INFORME ESPECIAL TI-09-05

15 de julio de 2008

RESULTADO DEL EXAMEN DE LOS CONTROLES Y EL USO DE LA RED DE COMUNICACIONES DE LA OFICINA DE SERVICIOS LEGISLATIVOS

(Unidad 5384 - Auditoría 12977)

Período auditado: 27 de noviembre de 2006 al 31 de mayo de 2007

CONTENIDO

Página

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

15 de julio de 2008

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

Realizamos un examen de los controles y el uso de la red de comunicaciones (Red) de la Oficina de Servicios Legislativos (OSL). Efectuamos el mismo 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 del 25 de julio de 1952** y en la **Ley Núm. 9 del 24 de julio de 1952**, según enmendada.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El 14 de noviembre de 1953 los presidentes de las Cámaras Legislativas encomendaron a un consultor efectuar un estudio y preparar un informe con recomendaciones para la creación de una Oficina de Servicios Legislativos similar a la que funciona en el Congreso de los Estados Unidos de América y otros cuerpos legislativos estatales.

El informe de dicho consultor fue sometido a la Comisión de Actividades Conjuntas de la Asamblea Legislativa, el cual fue aprobado con enmiendas por dicha Comisión el 27 de enero de 1954. Con la aprobación de este informe quedó constituida la OSL. Ésta tiene la responsabilidad, entre otras, de considerar y resolver consultas legales, redactar anteproyectos de ley y resoluciones, revisar borradores de medidas legislativas y redactar opiniones legales.

Las operaciones y el funcionamiento de la OSL son coordinados por un Director nombrado por mutuo acuerdo por los presidentes del Senado de Puerto Rico y de la Cámara de Representantes.

El Centro de Sistemas de Información (CSI) tiene la responsabilidad de administrar la red de la Asamblea Legislativa de Puerto Rico; mantener la seguridad y la integridad de los sistemas de información; desarrollar nuevas aplicaciones y mantener las aplicaciones existentes; administrar el correo electrónico; coordinar los trabajos de los consultores externos de sistemas de información; y mantener la conexión para la comunicación con las redes de la OSL, UPRNet, Oficina de Gerencia y Presupuesto, el Senado de Puerto Rico, la Cámara de Representantes, Superintendencia del Capitolio, la Oficina del Historiador de Puerto Rico y el Archivo de Documentos Legislativos de las Comisiones para permitir el intercambio de información vital en el proceso legislativo para los miembros de la Asamblea Legislativa. Para esto, el CSI cuenta con 13 servidores.

La OSL cuenta con una página de Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.oslpr.org/. Esta página provee información acerca de la entidad y de los servicios que presta.

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

El CSI no tenía presupuesto asignado. Los gastos de operación se sufragaban del presupuesto asignado a la OSL que para el año fiscal 2006-07 fue de $13,078,000.

RESPONSABILIDAD DE LA GERENCIA

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

1. Adoptar normas y procedimientos escritos que contengan controles internos de administración y de contabilidad eficaces, y observar que se cumpla con los mismos.

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

Examinamos el contenido de los archivos donde se registraban todas la páginas de direcciones de Internet (*web logs*) que fueron accedidas por las cuentas de usuarios de la OSL entre el 16 de junio y el 30 de noviembre de 2006.

Para efectuar la auditoría especial utilizamos la siguiente metodología:

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

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones del CSI en lo que concierne a los controles y el uso de la Red no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 5**, clasificados como principales.

En la parte de este **Informe Especial** titulada **RELACIÓN DETALLADA DE HALLAZGOS** se presentan dichos **hallazgos**.

RECOMENDACIONES

AL DIRECTOR DE LA OFICINA DE SERVICIOS LEGISLATIVOS

1. Ejercer una supervisión eficaz sobre el Director del CSI para que:

    a. 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:

        1) Páginas de los sondeos electrónicos. **[Hallazgo 1-a.1)]**

        2) Páginas de Internet con contenido ajeno a la gestión pública. **[Hallazgo 1-a.2)]**

    b. Revise el **Análisis de Riesgo 2005** para que se incluyan los criterios descritos en el **Hallazgo 2** y luego lo someta para su consideración y aprobación.

    c. Realice las gestiones pertinentes para la preparación de un **Plan de Continuidad de Negocios** que incluya el **Plan de Contingencias** actualizado y someta el mismo para su consideración y aprobación. **[Hallazgo 3]**

    d. Efectúe las modificaciones en los parámetros de seguridad de los servidores de la Red para habilitar la función de expiración a todas las contraseñas de las cuentas de usuarios. **[Hallazgo 4]**

    e. Redacte y someta para su aprobación las normas y los procedimientos escritos necesarios para asegurar que toda instalación correspondiente a la Red se realice con

uniformidad basado en sus requerimientos mínimos y cumpliendo los estándares y las mejores prácticas de la industria. Además, incluya la documentación mínima requerida sobre la configuración y cómo se debe documentar la infraestructura de la Red. **[Hallazgo 5]**

CARTAS A LA GERENCIA

Las situaciones comentadas en los hallazgos de este **Informe Especial** fueron sometidas al Director de la OSL, Lic. Francisco J. Domenech Fernández, en carta del 10 de marzo de 2008.

COMENTARIOS DE LA GERENCIA

En carta del 2 de abril de 2008 el Director de la OSL informó sus comentarios al borrador de los **hallazgos** de este **Informe Especial**. Los comentarios sometidos por el Director de la OSL fueron considerados en la redacción final del informe. Algunos de éstos se incluyen en la sección de este **Informe Especial** titulada HALLAZGOS DEL EXAMEN DE LOS CONTROLES Y EL USO DE LA RED DE COMUNICACIONES DE LA OFICINA DE SERVICIOS LEGISLATIVOS.

AGRADECIMIENTO

A los funcionarios y empleados de la OSL 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 DEL EXAMEN DE LOS CONTROLES Y EL USO DE LA RED DE COMUNICACIONES DE LA OFICINA DE SERVICIOS LEGISLATIVOS, 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 DEL EXAMEN DE LOS CONTROLES Y EL USO DE LA RED DE COMUNICACIONES DE LA OFICINA DE SERVICIOS LEGISLATIVOS

Los **hallazgos del 1 al 5** se clasifican como principales.

Hallazgo 1 - Accesos a Internet con fines ajenos a la gestión pública

a. La OSL mantenía un servidor[1] en la Red que permitía acceso a Internet a los usuarios autorizados. Dicho servidor producía diariamente un archivo en el cual se registraban todas las páginas de direcciones de Internet (*web logs*) que fueron accedidas por las cuentas de usuarios.

Examinamos los *web logs* del mencionado servidor correspondientes al período del 16 de junio al 30 de noviembre de 2006. El examen efectuado reveló lo siguiente:

1) Veinte cuentas de acceso de usuarios se utilizaron para realizar 894 enlaces a una página electrónica de Internet, correspondientes a 34 sondeos realizados en diferentes fechas por un periódico principal del País. Dicha página electrónica fue creada por el periódico con un formulario electrónico para los cibernautas interesados en contestar las preguntas sobre los sondeos de opinión pública. Los referidos enlaces fluctuaron entre 1 y 656 ocasiones por cuenta de usuario. Los enlaces realizados representan un fin ajeno a la gestión pública.

[1] El nombre del servidor se incluyó en el borrador de los hallazgos del informe sometido para comentarios al Director de la OSL.

2) Se accedieron páginas de Internet con contenidos ajenos a la gestión pública[2].

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 la **Norma OSLNS 99-021, Uso personal de la computadora y sistemas de comunicación del Manual de Normas de Seguridad de la Información de los Sistemas de Computadoras de la Oficina de Servicios Legislativos (Manual de Normas de Seguridad)**, aprobado el 1 de marzo de 1999 por el Director de la OSL, se establece que los sistemas de computadoras y de comunicación de la OSL se utilizarán para asuntos oficiales solamente. Además, en la **Carta Normativa Núm. 05-03**[3], **Enmiendas al Reglamento Manual de Normas de Seguridad de la Información de los Sistemas de Computadoras de marzo de 1999 de la Oficina de Servicios Legislativos**, aprobada el 22 de febrero de 2005 por el Director de la OSL, se dispone que los sistemas de correo electrónico se utilizarán sólo para asuntos oficiales, que el uso de los sistemas para asuntos personales o ajenos a los intereses de la OSL interfiere con las actividades normales de la agencia y que estas acciones están claramente prohibidas por la **Constitución** y las leyes, y el empleado que incurra en estas prácticas estará expuesto a sanciones disciplinarias.

El uso de las cuentas pertenecientes a la OSL para acceder a Internet para asuntos ajenos a la gestión pública es contrario al interés público y desvirtúa los propósitos para los cuales fueron creadas y asignadas. Además, provee al personal que indebidamente las utiliza unas ventajas, beneficios y privilegios que no están permitidos por ley.

---

[2] Dicha información fue suministrada al Director de la OSL en la carta del 10 de marzo de 2008.

[3] Esta **Carta Normativa** enmendó la **Norma OSLNS 99-96, Uso personal de los sistemas de correo electrónicos,** del **Manual de Normas de Seguridad de la Información de los Sistemas de Computadoras de la Oficina de Servicios Legislativos**.

Las situaciones comentadas se atribuyen, en parte, a que el Director del CSI no había establecido el mecanismo para impedir que las cuentas de acceso a Internet pudieran acceder los sondeos de opinión pública que se presentan en las páginas electrónicas de los periódicos principales del País y otras páginas con contenido ajeno a la gestión pública.

El Director de la OSL, en la carta que nos envió, informó, entre otras cosas, que:

> La aseveración hecha en los referidos incisos parte de una conclusión equivocada sobre los accesos a las páginas de sondeos. Surge de la documentación incluida, evidencia contundente que reduce dicha cifra en un 85 por ciento. Es decir, que 656 accesos fueron provocados por un código HTML de la página electrónica de un periódico principal del país, que fuerza una descarga automática sin autorización ni conocimiento del usuario y 104 récords que corresponden a la descarga de imágenes incorrectamente incluidos. **[Apartado a.1)]**
>
> El Centro de Sistemas de Información tiene la responsabilidad de identificar páginas con contenido ajeno a la gestión pública para prohibir el acceso a las mismas. Esperamos que el hallazgo no se refiera a tales entradas que son ejemplo de nuestro esfuerzo continuo por mantener nuestra red dentro de los estándares de seguridad y de ley aplicables. **[Apartado a.2)]**

Consideramos las alegaciones del Director de la OSL, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.a.

Hallazgo 2 - Falta de información en el Análisis de Riesgo

a. Al 28 de noviembre de 2006 el **Análisis de Riesgo 2005** carecía de la siguiente información, que debe ser parte esencial de un informe de avalúo de riesgo:

- El inventario de los activos de sistemas de información que detallara los equipos, programas y datos, y su valorización y clasificación de acuerdo con la misión y los servicios que presta la OSL.

- La identificación de las posibles amenazas y vulnerabilidades que podrían afectar los activos de la entidad junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas.

- El examen cualitativo y cuantitativo de las posibles amenazas, de acuerdo a un orden de prioridades.

- La selección e implantación de los controles de medidas de seguridad para proteger los activos.

- Las conclusiones de la gerencia en respuesta a su evaluación del riesgo (aceptación, transferencia, reducción o ignorar el riesgo).

En la **Norma OSLNS 99-070, Evaluación anual sobre la importancia de las aplicaciones de los usuarios del Manual de Normas de Seguridad** se establece que la Unidad de Trabajo del CSI, conjuntamente con los dueños de información relevante, deberá preparar periódicamente una evaluación del grado de importancia de todas las aplicaciones del usuario de computadora. Esto ayudará a mantener al día el plan de contingencia.

Las mejores prácticas en el campo de la tecnología de información sugieren que cada entidad deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Para ello deberá realizar un análisis de riesgos que incluya:

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

- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido a los datos) junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer con qué se van a proteger los activos identificados anteriormente.

Además, se deben establecer normas y procedimientos por escrito para garantizar la integridad, confidencialidad y disponibilidad de los sistemas críticos, de modo que se

garantice la continuidad de las operaciones en la eventualidad de que sucesos inesperados ocurran. Ello implica, entre otras cosas, que la entidad debe desarrollar e implantar un programa de avalúo y administración de riesgos para identificar los activos y recursos que se deben proteger, clasificando los mismos en términos de criticidad y sensibilidad. Luego de la identificación y clasificación de los activos y recursos, se identifican los elementos de riesgos que podrían afectar los mismos, específicamente los sistemas de información, para entonces determinar la probabilidad de que las amenazas o los eventos ocurran y el impacto que tendrían sobre las operaciones.

La situación comentada impide a la OSL evaluar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos. Además, impide el desarrollo de un **Plan de Continuidad de Negocios** donde se establezcan las medidas de control que minimizarían los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones de la entidad en caso de que surja alguna eventualidad. **[Véase el Hallazgo 3]**

La situación comentada se atribuye a que el Director del CSI no se aseguró de que se efectuara y documentara el análisis de riesgos conforme a las mejores prácticas en el campo de la tecnología de información.

El Director de la OSL, en la carta que nos envió, informó, entre otras cosas, las medidas implantadas para corregir la situación comentada.

Véase la Recomendación 1.b.

Hallazgo 3 - Falta de un Plan de Continuidad de los Negocios y de actualización del Plan de Contingencias para los sistemas de información de la OSL

a. La OSL carecía de un **Plan de Continuidad de Negocios** que incluyese los planes específicos, completos y actualizados del CSI. Ello era necesario para lograr un pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones del CSI, en caso de riesgos como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros.

Las mejores prácticas en el campo de la tecnología de información sugieren que las entidades deberán desarrollar un **Plan de Continuidad de Negocios** que incluya un **Plan para la Recuperación de Desastres** y un **Plan para la Continuidad de las Operaciones**.

b. El **Plan de Contingencias (Plan)** del CSI que nos fue provisto para examen el 11 de diciembre de 2006 no había sido actualizado conforme a los cambios de equipos y sistemas de información que se habían efectuado a partir de marzo de 1999.

En la **Norma OSLNS 99-071, Preparación y mantenimiento del plan de contingencia para sistemas de información en caso de emergencias y desastres del Manual de Normas de Seguridad** se establece que la administración deberá preparar, actualizar periódicamente y probar regularmente los planes de contingencia en casos de emergencia, lo cual permitiría a los sistemas esenciales de computadora continuar procesando en caso de degradación o interrupción del servicio o en caso de una pérdida mayor como inundación o terremoto.

En la **Norma OSLNS 99-074, Inventario anual del *hardware* y del *software* de los sistemas de información del Manual de Normas de Seguridad** se establece que para poder restablecer rápidamente el ambiente actual de las computadoras después de un desastre y como parte de la actualización periódica del **Plan de Contingencias**, la Unidad de Trabajo del CSI debe preparar un inventario anual de los sistemas de producción de información. Este inventario deberá indicar todo el *hardware*, programas y enlaces de comunicación de datos existente.

Las mejores prácticas utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados sugieren que como parte del **Plan de Continuidad de Negocios** se deberá preparar un **Plan de Contingencias**. Dicho **Plan** debe mantenerse actualizado y listo para implantarse cuando sea necesario.

De ocurrir una emergencia, la falta de planes por escrito o el desconocimiento de los mismos para atender la emergencia podría dar lugar a que el equipo no se proteja adecuadamente y sufra daños materiales, así como la pérdida de información importante.

Además, se podría atrasar el proceso de reconstrucción de archivos y de programas, así como el pronto restablecimiento y continuidad de las operaciones normales del Sistema. Esto tendría consecuencias adversas para la OSL.

Las situaciones comentadas se atribuyen a que el Director del CSI no se aseguró de que se actualizara el **Plan de Contingencias** y se preparara el **Plan de Continuidad de Negocios**, a fin de que sirvan como herramientas para responder ante cualquier incidente o desastre que ocurra.

El Director de la OSL, en la carta que nos envió, informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación 1.c.

Hallazgo 4 - Deficiencias en los parámetros de acceso lógico de los servidores de la Red

a. El examen realizado el 30 de noviembre de 2006 a los parámetros de seguridad relacionados con las cuentas de acceso en los 13 servidores de la OSL reveló que no se había establecido una fecha de expiración a la contraseña de una cuenta de acceso[4] creada localmente en 8 servidores[5] y 2 cuentas de acceso[4] creadas localmente en 3 servidores[5], lo que le permitía a los usuarios mantener la misma contraseña por tiempo indefinido. Dos de las cuentas de acceso[4] tenían asignados privilegios de administrador que permiten, entre otras cosas, crear, modificar, eliminar cuentas de usuarios y utilizar las herramientas de administración del servidor.

[4] Una relación de las cuentas de acceso se incluyó en el borrador de los hallazgos del informe sometido para comentarios al Director de la OSL.

[5] Una relación de los servidores se incluyó en el borrador de los hallazgos del informe sometido para comentarios al Director de la OSL.

En la **Norma OSLNS 99-007, Cambios periódicos obligatorios de las claves de acceso del Manual de Normas de Seguridad** se establece que todo usuario está obligado a cambiar su clave de acceso por lo menos una vez cada noventa (90) días. Ello implica que, como norma de sana administración, se activen y utilicen todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos.

La situación comentada impedía que el sistema les requiriera automáticamente a los usuarios el cambio de contraseña según el término establecido por la OSL. Mantener la misma contraseña por tiempo prolongado puede propiciar que personas no autorizadas adquieran conocimiento de ésta y logren acceso no autorizado al sistema y a la información. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que se puedan detectar a tiempo para fijar responsabilidades.

Las situaciones comentadas se debían, en parte, a que el Director del CSI, que fungía como Administrador de las Redes de Comunicaciones, no había puesto en vigor todas las opciones de seguridad de acceso lógico.

El Director de la OSL, en la carta que nos envió, informó, entre otras cosas, las medidas implantadas para corregir la situación comentada.

Véase la Recomendación 1.d.

Hallazgo 5 - Falta de normas y de procedimientos escritos para establecer los requerimientos mínimos para la instalación, configuración y documentación de la Red

a. Al 31 de mayo de 2007 la OSL no había establecido normas y procedimientos para establecer los requerimientos mínimos para la instalación, configuración y documentación de la Red.

Las mejores prácticas en el campo de la tecnología de información sugieren que se deben establecer por escrito normas, procedimientos y políticas de control interno eficaces que reglamenten las operaciones computadorizadas y que estén aprobadas por la alta gerencia.

Mediante las mismas se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuye a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia y facilita la labor de adiestramiento.

La situación comentada podría ocasionar que las operaciones de la Red no se efectúen uniformemente. Ello reduciría la eficacia y los controles de la misma, lo que expondría la información disponible en ésta a riesgos innecesarios. Además, afectaría la toma de decisiones al momento de modificar la Red o alguno de sus componentes.

La situación comentada denota falta de gestiones de parte del Director del CSI para que se prepararan y se le sometieran, para la consideración y aprobación del Director de la OSL, las normas y los procedimientos por escrito necesarios para reglamentar los procesos que se indican.

El Director de la OSL, en la carta que nos envió, informó, entre otras cosas, que el Centro de Sistemas de Información de la Oficina de Servicios Legislativos mantiene al día las normas y disposiciones que atienden aspectos neurálgicos, concernientes a las redes de comunicación. Tratándose de un tema tan abarcador y cambiante, procuramos la vigencia de cada uno de estos materiales. Es importante destacar que en el período comprendido en la auditoría, existían procedimientos, documentación y configuración relacionados a las redes de comunicación.

Consideramos las alegaciones del Director de la OSL, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.e.

ANEJO

RESULTADO DEL EXAMEN DE LOS CONTROLES Y EL USO DE LA RED DE COMUNICACIONES DE LA OFICINA DE SERVICIOS LEGISLATIVOS

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Lic. Francisco J. Domenech Fernández	Director de la Oficina de Servicios Legislativos	27 nov. 06	31 may. 07
Sr. Andrés Colón Pérez	Director del Centro de Sistemas de Información	27 nov. 06	31 may. 07