



Secretaría

MANUEL A. TORRES NIEVES
Manuel A. Torres Nieves
SECRETARIO DE SENADO

- Ver al dorso
- Para su información
- Notas
- Para mantenerle al día
- Expediente
- Dar Cuenta
- Registrar y Procesar

Senado
DE PUERTO RICO

EL CAPITOLIO
PO Box 9023431
San Juan, Puerto Rico
00902-3431

T: 787.722.3460
787.722.4012
F: 787.723.5413
E: mantorres@senadopr.us
W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

- Hacienda
- Gobierno
- Seguridad Pública y Judicatura
- Salud
- Educación y Asuntos de la Familia
- Desarrollo Económico y Planificación
- Urbanismo e Infraestructura
- Jurídico Penal
- Jurídico Civil
- Agricultura
- Recursos Naturales y Ambientales
- Comercio y Cooperativismo
- Turismo y Cultura
- Trabajo, Asuntos del Veterano y Recursos Humanos
- Bienestar Social
- Asuntos Municipales
- Recreación y Deportes
- Banca, Asuntos del Consumidor y Corporaciones Públicas
- Desarrollo de la Región del Oeste
- Asuntos de la Mujer
- Asuntos Internos
- Reglas y Calendario
- Asuntos Federales
- De la Montaña
- Ética

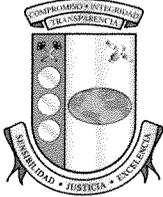
COMISIONES ESPECIALES

- Puerto de las Américas
- Derecho de Autodeterminación del Pueblo de Puerto Rico
- Sobre Reforma Gubernamental

COMISIONES CONJUNTAS

- Informes Especiales del Contralor
- Donativos Legislativos de Puerto Rico
- Internado Córdova-Fernós
- Internado Pilar Barbosa
- Internado Ramos Comas
- Código Penal
- Revisión y Reforma del Código Civil
- Alianzas Público Privadas
- Auditoría Fiscal y Manejo Fondos Públicos
- Revisión Continua Código Penal y Reforma de las Leyes

15 228



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

RECIBIDO SECRETARIA
2012 JAN 18 AM 9:34

Yesmín M. Valdivieso
Contralora

17 de enero de 2012

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Thomas Rivera Schatz
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-12-06* de la Oficina de Informática del Sistema de Retiro de los Empleados de la Autoridad de Energía Eléctrica de Puerto Rico aprobado por esta Oficina el 15 de diciembre de 2011. Publicaremos dicho *Informe* en nuestra página en Internet: <http://www.ocpr.gov.pr> para conocimiento de los medios de comunicación y de otras partes interesadas.

Estamos a sus órdenes para ofrecerle cualquier información adicional que estime necesaria.

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,

Yesmín M. Valdivieso
Yesmín M. Valdivieso

Anejo

RECIBIDO SECRETARIA
2012 JAN 17 12:12

n. u. ara



INFORME DE AUDITORÍA TI-12-06
15 de diciembre de 2011
Sistema de Retiro de los Empleados de la
Autoridad de Energía Eléctrica de Puerto Rico
Oficina de Informática
(Unidad 5131 - Auditoría 13244)

Período auditado: 8 de diciembre de 2008 al 18 de septiembre de 2009

CONTENIDO

	Página
INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....	3
RESPONSABILIDAD DE LA GERENCIA	5
ALCANCE Y METODOLOGÍA.....	5
OPINIÓN.....	6
INFORME DE AUDITORÍA ANTERIOR.....	6
RECOMENDACIONES	7
A LA JUNTA DE SÍNDICOS DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO.....	7
A LA ADMINISTRADORA DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO.....	7
CARTAS A LA GERENCIA.....	9
COMENTARIOS DE LA GERENCIA.....	9
AGRADECIMIENTO.....	10
RELACIÓN DETALLADA DE HALLAZGOS.....	11
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO.....	11
HALLAZGOS EN LA OFICINA DE INFORMÁTICA DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO.....	12
1 - Deficiencias relacionadas con el otorgamiento y la administración del contrato otorgado para el desarrollo y la implantación de un Plan de Continuidad de Negocios	12
2 - Falta de un Informe de Avalúo de Riesgos y de un Plan de Seguridad para los sistemas de información computadorizados	21
3 - Deficiencias relacionadas con el Plan de Continuidad de Negocios, con el Análisis de Impacto y con el Plan de Contingencias.....	24

4 - Falta de segregación de deberes y de supervisión de las tareas conflictivas realizadas por el Especialista en Administración de Banco de Datos..... 26

5 - Falta de normas y de procedimientos para reglamentar las operaciones de la Oficina de Informática 28

6 - Falta de participación de la Oficina de Auditoría Interna de la AEE en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados del Sistema de Retiro..... 30

ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS QUE ACTUARON DURANTE EL PERÍODO AUDITADO..... 32

ANEJO 2 - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO..... 33

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

15 de diciembre de 2011

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

Realizamos una auditoría de las operaciones de la Oficina de Informática del Sistema de Retiro de los Empleados de la Autoridad de Energía Eléctrica de Puerto Rico (Sistema de Retiro) 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 dos informes de esta auditoría. Este es el primer informe y contiene el resultado de nuestro examen de la administración del programa de seguridad, la segregación de deberes, y la evaluación de la continuidad del servicio, establecidos en la Oficina de Informática, y la participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Sistema de Retiro fue creado mediante la *Resolución Núm. 200 del 25 de junio de 1945* por la Junta de Directores de la Autoridad de Fuentes Fluviales de Puerto Rico, ahora Autoridad de Energía Eléctrica de Puerto Rico (AEE). Se estableció con el propósito de proveer pensiones y beneficios a los funcionarios y a los empleados de la AEE, acogidos al Sistema de Retiro.

Los poderes corporativos del Sistema de Retiro los ejerce una Junta de Síndicos, compuesta por ocho miembros. Por disposición reglamentaria, uno es el Director Ejecutivo de la AEE; tres los nombra la Junta de Gobierno de la AEE; tres son electos por los miembros activos del Sistema de Retiro; y uno es electo por los pensionados.

Las funciones ejecutivas del Sistema de Retiro las ejerce un Administrador nombrado por la Junta de Síndicos. Para llevar a cabo sus operaciones, el Sistema de Retiro cuenta con tres departamentos: Pensiones y Beneficios, Préstamos, y Contabilidad y Finanzas. Además, cuenta con la Oficina de Informática, la cual dirige una Supervisora de Proyectos de Informática.

Por disposiciones de la *Resolución Núm. 200*, la AEE paga de sus fondos los gastos administrativos del Sistema de Retiro. Entre ellos, los relacionados con la compra de materiales y equipo, y con el personal. El Sistema de Retiro se limita a realizar las funciones fiscales y administrativas del Fondo de Pensiones. Este recibe las aportaciones que realizan los miembros y la AEE, y los intereses que generan las inversiones que se realizan. Además, de ese fondo, el Sistema de Retiro también paga, entre otros, los gastos relacionados con los contratos de servicios profesionales y de consultoría. No obstante, en ocasiones, es la AEE quien incurre en los gastos de contratación para beneficio del Sistema de Retiro. Al 30 de abril de 2009, el Sistema de Retiro tenía 8,744 pensionados y 9,329 participantes activos.

Para los años fiscales del 2006-07 al 2008-09, el Sistema de Retiro generó ingresos por \$766,369,000 e incurrió en gastos operacionales por \$552,390,000, lo cual resultó en un saldo neto de ganancias al 30 de noviembre de 2008 de \$213,979,000.

Los **anejos 1 y 2** contienen una relación de los miembros principales de la Junta de Síndicos y de los funcionarios principales del Sistema de Retiro que actuaron durante el período auditado, respectivamente.

El Sistema de Retiro cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.aeepr.com/retiro>. 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*. Estos 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 8 de diciembre de 2008 al 18 de septiembre de 2009. En algunos aspectos se examinaron 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 de la Oficina de Informática, en lo que concierne a la administración del programa de seguridad, la segregación de deberes, y la continuidad del servicio, y a la participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 6**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

INFORME DE AUDITORÍA ANTERIOR

Una situación similar a la comentada en el **Hallazgo 1-a.3)** fue objeto de recomendación en el *Informe de Auditoría CPED-95-14* del 30 de junio de 1995. Esta recomendación no fue atendida.

El no atender, sin justa causa, las recomendaciones de los informes de auditoría de la Oficina del Contralor puede constituir una violación al Artículo 3.2(b) de la *Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental 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 SÍNDICOS DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO

1. Ver que la Administradora del Sistema de Retiro cumpla con las **recomendaciones de la 3 a la 9** de este *Informe*. **[Hallazgos del 1 al 5]**
2. Asegurarse de que, mediante el Comité de Auditoría, el Administrador de Auditoría Interna de la AEE efectúe auditorías periódicas sobre los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados del Sistema de Retiro. Además, vele por que se establezcan los controles de seguridad en las aplicaciones antes de que se implanten las mismas. **[Hallazgo 6]**

A LA ADMINISTRADORA DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO

3. Planificar de forma adecuada la contratación de los servicios para que se obtenga el mayor beneficio de los fondos utilizados y ver que la situación comentada no se repita. **[Hallazgo 1]**
4. Asegurarse de que para todo futuro proyecto relacionado con los sistemas de información se preparen previo al otorgamiento de un contrato: **[Hallazgo 1-a.1)]**
 - a. Estudios de viabilidad que permitan definir los requisitos de los usuarios y evaluar los beneficios y los costos asociados con cada una de las soluciones identificadas para satisfacer estos requisitos.
 - b. Solicitudes de propuestas detalladas que permitan evaluar el alcance y el costo de los servicios ofrecidos por los posibles contratistas antes de otorgar los contratos, y así obtener los mejores precios y condiciones.
5. Investigar y adjudicar responsabilidad a los funcionarios y a los empleados que participaron en la supervisión de los servicios prestados por la Compañía y de los desembolsos realizados por el Sistema de Retiro, sin que se concluyeran los trabajos. Además, velar por que dicha situación no se repita. **[Hallazgo 1-a.2)]**
6. Recobrar del contratista los \$7,980 pagados indebidamente por servicios prestados sin otorgar el contrato correspondiente. **[Hallazgo 1-a.3)]**

7. Asegurarse de que se formalicen los contratos escritos antes de que se reciban los servicios.
[Hallazgo 1-a.3)]
8. Ejercer una supervisión efectiva sobre la Supervisora de Proyectos de Informática para asegurarse de que:
 - a. Realice un 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. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. El mismo debe servir de base para el *Plan de Continuidad de Negocios*.
[Hallazgos 2-a. y 3-a.2)]
 - b. Realice las gestiones necesarias para revisar el *Plan de Continuidad de Negocios* preparado por la Compañía contratada, y asegurarse de que incluya un *Plan para la Recuperación de Desastres* y un *Plan para la Continuidad de Operaciones*, según se establece en la *Política Núm. TIG-003*. Además, vele por que se corrijan las situaciones comentadas en el **Hallazgo 3-a.1)** y **b**. Una vez el *Plan* sea revisado y aprobado, asegurarse de que se realicen pruebas periódicas y se divulgue a los empleados y a los funcionarios concernientes. Además, se mantenga una copia del mismo, en un lugar seguro fuera del Sistema de Retiro.
 - c. Prepare un *Plan de Contingencias* para que incluya los aspectos comentados en el **Hallazgo 3-c.** y lo remita para su aprobación.
 - d. Mantenga una segregación adecuada de las funciones conflictivas que realiza el Especialista en Administración de Banco de Datos o de la persona que en su lugar realice las tareas asignadas a este. De no poderlo realizar por limitaciones de recursos, implante medidas de controles compensatorios que mitiguen el riesgo resultante de una falta de segregación de funciones adecuada. **[Hallazgo 4]**

- e. En coordinación con la Administradora de la Oficina de Informática Corporativa (OIC) de la AEE, redacte y remita, para la consideración y aprobación de la Junta, las normas y los procedimientos escritos para regir las operaciones de la Oficina de Informática que se comentan en el **Hallazgo 5**.
9. Realizar las gestiones necesarias para que el Sistema de Retiro cuente con un *Plan de Seguridad* que incluya los criterios descritos en el **Hallazgo 2-b**. Además, se asegure de que se realicen pruebas periódicas al *Plan de Seguridad*, y que el mismo se divulgue a los empleados y a los funcionarios concernientes.

CARTAS A LA GERENCIA

Las situaciones comentadas en los **hallazgos** incluidos en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**, se informaron a la Sra. Marieolga Angleró Bruno, Administradora del Sistema de Retiro, mediante carta de nuestros auditores del 21 de septiembre de 2009.

El borrador de los **hallazgos** de este *Informe* se remitió a la Administradora del Sistema de Retiro y al Ing. Miguel A. Cordero López, Presidente de la Junta de Síndicos, para comentarios, por cartas del 8 de octubre de 2010. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al Sr. Otoniel Cruz Carrillo y al Sr. Rafael Gómez Irizarry, exadministradores del Sistema de Retiro, por cartas de esa misma fecha.

COMENTARIOS DE LA GERENCIA

En carta del 23 de octubre de 2009, la Administradora del Sistema de Retiro remitió sus comentarios a los **hallazgos** incluidos en la carta de nuestros auditores. Sus comentarios fueron considerados en la redacción del borrador de este *Informe*.

La Administradora del Sistema de Retiro contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 22 de noviembre de 2010. 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 LA OFICINA DE INFORMÁTICA DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO**.

Mediante carta del 25 de octubre de 2010, el señor Cruz Carrillo informó que sus comentarios serían incluidos en la contestación del Sistema de Retiro. Por carta del 19 de octubre de 2010, el señor Gómez Irizarry informó que la Administradora del Sistema de Retiro y el Comité de Auditoría de la Junta de Síndicos trabajaban en los comentarios a los **hallazgos** de este *Informe* y, por consiguiente, no presentaría comentarios sobre los mismos.

El Presidente de la Junta de Síndicos no contestó el borrador de los **hallazgos** de este *Informe* que le fue remitido para comentarios por carta del 8 de octubre de 2010, y mediante carta de seguimiento del 26 de octubre de 2010. No obstante, en la carta de la Administradora del Sistema de Retiro se incluyó una carta del 10 de noviembre de 2010 del Sr. Gilberto Rivera Lebrón, Administrador de la Oficina de Auditoría Interna de la AEE, quien remitió sus comentarios al **Hallazgo 6** de este *Informe*.

AGRADECIMIENTO

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

Oficina del Contralor
Por: *Erminio M. Urdanese*

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. Estos 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 exfuncionarios 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 LA OFICINA DE INFORMÁTICA DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO, de forma objetiva y conforme a las normas de nuestra

Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, este 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 LA OFICINA DE INFORMÁTICA DEL SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO

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

Hallazgo 1 - Deficiencias relacionadas con el otorgamiento y la administración del contrato otorgado para el desarrollo y la implantación de un Plan de Continuidad de Negocios

- a. Del 9 de agosto de 2001 al 30 de marzo de 2008, el Sistema de Retiro otorgó a una Compañía siete contratos por \$219,157 para recibir servicios de auditoría externa¹. El propósito de las auditorías efectuadas por la Compañía era expresar una opinión sobre los estados financieros del Sistema de Retiro. Sin embargo, como resultado de las mismas, la Compañía también presentaba, mediante cartas a la gerencia, su evaluación sobre los controles relacionados con los sistemas de información computadorizados del Sistema de Retiro. En todas las auditorías efectuadas por la Compañía, esta le comentó al Sistema de Retiro sobre la falta de un *Plan de Continuidad de Negocios (Plan)*.

El 26 de septiembre de 2007, en reunión del Comité de Auditoría del Sistema de Retiro, la Compañía, entre otras cosas, expuso su preocupación de que aún el Sistema de Retiro no contaba con un plan formal para la continuidad de sus operaciones, por lo que propuso adelantar la preparación del mismo. En esa reunión, la Supervisora de Proyectos de Informática sostuvo que, con la aprobación del Administrador, solicitó a la Compañía una cotización para preparar el *Plan*.

¹ Los contratos para los servicios de auditoría externa eran los números 2002-000001, 2004-000001, 2004-000005, 2005-000009, 2006-000005, 2007-000007, 2008-000011. Esta compañía prestó servicios de auditoría para el Sistema de Retiro hasta el 30 de septiembre de 2008.

El 28 de septiembre de 2007, la Compañía presentó al Sistema de Retiro una propuesta para desarrollar e implantar el *Plan* conforme a las necesidades del Sistema de Retiro. En la misma se estableció lo siguiente:

- El alcance del proyecto era desarrollar el *Plan*, que en términos generales, consistiría de los siguientes nueve componentes claves:
 - Un *Business Impact Analysis* que refleje las cantidades exactas de la posible pérdida potencial
 - Una evaluación profunda de las instalaciones en Aguadilla, en su rol de lugar alternativo
 - Una estrategia de recuperación adecuada para relocalizar las unidades del Sistema de Retiro, que tomen en consideración los requerimientos de comunicación
 - Una estrategia documentada para dar apoyo a los requerimientos del lugar alternativo
 - Un documento que especifique las estrategias de relocalización en el lugar de procesamiento alternativo
 - Una definición clara del *Recovery Time Objectives (RTO)* y del *Recovery Point Objectives (RPO)*
 - Una infraestructura de recuperación que apoye efectivamente todas las áreas afectadas
 - Una herramienta mecanizada que facilite el proceso de recuperación
 - Un conjunto de políticas y procedimientos documentados y aprobados para el Plan de Continuidad y de Recuperación de Desastres.
- La metodología que se utilizaría consistiría de tres fases: Fase I - Análisis de requerimientos, Fase II - Evaluación del lugar alternativo y Fase III - Documentación del plan e implantación del programa BCMS, luego de las cuales, el Sistema de Retiro contaría con el *Plan* completamente documentado e implantado.

Según esta propuesta, y basado en el alcance y la metodología establecida, los servicios profesionales contratados se realizarían en aproximadamente 260 horas, en un período

de 2 meses, por \$24,700. Además, el Sistema de Retiro pagaría \$5,170 por la licencia de un programa computadorizado para documentar el *Plan* y por el mantenimiento anual de este. Esto, para un total de \$29,870.

El 25 de octubre de 2007, el Administrador expuso ante la Junta de Síndicos del Sistema de Retiro que la Compañía era una de dos entidades certificadas en Puerto Rico para realizar este tipo de trabajo. Además, estableció que como medida de sana administración, al finalizar el contrato vigente no se le renovarían más contratos de auditoría. Ese mismo día, la propuesta fue aprobada por la Junta de Síndicos, mediante la *Resolución 2007-085*. En esta, se autorizó al Administrador a establecer el *Plan*, a contratar a la Compañía y a efectuar los pagos correspondientes.

El 3 de diciembre de 2007, el Sistema de Retiro formalizó el *Contrato Núm. 2008-000005* con la Compañía por \$29,870 para desarrollar el mencionado *Plan*. La vigencia del contrato fue del 3 de diciembre de 2007 al 3 de diciembre de 2008.

El 25 de abril de 2008, en reunión de la Junta de Síndicos, se indicó que el *Plan* estaba completado un poco más de 50 por ciento. El 1 de octubre de 2008, el Administrador sostuvo que la Compañía cobró un 70 por ciento por el trabajo realizado. Por otra parte, en reunión del 31 de octubre de 2008, se estableció que al 30 de septiembre de dicho año, el *Plan* estaba un 95 por ciento completado, y que a este solo le faltaba que se efectuaran las pruebas correspondientes en el centro alterno. El por ciento de terminación de las tareas completadas por la Compañía era determinado y certificado por la Supervisora de Proyectos de Informática.

El 31 de octubre de 2008, y con el propósito de que se completaran los trabajos pendientes del *Plan*, la Junta acordó extenderle el contrato a la Compañía por un año adicional, bajo los mismos términos y condiciones. Para esto, aprobó la *Resolución 2008-070*, producto de

la cual el socio principal de la Compañía y el Administrador firmaron² una *Carta de Aceptación* que fue notificada a la Oficina del Contralor de Puerto Rico el 4 de diciembre de 2008.

El 10 de noviembre de 2008, la Compañía presentó al Administrador una segunda propuesta en la que se indicaba que ayudaría al Sistema de Retiro a actualizar el *Plan* y a implantar el mismo. Para lograr la implantación del *Plan*, se requería completar las siguientes tres fases: Fase I - Seleccionar el lugar alternativo para la recuperación, Fase II - Modificar el plan existente, y Fase III - Preparar las pruebas en el lugar de recuperación. El importe de los servicios propuestos ascendía a \$19,900³. En esta propuesta se estableció que, a pesar de que el *Plan* estaba completamente documentado y computadorizado, el mismo no estaba totalmente implantado.

El 19 de diciembre de 2008, la Junta aprobó la *Resolución 2008-088* para finalizar el proyecto a un costo de \$19,900; y el 31 de diciembre de 2008, el Administrador notificó al representante de la Compañía sobre la aprobación de la segunda propuesta. En esta notificación, el Administrador indicó que no era necesario firmar un nuevo contrato.

Al 4 de junio de 2009, el Sistema de Retiro había pagado \$37,760 a la Compañía por servicios de consultoría relacionados con el desarrollo y la implantación del *Plan*, los cuales fueron prestados por la Compañía durante el período del 10 de enero de 2008 al 16 de abril de 2009, según las facturas presentadas. Al 11 de agosto de 2009, la Compañía evaluaba alternativas de lugares alternos para la recuperación que era la Fase I de su segunda propuesta.

El examen efectuado sobre el otorgamiento y la administración del *Contrato Núm. 2008-000005* reveló las siguientes deficiencias:

- 1) El Sistema de Retiro no tomó en consideración propuestas adicionales a la de la Compañía al contratar los servicios de preparación de un *Plan*. Esto impidió la participación de otras compañías que ofrecen los servicios contratados, y el examen de

² El socio principal firmó el 2 de diciembre y el entonces Administrador firmó el 3 de diciembre de 2008.

³ Consiste de \$19,000 para honorarios profesionales y \$900 para el mantenimiento anual de la licencia del programa computadorizado.

cuál proponente cumplía mejor y a menor costo con la necesidad de servicio identificada. Además, el Sistema de Retiro no le requirió a la Compañía evidencia de su cualificación para desarrollar el *Plan*, previo a su contratación.

En el *Procedimiento para el trámite y control de los contratos por servicios personales, profesionales o de expertos (Revisado)*, aprobado el 25 de octubre de 2000 por la Junta de Síndicos, se establece, entre otras cosas, que el Administrador gestiona propuestas para los servicios a contratarse, en coordinación con la Junta, y verifica que los contratistas evaluados estén cualificados de acuerdo con los criterios que sean aplicables.

En la *Política TIG-013, Marco Referencial de Adquisición Tecnológica Gubernamental*, promulgada mediante la *Carta Circular 80-06* del 30 de junio de 2006 por la Directora de la Oficina de Gerencia y Presupuesto, se sugieren como mejores prácticas en el campo de la tecnología de información al contratar servicios profesionales y consultivos:

- Obtener un mínimo de tres propuestas escritas por cada contrato.
- Mantener documentación clara y escrita para casos de único licitador.
- Adherirse a los principios de costo-efectividad; y el costo debe ser razonable aún en casos de único licitador.
- Contratar servicios profesionales y consultivos de firmas de buena reputación y con experiencia previa en los trabajos a contratarse.
- Asegurarse de que los servicios estén bien detallados en el contrato, de manera que sea fácil y claro establecer si el proveedor cumplió o no con los mismos.
- Identificar y eliminar cualquier conflicto de intereses.

La situación comentada brindó una ventaja indebida a la Compañía contratada, quien al conocer la necesidad del *Plan* por haber brindado los servicios de auditoría y

evaluación de los controles relacionados con los sistemas de información, se benefició de presentar una propuesta para el mismo. También pudo dar lugar a la comisión de irregularidades, favoritismos y a otras situaciones adversas al Sistema de Retiro.

2) Al 16 de septiembre de 2008, la Compañía había facturado y el Sistema de Retiro había pagado \$29,780 a pesar de que la Compañía no había completado los siguientes siete componentes claves del *Plan*:

- Una evaluación profunda de las instalaciones en Aguadilla, en su rol de lugar alternativo
- Una estrategia de recuperación adecuada para relocalizar las unidades del Sistema de Retiro, que tomen en consideración los requerimientos de comunicación
- Una estrategia documentada para dar apoyo a los requerimientos del lugar alternativo
- Un documento que especifique las estrategias de relocalización en el lugar de procesamiento alternativo
- Una definición clara del *RTO* y del *RPO*
- Una infraestructura de recuperación que apoye efectivamente todas las áreas afectadas
- Un conjunto de políticas y procedimientos documentados y aprobados para el Plan de Continuidad y de Recuperación de Desastres.

Al 8 de enero de 2009, el Sistema de Retiro no tenía un *Plan* completamente documentado como indicó la Compañía en su segunda propuesta.

En el Artículo 2-e. de la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada, se establece, como política pública, que cada dependencia o entidad corporativa deberá ejercer un control previo de todas sus operaciones que le permita al jefe de la entidad administrar efectivamente el desarrollo de los programas cuya dirección se le ha encomendado. En consonancia con dicha disposición, y como norma de sana administración, el funcionario a cargo de administrar los fondos de la entidad debe tomar las medidas necesarias para proteger

adecuadamente los intereses de esta. Conforme a ello, y como medida de control interno, el Sistema de Retiro debió asegurarse de que los procesos para la supervisión de los servicios contratados y la aprobación de los pagos relacionados con estos, se realizaran de forma tal que se protegieran los mejores intereses del Sistema de Retiro.

La situación comentada propició que el Sistema de Retiro desembolsara \$29,780, por un 22 por ciento de los componentes claves incluidos en el alcance del trabajo del mismo.

- 3) Al 4 de junio de 2009, la Compañía facturó y cobró \$7,980 de los \$19,900 estipulados en la segunda propuesta. Esto, a pesar de que no existía un contrato escrito entre las partes. Según las facturas de la Compañía, los servicios fueron prestados del 30 de diciembre de 2008 al 16 de abril de 2009.

Una situación similar se comentó en el *Informe de Auditoría CPED-95-14*.

En el Artículo VI, Sección 9 de la Constitución se dispone que: “Sólo se dispondrá de las propiedades y 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.B de la *Ley Núm. 237 del 31 de agosto de 2004, Ley para Establecer Parámetros Uniformes en los Procesos de Contratación de Servicios Profesionales o Consultivos para las Agencias y Entidades Gubernamentales*, se establece, entre otras cosas, que todo contrato entre una entidad gubernamental y un contratista debe formalizarse por escrito.

En la *Ley Núm. 18 del 30 de octubre de 1975*, según enmendada, se requiere que las entidades gubernamentales mantengan un registro de todos los contratos que otorgan y que remitan copias de los mismos a esta Oficina. Mediante la *Ley Núm. 127 del 31 de mayo de 2004*, la cual enmendó la *Ley Núm. 18*, se establece, entre otras cosas, que no se podrá exigir ninguna prestación o contraprestación objeto de un contrato podrá exigirse hasta tanto el mismo se presente para registro en la Oficina del Contralor, a tenor con lo dispuesto en dicha *Ley*. En el Artículo 5(f) del *Reglamento Núm. 33, Registro de Contratos, Escrituras y Documentos Relacionados, y Envío de Copias a la*

Oficina del Contralor del Estado Libre Asociado de Puerto Rico, promulgado el 20 de junio de 2008 por el Contralor de Puerto Rico, se establece una disposición relacionada con este particular.

En el caso *Colón v. Municipio de Arecibo*, 2007 T.S.P.R. 61 el Tribunal Supremo de Puerto Rico estableció que:

La facultad de los municipios de desembolsar fondos públicos para el pago de las obligaciones que contraen, está supeditada a que estas entidades públicas actúen acorde con los procedimientos establecidos por ley y nuestra jurisprudencia interpretativa.

De hecho, en la Exposición de Motivos de la ley se indicó que su propósito era “mantener y apoyar un sistema donde se protejan los intereses de las partes contratantes”, ciertamente, la mejor forma de lograr ese objetivo es asegurándose que los términos y condiciones del contrato consten con claridad para lo que es indispensable que el contrato se recoja a escrito. No se puede dejar en manos del mejor recuerdo del funcionario municipal o de un contratista la determinación de qué fue lo que se quiso pactar.

En el caso *De Jesús González v. Autoridad de Carreteras*, 148 D.P.R. 255 (1999), el Tribunal Supremo de Puerto Rico expresó:

[...] cuando la contratación involucra el uso de bienes o fondos públicos, hemos insistido, además, en la aplicación rigurosa de todas las normas pertinentes a la contratación y desembolso de esos fondos, a los fines de proteger los intereses y dineros del pueblo. Hemos enfatizado que el manejo prudente de fondos públicos está saturado de intereses de orden público [...]

La situación comentada es contraria al buen orden y al bienestar público. Además, propició que se realizaran pagos por trabajos inconclusos. También coloca en riesgo al Sistema de Retiro al no contar con un contrato escrito, según requerido por ley, y que esta Oficina lo considerara prontamente para los fines dispuestos por ley y registrarlo en el sistema computadorizado de información que se mantiene de los contratos que formalizan las entidades del Gobierno. Esto, para que los mismos estén disponibles a la ciudadanía en calidad de documentos públicos.

Las situaciones que se comentan se debieron a que el entonces Administrador y la Supervisora de Proyectos de Informática no protegieron adecuadamente los mejores intereses del Sistema de Retiro y actuaron en contra de la reglamentación aplicable.

La Administradora del Sistema de Retiro, en la carta que nos envió informó, entre otras cosas, que objetaba el **Hallazgo** por lo siguiente:

La ley de la Autoridad de Energía Eléctrica (Autoridad), establece lo siguiente: “Cuando se requieran servicios o trabajos profesionales o de expertos y la Autoridad estime que, en interés de una buena administración, tales servicios o trabajos deban contratarse sin mediar tales anuncios.” **[Apartado a.1)]**

Mediante la resolución 2008-088, la Junta de Síndicos aprobó la enmienda al acuerdo contractual propuesta por [...] el 19 de diciembre de 2008. Como parte del proceso para extender el contrato se había generado una Carta de Aceptación la cual fue debidamente registrada en la Oficina del Contralor de Puerto Rico (OCPR) el 4 de diciembre de 2008. Dicha compañía ya estaba contratada para llevar a cabo el *Plan* en el cual se requería la evaluación de un lugar alterno. **[Apartado a.3)]**

Consideramos las alegaciones de la Administradora del Sistema de Retiro con respecto al **apartado a.1) y 3) del Hallazgo**, pero determinamos que el mismo prevalece. La Sección 15 de la *Ley Núm. 83 del 2 de mayo de 1941*, según enmendada, en la cual se fundamenta la contestación de la Administradora del Sistema de Retiro, está dirigida a las solicitudes de subastas para contratos de construcción y compras. La situación que se comenta en el **apartado a.1) del Hallazgo** está relacionada con un contrato de servicios profesionales de tecnología de información, por lo que el Sistema de Retiro debía cumplir con lo establecido en el *Procedimiento para el trámite y control de los contratos por servicios personales, profesionales o de expertos (Revisado)*. Además, se requería la formalización de un nuevo contrato o de una enmienda al vigente porque en la segunda propuesta la Compañía ofreció servicios adicionales a los originalmente contratados, y por los que el Sistema de Retiro acordó pagar \$19,900 adicionales a la cuantía del contrato original. **[Apartado a.3)]**

Hallazgo 2 - Falta de un Informe de Avalúo de Riesgos y de un Plan de Seguridad para los sistemas de información computadorizados

a. Un avalúo de riesgos es un método para identificar las vulnerabilidades y las amenazas a los recursos de sistemas de información. Además, evalúa los posibles daños para determinar dónde implantar las medidas de seguridad para poder alcanzar y cumplir los objetivos de la entidad gubernamental. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.
- Identificar las vulnerabilidades y las amenazas de los recursos de sistemas de información.
- Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad gubernamental.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 22 de enero de 2009, en el Sistema de Retiro no se había realizado un avalúo de riesgos sobre los sistemas de información computadorizados. En su lugar, el Sistema de Retiro proveyó a nuestros auditores el *Plan de Trabajo Verificación de Controles Internos del 2007*, el cual solo tenía como objetivo servir de guía para efectuar auditorías de control interno.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece, entre otras cosas, que cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Para esto, deberá realizar un análisis de riesgos que incluya:

- Un inventario de los 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.

La situación comentada impidió al Sistema de Retiro desarrollar e implantar un programa de seguridad adecuado y los controles necesarios para reducir los riesgos que puedan afectar a sus activos.

- b. Al 10 de julio de 2009, el Sistema de Retiro no tenía un Plan de Seguridad aprobado por la Administradora que incluyera, entre otras cosas, disposiciones en cuanto a:
- La documentación de la validación de las normas de seguridad⁴
 - 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, y 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

⁴ 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*.

de seguridad de acuerdo con las características propias de los ambientes de tecnología de estas, 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 les 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.

La falta de un *Plan de Seguridad* podría provocar la inversión de recursos en medidas de control inapropiadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos.

Las situaciones que se comentan se atribuyen a que la Administradora del Sistema de Retiro no había efectuado las gestiones para la preparación y la documentación del avalúo de riesgos de los sistemas de información del Sistema de Retiro y para el desarrollo, la implantación y la actualización de un *Plan de Seguridad*, según lo establece la *Carta Circular Núm. 77-05*.

En la carta de la Administradora del Sistema de Retiro, esta indicó, entre otras cosas, que trabajan en el Avalúo de Riesgos [**Apartado a.**] y que el Plan de Seguridad para los sistemas de información computadorizados del Sistema de Retiro es parte de las responsabilidades de la OIC de la AEE [**Apartado b.**].

Consideramos las alegaciones de la Administradora del Sistema de Retiro con respecto al **apartado b. del Hallazgo**, pero determinamos que el mismo prevalece, porque el *Plan Estratégico de Seguridad, Sistemas de Información 2008-2010*, aprobado el 18 de noviembre de 2008 por la Administradora de la OIC de la AEE, incluido en la carta de la Administradora del Sistema de Retiro, no proveía disposiciones específicas para el Sistema de Retiro.

Hallazgo 3 - Deficiencias relacionadas con el Plan de Continuidad de Negocios, con el Análisis de Impacto y con el Plan de Contingencias

- a. El 8 de enero de 2009, la Supervisora de Proyectos de Informática nos proveyó para examen el *Plan de Continuidad de Negocios (Plan)* del Sistema de Retiro. El examen del *Plan* reveló las siguientes deficiencias:
 - 1) No estaba aprobado por la Administradora.
 - 2) No se basó en un avalúo de riesgos que, entre otros, le permitiera identificar y clasificar sus sistemas de información, y analizar las vulnerabilidades y las amenazas asociadas a estos.
- b. Un análisis de impacto de negocio tiene como objetivo cuantificar y calificar el impacto de negocio por pérdida o interrupción de las operaciones, y de las vulnerabilidades y las amenazas que fueron identificadas y clasificadas en el Avalúo de Riesgos. Además, debe proveer información para determinar las estrategias de recuperación más apropiadas. El análisis de impacto de negocio provisto para examen el 12 de febrero de 2009, carecía de lo siguiente:
 - La probabilidad de ocurrencia de las amenazas
 - La cuantificación del impacto financiero y operacional de las amenazas.
- c. El Sistema de Retiro carecía de un Plan de Contingencias que incluyera los siguientes requisitos que son necesarios para atender situaciones de emergencia:
 - La asignación clara de responsabilidades para la recuperación
 - Los procedimientos a seguir cuando a través de sus sistemas, los usuarios no puedan recibir ni transmitir información

- Un inventario completo de los equipos, de los sistemas operativos y de las aplicaciones
- La identificación de los archivos críticos del Sistema de Retiro
- Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos
- El detalle de la configuración de los equipos de comunicaciones que dan apoyo a los servidores que contienen información crítica del Sistema de Retiro y del contenido de los respaldos, así como los nombres de las librerías y de los archivos
- El nombre del encargado de activar el Plan y del personal de reserva, de forma tal que pueda ser ejecutado sin depender de individuos específicos
- Una hoja de cotejo para verificar los daños ocasionados
- Una lista de los números de teléfonos de los miembros de cada grupo de recuperación.

En el *Procedimiento para Desarrollar el Plan de Continuidad en Caso de Emergencia para los Sistemas*, aprobado el 23 de marzo de 2002 por el Director Ejecutivo de la AEE, se establece que los supervisores de las oficinas de informática de los directorados, junto a los supervisores custodios del equipo e información, confeccionan los planes de contingencia en caso de emergencia para los sistemas de información. El Administrador de la OIC los recomienda y el director correspondiente los aprueba. Además, en el *Procedimiento* se establece que los planes deben proveer instrucciones detalladas en cuanto al personal a ser activado durante el proceso de recuperación, plan de acción durante el proceso, identificación de información crítica y respaldos, tareas y responsabilidades de cada miembro de los grupos, entre otros.

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

Las mejores prácticas en el campo de la tecnología utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que como parte del *Plan de Continuidad de Negocios* se deberá preparar un *Plan de Contingencias*. Este es una guía que asegura la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presenten eventualidades inesperadas que afecten su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la entidad y deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del centro de cómputos o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable.

De ocurrir una emergencia, las situaciones comentadas podrían dar lugar a que el equipo no se proteja adecuadamente y sufra daños materiales, así como la pérdida de información importante. Además, se podría atrasar el proceso de reconstrucción de archivos y programas, y el pronto restablecimiento y la continuidad de las operaciones normales de los sistemas de información.

La situación comentada en el **apartado a.1)** se debía a que la Supervisora de Proyectos de Informática desconocía que el *Plan* debía estar aprobado.

Las situaciones comentadas en los **apartados a.2), b. y c.** se debían, en parte, a que la Supervisora de Proyectos de Informática no había ejercido una supervisión eficaz sobre la compañía contratada para que se tomaran en consideración los aspectos mencionados, **[Véase el Hallazgo 1]**

En la carta de la Administradora del Sistema de Retiro, esta nos indicó lo siguiente: “El Plan se aprobará por la Administradora cuando se finalice.” **[Apartado a.1)]**

Hallazgo 4 - Falta de segregación de deberes y de supervisión de las tareas conflictivas realizadas por el Especialista en Administración de Banco de Datos

- a. El Especialista en Administración de Banco de Datos se encargaba, como parte de sus funciones, de administrar la seguridad del Sistema de Préstamos y del Sistema Financiero,

y de velar por la integridad de los datos y su buen funcionamiento. Al 6 de agosto de 2009, al Especialista en Administración de Banco de Datos se le habían delegado las siguientes funciones que resultaban conflictivas e incompatibles con los deberes de su puesto:

- La programación del archivo que utiliza el Sistema de Retiro para efectuar ajustes en los pagos de depósito directo por concepto de nómina de jubilado
- El respaldo de los datos
- Las tareas asociadas con el privilegio de administrador asignado a los sistemas operativos.

La asignación de todas estas funciones le permitía al Especialista en Administración de Banco de Datos mantener un control total de los sistemas de información del Sistema de Retiro. Esta situación se agravaba al no existir un control alternativo de supervisión.

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 de información computadorizados 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 o se establezca la supervisión de las tareas conflictivas como control compensatorio. El objetivo primordial de dichas medidas de control es disminuir la probabilidad de que se cometan errores o irregularidades.

La falta de segregación de funciones propicia que se incurra en errores o irregularidades y que no se puedan detectar con prontitud, con los consiguientes efectos adversos para la entidad.

La situación comentada se atribuye a que la Supervisora de Proyectos de Informática no se había asegurado de mantener una segregación y supervisión adecuadas sobre las funciones realizadas por el Especialista en Administración de Banco de Datos.

En la carta de la Administradora del Sistema de Retiro, esta indicó lo siguiente: “Ante la falta de recursos técnicos corporativos y procurando la continuidad de los servicios del Sistema, maximizamos los recursos con los que contamos en la Oficina de Informática.”

Consideramos las alegaciones de la Administradora del Sistema de Retiro, pero determinamos que el **Hallazgo** prevalece. Cuando las funciones conflictivas no pueden ser segregadas por limitaciones de recursos, es necesario implantar medidas de controles compensatorios que mitiguen el riesgo resultante de una falta de segregación de funciones adecuada.

Hallazgo 5 - Falta de normas y de procedimientos para reglamentar las operaciones de la Oficina de Informática

a. Al 10 de julio de 2009, en el Sistema de Retiro no se habían promulgado las normas ni los procedimientos necesarios para reglamentar los siguientes procesos:

- El establecimiento de los criterios para clasificar los recursos de tecnología de información del Sistema de Retiro
- El control de acceso sobre los sistemas operativos utilizados por sus servidores
- La administración de la seguridad de sus bases de datos
- La verificación periódica del control de acceso físico sobre las áreas donde están localizados sus equipos y datos sensibles, y del acceso lógico que le otorga derechos y privilegios a los usuarios de los sistemas de información
- El uso y la revisión de los programas utilitarios
- El mantenimiento de los equipos computadorizados y la administración de problemas y cambios a los servidores para prevenir interrupciones no esperadas.

En el Artículo 6 del *Reglamento del Sistema de Retiro* se faculta a la Junta de Síndicos para crear las normas y los reglamentos que estime necesarios para llevar a cabo los fines, los propósitos y las actividades de la entidad. Cónsono con dicha disposición reglamentaria, y en ánimos de que la Junta cumpliera con su función, la Administradora, debió remitir para la consideración y la aprobación de dicho Cuerpo los procedimientos mencionados.

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 esta, 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 los mismos se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en casos de renunciaciones o ausencias del personal de mayor experiencia, y facilitan 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 de la Oficina de Informática, a los equipos y a la información a riesgos que pudieran afectar la continuidad de las operaciones.

La situación comentada denota que la Administradora del Sistema de Retiro no veló por que la Supervisora de Proyectos de Informática desarrollara las normas y los procedimientos escritos para regir las operaciones que se indican en el **Hallazgo**, y que se coordinara con la Administradora de la OIC de la AEE la inclusión o consideración de las normas y los procedimientos del Sistema de Retiro en las normas y los procedimientos corporativos.

En la carta de la Administradora del Sistema de Retiro, esta nos indicó, entre otras cosas, lo siguiente: “Las normas y los procedimientos de sistemas de información del Sistema de Retiro dependen de las responsabilidades corporativas de la OIC de la AEE.”

Consideramos las alegaciones de la Administradora del Sistema de Retiro, pero determinamos que el **Hallazgo** prevalece. El Sistema de Retiro y la OIC de la AEE no habían promulgado las normas ni los procedimientos necesarios para reglamentar los procesos indicados.

Hallazgo 6 - Falta de participación de la Oficina de Auditoría Interna de la AEE en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados del Sistema de Retiro

a. Al 7 de agosto de 2009, la Oficina de Auditoría Interna⁵ no había efectuado auditorías sobre los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados del Sistema de Retiro.

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, las operaciones y los 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 activos
- cumplimiento de las leyes, los reglamentos y los contratos.

La falta de fiscalización y de recomendaciones sobre los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados del Sistema de Retiro por parte de los auditores internos, puede propiciar que se cometan errores e irregularidades sin que los mismos se puedan detectar a tiempo para fijar responsabilidades. También priva a la gerencia de información necesaria sobre el funcionamiento de los sistemas, los controles y demás operaciones del Sistema de Retiro. Además, existe la posibilidad de que en los sistemas de información no se incluyan los controles básicos necesarios para evitar errores, irregularidades y otras situaciones adversas, lo que puede ser parte de las causas de los hallazgos que se comentan en este *Informe*.

⁵ En julio de 2007, el Director Ejecutivo de la AEE determinó reorganizar la Oficina de Auditoría Interna de la AEE para centralizar la función de auditoría interna, incluso la del Sistema de Retiro.

Esta situación se debía a que la Junta de Síndicos no se había asegurado de que el Comité de Auditoría requiriera a la Oficina de Auditoría Interna que incluyera en sus planes de trabajo efectuar auditorías periódicas de los sistemas de información del Sistema de Retiro.

En la carta del Administrador de la Oficina de Auditoría Interna de la AEE, incluida en la carta de la Administradora del Sistema de Retiro, este nos indicó lo siguiente:

La Oficina de Auditoría Interna fue reorganizada en julio de 2007. A pesar de los limitados recursos de personal y una alta cantidad de investigaciones por atender, realizamos intervenciones al Sistema de Retiro y se sometieron recomendaciones para mejorar los controles internos. Contamos con personal cualificado para realizar investigaciones, además de auditorías financieras, operacionales y de sistemas. El Sistema de Retiro está incluido en el Plan de Auditoría de este año.

ANEJO 1

**SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA
AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO
OFICINA DE INFORMÁTICA
MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS QUE
ACTUARON DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Ing. Miguel A. Cordero López	Presidente	15 en. 09	18 sep. 09
Ing. Juan F. Alicea Flores	"	8 dic. 08	14 en. 09
Sr. Rudy Cruz Vélez	Vicepresidente	8 dic. 08	18 sep. 09

ANEJO 2

**SISTEMA DE RETIRO DE LOS EMPLEADOS DE LA
AUTORIDAD DE ENERGÍA ELÉCTRICA DE PUERTO RICO
OFICINA DE INFORMÁTICA
FUNCIONARIOS PRINCIPALES QUE ACTUARON
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sra. Marieolga Angleró Bruno	Administradora	8 mar. 09	18 sep. 09
Sr. Rafael Gómez Irizarry	Administrador Interino	15 en. 09	7 mar. 09
Sr. Otoniel Cruz Carrillo	Administrador	8 dic. 08	14 en. 09
Sra. Maribel Serrano Ramírez	Supervisora de Proyectos de Informática	8 dic. 08	18 sep. 09

