Secretaría

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
W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

- [ ] Hacienda
- [ ] Gobierno
- [ ] Seguridad Pública y Judicatura
- [ ] Salud
- [x] Educación y Asuntos de la Familia
- [ ] Desarrollo Eonómico 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 de la Montaña
- [ ] Asuntos de la Mujer
- [ ] Asuntos Internos
- [ ] Reglas y Calendario
- [ ] Asuntos Federales
- [ ] 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

Iniciales

Oficina del Presidente

Katherine Erazo
Chief of Staff

Fecha 4 de abril 2011

Referido a Manuel Torres

Para su información
Evaluar y recomendar
Para trabajar y contestar directamente
✓ Dar cuenta al cuerpo
Para otorgar contrato
Para nombramiento
Autorizado

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

RECIBIDO SECRETARIA
SENADO DE P.R.
2011 APR -6 AM 9:16

4 de abril de 2011

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-11-02* 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 30 de marzo 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
PRESIDENTE SENADO
THOMAS RIVERA SCHATZ
2011 APR -4 AM 10:52

PO BOX 366069 SAN JUAN PUERTO RICO 00936-6069
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136
TEL. (787) 754-3030 FAX (787) 751-6768
E-MAIL: ocpr@ocpr.gov.pr INTERNET: http://www.ocpr.gov.pr

PO-14264

INFORME DE AUDITORÍA TI-11-02

30 de marzo de 2011

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

-f0-4264

CONTENIDO

Página

INFORMACIÓN SOBRE LA UNIDAD AUDITADA 4

RESPONSABILIDAD DE LA GERENCIA 6

ALCANCE Y METODOLOGÍA 7

OPINIÓN 7

RECOMENDACIONES 8

AL PRESIDENTE DE LA JUNTA DE SÍNDICOS 8

AL DIRECTOR EJECUTIVO DEL SISTEMA DE RETIRO PARA MAESTROS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO 8

CARTAS A LA GERENCIA 9

COMENTARIOS DE LA GERENCIA 10

AGRADECIMIENTO 11

RELACIÓN DETALLADA DE HALLAZGOS 12

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO 12

HALLAZGOS EN LA ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS DE INFORMÁTICA DEL SISTEMA DE RETIRO PARA MAESTROS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO 13

1 - Falta de controles físicos y ambientales en la ADSI 13

2 - Deficiencias relacionadas con la configuración y la revisión de las políticas de auditoría del servidor principal del SRM 18

3 - Deficiencias relacionadas con la documentación de las solicitudes para la creación y la cancelación de cuentas de acceso, y otras deficiencias relacionadas con el control y el mantenimiento de las cuentas de acceso 20

ANEJO 1 - MIEMBROS DE LA JUNTA DE SÍNDICOS QUE ACTUARON DURANTE EL PERÍODO AUDITADO 27

ANEJO 2 - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO 28

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

30 de marzo 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 Administración y Dirección de Sistemas de Informática (ADSI) del Sistema de Retiro para Maestros del Estado Libre Asociado de Puerto Rico (SRM) 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 segundo informe y contiene el resultado de nuestro examen de los controles de acceso físico y lógico a los sistemas de información del SRM. El primer informe se emitió el 23 de febrero de 2010, 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 de 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 (*Informe de Auditoría TI-10-13*).

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El SRM 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 SRM 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[1] el recibo de los beneficios que le corresponden en un tiempo justo. Además, mediante la *Ley Núm. 91*, se transfirieron al SRM 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 SRM todas las deudas, las obligaciones y las responsabilidades de dicha Junta.

El SRM 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 SRM 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,*

[1] Los participantes, denominados miembros del SRM en la *Ley Núm. 91*, incluyen los empleados miembros del SRM, los maestros activos, los maestros que ocupan puestos en el SRM, los maestros pensionados, los maestros acogidos a beneficios que pasen a ocupar puestos administrativos, los maestros que trabajen en la Asociación de Maestros de Puerto Rico, en la Cooperativa de Crédito de los Maestros de Puerto Rico, en la Federación de Maestros de Puerto Rico y demás organizaciones magisteriales o de servicio debidamente reconocidas por el Departamento de Educación y los miembros de la Asamblea Legislativa del Estado Libre Asociado de Puerto Rico, siempre que posean un certificado válido para ejercer como maestros.

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 SRM.

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

El SRM 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 SRM cuenta con una Oficina de Auditoría Interna que le responde directamente a la Junta.

La ADSI cuenta con los siguientes puestos: 1 Oficial Principal de Informática, 1 Director Asociado de Sistemas de Informática, 1 Director Auxiliar de Sistemas de Informática, 2 oficiales de Seguridad de Sistemas de Informática, 1 Oficial de Sistemas y Procedimientos, 1 Analista de Sistemas y Procedimientos, 1 Especialista en Microcomputadoras y Red de Comunicaciones, 1 Especialista en Sistemas Operativos de Informática, 1 Supervisor de Operaciones de Sistemas de Informática, 3 operadores Principales de Unidad Central de Sistemas de Informática, 3 operadores de Unidad Central de Sistemas de Informática, 1 Estadística, 4 desarrolladores Principales de Sistemas de Informática, 6 desarrolladores de Sistemas de Informática, 1 Asistente de Servicios de Oficina, y 1 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 SRM provienen principalmente de las aportaciones patronales e individuales, los intereses sobre préstamos y los

ingresos provenientes de las inversiones. Además, el SRM 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 SRM 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.

El SRM 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 de acceso físico y lógico a los sistemas de información del SRM no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 3**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

RECOMENDACIONES

AL PRESIDENTE DE LA JUNTA DE SÍNDICOS

1. Ver que el Director Ejecutivo del SRM cumpla con las **recomendaciones 2 y 3** de este *Informe*. **[Hallazgos del 1 al 3]**

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

2. Ejercer una supervisión eficaz sobre el Oficial Principal de Informática de la ADSI para asegurarse de que:

   a. Los oficiales de Seguridad de Sistemas de Informática:

      1) Establezcan las medidas necesarias para corregir las deficiencias de controles físicos y ambientales, 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 (Norma Núm. SRM-ADSI-003-07)*, aprobada el 10 de septiembre de 2007 por el Director Ejecutivo del SRM e incluida en el *Manual de Normas y Procedimientos de los Sistemas de Información (Manual)*; en la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada; y en las mejores prácticas en el campo de la tecnología de información. **[Hallazgo 1]**

2) Evalúen las opciones de seguridad disponibles en los sistemas de seguridad de los sistemas operativos, establezcan las medidas necesarias para mitigar los riesgos y las amenazas existentes, y examinen periódicamente los registros de seguridad. **[Hallazgo 2]**

3) Establezcan controles adecuados para la creación y la cancelación de cuentas de acceso para que los mismos sean autorizados de acuerdo con las funciones realizadas por los usuarios. **[Hallazgo del 3-a. al c.]**

4) Se aseguren de que, cuando sea indispensable otorgar privilegios de administrador al técnico de operaciones, se otorguen temporalmente para efectuar tareas específicas bajo estricta supervisión. **[Hallazgo 3-d.]**

b. Revise, y remita para su aprobación las políticas, las normas y los procedimientos sobre el uso de los sistemas de información para que incluyan directrices actualizadas y uniformes con los nuevos procesos y tecnologías utilizados por el SRM para la solicitud, la modificación y la cancelación de las cuentas de acceso a los sistemas de información. **[Hallazgo 3-a.]**

3. Ejercer una supervisión eficaz sobre la Directora de Servicios Generales para asegurarse de que el Supervisor de Almacén mantenga un control adecuado de las llaves de la ADSI asignadas y, actualizado el registro correspondiente. **[Hallazgo 1-a.2)a)]**

CARTAS A LA GERENCIA

Las situaciones comentadas en los **hallazgos del 1 al 3**, 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 16 de junio de 2010. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* al señor González Rosado, ex Director Ejecutivo, en carta de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por el SRM.

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 Director Ejecutivo y el Sr. Juan C. Puig Morales, entonces Presidente de la Junta de Síndicos, remitieron sus comentarios al borrador de los **hallazgos** de este *Informe* en carta del 25 de agosto de 2010 (carta del Director Ejecutivo y de la Junta de Síndicos)[2]. 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 de HALLAZGOS EN LA ADMINISTRACIÓN Y DIRECCIÓN DE SISTEMAS DE INFORMÁTICA DEL SISTEMA DE RETIRO PARA MAESTROS DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO.

El ex Director Ejecutivo no contestó el borrador de los **hallazgos** de este *Informe* que le fuera remitido para comentarios en nuestra carta del 16 de junio de 2010, y en carta de seguimiento del 2 de julio de 2010.

---

[2] La carta fue emitida por el Director Ejecutivo y el Secretario 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 SRM.

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yesmín M. Valdivieso

RELACIÓN DETALLADA DE HALLAZGOS

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO

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

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

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

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

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

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

En la sección sobre los **COMENTARIOS DE LA GERENCIA** se indica si el funcionario principal y los ex funcionarios de la unidad auditada efectuaron comentarios sobre el borrador de los hallazgos del informe, que les envía nuestra Oficina. Dichos comentarios se consideran al revisar el borrador del informe; y se incluyen al final del hallazgo correspondiente en la sección de HALLAZGOS EN 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 controles físicos y ambientales en la ADSI

a. La ADSI se componía de un Cuarto de Máquinas, de la sección Desarrollo de Sistemas, de la Cincoteca[3], y de las oficinas del Oficial Principal de Informática, del Director Asociado de Sistemas de Informática, del Director Auxiliar de Sistemas de Informática, de los dos oficiales de Seguridad de Sistemas de Informática y del Especialista en Microcomputadoras y Red de Comunicaciones. En el Cuarto de Máquinas se mantenían los servidores y los equipos de comunicaciones principales de la red del SRM. La Cincoteca, área donde operaba la Sección de Operaciones y Control, estaba ubicada al lado del Cuarto de Máquinas y en ésta se mantenían las computadoras asignadas al personal de operaciones, la documentación de las operaciones de los sistemas de información computadorizados y las copias de los respaldos de la información mantenida en estos sistemas.

[3] A la fecha de nuestra auditoría, la Cincoteca era conocida como el área de operaciones.

El examen de los controles ambientales[4] y físicos[5] en la ADSI reveló que no se habían establecido las condiciones de seguridad física[6] adecuadas para proteger los sistemas de información computadorizados del SRM, según se indica:

1) Relacionado con los controles ambientales:

a) El Cuarto de Máquinas de la ADSI no contaba con detectores de agua debajo del falso piso.

b) En el falso piso del Cuarto de Máquinas, no se había identificado el área donde estaban instalados los detectores de humo del Cuarto de Máquinas de la ADSI.

c) El acondicionador de aire del Cuarto de Máquinas y el sistema eléctrico del edificio principal del SRM no operaban eficientemente. El examen de los mensajes de advertencias emitidos automáticamente, del 15 al 22 de octubre de 2007, por un programa de monitoreo[7] de las condiciones ambientales y eléctricas del cuarto de máquinas reveló lo siguiente:

- El 22 de octubre de 2007, el programa de monitoreo había emitido 16 mensajes de advertencia sobre alta temperatura. Estos mensajes eran emitidos cuando las temperaturas excedían 90 grados *Fahrenheit* debido a deficiencias en la infraestructura eléctrica que afectaban el funcionamiento del acondicionador de

---

[4] Controles diseñados para proteger las instalaciones y los equipos de eventos inesperados que ocurren naturalmente o son ocasionados por el hombre. Entre éstos, tormentas, erupciones volcánicas, huracanes, tornados, ataques terroristas, vandalismo, descargas eléctricas y fallas de equipo.

[5] Controles diseñados para proteger la organización y sus instalaciones contra accesos no autorizados por medio de sistemas de cerraduras, remoción de discos innecesarios y sistemas de protección del perímetro, entre otros.

[6] Incluye los controles y los procedimientos establecidos para proteger a las personas, la información, los equipos, los sistemas y las instalaciones al utilizar mecanismos de seguridad que incluyen el diseño y la ubicación de las instalaciones, los componentes ambientales, las medidas de respuesta de emergencia, el control de acceso, la detección de intrusos, y la protección contra fuego y pérdida de energía.

[7] El programa de monitoreo enviaba los correos electrónicos de alerta a los dos oficiales de Seguridad de Sistemas de Informática, al Especialista de Microcomputadoras y Redes de Comunicaciones, y al Supervisor de Operaciones y Control.

aire central. La ADSI contaba con siete acondicionadores de aire portátiles que debían ser encendidos por el personal de la Sección de Operaciones y Control cuando el sistema de monitoreo emitía el mensaje de alarma. Éstos dependían de la energía provista por el sistema eléctrico o por la planta diésel del SRM.

- Del 16 al 19 de octubre de 2007, el programa de monitoreo había emitido seis mensajes de activación de la batería. La batería se activaba cuando ocurrían fluctuaciones o fallas de energía eléctrica, y la planta diésel no encendía. En estos casos, el personal de la Sección de Operaciones y Control procedía a apagar los sistemas principales de la ADSI. Este proceso debía ser completado durante los 20 minutos de energía alterna provistos por las baterías.

2) Relacionado con los controles físicos de la ADSI:

a) Al 21 de febrero de 2008, el *Registro de llaves asignadas a empleados y llaves no asignadas*, y los recibos de llaves suministrados para examen por el Supervisor de Almacén del Área de Servicios Generales y el *Registro de personas autorizadas (que tienen llaves) a tener acceso a ADSI* suministrado para examen por la ADSI contenían información incongruente sobre la asignación de llaves al personal de la ADSI[8]. Las llaves que tenían asignadas eran las que se incluían en el *Registro de personas autorizadas (que tienen llaves) a tener acceso a ADSI.*

b) Observamos que la puerta de salida de emergencia de la ADSI había sido clausurada. La única puerta disponible para el desalojo del área en caso de una emergencia era la puerta principal.

En la *Norma Núm. SRM-ADSI-003-07* se establece que las instalaciones de la ADSI tendrán el acceso físico controlado. Solamente podrá acceder el personal que esté debidamente autorizado.

[8] La información incongruente sobre la asignación de llaves al personal de la ADSI se incluyó en el borrador de los **hallazgos** de este *Informe*, remitido al Director Ejecutivo y al ex Director Ejecutivo para comentarios.

En la *Política Núm. TIG-003 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 el acceso a las instalaciones de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas. Esto implica que, para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- Se utilice el equipo y la tecnología adecuados para proteger los sistemas, tales como: detectores de humo, alarmas, sistemas de supresión de incendios, extintores portátiles inspeccionados anualmente, detectores de agua, sistemas de enfriamiento redundante, sistemas alternos de electricidad y cerraduras. Además, deben identificarse las áreas donde están ubicados estos equipos.

- Se mantenga la temperatura y la humedad requeridas para el buen funcionamiento de los equipos.

- Se instalen medios de fuente de energía adecuados que garanticen la operación de los sistemas de información.

- Se controle adecuadamente el acceso de personas ajenas a las operaciones de dichas áreas.

- Se provean salidas alternas que permitan el desalojo del personal en casos de emergencias.

Las situaciones comentadas en el **apartado a.1)** pueden propiciar daños a las instalaciones y a los equipos, y provocar eventos de interrupción de servicios. Esto puede afectar la continuidad de las operaciones de los sistemas de información computadorizados del SRM. Además, pueden aumentar los costos de mantenimiento debido al deterioro prematuro de los equipos.

La situación comentada en el **apartado a.2)a)** puede propiciar que personas no autorizadas y ajenas a la ADSI causen daños al equipo o accedan indebidamente la información mantenida en los sistemas de información. Esto, a su vez, disminuye la confiabilidad de la información computadorizada, aumenta el riesgo de destrucción y divulgación indebida de información, dificulta la adjudicación de responsabilidades a las personas que cometan estos actos, y afecta adversamente el funcionamiento de la red y la continuidad de las operaciones. Además, puede ocasionar la pérdida de equipo computadorizado y de información del SRM.

La situación comentada en el **apartado a.2)b)** puede poner en riesgo la seguridad de los empleados de la ADSI y los recursos sensitivos de los sistemas computadorizados.

Las situaciones comentadas se debían a que el Oficial Principal de Informática no se había asegurado de que los oficiales de Seguridad de Sistemas de Informática establecieran las medidas necesarias para que existieran las condiciones ambientales requeridas para el buen funcionamiento de los sistemas de información, se limitara el acceso a los equipos computadorizados principales, y se implantaran las estrategias de seguridad necesarias para proteger, en situaciones de emergencia, al personal y a los equipos ubicados en la ADSI.

La situación comentada en el **apartado a.2)a)** se debía a que la Directora de Servicios Generales no se había asegurado de que el Supervisor de Almacén estableciera un control adecuado de las copias de las llaves de la ADSI y mantuviera actualizados los registros correspondientes.

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

> El SRM adquirió una herramienta de tecnología y los detectores necesarios para detectar agua debajo del piso falso y se identificaron los detectores de humo del Cuarto de Máquinas de la ADSI. **[Apartado a.1)a) y b)]**
>
> El SRM tomó medidas correctivas para atender las situaciones señaladas en el hallazgo. Entre las medidas tomadas estuvo la reconfiguración y fortalecimiento del sistema de control de temperatura del Cuarto de

Máquinas. Además, se establecieron nuevas líneas de distribución de electricidad, se sustituyó el resguardo de baterías y se reemplazó la planta de generación eléctrica con una de mayor capacidad. [*sic*] **[Apartado a.1)c)]**

El SRM tomó las medidas necesarias para que exista uniformidad entre el Registro del Área de Servicios Generales y los empleados de ADSI que tienen llaves. **[Apartado a.2)a)]**

La ADSI se encuentra en un proceso de restructuración en sus áreas físicas, que tendrá como efecto modificar los accesos. Los accesos se realizarán de acuerdo a las regulaciones establecidas por el Cuerpo de Bomberos de Puerto Rico. **[Apartado a.2)b)]**

Hallazgo 2 - Deficiencias relacionadas con la configuración y la revisión de las políticas de auditoría del servidor principal del SRM

a. El sistema operativo del servidor principal del SRM proveía las opciones para configurar la política de auditoría (*Audit Policy*) que permitían producir registros sobre los eventos relacionados con los accesos a los sistemas de información y los cambios en las políticas de seguridad establecidas. El examen reveló que los oficiales de Seguridad de Sistemas de Informática no revisaban regularmente los registros de auditoría producidos por el sistema operativo. Tampoco habían evaluado la política de auditoría provista por el sistema para determinar la necesidad de activar aquellas opciones que producen registros cuando ocurren los siguientes eventos:

- El acceso a un objeto del *Active Directory* (*Audit directory service access*)
- La conexión o desconexión de una cuenta de acceso a una computadora conectada a la red (*Audit logon events*)
- Los accesos a los archivos, a los cartapacios (*folders*) y a las impresoras (*Audit object access*)
- Los cambios efectuados a las opciones de seguridad, a los privilegios de usuarios y a las políticas de auditoría (*Audit policy change*)
- El uso de los privilegios de los usuarios (*Audit priviledge use*)

- Las acciones ejecutadas por algún programa (*Audit process tracking*)

- El apagado y el reinicio de la computadora, y los eventos que afectan al sistema de seguridad (*Audit system events*).

En la *Norma Núm. SRM-ADSI-003-07* se establece que la ADSI:

- Llevará un sistema de seguridad que proporcionará métodos de monitoreo a las actividades de los usuarios en activos sensitivos que lo ameriten.

- Se encargará de tener los controles necesarios para evitar que, de forma intencionada o accidental, se inicien ataques desde la red interna o de sistemas de información externo.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que la información sea accedida de forma no autorizada y son responsables de desarrollar procedimientos para detectar, informar y responder a incidentes de seguridad, incluidos límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta. Esta norma se instrumenta, en parte, mediante la activación de las opciones para registrar los eventos de seguridad, de las aplicaciones y del sistema, y mediante la revisión continua, por el personal técnico especializado, de los registros computadorizados producidos por los servidores principales.

La situación comentada impide la detección temprana de errores críticos o problemas con los servidores que permitan tomar de inmediato las medidas preventivas y correctivas necesarias. Además, priva a la gerencia de las herramientas necesarias para supervisar eficientemente los trabajos realizados por los usuarios, y detectar el acceso y el uso indebido de los sistemas computadorizados.

La situación comentada se debía a que el Oficial Principal de Informática del SRM no se había asegurado de que los oficiales de Seguridad de Sistemas de Informática:

- Evaluaran las opciones de seguridad disponibles en los sistemas de seguridad de los sistemas operativos

- Activaran las opciones de seguridad necesarias para mitigar los riesgos y las amenazas existentes

- Examinaran periódicamente los registros de seguridad.

En la carta del Director Ejecutivo y de la Junta de Síndicos, éstos nos indicaron lo siguiente: "El SRM ha tomado las medidas para mejorar los sistemas de control sobre los eventos relacionados con los accesos a los sistemas de información".

Hallazgo 3 - Deficiencias relacionadas con la documentación de las solicitudes para la creación y la cancelación de cuentas de acceso, y otras deficiencias relacionadas con el control y el mantenimiento de las cuentas de acceso

a. El SRM contaba con las siguientes órdenes administrativas, normas y procedimientos para la solicitud, la modificación y la cancelación de las cuentas de acceso[9]:

- La *Orden Administrativa 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*, emitida el 5 de septiembre de 2007 por el Director Ejecutivo del SRM, que requería el uso de la *Hoja de Peticiones, Observaciones, Fallas y Comentarios* (*SRM-adsi-009*) y su trámite mediante un correo electrónico dirigido a la cuenta Peticiones de Servicios ADSI.

- La *Norma Núm. SRM-ADSI-001-07, Normas para el Control y Seguridad de la Comunicación Electrónica* que requería que el personal certificara, mediante la firma de un documento, que conocía la política sobre el uso de los sistemas de información y su

[9] En el **Hallazgo 4-b.2)** del *Informe de Auditoría TI-10-13* se comenta la falta de procedimientos uniformes para la solicitud y la cancelación de las cuentas de accesos a los sistemas de información.

compromiso para cumplir con ésta. Al 10 de septiembre de 2007, el SRM contaba con la *Solicitud Asignación o Cancelación de Acceso* (*SRM-adsi-003*) para obtener dicha certificación.

- El *Procedimiento Autorización Acceso Aplicaciones* que requería el uso de la aplicación *Smarter Ticket* para enviar la *Solicitud Asignación o Cancelación de Acceso* (*SRM-adsi-014*).

El examen de 16 peticiones de servicios a la cuenta Peticiones de Servicios ADSI relacionadas con la creación y la cancelación de cuentas de acceso reveló las siguientes deficiencias:

1) Diez de las peticiones de servicios se tramitaron mediante el envío del formulario *Hoja de Peticiones, Observaciones, Fallas y Comentarios* (*SRM-adsi-009*). Estos formularios no incluían la firma requerida de los usuarios y de los supervisores o encargados de área. Además, este formulario no requería el nombre, la firma y la fecha del Oficial de Seguridad de Sistemas de Informática que tramitó la solicitud ni el nombre, la firma y la fecha de la autorización del dueño de la aplicación para la cual se solicitaba el acceso.

2) Dos de las peticiones de servicios se tramitaron mediante el envío del formulario *Solicitud Asignación o Cancelación de Acceso* (*SRM-adsi-003*). Estos formularios no incluían la firma de los usuarios y de los supervisores y oficiales de Seguridad de Sistemas de Informática. Además, este formulario no requería el nombre, la firma ni la fecha de la autorización del dueño de la aplicación para la cual se solicitaba el acceso.

3) Cuatro de estas solicitudes se tramitaron sin el uso de algún formulario.

b. El examen sobre los controles establecidos para la creación y la administración de 33 cuentas de acceso que tenían privilegios de conexión remota reveló lo siguiente:

1) En la ADSI no se mantenía una lista actualizada de los usuarios con privilegios de conexión remota. La lista de los usuarios con conexión remota que el Director Asociado de la ADSI nos suministró fue preparada a solicitud de los auditores. La misma no

contenía una descripción detallada sobre los servicios, los servidores, los directorios o los archivos que el usuario podía acceder remotamente y la razón para tener acceso a cada uno de estos recursos.

2) No se suministró para examen evidencia de las autorizaciones emitidas por el Director Asociado de la ADSI para autorizar el acceso remoto otorgado al Administrador de Base de Datos y a dos consultoras externas. A la fecha de nuestro examen no se había establecido algún formulario para que el Director Asociado de la ADSI documentara su autorización.

3) Los formularios requeridos para documentar la solicitud de los accesos de conexión remota que habían sido otorgados al Administrador de Base de Datos, a la Directora Auxiliar del Área de Servicios de Retiro y a dos consultoras externas no fueron suministrados para examen.

c. Los oficiales de Seguridad de Sistemas de Informática no habían inactivado las cuentas de acceso al servidor principal del SRM de 11 empleados que habían cesado sus funciones, según se indica:

1) Al 12 de julio de 2007, no se habían inactivado nueve cuentas de acceso[10] asignadas a empleados que habían cesado sus funciones entre el 17 de agosto de 2005 y el 30 de junio de 2007. Estas cuentas permanecieron activas entre 12 y 694 días posteriores a la fecha de separación.

2) Al 6 de diciembre de 2007, no se habían inactivado dos cuentas de acceso[10] asignadas a empleados que habían cesado sus funciones entre el 15 de mayo y el 2 de diciembre de 2007. Estas cuentas permanecieron activas entre 4 y 205 días posteriores a la fecha de separación.

---

[10] Una relación de las cuentas de acceso se incluyó en el borrador de los **hallazgos** de este *Informe*, remitido al Director Ejecutivo y al ex Director Ejecutivo del SRM para comentarios.

d. Los oficiales de Seguridad de Sistemas de Informática no habían eliminado los privilegios de administrador otorgados a la cuenta de acceso[11] asignada a un técnico de operaciones de la ADSI para ejercer tareas relacionadas con las aplicaciones *legacy*[12]. Estos privilegios le permitían al técnico de operaciones efectuar funciones no relacionadas con sus deberes, tales como: crear y modificar cuentas de usuarios y grupos, administrar las políticas de seguridad, crear recursos, asignar los privilegios a los usuarios para utilizar los recursos, y eliminar registros de seguridad.

En la *Orden Administrativa 2007-13* se establece que se completará el formulario *Hoja de Peticiones, Observaciones, Fallas y Comentarios* (*SRM-adsi-009*) y se enviará vía correo electrónico al buzón Peticiones de Servicio ADSI para solicitar los servicios relacionados con la seguridad, bases de datos, redes, desarrollo, operacionales y de control.

En el *Procedimiento Autorización Acceso Aplicaciones*, aprobado el 10 de septiembre de 2007 por el Director Ejecutivo del SRM e incluido en el *Manual*, se establece que los usuarios deberán utilizar la aplicación *Smarter Ticket* para enviar la *Solicitud Asignación o Cancelación de Acceso* (*SRM-adsi-014*). Esta solicitud será recibida por el Oficial de Seguridad de Sistemas de Informática, quien deberá enviar una notificación al usuario cuando atienda la misma.

En el procedimiento *Coordinación Recursos Humanos y ADSI Empleados IN-OUT*, aprobado el 10 de septiembre de 2007 por el Director Ejecutivo del SRM e incluido en el *Manual*, se establece que el Oficial de Seguridad de Sistemas de Informática desactiva el acceso a las aplicaciones solicitadas por el supervisor de la unidad donde cesó funciones el empleado.

---

[11] Véase la nota al calce 10.

[12] Las aplicaciones *legacy* eran aquellas diseñadas en lenguajes, plataformas y técnicas antiguas, pero que permanecían en uso.

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

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

- La información y los programas de aplicación utilizados en las operaciones de las agencias deberán tener controles de acceso para su utilización de tal manera que solamente el personal autorizado pueda ver los datos que necesita ver, o usar las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.

- Si existe la necesidad de acceder a la red desde afuera de las instalaciones de la agencia (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación mediante Internet), deberán existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información.

- Cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de tal manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto, deberán establecerse procedimientos que incluyan una comunicación efectiva entre el área de Recursos Humanos, el área en que trabaja el empleado y el área de Sistemas de Información.

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

- El establecimiento de controles de acceso rigurosos a la red, a los programas y a los archivos, incluido el uso de formularios para solicitar la creación, la modificación o la eliminación de cuentas de acceso a los diferentes recursos disponibles a través de la red, para cada usuario.

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

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

- El establecimiento de normas y procedimientos específicos para la asignación del privilegio de acceso remoto a los usuarios, que requiera, entre otras cosas, la justificación por escrito para otorgar dicho privilegio.

- La notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones o de la modificación de las mismas para la acción correspondiente.

Las normas generalmente aceptadas en el campo de la tecnología de información establecen que las entidades tendrán la responsabilidad de desarrollar políticas y directrices que permitan establecer los controles adecuados en sus sistemas computadorizados que minimicen los riesgos de que la información sea accedida de forma no autorizada. Esta norma se instrumenta, en parte, mediante la revisión periódica de las cuentas activas en los sistemas de información del SRM.

Las situaciones comentadas en los **apartados a. y b.** impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y los privilegios a los usuarios. Esto puede dificultar que se fijen responsabilidades por el uso indebido de los sistemas computadorizados. Además, puede afectar la integridad de la información registrada en éstos.

Las situaciones comentadas en los **apartados c. y d.** propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas, sin que puedan ser detectados a tiempo para fijar responsabilidades.

Las situaciones comentadas se debían a que el Director Ejecutivo no se aseguró de que:

- Las políticas, las normas y los procedimientos sobre el uso de los sistemas de información incluyeran directrices actualizadas y uniformes con los nuevos procesos y tecnologías utilizadas por el SRM para la solicitud, la modificación y la cancelación de las cuentas de acceso a los sistemas de información. **[Apartado a.]**

- El Oficial Principal de Informática se asegurara de que los oficiales de Seguridad de Sistemas de Informática establecieran controles adecuados para la creación y la cancelación de las cuentas de acceso y asignaran los privilegios a las mismas a base de las funciones que los usuarios de éstas realizan. **[Apartados del a. al c.]** Además, no había requerido a los oficiales de Seguridad de Sistemas de Informática que se aseguraran de que los privilegios de administrador se otorgaran temporeramente al técnico de operaciones, bajo estricta supervisión, y sólo para efectuar tareas específicas cuando fuera necesario sustituir al Administrador de Redes. **[Apartado d.]**

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

> El SRM ha tomado las medidas para mejorar los sistemas de control sobre los eventos relacionados con los accesos a los sistemas de información. **[Apartado a.]**
>
> En la actualidad en el SRM se implantó una herramienta de tecnología "Asistencia a Usuarios" [...] con el propósito de controlar las peticiones de usuarios y el acceso a las aplicaciones, incluyendo el acceso remoto. **[Apartado b.]**
>
> En el SRM se establecieron los controles internos para deshabilitar las cuentas de acceso de empleados que cesan funciones en el Sistema. [*sic*] **[Apartado c.]**
>
> En el SRM existe un empleado que ocupa el puesto de Administrador de Redes. Se designó oficialmente a un Operador Principal para asistir al Administrador de Redes para sustituirlo, en caso de ausencias por vacaciones o enfermedad. Para que el Operador Principal pudiese realizar las tareas designadas oficialmente, fue necesario otorgarle accesos de administrador. [*sic*] **[Apartado d.]**

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[13]

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
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 Organización Magisterial Asociación de Maestros de Puerto Rico	10 sep. 07	31 oct. 08
Prof. Astrid J. Llanos Algarín	Miembro Representante de los Maestros Activos[14]	10 sep. 07	14 nov. 07
Prof. Jesús López Colón	Miembro Representante de los Maestros Jubilados	10 sep. 07	31 oct. 08
Prof. María C. Martínez Torres	"	10 sep. 07	31 oct. 08
CPA María Medina Rullán	Miembro Representante del Interés Público	10 sep. 07	31 oct. 08

[13] Del 10 de septiembre de 2007 al 31 de octubre 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.*

[14] Este puesto estuvo vacante del 15 de noviembre de 2007 al 31 de octubre de 2008.

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

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Sr. Harold González Rosado	Director Ejecutivo	10 sep. 07	31 oct. 08
CPA José Reyes Portalatín	Subdirector Ejecutivo - Área Fiscal	10 sep. 07	31 oct. 08
Vacante	Subdirector Ejecutivo	1 sep. 08	31 oct. 08
Sr. Andrés Ramón Miró	"	1 abr. 08	31 ag. 08
Vacante	"	10 sep. 07	31 mar. 08
Sra. Irma García Hernández	Directora de Servicios Generales	10 sep. 07	31 oct. 08
Sr. Víctor Rivera Aquino	Oficial Principal de Informática[15]	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 Informática[16]	10 sep. 07	30 sep. 08

[15] 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.

[16] Del 1 al 31 de octubre de 2008, el puesto de Director Asociado de Sistemas de Informática estuvo vacante.