INFORME DE AUDITORÍA TI-11-01

6 de diciembre de 2010

Administración de Compensaciones por Accidentes de Automóviles

Departamento de Informática

(Unidad 5010 - Auditoría 13202)

Período auditado: 29 de julio de 2008 al 25 de febrero de 2009

CONTENIDO

Página

INFORMACIÓN SOBRE LA UNIDAD AUDITADA 4

RESPONSABILIDAD DE LA GERENCIA 5

ALCANCE Y METODOLOGÍA 6

OPINIÓN 6

RECOMENDACIONES 7

A LA JUNTA DE DIRECTORES DE LA ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES 7

AL DIRECTOR EJECUTIVO DE LA ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES 7

CARTAS A LA GERENCIA 8

COMENTARIOS DE LA GERENCIA 8

AGRADECIMIENTO 8

RELACIÓN DETALLADA DE HALLAZGOS 9

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO 9

HALLAZGOS EN EL DEPARTAMENTO DE INFORMÁTICA DE LA ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES 10

1 - Deficiencia relacionada con el control de acceso al servidor donde está instalada la aplicación ACAA21 10

2 - Falta de un procedimiento para el manejo y la corrección de errores en la aplicación ACAA21 12

3 - Falta de participación de la Oficina de Auditoría Interna en el diseño, el desarrollo y la implantación de la aplicación ACAA21 13

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE DIRECTORES QUE ACTUARON DURANTE EL PERÍODO AUDITADO 15

ANEJO 2 - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO 16

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

6 de diciembre de 2010

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 el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico y, en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada.

Determinamos emitir tres informes de esta auditoría. Este es el tercer informe y contiene el resultado de nuestro examen sobre los controles para la documentación, y para la entrada y la validación de los datos de la aplicación ACAA21. 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*). El segundo informe se emitió el 3 de noviembre de 2009, 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 (*Informe de Auditoría TI-10-09*).

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 una relación de los miembros principales 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 2008-09 ascendió a $110,064,432, de los cuales $4,840,536 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 permite 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 administradores de redes, dos administradores de redes, un Técnico de Redes, una Bibliotecaria y dos operadores de computador.

La ACAA cuenta con una página en 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 del Estado Libre Asociado de Puerto Rico*, lo cual incluye divulgar sus disposiciones a todo el personal.

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 29 de julio de 2008 al 25 de febrero de 2009. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias.

Para efectuar la auditoría utilizamos la siguiente metodología:

- entrevistas a funcionarios, a empleados y a particulares
- inspecciones físicas
- examen y análisis de informes y de documentos generados por la unidad auditada
- examen y análisis de informes y de documentos suministrados por fuentes externas
- pruebas y análisis de procedimientos de control interno y de otros procesos
- confirmaciones de información pertinente.

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones del DI, en lo que concierne a los controles para la documentación, y para la entrada y la validación de los datos de la aplicación ACAA21, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 3**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE 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 la **Recomendación 3** de este *Informe*. **[Hallazgos 1 y 2]**

2. Ver que la Oficina de Auditoría Interna participe en el diseño, en el desarrollo y en la implantación de los sistemas de información computadorizados de la ACAA. **[Hallazgo 3]**

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

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

    a. Elimine las cuentas de acceso de los consultores de la compañía contratada al servidor donde está instalada la aplicación ACAA21 o, de ser necesario, limite sus privilegios de acuerdo con las necesidades del servicio. **[Hallazgo 1]**

    b. Para futuros proyectos de desarrollo e implantación de sistemas de información computadorizados, el personal concerniente del DI sea adiestrado en la operación de las aplicaciones y participe activamente en la etapa de desarrollo y de implantación de las mismas, de manera que puedan resolver los problemas que surjan con éstas. **[Hallazgo 1]**

    c. Prepare un procedimiento para el manejo y la corrección de los errores que ocurran durante el registro de los datos en la aplicación ACAA21, y lo remita para su aprobación. **[Hallazgo 2]**

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este *Informe* se remitió al Sr. Julio Alicea Vasallo, Director Ejecutivo de la ACAA, y al Lcdo. Hiram A. Meléndez Rivera, ex Director Ejecutivo de la ACAA, para comentarios, en cartas del 8 de abril de 2010.

COMENTARIOS DE LA GERENCIA

El Director Ejecutivo de la ACAA contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 22 de abril de 2010. En dicha carta indicó que aceptaba los hallazgos y que procederán a llevar a cabo las medidas correctivas para cumplir con nuestras recomendaciones.

El 3 de mayo de 2010, el ex Director Ejecutivo de la ACAA contestó el borrador de los **hallazgos** de este *Informe* mediante un mensaje por correo electrónico. Sus comentarios fueron considerados en la redacción final de este *Informe*; y se incluyen en la sección de la segunda parte de este *Informe*, titulada HALLAZGOS EN EL DEPARTAMENTO DE INFORMÁTICA DE LA ADMINISTRACIÓN DE COMPENSACIONES POR ACCIDENTES DE AUTOMÓVILES.

AGRADECIMIENTO

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

Oficina del Contralor
Por: Yesmín M. Valdivieso

RELACIÓN DETALLADA DE HALLAZGOS

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO

En nuestros informes de auditoría se incluyen los hallazgos significativos determinados por las pruebas realizadas. Éstos se clasifican como principales o secundarios. Los principales incluyen desviaciones de disposiciones sobre las operaciones de la unidad auditada que tienen un efecto material, tanto en el aspecto cuantitativo como en el cualitativo. Los secundarios son los que consisten en faltas o errores que no han tenido consecuencias graves.

Los hallazgos del informe se presentan según los atributos establecidos conforme a las normas de redacción de informes de nuestra Oficina. El propósito es facilitar al lector una mejor comprensión de la información ofrecida. Cada uno de ellos consta de las siguientes partes:

Situación - Los hechos encontrados en la auditoría indicativos de que no se cumplió con uno o más criterios.

Criterio - El marco de referencia para evaluar la situación. Es principalmente una ley, un reglamento, una carta circular, un memorando, un procedimiento, una norma de control interno, una norma de sana administración, un principio de contabilidad generalmente aceptado, una opinión de un experto o un juicio del auditor.

Efecto - Lo que significa, real o potencialmente, no cumplir con el criterio.

Causa - La razón fundamental por la cual ocurrió la situación.

En la sección sobre los **COMENTARIOS DE LA GERENCIA** se indica si el funcionario principal y los ex funcionarios de la unidad auditada efectuaron comentarios sobre el borrador de los hallazgos del informe, que les envía nuestra Oficina. Dichos comentarios se consideran al revisar el borrador del informe; y se incluyen al final del hallazgo correspondiente en la sección de HALLAZGOS EN EL 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 - Deficiencia relacionada con el control de acceso al servidor donde está instalada la aplicación ACAA21

a. En la ACAA se procesaban las reclamaciones de los lesionados en accidentes de automóviles y de sus dependientes beneficiarios mediante la aplicación ACAA21. Esta aplicación fue desarrollada e implantada por una compañía contratada. Este sistema controla, valida y adjudica los beneficios que se otorgan a las víctimas de accidentes de automóviles y a sus dependientes por concepto de servicios médico-hospitalarios, incapacidad, muerte, desmembramiento y funeral. Además, incluye un módulo para la emisión de cheques a los lesionados y a sus dependientes. La aplicación ACAA21 y la base de datos de ésta se mantienen en un servidor de la ACAA.

   El examen realizado el 10 de diciembre de 2008, relacionado con los accesos a la aplicación ACAA21 y al servidor, reveló que a dicha fecha no se habían eliminado del archivo de usuarios de la aplicación las cuentas de acceso[1] asignadas a dos consultores de la compañía contratada. Ambas cuentas estaban activas y tenían acceso irrestricto por tiempo indefinido a diferentes módulos de la aplicación. Estas cuentas se podían utilizar para registrar, editar y cancelar información relacionada con las reclamaciones remitidas por los lesionados a la ACAA. Las mencionadas cuentas debieron ser eliminadas luego de que la ACAA aceptara la aplicación y la instalara en producción el 21 de julio de 2004.

[1] Las cuentas de acceso se incluyeron en el borrador de los **hallazgos** de este *Informe*, remitido al Director Ejecutivo y al ex Director Ejecutivo para comentarios.

En la *Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto, se establece, entre otras cosas, 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 agencia deberán tener controles para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos que necesita, o usar las aplicaciones (o parte de las aplicaciones) que necesiten 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 el establecimiento de accesos rigurosos a las aplicaciones y a los archivos, que incluyan la creación de cuentas de acceso por un período determinado basado en las tareas y en la duración de las labores de los usuarios de éstas.

La situación comentada impide mantener un control adecuado sobre la información registrada en la aplicación ACAA21 y podría propiciar la alteración o el uso indebido de la información y, de este modo, comprometer la confidencialidad, la integridad y la disponibilidad de los datos contenidos en ésta.

La situación comentada se debió a que el personal del DI dependía de los consultores cuando surgían problemas con la operación de la aplicación ACAA21, ya que no tenían los conocimientos necesarios para resolverlos.

El ex Director Ejecutivo, en el mensaje de correo electrónico que nos envió, informó, entre otras cosas, que desconocía por qué no se hizo algo que debió hacerse desde julio de 2004.

Hallazgo 2 - Falta de un procedimiento para el manejo y la corrección de errores en la aplicación ACAA21

a. Al 21 de enero de 2009, la ACAA no contaba con un procedimiento escrito para el manejo y la corrección de los errores que ocurran durante el registro de los datos en la aplicación ACAA21.

En la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular Núm. 77-05,* se indica que se debe establecer una política del componente de datos e información mediante la cual las agencias mantengan uniformidad de los datos utilizados en sus sistemas. Los datos e información que las agencias mantienen son vitales para la toma de decisiones tanto para la agencia como para el desarrollo de estrategias que benefician los servicios ofrecidos por el Gobierno del Estado Libre Asociado de Puerto Rico. Las agencias deben establecer metodologías para asegurar la integridad y la confiabilidad de los datos producidos y almacenados. Esto implica que, como norma de sana administración, se deben establecer por escrito los procedimientos que detallen los pasos para el manejo y la corrección de los errores detectados por el sistema.

La situación comentada no permite establecer una metodología uniforme y controlada para el manejo y la corrección de errores en el sistema. Esto puede propiciar la comisión de errores e irregularidades, y afectar la integridad y la confiabilidad de la información provista por el sistema.

La situación comentada se atribuye a que el Director Ejecutivo no había impartido instrucciones al Director del DI para que éste preparara y remitiera para su aprobación un procedimiento para el manejo y la corrección de errores.

El ex Director Ejecutivo, en el mensaje de correo electrónico que nos envió, informó, entre otras cosas, que durante su incumbencia nadie le trajo a su atención la situación comentada. Además, que no podía conocer de la existencia de esta situación por no conocer el complejo mundo de la tecnología de informática.

Consideramos las alegaciones del ex Director Ejecutivo, pero determinamos que el **Hallazgo** prevalece.

Hallazgo 3 - Falta de participación de la Oficina de Auditoría Interna en el diseño, el desarrollo y la implantación de la aplicación ACAA21

a. El personal de la Oficina de Auditoría Interna no participó en el proceso de diseño, desarrollo e implantación de la aplicación ACAA21, para asegurarse de que la misma contiene los controles necesarios para una operación adecuada.

En las normas para la práctica profesional de la auditoría interna se establece, entre otras cosas, que la actividad de auditoría interna debe asistir a la organización mediante la identificación y la evaluación de las exposiciones de los riesgos, y contribuir al mejoramiento de los sistemas de gestión de riesgos y control. También se establece que la actividad de auditoría interna debe evaluar las exposiciones de riesgo referidas a gobierno, operaciones y sistemas de información con relación a lo siguiente:

- Confiabilidad e integridad de la información financiera y operativa
- Eficacia y eficiencia de las operaciones
- Protección de activo
- Cumplimiento de las leyes, los reglamentos y los contratos.

Además, como norma generalmente aceptada en el campo de la tecnología de información, los auditores internos deben participar en las diferentes etapas del desarrollo y la operación de los sistemas. Esta norma se fundamenta en la aportación que puedan hacer éstos en el desarrollo y en la implantación de los controles necesarios para una operación adecuada de dichos sistemas, y en la verificación continua del funcionamiento eficaz de los mismos. En consonancia con esta norma, la Oficina de Auditoría Interna tiene la responsabilidad de examinar las operaciones de los sistemas de información e informar a la gerencia sobre cualquier desviación de las normas establecidas.

Resulta difícil establecer controles adecuados en un sistema después que ha sido desarrollado e implantado. Además, existe la posibilidad de que al desarrollar un sistema no se incluyan los controles básicos necesarios, lo que podría propiciar que se cometan errores, irregularidades y otras situaciones adversas.

El Auditor Interno entendía que la participación de los auditores en el diseño y el desarrollo de una aplicación podría representar un conflicto de intereses cuando fueran a auditar la misma.

ANEJO 1

ADMINISTRACIÓN DE COMPENSACIONES
POR ACCIDENTES DE AUTOMÓVILES

DEPARTAMENTO DE INFORMÁTICA

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

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Lcdo. Manuel E. Sarmiento Vallecillo	Presidente	10 en. 09	25 feb. 09
Lcdo. Juan R. Zalduondo Viera	"	29 jul. 08	9 en. 09
Lcdo. Héctor R. Ramos Díaz	Secretario	10 en. 09	25 feb. 09
Sr. Salvador Calaf-Legrand	"	29 jul. 08	9 en. 09

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**
Sr. Julio H. Sepúlveda Ramos	Director Ejecutivo	17 feb. 09	25 feb. 09
"	Director Ejecutivo Interino	5 feb. 09	16 feb. 09
Sr. Fernando Batlle Burset	"	16 en. 09	4 feb. 09
Lcdo. Hiram A. Meléndez Rivera	Director Ejecutivo[2]	29 jul. 08	2 en. 09
CPA Humberto Muler Santiago	Auditor Interno Interino[3]	15 dic. 08	22 en. 09
"	Auditor Interno	29 jul. 08	14 dic. 08
Sr. Epifanio Delgado Vázquez	Director de Informática	23 en. 09	25 feb. 09
Sr. Virgilio Escobar Quiñones	Director de Informática Interino	15 dic. 08	22 en. 09
"	Director de Informática	29 jul. 08	14 dic. 08

[2] Puesto vacante del 3 al 15 de enero de 2009.

[3] Puesto vacante a partir del 23 de enero de 2009.