



*JUNTA DE SÍNDICOS
ADMINISTRACIÓN DE LOS SISTEMAS DE RETIRO
DE LOS EMPLEADOS DEL GOBIERNO Y LA JUDICATURA*

OFICINA DE AUDITORÍA

Informe de Auditoría OA-12-07
8 de mayo de 2012

OFICINA DE TECNOLOGÍA DE INFORMACIÓN
(CONTROLES EN EL SISTEMA DE APORTACIONES Y
BENEFICIOS INTEGRADOS (SABI))

Período Auditado: 1 de enero de 2009 al 31 de marzo de 2010

CONTENIDO

	<u>Página</u>
INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....	2
RESPONSABILIDAD DE LA GERENCIA.....	3
ALCANCE Y METODOLOGÍA.....	4
OPINIÓN.....	4
CLASIFICACIÓN Y CONTENIDO DE LOS HALLAZGOS.....	5
COMUNICACIONES A LA GERENCIA.....	6
COMENTARIOS DE LA GERENCIA.....	7
DETERMINACIÓN FINAL.....	7
AGRADECIMIENTO.....	7
HALLAZGOS:	
1. Datos incorrectos y no ingresados en el Sistema de Aportaciones y Beneficios Integrados (SABI) y en el Sistema de Información del Pensionado (SIP).....	8
2. Fallas en los controles de acceso lógico a SABI.....	12
3. Cuenta de acceso con permiso de consulta que puede eliminar y realizar cambios en los datos demográficos que están en SABI.....	16
4. Ausencia de políticas de seguridad que protejan el acceso a SABI.....	18
5. Ausencia de procedimientos escritos relacionados a la otorgación de accesos en las aplicaciones y normas relacionadas con el control de programas fuentes sin actualizar.....	20
ANEJOS (Los siguientes anejos están en formato electrónico):	
Anejo 1 - A Récorde de participantes con dos o más números de seguro social	
Anejo 1 - B Récorde de participantes con el número de seguro social inválido	
Anejo 1 - C Récorde de participantes con el campo de fecha de ingreso en blanco	
Anejo 1 - D Récorde de participantes con el campo de fecha de nacimiento en blanco	
Anejo 1 - E Récorde de participantes con el campo de dirección en blanco	
Anejo 1 - F Récorde de participantes con el campo nombre completo inválido	
Anejo 1 - G Récorde de pensionados con el dato 01/01/1905 en el campo de fecha de nacimiento	
Anejo 1 - H Récorde de pensionados con el campo de fecha de efectividad de la pensión en blanco	

- Anejo 1 - I Récorde de pensionados con fecha de efectividad anterior a la fecha de nacimiento
- Anejo 1 - J Récorde de pensionados con el campo de fecha de nacimiento en blanco
- Anejo 1 - K Récorde de pensionados fallecidos que se les continuaba emitiendo pagos de la pensión después de la fecha de muerte
- Anejo 1 - L Récorde de pensionados fallecidos con diferencia en la fecha de muerte que se indica en SIP con la que se indica en el Registro Demográfico
- Anejo 1 - M Cuentas de usuarios activos en SABI de empleados o personal externo que no trabaja en la ASR
- Anejo 1 - N Cuentas de usuarios con permisos y privilegios en SABI que no guardaban relación con sus funciones
- Anejo 2 Funcionarios principales de la ASR que actuaron durante el período auditado



Junta de Síndicos
Administración de los Sistemas de Retiro
de los Empleados del Gobierno y la Judicatura

OFICINA DE AUDITORIA

8 DE MAYO DE 2012

**Al Presidente de la Junta de Síndicos de la Administración de los
Sistemas de Retiro de los Empleados del Gobierno y la Judicatura:**

Realizamos una auditoría de las operaciones de la Oficina de Tecnología de Información (OTI) y de los sistemas y la tecnología de información de la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura (ASR) para determinar si se hicieron de acuerdo con la ley y la reglamentación aplicables y a las normas generalmente aceptadas en este campo. Efectuamos la auditoría a base de la facultad que se nos confiere mediante el Estatuto de la Oficina de Auditoría, aprobado por la Junta de Síndicos el 2 de abril de 2008.

Determinamos emitir este informe que contiene el resultado de nuestro examen sobre el Sistema de Aportaciones y Beneficios Integrados (SABI) en cuanto a políticas y procedimientos; controles de documentación; controles de acceso lógico; administración de la seguridad; controles de entrada, procesamiento y salida de datos e; integridad de la base de datos¹.

¹ Como parte del examen se realizaron pruebas a la base de datos del Sistema de Información de Pensionados (SIP), el cual es un módulo de SABI.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La OTI provee apoyo de recursos de informática en la ASR y es responsable de custodiar la información electrónica de la agencia. Dentro de los principales servicios que ofrece se encuentran, entre otras, los siguientes:

1. Apoyo a los usuarios en el uso del equipo de computadoras y en el manejo y administración de los diferentes programas de sistemas de información.
2. Configuración y mantenimiento de las estaciones de trabajo o PC's.
3. Desarrollo y mantenimiento de las aplicaciones electrónicas.
4. Acceso a las diferentes aplicaciones existentes en la ASR.
5. Servicio en línea en el portal de la ASR.

SABI se implementó en el 1996 por mediante los servicios de la compañía GM Group y a partir de esa fecha se continúa con el mantenimiento de la aplicación por parte de consultores externos. El contrato que estaba vigente durante nuestra auditoría, relacionado al mantenimiento de SABI era el 2010-000047 por \$288,000², con la compañía Info Providers. Este sistema consta de sesenta y un (61) módulos que produce hasta 283 informes, según determinen los usuarios que tienen el permiso o privilegio correspondiente.

El Anejo 2, en formato electrónico, contiene una relación de los funcionarios principales de la ASR que actuaron durante el período auditado.

² Este contrato se enmendó el 17 de noviembre de 2009 para disminuir la cuantía del mismo por \$96,000, lo que redujo el pago de los servicios a \$182,000.

RESPONSABILIDAD DE LA GERENCIA

Con el propósito de lograr una administración eficaz, regida por principios de calidad, la gerencia de toda entidad gubernamental, entre otras cosas, es responsable de:

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 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 sus oficinas de auditoría interna y de la Oficina del Contralor de Puerto Rico y atender las recomendaciones de los auditores externos.
9. Mantener un sistema adecuado de administración de personal que incluya la evaluación del desempeño y un programa de educación continua para todo el personal.
10. Cumplir con la Ley de Ética Gubernamental, lo cual incluye divulgar sus disposiciones a todo el personal.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de enero de 2009 al 31 de marzo de 2010. En algunos aspectos de examinaron transacciones con fechas anteriores. El examen se realizó de acuerdo con las normas de auditoría gubernamental generalmente aceptadas, en lo que concierne a los aspectos del desempeño o ejecución. Se efectuaron las pruebas consideradas necesarias de acuerdo con las circunstancias.

Para efectuar la auditoría se utilizó la siguiente metodología:

- Entrevistas a funcionarios, empleados y particulares.
- Inspecciones físicas.
- Análisis de información de procedimientos de control y otros procesos.
- Examen y análisis de informes y de documentos generados por la unidad auditada y externos.
- Análisis de información suministrada por fuentes de la ASR y externos.
- Confirmaciones de información pertinente.

OPINIÓN

Las pruebas efectuadas revelaron que las operaciones objeto de este informe se realizaron sustancialmente de acuerdo con la ley y la reglamentación aplicable, excepto por los hallazgos del 1 al 3, clasificados como principales, y los hallazgos 4 y 5, clasificados como secundarios, que se detallan en el Anejo 1.

CLASIFICACIÓN Y CONTENIDO DE LOS HALLAZGOS

En nuestros informes de auditoría se incluyen los hallazgos significativos determinados por las pruebas realizadas, los cuales se clasifican como principales o secundarios. Los principales incluyen violaciones de ley y de los reglamentos aplicables, además de 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 mismos pueden consistir en irregularidades y errores graves o significativos. Los secundarios son los que consisten en faltas o errores que no han tenido consecuencias graves o que se anticipa que no las tenga. En la sección anterior se ofrece información sobre la clasificación de los hallazgos de este informe.

Los hallazgos están presentados basándose en 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:

<u>Situación</u>	Hechos encontrados en la auditoría indicativos de que no se cumplió con uno o más criterios.
<u>Criterio</u>	El marco de referencia para evaluar la situación. Es principalmente una ley, reglamento, carta circular, memorando, procedimiento, norma de control interno, norma de sana administración, principio de contabilidad generalmente aceptado, opinión de un experto o juicio del auditor.
<u>Efecto</u>	La consecuencia, real o potencialmente, por no cumplir con el criterio.

<u>Causa</u>	Razón fundamental que dio origen a la situación.
<u>Comentarios de la Gerencia</u>	Se consideran al revisar el borrador del informe y se incluyen al final del hallazgo conforme a las normas de nuestra Oficina. Las observaciones de la gerencia a incluirse al final del hallazgo no excederán de cinco líneas.
<u>Determinación Final</u>	Luego de evaluados los comentarios de la gerencia determinamos si el hallazgo prevalece, requiere modificarse o se elimina.
<u>Recomendación</u>	Sugerencia o acción a seguir para corregir y/o prevenir la situación señalada o situaciones similares.

COMUNICACIONES A LA GERENCIA

El borrador de los hallazgos de este informe se sometió para comentarios mediante carta del 20 de julio de 2010 al Lic. Héctor M. Mayol Kauffmann, Administrador. Una copia fue tramitada al Director de Tecnología de Información, Sr. Daniel Casas Meléndez. Este informe de auditoría se tramitó mediante comunicación del 8 de mayo de 2012 al Administrador y una copia del mismo a través de correo electrónico al Director de Tecnología de Información y a la Directora de Sistemas y Procedimientos, Sra. Ingrid Vázquez Tirado.

COMENTARIOS DE LA GERENCIA

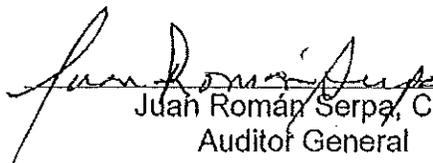
El Director de Tecnología de Información, Sr. Daniel Casas Meléndez, contestó el borrador de los hallazgos de este informe mediante comunicación del 20 de junio de 2011 (comunicación del Director de Tecnología de Información). Sus comentarios fueron considerados en la redacción final del informe y se incluyen en la sección Comentarios de la Gerencia en el hallazgo correspondiente, de forma objetiva y conforme a las normas de nuestra Oficina.

DETERMINACIÓN FINAL

Luego de evaluar los comentarios presentados por la gerencia al borrador de los hallazgos de este informe, determinamos que los hallazgos del 1 al 5 que fueron incluidos en el mismo prevalecen. Por otra parte, el hallazgo 6 fue eliminado de este informe como resultado de la evidencia presentada por la gerencia.

AGRADECIMIENTO

Agradecemos a los funcionarios y empleados de la ASR por toda la cooperación que nos brindaron durante nuestra auditoría.


Juan Román Serpa, CPA
Auditor General

HALLAZGOS

Hallazgo -1 Datos incorrectos y no ingresados en el Sistema de Aportaciones y Beneficios Integrados (SABI) y en el Sistema de Información del Pensionado (SIP)

Situación

A. Examinamos, a través de la herramienta de auditoría Audit Command Language (ACL), la información que contenía la tabla Participantes que está en el universo de SABI producción. Esta tabla contenía 486,102 récords de participantes de los sistemas de retiro de los empleados del gobierno y de la judicatura. Como resultado de las pruebas efectuadas encontramos, entre otras cosas, lo siguiente:

1. De los 486,102 récords que contenía la tabla Participantes, había 120,197 récords que pertenecían a participantes que tenían dos o más números de seguro social asignados (Véase Anejo 1-A en formato electrónico).

2. La tabla Participantes contenía 7,124 récords con el número de seguro social inválido. De éstos, 5,664 tenían menos de nueve (9) números en el seguro social o una combinación de números y caracteres y 925 correspondían a números de seguro social que comenzaban con 000 y 535, los cuales no habían sido asignados por la Oficina del Seguro Social de los Estados Unidos (Véase Anejo 1-B en formato electrónico).

3. En 43,372 récords la fecha de ingreso de los participantes en el campo establecido para este concepto estaba en blanco (Véase Anejo 1-C en formato electrónico).

4. En 127,629 récords la fecha de nacimiento de los participantes estaba en blanco (Véase Anejo 1-D en formato electrónico).

5. En 133,052 récords la dirección de los participantes estaba en blanco (Véase Anejo 1-E en formato electrónico).

6. Observamos 1,341 récords que en el campo titulado Nombre Completo tenían escrito "Beneficio por Muerte"; seis (6) tenían números en vez de caracteres y; siete (7) tenían escrito la frase "no nombre no apellido" (Véase Anejo 1-F en formato electrónico).

B. Por otro lado, examinamos las tablas: T_SIP01_CHK_PENSION, donde se mantenían los datos demográficos de los pensionados; T_ÚLTIMA_NOMINA, que mantenía la información de todos los pensionados que recibían un cheque y; T_SIP32_FALLECIDOS, que contenía la información de fallecidos que enviaba el Registro Demográfico de Puerto Rico a la ASR. Luego de realizar varias pruebas utilizando ACL, observamos, entre otras cosas, lo siguiente:

1. En la tabla T_SIP01_CHK_PENSION había 326 récords que tenían como fecha de nacimiento 01/01/1905 (Véase Anejo 1-G en formato electrónico).

2. En 1,181 récords de pensionados no se tenía escrito la fecha de efectividad de la pensión (Véase Anejo 1-H en formato electrónico).

3. En 1,723 récords de pensionados la fecha de efectividad de la pensión era previa a la fecha de nacimiento (Véase Anejo 1-I en formato electrónico).

4. En 929 récords de pensionados no se tenía una fecha de nacimiento, de éstos, 143 pertenecían a pensionados activos (Véase Anejo 1-J en formato electrónico).

5. En 2,414 récords de pensionados fallecidos entre el 3 de enero de 2000 al 28 de enero de 2010, se observó que al 28 de febrero de 2010 se les continuaba emitiendo pagos de la pensión (Véase Anejo 1-K en formato electrónico).

6. En 1,401 récords de pensionados la fecha de muerte en la tabla T_SIP01_CHK_PENSION era diferente a la fecha de muerte que contenía la tabla de fallecidos del Registro Demográfico (Véase Anejo 1-L en formato electrónico).

Al cierre de nuestra auditoría, el Director de Tecnología de Información estaba en el proceso de recolección de los datos demográficos de los participantes y pensionados, con la colaboración de los directores del Área de Servicios al Participante y el Área de Servicios al Pensionado, con el fin de actualizar la base de datos de SABI y SIP.

Criterio

En la Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica, 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 adelante la Carta Circular Núm. 77-05), se establece, entre otras cosas, que las aplicaciones deben ser diseñadas, adquiridas e implementadas para proveer crecimiento, flexibilidad y adaptabilidad. Además, dispone que toda aplicación que se desarrolle o adquiera debe tener una garantía que asegure que funciona apropiadamente y de acuerdo con los propósitos para los cuales fue desarrollada. Esto se logra, en gran medida estableciendo controles en las aplicaciones que impidan el registro de datos incorrectos o inválidos. Además, en la misma política se estableció que la duplicidad de datos en un mismo sistema debe ser evitado para asegurar la integridad de los mismos.

Efecto

Las situaciones mencionadas en el hallazgo no garantiza la exactitud de la información que contiene SABI/SIP y socava la utilidad de los datos de los

participantes y pensionados. Además, estas situaciones pueden ocasionar que la ASR emita decisiones incorrectas sobre los asuntos de los pensionados y participantes de la ASR.

Causa

Las situaciones comentadas denotan que los directores de Tecnología de Información que actuaron durante el período auditado no velaron que SABI contara con procesos de validación de datos activos en la entrada de información, que impidieran el registro de datos incorrectos, inválidos y campos en blanco.

Comentarios de la Gerencia

En la comunicación del Director de Tecnología de Información, éste nos informó lo siguiente:

Como parte de las mejoras en los sistemas de información procedimos a coleccionar datos faltantes de diferentes fuentes (AEELA, Dep. Hacienda) con el propósito de actualizar la base de datos. Una vez se completó la valoración actuarial se procedió a emitir los comunicados correspondientes a las áreas de Participantes y Pensionados para actualizar los datos en referencia. Esto fue completado.

Determinación Final

Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

Recomendación 1

Al Administrador

Instruir, si aún no se ha hecho, al Director de Tecnología de Información para que:

A. Desarrolle y lleve a cabo un proyecto de depuración de datos en SABI, de manera que se corrijan las situaciones comentadas en el hallazgo.

B. Se desarrollen procesos de validación de datos en la entrada de información en SABI para que no se repitan las situaciones comentadas en el hallazgo.

Hallazgo -2 Fallas en los controles de acceso lógico a SABI

Situación

A. Al 28 de enero de 2010, examinamos las cuentas de acceso de los usuarios de SABI y observamos que había veinte y cuatro (24) cuentas de usuarios activas de empleados que habían dejado de trabajar en la ASR y una correspondía a una consultora externa que había dejado de ofrecer servicios en la agencia. Para esa fecha, las cuentas llevaban entre 49 y 898 días activas luego de la fecha en que los empleados dejaron de trabajar en la ASR (Véase Anejo 1-M en formato electrónico). Además, existían tres (3) cuentas genéricas, SABIAPP, SABIUSER y SIJALA, que no estaban asignadas a un usuario en particular y tenían roles de consulta, supervisor, operador y técnico.

B. Durante nuestras pruebas observamos que había cinco (5) usuarios con dos (2) o más cuentas de usuarios creadas con permisos similares y diferentes.

	Nombre del usuario	Cuenta de usuario
1	Antonio Rivera Rosario	ARIVERA1, ARIVERA2
2	Sylvia Ramírez López	SRAMI01, SRAMI02
3	Vanessa Peña	VPENA01, VPENA02
4	Yamilet Cruz Amador	YAMAD01, YAMAD02
5	Yan Mercado Díaz	YMERC01, YMERCADO

C. Por otra parte, evaluamos cuarenta y una (41) cuentas de accesos activas y observamos que en veinte (20) de éstas o el 49 por ciento, se les había otorgado permisos inadecuados a los usuarios, ya que los privilegios no estaban de acuerdo a los puestos que éstos ocupaban. De las veinte (20) cuentas, cinco (5) tenían accesos a módulos que no estaban relacionados al área de trabajo de los usuarios (Véase Anejo 1-N en formato electrónico).

Criterio

En la Parte E, Controles Generales, de la Política Núm. TIG-003, Seguridad de los Sistemas de Información, de la Carta Circular Núm. 77-05 se establece, entre otras cosas, que la información y los programas de aplicación utilizadas en las operaciones de la agencia deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos que necesita ver. Además, dispone que los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.

Efecto

Las situaciones comentadas pueden ocasionar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. Además, pueden propiciar la comisión de irregularidades y la alteración, por error o

deliberadamente, de los datos contenidos en dicho sistema sin que puedan ser detectadas a tiempo para fijar responsabilidades. Por otro lado, la situación comentada en el apartado B también podría ocasionar una segregación de funciones inadecuada y otras situaciones impropias.

Causa

Las situaciones comentadas se debían, en parte, a que:

- Los directores de la OTI que actuaron durante el período auditado no observaron lo establecido en la Política Núm. TIG-003.
- No se habían aprobado normas y procedimientos internos con respecto a la administración y control de las cuentas de los usuarios a los sistemas de aplicaciones y a los recursos computadorizados.
- No existía una comunicación efectiva entre la Oficina de Recursos Humanos y Relaciones Laborales y las demás áreas u oficinas de la ASR con la OTI para la cancelación de las cuentas de acceso de los empleados y contratistas tan pronto éstos cesaban funciones en la ASR.
- Los funcionarios a cargo de la creación de cuentas no verificaban si había una cuenta activa antes de crearla, ni el sistema tenía dicha opción activa.
- Los funcionarios a cargo de la creación de cuentas en SABI, no creaban cuentas temporeras con fecha de expiración, de los usuarios que necesitaban acceso por un tiempo determinado. Tampoco el personal supervisor de la OTI les requirió a éstos crear cuentas temporeras para el personal externo que necesite utilizar el sistema por un tiempo determinado.

Comentarios de la Gerencia

En la comunicación del Director de Tecnología de Información, éste nos informó lo siguiente:

La lista de empleados que ya no trabajan con ASR fue revisada, todos estos usuarios se encuentran deshabilitados. Como parte de la acción correctiva se solicitó a Recursos Humanos un informe mensual donde se presenten las personas que se retiraron o renunciaron durante el pasado mes. En el caso de usuarios que tienen dos usuarios estos fueron identificados de acuerdo a las tablas suministradas y sus accesos corroborados con las áreas correspondientes. Las listas de usuarios con accesos inadecuados fueron revisadas y las correcciones necesarias completadas.

Determinación Final

Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

Recomendación 2

Al Administrador

Instruir, si aún no se ha hecho, al Director de Tecnología de Información para que:

- A. Las cuentas de los usuarios que cesen funciones en la ASR se deshabiliten inmediatamente el empleado deje de trabajar en la agencia.
- B. Se mantenga una comunicación continua entre la Oficina de Recursos Humanos y Relaciones Laborales y la Oficina de Tecnología de Información sobre los cambios de personal de la ASR.
- C. Se asignen cuentas temporeras a los consultores externos de acuerdo al tiempo que se estime que éstos proveerán sus servicios.

Hallazgo -3 Cuenta de acceso con permiso de consulta que puede eliminar y realizar cambios en los datos demográficos que están en SABI

Situación

Como parte de nuestro examen accedimos al módulo o unidad de Control de Solicitudes de SABI utilizando una cuenta de usuario con permiso de consulta. Nuestro resultado reflejó que a través de esta cuenta la aplicación nos permitió, entre otras cosas, con respecto al récord de dos participantes: eliminar la dirección y el número de teléfono; cambiar las fechas de nacimiento y; cambiar el estatus de éstos.

Criterio

Las normas de sana administración relacionadas a la tecnología de información definen el privilegio o rol de consulta como el privilegio más restringido, ya que solamente permite buscar información (sólo lectura) y no debe permitir al usuario que lo posea realizar cambios en la información y mucho menos eliminarla.

Efecto

La situación comentada podría ocasionar que usuarios con privilegios de lectura registren, cambien o eliminen información de los participantes y/o pensionados existentes en SABI y que dicha acción irregular no se pueda detectar. Además, aumenta los riesgos relacionados a situaciones de fraude y otras irregularidades.

Causa

Los funcionarios a cargo de la asignación de privilegios no implementaron políticas de seguridad relacionadas a las funciones que debe tener cada usuario de acuerdo al rol o permiso asignado a éste. Además, los diferentes directores de la

OTI que actuaron durante el período auditado no velaron a que se implementaran dichas políticas. Tampoco existen normas escritas en la ASR relacionadas a la creación de cuentas de acceso en la OTI.

Comentarios de la Gerencia

En la comunicación del Director de Tecnología de Información, éste nos informó lo siguiente:

Revisamos los niveles de seguridad dentro de la aplicación SABI y SIP. Centralizamos la otorgación o remoción de permisos de seguridad a través de la unidad de seguridad en OTI. Se implemento el uso de la Hoja de Seguridad para poder ganar o remover acceso a las aplicaciones.

Determinación Final

Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

Recomendación 3

Al Administrador

Se asegure que el Director de Tecnología de Información adquiera una herramienta de seguridad para la otorgación de accesos y privilegios en SABI/SIP de manera que los usuarios puedan realizar las funciones en SABI/SIP de acuerdo a los permisos otorgados a éstos.

Hallazgo -4 Ausencia de políticas de seguridad que protejan el acceso a SABI

Situación

Al 31 de marzo de 2010, SABI carecía de las siguientes políticas de seguridad:

- A. "Time out" o desconexión automática después de un tiempo de inactividad del usuario.
- B. Bloqueo automático de las cuentas de usuarios después de varios intentos infructuosos, al menos tres (3), de "logon".
- C. Las cuentas de usuarios no se inactivaban o bloqueaban después de un período de tiempo en que el usuario no accedía al sistema.
- D. Cambio de las contraseñas de los usuarios después de un tiempo transcurrido, por ejemplo noventa (90) días. Al cierre de nuestra auditoría, se había establecido en el "Active Directory" que las contraseñas vencieran a los noventa (90) días.

Criterio

En la Parte E, Controles Generales, de la Política Núm. TIG-003, Seguridad de los Sistemas de Información, de la Carta Circular Núm. 77-05 se establece, entre otras cosas, que la seguridad de la información deberá ser parte integral del diseño de cualquier programa de aplicación que se adquiera o desarrolle la agencia para facilitar las operaciones de la entidad y/o mejorar el servicio a los ciudadanos.

Las normas de sana administración relacionadas a la tecnología de información recomiendan que, para mantener un control adecuado en el acceso a las aplicaciones computadorizadas, es necesario emplear y hacer buen uso de programas de seguridad que controlen el sistema de cuentas y contraseñas de acceso y regulen el cambio periódico de éstas. Además, disponen que se establezcan requerimientos de "logon ID" que incluya el bloqueo de cuentas

después que un usuario no utilice los programas, aplicaciones o sesiones por un período de tiempo determinado, desconexión automática o "log off" automático después de un tiempo de inactividad.

Efecto

Las situaciones comentadas en los apartados A, B y D, podrían ocasionar que personas no autorizadas accedan al sistema y obtengan información confidencial de los participantes y pensionados haciendo uso indebido de la información obtenida. Por su parte, la situación C podría ocasionar que se mantengan cuentas activas de usuarios que dejen de trabajar en la ASR o no necesiten el acceso para realizar su trabajo.

Causa

Las situaciones comentadas se deben, en gran medida, a la falta de procedimientos escritos y a que los diferentes directores de la OTI que actuaron durante el período auditado no se habían percatado de la importancia de establecer controles adecuados de seguridad que impidieran estas situaciones, con sus posibles efectos adversos.

Comentarios de la Gerencia

En la comunicación del Director de Tecnología de Información, éste nos informó lo siguiente:

La aplicación de SABI adolece de un sistema de seguridad apropiado. A tales efectos nos encontramos en el proceso de adquirir una, la cual permita controlar el acceso. El módulo de seguridad de SABI está siendo mejorado por la empresa Info Providers como parte de los cambios para utilizar SABI

en el Sistema de Retiro para Maestros. Estos cambios serán implementados en ASR.

Determinación Final

Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

Recomendación 4

Al Administrador

Instruir, si aún no se ha hecho, al Director de Tecnología de Información para que adquiera un programa de seguridad que incluya, entre otras cosas: políticas de desconexión automática, bloqueo automático de las cuentas de usuarios después de varios intentos infructuosos, desactivación de cuentas de usuarios luego de un periodo de inactividad y cambios periódicos de las contraseñas de los usuarios.

Hallazgo -5 Ausencia de procedimientos escritos relacionados a la otorgación de accesos en las aplicaciones y normas relacionadas con el control de programas fuentes sin actualizar

Situación

A. A la fecha de nuestro examen encontramos que en la ASR no se hablan promulgado los procedimientos necesarios para reglamentar, entre otras cosas, los procesos para la otorgación de accesos a las diferentes aplicaciones de la agencia, que incluyera, entre otras cosas, la configuración de códigos y roles (permisos) de los usuarios de las diferentes aplicaciones de la ASR. Ello con el fin de establecer uniformidad en la otorgación de accesos.

B. La ASR tenía vigente desde el 18 de mayo de 2005 la Orden Administrativa Núm. 2005-02, Normas para el Control de Programas Fuentes SABI, SIP y Remesas. Dicha orden administrativa no respondía a la estructura actual ni al flujo de trabajo de la OTI, por lo que requiere revisarse y actualizarse.

Situaciones similares a las mencionadas en este hallazgo fueron comentadas en el informe de auditoría número OA-10-14 de la Oficina de Tecnología de Información.

Criterio

La Ley Núm. 447 del 15 de mayo de 1951, según enmendada, que crea el Sistema de Retiro de los Empleados del Gobierno del Estado Libre Asociado de Puerto Rico, establece en su artículo 4-103, entre otras cosas, que el Administrador tiene entre sus facultades y obligaciones preparar reglamentos, disponer de lo necesario para la instalación de un sistema completo y adecuado de contabilidad y registros y dirigir y supervisar toda la actividad técnica y administrativa de la ASR para su debido funcionamiento.

La Ley Núm. 230 del 23 de julio de 1974, conocida como Ley de Contabilidad del Gobierno de Puerto Rico, según enmendada, establece como política pública, entre otras cosas, que exista el control previo de todas las operaciones del Gobierno para que sirva de arma efectiva en el desarrollo de los programas encomendados a cada dependencia o entidad corporativa. En armonía con dicha disposición de ley, y como norma de sana administración y de control interno, el Administrador debe establecer reglamentos y normas actualizadas que reflejen los cambios en los procesos que realiza la ASR.

En la Política Núm. TIG-003, Seguridad de los Sistemas de Información, de la Carta Circular Núm. 77-05, se establece que será responsabilidad de cada agencia desarrollar políticas específicas de seguridad que consideren las características propias de los ambientes de tecnología de la agencia.

particularmente sus sistemas de misión crítica y del manejo de incidentes y cambios, y que las mismas estén de acuerdo a la legislación y los reglamentos vigentes. Por otra parte, en la Política Núm. TIG-008, Uso de los Sistemas de Información, de la Internet y del Correo Electrónico, de la misma carta circular se dispone como regla general de los sistemas de información, que cada entidad gubernamental será responsable de establecer las normas mediante las cuales se asignan las cuentas de acceso, incluyendo las medidas de seguridad aplicables.

Efecto

Las situaciones comentadas podrían ocasionar que las operaciones de los sistemas de aplicación de la ASR no se realicen de manera controlada, efectiva y 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.

Causa

Las situaciones comentadas denotan que los administradores de la ASR que actuaron durante el período auditado no habían requerido que se desarrollaran, revisaran, actualizaran y se sometieran para su consideración y aprobación las normas y los procedimientos escritos que permitieran regular los procesos que se indican.

Comentarios de la Gerencia

En la comunicación del Director de Tecnología de Información, éste nos informó lo siguiente:

Para todas las aplicaciones en ASR se crearon las hojas de seguridad correspondientes. Estas tienen que ser firmadas por el empleado, su supervisor, el

dueño de la aplicación, esto permite efectuar una revisión de los accesos a otorgar. Se generaron los procedimientos necesarios.

Determinación Final

Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

Recomendación 5

Al Administrador

Ejerza una supervisión eficaz sobre el Director de Tecnología de Información para que éste, en coordinación con el Director de Sistemas y Procedimientos:

- A. Preparen las normas y procedimientos necesarios para reglamentar las operaciones que se comentan en el apartado A de la situación y sometan los mismos para su aprobación.
- B. Actualicen la Orden Administrativa Núm. 2005-02 que se menciona en el apartado B de la situación para que responda a la estructura actual y al flujo de trabajo de la OTI y sometan la misma para aprobación.