INFORME DE AUDITORÍA TI-10-09

3 de noviembre de 2009

ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES

DEPARTAMENTO DE INFORMÁTICA

(Unidad 5010 - Auditoría 13121)

Período auditado: 28 de noviembre de 2007 al 27 de junio de 2008

CONTENIDO

Página

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

3 de noviembre 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 de 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 Núm. 9 del 24 de julio de 1952**, según enmendada.

Determinamos emitir varios informes de esta auditoría. Este es el segundo informe y contiene el resultado de nuestro examen sobre el desarrollo y el control de los cambios de las aplicaciones, la evaluación de la continuidad del servicio, y los controles de acceso establecidos en el DI. El primer informe se emitió el 24 de agosto de 2009 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 **(Informe de Auditoría TI-10-05)**.

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 2007-08 ascendió a $101,098,096, de los cuales $3,594,827 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, una Bibliotecaria 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 28 de noviembre de 2007 al 27 de junio de 2008. 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 al desarrollo y al control de los cambios de las aplicaciones, la evaluación de la continuidad del servicio y los controles de acceso establecidos en el DI, no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 10** de este **Informe**, clasificados como principales.

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

INFORME DE AUDITORÍA ANTERIOR

Una situación similar a la comentada en el **Hallazgo 7** de este **Informe** fue objeto de recomendación en el **Informe de Auditoría CPED-94-13 del 30 de junio de 1994**. Ésta no fue atendida.

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

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 6**. **[Hallazgos del 1 al 10]**

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

2. Realizar un análisis para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado para acceder a Internet. Luego de efectuado el análisis, someter la lista de las páginas autorizadas al DI. **[Hallazgo 1-a.]**

3. Realizar un análisis para determinar el personal clave de la ACAA que requiere tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. Luego de efectuado el análisis, someter la lista del personal clave al DI. **[Hallazgo 1-b.]**

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

    a. Se efectúen inspecciones periódicas necesarias para verificar el uso oficial de las cuentas para acceder a Internet y al correo electrónico. **[Hallazgo 1]**

    b. Se ofrezcan las orientaciones a los usuarios de los sistemas computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso de Internet y del correo electrónico. **[Hallazgo 1]**

c. El Supervisor de los administradores de redes se asegure de que:

1) Se limite el acceso a Internet para que el personal autorizado sólo pueda acceder las páginas electrónicas que son necesarias para cumplir con sus deberes y responsabilidades, según el análisis realizado por la gerencia. **[Hallazgo 1-a.]**

2) Se restrinjan los derechos y los privilegios para que solamente el personal clave de la ACAA pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis realizado por la gerencia. **[Hallazgo 1-b.]**

3) Se efectúen las modificaciones en los parámetros de seguridad de los servidores de la Red para:

a) Restringir el horario de acceso a los recursos de la Red, según las funciones y las responsabilidades de cada usuario, y activar en los servidores la opción para desconectar automáticamente las cuentas de acceso cuando éstas son utilizadas para acceder los recursos de la Red fuera de horas laborables. **[Hallazgo 2-a.1)]**

b) Desconectar automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la Red. **[Hallazgo 2-a.2)]**

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

d) Establecer un mínimo de ocho caracteres para la utilización de las contraseñas. **[Hallazgo 2-a.4)]**

e) Requerir a los usuarios cambiar sus contraseñas en un término fijo de, por lo menos, una vez al año. **[Hallazgo 2-c.1)]**

f) Establecer una fecha de expiración para las contraseñas de las cuentas de acceso. **[Hallazgo 2-c.2)]**

4) Se activen las opciones correspondientes en la pantalla de políticas de auditoría (*Audit Policies*) que se mencionan en el **Hallazgo 2-b.**, de manera que se pueda mantener un rastro de las actividades realizadas en los servidores de la ACAA.

5) Se realicen las gestiones necesarias para eliminar las cuentas de acceso que nunca se han utilizado. **[Hallazgo 2-c.3)]**

6) Se configuren las opciones de seguridad en el sistema operativo para controlar los accesos remotos mediante procedimientos de *call back*[1]. **[Hallazgo 5]**

d. Prepare y someta para aprobación:

1) El procedimiento para la creación, el mantenimiento y el control de las cuentas de acceso a la Red de la ACAA y a Internet. En éste se debe establecer la utilización de un formulario para la solicitud, la aprobación, la creación y la cancelación de las cuentas de acceso de los usuarios. **[Hallazgo 2-d.]**

2) Los procedimientos para la asignación de privilegio de acceso remoto a los usuarios. **[Hallazgo 5]**

3) El **Plan de Contingencias** en el que se incluyan los procedimientos para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información de acuerdo con los criterios que se mencionan en el **Hallazgo 6**.

[1] Es un control de acceso mediante el cual la computadora verifica que el número recibido está autorizado a conectarse remotamente para acceder a los sistemas de información computadorizados de la entidad.

4) El procedimiento de respaldos que describa, entre otras cosas: el proceso de respaldar la información y los programas, y para probar periódicamente los respaldos; el ciclo de reutilización, la rotulación y el almacenamiento de las cintas de respaldos; y la producción de un registro detallado sobre el contenido y el movimiento de éstas. **[Hallazgo del 8-a.1) al 5)]**

e. Tome las medidas necesarias para que el registro de accesos producido por el sistema electrónico de control de acceso sea revisado periódicamente. **[Hallazgo 3-a.]**

f. Se cumpla con las disposiciones establecidas en las **Normas de Acceso y Controles de Seguridad del Centro de Cómputos: Cuarto de Operaciones, Almacén y Bóveda Interna (Normas de Acceso)**, aprobadas el 29 de noviembre de 2004 por la Directora Ejecutiva de la ACAA, referentes a las medidas para controlar el acceso al Centro de Cómputos y a la Biblioteca. **[Hallazgo 3-b. y c.]**

g. Establezca las medidas de seguridad necesarias para controlar el acceso a los cuartos de distribución del cableado de la Red y proteger los equipos de telecomunicaciones, de manera que no estén accesibles al personal ajeno a las operaciones de la Red, y que los mismos se encuentren libres de materiales inflamables y de cualquier otro tipo de material que no esté relacionado con el funcionamiento de ésta. **[Hallazgo 4]**

h. Almacene una copia de los manuales de operación de todos los sistemas del DI, y de la documentación de las aplicaciones y de los programas en el centro de respaldo externo. **[Hallazgo 8-a.6)]**

i. Establezca, en coordinación con el Director de Recursos Humanos, un plan para ofrecer adiestramientos sobre el manejo y la operación de los equipos de prevención y de extinción de incendios, 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 9-a.3)]**

j. Se establezca un itinerario formal para proveer el servicio de mantenimiento preventivo requerido para los equipos computadorizados de acuerdo con las especificaciones de los manufactureros de éstos. **[Hallazgo 10]**

5. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus equipos en caso de desastres o emergencias en la ACAA, o considerar establecer su propio centro alterno en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra el DI. **[Hallazgo 7]**

6. Ejercer una supervisión efectiva sobre el Director de Administración de Propiedades para que se asegure de que los equipos de prevención y de extinción de incendios ubicados en el Centro de Cómputos del DI sean inspeccionados conforme a las regulaciones aplicables a los mismos. **[Hallazgo 9-a.1) y 2)]**

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este **Informe** se sometió, en cartas del 22 de septiembre de 2009, al Sr. Julio Alicea Vasallo, Director Ejecutivo de la ACAA, y al Lic. Hiram A. Meléndez Rivera, ex Director Ejecutivo de la ACAA, para comentarios.

COMENTARIOS DE LA GERENCIA

El Director Ejecutivo de la ACAA contestó el borrador de los **hallazgos** de este **Informe** mediante carta del 30 de septiembre de 2009, recibida en nuestra Oficina el 5 de octubre de 2009. En dicha carta indicó que aceptaba los hallazgos y que se comenzó a preparar un plan de acción para corregir las situaciones comentadas.

El 19 de octubre de 2009 el ex Director Ejecutivo de la ACAA envió un mensaje por correo electrónico para informar, entre otras cosas, que espera que cualquier deficiencia comentada esté corregida o en vías de ser corregida.

AGRADECIMIENTO

A los funcionarios y a los empleados de la ACAA, les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

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 DEPARTAMENTO DE INFORMÁTICA DE LA ADMINISTRACIÓN DE COMPENSACIONES 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 - Uso de los servicios de Internet para fines ajenos a la gestión pública y falta de controles de los mensajes de correo electrónico recibidos y enviados de fuentes externas a la ACAA

a. La ACAA mantenía un servidor[2] en la Red que permitía acceso a Internet a los usuarios autorizados. El examen del registro de direcciones de Internet visitadas por los usuarios de la ACAA del 11 al 31 de marzo de 2008 reveló que en dicho período se había utilizado este servicio para acceder 4,898 páginas de Internet. De éstas, 4,558 (93 por ciento) eran páginas de Internet con contenido ajeno a la gestión pública. No se pudieron determinar las cuentas de acceso de los usuarios que visitaron las mismas porque el servidor no estaba debidamente configurado para que se registrara el nombre del usuario que accedía a las páginas de Internet.

b. La ACAA mantenía un servidor[2] en la Red que permitía a los empleados el envío y el recibo de mensajes de correo electrónico. Dicho servidor producía diariamente un archivo en el cual se registraban todos los mensajes enviados y recibidos por las cuentas de usuarios (*message tracking logs*). El examen del registro del correo electrónico del 17 al 25 de abril de 2008 reveló que los usuarios podían recibir y enviar mensajes de correo electrónico de fuentes externas a la ACAA sin ningún tipo de restricción.

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

En la **Sección 9 del Artículo VI de la Constitución del Estado Libre Asociado de Puerto Rico** se establece que sólo se dispondrá de las propiedades y de los fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado y en todo caso por autoridad de ley.

En el **Artículo 3.2(c) de la Ley Núm. 12** se dispone, entre otras cosas, que ningún funcionario o empleado público utilizará propiedad pública para obtener directa o indirectamente ventajas, beneficios o privilegios que no estén permitidos por ley.

En las **Normas sobre el Uso de los Sistemas Electrónicos**, aprobadas el 11 de febrero de 2005 por el Director Ejecutivo, se establece, entre otras cosas, que los sistemas electrónicos de la ACAA no se podrán usar para propósitos personales, de recreo, diversión, juego, negocios o asuntos privados del usuario o cualquier otra persona, envío de mensajes en cadena, chistes y bromas, entre otros. De igual forma, el usuario no podrá utilizar los recursos electrónicos de la ACAA para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento ni cualesquiera otros servicios ajenos a su trabajo y a las funciones de la Agencia.

En la **Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales**, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto, se establece, entre otras cosas, lo siguiente:

- Los sistemas de información y las herramientas asociadas, como el correo electrónico y la Internet, sólo podrán ser utilizados por personal debidamente autorizado. Será responsabilidad de cada entidad gubernamental definir las tareas que conllevan acceso a tal herramienta. El uso de tales recursos constituye un privilegio otorgado con el propósito de agilizar los trabajos de la entidad gubernamental y no es un derecho.

- Los sistemas de comunicación y acceso a Internet son propiedad de la entidad gubernamental y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la entidad y nunca con fines no oficiales o para actividades personales o con fines de lucro.

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

Por otro lado, el acceso a páginas de Internet ajenas al fin público expone a los equipos y a la información sensitiva almacenada en los sistemas, a riesgos innecesarios como son la propagación de virus, *spyware*[3], *phishing*[4], *spoofing*[5], *spamming*[6] y ataques de negación de servicios[7], entre otros, que pudieran afectar la continuidad de las operaciones de la ACAA.

Las situaciones comentadas se debían, en parte, a la falta de:

- Orientaciones periódicas a los usuarios de los sistemas de información computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso y el manejo de las cuentas para acceder a Internet y al correo electrónico

---

[3] Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

[4] Es un tipo de ataque de correo electrónico que trata de convencer a un usuario de que el originador es auténtico, pero con la intención de obtener información.

[5] Es un ataque activo en el que el intruso presenta una identidad que no es la identidad original. En este ataque, el propósito es obtener acceso a los datos sensitivos o a los recursos de los sistemas de información computadorizados a los que no se permite el acceso bajo la identidad original.

[6] Es el envío de correspondencia electrónica a cientos o a miles de usuarios.

[7] Ocurren cuando una computadora conectada a Internet es inundada con datos y solicitudes que deben ser atendidas. La computadora se dedica exclusivamente a atender estos mensajes y queda imposibilitada de realizar otras actividades.

- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento de las normas establecidas para el uso oficial de los equipos computadorizados y de las cuentas para acceder a Internet

- Análisis para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado a acceder a Internet. Esto, para que el encargado de administrar la Red limite el acceso a las páginas autorizadas

- Análisis para determinar los funcionarios y los empleados a quienes debían otorgarse los privilegios para recibir y enviar mensajes de correo electrónico de fuentes externas, de acuerdo con las necesidades de la ACAA y con los deberes y las responsabilidades de sus puestos. Esto, para que el encargado de administrar la Red configure las cuentas de los usuarios.

Véanse las recomendaciones de la 1 a la 4.c.2).

Hallazgo 2 - Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de la Red

a. El examen realizado el 18 de marzo de 2008 de los parámetros de seguridad relacionados con las cuentas de acceso (*Account Policies*) de cinco servidores[8] de la Red reveló las siguientes deficiencias:

   1) No se había restringido el tiempo de acceso a la Red para todas las cuentas de acceso de acuerdo con las funciones de cada usuario (*Do not force logoff when logon hours expire*). El sistema les permitía a los usuarios tener acceso los 7 días de la semana y las 24 horas.

   2) No se había definido un término fijo de intentos de acceso sin éxito a los recursos de la Red para que el sistema inhabilitara automáticamente las cuentas de acceso de los usuarios (*No account lockout*).

[8] Véase la nota al calce 2.

3) No requería, al menos, un mínimo de 10 días para que el sistema le permitiera al usuario cambiar la contraseña nuevamente (*Minimum password age*).

4) No requería, al menos, un mínimo de ocho caracteres para la utilización de las contraseñas. El mínimo de caracteres requeridos para la utilización de las contraseñas se había establecido a cinco (*Minimum password length: 5 chars*).

b. Identificamos las siguientes deficiencias en los parámetros relacionados con las políticas de auditoría (*Audit Policies*) de los cinco servidores examinados:

1) En tres servidores[9] no se habían activado las opciones correspondientes a las políticas de auditoría (*Audit Policies: All auditing disabled*)

2) En dos servidores[9] no se habían definido las políticas de auditoría para que el sistema produzca un registro cuando ocurran los siguientes eventos:

- El encendido y apagado de la computadora (*Restart and Shutdown*)
- El acceso a los archivos y los objetos (*File/Object Access*)
- El uso de los privilegios asignados a los usuarios (*Use of User Right*)
- El seguimiento de los procesos (*Process Tracking*)
- Los cambios a la política de seguridad (*Security Policy Changes*)
- La administración de usuarios o grupos (*User/Group Management*)
- El acceso al directorio de servicio (*Directory Service Access*).

[9] Véase la nota al calce 2.

c. El examen realizado el 18 de marzo de 2008 a un servidor[10] reveló que había 1,177 cuentas de usuarios para acceder a la Red. De éstas, identificamos 299 cuentas de acceso que tenían las siguientes deficiencias:

1) Había 116 cuentas de acceso de usuarios que no habían cambiado su contraseña por un período mayor de 360 días.

2) No se había establecido una fecha de expiración para las contraseñas de 70 cuentas de acceso.

3) Había 112 cuentas que nunca fueron utilizadas por sus usuarios (*never logon*). Las mismas estaban activas al momento de nuestro examen.

d. La ACAA no había establecido un formulario para la solicitud, la aprobación, la creación y la cancelación de las cuentas para acceder a la Red y a Internet. Las solicitudes se realizaban mediante una comunicación por correo electrónico de los supervisores del área donde trabajaban los usuarios. Sin embargo, esta comunicación no proveía información sobre la acción tomada por el personal del DI para la creación o la cancelación de las cuentas de acceso.

En la **Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05**, se establece lo siguiente:

- Las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada.

- La información y los programas de aplicación utilizados en las operaciones de la entidad gubernamental deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos que necesita, o usar las

[10] Véase la nota al calce 2.

aplicaciones (o parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.

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

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

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

- La renovación periódica de la contraseña de cada usuario, según las necesidades de la entidad gubernamental y los procedimientos establecidos

- La desactivación inmediata de todas las cuentas de acceso que no estén en uso

- La limitación del tiempo de acceso para todas las cuentas de acceso de acuerdo con las funciones de cada usuario

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

- El mantenimiento de registros confiables y actualizados de las cuentas solicitadas y autorizadas.

En la **Carta Circular Núm. OC-98-11, Sugerencias sobre Normas y Controles para el Uso de los Sistemas Computadorizados**, promulgada el 18 de mayo de 1998 por el Contralor de Puerto Rico, se establece que para tener acceso al sistema, el usuario deberá registrar una contraseña (*password*) de por lo menos ocho caracteres, deberá ser una combinación de caracteres alfanuméricos (letras, números y símbolos) en cualquier proporción y arreglo, y que sólo será de su conocimiento.

Las situaciones comentadas en los **apartados del a. al c.** propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta.

Además, mantener la misma contraseña por tiempo prolongado puede propiciar que personas no autorizadas adquieran conocimiento de ésta y logren acceso no autorizado a los sistemas y a la información. Esto puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada en el **Apartado d.** impide mantener la evidencia requerida para otorgar o cancelar los accesos y los privilegios a los usuarios. Esto puede dificultar que se fijen responsabilidades por el uso indebido de los sistemas computadorizados. Además, puede afectar la integridad de la información registrada en éstos.

Las situaciones comentadas en los **apartados del a. al c.** se debían, en parte, a que el personal encargado de administrar los sistemas operativos no había puesto en vigor las opciones de seguridad de acceso lógico que proveen los sistemas operativos ni habían establecido controles adecuados para el mantenimiento de las cuentas de acceso a la Red.

La situación comentada en el **Apartado d.** se debía a que el Director Ejecutivo no le había requerido al Director del DI que desarrollara y le sometiera para aprobación un procedimiento para la creación, el mantenimiento y el control de las cuentas de acceso a la Red de la ACAA y a Internet que incluyera, entre otras cosas, la utilización y el control de un formulario para la solicitud, la creación, la aprobación y la cancelación de las cuentas de acceso de los usuarios.

Véanse las recomendaciones 1, y de la 4.c.3) a la 5) y d.1).

Hallazgo 3 - Falta de revisiones periódicas al registro de accesos al Centro de Cómputos, y deficiencias en el control de acceso físico en el Centro de Cómputos y en la Biblioteca

a. La ACAA utilizaba un sistema electrónico de control de acceso mediante la utilización de tarjetas para controlar y registrar el acceso al Centro de Cómputos y a otras áreas del DI. En el Centro de Cómputos estaban ubicados 22 servidores de la ACAA y el área de la Biblioteca. El sistema electrónico de control de acceso producía un registro de accesos en el cual se indicaba la fecha, la hora, el evento, el nombre de la persona que accedió, el número

de identificación de su tarjeta y el área visitada. La gerencia del DI no realizaba una revisión del registro de accesos al Centro de Cómputos.

b. Durante una visita realizada al Centro de Cómputos el 10 de enero de 2008, observamos que no se mantenía un registro de visitas para anotar aquellas personas que no tuvieran una tarjeta electrónica asignada para acceder a éste.

c. En una visita realizada al Centro de Cómputos el 22 de enero de 2008, observamos que la puerta que daba acceso a la Biblioteca, situada dentro de éste, se encontraba abierta mientras la Bibliotecaria no se encontraba en ésta. También estaba abierta la puerta de la bóveda de seguridad.

   En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que el acceso a las instalaciones de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas. En consonancia con dicha política pública y para salvaguardar la confidencialidad, la integridad y la disponibilidad de la información y garantizar la seguridad de los equipos computadorizados, es necesario que:

   - Se controle adecuadamente el acceso de personas a dichas instalaciones.

   - Se revisen periódicamente los registros de acceso que produce el sistema.

   En las **Normas de Acceso** se establece, entre otras cosas, que el empleado a cargo del Centro de Cómputos documentará en una bitácora los accesos otorgados con el nombre y la firma de la persona, el motivo de su visita, y el horario de entrada y de salida. Además, se establece que la Bibliotecaria deberá cerrar la bóveda interna cuando se ausente o se retira del área. En esos casos, el empleado a cargo del Centro de Cómputos sería la única persona que podría abrir la bóveda para localizar la información archivada. Por otro lado, en las referidas **Normas de Acceso** se menciona el personal que está autorizado a entrar al área del Centro de Cómputos y a la bóveda.

Las situaciones comentadas facilitan que personas ajenas a las operaciones del Centro de Cómputos tengan acceso a los equipos y a los recursos sensitivos de los sistemas computadorizados, y que puedan hacer uso indebido del equipo, manipular o destruir datos, o causar daños físicos a la propiedad. Esto representa un riesgo para la continuidad de los servicios que ofrece la ACAA, así como la confidencialidad de la información que se procesa.

La situación comentada en el **Apartado a.** se debió a que las **Normas de Acceso** no incluían una disposición para que se revisara el registro de accesos al Centro de Cómputos producido por el sistema electrónico de control de acceso.

Las situaciones comentadas en los **apartados b. y c.** se debieron a que el Director del DI y el empleado encargado del Centro de Cómputos no cumplieron con las disposiciones establecidas en las **Normas de Acceso**.

Véanse las recomendaciones 1, y 4.e. y f.

Hallazgo 4 - Deficiencias en los cuartos de distribución del cableado (*wiring closets*) de la Red

a. El examen efectuado el 10 de enero de 2008 a los siete cuartos de distribución del cableado (*wiring closets*) de la Red ubicados en el edificio central de la ACAA, reveló las siguientes deficiencias:

1) Seis cuartos de cableado (86 por ciento) no cumplían con las condiciones ambientales adecuadas para proteger los equipos de comunicaciones. En dichos cuartos se almacenaban materiales inflamables, tales como: cajas de cartón, puertas y pedazos de madera, paneles acústicos de techo, manuales, divisiones de cubículos, rollos de cable, latas de pintura y bombillas fluorescentes.

2) El Director de Administración de Propiedades y el Supervisor de los administradores de la Red, quienes tenían la custodia de las llaves de los cuartos de cableado, no mantenían un registro del uso de estas llaves.

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 la agencia, particularmente sus sistemas de misión crítica. Esto implica que, para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- Se mantengan los equipos de comunicaciones en un lugar seguro donde no se almacenen materiales que entorpezcan el libre movimiento en las referidas áreas y puedan causar daños a los equipos

- Se controle adecuadamente el acceso a las áreas donde están ubicados los equipos de comunicaciones.

La situación que se comenta en el **Apartado a.1)** puede ocasionar daños y deterioros prematuros a los equipos de la Red y a los equipos de computadoras, lo que dificultaría obtener el rendimiento máximo en términos de los servicios que ofrecen estos equipos. Además, pone en peligro la disponibilidad de la información que se procesa y almacena en la Red.

La situación comentada en el **Apartado a.2)** pudiera ocasionar que personas ajenas a la custodia, el funcionamiento y el mantenimiento de los cuartos de cableado tengan acceso a éstos, y ocasionar daños a los equipos de comunicaciones o a la información de la Red, sin que se pudieran fijar responsabilidades.

Las situaciones comentadas se debían a que el Director del DI no había cumplido con su deber de velar por que las instalaciones de equipos de comunicaciones estuvieran ubicadas en lugares adecuados y seguros. Tampoco había impartido instrucciones para que se implantaran medidas de control para la seguridad y el acceso físico de las instalaciones de la Red.

Véanse las recomendaciones 1 y 4.g.

Hallazgo 5 - Deficiencias relacionadas con el proceso de otorgación de privilegios de conexión remota

a. El examen efectuado el 4 de abril de 2008 a las 62 cuentas de acceso asignadas a usuarios que tenían el privilegio de conexión remota reveló lo siguiente:

1) No le fueron suministrados a nuestros auditores los documentos justificantes para la otorgación del privilegio de conexión remota para cinco cuentas de acceso[11].

2) Sesenta y una cuentas (98 por ciento) no se habían configurado para controlar los accesos remotos mediante procedimientos de *call back*.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que, si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la entidad gubernamental (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información. Esta norma se instrumenta, en parte, mediante:

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

- El establecimiento de normas y procedimientos específicos para la asignación del privilegio de acceso remoto a los usuarios, donde se incluya, entre otras cosas, la justificación para la otorgación de dicho privilegio.

Las situaciones comentadas impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y privilegios a los usuarios de conexión remota. También propician que personas no autorizadas puedan lograr acceso a información confidencial y

[11] Las cuentas de acceso se incluyeron en el borrador de los **hallazgos** del **Informe** sometido al Director Ejecutivo y al ex Director Ejecutivo de la ACAA, para comentarios.

hacer uso indebido de ésta. Además, pueden propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

Las situaciones comentadas se debían, en parte, a que el Director del DI no había preparado ni sometido al Director Ejecutivo, para aprobación, los procedimientos para la asignación de privilegio de acceso remoto a los usuarios. Además, el personal encargado de administrar los sistemas no había puesto en vigor las opciones de seguridad que provee el sistema operativo para controlar los accesos remotos.

Véanse las recomendaciones 1, y 4.c.6) y d.2).

Hallazgo 6 - Falta de un Plan de Contingencias

a. Al 25 de marzo de 2008, la ACAA carecía de un **Plan de Contingencias** para los sistemas de información, en el que se estableciera lo siguiente:

- Las medidas a considerarse en caso de ocurrir algún desastre o circunstancia que afectara las operaciones del Sistema

- Un plan escrito en donde se especifiquen los pasos a seguir para la reconstrucción de los archivos dañados o destruidos.

Las mejores prácticas en el campo de la tecnología de información sugieren que, para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados, se debe 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 entidad y deberá incluir, entre otras cosas:

- Grupos de recuperación que asuman las funciones de decisiones gerenciales, coordinación, restauración en el centro primario, activación y operación del centro alterno. Para cada grupo se deben identificar sus respectivos miembros y una lista

detallada con la información (números de teléfono residencial y del celular y dirección, entre otros) para una comunicación inmediata con éstos.

- Convenios escritos con los proveedores de los equipos y de los materiales necesarios para la recuperación de las operaciones, donde se estipulen las necesidades y los servicios requeridos para afrontar la emergencia.

- Itinerario de restauración identificado por grupos y por tareas, y especificado de manera secuencial. Para cada tarea deben detallarse todos los procesos que conlleve al igual que las funciones de cada uno de los miembros del grupo. Además, las personas asignadas a cada proceso deberán utilizar una identificación como participante del **Plan de Contingencias**.

- Una sección de aplicaciones que provea un detalle del orden de las prioridades de las aplicaciones a restaurar.

- Un detalle de todos los equipos utilizados en el centro primario, los requisitos mínimos necesarios para continuar las operaciones y los existentes en el centro alterno.

- Evidencia de los simulacros efectuados dos veces al año en el centro alterno.

La situación comentada podría propiciar la improvisación y, que en casos de emergencia, se tomen medidas inapropiadas y en forma desordenada. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, e interrupciones prolongadas de los servicios a los usuarios y a los beneficiarios de la ACAA.

La situación comentada se atribuye a que el Director Ejecutivo no había promulgado una directriz sobre la realización e implantación de un **Plan de Contingencias** para el DI con el propósito de garantizar la continuidad de las operaciones en caso de surgir algún desastre o emergencia.

Véanse las recomendaciones 1 y 4.d.3).

Hallazgo 7 - Falta de acuerdos para mantener un centro alterno de recuperación de sistemas de información

a. Al 25 de marzo de 2008, la ACAA no había formalizado acuerdos con otra entidad para establecer, en las instalaciones de ésta, un centro alterno de sistemas de información que permita restaurar las operaciones computadorizadas en casos de emergencia.

Una situación similar se comentó en el informe de auditoría anterior **CPED-94-13**.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del **Plan de Contingencias**, deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. Debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la entidad gubernamental, 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 entidad.

La situación comentada podría retrasar o impedir una pronta restauración de las operaciones de la ACAA y afectar las funciones de ésta, así como los servicios de las aplicaciones que ésta utiliza para brindar servicios a los lesionados en accidentes de tránsito y a sus beneficiarios. Esto, porque no tendría disponible unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento.

La situación comentada se atribuye a que el Director Ejecutivo de la ACAA no había realizado las gestiones necesarias para identificar un lugar disponible y adecuado como centro alterno, y formalizar los acuerdos necesarios para la utilización del mismo en casos de emergencia.

Véanse las recomendaciones 1 y 5.

Hallazgo 8 - Deficiencias en el manejo y el almacenamiento de los respaldos, y falta de copia de la documentación de las aplicaciones y de los manuales de operación en un lugar seguro fuera de los predios de la Oficina Central de la ACAA

a. El DI realizaba respaldos diarios de tres aplicaciones[12]. También realizaba un respaldo semanal de los archivos de información computadorizados que se mantenían en los servidores de la Oficina Central de la ACAA. En las oficinas regionales de la ACAA se realizaban respaldos diarios de una aplicación[12]. Estos respaldos se realizaban automáticamente desde el DI y el personal de cada Oficina Regional era responsable de colocar el medio magnético para preparar los mismos. La ACAA mantenía un acuerdo contractual con una compañía con el propósito de mantener los respaldos en un lugar fuera de los predios de la ACAA.

   El examen realizado del 21 de diciembre de 2007 al 25 de enero de 2008 de los procesos relacionados con la preparación y el almacenamiento de los respaldos de información que se realizaban en el DI y en las oficinas regionales, reveló las siguientes deficiencias:

   1) Los respaldos de información realizados por el DI no son sometidos a pruebas periódicas de restauración, de manera que la gerencia del DI pueda asegurarse de que la información almacenada esté completa, íntegra y disponible.

   2) El DI no había establecido la frecuencia con que se enviarían los respaldos a la compañía (bóveda externa). Al 16 de enero de 2008, el último respaldo que se había enviado a la bóveda externa era del 14 de noviembre de 2007.

   3) No se había establecido la frecuencia con que se enviarían al DI los respaldos preparados en las oficinas regionales de la ACAA. Estos respaldos se mantenían en cada Oficina Regional, por lo que estaban expuestos a las mismas posibles amenazas de desastres que la información almacenada en los servidores de éstas.

[12] El nombre de las aplicaciones se incluyó en el borrador de los **hallazgos** del **Informe** sometido al Director Ejecutivo y al ex Director Ejecutivo de la ACAA, para comentarios.

4) Las etiquetas de las cintas de los respaldos no tenían la fecha de actualización de la información almacenada.

5) En el formulario **Inventario de Cintas Magnéticas** que preparaba la Bibliotecaria del Centro de Cómputos del DI, no se habían registrado las fechas de creación, de expiración, y de entrada y de salida, el volumen ni el nombre del archivo de algunas cintas magnéticas almacenadas en la compañía.

6) No se mantenía una copia de los manuales de operación de los sistemas de información ni de la documentación de las aplicaciones y de los programas en un lugar seguro fuera de los predios de la Oficina Central de la ACAA.

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 sistemas esenciales e importantes para las operaciones de la entidad gubernamental. En consonancia con dicha política pública es necesario, entre otras cosas, que toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar seguro fuera de los predios de la entidad. Esto, con el propósito de recuperar la mayor cantidad de información posible en caso de una emergencia o desastre. Además, es necesario mantener un inventario detallado de las cintas de respaldos y que las mismas estén debidamente rotuladas para facilitar su localización y para sustituir periódicamente, por cintas nuevas, las utilizadas para respaldos.

En la **Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular Núm. 77-05** se establece, entre otras cosas, que los datos producidos y mantenidos en las entidades gubernamentales deben ser respaldados y mantenidos con una frecuencia conforme a la sensibilidad de los datos y el volumen de trabajo diario.

Como norma de sana administración y de control interno, se requiere que las entidades gubernamentales mantengan una copia actualizada de los manuales de operación de los sistemas de información y de la documentación de las aplicaciones y de los programas en un

lugar seguro fuera del edificio donde radica el centro. Además, se requiere que los respaldos de información se sometan a pruebas periódicas de restauración. Esto es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado en las instalaciones de la ACAA.

Las situaciones comentadas en el **Apartado del a.1) al 5)** impiden mantener un control adecuado de los respaldos de información y pueden ocasionar que en casos de emergencias la ACAA no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

La situación comentada en el **Apartado a.6)** podría afectar la continuidad de las operaciones normales del DI si ocurriera alguna eventualidad que afectara las instalaciones de ésta y destruyera toda la documentación y los manuales que allí se almacenan.

Las situaciones comentadas en el **Apartado del a.1) al 5)** se debieron a la falta de un procedimiento detallado y aprobado por el Director Ejecutivo para la creación, la rotulación, las pruebas, el envío y el almacenamiento de las cintas de respaldos.

La situación comentada en el **Apartado a.6)** se atribuye a que el Director del DI no había impartido instrucciones para que se enviaran y mantuvieran en un lugar fuera de los predios de la ACAA los documentos mencionados.

Véanse las recomendaciones 1, y 4.d.4) y h.

Hallazgo 9 - Falta de inspecciones de los sistemas para la prevención de incendios y de adiestramientos al personal para el uso de los mismos

a. En una inspección realizada el 5 de febrero de 2008 al Centro de Cómputos del DI, y mediante entrevista a empleados, identificamos las siguientes deficiencias:

1) Los dos extintores ubicados en el Centro de Cómputos no habían sido inspeccionados desde septiembre de 2006.

2) El sistema de supresión de incendios FM-200 no se había inspeccionado desde el 17 de noviembre de 2004. El ciclo mínimo de inspección recomendado por el manufacturero de este sistema era de 12 meses.

3) Los empleados del Centro de Cómputos no habían recibido adiestramientos sobre el uso de los extintores ni de la operación del sistema de supresión de incendios FM-200.

En la **Sección 1300.5**, **Extintores Portátiles para Combatir Incendios del Código para la Prevención de Incendios**, aprobado el 21 de junio de 1998 por el Jefe del Cuerpo de Bomberos de Puerto Rico, se establece que, por lo menos, una vez al año los extintores deben ser examinados minuciosamente o recargados. Además, se debe fijar firmemente una tarjeta que indique cuándo y por quiénes fueron inspeccionados, recargados o reparados. También éstos deben ser inspeccionados por un técnico autorizado por el Cuerpo de Bomberos de Puerto Rico.

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, realizará estudios anualmente 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

- 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 tener conocimiento actualizado 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.

Las situaciones comentadas pueden poner en riesgo la seguridad de los empleados y de los sistemas computadorizados. Además, podrían impedir la disponibilidad de los sistemas y, por consiguiente, limitar los servicios que presta la ACAA.

Las situaciones comentadas en el **Apartado a.1) y 2)** se debían a que el Director de Administración de Propiedades no cumplió con su deber de velar por que se inspeccionaran los equipos de prevención y extinción de incendios en el período requerido por las regulaciones del mismo.

La situación comentada en el **Apartado a.3)** se debía a que el Director del DI no había identificado las necesidades de adiestramiento del personal del DI sobre el manejo y la operación de los equipos de prevención y de extinción de incendios a los fines de informar al Director de Recursos Humanos para que éste planifique y desarrolle un plan de adiestramiento para éstos.

Véanse las recomendaciones 1, 4.i. y 6.

Hallazgo 10 - Falta de itinerarios de mantenimiento a los equipos computadorizados

a. Al 24 de marzo de 2008, el DI no mantenía un itinerario para proveer el mantenimiento preventivo requerido para los equipos computadorizados de la ACAA, según las recomendaciones de mantenimiento del manufacturero del equipo.

   En la **Política Núm. TIG-004, Servicios de Tecnología de la Carta Circular Núm. 77-05** se establece que el personal de la oficina de tecnología de información de la entidad gubernamental será el responsable de proveer apoyo a sus usuarios, así como del mantenimiento de sus sistemas internos. Además, revisará regularmente sus sistemas para verificar que funcionen adecuadamente.

   La situación comentada podría propiciar que fallas en dichas unidades no sean detectadas a tiempo. Esto, a su vez, puede resultar en una falla mayor en el sistema que interrumpa las operaciones de la ACAA y, por ende, el servicio que la entidad debe prestar a sus usuarios y beneficiarios.

   Esta situación se debía a que el Director del DI no había impartido instrucciones para que se implantaran medidas de control para mantener un plan de mantenimiento preventivo de los equipos computadorizados.

   Véanse las recomendaciones 1 y 4.j.

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	28 nov. 07	27 jun. 08
Sr. Salvador Calaf Legrand	Secretario	28 nov. 07	27 jun. 08
Dra. Rosa Pérez Perdomo	Miembro	28 nov. 07	27 jun. 08
Sr. Edgardo R. Martínez	"	28 nov. 07	27 jun. 08
Vacante	"	28 nov. 07	27 jun. 08

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	28 nov. 07	27 jun. 08
Sra. María del C. Pagán Ortiz	Subdirectora Ejecutiva de Inversiones, Presupuesto y Asuntos Financieros	28 nov. 07	27 jun. 08
Sra. Faride El Hage Bucheme	Subdirectora Ejecutiva de Asuntos Administrativos y Gerenciales	28 nov. 07	27 jun. 08
Sr. Reinaldo Díaz Alicea	Subdirector Ejecutivo de Operaciones Regionales y Servicios al Asegurado	28 nov. 07	27 jun. 08
Lic. Rebecca Cotto Oyola	Directora de Finanzas	28 nov. 07	27 jun. 08
CPA Humberto Muler Santiago	Auditor Interno	28 nov. 07	27 jun. 08
Sr. Virgilio Escobar Quiñones	Director de Informática	28 nov. 07	27 jun. 08
Sr. Rafael A. Cordero Rodríguez	Director de Recursos Humanos	28 nov. 07	27 jun. 08
Sr. Félix González Santiago	Director de Administración de Propiedades	28 nov. 07	27 jun. 08