INFORME DE AUDITORÍA TI-10-15

16 de abril de 2010

Senado de Puerto Rico

Centro de Sistemas de Información

(Unidad 5387 - Auditoría 13064)

Período auditado: 31 de agosto de 2007 al 25 de agosto de 2008

CONTENIDO

Página

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

16 de abril de 2010

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

Realizamos una auditoría de las operaciones del Centro de Sistemas de Información (CSI) del Senado de Puerto Rico (Senado) 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 el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico y, en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

En el Artículo III de la Constitución se establece, entre otras cosas, que el Poder Legislativo se ejercerá por una Asamblea Legislativa, que se compondrá de dos cámaras: el Senado y la Cámara de Representantes, cuyos miembros serán electos por votación directa en cada elección general. Se establece, además, que el Senado se compondrá de 27 senadores[1]: 16 senadores por Distrito[2] y 11 por acumulación.

En el Artículo III, Sección 9 de la Constitución se establece, entre otras cosas, que cada cámara adoptará las reglas propias de los cuerpos legislativos para sus procedimientos y gobierno interno.

---

[1] En caso de que en una elección general resultaran electos más de dos terceras partes de los miembros del Senado por un solo partido o bajo una sola candidatura, se aumentará el número de los miembros del Senado en representación del partido o partidos de minoría, hasta un total de 9 senadores. Estos senadores adicionales se considerarán senadores por acumulación.

[2] Dos por cada uno de los ocho distritos senatoriales.

El Senado es dirigido por su Presidente, quien tiene, entre sus facultades y obligaciones, dirigir los asuntos administrativos de éste. En tal capacidad, organiza y dirige las actividades relacionadas con el funcionamiento de dicho Cuerpo Legislativo. Además, tiene la responsabilidad de adoptar y hacer cumplir aquellas normas y reglas que garanticen la confiabilidad de los procedimientos en cada caso en particular, y que hagan más efectiva la ejecución de las gestiones administrativas. Bajo la Presidencia están, entre otras oficinas, la Secretaría del Senado, Finanzas, Recursos Humanos y Asesores Legislativos.

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

El CSI se estableció con el propósito de administrar los recursos humanos, equipos y materiales que sirven las necesidades del Senado en lo que respecta al procesamiento electrónico de datos, así como para dar apoyo a todas las oficinas administrativas y legislativas del Cuerpo.

El Senado tiene una red de comunicaciones (red) de 12 servidores. También cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.senadopr.us. Esta página provee información acerca de la entidad y de los servicios que presta.

Los gastos de operación del CSI se sufragan del presupuesto asignado al Senado, que para los años fiscales 2007-08 y 2008-09 ascendió a $37,430,000 y $39,118,000, respectivamente.

Al 25 de agosto de 2008, el Senado no tenía demandas pendientes de resolución por los tribunales relacionadas con los sistemas de información computadorizados.

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 del Estado Libre Asociado de Puerto Rico*, 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. Se puede acceder a ambas cartas circulares a través de nuestra página en Internet: http://www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 31 de agosto de 2007 al 25 de agosto de 2008. 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
- examen y análisis de informes y de documentos suministrados por fuentes externas
- pruebas y análisis de procedimientos de control interno y de otros procesos
- confirmaciones de información pertinente.

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones del CSI en lo que concierne al control de acceso lógico, las aplicaciones de sistemas, el desarrollo y el control de cambios a las aplicaciones, y la segregación de deberes establecidos en el CSI del Senado no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 7**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

RECOMENDACIONES

AL PRESIDENTE DEL SENADO DE PUERTO RICO

1. Ver que el Secretario del Senado ejerza una supervisión eficaz sobre el Director del CSI para asegurarse de que:

   a. Tome las medidas necesarias para que se mantenga una supervisión y segregación adecuada de las funciones conflictivas realizadas por el Programador de Sistemas Electrónicos I. **[Hallazgo 1]**

b. Prepare y remita para aprobación:

1) Los procedimientos para la asignación de privilegios de administrador de los sistemas operativos y de conexión remota. En éstos se debe establecer la utilización de un formulario en el que se documente la justificación y la autorización para otorgar dichos privilegios. **[Hallazgo 2]**

2) Las normas y los procedimientos necesarios para reglamentar la producción, el almacenamiento y la conservación de los respaldos, y que establezca la necesidad de mantener un inventario de los medios magnéticos utilizados para los respaldos. **[Hallazgo 4-a.1)]**

3) Los cambios necesarios para la actualización del *Manual de Políticas y Procedimientos*[3], aprobado el 20 de octubre de 1994 por la Secretaria del Senado, y del *Design, Development and Implementation Standards*. Además, redacte y remita para aprobación, las normas y los procedimientos escritos necesarios para el control y la administración de los sistemas operativos y de los programas utilitarios. Una vez aprobados, asegurarse de que sean divulgados para conocimiento de los funcionarios y de los empleados del Senado correspondientes. **[Hallazgo 6]**

c. Establezca los controles necesarios para que se corrijan las situaciones comentadas en el **Hallazgo 3-a.1) y 2)d)**, 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.

d. Establezca las medidas necesarias para la protección física de los equipos de telecomunicaciones, de manera que no estén accesibles al personal ajeno a las operaciones de la red. **[Hallazgo del 3-a.2)a) al c)]**

[3] En el *Manual* se indicaba que la última revisión fue en septiembre de 1995.

e. Almacene una copia de la documentación de las aplicaciones y los programas, y de los manuales de operación de los sistemas de información en la bóveda de la compañía contratada o en un lugar seguro fuera de los predios del Senado. **[Hallazgo 4-a.2)]**

f. El encargado de la administración de la red y de la seguridad de los sistemas de información:

1) Active las opciones correspondientes en la pantalla de políticas de auditorías (*Audit Policy*) que se mencionan en el **Hallazgo 5-a.1) y 2)**, de manera que se pueda mantener un rastro de las actividades realizadas en los servidores del Senado.

2) Evalúe e instale en los sistemas operativos de los servidores del Senado las actualizaciones de seguridad[4] y los *Update Rollups and Service Packs*[5] emitidos por el proveedor de dichos sistemas para mantener los mismos actualizados y así asegurar un funcionamiento más efectivo y eficaz de los sistemas de información. **[Hallazgo 5-a.3)]**

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

4) Elimine el acceso a los programas en producción otorgado a los programadores. **[Hallazgo 7]**

g. Se habiliten las librerías necesarias, distintas a la que se mantiene de los programas en producción, para que los programadores puedan realizar las pruebas para evaluar la efectividad y funcionalidad de los cambios efectuados a los programas.

---

[4] Programación publicada para atender algunas vulnerabilidades de seguridad descubiertas en el producto o programa.

[5] Es una actualización del sistema operativo que introduce nuevos atributos y funcionalidades, y mejora la confiabilidad del mismo.

El encargado de la seguridad de los sistemas de información debe ser responsable de copiar los programas correspondientes a la librería de prueba para que el programador pueda hacer los cambios solicitados. Cuando se obtenga la aprobación del usuario y la autorización de la persona designada para mantener la calidad, el encargado de la seguridad de los sistemas de información debe transferir dichos programas a la librería de producción. **[Hallazgo 7]**

2. Ver que el Secretario de Administración del Senado ejerza una supervisión eficaz sobre la Directora de Recursos Humanos para asegurarse de que notifique prontamente al CSI el cese de un usuario en sus funciones para la cancelación de su cuenta de acceso. **[Hallazgo 5-b.]**

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este *Informe* se remitió al Hon. Thomas Rivera Schatz, Presidente del Senado, para comentarios, en carta del 11 de febrero de 2009. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al Hon. Kenneth McClintock Hernández, ex Presidente del Senado, en carta de esa misma fecha.

COMENTARIOS DE LA GERENCIA

El Sr. Roberto Maldonado Vélez, Secretario de Administración del Senado, contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 8 de marzo de 2010[6]. El ex Presidente contestó el borrador de los **hallazgos del 1 al 5 y 7** de este *Informe* mediante carta del 1 de marzo de 2010. Los comentarios de dichos funcionarios fueron considerados en la redacción final del informe. Algunos de sus comentarios se incluyen en la segunda parte de este *Informe*, titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección HALLAZGOS EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DEL SENADO DE PUERTO RICO.

[6] En carta del 16 de marzo de 2010, el Presidente del Senado indicó que dicho documento fue remitido a esta Oficina como parte de la reacción del Senado al borrador de los **hallazgos** de este *Informe*.

AGRADECIMIENTO

A los funcionarios y a los empleados del Senado de Puerto Rico, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Por: Oficina del Contralor

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, un reglamento, una carta circular, un memorando, un procedimiento, una norma de control interno, una norma de sana administración, un principio de contabilidad generalmente aceptado, una opinión de un experto o un 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, las irregularidades o los 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 el borrador de los hallazgos 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 EL CENTRO DE SISTEMAS DE INFORMACIÓN DEL SENADO DE PUERTO RICO, 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 EL CENTRO DE SISTEMAS DE INFORMACIÓN DEL SENADO DE PUERTO RICO

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

Hallazgo 1 - Falta de segregación en las funciones realizadas por un Programador de Sistemas Electrónicos I

a. Al 9 de junio de 2008, un Programador de Sistemas Electrónicos I realizaba las funciones correspondientes a los puestos de Administrador y de Oficial de Seguridad de la Red. Estas funciones eran incompatibles con las que realizaba como Programador de Sistemas Electrónicos I, ya que le permitían otorgarse privilegios de acceso no autorizados, tanto al sistema operativo como al área de programación. Esta situación se agravaba al no existir un control alterno de supervisión por parte del Director del CSI sobre las tareas de este empleado.

   Una situación similar fue comentada en el informe *OAI-2008-02 del 18 de octubre de 2007* emitido por la Oficina de Auditoría Interna del Senado.

   En la *Política Núm. POL110, Segregación de Tareas*, del *Manual* se indica que esta política se emite con el propósito de establecer la segregación de tareas para evitar que los usuarios, programadores, analistas y operadores obtengan un nivel de acceso que podría perjudicar el sistema y la integridad de su información. Además, en dicha *Política* se establece que las actividades que realicen los programadores deben ser limitadas a la prueba de programas

y archivos, y que éstos no deben tener acceso a los archivos de producción, tener responsabilidades de usuario y tener acceso al uso de utilidades, tales como: descargar datos y realizar respaldos, y operar el sistema o acceder las librerías de aplicación.

Esta disposición es cónsona con las normas de control interno que requieren la segregación de funciones, de tal forma que no recaiga en la misma persona la ejecución de varias tareas que resulten conflictivas. Además, las normas generalmente aceptadas en el campo de la tecnología de información establecen que para poder fortalecer los controles establecidos sobre la información de la entidad es necesario que se segreguen las tareas relacionadas con el procesamiento de dicha información. Estos controles se mantienen, en parte, mediante la segregación de las tareas de administración y seguridad de la red, de aquellas relacionadas con la programación. El objetivo principal de dichos controles es disminuir la probabilidad de que se cometan errores o irregularidades y que no se detecten a tiempo.

La situación comentada puede propiciar que se incurra en errores o irregularidades y que no se puedan detectar con prontitud, con los consiguientes efectos adversos para el Senado.

La situación comentada se atribuye a que el Director del CSI no se había asegurado de mantener una segregación y supervisión adecuadas sobre las funciones realizadas por el Programador de Sistemas Electrónicos I.

En la carta del Secretario de Administración del Senado, éste indicó lo siguiente:

> El Centro de Sistemas de Información cuenta con un Manual de Políticas y Procedimientos efectivo el 20 de octubre de 2002 y que actualmente se encuentra vigente, debido a que el nuevo está en proceso de revisión y aprobación final. En la Política POL110, Segregación de Tareas, se indica que esto es con el propósito de evitar que los usuarios, programadores, analistas y operadores obtengan un nivel de acceso y comprensión que podría perjudicar el sistema y la integridad de su información. El Programador de Sistemas Electrónicos I, quien ejercía como Administrador de la Red, no afectaba o complicaba sus funciones, ya que en esos momentos el Centro contaba con dos programadores adicionales que cubrían las necesidades del Departamento. [*sic*]

En la carta del ex Presidente del Senado, éste indicó lo siguiente:

> Debido a que nuestra administración fue basada en concentrar los recursos económicos en lo que realmente es el proceso legislativo y enmarcada en la realidad fiscal donde el presupuesto del Senado, durante mi incumbencia fue igual o menor al anterior por cuatro años consecutivos, el reclasificar a un programador al título de administrador de la red representaría una erogación considerable ante nuestra realidad fiscal.

Consideramos las alegaciones del Secretario de Administración y del ex Presidente del Senado, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.a.

Hallazgo 2 - Falta de documentación de la justificación y de la autorización de los accesos a las cuentas de administrador de los sistemas operativos, y de la otorgación de privilegios de conexión remota a los sistemas de información

a. Al 28 de mayo de 2008, el personal del CSI no le proveyó a nuestros auditores los documentos justificantes autorizados de los accesos otorgados al Director del CSI, al *Webmaster*[7] y a un Programador de Sistemas Electrónicos I, quienes tenían asignada una cuenta con privilegios de administrador de los sistemas operativos. Una cuenta como ésta tiene amplios privilegios que permiten, entre otras cosas, realizar cambios a la configuración del sistema, instalar programas y equipos, acceder a todos los archivos de la computadora y realizar cambios a las cuentas de otros usuarios. Tampoco proveyó evidencia de los documentos justificantes autorizados para proveerle a dichos funcionarios y empleados el privilegio de conexión remota. Este tipo de privilegio permite acceder y utilizar la información computadorizada de una entidad gubernamental desde un lugar remoto o distinto de donde está guardada la misma. Además, permite administrar y realizar diagnósticos del funcionamiento de la red.

[7] Es la persona responsable del mantenimiento de una página en Internet.

Las normas generalmente aceptadas en el campo de la tecnología de información establecen que, si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la entidad gubernamental (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información. Esta norma se instrumenta, en parte, mediante:

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

- El establecimiento de normas y procedimientos específicos para la asignación del privilegio de administrador de los sistemas operativos y de acceso remoto a los usuarios, donde se incluya, entre otras cosas, el uso de un formulario en el que se documente la justificación para la otorgación de dichos privilegios.

La situación comentada impide mantener la evidencia requerida para otorgar los privilegios de administrador de los sistemas operativos y de conexión remota. También propicia que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada se atribuye a que al Director del CSI no había preparado ni remitido al Secretario del Senado, para aprobación, los procedimientos para la asignación del privilegio de administrador de los sistemas operativos y de conexión remota.

En la carta del Secretario de Administración del Senado, éste indicó lo siguiente:

> La documentación del Centro de Sistemas de Información no contiene políticas que establezcan el requisito de autorización para el uso de privilegios administrativos y el acceso a conexiones remotas. Se está evaluando modificar nuevamente el Formulario de Acceso al

> Sistema CSI-FOR-02 para que el mismo cumpla con las actualizaciones tecnológicas y éste a su vez incluya un área para la autorización al acceso a conexiones remotas.

En la carta del ex Presidente del Senado, éste indicó lo siguiente:

> Como debe ser de su conocimiento, el Director del CSI, es la autoridad administradora de los sistemas de información del Senado de Puerto Rico, incluso dentro de su descripción de tareas, del cual existe copia en su expediente establece como una de sus funciones el administrar la red del Senado de Puerto Rico por lo cual debe tener acceso a todos los niveles de acceso de los Sistemas de Información.
>
> Los Programadores I no tenían acceso total a los sistemas de información. Solo había un programador con privilegio de administrador, el Sr. […], quien realizaba funciones de administrador de la red. Por otro lado, el webmaster, tenía privilegios parciales de administrador de la red ya que adicional a sus funciones de webmaster, en sus funciones se encontraban el crear y modificar cuentas de usuarios. [*sic*]

Consideramos las alegaciones del Secretario de Administración y del ex Presidente del Senado, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.b.1).

Hallazgo 3 - Falta de controles ambientales y físicos en los cuartos de distribución de cableado de la red

a. El Senado tiene 11 cuartos de distribución de cableado de la red ubicados en 8 edificios[8]. El examen efectuado del 21 de diciembre de 2007 al 14 de febrero de 2008 de los controles ambientales[9] y físicos[10] existentes en los 11 cuartos de distribución, reveló que no existían

[8] Una relación de los cuartos de distribución de cableado y de los edificios donde estaban ubicados se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Presidente y al ex Presidente del Senado de Puerto Rico para comentarios.

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

[10] 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.

las condiciones de seguridad física adecuadas para proteger los sistemas de información computadorizados del Senado, según se indica:

1) Relacionado con los controles ambientales:

   a) Uno de los cuartos de distribución de cableado[11] tenía filtraciones de agua en el techo. Durante nuestro examen observamos que el equipo de la red estaba cubierto con un plástico para evitar que se mojara el mismo.

   b) En tres de los cuartos de distribución de cableado[11] se habían almacenado materiales inflamables, tales como: cajas de cartón, contenedores de pintura, rollos de cable de comunicación y teléfono, equipos de computadora, paneles de madera, y bolsas plásticas.

   c) El equipo de la red instalado en uno de los cuartos de distribución de cableado[11] tenía polvo acumulado.

2) Relacionado con los controles físicos:

   a) No se mantenía un control adecuado de las llaves de los cuartos de distribución de cableado, las cuales eran custodiadas por una Auxiliar en Sistemas de Oficina II del CSI. Al personal que se le facilitaba las mismas no se le requería que firmara la bitácora de las llaves. Además, las llaves de dos cuartos de distribución de cableado[11] no estaban bajo la custodia del personal del CSI. Estas llaves eran custodiadas por la Supervisora de Servicios Telefónicos del Senado y por un empleado del Centro de Sistemas de Información de la Oficina de Servicios Legislativos, respectivamente.

   b) Las puertas que daban acceso a tres de los cuartos de distribución de cableado[11] estaban abiertas.

[11] Véase la nota al calce 8.

c) Los armarios de seguridad utilizados para la distribución de cableado localizados en dos de los edificios[12] estaban abiertos.

d) Los cables de transmisión de los concentradores localizados en dos de los cuartos de distribución de cableado[12] no estaban debidamente organizados o distribuidos.

Las mejores prácticas en el campo de la tecnología de información sugieren que las entidades deberán tomar los cuidados necesarios para proteger y mantener en óptimas condiciones los equipos computadorizados, y evitar daños y averías. El propósito es asegurar la integridad, la exactitud y la disponibilidad de la información, y protegerla contra la destrucción accidental, entre otras cosas. Para garantizar razonablemente la seguridad de los equipos y los sistemas computadorizados, es necesario que se mantengan los equipos de computadoras y de comunicaciones en un lugar seguro, que provea las condiciones ambientales y físicas adecuadas, y que se controle adecuadamente el acceso a los mismos.

Las situaciones comentadas podrían limitar la disponibilidad de los sistemas computadorizados y, por consiguiente, limitar los servicios que presta el CSI.

Las situaciones comentadas en el **apartado a.1) y 2)d)** pudieran ocasionar daños y deterioros prematuros a los equipos de la red y a los de computadoras, lo que podría impedir el obtener el rendimiento máximo en términos de los servicios que éstos ofrecen.

Las situaciones comentadas en el **apartado del a.2)a) al c)** pudieran ocasionar que personas ajenas a la operación de la red tengan acceso a los cuartos de distribución de cableado y causen daño al equipo, por error o intención. Esto podría afectar adversamente el funcionamiento de la red y la continuidad de las operaciones.

Las situaciones comentadas en el **apartado a.** se debían, en parte, a que el Director del CSI no había tomado las medidas necesarias para que las instalaciones de los equipos computadorizados estuvieran ubicadas en lugares adecuados y seguros.

[12] Véase la nota al calce 8.

En la carta del Secretario de Administración del Senado, éste indicó lo siguiente:

> El Senado de Puerto Rico, consciente de la situación y carencia de controles ambientales y físicos en algunos de sus cuartos de comunicación, estudia la posibilidad de mudar algunas oficinas a edificios más seguros y a su vez revisará e implantará medidas y controles de seguridad en los mismos.

En la carta del ex Presidente del Senado, éste indicó lo siguiente:

> La operación del CSI estaba enmarcada en el Distrito Capitolino que lo conforman estructuras antiguas e históricas. Además, el mantenimiento físico de estas estructuras recaía sobre la Superintendencia del Capitolio la cual fuimos sumamente diligentes en la notificación y seguimiento en las peticiones de mejoras y reparaciones a la planta física, pero que no recibió un solo centavo de asignación de fondos para mejoras permanentes, habiendo vetado el Gobernador […] una asignación de $5 millones a esos efectos. [*sic*]

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

Véase la Recomendación 1.c. y d.

Hallazgo 4 - Falta de un registro de los respaldos enviados a la bóveda de la compañía contratada y, de almacenamiento de la documentación de las aplicaciones, los programas y los manuales de operación en un lugar seguro fuera de los predios del Senado

a. El CSI realizaba respaldos diarios de la información almacenada en los servidores de documentos (*Archive*) y en los que tenían las bases de datos con la información del Senado. Dichos respaldos se mantenían en los servidores, y semanalmente se preparaba una copia de éstos, la cual era entregada al personal de la compañía contratada con el propósito de mantenerlos almacenados fuera de los predios del Senado. El examen realizado del 8 al 16 de abril de 2008 sobre los respaldos de información reveló las siguientes deficiencias:

1) En el CSI no se mantenía un registro de las cintas enviadas a la bóveda de la compañía, 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 alguna, durante la preparación de los respaldos.

Una situación similar fue comentada en el informe *OAI-2008-02* emitido por la Oficina de Auditoría Interna del Senado.

Las mejores prácticas en el campo de la tecnología sugieren que las entidades deben establecer controles adecuados en sus sistemas computadorizados para garantizar la confiabilidad, la integridad y la disponibilidad de la información que manejan. Estos controles incluyen preparar y mantener copias de respaldo recurrente de la información, y de los programas de aplicación y de sistema esenciales e importantes para las operaciones de la entidad. Además, es necesario mantener un inventario detallado de estas copias de respaldo para facilitar su localización y para sustituir periódicamente, por cintas nuevas, las utilizadas para los respaldos. Este inventario permite, además, documentar el cumplimiento de las normas y los procedimientos establecidos.

2) El CSI no mantenía copia de la documentación de las aplicaciones y los programas, ni de los manuales de operación de sus sistemas de información en la compañía contratada o en un lugar seguro fuera de los predios del Senado.

Como norma de sana administración y de control interno, se requiere que las entidades gubernamentales mantengan copia actualizada de la documentación de las aplicaciones y los programas, y de los manuales de operación de sus sistemas de información, en un lugar seguro fuera del edificio donde radica el centro. Esto, es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado.

La situación comentada en el **apartado a.1)** no permitía mantener el control de los respaldos preparados y guardados en el servidor, ni de los enviados a la bóveda de la compañía contratada. Esto, de manera que pudiera asegurarse la protección y la disponibilidad de la información contenida en estos respaldos y evitar su pérdida permanente.

La situación comentada en el **apartado a.2)** podría afectar la continuidad de las operaciones normales del CSI si ocurriera alguna eventualidad que afectara las instalaciones de éste y destruyera toda la documentación y los manuales que allí se almacenan. Además, de ocurrir una emergencia que impida el acceso al CSI, el encargado de activar el *Plan de Contingencias* no tendría acceso a éstos para iniciar el proceso de reconstrucción de archivos y programas, y el restablecimiento y la continuidad de las operaciones normales de los sistemas de información en un tiempo razonable.

La situación comentada en el **apartado a.1)** se debía a que el Director del CSI no había preparado directrices específicas y detalladas para establecer un procedimiento escrito para los respaldos que describiera, entre otras cosas, el proceso de respaldar la información y los programas, el ciclo de reutilización de las cintas, la identificación adecuada de las cintas y el mantenimiento de un inventario actualizado de éstas.

La situación comentada en el **apartado a.2)** se debía a que el Director del CSI no había efectuado las gestiones necesarias para mantener copia de la documentación de las aplicaciones y los programas, y de los manuales de operación de los sistemas de información en un lugar seguro fuera de los predios del Senado.

En la carta del Secretario de Administración del Senado, éste indicó lo siguiente:

> Con el fin de cumplir con las mejores prácticas en el campo de la tecnología, el Centro de Sistemas de Información tomo acciones para corregir y mejorar los comentarios señalados en este hallazgo. El Centro adquirió equipos y facilidades nuevas para llevar a cabo mejor el proceso del almacenamiento de los respaldos de información. [*sic*]

Véase la Recomendación 1.b.2) y e.

Hallazgo 5 - Deficiencias en los parámetros de seguridad configurados en el sistema operativo de los servidores de la red y en el proceso de desactivar las cuentas de acceso de los ex empleados

a. El examen efectuado el 16 de junio de 2008 sobre los parámetros de seguridad configurados en el sistema operativo de tres servidores[13], reveló las siguientes deficiencias:

1) En dos de los servidores no se había activado la política de auditoría (*Audit Policy*) para que el sistema produjera un registro cuando ocurrieran los siguientes eventos:

- La creación, modificación o eliminación de una cuenta o grupo de usuarios, el cambio de nombre o contraseña y la activación o desactivación de una cuenta o grupo de usuarios (*Audit account management*)

- Los accesos a los archivos, cartapacios (*folders*) e impresoras (*Audit object access*)

- Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Audit policy change*)

- El uso de los privilegios de los usuarios (*Audit priviledge use*)

- Las acciones ejecutadas de los procesos (*Audit process tracking*)

- El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*Audit system events*).

2) En un servidor no se había activado la política de auditoría para que el sistema produzca un registro de las solicitudes al servidor para validar una cuenta de usuario (*Audit account logon events*).

[13] Una relación de los servidores se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Presidente y al ex Presidente del Senado de Puerto Rico para comentarios.

3) En los servidores no se habían instalado actualizaciones de seguridad y *Update Rollups and Service Packs*, según se indica:

   - Un servidor tenía seis actualizaciones de seguridad y un *Update Rollups and Service Packs* sin instalar.

   - Un servidor tenía cinco actualizaciones de seguridad y dos *Update Rollups and Service Packs* sin instalar.

   - Un servidor tenía cuatro actualizaciones de seguridad y un *Update Rollups and Service Packs* sin instalar.

Las mejores prácticas en el campo de la tecnología de información sugieren que se deberán implantar controles que minimicen los riesgos de que los sistemas computadorizados dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Estos controles se establecen, en parte, mediante:

- La activación de todas las opciones para registrar los eventos de seguridad de las aplicaciones y del sistema operativo

- La instalación de las actualizaciones de seguridad, de manera que se puedan atender las vulnerabilidades descubiertas en los sistemas y evitar nuevas amenazas a los mismos.

Las situaciones comentadas en el **apartado a.1) y 2)** impiden la detección temprana de errores críticos o problemas con los servidores, que permita tomar de inmediato las medidas preventivas y correctivas necesarias. Además, privan a la gerencia de las herramientas necesarias para supervisar eficientemente los trabajos realizados por los usuarios y detectar el acceso y uso indebido de los sistemas computadorizados.

La situación comentada en el **apartado a.3)** puede impedir la prevención y la detección de programas no deseados, y permitir que éstos puedan propagarse a los sistemas de información, lo que afectaría la integridad, la confidencialidad y la disponibilidad de los sistemas de información del Senado.

Las situaciones comentadas se debían, en parte, a que el Director del CSI no le había impartido instrucciones al Programador de Sistemas Electrónicos I para que:

- Activara las opciones de seguridad que proveen los sistemas operativos y examinara periódicamente los registros de seguridad **[Apartado a.1) y 2)]**

- Instalara en los sistemas operativos de los servidores antes mencionados, las últimas actualizaciones de seguridad y los *service packs* emitidos por el proveedor de dichos sistemas. **[Apartado a.3)]**

b. El examen efectuado del 25 al 29 de agosto de 2008 reveló que no se habían eliminado de los sistemas de información del Senado las cuentas de acceso de nueve ex empleados[14]. Éstos habían renunciado entre el 30 de junio de 2006 y el 30 de abril de 2008.

En el *Procedimiento Núm. PRO520, Revocar el Acceso al Sistema,* del *Manual* se establece, entre otras cosas, que el Director de Personal enviará mensualmente al Oficial de Seguridad una lista de los ex empleados del Senado para que desactive sus cuentas y las elimine del sistema.

Las normas generalmente aceptadas en el campo de la tecnología de información establecen que las entidades tendrán la responsabilidad de desarrollar políticas y directrices que permitan establecer los controles adecuados en sus sistemas computadorizados para minimizar los riesgos de que la información sea accedida de forma no autorizada. Esto se instrumenta, en parte, mediante la notificación inmediata al Director del CSI del cese de un usuario en sus funciones para la cancelación de su cuenta de acceso.

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

[14] Los nombres de los ex empleados se incluyeron en el borrador de los **hallazgos** de este *Informe* remitido al Presidente y al ex Presidente del Senado de Puerto Rico para comentarios.

La situación comentada se atribuye a la falta de comunicación efectiva entre la Oficina de Recursos Humanos, el área de trabajo del empleado y el CSI, para informar los cambios en las funciones de los usuarios de los sistemas de información, de modo que los privilegios de acceso se mantuvieran actualizados.

En la carta del Secretario de Administración del Senado, éste indicó lo siguiente:

> El Centro de Sistemas de Información cuenta con equipos tecnológicos dedicados a los sistemas de información, los cuales están configurados conforme con la realidad y necesidad del Senado de Puerto Rico. Como medida preventiva de seguridad y luego de analizar los puntos señalados en este hallazgo, los parámetros de seguridad de los sistemas fueron revisados y modificados, no obstante, la configuración y los hallazgos encontrados a la hora del examen realizado, no representaban un riesgo para la seguridad de los sistemas de información del Senado de Puerto Rico.

En la carta del ex Presidente del Senado, éste indicó lo siguiente:

> Debemos señalar que la sección (a) del hallazgo 5 fue corregida en medio del proceso de auditoría.
>
> En la sección b del hallazgo 5, establece que 9 de sobre probablemente 900 usuarios que mantuvo el Senado de Puerto Rico durante ese período, que a su vez representa quizás el 1 por ciento de los usuarios, mantuvieron cuentas activas luego de cesar como empleados. Aunque entendemos que nuestra meta siempre fue el cero por ciento nos parece que el 1 por ciento se encuentra dentro de los parámetros razonables de error. No obstante, el CSI dependía de la notificación por parte del Departamento de Recursos Humanos del Senado de Puerto Rico para proceder con la desactivación de la cuenta. El acceso que tenían estos usuarios, según me ha informado, no era en áreas particularmente sensitivas y reflejaba, en gran medida, los accesos a los que tenía un ciudadano particular que accediera a nuestro sistema en búsqueda de información.

Consideramos las alegaciones del ex Presidente del Senado con respecto al **apartado b. del Hallazgo**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones de la 1.f.1) a la 3) y 2.

Hallazgo 6 - Falta de actualización del Manual de Políticas y Procedimientos y del *Design, Development and Implementation Standards,* y de normas y procedimientos escritos para la administración y el control de los sistemas operativos y de los programas utilitarios

a. El *Manual* tiene como propósito definir en forma clara las responsabilidades del CSI. Este consiste de dos tipos de documentos: políticas y procedimientos. El examen realizado el 11 de marzo de 2008 sobre el *Manual*, reveló que el mismo no se había revisado desde septiembre de 1995, por lo que en los procedimientos se hacía referencia a equipos y a puestos[15] que ya no existían en el CSI. Además, en el *Manual* no se incluía el puesto de Administrador de la Red.

b. El objetivo del *Design, Development and Implementation Standards* es definir claramente los estándares que deberá cumplir el personal del CSI que labora en el diseño, el desarrollo y la implantación de los sistemas computadorizados. El examen realizado al contenido de este manual reveló que no había sido revisado desde septiembre de 1999. Además, el personal del Área de Programación no tenía conocimiento de la existencia del mismo.

   Situaciones similares fueron comentadas en el informe *OAI-2008-02* emitido por la Oficina de Auditoría Interna del Senado.

c. Al 20 de mayo de 2008, el Senado no había promulgado normas ni procedimientos escritos necesarios para reglamentar los siguientes procesos relacionados con la administración y el control de los sistemas operativos y de los programas utilitarios:

   - El control de acceso y el uso de los programas utilitarios
   - La instalación de los sistemas operativos
   - La identificación y la documentación de los problemas relacionados con los sistemas operativos
   - El control de cambios para la configuración de la aplicación de sistemas operativos

[15] La información detallada de los equipos y de los puestos se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Presidente y al ex Presidente del Senado de Puerto Rico para comentarios.

En el Artículo 7, Funciones y Deberes del Director, del *Reglamento del Centro de Sistemas de Información del Senado de Puerto Rico*[16], según enmendado, aprobado por el Presidente del Senado mediante la *Orden Administrativa 07-08 del 30 de junio de 2007*, se establece, entre otras cosas, que:

> El Director del Centro preparará y someterá al Presidente un documento contentivo de las normas y reglas de organización y funcionamiento interno de dicho Centro, el cual deberá ser aprobado por el Presidente. Dicho documento contendrá, entre otras cosas, todas las normas y los procedimientos relativos a las áreas operacionales del Centro, incluido la activación de sistemas, la producción de copias de respaldo, las normas de acceso y seguridad, y el control y la retención de archivos.

En el *Manual* se establece la importancia de que el mismo se mantenga al día. Cada vez que ocurra un cambio operacional en el CSI, éste debe ser incluido en el *Manual*. En éste se recomienda que todas las políticas y los procedimientos sean revaluados, por lo menos, cada dos años.

Las mejores prácticas en el campo de la tecnología sugieren que se establezcan por escrito normas, procedimientos y políticas de control eficaces que reglamenten las operaciones computadorizadas y que estén aprobadas por la alta gerencia. Mediante los mismos, se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en casos de renuncias o ausencias de personal de mayor experiencia y facilitan la labor de adiestramiento. Una vez establecidos, las normas, los procedimientos y las políticas deben ser divulgados al personal pertinente, y deben ser revisados y actualizados conforme a los cambios ocurridos en los sistemas, los equipos y el personal.

Las situaciones comentadas podrían ocasionar que las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar

[16] Mediante la *Orden Administrativa Núm. 07-10 del 20 de septiembre de 2007* se le asignó el número 42 a dicho *Reglamento* y se enmendó el Artículo 8 del mismo.

responsabilidades y tomar las medidas correctivas necesarias. Además, podría exponer al personal, a los equipos y a la información del Senado a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a que el Director del CSI no había realizado las gestiones necesarias para que se actualizara el *Manual* y el *Design, Development and Implementation Standards* conforme a los cambios operacionales ocurridos desde la última revisión de los mismos.

La situación comentada en el **apartado c.** denota la falta de gestiones de parte del Director del CSI para que se prepararan y se le remitieran, para la consideración y aprobación del Secretario del Senado, las normas y los procedimientos escritos necesarios para el control y la administración de los sistemas operativos y de los programas utilitarios.

En la carta del Secretario de Administración del Senado, éste indicó lo siguiente:

> El Centro de Sistemas de Información junto a la Administración del Senado de Puerto Rico, se encuentra en el proceso de creación y revisión de los manuales existentes relacionados con la operación del Centro y su Departamento de Programación.

Véase la Recomendación 1.b.3).

Hallazgos 7 - Cambios realizados en las librerías de los programas en producción

a. El examen efectuado el 5 de mayo de 2008 reveló que los cambios a los programas que estaban en producción no se realizaban en librerías de prueba. Estos cambios eran realizados directamente en las librerías de producción.

Situaciones similares fueron comentadas en el informe *OAI-2008-02* emitido por la Oficina de Auditoría Interna del Senado.

En la *Política Núm. POL200* del *Manual* se establece, entre otras cosas, que la librería de producción es sólo accesible al Oficial de Seguridad. Ésta será la persona a quien los programadores le solicitarán que copie programas o archivos en sus librerías de prueba para

programar. Además, se establece que cada programador tiene su librería de prueba en la que podrá hacer las modificaciones o los desarrollos requeridos, los cuales tienen que ser aprobados por el usuario y la persona designada para mantener la calidad, antes de que se autorice su paso a la librería de producción. El Oficial de Seguridad será la persona responsable de pasar los cambios a las librerías de producción correspondientes.

La situación comentada puede propiciar que un cambio o modificación sea implantado en una de las librerías de producción, sin antes haber sido debidamente autorizado. Además, dificulta el mantener un rastro de las modificaciones implantadas, lo que impide mantener el debido control de calidad y la documentación necesaria del proceso de desarrollo o cambio realizado a las aplicaciones.

La situación comentada se atribuye a que en el CSI no se había establecido una librería para realizar las pruebas a los cambios efectuados a los programas. Tampoco se le había restringido el acceso a los programadores a la librería donde se mantenían los programas en producción.

En la carta del Secretario de Administración del Senado, éste indicó lo siguiente:

> El Departamento de Programación tiene la tarea de mecanizar los procesos de acuerdo a las necesidades de los empleados del Senado de Puerto Rico. Estos procesos son relacionados estrictamente al trabajo legislativo y no conllevan un riesgo para el Senado, ya que los mismos sirven para agilizar procesos y no para almacenar información crítica. La información crítica y sensitiva relacionada a las funciones administrativas del Senado de Puerto Rico no es modificada por los programadores, manteniendo así la seguridad e integridad de la misma. Cabe señalar que estos datos son custodiados por el Centro y a su vez están sujetos a las políticas de resguardo de información a llevarse a cabo el Centro. [*sic*]

En la carta del ex Presidente del Senado, éste indicó lo siguiente:

> Como se le explicó a los auditores en el proceso de auditoría, en ocasiones las dependencias del Senado de Puerto Rico requerían cambios pequeños en sus aplicaciones a ser realizados en un limitado período de tiempo que no requerían ser trabajadas en un ambiente de prueba y eran trabajados directamente en la aplicación en producción.

Consideramos las alegaciones del Secretario de Administración y del ex Presidente del Senado, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.f.4) y g.

ANEJO

SENADO DE PUERTO RICO

CENTRO DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Hon. Kenneth McClintock Hernández	Presidente del Senado	31 ag. 07	25 ag. 08
Sr. Manuel A. Torres Nieves	Secretario del Senado	31 ag. 07	25 ag. 08
Sr. Freddy Vélez García	Secretario de Administración del Senado	31 ag. 07	25 ag. 08
Sr. Luis Caraballo Cartagena	Director del Centro de Sistemas de Información	31 ag. 07	25 ag. 08