INFORME DE AUDITORÍA TI-09-07

25 de septiembre de 2008

OFICINA DEL GOBERNADOR

OFICINA DE SISTEMAS DE INFORMACIÓN

(Unidad 5375 - Auditoría 12939)

Período auditado: 1 de julio de 2006 al 15 de mayo de 2007

CONTENIDO

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

25 de septiembre 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 dos informes de dicha auditoría. Este es el segundo informe y contiene el resultado de nuestro examen de los controles establecidos para el uso de las computadoras, la red de comunicaciones (Red) e Internet y los controles de acceso lógico a los sistemas de información computadorizados. El primer informe se emitió el 3 de julio de 2008 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 **(Informe de Auditoría TI-09-01)**.

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 contaba 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 2006-07 ascendió a $5,079,000.

---

[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.

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 julio de 2006 al 15 de mayo de 2007. 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 y la evidencia en nuestro poder demuestran serias desviaciones a las normas generalmente aceptadas en este campo en lo que concierne a los controles establecidos para el uso de las computadoras examinadas, la Red e Internet y los controles de acceso lógico a los sistemas de información computadorizados, según los **hallazgos del 1 al 7** de este **Informe**, clasificados como principales. Por carecer de información competente, suficiente y relevante acerca de los controles establecidos para las computadoras, nuestra Oficina se abstiene de emitir una opinión sobre los mismos. **[Véase el Comentario Especial]**

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

COMENTARIO ESPECIAL

En esta sección se comentan situaciones que no necesariamente impliquen violaciones de leyes y de reglamentos, pero que sean significativas para las operaciones de la entidad auditada. Por ejemplo: litigios o demandas pendientes, y pérdidas en las operaciones de la entidad. También se incluyen otras situaciones que no están directamente relacionadas con las operaciones de la entidad, las cuales pueden constituir violaciones de ley y reglamento que afectan al erario.

Impedimento a nuestra gestión fiscalizadora por la negativa del Administrador a permitirnos examinar el uso de las computadoras de la Oficina del Gobernador

Esta Oficina notificó al Gobernador del Estado Libre Asociado de Puerto Rico el inicio de la auditoría de los sistemas de información computadorizados de la Oficina del Gobernador, en carta del 23 de enero de 2006. En dicha carta se informó, entre otras cosas, que la fecha de inicio de la auditoría sería el 16 de febrero de 2006 y que la reunión inicial sería coordinada por la auditora a cargo de la misma.

El 1 de febrero de 2006 el Administrador de la Oficina del Gobernador (Administrador) aprobó el **Reglamento sobre Normas y procedimientos para el buen uso y manejo de los Sistemas Computadorizados de La Oficina del Gobernador (Reglamento)**. En el **Inciso 1 del Artículo 20 – Fiscalización Mediante Monitorías y Auditorías** de dicho **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.

En nuestro **Informe de Auditoría TI-09-01** comentamos que dicha disposición reglamentaria 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.

El 6 de febrero de 2006 el Secretario de la Gobernación envió una carta al Contralor de Puerto Rico para confirmar la reunión inicial, coordinada por nuestra auditora, la cual se efectuaría el 9 de febrero de 2006. En dicha carta éste expresó que en la reunión se discutirían asuntos relacionados con el ámbito, el alcance, la extensión, el grado y la magnitud de la auditoría, para que la Oficina del Contralor pudiera cumplir con su deber ministerial y se protegiera el derecho del Gobernador a mantener la confidencialidad de sus comunicaciones dirigidas a la implantación de la política pública.

En la reunión del 9 de febrero de 2006 efectuada por nuestros auditores con el Administrador y los asesores de la Oficina del Gobernador éstos presentaron el asunto de la confidencialidad de la información mantenida en las computadoras del Gobernador y de sus asesores. Les indicaron a nuestros auditores que el acceso de la Oficina del Contralor a estas computadoras estaba restringido, en virtud de la protección que le brinda el Privilegio Ejecutivo y la información confidencial y privilegiada entre abogado y cliente.

Luego de concluidos varios procesos de la auditoría de los sistemas de información computadorizados, el 1 de febrero de 2007 iniciamos nuestro examen para verificar el uso de las computadoras y de las cuentas de acceso al correo electrónico y al servicio de Internet de la Oficina del Gobernador. A dicha fecha, la Oficina del Gobernador tenía 300 computadoras las cuales fueron adquiridas a un costo de $361,823.

El 7 de febrero de 2007 nuestros auditores le notificaron al Administrador que realizarían el examen de los sistemas computadorizados asignados al personal en los edificios Mansión Ejecutiva de La Fortaleza, Pabellones, Palacio Rojo y Fortaleza 63. El 13 de febrero de 2007, a solicitud del Administrador, nuestros auditores participaron en una reunión con éste y el Asesor Legal del Gobernador. En dicha reunión éste último le indicó a nuestros auditores que, a base del Privilegio Ejecutivo, su información y la mantenida por sus asesores es confidencial y no estaba disponible para examen. Además, expresó que como abogado no podía permitir al personal de la Oficina del Contralor examinar la información grabada en los sistemas de información computadorizados de la Oficina del Gobernador por el privilegio abogado-cliente. Nuestros auditores le indicaron que dicha situación representaría una limitación de alcance de la auditoría y, por consiguiente, un impedimento a nuestra función fiscalizadora. No obstante, el Administrador le indicó a los auditores que suministraría una lista del personal cuyas computadoras no podían ser examinadas.

Mediante carta del 15 de febrero de 2007 el Administrador nos sometió una lista de 101 usuarios cuyas computadoras, según su opinión, no podrían ser objeto de intervención por esta Oficina. El 16 de febrero de 2007 el Administrador sometió una lista enmendada en la cual eliminó a un usuario e incluyó otros 10 usuarios, para un total de 110 usuarios.

Del 17 de febrero al 23 de mayo de 2007, nuestra Oficina realizó varias gestiones y reuniones con el Administrador con el fin de que se nos permitiera cumplir con nuestra función fiscalizadora sin limitaciones de alcance. En ese mismo período la Oficina del Gobernador inició un proceso de sustitución de las computadoras asignadas al personal mediante la adquisición de computadoras nuevas. El 24 de mayo de 2007 el Administrador entregó a nuestros auditores una nueva lista de 82 usuarios de computadoras que, según su opinión, no podían ser auditadas por esta Oficina.

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 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...

El Secretario de Justicia en la **Opinión Núm. 6 del 11 de marzo de 1991**, en la página 35, expresó lo siguiente y citamos:

> Tomando en consideración todo lo antes expuesto, es preciso reiterar una vez más la norma establecida por el Departamento de Justicia, al efecto de que el requisito de confidencialidad de la información contenida en los expedientes de los clientes de la O.P.P.I. es aplicable a terceras personas, es decir, a ciudadanos particulares, **pero no a la Oficina del Contralor, teniendo presente la naturaleza y el propósito de su función fiscalizadora, por lo que procede que se cumpla con la solicitud en cuestión**. (Énfasis nuestro)

Los hechos indicados le impidieron a esta Oficina examinar el uso de los sistemas de información computadorizados de la Oficina del Gobernador, relevante al objetivo de nuestra auditoría, lo que provocó que se afectara nuestra función fiscalizadora.

Véanse las recomendaciones 1 y 2.

RECOMENDACIONES

AL GOBERNADOR DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO

1. Considerar los hechos que se indican en el **Comentario Especial** y en los **hallazgos del 1 al 7** de este **Informe** e impartir las instrucciones que entienda pertinentes para que se corrijan y no se repitan las situaciones comentadas.

2. Tomar las medidas necesarias para asegurarse de que el Administrador de la Oficina del Gobernador cumpla con lo requerido por esta Oficina para efectuar el examen de las computadoras de la Oficina del Gobernador. **[Comentario Especial]**

3. Ver que el Administrador de la Oficina del Gobernador se asegure de que el Director de la OSI:

    a. En coordinación con la Directora de la Oficina de Recursos Humanos:

        1) Establezca un plan de adiestramientos por escrito, para ofrecer orientación periódica a los usuarios de los equipos computadorizados sobre las restricciones para el uso oficial de éstos y de las cuentas para acceder a Internet y al correo electrónico, y conservar evidencia de dichas orientaciones. **[Hallazgo 1]**

        2) Se efectúen las inspecciones periódicas, según se establece en el **Reglamento**, para verificar el cumplimiento con las normas establecidas para el uso de los sistemas computadorizados. **[Hallazgo 1]**

        3) Se ofrezcan adiestramientos técnicos al personal a cargo de administrar los sistemas de información de la Oficina del Gobernador. **[Hallazgo 7]**

    b. Establezca los mecanismos de control necesarios en el servidor que permite el acceso a Internet para impedir que las cuentas de acceso con dicho privilegio puedan acceder a páginas de Internet con contenido ajeno a la gestión pública. **[Hallazgo 1]**

c. Configure los parámetros de seguridad de los servidores de la Red para:

1) Establecer un mínimo de ocho caracteres para la utilización de todas las contraseñas. **[Hallazgo 2-a.1)]**

2) Requerir y asegurarse de que los usuarios cambien su contraseña cada 180 días. **[Hallazgo 2-a.2)]**

3) Requerir un mínimo de 10 días para que el sistema le permita al usuario cambiar la contraseña nuevamente. **[Hallazgo 2-a.3)]**

d. Establezca las políticas de auditoría del sistema para que éste produzca un registro cuando ocurran los eventos que se indican en el **Hallazgo 2-b.1)**.

e. Revise y defina adecuadamente las opciones de seguridad (*Security Options*) y privilegios de los usuarios (*User Rights Assignments*) configurados en el servidor primario. **[Hallazgo del 2-b.2) al 4)]**

f. Efectúe revisiones periódicas de los eventos o incidentes grabados en el *Security Log* y *System Log* provistos por el sistema operativo del servidor configurado como *Primary Domain Controller* (*PDC*) y documente en un registro las revisiones e investigaciones efectuadas. **[Hallazgo 2-c.]**

g. Revise las propiedades de las cuentas de acceso de los usuarios establecidas en el servidor configurado como *PDC*, se asegure de que se asignen los horarios, privilegios de accesos y grupos a los que pertenecen de acuerdo con las funciones efectuadas por los usuarios, y de que los usuarios cumplan con las políticas de cambio de contraseña establecidas en el **Reglamento**. **[Hallazgos 2-d. y 3-a.1)a) y b), 2)a) y b), y b.]**

h. Revise y elimine las cuentas de acceso de usuarios inactivas y *Guest*, si aún no se ha hecho. **[Hallazgo 3-a.1)c) y 2)a) y c), y c.]**

i. Enmiende la **Solicitud de Acceso al Sistema de Información** para que contenga la información relacionada con los accesos solicitados, la justificación y la firma del usuario, supervisor y personal encargado de crear la cuenta en el sistema. Además, se asegure de que se complete la misma antes de crear las cuentas de acceso en los sistemas de información de la Oficina del Gobernador. **[Hallazgo 4]**

j. Revise los informes provistos por el sistema central de antivirus y se asegure de que las definiciones de antivirus sean actualizadas automáticamente en todas las computadoras conectadas a la Red y que todas las alertas de seguridad sean atendidas prontamente. **[Hallazgo 5]**

k. Prepare y mantenga actualizado un diagrama de la configuración de la Red que incluya información sobre los puertos de conexión, los terminales y el equipo conectado en cada oficina. **[Hallazgo 6-a.]**

l. Se asegure de que la documentación sobre las configuraciones de los sistemas principales se mantiene actualizada. **[Hallazgo 6-a. y c.]**

m. Coordine con el Encargado de la Propiedad el establecimiento de un itinerario para el mantenimiento preventivo del equipo. **[Hallazgo 6-b.]**

n. Se asegure de que todos los cambios a la configuración de los sistemas computadorizados efectuados por consultores externos son supervisados adecuadamente, e informados al personal a cargo de la administración de los sistemas de información. **[Hallazgo 6-c.]**

o. Someta para su consideración y aprobación, los siguientes procedimientos relacionados con la seguridad de los sistemas de información:

   1) Procedimiento para solicitar la creación, modificación y cancelación de las cuentas de acceso a los sistemas de información, que incluya el uso de un formulario de acceso cuyo contenido cumpla con lo requerido 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, 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. **[Hallazgo 4]**

2) Procedimiento para solicitar autorización para modificar las configuraciones de los sistemas de información y mantener la documentación de las configuraciones establecidas en los sistemas principales de la Oficina del Gobernador. **[Hallazgo 6-c.]**

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 26 de junio 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 9 de julio de 2008. Las observaciones sometidas por dicho funcionario fueron consideradas en la redacción final del informe. Algunas de las 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 DE LA OFICINA DEL GOBERNADOR.

AGRADECIMIENTO

A los funcionarios y empleados de la Oficina del Gobernador 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 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 - Computadoras y cuentas para acceder a Internet y al correo electrónico utilizadas para fines ajenos a la gestión pública

a. El examen del registro de direcciones de Internet (*Log* del servidor configurado para el servicio de Internet) visitadas por los usuarios de la Oficina del Gobernador del 14 al 17 de agosto de 2006 reveló que en dicho período se había utilizado este servicio para acceder 234 páginas de Internet con contenido ajeno a la gestión pública[2]. No se pudieron determinar las cuentas de acceso de usuarios que visitaron las mismas porque no se incluía dicha información en el campo *client user name* del *Log*.

b. Al 1 de febrero de 2007 el **Inventario del equipo computadorizado de la Oficina del Gobernador** contenía 300 computadoras (274 de escritorio y 26 portátiles) y 6 servidores adquiridos por $399,395. El examen realizado entre el 15 y el 26 de febrero de 2007 sobre el uso de 6 computadoras reveló lo siguiente:

    1) Cinco computadoras[3] contenían 32 archivos ajenos a la gestión pública.

[2] Dicha información se incluyó en el borrador de los **hallazgos del Informe** sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

[3] Una relación de las computadoras se incluyó en el borrador de los **hallazgos del Informe** sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

2) Las 6 computadoras[4] se utilizaron para acceder en varias ocasiones páginas de Internet con contenido ajeno a la gestión pública.

3) Tres computadoras[4] fueron utilizadas en varias ocasiones para enviar y recibir mensajes de correo electrónico con contenido ajeno a los intereses y la gestión pública.

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 de la Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental**, 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 la **Política Núm. TIG-008 de la Carta Circular Núm. 77-05** se establece, entre otras cosas, lo siguiente:

- 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.

- 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

[4] Véase la nota al calce 3.

actividades personales con fines de lucro o en menoscabo de la imagen de la entidad gubernamental o sus empleados.

En el **Reglamento** se establece lo siguiente:

- Los Sistemas de Información Computadorizados, los programas y la información desarrollada, guardada y transmitida a través de estos equipos son propiedad de La Oficina del Gobernador y sólo se utilizarán para fines estrictamente oficiales. **[Artículo 7, Control de Acceso a los Documentos y Programas]**

- No se podrá acceder a la Internet para uso ajeno al fin público y que ningún usuario podrá utilizar el correo electrónico (*e-mail*) para uso personal. **[Artículo 29, Acceso a la Red Internet y Correo Electrónico]**

El uso de las computadoras y de las cuentas para acceder a Internet y al correo electrónico pertenecientes a la Oficina del Gobernador para procesar documentos y examinar archivos de carácter privado es contrario al interés público y desvirtúa los propósitos para los cuales fueron adquiridas. Además, provee al funcionario o empleado que indebidamente las utiliza ventajas, beneficios y privilegios que no están permitidos por ley.

Las situaciones comentadas se atribuyen, en parte, a que:

- No se ofrecían orientaciones periódicas a todos los usuarios de los equipos computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso de éstos, del correo electrónico e Internet.

- No se habían establecido controles para impedir el acceso a páginas de Internet con contenido ajeno a la gestión pública.

- No se realizaban inspecciones periódicas para verificar el cumplimiento por los usuarios de las normas establecidas para el uso oficial de los equipos computadorizados y de las cuentas para acceder a Internet y al correo electrónico.

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

> Esta administración estableció políticas de seguridad para limitar el acceso a páginas ajenas a la gestión pública. Se envió electrónicamente a todos los usuarios el reglamento sobre normas y procedimientos para el buen uso y manejo de los sistemas computadorizados de la Oficina del Gobernador.

Véanse las recomendaciones 1 y 3.a.1) y 2) y b.

Hallazgo 2 - Deficiencias en los controles de acceso lógico a los servidores de la Red y en las revisiones periódicas de los registros de eventos de los servidores

a. El examen efectuado a 9[5] de los 11 servidores[6] de la Oficina del Gobernador, en cuanto a los parámetros de seguridad relacionados con las cuentas de acceso (*Account Policies*) establecidos al 19 de mayo de 2006, reveló que en los 9 no se habían configurado los parámetros de seguridad para requerir:

1) Al menos, un mínimo de seis caracteres para la utilización de las contraseñas (*Minimum Password Length*).

2) Que los usuarios modificaran las contraseñas de acceso al menos cada 180 días (*Max Password Age*).

3) Al menos, un mínimo de 10 días para que el sistema le permita al usuario cambiar la contraseña nuevamente (*Min Password Age*).

[5] Una relación de los servidores se incluyó en el borrador de los **hallazgos del Informe** sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

[6] Al 19 de mayo de 2006 la Oficina del Gobernador tenía 11 servidores.

En el **Artículo 7: Control de Acceso a los Documentos y Programas del Reglamento** se establece que las contraseñas serán de más de seis y no mayor de ocho caracteres, que deberán ser cambiadas cada 180 días y que el sistema le pedirá al usuario el cambio de contraseña cuando se haya cumplido dicho período.

b. El examen efectuado el 26 de diciembre de 2006 de la configuración de las políticas de auditoría (*Audit Policy*), los privilegios de los usuarios (*User Rights Assignment*) y las opciones de seguridad (*Security Options*) establecidas en el servidor configurado como *PDC*, reveló que no se habían establecido los parámetros de acuerdo con las recomendaciones incluidas en las guías de seguridad publicadas por el proveedor, según se indica:

1) No se había definido la política de auditoría (*Audit Policy*) para que el sistema produjera un registro cuando ocurrieran 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*)

2) No se habían definido las opciones para activar o desactivar 53 parámetros de seguridad (*Security Options*)[7].

[7] Una relación de los 53 parámetros de seguridad se incluyó en el borrador de los **hallazgos del Informe** sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

3) No se habían definido (*Not defined*) 10 opciones para asignarle a los usuarios los siguientes privilegios (*User Rights Assignment*):

- Permitir la conexión local (*Allow logon on locally*). Este privilegio debe ser otorgado a los administradores y a los operadores de respaldos y de servidores.

- Permitir la conexión a través del *Terminal Services*. Este privilegio debe ser otorgado a los administradores.

- Depurar programas (*Debug programs*). Este privilegio debe ser otorgado a los administradores.

- Prohibir el acceso a la computadora desde la Red (*Deny access to this computer from the network*). Este privilegio debe ser asignado a cuentas de acceso específicas de apoyo técnico.

- Prohibir la conexión de procesamiento en grupo (*Deny logon as a batch job*). Este privilegio debe ser asignado a cuentas de apoyo técnico.

- Prohibir la conexión a través del *Terminal Services*. Este privilegio debe ser otorgado a las cuentas de acceso de visitantes (*Guest*).

- Cambiar la hora del sistema. Este privilegio debe ser otorgado al administrador.

- Cargar y descargar los programas utilitarios de los equipos (*device drivers*). Este privilegio debe ser otorgado al administrador.

- Restaurar archivos y directorios. Este privilegio debe ser otorgado al administrador.

- Apagar el sistema. Este privilegio debe ser otorgado al administrador.

4) No se habían definido adecuadamente tres opciones para asignar a los usuarios los siguientes privilegios (*User Rights Assignment*):

- El privilegio para acceder la computadora desde la Red había sido asignado a la cuenta de usuario *Everyone*. Mediante esta cuenta se podía otorgar el acceso a las cuentas y a los grupos de visitantes (*Guest*), las cuales pueden ser utilizadas para efectuar ataques a la Red. Este privilegio debe ser otorgado a los administradores, servidores primarios y usuarios autenticados en un ambiente de funcionalidad limitada de un sistema de seguridad especializado (*Specialized Security-Limited Functionality Environment*). Este ambiente se caracteriza por el uso de configuraciones de seguridad muy restrictivas que podrían afectar el funcionamiento de algunas aplicaciones y la comunicación con computadoras que no hayan sido configuradas bajo los mismos estándares de seguridad.

- El privilegio para actuar como parte del sistema operativo (*Act as part of the operating system)* había sido otorgado a las cuentas de acceso incluidas en el grupo de *domain administrators*. Este privilegio permite a estos usuarios asumir la identidad de cualquier usuario y acceder los recursos autorizados a todas las cuentas de acceso de usuario. En el **Hallazgo 3-a.2)c)** se comenta la asignación inadecuada de cuentas de *domain administrator* en el servidor configurado como *PDC*. Este privilegio sólo debe ser definido como *no one* en un ambiente de funcionalidad limitada de un sistema de seguridad especializado. Esto, para evitar que el grupo de seguridad y las cuentas de seguridad accedan dicho privilegio.

- El privilegio para efectuar respaldos a los archivos y directorios (*Back up files and directories*)[8] había sido otorgado a las cuentas incluidas en el grupo de *domain administrator*. Este privilegio se asigna sólo a los administradores de un ambiente de funcionalidad limitada de un sistema de seguridad especializado.

[8] El privilegio para efectuar respaldos a la computadora se utiliza sólo cuando una aplicación intenta acceder con utilidades como *NTbackup.exe* a través del *NTFS backup application programming interface* (*API*). De otra forma deben aplicarse los privilegios normales de directorios y archivos.

c. Al 30 de diciembre de 2006 el Subdirector de la OSI, quien era responsable de administrar la Red y los sistemas computadorizados, no revisaba periódicamente los eventos o incidentes grabados en los registros *Security Log*[9] y *System Log*[10] provistos por el sistema operativo del servidor configurado como *PDC*. Ello 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. Por ello, no se investigaron 3 eventos grabados el 21 de agosto de 2006 en el *Security Log* y 10 eventos grabados entre el 14 de agosto y el 19 de agosto de 2006 en el *System Log*, según se indica:

- Un *Account Logon Event (Event ID 675)* grabado en el *Security Log*. Este evento se registra cuando un usuario intenta conectarse a una computadora con una cuenta válida del *domain*[11], pero registra una contraseña errónea. Este permite identificar cada intento fallido de acceso utilizando contraseñas erróneas y el *IP Address* del sistema que intentó el acceso.

- Dos *Object Access Event (Event ID 560)* grabados en el *Security Log*. Este evento permite identificar los intentos fallidos y exitosos para acceder archivos y otros objetos del sistema operativo.

- Diez eventos de la categoría *Warning* grabados en el *System Log*. Nueve de estos eventos estaban identificados con el código *Event ID 47* y uno con el código *Event ID 22*. Los eventos de esta categoría pueden anticipar problemas futuros en los sistemas de información.

[9] El registro de la seguridad puede registrar acontecimientos de la seguridad, tales como tentativas válidas e inválidas de la conexión y acontecimientos relacionados con el uso del recurso, tales como crear, abrir, o suprimir archivos. Un administrador puede especificar qué acontecimientos se registran en el registro de la seguridad.

[10] El registro del sistema contiene los acontecimientos registrados por los componentes del sistema operativo del servidor.

[11] Conjunto de ordenadores conectados en una red que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.

d. El examen sobre los accesos a la Red efectuado el 15 de febrero de 2007 a una computadora y el 21 de febrero de 2007 a otra computadora[12] reveló que los usuarios de éstas tenían acceso a documentos confidenciales no relacionados con sus funciones. Entre estos documentos se incluían cartas para la firma del Gobernador, documentos de la Oficina de la Primera Dama, informe de nómina de la Oficina de Recursos Humanos y un Informe de Avalúo de Riesgo de la OSI.

   En la **Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05** se establecen las directrices generales que permitirán a las agencias la confidencialidad, la integridad y la disponibilidad de la información que manejan. 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 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 renovación periódica de la contraseña de cada usuario, según las necesidades de la agencia y los procedimientos establecidos.

   - La asignación de privilegios a las cuentas de acceso de usuarios a base de la necesidad de los trabajos a realizar en la Red.

   - La revisión continua por el personal técnico especializado de los informes en los que se registran todos los eventos de seguridad de la Red.

[12] Los números de propiedad de estas computadoras se incluyeron en el borrador de los **hallazgos del Informe** sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

Las situaciones comentadas en los **apartados a., del b.2) al 4) y d.** propician que personas no autorizadas puedan lograr acceso a información confidencial 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.

Las situaciones comentadas en los **apartados b.1) y c.** impiden la detección temprana de errores críticos o problemas con los servidores que permitan tomar de inmediato las medidas preventivas y correctivas necesarias. Además, privan a la gerencia de los medios necesarios para supervisar eficazmente el desempeño de los usuarios y detectar el acceso y uso indebido de los sistemas computadorizados.

Las situaciones comentadas en los **apartados del a. al d.** se debían, principalmente, a que el Director de la OSI no se había asegurado de que el personal encargado de administrar los sistemas de información pusiera en vigor todas las opciones de seguridad de acceso lógico que proveen los sistemas operativos, estableciera los controles adecuados para el mantenimiento de las cuentas de acceso a la Red, limitara el acceso a los archivos de datos de los usuarios y examinara periódicamente los registros de seguridad.

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

> Se estableció la política de requerir un mínimo de seis caracteres para la utilización de las contraseñas (Mínimo password length). **[Apartado a.1)]**
>
> Se estableció que la contraseña de acceso debe modificarse cada 180 días y que el sistema le brinde al usuario 10 días para cambiar la contraseña nuevamente. **[Apartado a.1)]**
>
> Esta administración definió la política de auditoría (Audit Policy) para que el sistema produzca un registro de privilegios de los usuarios y las opciones de seguridad según publicadas por el proveedor. **[Apartado b.1) y 2)]**
>
> La OSI definió las opciones para asignar a los usuarios los privilegios de conexión local a los administradores operadores de respaldos y la de los servidores. **[Apartado b.3) y 4)]**

Esta administración está considerando reclutar personal que se encargue de monitorear los eventos e incidentes grabados en los registros provistos por el sistema operativo del servidor principal. **[Apartado c.]**

Se crearon las Políticas necesarias para que cada usuario tenga el privilegio al fólder del área que trabaja exclusivamente. **[Apartado d.]**

Véanse las recomendaciones 1 y de la 3.c. a la g.

Hallazgo 3 - Deficiencias relacionadas con la administración de las cuentas de acceso de usuarios definidas en el servidor configurado como *PDC*

a. El servidor configurado como *PDC* tenía definidas 376 cuentas de acceso de usuarios, de las cuales 366 estaban activas y 10 inactivas. El examen efectuado sobre las propiedades (*User Account Properties*) y los privilegios de dichas cuentas establecidos al 19 de mayo de 2006 reveló las siguientes deficiencias:

1) Relacionado con las propiedades de las 366 cuentas de acceso de usuarios activas:

a) No se había restringido el tiempo de acceso a la Red para todas las cuentas de acceso de acuerdo con las funciones de cada usuario (*User/Accounts/Logon Hours*). En una certificación emitida por el Administrador de la Oficina del Gobernador se nos indicó que los únicos empleados que debían tener acceso en un horario ilimitado eran los asesores, los asesores auxiliares, los directores de la OSI y de Operaciones y la Directora de Prensa. A la fecha de nuestro examen, existían 235 cuentas de acceso de usuarios activas (64 por ciento), que no correspondían a los funcionarios incluidos en la certificación del Administrador y a las cuales no se le había restringido el tiempo de acceso a la Red conforme a las funciones que realizaban. De éstas, 147 cuentas de acceso de usuarios tenían acceso al sistema en un horario ilimitado y otras 88 cuentas de acceso de usuarios podían acceder al Sistema durante los 7 días de la semana.

b) No se había establecido el cambio de contraseñas (*User/Password/Password Never Expire* y *User/Password/Password Expire Time Unknown*) a las 366 cuentas de acceso de usuarios activas. Éstas habían sido asignadas a 123 funcionarios

administrativos, 177 empleados, 10 practicantes de la Oficina del Procurador de Personas con Impedimentos, 1 consultor externo, 17 cuentas de sistema y 38 cuentas de correo electrónico y de uso común.

c) No se habían inhabilitado tres cuentas de acceso, clasificadas como cuentas de invitados (*Guest*)[13]. El uso de dichas cuentas, creadas por *default*[14] en el sistema operativo hace que el sistema esté vulnerable a accesos no autorizados.

2) Relacionado con las cuentas de acceso de usuarios activas que pertenecen al grupo de administrador, *domain administrator* y usuarios visitantes (*Guest*) determinamos las siguientes deficiencias:

a) La cuenta de usuario asignada a la Subdirectora de Finanzas y una cuenta de usuario creada por *default* durante la instalación pertenecía al grupo de administrador (*administrator*). La cuenta creada por *default* no había sido utilizada por un período de 59 días. Las cuentas de administrador tienen privilegios que le permiten conectarse a cualquier computadora, acceder cualquier archivo, instalar aplicaciones, remover y otorgar accesos, y modificar las políticas de seguridad, entre otros.

b) Las cuentas de acceso asignadas a 2 directores, 1 Subdirector, 2 asistentes administrativos, 1 ayudante especial, 1 analista de sistema, 1 ayudante especial auxiliar, 1 ayudante administrativo, 1 consultor externo y 2 cuentas de sistemas que no habían sido utilizadas por un período de entre 59 y 896 días pertenecían al grupo de *domain administrator*. Los miembros de este grupo tienen control total del *domain*[15].

---

[13] Cuentas predefinidas en el sistema operativo que no están asignadas a un usuario.

[14] Valor o parámetro asignado a un equipo o entidad automáticamente por el sistema operativo sin que el usuario lo especifique o elija.

[15] Véase la nota al calce 11.

c) Una cuenta creada por *default* para el acceso anónimo a los servicios de Internet pertenecía al grupo de usuarios visitantes (*Guest*). Los miembros de este grupo tienen privilegios limitados que le permiten conectarse a la Red mediante una cuenta no asignada a un usuario en específico. Esta cuenta nunca había sido utilizada y su contraseña no expiraba.

b. El examen realizado de una muestra de 45 cuentas de acceso de usuarios activas, que al 19 de mayo de 2006 se les requería el uso de contraseña y se les permitía efectuar el cambio de la misma, reveló lo siguiente:

1) Las contraseñas de 35 cuentas de acceso de usuarios (78 por ciento) no habían sido cambiadas luego de haber transcurrido 180 días desde la fecha en que fueron establecidas en el *Active Directory* del servidor configurado como *PDC*. Estas contraseñas habían sido utilizadas entre 4 y 1,455 días en exceso a los 180 días establecidos en el **Reglamento**.

2) Las contraseñas de dos cuentas de acceso de usuario (4 por ciento) no habían sido cambiadas desde el 24 de abril de 2006, fecha de creación de las mismas. Al 19 de mayo de 2006 estas cuentas de acceso de usuarios no habían sido utilizadas. Éstas fueron configuradas para permanecer activas hasta el 27 de enero de 2007, es decir, un total de 276 días desde la fecha de creación.

c. Al 19 de mayo de 2006 no se habían eliminado del servidor configurado como *PDC* las siguientes cuentas de acceso de usuarios:

- Dos cuentas de acceso de usuarios asignadas a empleados que habían cesado sus funciones entre el 15 y el 31 de marzo de 2006. A dicha fecha habían transcurrido entre 49 y 65 días desde la fecha del cese y permanecían activas.

- Cuarenta y cinco cuentas de acceso de usuarios que habían sido creadas en el sistema entre el 13 de abril de 2002 y el 24 de abril de 2006 y nunca habían sido utilizadas. Habían transcurrido entre 25 y 1,497 días desde la fecha de su creación. De

las 45 cuentas, 5 (11 por ciento) habían sido inhabilitadas y 40 (89 por ciento) permanecían activas.

- Doscientas ochenta y nueve cuentas de acceso de usuarios cuya última conexión al sistema había ocurrido entre el 19 de abril de 2002 y el 29 de diciembre de 2005. Habían transcurrido entre 141 y 1,491 días desde su última conexión al sistema. Una de estas cuentas había sido inhabilitada y 288 permanecían activas.

- Cuatro cuentas de acceso de usuarios que habían sido inhabilitadas y habían transcurrido entre 4 y 59 días desde su última conexión.

En el **Artículo 7: Control de Acceso a los Documentos y Programas del Reglamento** se establece que las contraseñas deberán ser cambiadas cada 180 días y que el sistema le pedirá al usuario el cambio de contraseña cuando se haya cumplido dicho período.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que cada agencia deberá implantar controles que minimicen los riesgos de que la información sea accedida de forma no autorizada. Esta norma se instrumenta, en parte, mediante lo siguiente:

- La asignación de privilegios de acceso a las cuentas de acceso de usuarios a base de las funciones que realizan.

- 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.

- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos.

- La adopción de normas y procedimientos para el mantenimiento de las cuentas de acceso de usuarios.

- La notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones o de la modificación de las mismas para la acción correspondiente.

Las situaciones mencionadas pueden propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. Además, pueden propiciar 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.

Las situaciones comentadas se debían principalmente, a que el Director de la OSI no se había asegurado de que el personal encargado de administrar los sistemas de información estableciera los controles adecuados para el mantenimiento de las cuentas de acceso a la Red.

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

> Las cuentas de usuario a las que no se había restringido el tiempo de acceso a la red corresponden al personal que labora directamente con los Asesores, Asesores Auxiliares, Directores de Oficinas, Director de la OSI, Secretaria de la Gobernación, Oficina del Gobernador, La Oficina de la Primera Dama y Secretaria de Asuntos Públicos. **[Apartado a.1)a)]**
>
> Se estableció la política para que el cambio de contraseñas se efectúe cada 180 días. **[Apartados a.1)b) y c) y b.1) y 2)]**
>
> Se eliminaron del sistema todas las cuentas guest y las que no se estaban utilizando. **[Apartados del a.2)a) al c) y b.3)]**
>
> En la actualidad no existen cuentas de invitados (Guest account). **[Apartado a.2)c)]**

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

Véanse las recomendaciones 1 y 3.g. y h.

Hallazgo 4 - Deficiencias en los formularios para otorgar acceso a la Red

a. En la Oficina del Gobernador se utilizaba la **Solicitud de Acceso al Sistema de Información** para autorizar la creación, modificación y cancelación de las cuentas de acceso de los usuarios. En dicho formulario se requería, entre otra información, el nombre y puesto de los usuarios, la fecha de solicitud para la creación de las cuentas de acceso, la fecha de creación de las cuentas de acceso, la fecha de autorización y procesamiento de las solicitudes, y la justificación para obtener acceso a Internet.

   El examen de 48 **solicitudes** para autorizar la creación de cuentas de usuarios entre el 1 de febrero y el 22 de agosto de 2006, y de los correos electrónicos para notificar el cese de empleados del 1 de enero al 31 de marzo de 2006, reveló que:

   1) No se utilizó la **Solicitud** para la cancelación de las cuentas de acceso de 11 empleados, cuya fecha de separación había ocurrido en febrero y marzo de 2006.

   2) Los asesores y directores de la Oficina del Gobernador prepararon 29 **solicitudes** para, entre otras cosas, solicitar el acceso a Internet para 31 empleados. En 27 de éstas, no se indicó la razón para otorgar el acceso. A pesar de ello, la OSI autorizó y procesó dichas **solicitudes**.

   3) En las **solicitudes** se indicaba que el acceso a los sistemas constituye una aceptación de los términos y las condiciones de uso establecidos en las políticas y los procedimientos de la OSI. Sin embargo, no se requería la firma del usuario a quien le otorgaban el acceso para constar dicha aceptación.

   4) Una **Solicitud** se preparó con el nombre de una funcionaria de la Oficina del Gobernador para solicitar acceso a Internet para otros tres empleados[16] que utilizaban la computadora asignada a ésta.

[16] Dicha información se incluyó en el borrador de los **hallazgos del Informe** sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

5) En dos **solicitudes** se utilizaron nombres genéricos, en lugar del nombre del usuario autorizado a utilizar estas cuentas para acceder a los sistemas de información. En una de éstas la fecha de la **solicitud** era un año posterior a la fecha en que la OSI procesó la misma.

6) En 22 (46 por ciento) de las 48 **solicitudes** examinadas el Director de la OSI no incluyó la fecha en que aprobó la creación de estas cuentas.

7) En 4 (8 por ciento) de las 48 **solicitudes** la fecha en que el empleado de la OSI procesó la **solicitud** fue anterior a la fecha en que el Director de la OSI aprobó la misma.

En el **Artículo 7: Control de Acceso a los Documentos y Programas del Reglamento** se establece que para utilizar los sistemas de información computadorizados, cada usuario deberá solicitar por escrito, con la autorización del supervisor inmediato, a cuál de los sistemas es que se solicita el acceso.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece lo siguiente:

- 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.

- La información y los programas de aplicación utilizados en las operaciones de la agencia deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos que necesita, o usar las aplicaciones (o parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.

- Cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto, deberán establecerse procedimientos que incluyan una comunicación efectiva entre el área de Recursos Humanos, el área en que trabaja el empleado y el área de Sistemas de Información.

- Los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.

Esta norma se instrumenta, en parte, mediante lo siguiente:

- La notificación inmediata al encargado de crear las cuentas de acceso del cese de un usuario en sus funciones por motivo de renuncia, separación o traslado para que éste cancele su cuenta de acceso.

- El establecimiento de controles de acceso rigurosos a los programas y a los archivos, incluido el uso de formularios para solicitar la creación, modificación o eliminación de cuentas de acceso para cada usuario.

En la **Política Núm. TIG-008 de la Carta Circular Núm. 77-05** se establece, entre otras cosas, que cada entidad gubernamental será responsable de crear una política interna que regule el uso de los sistemas de información de la entidad, y de las herramientas de Internet y correo electrónico. En ésta se indicarán los usos permitidos, los no permitidos y las sanciones o medidas disciplinarias que se aplicarían a los usuarios que incumplieran con la misma. Asimismo, será responsabilidad de cada entidad particular notificar debidamente a los empleados del contenido de la misma. Los usuarios, a su vez, firmarán un documento en donde indicarán que conocen la política y que cumplirán con ella.

Las situaciones comentadas impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y privilegios a los usuarios. También propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. La situación comentada en el **Apartado a.3)** priva a la Oficina del Gobernador de la evidencia sobre la aceptación y el compromiso del usuario a cumplir con las normas y los procedimientos establecidos en el **Reglamento**.

Las situaciones comentadas se debían 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 un procedimiento para solicitar la creación, modificación y cancelación de las cuentas de acceso a los sistemas de información. Además, no había

requerido, antes de aprobar el acceso, que los supervisores inmediatos completaran en su totalidad las **solicitudes** ni habían revisado adecuadamente la información incluida en éstas.

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

> Se instruyó a la oficina de recursos humanos para que cada vez que un empleado cese sus funciones cumplimente la forma "Solicitud de Acceso" para la cancelación de este privilegio y la misma enviarla a la oficina de Sistema de Información. **[Apartado a.1)]**
>
> Se instruyó a todos los supervisores para que al solicitar acceso a la red para algún empleado incluya la justificación y la firma del nuevo usuario. **[Apartado a.2)]**

Véanse las recomendaciones 1 y 3.i. y o.1).

Hallazgo 5 - Deficiencias relacionadas con la actualización de las definiciones de antivirus en las computadoras conectadas a la Red

a. El examen efectuado el 10 de octubre de 2006 de la información incluida en los informes *Users*[17] y *Audit Network*[18] provistos por el sistema centralizado de antivirus, reveló las siguientes deficiencias:

   1) Durante las revisiones (*scan*) automáticas, efectuadas entre el 15 de septiembre y el 11 de octubre de 2006, sobre los riesgos de seguridad y las definiciones de antivirus instaladas en las computadoras administradas por el sistema centralizado de antivirus, se

[17] El informe *Users* proveía información de las computadoras que en algún momento habían sido administradas por el sistema centralizado de antivirus.

[18] El informe *Audit Network* proveía información de los resultados del examen de todas las computadoras conectadas a la red en relación con la instalación del sistema de antivirus, tipo de instalación u otro tipo de sistema de antivirus instalado.

habían reportado cuatro mensajes de alerta que los administradores de la Red no habían atendido de forma inmediata, según se indica:

- Una computadora[19] tenía las definiciones de antivirus vencidas. Habían transcurrido 204 días desde que había sido instalada la última definición de antivirus.

- Dos computadoras[19] estaban bajo una alerta de riesgo de seguridad. Esta alerta permaneció durante la última revisión automática efectuada a estas computadoras el 11 de octubre de 2007.

- Una computadora[19] no tenía instalada las definiciones de antivirus. Esta alerta permaneció durante la última revisión automática efectuada a esta computadora por el sistema centralizado de antivirus el 10 de octubre de 2007.

2) Durante la auditoría a la Red efectuada por la opción *Audit Network* del sistema centralizado de antivirus determinamos que de las 180 computadoras conectadas a la Red al momento del examen, 111 computadoras (62 por ciento) no estaban administradas por el sistema centralizado de antivirus.

En el **Artículo 14: Prevención de Virus de Sistemas de Información Computadorizados del Reglamento** se establece que los sistemas deben mantenerse libre de virus y deberá tener instalado un programa de antivirus actualizado para detectar y eliminar los virus y prevenir daños al sistema y a la información grabada en estos.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que las agencias deberán instalar controles automáticos para la prevención y detección de

[19] Los números de propiedad o de serie de estas computadoras se incluyeron en el borrador de los **hallazgos del Informe** sometido para comentarios al Gobernador del Estado Libre Asociado de Puerto Rico.

programas no deseados (virus, *spyware*[20], *adware*[21] y *updates* automáticos). Como norma de sana administración, dichos programas deberán estar actualizados, de manera que los mismos puedan detectar y eliminar nuevas amenazas.

Las situaciones comentadas pueden impedir la prevención y detección de programas no deseados y permitir que éstos puedan propagarse a los sistemas de información, lo que afectaría la integridad, confidencialidad y disponibilidad de los sistemas de información de la Oficina del Gobernador.

Las situaciones comentadas, se debían, en parte a que el Subdirector de la OSI, a cargo de verificar la operación de los servidores, no había establecido los controles para la revisión de los informes producidos por la consola de administración del sistema centralizado de antivirus.

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

> Se implementó una nueva versión de antivirus la cual genera informes periódicamente para así poder detectar cualquier virus o intruso en la red. En la actualidad se está verificando el 100% de las computadoras para verificar que todos los antivirus estén actualizados.

Véanse las recomendaciones 1 y 3.j.

Hallazgo 6 - Deficiencias relacionadas con la documentación de la configuración de la Red de la Oficina del Gobernador y falta de itinerarios de mantenimiento a los equipos conectados a la Red

a. La documentación de la configuración o estructura de la Red de la Oficina del Gobernador, suministrada para examen el 16 de marzo de 2006, no contenía información sobre los

[20] 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.

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

puertos de conexión, las computadoras y los equipos conectados a la Red con sus respectivas identificaciones y localizaciones.

b. A la fecha del examen, 17 de enero de 2007, la OSI no mantenía un itinerario para el mantenimiento de los equipos conectados a la Red.

c. Al 26 de diciembre de 2006, la OSI no mantenía la documentación de la configuración de los servidores principales que incluyera las modificaciones efectuadas a la configuración de éstos. Por ello, el Subdirector de la OSI, responsable de mantener la seguridad física y lógica de los sistemas de información de la Oficina del Gobernador, desconocía las modificaciones efectuadas a la configuración del servidor configurado como *PDC*.

En la **Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular Núm. 77-05** se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar e 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. Como parte de ello, el diseño de la Red debe estar documentado y las redes deben ser diseñadas e implantadas para cumplir con la **Política Núm. TIG-003**.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que la agencia es responsable de diseñar procedimientos que permitan que los cambios a la seguridad de los sistemas sean realizados y documentados adecuadamente. Como parte de ello, debe mantenerse la documentación de la configuración de los servidores que permita restablecer la misma en caso de que los respaldos no puedan ser utilizados. Además, las modificaciones efectuadas deben ser documentadas para futuras referencias.

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.

Las referidas situaciones impiden a la Oficina del Gobernador tener una comprensión clara y precisa de los componentes de la Red y dificulta mantener control eficaz en la administración y el mantenimiento de la misma. Además, dificulta la atención de problemas de conexión en un tiempo razonable y que se planifiquen efectivamente las mejoras a la Red, según el crecimiento de sus sistemas.

Las situaciones comentadas se debían, en parte, a que el Director de la OSI no había establecido los controles para documentar adecuadamente la Red y la configuración de los servidores. **[Apartados a. y c.]** Tampoco había establecido un itinerario para el mantenimiento de los equipos computadorizados. **[Apartado b.]**

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

> Se instruyó al director Interino de la OSI para la depuración de la información sobre los puertos de conexión, las computadoras y todos los equipos conectados a la red con sus respectivas identificaciones y localizaciones. **[Apartado a.]**
>
> El mantenimiento de los equipos conectados a la red se efectúa periódicamente por instrucciones del director de OSI. **[Apartado b.]**

Véanse las recomendaciones 1 y de la 3.k. a la n. y o.2).

Hallazgo 7 - Falta de adiestramientos periódicos al funcionario y a los empleados que tenían compartidas las funciones de Administrador de la Red

a. Al 6 de septiembre de 2006 dos especialistas de Sistemas de Información y el Subdirector de la OSI, quienes tenían funciones compartidas de Administrador de la Red, no recibían adiestramientos continuos sobre temas relacionados con sus funciones, tales como:

- Sistemas operativos
- Protocolos de la Red
- Diseño, instalación, configuración y mantenimiento de la Red

- Monitoreo de la Red, herramientas para la autoevaluación de la misma y detección de intrusos

- Análisis de problemas

- Novedades, actualizaciones o mejoras en los sistemas

- Nuevas amenazas y posibles soluciones

- Seguridad y confidencialidad de la información

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que las agencias deben establecer controles adecuados en los sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. También se establece que las agencias son responsables de:

- Proveer adiestramientos al personal de sistemas de información y telecomunicaciones sobre los asuntos de seguridad de sus áreas.

- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

La situación comentada podría reducir la efectividad de los sistemas computadorizados, exponer los datos a riesgos innecesarios y afectar la continuidad de las operaciones de la Oficina del Gobernador.

La referida situación se atribuye a que el Director de la OSI no había efectuado gestiones con la Oficina de Recursos Humanos para solicitar adiestramientos para el personal a cargo de administrar los sistemas de información de la Oficina del Gobernador.

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

> Se solicitó a la oficina de recursos humanos que incluyera en el plan de adiestramientos anual al personal de la OSI para tomar adiestramientos relacionados con los sistemas operativos, protocolo de Red, diseño, instalación, configuración y mantenimiento de la red, análisis de problemas y cualquier otro seminario relacionado.

Véanse las recomendaciones 1 y 3.a.3).

ANEJO

OFICINA DEL GOBERNADOR

OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Aníbal Acevedo Vilá	Gobernador del Estado Libre Asociado de Puerto Rico	1 jul. 06	15 may. 07
Hon. Jorge Silva Puras	Secretario de la Gobernación	22 jun. 06	15 may. 07
Sr. Aníbal J. Torres Torres	"	16 feb. 06	20 jun. 06
Sr. José A. Hernández Arbelo	Administrador de la Oficina del Gobernador	1 jul. 06	15 may. 07
Sr. Pedro Ramos Rosado	Director de la Oficina de Finanzas	1 jul. 06	15 may. 07
Lic. Mayra Vázquez Irizarry	Directora de la Oficina de Recursos Humanos	1 jul. 06	15 may. 07
Sr. Alfredo Vélez González	Director de la Oficina de Sistemas de Información	1 jul. 06	15 may. 07