INFORME DE AUDITORÍA TI-06-12

12 de junio de 2006

Comisión Industrial de Puerto Rico

Área de Tecnología y Sistemas de Información

(Unidad 5222 - Auditoría 12686)

Período auditado: 22 de noviembre de 2004 al 15 de agosto de 2005

CONTENIDO

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

12 de junio de 2006

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

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

Determinamos emitir varios informes de esta auditoría. Este es el primer informe y contiene el resultado de nuestro examen sobre el desarrollo y control de los cambios de las aplicaciones, los controles de acceso, la administración del programa de seguridad, la segregación de deberes, los controles de los sistemas operativos y la evaluación de la continuidad del servicio establecidos en el ATSI.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Comisión fue creada mediante la **Ley Núm. 45 del 18 de abril de 1935**, **Ley del Sistema de Compensación por Accidentes del Trabajo**, según enmendada. La Comisión tiene funciones de naturaleza cuasijudicial y cuasitutelar para la investigación y resolución de todos los casos de accidentes en los cuales el Administrador de la Corporación del Fondo del Seguro

del Estado y el obrero o empleado lesionado, o sus beneficiarios, no llegasen a un acuerdo con respecto a la compensación por accidentes del trabajo.

La Comisión consta de cinco comisionados, los cuales son nombrados por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico. En la **Ley Núm. 45** se dispone que de los cinco, tres serán abogados, uno será médico de reputado conocimiento e interés en el campo de la medicina ocupacional y el otro será una persona de reconocida simpatía e identificación con el movimiento obrero organizado en Puerto Rico. El Gobernador, con el consejo y consentimiento del Senado, designará el Presidente, quien a su vez será uno de los comisionados, cuyo término vencerá el 31 de diciembre del año en que se celebren las elecciones generales. Los demás comisionados serán nombrados inicialmente por los siguientes términos: dos por dos años y dos por tres años. Todos los nombramientos subsiguientes serán por seis años.

El Presidente es el jefe administrativo y la autoridad nominadora de la Comisión. Éste le responde directamente al Gobernador. Como principal oficial ejecutivo, tiene la responsabilidad de adoptar todas las determinaciones de personal y es el responsable de hacer cumplir la política pública y los propósitos de esta **Ley**. También tiene la facultad para contratar y nombrar las personas y funcionarios para llevar a cabo las funciones de la Comisión, de acuerdo con las disposiciones de esta **Ley**. Podrá comprar, contratar o de otro modo proveer a la Comisión todos los materiales, suministros, equipo, piezas o servicios que estime convenientes para la operación de la Comisión.

La Comisión está compuesta por las oficinas del Presidente, de los Comisionados, del Director Ejecutivo, de Asesoramiento Legal, de Asesoramiento Médico, de Auditoría Interna, de Comunicaciones y Relaciones con la Comunidad, de Gerencia y Presupuesto y de Secretaría; las áreas de Administración y Finanzas, de Recursos Humanos y Asuntos Laborales y de Tecnología y Sistemas de Información. La Comisión tiene Sala de Vistas en San Juan, Arecibo, Humacao, Mayagüez y Ponce.

A la fecha de nuestra auditoría, el ATSI de la Comisión tenía en operación una red de área amplia (*WAN*, por sus siglas en inglés) compuesta por 11 servidores con un sistema

operativo **Windows 2000**, Versión Server y 268 microcomputadoras con sus respectivos equipos periferales conectadas a la misma. Dicha red permite el acceso del personal autorizado de la Oficina Central y sus oficinas regionales al sistema mecanizado. Además, proveía servicios de impresión, correo electrónico y acceso a Internet. El personal del ATSI está compuesto por un Administrador, un Gerente de Proyectos y Sistemas de Información, cinco Analistas de Tecnología y Sistemas de Información y cuatro Técnicos de Sistemas Operativos y Sistemas de Información.

El presupuesto de la Comisión para el año fiscal 2004-05 ascendió a $20,183,963 del cual se asignaron $1,044,966 para las operaciones del ATSI.

RESPONSABILIDAD DE LA GERENCIA

Con el propósito de lograr una administración eficaz, regida por principios de calidad, la gerencia de todo organismo gubernamental, entre otras cosas, es responsable de:

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 22 de noviembre de 2004 al 15 de agosto de 2005. 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 información financiera, de procedimientos de control interno y de otros procesos
- Confirmaciones de otra información pertinente

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones del ATSI en lo que concierne al desarrollo y control de los cambios de las aplicaciones, los controles de acceso, la administración del programa de seguridad, la segregación de deberes, los controles de los sistemas operativos y la evaluación de la continuidad del servicio no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 7** de este **Informe**, clasificados como principales. Las pruebas efectuadas, también, revelaron que las demás operaciones objeto de este **Informe** se realizaron sustancialmente de acuerdo con la ley y la reglamentación, excepto por la situación que se comenta en el **Hallazgo 8**.

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

INFORME DE AUDITORÍA ANTERIOR

Una situación similar a la comentada en el **Hallazgo 1** de este **Informe** fue objeto de recomendaciones en el **Informe de Auditoría CPED-93-15 del 30 de junio de 1993**.

El no atender sin justa causa, las recomendaciones de los informes de auditoría de la Oficina del Contralor puede constituir una violación al **Artículo 3.2(b) de la Ley Núm. 12 del 24 de julio de 1985**, **Ley de Ética Gubernamental**, según enmendada. A estos efectos, el 30 de enero de 1987 el Administrador Ejecutivo de la Oficina de Ética Gubernamental emitió la **Carta Circular Núm. 86-4**, mediante la cual exhortó a los funcionaros de la Rama Ejecutiva del Gobierno a cumplir con las mismas.

RECOMENDACIONES

A LA PRESIDENTA DE LA COMISIÓN INDUSTRIAL DE PUERTO RICO

1. Ver que la Directora Ejecutiva se asegure de que:

    a. El Administrador del ATSI:

        1) Efectúe los estudios de necesidad y viabilidad que son requeridos, previo a la preparación de la solicitud de propuestas para adquirir equipos e implantar los sistemas de información computadorizados en la Comisión. **[Hallazgo 1-a.1) y 2)]**

        2) Informe por escrito a la Encargada de Propiedad de cualquier equipo computadorizado que no esté en uso para que sea reasignado o que se disponga del mismo, según proceda. **[Hallazgo 1-a.1) y 2)]**

        3) Realice las gestiones pertinentes para la preparación de un **Plan de Continuidad de Negocios**, que incluya un **Plan de Contingencias** actualizado, según lo establecido en la **Carta Circular Núm. 77-05**. Además, mantener una copia de dichos planes en un lugar seguro fuera de los predios de la Comisión. **[Hallazgo del 3-a. al c.]**

        4) En coordinación con el Oficial de Seguridad, desarrolle las medidas de control necesarias para corregir las situaciones comentadas y las someta para su

consideración y aprobación. Implante dichas medidas tan pronto sean aprobadas, y vea que se cumpla con las mismas. **[Hallazgo 5]**

5) Revise y actualice el **Manual de Procedimientos para realizar Backup** y lo someta para su consideración y aprobación. **[Hallazgo 6-a.1)]**

6) Realice las gestiones pertinentes para proveer al ATSI de los medios necesarios para salvaguardar las cintas de los respaldos hasta el día de su recogido. **[Hallazgo 6-a.2)]**

7) Mantenga copia de la documentación relacionada con las instalaciones y configuraciones del sistema computadorizado y de los programas de aplicaciones utilizados en un lugar seguro fuera de los predios de la Comisión. **[Hallazgo 6-a.3)]**

8) Identifique y evalúe un programa especializado para efectuar respaldos que permita manejar de manera efectiva y eficiente el volumen de datos de los sistemas de información de la Comisión y someta para su consideración y aprobación el programa seleccionado. **[Hallazgo 6-a.4)]**

b. El Director de Administración y Finanzas vea que el Encargado de la Propiedad cumpla con los procedimientos establecidos para el control de la propiedad. **[Hallazgo 1-a.2)]**

c. El Oficial de Seguridad, dentro de un término razonable:

1) Revise y actualice el **Plan de Seguridad** y someta el mismo para su consideración y aprobación. **[Hallazgos 4, 5 y 7]**

2) Corrija las situaciones comentadas en el **Hallazgo 4**.

d. El Director de Recursos Humanos, dentro de un término razonable, complete la preparación y actualización de las hojas de descripción de deberes de los empleados del ATSI. **[Hallazgo 8]**

2. Asegurarse de que se realice el análisis de riesgos según se establece en la **Política Núm. TIG-003**. **[Hallazgo 2]**

3. Formalizar un acuerdo por escrito con un centro alterno que acepte la utilización de sus respectivos equipos en caso de desastres o emergencias en la Comisión, o considerar establecer su propio centro alterno en alguna de las salas regionales de la Comisión. **[Hallazgo 3-d.]**

CARTAS A LA GERENCIA

Las situaciones comentadas en los hallazgos de este **Informe** fueron sometidas a la Presidenta de la Comisión, Lic. Siomari Collazo Colón, en carta de nuestro auditor del 1 de septiembre de 2005.

El borrador de los hallazgos de este **Informe** se sometió para comentarios a la Presidenta y al ex Presidente de la Comisión, Lic. Gilberto M. Chárriez Rosario, en cartas del 10 de abril de 2006.

COMENTARIOS DE LA GERENCIA

En carta del 19 de septiembre de 2005 la Presidenta informó sobre las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en la carta de nuestro auditor.

La Presidenta contestó el borrador de los hallazgos de este **Informe** en carta del 24 de abril de 2006. Sus observaciones fueron consideradas en la redacción final del informe y se incluyen en la parte de este **Informe** titulada **RELACIÓN DATALLADA DE HALLAZGOS**, bajo la sección HALLAZGOS EN EL ÁREA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN DE LA COMISIÓN INDUSTRIAL DE PUERTO RICO.

El ex Presidente no contestó el borrador de los hallazgos de este **Informe** que le fuera sometido.

AGRADECIMIENTO

A los funcionarios y empleados de la Comisión 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 EL ÁREA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN DE LA COMISIÓN INDUSTRIAL 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 ÁREA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN DE LA COMISIÓN INDUSTRIAL DE PUERTO RICO

Los **hallazgos del 1 al 7** se clasifican como principales y el **Hallazgo 8** como secundario.

Hallazgo 1 - Adquisición de equipos de computadoras que a julio de 2005 no eran utilizados

a. Entre mayo de 1998 y septiembre de 1999 la Comisión adquirió los siguientes equipos computadorizados por $18,345 que a la fecha de nuestro examen no se utilizaban:

   1) El 20 de mayo de 1998 la Comisión recibió una impresora de impacto marca Genicom, modelo 4490 XT adquirida mediante la **Subasta Núm. 77-134** por $16,670. Al 21 de julio de 2005 dicha impresora se mantenía ubicada en una esquina del Salón de Operaciones[1] del ATSI y no se había utilizado.

   2) Entre el 4 de abril y el 27 de septiembre de 1999 la Comisión recibió cinco módems externos marca US-Robotics Courier adquiridos mediante la **Obligación y Orden de Compra Núm. 9930440091** por $1,675. Al 6 de junio de 2005 cuatro de éstos se mantenían almacenados encima de un archivo en el Salón de Operaciones y nunca se habían utilizado; permanecían en sus empaques originales. El otro módem se había utilizado, pero se desconocía la localización del mismo. Ninguno de los módems tenía asignado el número de propiedad.

[1] Lugar donde estaban localizadas las computadoras principales de los sistemas de información de la Comisión.

En el **Artículo 10(a) de la Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico**, según enmendada, se establece que la custodia, el cuidado y el control físico de la propiedad pública será responsabilidad del jefe de la propia dependencia o entidad corporativa o su representante autorizado.

En el **Reglamento Núm. 11, Normas Básicas para el Control y Contabilidad de los Activos Fijos**, aprobado el 8 de abril de 2002 por el Secretario de Hacienda, se establecen los procedimientos para controlar la propiedad. En el mismo se dispone que los jefes de las agencias serán responsables de la custodia, el cuidado, la protección, la conservación y el uso adecuado de toda la propiedad sujeta a su jurisdicción. Se establece, además, que el Encargado de la Propiedad:

- numerará todo activo fijo para propósitos de identificación y control[2]
- mantendrá al día los expedientes de la propiedad y
- mantendrá recibos firmados por todas las personas que usen o tengan bajo custodia directa propiedad pública

Es responsabilidad de la gerencia de toda entidad gubernamental maximizar la inversión de los fondos públicos mediante la utilización de la propiedad pública. Además, es responsable de garantizar la inversión adecuada de los fondos y la utilización efectiva de los recursos disponibles.

Las situaciones que se comentan ocasionaron que se adquirieran equipos por $18,345 de los cuales no se había obtenido ningún rendimiento o beneficio. Además, la situación del **Apartado a.2)** puede propiciar el uso indebido y la pérdida de la propiedad, y otras situaciones adversas, sin que se puedan detectar a tiempo para fijar responsabilidades.

[2] Se considera activo fijo todos los bienes muebles e inmuebles adquiridos o que puedan adquirir las agencias, cuyo costo por unidad es de $100 o más con una vida útil de dos años o más, ya sea mediante compra, traspaso, cesión, donación o por otros medios.

Las situaciones comentadas se atribuyen a que el entonces Administrador del ATSI no preparó un estudio de necesidades previo a la adquisición de los equipos. La situación que se comenta en el **Apartado a.2)** se atribuye a que la Encargada de la Propiedad no cumplió con las disposiciones reglamentarias relacionadas con el control de la propiedad.

La Presidenta, en la carta que nos envió informó, entre otras cosas las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación 1.a.1) y 2) y b.

Hallazgo 2 - Falta de un Informe de Avalúo de Riesgos

a. A la fecha de nuestro examen, 12 de mayo de 2005, la Comisión no había realizado un avalúo de riesgos sobre sus sistemas de información. Esto es necesario para evaluar las medidas de control viables que permitan minimizar las posibles amenazas en los casos de que los sistemas de información dejen de funcionar correctamente y de que la información pudiese ser accedida de forma no autorizada o maliciosa.

   En la **Política Núm. TIG-003 - Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, 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, se establece que cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada y/o maliciosa. Para ello deberá realizar 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 al nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo a su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.

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

Las mejores prácticas en el campo de la tecnología de información sugieren que 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 agencia debe desarrollar e implantar un programa de avalúo o 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 eventos ocurran y el impacto que tendrían sobre las operaciones.

La situación comentada impide a la Comisión evaluar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de la agencia. 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. Dicho **Plan** también debe contener los pasos a seguir para restablecer las operaciones de la agencia en caso de que surja alguna eventualidad. **[Véase el Hallazgo 3]**

La situación comentada se atribuye a que la Presidenta de la Comisión no había requerido el que se efectuara el análisis de riesgo dispuesto en la **Carta Circular Núm. 77-05**.

La Presidenta, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación 2.

Hallazgo 3 - Ausencia de un Plan para la Continuidad de los Negocios y deficiencias en el Plan de Contingencias para los sistemas de información de la Comisión

a. La Comisión carecía de un **Plan para la Continuidad de Negocios** para los sistemas de información con las medidas preventivas específicas para continuar con sus operaciones en caso de riesgos como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros.

   En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que las agencias deberán desarrollar un **Plan de Continuidad de Negocios** que incluya un **Plan para la Recuperación de Desastres** y un **Plan para la Continuidad de las Operaciones**.

b. El **Plan de Contingencias (Plan)** del ATSI que nos fuera provisto para examen el 7 de febrero de 2005, no había sido aprobado por la Presidenta. Tampoco había sido actualizado conforme a los cambios de equipos, sistemas de información y personal. Además, no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:

   - Estrategias a utilizarse para efectuar y documentar pruebas o simulacros que certifique la efectividad del **Plan**.

   - Nombre del encargado de activar el **Plan**.

   - Nombres de las personas que integran los grupos de recuperación, sus direcciones, los números de teléfono donde puedan ser localizados y la responsabilidad asignada a cada uno de ellos.

   - Lista detallada con todos los medios de comunicación de los diferentes miembros de cada grupo de recuperación, incluidos los empleados del área de sistemas de información.

   - Plan general de acción identificado por grupo y tareas de forma secuencial.

   - Inventario de equipos, sistemas operativos, de aplicaciones, y archivos críticos del ATSI.

- Identificación detallada de la configuración crítica y del contenido de los respaldos y el nombre de los archivos.

- Detalle de la configuración de los sistemas utilizados en el ATSI y requeridos para el centro de sistemas de información alterno (centro alterno).

- Itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos.

- Identificación de los proveedores primarios que incluya el número de teléfono y el nombre del personal de enlace con la Comisión.

- Acuerdos por escrito para el uso de instalaciones de un centro alterno.

- Detalles del equipo de comunicaciones utilizado en el Centro Primario y el requerido para el centro alterno para propósitos de restauración.

- Procedimientos para efectuar pruebas en el centro alterno.

- Hoja de cotejo para daños.

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**. Éste es una guía para garantizar la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afecten su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la agencia.

Las mejores prácticas utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados sugieren que las entidades deben mantener un plan de contingencias actualizado y listo para implantarse cuando sea necesario.

Las situaciones que se comentan en los **apartados a. y b.** podrían propiciar la improvisación, y que en casos de emergencia se tomen medidas inapropiadas y en forma desordenada, con los consiguientes efectos adversos. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios a los usuarios de la Comisión.

c. No se mantenía copia del **Plan** en un lugar seguro fuera de las instalaciones de la Comisión.

Como norma de sana administración y control se requiere que las entidades gubernamentales mantengan copia actualizada del **Plan de Continuidad de Negocios**, que incluye el **Plan de Contingencias**, en un lugar seguro fuera del edificio donde radica el Salón de Operaciones. Ello es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado.

De ocurrir una emergencia que impida el acceso a la Comisión, el encargado de activar el **Plan** no tendría acceso a éste 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.

d. La Comisión no había formalizado acuerdos con otros centros de sistemas de información para restaurar sus operaciones computadorizadas en casos de emergencia.

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

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

La falta de acuerdos por escrito con un centro alterno podría afectar las funciones de la Comisión y los servicios del ATSI, ya que no tendrían disponibles unas instalaciones para continuar operando después de una emergencia o evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales del ATSI.

Las situaciones comentadas se atribuyen a que la Presidenta no había requerido que se efectuara un **Avalúo de Riesgo (Véase el Hallazgo 2)** que sirviera de base para el desarrollo, aprobación e implantación de un **Plan de Continuidad de Negocios** que incluya un **Plan para la Continuidad de las Operaciones** y un **Plan de Contingencias**, a fin de que sirvan como herramientas para responder ante cualquier incidente o desastre que ocurra.

La Presidenta, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

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

Hallazgo 4 - Deficiencias en los controles de prevención y detección de acceso físico a las diferentes áreas de la Comisión

a. La Comisión contaba con un sistema de cámaras de seguridad ubicadas cerca de las puertas de entrada y salida, y del área de estacionamiento. Además, se habían instalado cámaras de seguridad en los tres pisos donde estaban ubicadas las diferentes áreas de trabajo de la Comisión. A la fecha de nuestro examen, abril de 2005, se determinó que existían las siguientes faltas de controles:

   1) No se habían promulgado normas ni procedimientos escritos para la administración del sistema de cámaras de seguridad que incluya, entre otros, la conservación de los vídeos que se producían mediante dicho sistema.

   2) El sistema de cámaras de seguridad que se había instalado en la Comisión no funcionaba.

   3) Los monitores del sistema de cámaras de seguridad no estaban localizados en un área separada para asegurar que sólo personal autorizado tuviese acceso a los mismos. Dichos

monitores estaban ubicados en un área abierta dentro del Área de Administración y Finanzas.

4) No se había asignado a una persona la responsabilidad de la administración del sistema de las cámaras de seguridad.

5) Los guardias de la compañía de seguridad no tenían acceso a los monitores del sistema de cámaras de seguridad para prestar vigilancia a las diferentes áreas de la Comisión.

6) Las puertas que daban acceso al edificio no estaban conectadas a un sistema de alarmas.

En el **Artículo 2(e) de la Ley Núm. 230** se dispone, que cada dependencia o entidad corporativa deberá mantener el control previo de todas sus operaciones para que sirva de arma efectiva al jefe de la dependencia o entidad corporativa en el desarrollo del programa o programas cuya dirección se le ha encomendado. Conforme con dicha disposición, y como norma de sana administración, se debe implantar un programa formal de seguridad en la agencia para proteger la propiedad y los fondos públicos.

Las situaciones comentadas privan a la Comisión de poder prevenir y detectar la pérdida de la propiedad y los fondos públicos, y dificultan fijar responsabilidades. Además, puede permitir que la Comisión sea vulnerable al hurto de equipo computadorizado como sucedió en agosto de 2004 cuando desconocidos hurtaron 55 microcomputadoras adquiridas por $79,870[3].

Las situaciones comentadas se atribuyen a que no se había implantado un **Plan de Seguridad** en la Comisión para salvaguardar la propiedad y los fondos públicos de la agencia contra eventos o acciones, por error o intención, como fraude, pérdida o hurto.

[3] La Comisión notificó los hechos a la Policía de Puerto Rico, mediante la **Querella Núm. 2004-1-282-13411** del 15 de agosto de 2004. También notificó al Secretario de Justicia y al Contralor de Puerto Rico, según dispuesto por ley.

La Presidenta, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación 1.c.

Hallazgo 5 - Fallas en los controles de acceso físico y ambientales del ATSI y del Salón de Operaciones

a. El examen de los controles de acceso físico al ATSI y al Salón de Operaciones (Salón)[4] reveló las siguientes faltas:

1) No existía una lista de las personas a las que el Administrador Interino de Tecnología de Sistemas de Información había provisto acceso al ATSI y al Salón.

2) No siempre estaba presente el personal de operaciones en el Salón cuando el personal de mantenimiento realizaba las labores de limpieza o cuando los consultores externos daban apoyo al sistema computadorizado.

3) No se cambiaba la contraseña numérica de la cerradura con combinación de la puerta de acceso al ATSI.

4) La puerta de acceso al Salón carecía de una cerradura para controlar el acceso al personal no autorizado.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que el acceso a las facilidades de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas.

b. La inspección de los controles ambientales del ATSI y del Salón reveló las siguientes faltas:

1) No se había instalado una fuente de energía alterna que asegurara la continuidad de las operaciones en caso de fallas prolongadas en el servicio de energía eléctrica.

[4] Véase la nota al calce 1 en la página 12.

2) El Salón no contaba con un sistema automático de supresión de incendios.

3) No se habían instalado detectores de humo por encima y por debajo del techo acústico y por debajo del piso falso del Salón.

4) No se había instalado un interruptor de energía eléctrica de emergencia fuera del Salón.

5) Las paredes y el techo acústico ubicados alrededor del Salón no eran de materiales resistentes al fuego.

6) La construcción de las paredes del Salón no era desde el piso hasta el techo, por lo que quedaba un espacio que permitía el acceso al lugar.

7) No se realizaba una limpieza adecuada a las áreas debajo del falso piso del Salón. Se encontraron pedazos de madera y otros materiales inflamables en dichas áreas.

8) Los cables eléctricos se encontraron fuera de los conductos sobre el techo acústico del Salón y área administrativa del ATSI.

9) Uno de los extintores manuales de incendios del área administrativa del ATSI estaba parcialmente bloqueado por dos archivos, lo que impedía que fuera fácilmente visible y accesible para el personal de dicha área.

10) El área administrativa del ATSI sólo contaba con un detector de humo, cuya alarma no era audible fuera de las instalaciones de dichas áreas.

11) Los empleados del ATSI no habían participado en adiestramientos sobre las medidas a tomar en caso de una emergencia.

En la **Política Núm. 3 de la Carta Circular Núm. 77-05** se establece que cada agencia será responsable de desarrollar políticas específicas de seguridad tomando en cuenta las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas críticos. Ello implica que, como norma de sana administración, las agencias deberán tomar los cuidados necesarios para proteger y mantener funcionando en óptimas

condiciones los equipos electrónicos para evitar daños y averías. El propósito es asegurar la integridad, exactitud y disponibilidad de la información y protegerla contra la destrucción accidental, entre otras cosas. Para garantizar razonablemente la seguridad de los equipos y sistemas computadorizados, es necesario tener un salón de computadoras que reúna las condiciones de seguridad y los equipos de detección y protección adecuados. También, se deben ofrecer conferencias periódicas sobre las medidas a tomar en caso de una emergencia. Ambas prácticas tienen el objetivo de proteger tanto al personal como al equipo y otras propiedades.

Las situaciones comentadas pueden poner en riesgo la seguridad de los empleados y los recursos sensitivos de los sistemas computadorizados. Además podría impedir la disponibilidad de los sistemas y, por ende, limitar los servicios que presta la Comisión.

Las situaciones comentadas se atribuyen a la ausencia de revisión, aprobación e implantación del **Plan de Seguridad** y al incumplimiento de las normas citadas.

La Presidenta, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación 1.a.4) y c.1).

Hallazgo 6 - Deficiencias en la preparación y el manejo de los respaldos de los archivos computadorizados de información

a. La Comisión mantenía un acuerdo contractual con una institución privada con el propósito de mantener los respaldos diarios y mensuales de información de los sistemas computadorizados en un lugar fuera de los predios de ésta. Como parte de dicho acuerdo se había establecido que la institución privada recogería las cintas de los respaldos diarios de información los lunes y jueves de cada semana y recogería el respaldo mensual de fin de mes. El examen realizado en mayo de 2005 sobre los respaldos de información reveló las siguientes deficiencias:

1) El Manual de **Procedimientos para Realizar Backup** para la realización de los respaldos diarios de información no habían sido revisados ni aprobados por los funcionarios autorizados.

2) Las cintas de los respaldos diarios que se mantenían en el Salón hasta el día de su recogido (lunes y jueves) no se mantenían en un lugar seguro. Éstas se guardaban en una caja plástica para almacenar cintas que se mantenía sobre una mesa del Salón.

3) No se mantenía copia de la documentación sobre las instalaciones, las configuraciones, los programas de aplicaciones y las actualizaciones realizadas a los sistemas de información en un lugar seguro fuera de los predios del edificio donde está ubicada la Comisión.

4) El programa **Microsoft Windows Backup, Versión 5** que se utilizaba para realizar el respaldo de la información almacenada en los servidores **CIPR1SRV, CIPR2SRV, CIPRSRV3200, CIPR2000MSG y CIPR01ISA** no permitía que se respaldaran los archivos que eran accedidos por los usuarios al momento en que se realizaban dichos respaldos. Además, el respaldo diario de la información de la Aplicación **Workflow** que estaba almacenada en el servidor **CIPR1SRV** demoraba dos días en completarse.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que deberán existir procedimientos para tener y mantener una copia de respaldo (*backup*) recurrente de la información y de los programas de aplicación y de sistema esenciales e importantes para las operaciones de la agencia.

Las situaciones comentadas podrían ocasionar la pérdida permanente de información importante sin la posibilidad de poder restaurarla en casos de contingencias o emergencias, lo que afectaría adversamente las operaciones de la Comisión.

La situación comentada en el **Apartado a.1)** se atribuye a que el Administrador del ATSI no había revisado y actualizado el Manual de **Procedimientos para Realizar Backup**.

La situación comentada en el **Apartado a.2)** se atribuye a que el ATSI no contaba con los medios para salvaguardar las cintas que permanecen en el área hasta que son llevadas fuera de los predios de la Comisión.

La situación comentada en el **Apartado a.3)** se atribuye a que el Administrador de la ATSI no se había percatado de la importancia de mantener copia de la documentación relacionada con las instalaciones, las configuraciones del sistema computadorizado y los programas de aplicaciones utilizados en un lugar seguro fuera de los predios de la Comisión.

La situación comentada en le **Apartado a.4)** se debía a que el programa utilizado para la creación de los respaldos no está diseñado para el volumen de data manejada en dicha área.

La Presidenta, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación de la 1.a.5) a la 8).

Hallazgo 7 - Deficiencias relacionadas con el Plan de Seguridad

a. El **Plan de Seguridad (Plan)** de la Comisión que nos fuera provisto para examen el 7 de febrero de 2005 carecía de la firma de la Presidenta y de la fecha de su preparación.

   En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que será responsabilidad de cada agencia el desarrollar políticas específicas de seguridad tomando en cuenta las características propias de los ambientes de tecnología.

   La falta de un **Plan** completo y aprobado podría dar lugar a no poder cumplir con el propósito del mismo; evitando así proteger los recursos sensitivos de los sistemas computadorizados y limitando la disponibilidad y el apoyo a todas las operaciones de la agencia.

   La situación comentada se atribuye a que la Presidenta no había promulgado una directriz sobre la implantación y continua actualización del **Plan**.

La Presidenta, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación 1.c.1).

Hallazgo 8 - Falta de preparación y distribución de las hojas de descripción de deberes de los empleados del ATSI conforme el nuevo Plan de Clasificación y Retribución de la Comisión

a. Al 22 de abril de 2005 no se había preparado y entregado una hoja de descripción de deberes del puesto a los 11 empleados del ATSI de la Comisión, conforme a los cambios en las funciones del mismo, como consecuencia de la implantación del nuevo **Plan de Clasificación de Puestos y Estructura Retributiva** aprobado el 1 de julio de 2004 por el Presidente de la Comisión.

   En la **Sección 10.2 del Reglamento de Recursos Humanos de la Comisión Industrial de Puerto Rico** aprobado el 13 de noviembre de 2004 por el Director Ejecutivo se establece que conforme al plan organizativo funcional de la Comisión se preparará y mantendrá al día, para cada puesto autorizado, una hoja de deberes del puesto con una descripción clara y precisa de los deberes y las responsabilidades esenciales y, si es necesario, las funciones marginales según surjan de los puestos, así como del grado de autoridad y de supervisión inherentes al mismo y las condiciones de trabajo presentes en cada puesto. También se establece que copia del cuestionario se entregará al empleado al ser nombrado y tomar posesión del puesto y cuando ocurran cambios en las funciones del mismo que resultasen en la formalización de un nuevo cuestionario.

   La situación que se comenta puede ocasionar, entre otras cosas, que los empleados desconozcan los límites y el alcance de las tareas inherentes a sus puestos, y que se dificulte la evaluación del desempeño de los mismos. Además, puede tener consecuencias adversas en caso de que algún empleado se querelle sobre las funciones que desempeña.

   La situación que se comenta se debía a que la Oficina de Recursos Humanos se encontraba en el proceso de actualización de las hojas de descripción de deberes para todos los

empleados de la Comisión conforme al nuevo **Plan de Clasificación de Puestos y Estructura Retributiva**.

La Presidenta, en la carta que nos envió, informó, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas.

Véase la Recomendación 1.d.

ANEJO 1

COMISIÓN INDUSTRIAL DE PUERTO RICO

ÁREA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN

COMISIONADOS QUE ACTUARON DURANTE EL PERIODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Lic. Siomari Collazo Colón	Presidenta	11 ene. 05	15 ago. 05
Lic. Gilberto M. Chárriez Rosario	Presidente	22 nov. 04	10 ene. 05
Lic. Carlos Rodríguez García	Comisionado	11 ene. 05	15 ago. 05
Lic. Julio Santiago Pomales	"	15 dic. 04	15 ago. 05
Lic. Siomari Collazo Colón	Comisionada	22 nov. 04	10 ene. 05
Dr. Fernando J. Cabrera de la Rosa	Comisionado	22 nov. 04	15 ago. 05
Lic. Carmen J. Fernández Padilla	Comisionada	22 nov. 04	15 ago. 05

ANEJO 2

COMISIÓN INDUSTRIAL DE PUERTO RICO

ÁREA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DEL NIVEL EJECUTIVO QUE ACTUARON DURANTE EL PERIODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Lic. Siomari Collazo Colón	Presidenta	11 ene. 05	15 ago. 05
Lic. Gilberto M. Chárriez Rosario	Presidente	22 nov. 04	10 ene. 05
Sra. Laura I. Santa Sánchez	Directora Ejecutiva	10 feb. 05	15 ago. 05
Sr. Guillermo A. Rivera Bermúdez	Director Ejecutivo Interino	22 nov. 04	9 feb. 05
Lic. María M. Crespo González	Ayudante Especial	22 feb. 05	15 ago. 05
Sr. José L. Guadalupe Camacho	"	25 ene. 05	15 ago. 05
Sr. Héctor L. González Cruz	"	22 nov. 04	15 ago. 05
Sr. Rey F. Rivera Rivera	"	22 nov. 04	15 ago. 05
Lic. Adymara Rodríguez Rodríguez	Directora de Asesoramiento Legal	22 feb. 05	15 ago. 05
Lic. María M. Crespo González	"	22 nov. 04	21 feb. 05
Sra. Lynette Ortiz Martínez	Secretaria Ejecutiva[5]	26 ene. 05	15 ago. 05
Sra. María de los A. Rosa Rosa	Directora de Recursos Humanos Interina	22 nov. 04	15 ago. 05
Sr. Gamalier Rodríguez Casillas	Director de Administración y Finanzas Interino	22 nov. 04	15 ago. 05
Sr. Jorge L. Sanabria Merced	Administrador de Tecnología y Sistemas de Información Interino	22 nov. 04	15 ago. 05
Sr. Rafael A. Maldonado Muñoz	Director de Auditoría Interna[6]	15 feb. 05	15 ago. 05

[5] Del 17 de noviembre de 2004 al 25 de enero de 2005 el cargo de Secretario Ejecutivo estuvo vacante.

[6] Del 22 de noviembre de 2004 al 14 de febrero de 2005 el cargo de Director de Auditoría Interna estuvo vacante.