



*Secretaria*

**MANUEL A. TORRES NIEVES**

*Manuel A. Torres Nieves*  
SECRETARIO DEL 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](mailto:mantorres@senadopr.us)  
W: [www.senadopr.us](http://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

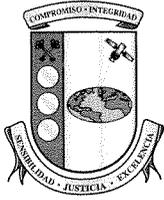
---

- 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



Estado Libre Asociado de Puerto Rico  
**Oficina del Contralor**

RECIBIDO  
SENADO DE PUERTO RICO  
2010 FEB 26 PM 2:04

26 de febrero de 2010

**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-10-13* de la Administración y Dirección de Sistemas de Informática del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico aprobado por esta Oficina el 23 de febrero de 2010. 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.

Contamos con su cooperación para mejorar la fiscalización y la administración de la propiedad y de los fondos públicos.

Cordialmente,

Natanael Arroyo Cruz  
Contralor Interino

Anejo

PO 8478

**INFORME DE AUDITORÍA TI-10-13**

23 de febrero de 2010

**Sistema de Retiro para Maestros del  
Estado Libre Asociado de Puerto Rico**

**Administración y Dirección de  
Sistemas de Informática**

(Unidad 5350 - Auditoría 13023)

Período auditado: 10 de septiembre de 2007 al 31 de octubre de 2008



## CONTENIDO

|  | Página    |
|--|-----------|
| <b>INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....</b>   | <b>3</b>  |
| <b>RESPONSABILIDAD DE LA GERENCIA .....</b>  | <b>6</b>  |
| <b>ALCANCE Y METODOLOGÍA.....</b>  | <b>7</b>  |
| <b>OPINIÓN.....</b>  | <b>7</b>  |
| <b>INFORME DE AUDITORÍA ANTERIOR.....</b>  | <b>8</b>  |
| <b>RECOMENDACIONES .....</b>   | <b>8</b>  |
| AL PRESIDENTE DE LA JUNTA DE SÍNDICOS .....  | 8         |
| AL DIRECTOR EJECUTIVO DEL SISTEMA DE RETIRO PARA MAESTROS<br>DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO.....   | 8         |
| <b>CARTAS A LA GERENCIA.....</b>   | <b>10</b> |
| <b>COMENTARIOS DE LA GERENCIA .....</b>  | <b>11</b> |
| <b>AGRADECIMIENTO .....</b>  | <b>12</b> |
| <b>RELACIÓN DETALLADA DE HALLAZGOS.....</b>  | <b>13</b> |
| CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO .....   | 13        |
| HALLAZGOS EN LA ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS<br>DE INFORMÁTICA DEL SISTEMA DE RETIRO PARA MAESTROS DEL<br>ESTADO LIBRE ASOCIADO DE PUERTO RICO .....   | 14        |
| 1 - Falta de un Informe de Avalúo de Riesgos .....   | 14        |
| 2 - Falta de un Plan de Seguridad .....  | 17        |
| 3 - Falta de un Plan de Continuidad de Negocios.....   | 19        |
| 4 - Deficiencias en las políticas, las normas y los procedimientos relacionados<br>con la administración, la seguridad y el uso de los sistemas computadorizados<br>del Sistema, y falta de normas y procedimientos para reglamentar varios<br>procesos de la ADSI ..... | 21        |

|  |           |
|--|-----------|
| 5 - Deficiencias relacionadas con los controles para la preparación, el manejo y el almacenamiento de los respaldos de información, y copias de los manuales de operaciones y de la documentación de las aplicaciones, de los programas y de las bases de datos no mantenidas en instalaciones externas de la ADSI ..... | 27        |
| 6 - Atrasos en la revisión de los informes de operaciones diarias .....  | 30        |
| 7 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información .....   | 32        |
| 8 - Falta de adiestramientos sobre las normas y los procedimientos para el uso y la seguridad de los sistemas de información .....   | 33        |
| 9 - Falta de evaluaciones periódicas sobre el desempeño de los empleados de la ADSI .....  | 35        |
| <b>ANEJO 1 - MIEMBROS DE LA JUNTA DE SÍNDICOS QUE ACTUARON DURANTE EL PERÍODO AUDITADO .....</b>   | <b>37</b> |
| <b>ANEJO 2 - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO .....</b>   | <b>38</b> |

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

23 de febrero de 2010

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

Realizamos una auditoría de las operaciones de la Administración y Dirección de Sistemas de Informática (ADSI) del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico (Sistema) 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 varios informes de esta auditoría. Este es el primer informe y contiene el resultado de nuestro examen de los controles internos relacionados con la administración del programa de seguridad, la evaluación de la continuidad de servicio, el desarrollo y el control de los cambios de las aplicaciones, 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 se creó en virtud de la *Ley Núm. 91 del 29 de marzo de 2004, Ley del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico*, según enmendada. Esta *Ley* derogó la *Ley Núm. 218 del 6 de mayo de 1951, Ley de Retiro para Maestros*. Con la *Ley Núm. 91*, entre otras cosas, se creó una nueva estructura organizacional con el fin de dotar al Sistema de agilidad y rapidez en los procesos que lleva a cabo; otorgarle

autonomía gerencial y administrativa al separarlo de la intervención de otras agencias; establecer una política anticorrupción; y garantizar a los participantes el recibo de los beneficios que le corresponden en un tiempo justo. Además, mediante la *Ley Núm. 91*, se transfirieron al Sistema todos los recursos y las facilidades en conexión con los programas y las funciones de la Junta de Retiro para Maestros. También se transfirieron al Sistema todas las deudas, las obligaciones y las responsabilidades de dicha Junta.

El Sistema es responsable de administrar eficaz y eficientemente un Fondo de Anualidades y Pensiones mediante el desarrollo de estrategias de inversión que redunden en su solvencia económica. Además, tiene la responsabilidad de proveer seguridad económica para el futuro de sus participantes.

Los poderes del Sistema son ejercidos por una Junta de Síndicos (Junta) compuesta por nueve miembros: el Secretario de Hacienda, quien actúa como Presidente, el Secretario de Educación, el Presidente del Banco Gubernamental de Fomento para Puerto Rico (BGF), el presidente de una organización magisterial, un maestro en representación de los maestros en servicio activo, dos maestros en representación de los maestros jubilados, el presidente de la entidad que representa la unidad apropiada bajo la *Ley Núm. 45 del 25 de febrero de 1998, Ley de Relaciones del Trabajo para el Servicio Público de Puerto Rico*, según enmendada, y un miembro en representación del interés público. La Junta tiene la responsabilidad de nombrar un Director Ejecutivo quien se encarga, entre otras cosas, de dirigir y administrar el Sistema.

El **ANEJO 1** contiene una relación de los miembros de la Junta de Síndicos que actuaron durante el período auditado.

El Sistema realiza sus operaciones a través de las siguientes unidades: el Área de Finanzas e Inversiones, el Área Operacional, la Oficina de Asuntos Legales y Laborales, la Oficina de Desarrollo Institucional, el Área de Servicios Auxiliares, la Oficina de Asuntos Laborales, la Oficina de Recursos Humanos y la ADSI. Estas unidades le responden directamente al Director Ejecutivo. Además, el Sistema cuenta con una Oficina de Auditoría Interna que le responde directamente a la Junta.

La ADSI cuenta con los siguientes puestos: un Oficial Principal de Informática, un Director Asociado de Sistemas de Informática, un Director Auxiliar de Sistemas de Informática, dos oficiales de Seguridad de Sistemas de Informática, una Oficial de Sistemas y Procedimientos, una Analista de Sistemas y Procedimientos, un Especialista en Microcomputadoras y Red de Comunicaciones, un Especialista en Sistemas Operativos de Informática, un Supervisor de Operaciones de Sistemas de Informática, tres operadores Principales de Unidad Central de Sistemas de Informática, tres operadores de Unidad Central de Sistemas de Informática, una Estadística, cuatro desarrolladores Principales de Sistemas de Informática, seis desarrolladores de Sistemas de Informática, una Asistente de Servicios de Oficina y una Asistente Administrativo Principal. Al 31 de octubre de 2008, estaban vacantes los puestos de Director Asociado de Sistemas de Informática y de Supervisor de Desarrollo de Sistemas de Informática.

El ANEJO 2 contiene una relación de los funcionarios principales que actuaron durante el período auditado.

Los recursos para financiar las actividades operacionales del Sistema provienen principalmente de las aportaciones patronales e individuales, los intereses sobre préstamos y los ingresos provenientes de las inversiones. Además, el Sistema recibe aportaciones del Fondo General del Gobierno del Estado Libre Asociado de Puerto Rico para cubrir beneficios garantizados a los pensionados mediante leyes especiales.

Los recursos asignados por el Sistema para las operaciones de la ADSI y para el Proyecto de Mecanización durante los años fiscales del 2005-06 al 2007-08 ascendieron a \$6,885,095 y \$5,756,360, respectivamente, según se indica:

| <b>AÑO FISCAL</b> | <b>ADSI</b>               | <b>PROYECTO DE MECANIZACIÓN</b> |
|-------------------|---------------------------|---------------------------------|
| 2005-06           | \$2,070,881               | \$3,637,523                     |
| 2006-07           | 2,304,036                 | 1,577,637                       |
| 2007-08           | <u>2,510,178</u>          | <u>541,200</u>                  |
| <b>TOTAL</b>      | <b><u>\$6,885,095</u></b> | <b><u>\$5,756,360</u></b>       |

Al 4 de diciembre de 2008, el Sistema no tenía demandas pendientes de resolución por los tribunales relacionadas con los sistemas de información computadorizados.

El Sistema cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.srm.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 10 de septiembre de 2007 al 31 de octubre de 2008. 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 ADSI en lo que concierne a los controles internos relacionados con la administración del programa de seguridad, la evaluación de la continuidad del servicio y el desarrollo y el control de los cambios de las aplicaciones, y con 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 9**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

## INFORME DE AUDITORÍA ANTERIOR

Situaciones similares a las comentadas en los **hallazgos 3 y 4-a.5)** de este *Informe* fueron objeto de recomendaciones en el *Informe de Auditoría CPED-93-16* del 30 de junio de 1993. Éstas no fueron atendidas.

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

### AL PRESIDENTE DE LA JUNTA DE SÍNDICOS

1. Ver que el Director Ejecutivo del Sistema cumpla con las **recomendaciones de la 3 a la 7** de este *Informe*. [**Hallazgos del 1 al 6, 8 y 9**]
2. Ver que la Oficina de Auditoría Interna efectúe auditorías periódicas sobre los procedimientos, los controles y el funcionamiento de sus sistemas de información computadorizados. [**Hallazgo 7**]

### AL DIRECTOR EJECUTIVO DEL SISTEMA DE RETIRO PARA MAESTROS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO

3. Asegurarse de que se realice y se documente el análisis de riesgos, según se establece en la *Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales*, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto, en la *Norma Núm. SRM-ADSI-003-07, Normas para la Seguridad de los Sistemas de Información*, aprobada el 10 de septiembre de 2007 por el Director Ejecutivo del Sistema e incluida en el *Manual de Normas y Procedimientos de los Sistemas de*

*Información* y, se sugieren en las mejores prácticas en el campo de tecnología. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. **[Hallazgo 1]**

4. Ejercer una supervisión eficaz sobre el Oficial Principal de Informática de la ADSI para asegurarse de que:
  - a. Realice las gestiones pertinentes para la preparación de un plan de seguridad para la ADSI que incluya los criterios descritos en el **Hallazgo 2** y luego lo remita para aprobación. Una vez aprobado, asegurarse de que se realicen pruebas periódicas y se divulgue a los empleados y a los funcionarios concernientes.
  - b. Realice las gestiones pertinentes para la preparación de un *Plan de Continuidad de Negocios* 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* y en la *Norma Núm. SRM-ADSI-002-07, Norma de Resguardo y Procedimientos de los Sistemas de Información*, aprobada el 10 de septiembre de 2007 por el Director Ejecutivo del Sistema, e incluida en el *Manual*. **[Hallazgo 3]**
  - c. Prepare y remita para aprobación, las normas y los procedimientos necesarios para reglamentar los procesos que se indican en el **Hallazgo 4-a.4)** y **d.**
  - d. Imparta instrucciones a los empleados de la ADSI responsables de preparar y custodiar los respaldos de información para que se aseguren de que las etiquetas externas utilizadas para identificar los medios de almacenamiento incluyan la información que se indica en el **Hallazgo 5-a.1)**.
  - e. Establezca un registro de los respaldos que incluya la información actualizada y necesaria para mantener el control de los medios magnéticos, y para corregir la situación comentada en el **Hallazgo 5-a.2)**. Además, imparta instrucciones para que se mantengan organizadas y archivadas las hojas de trámite que incluyen información sobre las transferencias de los medios magnéticos al centro de almacenamiento externo y la devolución de éstos a la ADSI.

- f. Mantenga en el centro de almacenamiento externo una copia de la documentación de las aplicaciones y de los programas, y de los manuales relacionados con la operación de los sistemas de información del Sistema. **[Hallazgo 5-b.]**
  - g. El Supervisor de Operaciones de Sistemas de Informática y los oficiales de la seguridad revisen diariamente los informes de operaciones diarias. **[Hallazgo 6]**
5. Asegurarse de que las normas y los procedimientos aprobados sean revisados y actualizados de acuerdo con las funciones asignadas al personal del Sistema y la transformación tecnológica ocurrida en el Sistema. **[Hallazgo 4-a.1) y 5), b. y c.]**
6. Establecer normas y procedimientos para la creación, la aprobación y la modificación de la reglamentación interna del Sistema, y establecer medidas para que no ocurran las situaciones comentadas en el **Hallazgo 4-a.2) y 3)**.
7. Ejercer una supervisión eficaz sobre la Directora de Recursos Humanos para asegurarse de que:
- a. El Centro para el Desarrollo Profesional efectúe un estudio sobre las necesidades de adiestramientos para los funcionarios y los empleados del Sistema, y ofrezca adiestramientos sobre las normas y los procedimientos relacionados con el uso y la seguridad de los sistemas de información. **[Hallazgo 8]**
  - b. Efectúe las gestiones necesarias para reestructurar y actualizar el sistema de evaluación de desempeño del personal del Sistema, y se asegure de que estas evaluaciones se realicen periódicamente. **[Hallazgo 9]**

### **CARTAS A LA GERENCIA**

Las situaciones comentadas en los **hallazgos del 1 al 9**, incluidos en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**, se informaron al Sr. Harold González Rosado, entonces Director Ejecutivo, en carta de nuestros auditores del 24 de noviembre de 2008.

El borrador de los **hallazgos** de este *Informe* se remitió al Sr. Héctor Mayol Kauffmann, Director Ejecutivo, para comentarios, en carta del 21 de septiembre de 2009. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al señor González Rosado, ex Director Ejecutivo, en carta del 9 de octubre de 2009, por correo certificado con acuse de recibo, a una dirección provista por el Sistema.

### COMENTARIOS DE LA GERENCIA

El 23 de diciembre de 2008, el señor González Rosado, entonces Director Ejecutivo, remitió sus comentarios sobre los **hallazgos** incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador del *Informe*.

El 30 de septiembre de 2009, la Subdirectora Ejecutiva del Sistema solicitó una prórroga para remitir los comentarios al borrador de los **hallazgos** de este *Informe*. El 2 de octubre de 2009, le concedimos una prórroga al Director Ejecutivo para remitir sus comentarios hasta el 21 de octubre de 2009. El 14 de octubre de 2009, la Subdirectora Ejecutiva del Sistema solicitó prórroga adicional de 9 días. Ese mismo día le concedimos la prórroga adicional al Director Ejecutivo hasta el 30 de octubre de 2009. El Director Ejecutivo y el Hon. Juan C. Puig Morales, Presidente de la Junta de Síndicos, remitieron sus comentarios al borrador de los **hallazgos** de este *Informe* en carta del 28 de octubre de 2009 (carta del Director Ejecutivo y de la Junta de Síndicos)<sup>1</sup>. Además, el Sr. Edwin Mercado Brignoni, Director de la Oficina de Auditoría Interna, contestó el borrador del **Hallazgo 7** de este *Informe* en carta del 28 de octubre de 2009. Los comentarios de dichos funcionarios fueron considerados en la redacción final de este *Informe*; y se incluyen en la segunda parte de este *Informe*, titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección HALLAZGOS EN LA ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS DE INFORMÁTICA DEL SISTEMA DE RETIRO PARA MAESTROS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO.

---

<sup>1</sup> La carta fue emitida por el Director Ejecutivo y la Secretaria de Actas de la Junta. En la misma se indica que se incluyen los comentarios de la Junta de Síndicos y de la Gerencia del Sistema.

El ex Director Ejecutivo no contestó el borrador de los **hallazgos** de este *Informe* que le fuera remitido para comentarios en nuestra carta del 9 de octubre de 2009, y en carta de seguimiento del 27 de octubre de 2009.

### AGRADECIMIENTO

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

Por: *Oficina del Contralor  
Patricio J. G. G.*

## 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.

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, las irregularidades o los 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 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 ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS DE INFORMÁTICA DEL SISTEMA DE RETIRO PARA MAESTROS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO, de forma objetiva y conforme a las normas de nuestra Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, éste prevalece y se añade al final del mismo la siguiente aseveración: Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

#### HALLAZGOS EN LA ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS DE INFORMÁTICA DEL SISTEMA DE RETIRO PARA MAESTROS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO

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

##### **Hallazgo 1 - Falta de un Informe de Avalúo de Riesgos**

- 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 con 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 21 de septiembre de 2007, en el Sistema no se había realizado un avalúo de riesgos sobre los sistemas de información. A dicha fecha, en el Sistema sólo se había efectuado una evaluación de los procesos relacionados con el procesamiento de la información de nóminas, provista por los departamentos de Hacienda y de Educación, y de la seguridad de la infraestructura tecnológica utilizada en dichos procesos.

En la *Norma Núm. SRM-ADSI-003-07* incluida en el *Manual de Normas y Procedimientos de los Sistemas de Información*, se establece, entre otras cosas, que la ADSI llevará un inventario de activos de sistemas de información que incluya el equipo, los programas y los datos. Los activos serán clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones, y los datos electrónicos serán clasificados de acuerdo con el nivel de confidencialidad para establecer lo que se va a proteger. Además, se identificarán todo tipo de amenazas que puedan afectar la continuidad de las operaciones.

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 activos de sistemas de información que incluya el equipo, los programas y los datos. Todos los activos deberán ser clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.
- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido a los datos, entre otras), junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

Las mejores prácticas en el campo de la tecnología sugieren que se deben establecer normas y procedimientos escritos para garantizar la integridad, la confidencialidad y la disponibilidad de los sistemas críticos, de modo que se garantice la continuidad de las operaciones en la eventualidad de que sucesos inesperados ocurran. Esto implica, entre otras cosas, que la entidad desarrolle e implante un programa de avalúo y administración de riesgos para identificar los activos y los recursos que se deben proteger, y clasificar los mismos en términos de criticidad y sensibilidad. Luego de la identificación y la clasificación de los activos y los recursos, se identifican los elementos de riesgo que podrían afectar los mismos, específicamente los sistemas de información, para entonces determinar la probabilidad de que las amenazas o los eventos ocurran y el impacto que tendrían en las operaciones.

La situación comentada impide al Sistema evaluar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de éste, y considerar cómo protegerlos para reducir los riesgos de daños materiales y pérdida de información. Además, impide el desarrollo de un *Plan de Continuidad de Negocios* donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones del Sistema, en caso de que surja alguna eventualidad. **[Véase el Hallazgo 3]**

La situación comentada se atribuye a que en el Sistema no se había completado el proceso de evaluación de propuestas para contratar una firma especializada en la preparación de informes de avalúo de riesgos sobre los sistemas de información.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

En los pasados años el Sistema de Retiro para Maestros ha tomado importantes pasos para fortalecer las operaciones y mejorar los servicios a los participantes mediante soluciones tecnológicas. Cada proyecto encausado ha integrado consideraciones propias del manejo de riesgos. El Sistema aplica prácticas alternas durante situaciones que afectan la normalidad de las

operaciones que le han permitido dar continuidad a los servicios a los participantes. El Sistema contrató los servicios de una compañía especializada y actualmente cuenta con un informe de avalúo de riesgos. [sic]

**Véanse las recomendaciones 1 y 3.**

### **Hallazgo 2 - Falta de un Plan de Seguridad**

- a. El 5 de diciembre de 2007, el Sistema nos proveyó la *Certificación Plan de Seguridad del Área de Seguridad de Sistemas de Información*, la cual incluía una lista general de las medidas que había implantado para aumentar la seguridad de sus sistemas de información. Sin embargo, a esa fecha el Sistema no tenía un *Plan de Seguridad* aprobado por el Director Ejecutivo que incluyera, entre otras cosas, disposiciones en cuanto a:
- La documentación de la validación de las normas de seguridad<sup>2</sup>
  - La evidencia de un análisis de riesgo actualizado, que sea base del *Plan*
  - La responsabilidad de la gerencia, los oficiales de seguridad y de los demás componentes de la unidad, tales como: los dueños y los usuarios de los recursos de información, el personal administrativo de la ADSI, el personal a cargo del procesamiento de los datos y los administradores de seguridad, entre otros
  - 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 que permita mantener los conocimientos actualizados
  - La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros).

---

<sup>2</sup> 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*.

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. 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 actualicen los conocimientos sobre los aspectos de seguridad de sus áreas.
- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que les apliquen.

Las mejores prácticas en el campo de tecnología de información sugieren que las entidades deben mantener un plan escrito que describa claramente el programa de seguridad y los procedimientos relacionados con éste. Los mismos deben considerar los sistemas y las facilidades principales, e identificar los deberes de los dueños y de los usuarios de los sistemas de información de la entidad, y de los empleados responsables de velar por la seguridad de dichos sistemas.

La falta de un *Plan de Seguridad* podría provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos. Además, de ocurrir una emergencia, la falta de dicho *Plan* y de los correspondientes adiestramientos y simulacros podría dar lugar a:

- Pérdidas de vidas humanas

- Daños a los equipos de sistemas de información, así como la pérdida de datos importantes
- Atrasos en el proceso de reconstrucción de datos y programas, y en el restablecimiento y la continuidad de las operaciones normales y otras situaciones adversas.

La situación comentada se atribuye a que el Director Ejecutivo no había impartido las directrices para que los oficiales de seguridad prepararan un *Plan de Seguridad*, basado en un avalúo de riesgos de los sistemas de información, y para la implantación y la actualización continua del mismo, según lo establecido en la *Carta Circular Núm. 77-05*. Además, los oficiales de seguridad no se percataron de la importancia de documentar, de forma detallada, las estrategias de seguridad implantadas para proteger la información mantenida en los sistemas de información de la entidad gubernamental contra los riesgos y las amenazas que podrían afectar la integridad, la disponibilidad y el uso efectivo de la misma.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

El Sistema de Retiro para Maestros siempre ha estado consciente de la importancia de la seguridad en los sistemas de informática y ha mantenido planes de contingencia para preservar los activos de la Agencia. A la fecha de emisión de este informe, el Sistema tiene ante su consideración un Plan de Seguridad sobre sus sistemas de informática.

**Véanse las recomendaciones 1 y 4.a.**

### **Hallazgo 3 - Falta de un Plan de Continuidad de Negocios**

- a. Al 27 de noviembre de 2007, el Sistema carecía de un *Plan de Continuidad de Negocios* que incluyera los planes específicos, completos y actualizados de la ADSI. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la ADSI en caso de riesgos como:

variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, desastres naturales, entre otros.

Una situación similar se comentó en el informe de auditoría anterior *CPED-93-16*.

En la *Norma Núm. SRM-ADSI-002-07* se establece que el Sistema contará con un *Plan de Contingencias* que se activará para ofrecer los servicios en la Oficina Central y en las oficinas regionales para asegurar la continuidad de las operaciones.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las entidades 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*.

La situación comentada puede propiciar la improvisación, y que en casos de emergencia se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, e interrupciones prolongadas de los servicios ofrecidos a los usuarios del Sistema.

La situación comentada se atribuye a que en el Sistema no se había terminado el proceso para contratar una firma especializada en la preparación del *Avalúo de Riesgos (Véase el Hallazgo 1)* y del *Plan de Continuidad de Negocios*.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

El Sistema de Retiro para Maestros ha mantenido los datos e información crítica en un sistema de resguardo en una localización separada de la Agencia, como medida para proteger la continuidad de las operaciones. El Sistema contrató los servicios de una compañía especializada y actualmente se encuentra en el proceso de implementar un plan de continuidad de negocios más completo en beneficio de los participantes del Sistema. [sic]

**Véanse las recomendaciones 1 y 4.b.**

**Hallazgo 4 - Deficiencias en las políticas, las normas y los procedimientos relacionados con la administración, la seguridad y el uso de los sistemas computadorizados del Sistema, y falta de normas y procedimientos para reglamentar varios procesos de la ADSI**

a. Al 25 de septiembre de 2007, el *Manual de Normas y Procedimientos de los Sistemas de Información* incluía lo siguiente:

- *Norma Núm. SRM-ADSI-001-07, Normas para el Control y Seguridad de la Comunicación Electrónica*
- *Norma Núm. SRM-ADSI-002-07, Normas de Resguardo y Recuperación de los Sistemas*
- *Norma Núm. SRM-ADSI-003-07, Normas para la Seguridad de los Sistemas de Información*
- *Procedimiento Autorización Acceso Aplicaciones*
- *Procedimiento Coordinación Recursos Humanos – ADSI Empleados IN-OUT*
- *Procedimiento Desarrollo o Modificación de Aplicaciones y Movida a Producción*
- *Procedimiento Resguardo Base de Datos PRETDB*
- *Procedimiento para Prueba de Recuperación de Resguardo (Backup)*

El examen de estas normas y de estos procedimientos efectuado del 25 de septiembre de 2007 al 28 de marzo de 2008 reveló lo siguiente:

- 1) La *Norma SRM-ADSI-002-07* no había sido revisada para corregir el puesto del personal a cargo de generar los respaldos incrementales en la ADSI. A la fecha de nuestro examen, la *Norma* establecía incorrectamente que el personal de la Sección de Desarrollo de Sistemas debía preparar estos respaldos. Esto, a pesar de que esta función nunca la había realizado el personal de la Sección de Desarrollo de Sistemas, sino que estaba asignada al personal de la Sección de Redes de Comunicación.

- 2) Al 27 de noviembre de 2007, el Director Ejecutivo del Sistema no había aprobado el *Procedimiento Autorización Acceso Aplicaciones*, el *Procedimiento Coordinación Recursos Humanos – ADSI Empleados IN-OUT*, el *Procedimiento Desarrollo o Modificación de Aplicaciones y Moviada a Producción*, el *Procedimiento Resguardo Base de Datos PRETDB* y el *Procedimiento para Prueba de Recuperación de Resguardo (Backup)*. [sic] El 12 de febrero de 2008, se nos proveyeron estos procedimientos aprobados y el examen de estos reveló que:
- a) El *Procedimiento Autorización Acceso Aplicaciones*, el *Procedimiento Coordinación Recursos Humanos – ADSI Empleados IN-OUT*, el *Procedimiento Desarrollo o Modificación de Aplicaciones y Moviada a Producción* y el *Procedimiento para Prueba de Recuperación de Resguardo (Backup)* fueron aprobados con fecha retroactiva del 10 de septiembre de 2007 por el Director Ejecutivo. [sic]
  - b) El *Procedimiento Resguardo Base de Datos PRETDB* había sido aprobado por el Director Ejecutivo, pero no incluía la fecha de aprobación. [sic]
- 3) Los procedimientos no tenían asignado el número control requerido en el *Formulario SRM-ads-393*. Este número era utilizado para identificar de forma oficial la agencia, división y la secuencia numérica asignada a los procedimientos, de acuerdo a la fecha de aprobación de los mismos.
- 4) El *Procedimiento Desarrollo o Modificación de Aplicaciones y Moviada a Producción* no incluía disposiciones en cuanto a:
- La aplicabilidad del procedimiento a los contratistas que ofrecían servicios relacionados con el desarrollo o la modificación de aplicaciones
  - La metodología a seguir para documentar la información sobre los requerimientos del solicitante que era recopilada por los desarrolladores

- Los procedimientos a seguir para conceder a los desarrolladores la copia del código fuente de la aplicación que debía modificar
  - Los criterios a ser utilizados para el diseño y la documentación de las pruebas efectuadas por el usuario antes de la aceptación final de la aplicación
  - El uso de la *Hoja de Migración* para documentar la solicitud y autorizar la instalación de la aplicación en ambiente de desarrollo, prueba o producción, según corresponda
  - La intervención del Oficial Principal de Informática en el proceso de aceptación de la aplicación y del desarrollador a cargo de la documentación para recibir y controlar la documentación preparada por el desarrollador.
- 5) El *Procedimiento Desarrollo o Modificación de Aplicaciones y Movida a Producción* requería que el usuario, el Oficial de Seguridad de Informática y el Supervisor de Desarrollo de Sistemas utilizaran el formulario *Hoja de Aceptación de Aplicación (SRM-ads-i-012)* para que certificaran que el sistema operaba de acuerdo a las especificaciones, que la aplicación cumplía con todos los requisitos de seguridad establecidos y que había sido transferida a ambiente de producción. Además, requería que el Especialista de Sistemas Operativos de Informática informara por escrito al Supervisor de Desarrollo de Sistemas que la aplicación había sido instalada en el servidor de producción. El examen del formulario *SRM-ads-i-012* reveló que éste no proveía para que el Especialista de Sistemas Operativos de Informática y el Supervisor de Desarrollo de Sistemas de Informática certificaran su intervención en el proceso de desarrollo o modificación de la aplicación, según correspondiera.

Una situación similar se comentó en el informe de auditoría anterior *CPED-93-16*.

b. El 5 de septiembre de 2007, el Director Ejecutivo del Sistema aprobó la *Orden Administrativa Núm. 2007-13, Política sobre el Uso de Servicios y Acceso a las Aplicaciones en el Área de Administración y Dirección de los Sistemas de Informática*. El examen de la *Orden Administrativa* reveló lo siguiente:

1) La *Orden Administrativa* hacía referencia a las disposiciones incluidas en la *Norma Núm. SRM-ADSI-001-07*. Esto, a pesar de que la referida norma fue aprobada el 10 de septiembre de 2007, luego de la *Orden Administrativa*. Además, en el Inciso IV de la *Orden Administrativa* se citaban tres disposiciones que no fueron incluidas en la referida *Norma*. Las disposiciones citadas erróneamente eran las siguientes:

- Cada Supervisor será responsable de solicitar asignación o cancelación de acceso para los funcionarios que estén bajo su supervisión
- Todo usuario al que se le asigne acceso a la red, será responsable del uso de esta herramienta de trabajo
- Todo usuario que cese funciones, será responsable de entregar los documentos que trabajó durante el período que laboró para el Sistema de Retiro para Maestros antes de su último día de trabajo.

2) La *Orden Administrativa* y el *Procedimiento Autorización Acceso Aplicaciones* no establecían procedimientos uniformes para la solicitud y la cancelación de las cuentas de accesos a los sistemas de información.

c. La ADSI implantó un sistema para recibir, procesar y asignar de forma computadorizada las solicitudes de servicio de seguridad, de bases de datos, de redes, de desarrollo de aplicaciones, y de operaciones y control que eran requeridas por los usuarios. Mediante estas solicitudes, los usuarios informaban a la ADSI las situaciones relacionadas con la creación, la modificación o la eliminación de cuentas de acceso, la reparación de equipo, las solicitudes de creación o modificación de las aplicaciones y los problemas con el procesamiento o uso de los sistemas de información, entre otros. Esta información era

utilizada para asignar las tareas al personal de la ADSI que debía evaluar y resolver las situaciones informadas por los usuarios. Al 2 de enero de 2008, el *Procedimiento Autorización Acceso Aplicaciones* y el *Procedimiento Desarrollo o Modificación de Aplicaciones y Movida a Producción* no habían sido actualizados para requerir a los usuarios el uso de este sistema y derogar el uso de los formularios *Hoja de Peticiones, Observaciones, Fallas y Comentarios (SRM-ads-i-009)* y *Solicitud Asignación o Cancelación de Acceso (SRM-ads-i-003)*, según corresponda. Estos formularios permanecían disponibles a los usuarios en el *Portal Informativo ADSI-SRM*.

d. A la fecha de nuestro examen, no se habían establecido las normas necesarias para reglamentar los siguientes procesos de la ADSI:

- La administración de la seguridad física de la ADSI, el cuarto de máquinas<sup>3</sup> y el equipo de telecomunicaciones
- La producción y la revisión de los registros de eventos de los servidores
- La administración de la seguridad y las funciones de mantenimiento del sistema de administración de base de datos.

Además, no se habían establecido los procedimientos necesarios para reglamentar los siguientes procesos de la ADSI:

- La utilización, el almacenamiento y la disposición de las cintas o medios magnéticos y digitales
- La autorización y la documentación de los cambios de emergencia efectuados a las aplicaciones
- La disposición de los equipos y la eliminación de información grabada en los discos duros

---

<sup>3</sup> El centro de cómputos del Sistema se conocía como el cuarto de máquinas.

- La investigación, la documentación y el manejo de incidentes no esperados
- La documentación de la configuración de los servidores.

En el Artículo 13(b) de la *Ley Núm. 91* se establece que el Director Ejecutivo será responsable del debido funcionamiento del Sistema. En consonancia con esto, y como norma de sana administración, el Sistema debe promulgar las normas o los procedimientos escritos necesarios para el desarrollo y el control de sus actividades operacionales, entre éstas, las relacionadas con la administración, la seguridad y el uso de los sistemas computadorizados.

En la *Orden Administrativa Núm. 2007-13* se indica que para facilitar y fomentar la sana administración la ADSI debe establecer uniformidad en los procesos, tales como: solicitar servicios y conceder o cancelar los accesos a las aplicaciones.

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, como norma de sana administración, se deben establecer por escrito normas, procedimientos y políticas de control interno eficaces que reglamenten las operaciones computadorizadas, estén aprobados por la alta gerencia y sean uniformes entre sí. 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 renuncias o ausencias del personal de mayor experiencia y facilita la labor de adiestramiento.

Las situaciones comentadas podrían 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 ADSI, a los equipos y a la información a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

Las situaciones comentadas obedecen, principalmente, a que el Director Ejecutivo:

- No se había asegurado de que las normas y los procedimientos aprobados fueran revisados y actualizados de acuerdo con las funciones asignadas al personal del Sistema y la transformación tecnológica ocurrida en el Sistema. [**Apartados a.1) y 5), b. y c.**]
- No había establecido procedimientos escritos que incluyeran las medidas de control necesarias para la creación e identificación de la reglamentación interna del Sistema. [**Apartado a.2) y 3)**]
- No le había requerido al Oficial Principal de Informática de la ADSI que desarrollara y sometiera para su consideración y aprobación las normas y los procedimientos por escrito necesarios para regular los procesos que se indican en los **apartados a.4) y d.**

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

El Sistema de Retiro para Maestros está en un proceso de transformación tecnológica el cual hace necesario atemperar todas las políticas, normas y procedimientos relacionados con la administración. Una vez asentada la transformación organizacional se revisarán todas las políticas, las normas y los procedimientos relacionados con la administración, la seguridad y el uso de los sistemas computadorizados. [*sic*]

**Véanse las recomendaciones 1, 4.c., 5 y 6.**

**Hallazgo 5 - Deficiencias relacionadas con los controles para la preparación, el manejo y el almacenamiento de los respaldos de información, y copias de los manuales de operaciones y de la documentación de las aplicaciones, de los programas y de las bases de datos no mantenidas en instalaciones externas de la ADSI**

- a. Al 28 de marzo de 2008, el personal de la Sección de Operaciones y Control era responsable de preparar los respaldos de la información mantenida en los servidores, que incluían las aplicaciones de Préstamos y Retiro, y el Especialista en Microcomputadoras y Redes de Comunicación era responsable de preparar los respaldos de la información mantenida en los otros servidores de la ADSI. La información sobre los medios magnéticos

utilizados para preparar los respaldos de información era registrada manualmente en el sistema *Tapesys*.

A partir del 14 de marzo de 2008, el Sistema contaba con los servicios de acarreo de cintas y de arrendamiento de gabinetes de una compañía para salvaguardar los respaldos de información. En estos gabinetes se mantenían los respaldos que eran producidos por la ADSI y algunos documentos de carácter legal del Sistema.

El examen de los controles establecidos por la ADSI para la preparación, el manejo y el almacenamiento de los respaldos de información reveló las siguientes deficiencias:

- 1) En una inspección realizada el 28 de marzo de 2008 sobre la información incluida manualmente en las etiquetas utilizadas para identificar los respaldos de información observamos que los que permanecían en los gabinetes ubicados en la ADSI y que habían sido preparados por el Especialista en Microcomputadoras y Redes de Comunicación, no incluían en su etiqueta la siguiente información:
  - La descripción clara de los archivos respaldados
  - La identificación de la procedencia de los archivos
  - El tamaño del respaldo
  - El lugar asignado para su almacenamiento.
- 2) Al 14 de marzo de 2008, la ADSI carecía de un registro de los respaldos de información que permitiera mantener el control de los medios magnéticos almacenados en ésta y de los enviados al centro de almacenamiento externo. Además, no se mantenían hojas de trámite que incluyeran información sobre las transferencias de los medios magnéticos al centro de almacenamiento externo y la devolución de éstos a la ADSI.

En la *Norma Núm. SRM-ADSI-002-07* se establece que todas las copias de respaldos tienen que estar claramente etiquetadas con la siguiente información: equipo al que pertenece, fecha y hora de ejecución, frecuencia (año fiscal mensual, semanal, diario), número de

secuencia o lote al que pertenece, tipo de respaldo (completo, diferencial o acumulativo), identificación de los cartuchos que integran el respaldo de la aplicación o sistema y el lugar asignado para el almacenamiento. Además, se establece que el personal de Seguridad para Informática hará una revisión periódica del registro de los respaldos y certificará que se cumpla en tiempo y forma. Esto implica que para poder revisar el registro de respaldos el personal de Seguridad debe asegurarse de que el personal a cargo de la preparación de los respaldos mantenga dicho registro.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las agencias deben establecer controles adecuados en sus sistemas de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Además, se establece que deberán existir procedimientos para tener y mantener una copia de respaldo (*backup*) recurrente de la información y de los programas de aplicación y de sistema esenciales e importantes para la agencia. En consonancia con dicha política pública, es necesario, entre otras cosas, mantener un inventario detallado de las cintas de respaldos para facilitar su localización y que permita, además, documentar el cumplimiento de las normas y los procedimientos establecidos. Las cintas o los cartuchos deben estar rotulados con la información que permita su pronta localización.

Las situaciones comentadas privan al Sistema de mantener un control adecuado de las cintas de respaldos, lo que podría afectar la continuidad de las operaciones debido a la pérdida de información importante, con los consiguientes efectos adversos.

Las situaciones comentadas se debían a que el Oficial Principal de Informática no se había asegurado de establecer los controles necesarios para la protección de los respaldos.

- b. El Sistema no mantenía copias de los manuales de operaciones de los sistemas de información y la documentación de las aplicaciones, de los programas y de las bases de datos en un lugar seguro fuera de los predios de ésta.

Como norma de sana administración y de control interno, se requiere que las entidades gubernamentales mantengan copias actualizadas de los manuales de operación de los

sistemas de información y de la documentación de las aplicaciones, de los programas y de las bases de datos, en un lugar seguro fuera del edificio donde se ubica el centro. Esto es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado.

La situación comentada podría afectar la continuidad de las operaciones normales de la ADSI si ocurriera alguna eventualidad que afectara las instalaciones de ésta y destruyera toda la documentación y los manuales que allí se almacenan. Además, el Sistema no tendría acceso para iniciar el proceso de reconstrucción de archivos y programas, y el restablecimiento y la continuidad de las operaciones normales de los sistemas de información en un tiempo razonable.

La situación comentada se debía a que el Oficial Principal de Informática no se había percatado de la importancia de mantener copia de la documentación mencionada en un lugar seguro fuera de los predios del Sistema.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

El Sistema de Retiro para Maestros ha mantenido los datos e información crítica en un sistema de resguardo en una localización separada de la Agencia, como medida para proveer la continuidad de las operaciones en casos de emergencia. El Sistema ha tomado acciones dirigidas a actualizar los sistemas como parte de los procesos encaminados a mejorar la calidad de los sistemas de resguardo. [sic]

**Véanse las recomendaciones 1 y de la 4.d. a la f.**

#### **Hallazgo 6 - Atrasos en la revisión de los informes de operaciones diarias**

- a. La Sección de Operaciones y Control de la ADSI utilizaba el formulario *Informe de Operaciones Diarias* para documentar, entre otras cosas, la revisión de las baterías, del sistema operativo, del sistema de base de datos, de la temperatura y de la humedad, y para registrar los respaldos efectuados y los problemas ocurridos durante el procesamiento y la actualización de los datos en cada turno de los operadores. Este *Informe* requería la firma

del Operador, del Supervisor de Operaciones de Sistemas de Informática, del Oficial de Seguridad de Sistemas de Informática, del Director Auxiliar y del Director Asociado de Sistemas de Informática para evidenciar la revisión realizada a éstos. El examen realizado de la revisión de estos funcionarios y empleados de los 30 *informes de Operaciones Diarias*, preparados del 8 de enero al 22 de febrero de 2008 por el personal de la Sección de Operaciones y Control de la ADSI, reveló lo siguiente:

- 1) Doce *informes* (40 por ciento) fueron firmados por el Supervisor de Operaciones de Sistemas de Informática de 1 a 7 días laborables posteriores a la preparación de los mismos. Un *Informe* no tenía la firma de éste.
- 2) Veinticinco *informes* (83 por ciento) fueron firmados por el Oficial de Seguridad de Sistemas de Informática de 1 a 11 días laborables posteriores a la preparación de los mismos. Dos *informes* no tenían la firma de éste, del Director Auxiliar ni del Director Asociado de Sistemas de Informática.

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 revisen los informes sobre las operaciones diarias.

La situación comentada podría provocar que el personal a cargo de las operaciones y de la seguridad de los sistemas computadorizados no identifique y actúe oportunamente para corregir las situaciones que pueden afectar el funcionamiento de los sistemas computadorizados.

La situación comentada se debía a que el Oficial Principal de Informática no se había asegurado de que dichos funcionarios revisaran diariamente los *informes de Operaciones Diarias*.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

[...] Como parte de las medidas establecidas para evitar retrasos en la actualización de los registros, se impartieron instrucciones escritas al personal sobre el proceso para la revisión de los informes de operaciones diarias. Además se ha designado personal para validar y dar seguimiento al cumplimiento de las políticas. [sic]

**Véanse las recomendaciones 1 y 4.g.**

**Hallazgo 7 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información**

- a. El Sistema cuenta con una Oficina de Auditoría Interna, la cual responde directamente a la Junta de Síndicos. Dicha Oficina tiene la función principal de realizar auditorías para examinar y evaluar las operaciones del Sistema. Al 19 de septiembre de 2007, la Oficina de Auditoría Interna del Sistema no había efectuado auditorías sobre los procedimientos, los controles y el funcionamiento de sus sistemas de información computadorizados.

En la Sección 2110 de las *Normas para el Ejercicio Profesional de la Auditoría Interna*, emitidas por el Instituto de Auditores Internos, 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.

En la Sección 2110.A2 de dichas *Normas* se establece, además, 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 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 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. Además, existe la posibilidad de que en los sistemas de información no se incluyan los controles básicos necesarios para evitar incurrir en errores, irregularidades y otras situaciones adversas.

Esta situación se debía a que el Director Ejecutivo le había requerido a la Oficina de Auditoría Interna que enfocara sus esfuerzos en aspectos relacionados con el Área de Préstamos.

El Director de la Oficina de Auditoría Interna del Sistema, en la carta que nos envió informó, entre otras cosas, lo siguiente:

La Oficina de Auditoría Interna ha comenzado un proceso de adiestramiento de sus recursos internos y en el Plan de Trabajo para el año fiscal 2009-2010 se ha incluido la intervención al Área de Administración y Dirección de Sistemas de Informática. Además, hemos asignado a un Auditor Certificado en Sistemas de Informática de la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura para el seguimiento a los hallazgos del informe en borrador y final de la Oficina del Contralor de Puerto Rico. [sic]

**Véase la Recomendación 2.**

**Hallazgo 8 - Falta de adiestramientos sobre las normas y los procedimientos para el uso y la seguridad de los sistemas de información**

- a. El examen del registro de adiestramientos ofrecidos del 1 de enero de 2005 al 31 de diciembre de 2007 por el Centro para el Desarrollo Profesional del Sistema reveló que a los empleados no se les habían ofrecido adiestramientos sobre el uso y la seguridad de los sistemas de información, y las normas y los procedimientos incluidos en el *Manual*. Estos

adiestramientos son necesarios para asegurarse de que el personal esté capacitado para ejercer sus funciones y cumplir con sus responsabilidades relacionadas con la seguridad de los sistemas de información.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece, entre otras cosas, que la entidad gubernamental es responsable 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 de los beneficios correspondientes.
- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que les apliquen.

La situación comentada ocasionaba que los usuarios de los sistemas de información del Sistema desconocieran la *Norma Núm. SRM-ADSI-001-00*. En un examen realizado se determinó que 23 (58 por ciento) de 40 usuarios entrevistados desconocían dicha *Norma*. La falta de conocimiento de las normas de seguridad relacionadas con los sistemas de información ocasiona el incumplimiento de las mismas, con los consiguientes efectos adversos en cuanto a la protección de la información y del equipo. Esto, a su vez, podría afectar la integridad, la disponibilidad y la confiabilidad de la información manejada por los usuarios.

La situación comentada se debía, en parte, a que el Director Ejecutivo no le había requerido a la Directora de Recursos Humanos que efectuara estudios sobre las necesidades de adiestramientos para los funcionarios y los empleados del Sistema y, que se asegurara de que el Centro para el Desarrollo Profesional ofreciera adiestramientos sobre las normas y los procedimientos relacionados con el uso y la seguridad de los sistemas de información.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

En el Sistema de Retiro para Maestros existen políticas y órdenes administrativas claras y precisas para el uso y manejo de equipos y aplicaciones. Estas normativas han estado disponibles para todo el personal. Además, el sistema al identificar el usuario requiere la aceptación de las políticas previo al acceso de aplicaciones del Sistema. [sic]

Consideramos las alegaciones de la Secretaria de Actas de la Junta y el Director Ejecutivo, pero determinamos que el **Hallazgo** prevalece.

**Véanse las recomendaciones 1 y 7.a.**

**Hallazgo 9 - Falta de evaluaciones periódicas sobre el desempeño de los empleados de la ADSI**

- a. Al 28 de noviembre de 2007, no se realizaban evaluaciones periódicas sobre la labor efectuada por los empleados de la ADSI. Las evaluaciones periódicas sobre la labor efectuada por los empleados son un instrumento necesario para identificar la necesidad de capacitación y de conocimientos requeridos por el puesto, y para evaluar el cumplimiento de las políticas, las normas y los procedimientos de seguridad, entre otros.

En el Artículo 13(c) de la *Ley Núm. 91* se establece que el Director Ejecutivo adoptará los reglamentos necesarios para el establecimiento de un sistema de personal, aprobado por la Junta de Síndicos. Esto implica que, como parte de las disposiciones reglamentarias de personal, se establezca un sistema para la evaluación periódica del desempeño a los fines de determinar si los empleados satisfacen los criterios de productividad, eficiencia, orden y disciplina que deben prevalecer en el servicio público. Además, las evaluaciones sobre el desempeño permiten identificar las necesidades de capacitación de los empleados.

La situación comentada priva al Sistema de información sobre las ejecutorias de sus empleados. Esto es importante para conocer las tareas en que el empleado debe mejorar y en las que sobresale con el objetivo de ofrecerle adiestramiento o compensarle por las labores realizadas.

La situación comentada se debía, en parte, a que el Sistema no había terminado el proceso de actualización de los informes de funciones de sus empleados, los cuales eran necesarios para reestructurar el sistema de evaluación de desempeño y actualizarlo con los cambios ocasionados por el proceso de mecanización y reorganización del Sistema.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron, entre otras cosas, lo siguiente:

En la actualidad el Sistema de Retiro para Maestros cuenta con un Sistema de Evaluación de Desempeño. El Sistema ha estado en un proceso intenso de evolución institucional asociado a la mecanización, proyectos especiales y reorganización de oficinas regionales a sucursales. Ello ha requerido reasignación de tareas, adiestramientos, consolidación de oficinas, eliminación de puestos y múltiples transacciones de personal. Ante todos los cambios experimentados, era impráctico realizar evaluaciones de desempeño sobre puestos y tareas que estaban en un proceso de evolución. Sin embargo, gran parte de los procesos de transformación institucional han concluido o se encuentran en etapas finales, por lo que se actualizan las hojas de deberes de los empleados y se contempla desarrollar un nuevo instrumento de medición de desempeño. [sic]

Consideramos las alegaciones de la Secretaria de Actas de la Junta y el Director Ejecutivo, pero determinamos que el **Hallazgo** prevalece.

**Véanse las recomendaciones 1 y 7.b.**

**ANEJO 1**

**SISTEMA DE RETIRO PARA MAESTROS  
DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO  
ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS DE INFORMÁTICA  
MIEMBROS DE LA JUNTA DE SÍNDICOS QUE ACTUARON  
DURANTE EL PERÍODO AUDITADO<sup>4</sup>**

| <b>NOMBRE</b>                    | <b>CARGO O PUESTO</b>   | <b>PERÍODO</b> |              |
|----------------------------------|---|----------------|--------------|
|                                  |   | <b>DESDE</b>   | <b>HASTA</b> |
| Lcdo. Ángel A. Ortiz García, CPA | Presidente  | 30 m. 08       | 31 oct. 08   |
| CPA José Guillermo Dávila Matos  | "   | 1 en. 08       | 29 m. 08     |
| CPA Rolando Rivera Silva         | "   | 10 sep. 07     | 31 dic. 07   |
| Sr. Jorge Irizarry Herrans       | Miembro   | 10 sep. 07     | 31 oct. 08   |
| Dr. Rafael Aragunde Torres       | "   | 10 sep. 07     | 31 oct. 08   |
| Prof. William Ortiz Ramírez      | Miembro Representante de la<br>Organización Magisterial<br>Asociación de Maestros de<br>Puerto Rico | 10 sep. 07     | 31 oct. 08   |
| Prof. Astrid J. Llanos Algarín   | Miembro Representante de los<br>Maestros Activos  | 10 sep. 07     | 31 oct. 08   |
| Prof. Jesús López Colón          | Miembro Representante de los<br>Maestros Jubilados  | 10 sep. 07     | 31 oct. 08   |
| Prof. María C. Martínez Torres   | Miembro Representante de los<br>Maestros Jubilados  | 10 sep. 07     | 31 oct. 08   |
| CPA María Medina Rullán          | Miembro Representante del<br>Interés Público  | 10 sep. 07     | 31 oct. 08   |

<sup>4</sup> Del 10 de septiembre de 2007 al 16 de marzo de 2008 los cargos de Vicepresidente y Tesorero estuvieron vacantes. Además, durante dicho período no hubo miembros representantes de la entidad que representa la unidad apropiada bajo la *Ley Núm. 45 del 25 de febrero de 1998*.

**ANEJO 2**

**SISTEMA DE RETIRO PARA MAESTROS  
DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO  
ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS DE INFORMÁTICA  
FUNCIONARIOS PRINCIPALES QUE ACTUARON  
DURANTE EL PERÍODO AUDITADO**

| <b>NOMBRE</b>                          | <b>CARGO O PUESTO</b>  | <b>PERÍODO</b> |              |
|--|--|----------------|--------------|
|  |  | <b>DESDE</b>   | <b>HASTA</b> |
| Sr. Harold González Rosado             | Director Ejecutivo   | 10 sep. 07     | 31 oct. 08   |
| CPA José Reyes Portalatín              | Subdirector Ejecutivo  | 10 sep. 07     | 31 oct. 08   |
| Sr. Andrés Ramón Miró                  | "  | 1 abr. 08      | 31 ag. 08    |
| Sr. José Matos Miranda                 | Director Auxiliar de Auditoría                               | 10 sep. 07     | 31 oct. 08   |
| Sra. María Vázquez Fontán              | Directora de Recursos Humanos                                | 10 sep. 07     | 31 oct. 08   |
| Lcdo. Francisco del Castillo<br>Orozco | Director de Asesoramiento Legal                              | 10 sep. 07     | 31 oct. 08   |
| Sra. Irma García Hernández             | Directora del Área de Servicios<br>Generales                 | 10 sep. 07     | 31 oct. 08   |
| Sr. Víctor Rivera Aquino               | Oficial Principal de Informática <sup>5</sup>                | 1 oct. 08      | 31 oct. 08   |
| Sr. José Figueroa Corcino              | "  | 17 mar. 08     | 31 ag. 08    |
| Sr. Víctor Rivera Aquino               | Director Asociado de Sistemas de<br>Informática <sup>6</sup> | 10 sep. 07     | 30 sep. 08   |

<sup>5</sup> El puesto de Oficial Principal de Informática fue creado el 17 de marzo de 2008. Este puesto estuvo vacante del 1 al 30 de septiembre de 2008.

<sup>6</sup> Del 1 al 31 de octubre de 2008 el puesto de Director Asociado de Sistemas de Informática estuvo vacante.