INFORME DE AUDITORÍA TI-10-05

24 de agosto de 2009

ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES

DEPARTAMENTO DE INFORMÁTICA

(Unidad 5010 - Auditoría 13015)

Período auditado: 1 de junio al 27 de noviembre de 2007

CONTENIDO

Página

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

24 de agosto de 2009

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

Realizamos una auditoría de las operaciones del Departamento de Informática (DI) de la Administración de Compensaciones por Accidentes de Automóviles (ACAA) 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 Num. 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 los controles internos relacionados con las normas y los procedimientos operacionales del DI, el avalúo de riesgos y el plan de seguridad, y el acceso y la seguridad de los sistemas operativos.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La ACAA fue creada por virtud de la **Ley Núm. 138 del 26 de junio de 1968, Ley de Protección Social por Accidentes de Automóviles**, según enmendada. Ésta se creó como una corporación pública con el propósito de reducir al mínimo los efectos económicos y sociales producidos por los accidentes de tránsito sobre la familia y sus dependientes. Los poderes de la ACAA son ejercidos por una Junta de Directores compuesta por un miembro del Gabinete del Gobernador y cuatro personas nombradas por el Gobernador con el consentimiento del Senado.

Dicha Junta nombra al Director Ejecutivo de la ACAA. Los servicios a los lesionados se prestan en la Oficina Central y en 10 oficinas regionales ubicadas en Aguadilla, Arecibo, Bayamón, Caguas, Carolina, Guayama, Humacao, Mayagüez, Ponce y San Juan.

Los **ANEJOS 1 y 2** contienen la relación de los miembros de la Junta de Directores y de los funcionarios principales de la ACAA, respectivamente, que actuaron durante el período auditado.

Los recursos para financiar las actividades operacionales de la ACAA provienen, principalmente, de las primas del seguro que anualmente pagan los dueños de vehículos de motor y de los ingresos que genera mediante su cartera de inversiones. El presupuesto de la ACAA para el año fiscal 2006-07 ascendió a $105,561,000, de los cuales $4,206,211 fueron asignados para las operaciones del DI.

A la fecha de nuestra auditoría el DI tenía en operación una red de comunicaciones (Red) de área amplia (*WAN*, por sus siglas en inglés). Dicha Red permitía el acceso del personal autorizado de la Oficina Central y sus oficinas regionales a los sistemas de información computadorizados. El DI contaba con un Director, un Subdirector, un Gerente de Proyectos, un Administrador de Base de Datos, un Supervisor de Programación, dos programadores, un Supervisor de los administradores de Redes, dos administradores de Redes, un Técnico de Redes, un Bibliotecario y dos operadores de Computador.

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

RESPONSABILIDAD DE LA GERENCIA

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

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

2. Mantener una oficina de auditoría interna competente.

3. Cumplir con los requisitos impuestos por las agencias reguladoras.

4. Adoptar un plan estratégico para las operaciones.

5. Mantener el control presupuestario.

6. Mantenerse al día con los avances tecnológicos.

7. Mantener sistemas adecuados de archivo y de control de documentos.

8. Cumplir con el **Plan de Acción Correctiva** de la Oficina del Contralor de Puerto Rico, y atender las recomendaciones de los auditores externos.

9. Mantener un sistema adecuado de administración de personal que incluya la evaluación del desempeño, y un programa de educación continua para todo el personal.

10. Cumplir con la **Ley de Ética Gubernamental**, lo cual incluye divulgar sus disposiciones a todo el personal.

El 27 de junio de 2008, mediante la **Carta Circular OC-08-32**, divulgamos la revisión de los mencionados diez principios establecidos en nuestra **Carta Circular OC-98-09 del 14 de abril de 1998**. Ambas **cartas circulares** se pueden acceder a través de nuestra página de Internet: http://www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de junio al 27 de noviembre de 2007. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los

sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias.

Para efectuar la auditoría utilizamos la siguiente metodología:

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

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones del DI en lo que concierne a los controles internos relacionados con las normas y los procedimientos operacionales del DI, el avalúo de riesgo y el plan de seguridad, y el acceso y la seguridad de los sistemas operativos no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 9** de este **Informe**, clasificados como principales.

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

RECOMENDACIONES

A LA JUNTA DE DIRECTORES DE LA ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES

1. Tomar las medidas necesarias para asegurarse de que el Director Ejecutivo de la ACAA cumpla con las **recomendaciones de la 2 a la 4** de este **Informe**. **[Hallazgos del 1 al 9]**

AL DIRECTOR EJECUTIVO DE LA ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES

2. Asegurarse de que se realice y se documente el análisis de riesgos, según se establece 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, y se incluya en el avalúo de riesgos los elementos mencionados en el **Hallazgo 1**. El informe, producto de este avalúo de riesgos, debe ser sometido para su revisión y aprobación.

3. Ejercer una supervisión efectiva sobre el Director del DI para asegurarse de que:

   a. Prepare y someta, para su consideración y aprobación, un plan de seguridad en el que se establezcan los proyectos, las tareas y las actividades requeridos para proteger al personal y a los activos de sistemas de información. Una vez aprobado, asegurarse de que se divulgue a los funcionarios y a los empleados concernidos, y se realicen pruebas periódicas del mismo. **[Hallazgo 2]**

   b. Los accesos con privilegios de administrador de los sistemas operativos otorgados a los administradores de Redes estén debidamente justificados, autorizados y documentados. **[Hallazgo 3]**

   c. Los administradores de Redes revisen, periódicamente, los eventos registrados en los servidores de la Red, documenten su revisión y, de ser necesario, tomen de inmediato las medidas preventivas y correctivas necesarias. **[Hallazgo 4-a.]**

   d. Diseñe y mantenga un registro de las actualizaciones realizadas al sistema operativo con el propósito de mantener un control de éstas y asegurar un funcionamiento más efectivo y eficaz de los sistemas de información. **[Hallazgo 4-b.]**

   e. Redacte y someta, para su consideración y aprobación, las normas y los procedimientos escritos necesarios para regir las operaciones del DI que se comentan en el **Hallazgo 5**.

f. Establezca, en coordinación con el Director de Recursos Humanos, un plan para ofrecer adiestramientos sobre el uso y la seguridad de los sistemas de información computadorizados al personal de la ACAA que utiliza los mismos, de manera que se cumpla con lo establecido en las **secciones de la 12.4 a la 12.6 del Reglamento de Personal para los Empleados Gerenciales de la ACAA**, aprobado el 19 de julio de 2005 por la Junta de Directores. **[Hallazgo 6]**

g. Diseñe un registro detallado para mantener el control de los programas adquiridos por la ACAA e instalados en las computadoras. Esto, con el fin de mantener un inventario de los mismos y evitar la posible instalación de programas no autorizados, y la pérdida y el uso indebido de programas adquiridos. **[Hallazgo 7]**

h. Tome las medidas necesarias para que se mantenga una segregación adecuada de las funciones conflictivas que realizan el Supervisor de los administradores de Redes y un Administrador de Redes. **[Hallazgo 8]**

4. Tomar las medidas que correspondan para que el DI le responda a la alta gerencia de la ACAA como una unidad independiente de sus usuarios. **[Hallazgo 9]**

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este **Informe** se sometió para comentarios al Sr. Julio Alicea Vasallo, Director Ejecutivo, en carta del 12 de junio de 2009. Con el mismo propósito, sometimos el borrador de los **hallazgos** de este **Informe** al Lic. Hiram A. Meléndez Rivera, ex Director Ejecutivo, en carta de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por la ACAA.

El 1 de julio de 2009 se envió una carta de seguimiento al ex Director Ejecutivo de la ACAA y se le concedió hasta el 9 de julio de 2009 para someter los comentarios al borrador de los **hallazgos** de este **Informe**.

El 7 de julio de 2009 el ex Director Ejecutivo de la ACCA envió un mensaje por correo electrónico para informar que no había recibido el borrador de los **hallazgos** de este **Informe** al

cual se hacía referencia en la carta del 1 de julio de 2009 y suministró una dirección postal para que le enviáramos el mismo. Para esa misma fecha, se le envió una carta con el borrador de los **hallazgos** de este **Informe** y se le concedió hasta el 22 de julio de 2009 para someter los comentarios al mismo.

COMENTARIOS DE LA GERENCIA

El Director Ejecutivo de la ACAA contestó el borrador de los **hallazgos** de este **Informe** mediante carta del 26 de junio de 2009, recibida en nuestra Oficina el 30 de junio de 2009. En dicha carta incluyó las medidas correctivas que se proponía implantar para corregir las situaciones comentadas.

El 23 de julio de 2009 el ex Director Ejecutivo de la ACAA envió un mensaje por correo electrónico para informar, entre otras cosas, que los hallazgos son correctos y que se espera que los mismos puedan ser corregidos en el futuro, si no los han corregido al presente.

AGRADECIMIENTO

A los funcionarios y a los empleados de la ACAA, 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, 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 DEPARTAMENTO DE INFORMÁTICA DE LA ADMINISTRACIÓN DE COMPESACIONES POR ACCIDENTES DE AUTOMÓVILES, 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 DEPARTAMENTO DE INFORMÁTICA DE LA ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES

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

Hallazgo 1 - Deficiencias en el Avalúo de Riesgos

a. El examen de la **Evaluación de Riesgos 2007**, aprobada el 27 de diciembre de 2006 por el Director Ejecutivo, reveló las siguientes deficiencias:

- No incluía una lista del inventario de los activos de sistemas de información. La misma debe contener la descripción de los equipos, los programas y los datos; su valoración y la clasificación de acuerdo con la misión y los servicios de la ACAA.
- No identificaba las posibles amenazas y vulnerabilidades lógicas y físicas que podrían afectar los activos de sistemas de información de la ACAA ni la probabilidad de que ocurran esas amenazas.
- No se realizó un análisis del impacto sobre las operaciones de la ACAA en caso de que se materialice alguna amenaza.
- No incluía información sobre las medidas de control establecidas para proteger cada uno de los activos de sistemas de información y determinar si los controles existentes para mitigar el riesgo eran eficaces.
- No incluía las conclusiones de la gerencia en respuesta a su evaluación del riesgo (aceptación, transferencia, reducción o asumir el riesgo).

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece 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 esto, deberá llevar a cabo un análisis de riesgos que incluya:

- Un inventario de activos de sistemas de información incluidos 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, entre otras) junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

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, la confidencialidad y la disponibilidad de los sistemas críticos, de modo que se garantice la continuidad de las operaciones en la eventualidad de que sucesos inesperados ocurran. Esto implica, entre otras cosas, que la ACAA desarrolle e implante un programa de avalúo y administración de riesgos para identificar los activos y recursos que se deben proteger, y clasificar los mismos como críticos y sensitivos, entre otros. 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 en las operaciones.

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

La situación comentada se atribuye a que el Director Ejecutivo de la ACAA no había requerido que se documentara el análisis de riesgos **(Evaluación de Riesgos 2007)**, según lo establecido en la **Carta Circular Núm. 77-05**.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Falta de un Plan de Seguridad

a. Al 29 de mayo de 2007 la ACAA no tenía un **Plan de Seguridad** aprobado por el Director Ejecutivo que incluyera, entre otras cosas, disposiciones en cuanto a:

- La documentación de la validación de las normas de seguridad[1]
- La evidencia de un análisis de riesgos actualizado, que sea la base del **Plan**
- La responsabilidad de la gerencia y de los demás componentes de la unidad
- Un programa de adiestramiento especializado al equipo clave de seguridad
- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, contratistas y usuarios, el cual permita mantener los conocimientos actualizados
- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipo y personal, entre otros)
- La documentación de la interconexión de los sistemas.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de

[1] La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el **Avalúo de Riesgos**. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del **Plan de Seguridad**.

éstas, particularmente sus sistemas de misión crítica. También se establece que las entidades gubernamentales son responsables de:

- Proveer adiestramientos a toda la gerencia y a los supervisores de la entidad gubernamental para que estén al tanto de los controles de seguridad y los beneficios correspondientes.

- Proveer adiestramientos al personal de sistemas de información y telecomunicaciones para que se le transmitan conocimientos actualizados sobre los aspectos de seguridad de sus áreas.

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

De ocurrir una emergencia, la falta de un **Plan** y de los correspondientes adiestramientos y simulacros podría dar lugar a:

- Pérdidas irreparables de vidas humanas
- Daños materiales a los equipos de sistemas de información, así como la pérdida de datos de suma importancia
- Atrasos en el proceso de reconstrucción de datos y programas, y en el restablecimiento y la continuidad de las operaciones normales y otras situaciones adversas.

La situación comentada se atribuye a que los funcionarios de la ACAA no se percataron de la importancia de la información que se recopila en ésta ni de los riesgos que podrían afectar la integridad, la disponibilidad y el uso efectivo de la información. Además, a que el Director Ejecutivo no había promulgado una directriz para la implantación y la actualización continua del **Plan de Seguridad**, según lo establecido en la **Carta Circular Núm. 77-05**.

Véanse las recomendaciones 1 y 3.a.

Hallazgo 3 - Falta de documentación de la justificación y de la autorización de los accesos a las cuentas de administrador de los sistemas operativos

a. Al 25 de junio de 2007 el personal del DI no pudo proveer a nuestros auditores la documentación de la justificación y de la autorización de los accesos otorgados a los administradores de Redes que tenían una cuenta con privilegios de administrador de los sistemas operativos.

   En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que la información y los programas de aplicación utilizados en las operaciones de la entidad gubernamental deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos necesarios, o usar las aplicaciones (o la parte de las aplicaciones) que necesita. Estos controles deberán incluir mecanismos de autenticación y autorización.

   La situación comentada impide mantener la evidencia requerida para determinar si las cuentas de acceso con los privilegios de administrador de los sistemas operativos están debidamente autorizadas y si éstas son asignadas conforme a las funciones y los deberes de los administradores de Redes.

   Esta situación se debió a que al Director del DI no se le requería mantener la documentación de la justificación ni de la autorización para otorgar a los administradores de Redes los accesos a las cuentas con privilegios de administrador de los sistemas operativos.

   Véanse las recomendaciones 1 y 3.b.

Hallazgo 4 - Falta de revisiones continuas de los registros provistos por el sistema operativo y falta de un registro de las actualizaciones a éste

a. A junio de 2007 los administradores de Redes no examinaban periódicamente los registros de seguridad provistos por el sistema operativo. Esto, para conocer las posibles violaciones de seguridad que pudieran ocurrir en los servidores y en la Red, y tomar prontamente las medidas preventivas y correctivas necesarias.

b. En el examen realizado el 14 de noviembre de 2007 sobre los controles implantados por la ACAA para la instalación de las actualizaciones al sistema operativo de la Red, encontramos que el DI no mantenía un registro de estas instalaciones.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se incluyen las directrices generales que permitirán a las entidades gubernamentales establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Además, se establece que será responsabilidad de cada entidad gubernamental desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnologías de ésta, particularmente sus sistemas de misión crítica. Esta norma se instrumenta, en parte, mediante lo siguiente:

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

- El registro de las actualizaciones realizadas a los sistemas operativos.

La situación comentada en el **Apartado a.** priva a la gerencia de las herramientas necesarias para supervisar eficientemente las actividades realizadas por los usuarios y detectar el acceso indebido de los recursos de la Red.

La situación comentada en el **Apartado b.** no permitía que el DI tuviera un control efectivo y documentado dirigido a mantener actualizado y en óptimas condiciones el sistema operativo instalado en los servidores de la Red. Esto mantenía al DI al margen de los avances tecnológicos, y no le permitía tener a su disposición las mejores herramientas que promovieran una administración más efectiva y eficiente de los recursos de la Red.

La situación comentada en el **Apartado a.** se debía, en parte, a que el Director del DI no había preparado, para la aprobación del Director Ejecutivo, los procedimientos para la administración de la Red donde se impartieran las instrucciones para que los

administradores de Redes revisen periódicamente los registros de seguridad provistos por el sistema operativo. **[Véase el Hallazgo 5]**

La situación comentada en el **Apartado b.** se debía a que el Director del DI no había considerado la importancia de mantener un registro de las actualizaciones hechas al sistema operativo.

Véanse las recomendaciones 1, y 3.c. y d.

Hallazgo 5 - Falta de normas y de procedimientos para reglamentar las operaciones del DI

a. Al 21 de agosto de 2007 la ACAA no había promulgado las normas y los procedimientos escritos necesarios para reglamentar y controlar eficazmente las siguientes operaciones:

- El establecimiento de los criterios para clasificar los recursos de tecnología de información
- La disposición de información sensitiva y de los programas, antes de transferir o dar de baja los equipos computadorizados y los medios de almacenamiento de información
- El establecimiento de acuerdos de confidencialidad y de no divulgación de información sensitiva contenida en los sistemas de información, y de las contraseñas de acceso utilizadas para acceder la misma
- La creación, la modificación y la cancelación de las cuentas de acceso de los usuarios de la Red
- La restricción de acceso a las aplicaciones del sistema operativo
- La identificación, la selección, la instalación y la modificación de los sistemas operativos de las computadoras y de los servidores
- El control de los cambios de emergencia a la configuración de la aplicación de los sistemas operativos
- El uso y la revisión de los programas utilitarios
- El desarrollo y el control de los cambios a las aplicaciones computadorizadas

- La administración de la seguridad de los sistemas de bases de datos y de la Red
- La verificación periódica de los derechos y los privilegios otorgados a los empleados con acceso físico a las áreas sensitivas del DI y los de acceso lógico otorgados a los usuarios de los sistemas de información
- La identificación y la documentación de los problemas relacionados con las aplicaciones de los sistemas operativos.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establecen las directrices generales que permiten a las entidades gubernamentales establecer controles adecuados en sus sistemas de información computadorizados para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Será responsabilidad de cada entidad gubernamental desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de ésta, particularmente sus sistemas de misión crítica. Esto implica que, como norma de sana administración, se deben establecer por escrito políticas, normas y procedimientos de control interno eficaces que reglamenten las operaciones computadorizadas y que estén aprobadas por la alta gerencia. Mediante las mismas se logra 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 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 responsabilidades y tomar las medidas correctivas necesarias. Además, podría exponer al personal del DI, a los equipos y a la información a riesgos que pudieran afectar la continuidad de las operaciones.

La situación comentada se atribuye, principalmente, a que el Director Ejecutivo no le había requerido al Director del DI que desarrollara y sometiera, para su consideración y aprobación, las normas y los procedimientos escritos para regir las operaciones que se indican.

Véanse las recomendaciones 1 y 3.e.

Hallazgo 6 - Falta de un plan de adiestramiento sobre la seguridad de los sistemas de información

a. Al 16 de agosto de 2007 el DI carecía de un plan de adiestramiento sobre la seguridad de los sistemas de información para el personal de la ACAA.

En la **Sección 12.4, Necesidades de Adiestramiento, del Reglamento de Personal para los Empleados Gerenciales de la ACAA** se establece que la ACAA, a través del Departamento de Recursos Humanos, anualmente realizará estudios mediante diferentes mecanismos para la identificación y el análisis de las necesidades de adiestramiento para el desarrollo de los empleados. En coordinación con los niveles de supervisión establecerá estrategias planificadas para satisfacer las demandas de adiestramiento y proveer la capacitación necesaria al personal de la ACAA para su ejecución óptima. Además, en la **Sección 12.5, Plan Anual de Adiestramiento, Capacitación y Desarrollo** de dicho **Reglamento** se establece, entre otras cosas, que los directores de Departamento y Oficina, determinarán anualmente sus necesidades de adiestramiento y su costo; establecerán un orden de prioridad a estas necesidades y los medios que utilizarán para atenderlas. También en la **Sección 12.6, Responsabilidades del Departamento de Recursos Humanos** del referido **Reglamento**, se establece, entre otras cosas, lo siguiente:

- El Departamento de Recursos Humanos desarrollará anualmente un Plan de Adiestramiento, Capacitación y Desarrollo de Empleados, basado en las necesidades identificadas y en armonía con lo presupuestado. Luego de aprobado, lo circulará entre el personal supervisor de las diversas unidades de trabajo.

- Administrará y coordinará las actividades de adiestramientos programadas durante el año para atender necesidades técnicas, generales y comunes.

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

- Será responsabilidad de cada entidad gubernamental desarrollar políticas específicas de seguridad que consideren las características propias de los ambientes de tecnología de ésta, particularmente sus sistemas de misión crítica.
- La entidad gubernamental es responsable de proveer adiestramientos a toda la gerencia y a los supervisores de ésta para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimientos actualizados sobre los aspectos de seguridad de sus áreas.
- La entidad gubernamental es responsable de crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

La situación comentada podría reducir la efectividad en el uso de los sistemas computadorizados y exponer los datos a riesgos innecesarios, tales como: la pérdida de información almacenada, la apropiación indebida de recursos, la propagación de virus electrónicos, el robo de identidad, la ejecución de funciones incompatibles y afectar la continuidad de las operaciones de la ACAA.

La situación comentada se debía a que el Director del DI no había identificado las necesidades de adiestramiento sobre el uso y la seguridad de los sistemas de información del personal de la ACAA a los fines de informar al Director de Recursos Humanos para que éste planifique y desarrolle un plan de adiestramiento para todo el personal que utiliza los sistemas computadorizados.

Véanse las recomendaciones 1 y 3.f.

Hallazgo 7 - Falta de un inventario de las licencias de las aplicaciones y faltas en el control de las instalaciones de éstas

a. La ACAA utiliza diferentes programas en sus sistemas de información. El uso de estos programas está restringido a la cantidad de licencias adquiridas. El examen realizado el 27 de septiembre de 2007 reveló las siguientes deficiencias:

1) El DI no mantenía un inventario de las licencias de los programas adquiridos e instalados en las computadoras que incluyera, entre otras cosas, el número de la licencia del programa, el nombre del proveedor, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el número de propiedad asignado y el total de licencias adquiridas.

2) El registro **Bitácora de Entrada y Salida de Software**, utilizado para controlar las licencias, no incluía el número de la licencia del programa, el número de propiedad del programa, el nombre del usuario ni la descripción y el número de propiedad de la computadora donde sería instalado el programa.

En la **Política Núm. TIG-008**, **Uso de Sistemas de Información, de la Internet y del Correo Electrónico de la Carta Circular Núm. 77-05** se establece lo siguiente:

- Los sistemas de información de las entidades gubernamentales, incluido los programas, aplicaciones y archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que debe constar en el inventario de las respectivas entidades gubernamentales y sólo pueden utilizarse para fines estrictamente oficiales y legales.

- Los usuarios de los sistemas de información están obligados a respetar los derechos de propiedad intelectual de los autores de las obras, programas, aplicaciones u otros, manejadas o accedidas a través de dicho sistema.

- Los programas y recursos utilizados en los sistemas de información de las entidades gubernamentales deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas.

Las mejores prácticas en el campo de la tecnología sugieren que se mantenga un registro de todos los programas en el cual se indique lo siguiente: el número de la licencia, el nombre del proveedor, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el equipo donde está instalado (número de propiedad o de serie), la ubicación física de la licencia, los disquetes y los manuales, el nombre del usuario, el número de propiedad asignado, la lista de inventario (licencia, disquetes, manuales, equipo) y el costo.

Las situaciones comentadas impiden ejercer un control eficaz de los programas y de las licencias correspondientes. Además, propician la instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para la ACAA.

Las situaciones comentadas se debían, en parte, a que el Director del DI no se había percatado de la necesidad de mantener un registro detallado y actualizado de los programas adquiridos e instalados en las computadoras de la ACAA.

Véanse las recomendaciones 1 y 3.g.

Hallazgo 8 - Funciones incompatibles realizadas por el Supervisor de los administradores de Redes y por un Administrador de Redes

a. El DI contaba con dos administradores de Redes los cuales le respondían al Supervisor de los administradores de Redes. El examen realizado el 14 de noviembre de 2007 de los perfiles de acceso de estos funcionarios, las hojas de deberes y las funciones que éstos realizaban reveló que el Supervisor de los administradores de Redes y un Administrador de Redes realizaban funciones incompatibles, según se indica:

    1) El Supervisor de los administradores de Redes creaba y modificaba las cuentas de acceso de los usuarios de la Red y, además, revisaba y autorizaba la creación y la modificación de dichas cuentas. Estas funciones resultaban incompatibles y conflictivas al ser llevadas a cabo por una misma persona.

2) Un Administrador de Redes realizaba funciones de programación para una aplicación, con su cuenta de acceso de administrador, e instalaba la misma en el área de producción. Estas funciones eran incompatibles entre sí y con las de administración de la seguridad de la Red realizadas por el administrador, las cuales se le habían asignado como parte de las funciones propias de su puesto.

Estas situaciones se agravaban al no existir un control alterno de supervisión de las funciones incompatibles realizadas por ambos funcionarios.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se dispone que las entidades gubernamentales deberán establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Conforme a dicha política y como norma de sana administración, es necesario que se segreguen las funciones relacionadas con las operaciones de los sistemas de información de la entidad. El objetivo primordial de dichas medidas de control es disminuir la probabilidad de que se cometan errores o irregularidades.

Las situaciones comentadas pueden propiciar que se cometan errores e irregularidades y, que no se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias.

Las situaciones comentadas se atribuyen, en parte, a que el Director del DI no había considerado el conflicto en las funciones que realizaban el Supervisor de los administradores de Redes y el Administrador de Redes. Además, la situación comentada en el **Apartado a.2)** se debía, en parte, a la falta de personal capacitado para trabajar en los nuevos lenguajes de programación[2].

Véanse las recomendaciones 1 y 3.h.

[2] Dicha información se incluyó en el borrador de los **hallazgos del Informe** sometido para comentarios al Director Ejecutivo y al ex Director Ejecutivo de la ACAA.

Hallazgo 9 - Falta de independencia organizacional del DI

a. El DI no tenía independencia organizacional con respecto a los usuarios que servía. Éste le respondía a la Subdirectoría de Operaciones Regionales y Servicios al Asegurado, que era uno de sus usuarios. Dicha estructura no proveía para mantener un sistema de control administrativo adecuado y ofrecer servicios a base de las necesidades de las distintas dependencias de la ACAA.

   Toda unidad de sistemas de información se debe reconocer como una unidad de servicios para todas las dependencias. Ésta debe ser independiente de las oficinas a las que sirve y solamente responder a los niveles gerenciales más altos de la entidad. Esto es necesario para garantizar un servicio equitativo a todos los usuarios del DI.

   La situación comentada puede propiciar el uso inadecuado de los recursos computadorizados y, que la utilización de los mismos se concentre en las áreas del usuario que tiene autoridad en las decisiones del DI. Además, puede afectar el desarrollo de aplicaciones, y ocasionar un estancamiento en el desarrollo y la implantación de los sistemas de los demás usuarios.

   Dicha situación se debía, en parte, a que en el **Diagrama Organizacional** no se clasificó al DI como una unidad independiente de sus usuarios.

   Véanse las recomendaciones 1 y 4.

ANEJO 1

ADMINISTRACIÓN DE COMPENSACIONES
POR ACCIDENTES DE AUTOMÓVILES

DEPARTAMENTO DE INFORMÁTICA

MIEMBROS DE LA JUNTA DE DIRECTORES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Lic. Juan R. Zalduondo Viera	Presidente	1 jun. 07	27 nov. 07
Sr. Salvador Calaf Legrand	Secretario	1 jun. 07	27 nov. 07
Dra. Rosa Pérez Perdomo	Miembro	1 jun. 07	27 nov. 07
Lic. Francisco Colón Pagán	"	1 jun. 07	27 nov. 07
Sr. Edgardo R. Martínez	"	1 jun. 07	27 nov. 07

ANEJO 2

ADMINISTRACIÓN DE COMPENSACIONES
POR ACCIDENTES DE AUTOMÓVILES

DEPARTAMENTO DE INFORMÁTICA

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Lic. Hiram A. Meléndez Rivera	Director Ejecutivo	1 jun. 07	27 nov. 07
Sra. María del C. Pagán Ortiz	Subdirectora Ejecutiva de Inversiones, Presupuesto y Asuntos Financieros	1 jun. 07	27 nov. 07
Sra. Faride El Hage Bucheme	Subdirectora Ejecutiva de Asuntos Administrativos y Gerenciales	1 jun. 07	27 nov. 07
Sr. Reinaldo Díaz Alicea	Subdirector Ejecutivo de Operaciones Regionales y Servicios al Asegurado	1 jun. 07	27 nov. 07
Lic. Rebecca Cotto Oyola	Directora de Finanzas	31 ago. 07	27 nov. 07
CPA William Jiménez Marrero	Director de Finanzas	1 jun. 07	30 ago. 07
CPA Humberto Muler Santiago	Auditor Interno	31 ago. 07	27 nov. 07
Lic. Rebecca Cotto Oyola	Auditora Interna	1 jun. 07	30 ago. 07
Sr. Virgilio Escobar Quiñones	Director de Informática	1 jun. 07	27 nov. 07
Sr. Rafael A. Cordero Rodríguez	Director de Recursos Humanos	1 jun. 07	27 nov. 07