada en el **Apartado c.** podría propiciar la improvisación, y que en casos de emergencia, se tomen medidas inapropiadas y en forma desordenada. 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 Oficina del Gobernador.

Dichas situaciones ocurrieron, en parte, debido a que el Administrador de la Oficina del Gobernador no requirió que se efectuara el análisis de riesgos y se preparara el **Plan de Continuidad de Negocios**. Tampoco solicitó que se efectuaran simulacros para comprobar la efectividad del **Plan de Contingencias** y que se ofrecieran adiestramientos al personal asignado.

Véanse las recomendaciones 1, 4, 5, y 6.b. y c.

Hallazgo 5 - Falta de normas y procedimientos para la administración, la seguridad y el uso de los sistemas de información computadorizados de la Oficina del Gobernador

a. El examen de las normas y los procedimientos establecidos para regir las operaciones de la OSI[11] reveló que no contenían normas y procedimientos para:

- Mantener y actualizar la documentación de la configuración y topología[12] de la Red, incluidas las especificaciones de los servidores y demás componentes.
- Efectuar modificaciones a la composición o configuración de la Red.
- Crear y eliminar las cuentas de acceso de los usuarios de la Red.
- Mantener y actualizar un registro de los respaldos efectuados por la OSI.
- Mantener y actualizar un registro de programas y aplicaciones instalados en las computadoras de la Oficina del Gobernador e identificar instalaciones no autorizadas.
- Borrar información sensitiva y programas antes de disponer o transferir un equipo.
- Restaurar los programas y datos.

Tampoco contenían los procedimientos para:

- Preparar los respaldos de la información que no se mantiene en la red y especificar la frecuencia de estos respaldos, según requerido en el **Artículo 12: Resguardo de Información del Reglamento**.

---

[11] Éstos estaban incluidos en el **Reglamento**, el **Plan de Seguridad, Oficina de Sistemas de Información**, aprobado el 16 de marzo de 2006 por el Administrador de la Oficina del Gobernador, el **Informe de Análisis, Manejo y Mitigación de Riesgos para la Oficina de Sistemas de Información de La Fortaleza**, el **Plan de Contingencias**, el memorando sobre **Normas y Controles Para el Uso del Correo Electrónico e Internet**, emitido el 7 de octubre de 2002 por el Administrador de la Oficina del Gobernador; el memorando sobre **Normas y Controles Para el Uso de Sistemas de Información,** emitido el 14 de febrero de 2005 por el Administrador de la Oficina del Gobernador y el memorando sobre **Recordatorio Normas y Controles Para el Uso de Sistemas de Información** emitido el 18 de mayo de 2005 por el Administrador de la Oficina del Gobernador.

[12] Es la disposición física de cómo están conectadas las computadoras en la Red. Los ejemplos de topología incluyen el anillo, la estrella y el *bus*.

- Establecer los medios de disposición de documentos o informes confidenciales como parte del **Artículo 13: Disposición de Documentos del Reglamento**.

- Proteger los archivos con información confidencial contra la divulgación, manipulación o destrucción, según requerido en el **Artículo 8: Protección de la Información del Reglamento**.

- Verificar la existencia de virus en unidades removibles, según requerido en el **Artículo 14: Prevención de Virus de Sistemas de Información Computadorizados del Reglamento**.

- Dar mantenimiento a la correspondencia electrónica archivada en el servidor de correo electrónico según requerido en el **Artículo 29: Acceso a la Red Internet y Correo Electrónico del Reglamento**.

Una situación similar fue comentada en el informe **Evaluación Sistemas de Información 2005, Diagnóstico y Recomendaciones**.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política pública que las agencias deben establecer controles adecuados en sus sistemas de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Como parte de ello, deberán desarrollar y publicar normas y procedimientos aplicables que le permitan cumplir con la política pública.

En el **Artículo 18: Acceso a los Servidores en Sistemas en Redes del Reglamento** se dispone que el administrador de la red establecerá procedimientos internos para restringir el acceso al área de los servidores y cumplir con los parámetros de seguridad.

La situación comentada propicia que las medidas de control y las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme, lo que podría reducir su eficacia, afectar la continuidad de las operaciones y exponer la información a riesgos innecesarios. Además, ocasionó que el personal de la Oficina del Gobernador no cumpliera con las normas de seguridad relacionadas con la preparación de

respaldos (*backups*) de la información que no se mantenía en el servidor. **[Véase el Hallazgo 6]**

La situación comentada obedece, principalmente, a que el Administrador de la Oficina del Gobernador no había requerido al Director de la OSI que preparara y sometiera para su consideración y aprobación las normas y los procedimientos necesarios para reglamentar los procesos que se indican. Tampoco cumplió con las disposiciones del **Reglamento**.

Véanse las recomendaciones 1, 5 y 6.d.

Hallazgo 6 - Deficiencias relacionadas con la preparación e identificación de los respaldos de los archivos computadorizados de información

a. La OSI realizaba dos copias de los respaldos diarios, semanales, mensuales y anuales de los archivos computadorizados de información que se mantenían en los servidores de la Oficina del Gobernador. El respaldo principal era la copia que se mantenía en el centro de cómputos alterno y el respaldo secundario era la copia que se mantenía en una bóveda externa. El examen de los procedimientos utilizados por los empleados de la OSI para la preparación e identificación de los respaldos, reveló que:

1) La OSI no mantenía un registro de los respaldos preparados en el cual se detallara la descripción de los archivos respaldados, el nombre del servidor donde se mantenían estos archivos, la última fecha de actualización de la información y la explicación de fallas o situaciones especiales que ocurrieron, si alguno, durante la preparación de los respaldos. En su lugar, se utilizaba el formulario **Sistemas de Información** donde se anotaban los nombres de las personas que iban a hacer algún trabajo en los servidores. Cuando se preparaban los respaldos registraban la palabra *backup* en la columna de propósito de dicho formulario.

2) Al 7 de marzo de 2006 los cartuchos que se mantenían en el centro de cómputos alterno de la OSI, que contenían los respaldos diarios principales, no habían sido identificados con una etiqueta que incluyera una descripción clara de la información respaldada y la

fecha de actualización de la información almacenada. En la etiqueta del cartucho sólo se anotaba el día de la semana que se preparó el respaldo y el número de cartucho.

Una situación similar a la del **Apartado a.1)** fue comentada en el informe **Evaluación Sistemas de Información 2005, Diagnóstico y Recomendaciones**.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que las agencias deben establecer controles adecuados en sus sistemas de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Además, se establece que deberán existir procedimientos para tener y mantener una copia de respaldo (*backup*) recurrente de la información y de los programas de aplicación y de sistema esenciales e importantes para las operaciones de la agencia. En consonancia con dicha política pública es necesario, entre otras cosas, mantener un inventario detallado de las cintas de respaldos para facilitar su localización y para sustituir periódicamente, por cintas nuevas, las utilizadas para los respaldos y que permita, además, documentar el cumplimiento con las normas y los procedimientos establecidos. Las cintas o cartuchos también deben estar rotulados con la información que permita su pronta localización.

La situación comentada limitó el alcance de nuestro examen para determinar si los respaldos diarios principales y secundarios, semanales y mensuales se habían preparado con la regularidad requerida. Además, no mantener control de los respaldos podría ocasionar la pérdida permanente de información importante, con los consiguientes efectos adversos para las operaciones de la Oficina del Gobernador.

El Director de la OSI no había requerido al Subdirector de la OSI que:

- Preparara un registro de respaldos que le permitiera documentar la preparación de los respaldos y controlar los mismos. **[Apartado a.1)]**

- Identificara los cartuchos con la información necesaria para mantener un control adecuado de éstos. **[Apartado a.2)]**

Véanse las recomendaciones 1 y 6.e.

Hallazgo 7 - Deficiencias relacionadas con la cancelación de las cuentas de acceso a los sistemas de información cuando los empleados cesan en sus funciones

a. A la fecha de nuestro examen, 5 de abril de 2006, no se habían eliminado las cuentas de acceso de cinco empleados de la Oficina del Gobernador que cesaron en sus funciones entre el 28 de febrero y el 31 de marzo de 2006. A dicha fecha, entre 5 y 36 días posteriores a la fecha de separación, estas cuentas permanecían activas. La Ayudante Administrativa de la Oficina de Recursos Humanos notificó al Director de la OSI la separación de cuatro de estos empleados para la cancelación de las cuentas de acceso antes de la efectividad del cese. Para el otro empleado no se hizo la notificación.

   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 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.

   En el **Artículo 7: Control de Acceso a los documentos y programas del Reglamento** se establece que deberán observarse las siguientes normas para el uso y manejo de la información computadorizada:

   - El director(a) o el administrador de la red deberá asegurarse de que se inhabilite la contraseña cuando ocurra una renuncia o desplazamiento de algún usuario.

- Es política pública de la Oficina del Gobernador el permitir acceso a los programas, únicamente a aquellos usuarios que generan transacciones o documentos como parte del flujo de los servicios ofrecidos y que estén debidamente autorizados por el director de la oficina a la cual pertenecen.

La situación comentada puede ocasionar que personal que ha cesado en sus funciones acceda indebidamente la información mantenida en los sistemas de información, lo que aumenta el riesgo de destrucción o divulgación no autorizada de información y disminuye la confiabilidad de la información computadorizada.

La situación comentada se debió a que la Directora de Recursos Humanos no veló por que se notificara al Director de la OSI del cese de un usuario en sus funciones para la cancelación de su cuenta de acceso. Tampoco el Director de la OSI veló por que se cancelaran las cuentas de los empleados luego de recibir la notificación de la Oficina de Recursos Humanos, conforme a lo dispuesto en el **Reglamento**.

Véanse las recomendaciones 1, 5, 6.f. y 7.a.

Hallazgo 8 - Falta de adiestramientos continuos a los usuarios sobre el uso de los sistemas de información y las políticas de seguridad y otras deficiencias en la implantación de éstas

a. Sometimos un **Cuestionario sobre la satisfacción de los usuarios**[13] a 31 usuarios activos de los sistemas de información computadorizados de la Oficina del Gobernador,

[13] En dicho **Cuestionario** se solicita información, entre otras cosas, de las aplicaciones utilizadas, la implantación y los adiestramientos de las políticas de seguridad y la solución de problemas relacionados con el uso de los sistemas de información.

seleccionados al azar. La información obtenida mediante los cuestionarios y las inspecciones efectuadas en 17 oficinas visitadas reveló lo siguiente:

1) A varios usuarios no se les habían ofrecido adiestramientos u orientaciones en cuanto al uso de los sistemas de información y las normas de seguridad establecidas en el **Reglamento**, según se detalla a continuación:

   a) Cuatro de los usuarios (13 por ciento) no habían recibido adiestramientos en cuanto al uso de los sistemas de información.

   b) Catorce usuarios (45 por ciento) no habían recibido adiestramientos sobre la preparación de los respaldos de información.

   c) Dos usuarios (6 por ciento) no habían recibido adiestramientos sobre el uso del correo electrónico.

   d) Ocho usuarios (26 por ciento) no habían recibido adiestramientos sobre el cambio de contraseña.

   e) Cuatro usuarios no habían recibido adiestramientos sobre el uso de Internet.

   f) Once usuarios (35 por ciento) no habían recibido adiestramientos sobre los derechos de autor o piratería.

   g) Dieciocho usuarios (58 por ciento) desconocían las políticas de contraseñas establecidas en el **Reglamento**. Ocho de estos usuarios habían configurado sus contraseñas de acceso con seis caracteres o menos, cinco desconocían cuántos intentos fallidos permitía el sistema de seguridad antes de bloquear la cuenta y cinco desconocían ambas normas.

2) Trece usuarios (42 por ciento) no tenían en su área de trabajo el **Reglamento**, ni el correo electrónico mediante el cual se le envió copia del mismo.

3) Las computadoras asignadas a 15 usuarios (48 por ciento), identificadas con los números de propiedad OG-00029, OG-00056, OG-00134, OG-00142, OG-00143, OG-16569, OG-16593, OG-17210, OG-17262, OG-17483, OG-18593, OG-18603 y OG-18644, y con los números de serie 23PA627 y 23PB460[14] no tenían instalada una batería (UPS). Además, las computadoras asignadas a 8 usuarios (26 por ciento) identificadas con los números de propiedad OG-16590, OG-17211, OG-17310, OG-17384[15], OG-17478 y OG-18601 y con los números de serie 23PA182 y 23PB343[16] tenían instaladas baterías que estaban dañadas.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política que las entidades gubernamentales deberán garantizar el buen uso, manejo, integridad, exactitud y preservación de la información del gobierno y protegerla contra la modificación, divulgación y manipulación. Como parte de ello, las agencias mantendrán al día un programa de concienciación sobre seguridad de información dirigida a todos los usuarios en todos los niveles.

En el **Reglamento** se establece, entre otras cosas, que:

- Los supervisores o directores de Departamento deberán coordinar la asistencia de los usuarios a adiestramientos, seminarios o cursos relacionados a los programas que utilicen y cualquier otro tema relacionado a sistemas de información computadorizados, de acuerdo con las necesidades de la oficina, para que los recursos se utilicen al máximo.

- Los usuarios serán responsables de conocer y cumplir con las normas y los procedimientos establecidos por la Oficina del Gobernador.

[14] Las computadoras con los números de serie 23PA627 y 23PB460 no tenían asignado un número de propiedad. En los registros de propiedad eran identificadas con el número de serie.

[15] El número de propiedad se había adherido al monitor.

[16] Las computadoras con los números de serie 23PA182 y 23PB343 no tenían asignado un número de propiedad. En los registros de propiedad eran identificadas con el número de serie.

- La política pública de la Oficina del Gobernador prohíbe el uso ilegal e inadecuado de programas y sistemas operativos y promueve el uso exclusivamente oficial de los equipos.

- Los sistemas de información computadorizados, los programas y la información desarrollada y transmitida a través de estos equipos son propiedad de la Oficina del Gobernador y sólo se utilizarán para fines estrictamente oficiales.

- Las contraseñas de acceso deben ser individuales y confidenciales y deben ser cambiadas cada 180 días.

- Las contraseñas serán de más de seis caracteres y no mayor de ocho, los cuales deberán ser una combinación de letras y números.

- El usuario deberá respaldar la información grabada fuera de la red en unidades removibles de almacenamiento de información identificadas.

- Ningún usuario debe utilizar el correo electrónico para uso personal.

- No se podrá acceder a Internet para uso ajeno al fin público.

- Los sistemas de información computadorizados deben tener una batería (UPS) instalada para evitar perder la información, de ocurrir alguna interrupción del servicio de energía eléctrica.

Las mejores prácticas utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados sugieren que para que un plan de seguridad sea efectivo, se deben ofrecer orientaciones periódicas para mantener informado al personal responsable de cumplir con el mismo. Entre otras cosas, se le debe informar sobre las políticas de seguridad establecidas, la responsabilidad individual de cumplir con las mismas, la importancia del manejo de la información y las razones legales y administrativas para mantener su integridad y confidencialidad.

Las situaciones comentadas en el **Apartado a.1) y 2)** aumentan el riesgo de pérdida y divulgación no autorizada de la información, al propiciar el uso indebido de los sistemas computadorizados y el acceso no autorizado a los programas o datos de la Oficina del Gobernador. Además, la falta de conocimiento de las normas de seguridad relacionadas con los sistemas de información ocasiona el incumplimiento de las mismas con los consiguientes efectos adversos en cuanto a la protección de la información y del equipo.

La situación comentada en el **Apartado a.3)** podría ocasionar la pérdida de información y daños a las computadoras en casos de interrupciones del servicio de energía eléctrica.

La Directora de Recursos Humanos no mantenía un programa continuo de adiestramientos al personal que incluyera las orientaciones sobre las normas, los reglamentos y los procedimientos relacionados con los sistemas de información computadorizados. **[Apartado a.1) y 2)]**

El Director de la OSI no efectuó las gestiones requeridas para que la Oficina del Gobernador adquiriera las baterías necesarias para todas las computadoras instaladas. **[Apartado a.3)]**

Véanse las recomendaciones 1, 5, 6.g. y 7.b.

ANEJO

OFICINA DEL GOBERNADOR

OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DEL NIVEL EJECUTIVO QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Hon. Aníbal Acevedo Vilá	Gobernador	16 feb. 06	30 jun. 06
Hon. Jorge Silva Puras	Secretario de la Gobernación	22 jun. 06	30 jun. 06
Sr. Aníbal J. Torres Torres	"	16 feb. 06	20 jun. 06
Sr. José A. Hernández Arbelo	Administrador de la Oficina del Gobernador	16 feb. 06	30 jun. 06
Sr. Pedro Ramos Rosado	Director de la Oficina de Finanzas	16 feb. 06	30 jun. 06
Lic. Mayra Vázquez Irizarry	Directora de la Oficina de Recursos Humanos	16 feb. 06	30 jun. 06
Sr. Alfredo Vélez González	Director de la Oficina de Sistemas de Información	16 feb. 06	30 jun. 06