

Ponencia del Sr. Rojas
24/Sept/2012



Secretaría

- 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
W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

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

COMISIONES ESPECIALES

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

COMISIONES CONJUNTAS

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

INFORME DE AUDITORÍA TI-13-06

12 de septiembre de 2012

**Administración de los Sistemas de Retiro
de los Empleados del Gobierno y la Judicatura**

Oficina de Tecnología de Información

(Unidad 5060 - Auditoría 13436)

Período auditado: 15 de marzo al 31 de agosto de 2010

CONTENIDO

	Página
ALCANCE Y METODOLOGÍA.....	2
CONTENIDO DEL INFORME.....	2
INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....	3
COMUNICACIÓN CON LA GERENCIA.....	5
OPINIÓN Y HALLAZGOS	6
1 - Falta de un plan de seguridad.....	7
2 - Deficiencia relacionada con el plan de contingencias de la OTI.....	9
3 - Deficiencias en los parámetros de seguridad y en otros controles de acceso lógico de los servidores principales de la red	11
4 - Falta de restricciones para enviar y recibir mensajes de correo electrónico de fuentes externas, y de revisiones periódicas a los registros de los accesos a las páginas de direcciones en Internet	14
5 - Falta de normas y de procedimientos para reglamentar la administración, la seguridad y el uso de los sistemas computadorizados	17
6 - Falta de un registro de programas instalados en cada computadora.....	20
RECOMENDACIONES.....	22
AGRADECIMIENTO.....	23
ANEJO 1 - MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS DURANTE EL PERÍODO AUDITADO	24
ANEJO 2 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO	25

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

12 de septiembre de 2012

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

Realizamos una auditoría de las operaciones de la Oficina de Tecnología de Información (OTI) de la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura (Administración), 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.

**ALCANCE Y
METODOLOGÍA**

La auditoría cubrió del 15 de marzo al 31 de agosto de 2010. 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, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

**CONTENIDO DEL
INFORME**

Este *Informe* contiene seis hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración de la seguridad, el acceso lógico a los sistemas de información

computadorizados, la continuidad del servicio, la segregación de deberes, las aplicaciones y las computadoras. El mismo está disponible en nuestra página en Internet: <http://www.ocpr.gov.pr>.

**INFORMACIÓN SOBRE
LA UNIDAD AUDITADA**

La Administración comprende dos sistemas de retiro bajo una misma unidad: el Sistema de Retiro de los Empleados del Gobierno del Estado Libre Asociado de Puerto Rico (Sistema) y el Sistema de Retiro de los Empleados de la Judicatura de Puerto Rico. Los mismos se crearon en virtud de la *Ley Núm. 447 del 15 de mayo de 1951* y de la *Ley Núm. 12 del 19 de octubre de 1954*, según enmendadas, respectivamente. En estas leyes se establecieron entre las funciones de la Administración:

- Proveer estabilidad y seguridad económica a los servidores públicos mediante la concesión de pensiones y otros beneficios, tales como, préstamos hipotecarios, personales y de viajes culturales.
- Administrar y custodiar los recursos que anualmente se consignan en la *Resolución Conjunta del Presupuesto General de Gastos* para el pago de pensiones y de aportaciones a los planes médicos de los pensionados.
- Invertir en valores los fondos acumulados que autoriza la propia *Ley*.

Efectivo en enero de 2000, mediante la *Ley 305-1999*, se enmendó la *Ley Núm. 447* y se realizó una reforma en la base estructural del Sistema conocida como Sistema 2000. Se estableció un programa de ahorros para el retiro que se conocerá como el Programa de Cuentas de Ahorro para el Retiro (Programa) basado en un modelo de aportaciones definidas. Este nuevo programa es compulsorio para todas las personas que ingresen al Sistema en o después del 1 de enero de 2000, y voluntario para las personas que ya eran parte del mismo a dicha fecha. Mediante este Programa, se crea una cuenta de ahorro para el participante, nutrida solamente por sus aportaciones y el rendimiento que genere la alternativa de inversión que este seleccione. En este Programa el empleado realiza una aportación mensual de su salario que fluctúa entre el 8.275 y el 10 por ciento, la cual es administrada por el Sistema. Los participantes

podrán seleccionar que la rentabilidad de su cuenta se determine entre alternativas de inversión, tales como Ingreso Fijo o Cartera de Inversión del Sistema.

La Junta de Síndicos (Junta) es el fiduciario de la Administración y, como tal, es responsable del funcionamiento adecuado de esta. La Junta está constituida por 7 miembros, de los cuales 4 son miembros natos: el Secretario de Hacienda, el Comisionado de Asuntos Municipales, el Presidente del Banco Gubernamental de Fomento para Puerto Rico y el Director de la Oficina de Capacitación y Asesoramiento en Asuntos Laborales y de Administración de Recursos Humanos. El Gobernador nombra a los 3 miembros restantes por un término de 3 años. Dos de estos 3 miembros deben ser participantes de la Administración con, por lo menos, 10 años de servicio acreditables y 1 debe ser un pensionado de la Administración.

La Junta nombra al Administrador y fija su sueldo. Además, la Junta tiene el deber de adoptar las reglas para la organización y el funcionamiento interno de la Administración, y de aprobar y promulgar los reglamentos que prepare el Administrador para la administración de la misma, de conformidad con la *Ley Núm. 447*. El Administrador es responsable de dirigir y supervisar todas las actividades técnicas y administrativas de esta agencia.

La Administración cuenta con las siguientes áreas para llevar a cabo sus funciones: Centro de Orientación; áreas de Servicios al Pensionado, de Servicios al Participante, y de Préstamos; y las oficinas de Determinación de Incapacidad e Investigaciones, del Procurador de Asuntos de Retiro, de Inversiones y Tesorería, de Actuariales y Estadísticas, de Contraloría, de Presupuesto, de Servicios Administrativos, de Tecnología de Información, de Sistemas y Procedimientos, de Comunicaciones, de Recursos Humanos y Relaciones Laborales, de Asuntos Legales, y de Auditoría Interna.

Los **anejos 1 y 2** contienen una relación de los miembros principales de la Junta y de los funcionarios principales de la Administración que actuaron del 15 de marzo al 31 de agosto de 2010, respectivamente.

La estructura organizacional de la OTI está compuesta por 14 empleados: 1 Director de Tecnología de Información, 1 Auxiliar en Procesamiento y Control de Sistemas de Información, 4 Especialistas en Sistemas de Información, 1 Analista Programador de Sistemas de Información, 1 Gerente de División, 2 Analistas Desarrollador de Sistemas de Información, 1 Analista Programador de Sistemas de Información, 2 Administradores de Red de Computadoras y 1 Auxiliar de Sistemas de Oficina. La OTI brinda apoyo tecnológico a todas las áreas y oficinas que componen la Administración. Es responsable de custodiar la información electrónica de la Administración. Además, ofrece apoyo a los usuarios (*Help Desk*), en el manejo y la administración de los diferentes programas de sistemas de información y de los equipos computadorizados, y en el desarrollo de las aplicaciones.

Los recursos para financiar las actividades operacionales de la Administración provienen principalmente de las aportaciones patronales e individuales, los intereses sobre préstamos y los ingresos provenientes de las inversiones. Además, la Administración recibe aportaciones del Fondo General del Gobierno del Estado Libre Asociado de Puerto Rico para cubrir beneficios garantizados a los pensionados mediante leyes especiales. El presupuesto de la Administración y de la OTI para el año fiscal 2009-10 ascendió a \$40,615,040 y a \$2,948,693, respectivamente.

La Administración cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.asr.gobierno.pr>. Esta página provee información acerca de la entidad y de los servicios que presta.

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* fueron remitidas al Lcdo. Héctor M. Mayol Kauffman, Administrador, mediante carta de nuestros auditores del 19 de octubre de 2010. En la referida carta se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante carta del 22 de noviembre de 2010, el Sr. Daniel Casas Meléndez, Director de la Oficina de Tecnología de Información, en representación del Administrador, remitió sus comentarios a los hallazgos incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al Administrador, para comentarios, por carta del 3 de febrero de 2012.

El 21 de febrero de 2012, el Sr. Manuel Iglesias Beléndez, Subadministrador, solicitó una prórroga de 15 días para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. Ese mismo día, le concedimos al Subadministrador la prórroga hasta el 6 de marzo de 2012. El Subadministrador, en representación del Administrador, contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 6 de marzo de 2012. Sus comentarios fueron considerados en la redacción final de este *Informe*; y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones de la OTI en lo que concierne a los controles internos establecidos para la administración de la seguridad, el acceso lógico a los sistemas de información computadorizados, la continuidad del servicio, la segregación de deberes, las aplicaciones y las computadoras no se realizaron conforme a las normas generalmente aceptadas en este campo. A continuación se comentan los **hallazgos del 1 al 6**.

Hallazgo 1 - Falta de un plan de seguridad

Situación

- a. Al 8 de junio de 2010, la Administración no tenía un plan de seguridad aprobado por el Administrador que incluyera, entre otras cosas, disposiciones en cuanto a:
- La documentación de la validación de las normas de seguridad¹
 - La evidencia de un análisis de riesgo actualizado, que sea base del plan de seguridad
 - 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 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 OTI, el personal a cargo del procesamiento de los datos y los administradores de seguridad, entre otros
 - La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros).

Criterios

La situación comentada es contraria a lo establecido 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 (OGP). En esta se

¹ 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.

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.

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 este. Los mismos deben considerar los sistemas y las instalaciones 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.

Efectos

La situación comentada 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.

Causa

La situación comentada se atribuye a que el Administrador no había promulgado una directriz para la preparación de 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*.

Comentarios de la Gerencia

En la carta del Subadministrador, este nos indicó, entre otras cosas, lo siguiente:

[...] Para el 15 de octubre de 2010 le fue presentado al Administrador de la Agencia [...] los documentos referentes a la contingencia, validación de normas de seguridad, análisis de riesgo. [sic]

Se creó un comité de emergencia al cual se le suministro los adiestramientos necesarios en seguridad coordinado por la Agencia para el Manejo de Emergencias. [...] [sic]

Se han efectuado ejercicios cada seis meses para asegurarnos todo el personal esta consiente de cómo actuar en caso de una emergencia. [sic]

La documentación de los controles administrativos, técnicos y físicos de los activos de información están incluidos en la documentación del Plan de emergencias de la Oficina de Tecnología de Información, el Plan de Recuperación de Negocios de ASR y el Plan de emergencias coordinado con la Agencia para el Manejo de Emergencias. Este plan fue presentado a la Agencia para el Manejo de Emergencias y es revisado en base anual. [sic]

Consideramos las alegaciones del Subadministrador, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que los documentos enviados con la contestación no evidencian que se haya preparado y aprobado un *Plan de Seguridad*, o algún otro documento que incluya las disposiciones indicadas en el **Hallazgo**.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Deficiencia relacionada con el plan de contingencias de la OTI

Situación

- a. El examen del *Plan de Continuidad de Operaciones de ASR (Plan)*, que nos fue provisto como el plan de contingencias de la OTI el 26 de marzo de 2010, reveló que el mismo no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:
 - La identificación de los integrantes de los grupos de recuperación, a pesar de que detallaba las responsabilidades asignadas a cada uno de ellos
 - Una lista actualizada del personal responsable de ejecutar los procedimientos a seguir en caso de desastres. La lista provista incluía a dos exempleados de la Administración y a una empleada que ya no ocupaba el puesto mencionado
 - El nombre del encargado de activar el *Plan*
 - Una lista de los proveedores principales, que incluya el número de teléfono y el nombre del personal de enlace con la entidad

- Una hoja de cotejo para verificar los daños ocasionados.

Una situación similar se comentó en nuestro informe de auditoría anterior *TI-98-6* del 18 de marzo de 1998.

Criterio

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

Efecto

La situación comentada podría 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 de la Administración.

Causa

La situación comentada se debía, en parte, a que el Administrador no había promulgado una directriz sobre la aprobación, la implantación y la actualización continua del *Plan*.

Comentarios de la Gerencia

En la carta del Subadministrador, este nos indicó, entre otras cosas, lo siguiente:

[...] el documento del Plan de Continuidad de Negocios así como el Plan de Recuperación de Desastres de OTI contienen los integrantes de los grupos de recuperación y la lista actualizada del

personal responsable de ejecutar procedimientos a seguir en caso de desastres. Adicional a estos documentos el Plan de Emergencia de la Agencia contempla estas listas. [sic]

Consideramos las alegaciones del Subadministrador, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que los documentos enviados con la contestación no evidencian que se haya incluido en el *Plan de Continuidad de Negocio* o en el *Plan de Recuperación de Desastres de OTI*, toda la información indicada en el **Hallazgo**.

Véanse las recomendaciones 1 y 3.a.

Hallazgo 3 - Deficiencias en los parámetros de seguridad y en otros controles de acceso lógico de los servidores principales de la red

Situaciones

- a. Al 9 de julio de 2010, la Administración tenía en operación dos servidores principales². El primero controlaba la seguridad local de las cuentas de los usuarios de la Administración y el segundo las cuentas de los usuarios de la Oficina y Secretaría de la Junta de Síndicos y de la Oficina de Auditoría Interna.

El examen efectuado sobre los parámetros de control de acceso y de seguridad definidos en el sistema operativo de estos dos servidores, al 21 de abril y 9 de julio de 2010, respectivamente, reveló las siguientes deficiencias:

- 1) En la opción *Account Lockout Policy* de los servidores existían deficiencias en la configuración de los parámetros, según se indica:
 - Luego de tres intentos para acceder a los recursos de la red sin éxito, la cuenta de acceso se desactivaba solo por media hora (*Account lockout duration*).
 - Se había definido solo media hora en la instrucción para reiniciar el conteo de intentos para acceder a los recursos de la red sin éxito (*Reset account lockout counter after*).

² El nombre de los servidores se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Administrador para comentarios.

- 2) No se había definido la política de auditoría (*Audit Policy*) en los servidores para que el sistema produjera un registro cuando las solicitudes al servidor para validar una cuenta de usuario fueran fallidas (*Audit account logon events*).

Criterios

Las situaciones comentadas son contrarias a lo establecido en el Apartado VIII, Disposiciones Generales, de la *Orden Administrativa Núm. 2006-01, Normas para Establecer los Controles de Seguridad y Regular el Uso de los Sistemas de Información, de la Internet y del Correo Electrónico (Orden Administrativa Núm. 2006-01)*, aprobada el 29 de marzo de 2006 por el Administrador. En esta se dispone que la Administración será responsable de establecer las normas mediante las cuales se asignan las cuentas de acceso, incluidas las medidas de seguridad aplicables, como son las claves de acceso, los controles de acceso a los servidores y los sistemas para auditar el uso de los sistemas, la integridad y la seguridad de los datos, y las comunicaciones que se envían.

Además, las situaciones comentadas son contrarias a lo establecido en la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05*. En esta se establece que 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.

Efectos

Las situaciones comentadas en el **apartado a.1)** propician que personas no autorizadas puedan lograr acceso a la información confidencial mantenida en los sistemas computadorizados, y hacer uso indebido de esta. 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.

La situación comentada en el **apartado a.2)** priva a la gerencia de los medios necesarios para supervisar eficazmente el desempeño de los usuarios y detectar el acceso y uso indebido de los sistemas computadorizados.

Causas

Las situaciones comentadas en el **apartado a.1)** se debían a que en la Administración consideraban que los parámetros de tiempo establecidos eran suficientes, por lo que el Director de la OTI no le había requerido al personal encargado de administrar los sistemas de información que estableciera un tiempo mayor, que permitiera reducir la posibilidad de accesos indebidos.

La situación comentada en el **apartado a.2)** se debía a que el Director de la OTI no había considerado la necesidad de establecer la opción de las políticas de auditoría del sistema para que se produzca un registro cuando las solicitudes al servidor para validar una cuenta de usuario sean fallidas.

Comentarios de la Gerencia

En la carta del Subadministrador, este nos indicó, entre otras cosas, lo siguiente:

[...] nuestros servidores tienen establecidos cantidad de intentos y tiempo de suspensión. Los documentos de OGP que rigen los parámetros de seguridad establecen que hay que tener número de intentos y tiempo de suspensión pero no indican cantidades. La ASR entiende la cantidad de intentos y tiempo de suspensión es suficiente. [sic] [**Apartado a.1)**]

[..] Se definieron las políticas de auditoría en los servidores para los eventos de validar una cuenta de usuario, [...] [sic] [**Apartado a.2)**]

Consideramos las alegaciones del Subadministrador, pero determinamos que el **Hallazgo** prevalece porque las medidas implantadas por la Administración no son suficientes para asegurar la prevención y la detección efectiva de accesos no autorizados a los sistemas de información. Con relación al **apartado a.1)**, el tiempo establecido tanto para que la cuenta permanezca inactiva luego de tres intentos de acceso sin éxito, como para volver a reiniciar el conteo de estos intentos, permite que

personas no autorizadas tengan mayor oportunidad de intentar acceder indebidamente los sistemas de información. Con relación al **apartado a.2)**, la política establecida en el servidor fue para registrar solo los eventos exitosos cuando ocurrieran solicitudes al servidor para validar una cuenta de usuario (*Audit account logon events*), por lo que no se registraban los intentos fallidos. Esto dificulta detectar intentos de acceso no autorizados a los sistemas computadorizados.

Véanse las recomendaciones 1 y 3.b.

Hallazgo 4 - Falta de restricciones para enviar y recibir mensajes de correo electrónico de fuentes externas, y de revisiones periódicas a los registros de los accesos a las páginas de direcciones en Internet

Situaciones

- a. A partir del 5 de marzo de 2010, la OGP mantenía los servidores que permitían a los empleados de la Administración el envío y el recibo de mensajes de correo electrónico. Dichos servidores³ producían diariamente un archivo en el cual se registraban todos los mensajes enviados y recibidos por las cuentas de usuarios (*message tracking logs*). El examen de 32 registros del correo electrónico correspondientes al período del 9 al 15 de mayo de 2010 reveló que los usuarios podían enviar y recibir mensajes de correo electrónico de fuentes externas a la Administración sin ningún tipo de restricción.
- b. La Administración mantenía un servidor³ en la red, el cual permitía el acceso a Internet a los usuarios autorizados. Al 26 de marzo de 2010, la Administración tenía 217 cuentas con los privilegios de acceder a Internet mediante dicho servidor. La Administración utilizaba un *firewall*⁴ para controlar el acceso de los usuarios a Internet. Este *firewall* producía diariamente un archivo en el cual se registraban todas las páginas de direcciones de Internet (*web logs*) que fueron accedidas por las cuentas de usuarios. Sin embargo, el registro de

³ Véase la nota al calce 2.

⁴ Sistema que se coloca entre una red de comunicaciones e Internet. La regla básica es asegurar que todas las comunicaciones entre dicha red e Internet se realicen conforme a las políticas de seguridad de la organización que lo instala. Además, estos sistemas suelen incorporar elementos de privacidad y autenticación, entre otros.

direcciones de Internet visitadas por los usuarios no se examinaba periódicamente. Esto, para auditar las páginas en Internet que acceden los usuarios autorizados.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política Núm. TIG-008, Uso de Sistemas de Información de la Internet y del Correo Electrónico*, de la *Carta Circular Núm. 77-05*. En esta se establece que cada entidad gubernamental será responsable de crear una política interna que regule el uso de los sistemas de información de la entidad, y de las herramientas de Internet y correo electrónico. En esta se indicarán las normas mediante las cuales se asignan las cuentas de correo electrónico, incluidas las medidas de seguridad aplicables, como son los códigos de acceso y las contraseñas, los controles de acceso al servidor, las restricciones en la configuración de correos electrónicos, los sistemas para auditar el uso del sistema, la integridad y la seguridad de los datos, y las comunicaciones enviadas. Esta política se instrumenta, en parte, mediante la restricción de las cuentas de correo electrónico que puedan enviar y recibir mensajes de correo electrónico de fuentes externas a la Administración, y la revisión periódica de los registros de direcciones de Internet visitadas por los usuarios.

Efectos

La situación comentada en el **apartado a.** impide a la Administración mantener un control efectivo de los mensajes de correo electrónico que se envían y se reciben de fuentes externas.

La situación comentada en el **apartado b.** impide la detección temprana de actividades o usos de Internet no autorizados que permita a la gerencia tomar medidas preventivas y correctivas a tiempo.

Causas

La situación comentada en el **apartado a.** se debía, en parte, a la falta de un análisis para determinar los funcionarios y los empleados a quienes debían otorgarse los privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas, de acuerdo con las responsabilidades de sus puestos y con las necesidades de la Administración.

La situación comentada en el **apartado b.** se debía, en parte, a que el *firewall* estaba configurado para que el referido registro se produjera en un formato que el Administrador de Redes no podía analizar, ya que no tenía disponibles las aplicaciones necesarias.

Comentarios de la Gerencia

En la carta del Subadministrador, este nos indicó, entre otras cosas, lo siguiente:

[...] Todo correo electrónico generado desde la ASR o de fuera de ASR hacia nosotros es filtrado por OGP. [...] A esos efectos el correo es filtrado a través de los productos de [...] para correos electrónicos. Debido a los servicios que presta la ASR a Pensionados y Participantes es necesario permitir recibir correos electrónicos de fuentes diversas ya que los Pensionados y Participantes se pueden comunicar con nosotros desde su hogar. [sic] **[Apartado a.]**

Hoy día tenemos filtrado por parte de OGP para el correo electrónico y toda transacción de Internet. De los más de seiscientos empleados que tenía la ASR en el año 2010 solo 217 empleados tenían acceso a Internet para completar sus funciones. Adicional al filtrado de OGP poseemos los servicios de un appliance marca [...] el cual nos protege de virus, spams y sites no aptos para adultos. El software [...] fue eliminado por su obsolescencia. Cada seis meses se corroboran los accesos a Internet con los directores de áreas para asegurarnos solo los que sus tareas lo requieren tengan el acceso. [sic] **[Apartado b.]**

Consideramos las alegaciones del Subadministrador, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que en el examen se encontraron usuarios cuyas funciones no estaban relacionadas con los servicios que presta la Administración a los pensionados y participantes. Además, en la contestación no suministraron evidencia de las evaluaciones realizadas por el personal de la OGP o de la Administración del contenido de las páginas que acceden los usuarios que tienen cuentas con los privilegios de acceder a Internet.

Véanse las recomendaciones 1, 3.c. y d., y 4.

Hallazgo 5 - Falta de normas y de procedimientos para reglamentar la administración, la seguridad y el uso de los sistemas computadorizados

Situación

- a. La OTI es responsable de brindar apoyo tecnológico a todas las áreas y las oficinas de la Administración. Además, es responsable de custodiar la información electrónica de la Administración, desarrollar y mantener las aplicaciones, y ofrecer apoyo a los empleados en el uso del equipo de computadora. Al 14 de junio de 2010, la Administración no había preparado las normas ni los procedimientos necesarios para reglamentar los siguientes procesos relacionados con la administración, la seguridad y el uso de los sistemas computadorizados:
- La detección, la notificación y la respuesta a incidentes de seguridad
 - El otorgamiento, la modificación, o la cancelación del acceso local y remoto a los usuarios⁵
 - La administración de la seguridad y el acceso físico a la OTI y al equipo de sistemas de información
 - La prevención y la detección de los accesos no autorizados
 - El desarrollo y la adquisición de las aplicaciones⁵

⁵ Para este proceso se había preparado un procedimiento el cual estaba en etapa de borrador.

- La identificación, la selección, la instalación y la modificación del sistema operativo de las computadoras
- La instalación y la configuración de la red de comunicaciones
- El mantenimiento al equipo, la administración y la documentación de los problemas y los cambios, de manera que se prevengan las interrupciones no esperadas
- El uso y la revisión de los programas de utilería
- Los cambios a efectuar en los sistemas y las pruebas de los mismos, incluidos los que ocurren en situaciones de emergencia⁶
- La preparación y la custodia de los respaldos de información en un lugar interno y externo⁶
- La disposición del equipo computadorizado, y de la información sensitiva y de programas antes de transferir o disponer de los equipos computadorizados y los medios de almacenamiento de información

Una situación similar se comentó en el informe de auditoría anterior *TI-98-6*, y en el *Informe de Auditoría OA-10-14* del 30 de noviembre de 2009 de la Oficina de Auditoría Interna de la Administración.

Crterios

La situación comentada es contraria a lo establecido en el Artículo 4-103, inciso 6 de la *Ley Núm. 447*. En esta se establece, entre otras cosas, que el Administrador tiene la obligación de preparar los reglamentos necesarios para el control de las operaciones de la Administración y remitir los mismos para la revisión y la aprobación de la Junta de Síndicos.

Además, la situación comentada es contraria a lo establecido en la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05*. En esta se establece que las entidades gubernamentales tienen la responsabilidad de desarrollar políticas y directrices generales que le permitan establecer controles

⁶ Véase la nota al calce 5.

adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Además, se aparta de lo establecido en la *Política Núm. TIG-007, Disposición de Equipo y Licencias* de dicha *Carta Circular*. En esta se establecen los mecanismos que las entidades gubernamentales implantarán para asegurarse de que se disponga apropiadamente del equipo de tecnologías de información, así como de los programas que tuviesen los mismos instalados, si alguno.

Efectos

La situación comentada podría ocasionar que las operaciones de los sistemas de información de la Administración 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. Además, podría exponer al personal, a los equipos y a la información de la Administración a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

Causa

La situación comentada se atribuye, principalmente, a que el Administrador no le había requerido al Director de la OTI que desarrollara y remitiera para su revisión y aprobación, y la de la Junta de Síndicos, las normas y los procedimientos escritos necesarios para reglamentar los procesos indicados.

Comentarios de la Gerencia

En la carta del Subadministrador, este nos indicó, entre otras cosas, lo siguiente:

En el año 2009, la Oficina de Tecnología de Información carecía de reglamentaciones internas teniendo un sistema con falta de controles internos. Esta oficina contaba solo con un (1) procedimiento, una (1) orden administrativa y cinco (5) formularios. A partir del año 2010, en un esfuerzo por cumplir con las disposiciones 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 y las doce (12) Políticas de Tecnología de la Oficina de Gerencia y Presupuesto, se implementaron dos (2) nuevos procedimientos

adicionales, cuatro (4) estándares, dos (2) manuales de servicios y trece (13) nuevos formularios fortaleciendo los sistemas teniendo mas y mejores controles internos que garanticen el uso adecuado de los recursos de los sistemas de información y su seguridad. [sic]

Véanse las recomendaciones 1 y 3.e.

Hallazgo 6 - Falta de un registro de programas instalados en cada computadora

Situación

- a. Al 28 de junio de 2010, la OTI no mantenía un registro de los programas adquiridos e instalados en cada computadora que incluyera, entre otras cosas, el número de licencia de los programas instalados, el nombre del usuario, el número de propiedad, la descripción de la computadora donde estaban instalados los programas y el costo de los mismos.

Criterio

La situación comentada es contraria a lo establecido en la *Política Núm. TIG-008* de la *Carta Circular Núm. 77-05*. En esta se establece que los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas agencias y solo pueden utilizarse para fines estrictamente oficiales y legales. Además, los programas y los recursos utilizados en los sistemas de información de las entidades gubernamentales deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas solo podrán ser instalados por el personal autorizado. Además, no podrán instalarse programas sin la autorización previa del Departamento de Sistemas de Información, aunque sean programas libre de costo.

Efectos

La situación comentada impide ejercer un control eficaz de los programas y de las licencias correspondientes. Además, propicia la instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para la Administración. También dificulta nuestra gestión fiscalizadora.

Causa

La situación comentada se debía a que el Director de la OTI no había tomado las medidas necesarias para mantener un registro y un control adecuado de los programas adquiridos e instalados en las computadoras de la Administración.

Comentarios de la Gerencia

En la carta del Subadministrador, este nos indicó, entre otras cosas, lo siguiente:

Utilizamos la aplicación provista por OGP para el control de licencias en las estaciones de trabajo y servidores el cual genera el informe que acompañamos como ejemplo. La Oficina de Tecnología de Información mantiene un inventario de todas las licencias instaladas en los servidores de la OTI así como de las estaciones de trabajo. Estas se encuentran bajo llave en la OTI y la lista es actualizada cada vez que se obtiene una licencia. [sic]

Consideramos las alegaciones del Subadministrador, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que el informe que produce la aplicación utilizada para el control de las licencias en las estaciones de trabajo y los servidores no contiene la información del nombre del usuario, el número de licencia del programa, la descripción de la computadora donde estaban instalados los programas y el costo de los mismos.

Véanse las recomendaciones 1 y 3.f.

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

1. Tomar las medidas necesarias para asegurarse de que el Administrador de la Administración cumpla con las recomendaciones de la 2 a la 4. [Hallazgos del 1 al 6]

Al Administrador de la Administración de los Sistemas de Retiro de los Empleados del Gobierno y la Judicatura

2. Realizar las gestiones necesarias para que la Administración cuente con un plan de seguridad que incluya los criterios descritos en el **Hallazgo 1**. Además, asegurarse de que se realicen pruebas periódicas al plan de seguridad, y que el mismo se divulgue a los empleados y a los funcionarios concernientes.
3. Ejercer una supervisión efectiva sobre el Director de la OTI para asegurarse de que:
 - a. Revise, si aún no se ha hecho, el *Plan de Continuidad de Operaciones de ASR* para que incluya los aspectos comentados en el **Hallazgo 2** y lo remita para aprobación.
 - b. El personal encargado de administrar los sistemas efectúe las modificaciones en los parámetros de seguridad del sistema operativo para:
 - 1) Establecer un tiempo mayor al actualmente definido tanto para que la cuenta permanezca inactiva, luego de tres intentos de acceso sin éxito, como para volver a reiniciar el conteo de dichos intentos. Esto, de manera que se reduzcan las posibilidades de que personas no autorizadas puedan acceder indebidamente los sistemas de información. [Hallazgo 3-a.1]
 - 2) Establecer las políticas de auditoría del sistema para que este produzca un registro cuando las solicitudes al servidor para validar una cuenta de usuario sean fallidas. [Hallazgo 3-a.2]

- c. Restrinja los derechos y los privilegios para que solamente el personal clave de la Administración pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis realizado por la gerencia. **[Hallazgo 4-a.]**
 - d. Identifique y evalúe la adquisición de una aplicación para analizar los registros de direcciones en Internet visitadas por los usuarios y registradas en el servidor que provee dicho servicio; adiestre al Administrador de Redes sobre la utilización de la misma; y le asigne la responsabilidad de examinar periódicamente dichos registros. **[Hallazgo 4-b.]**
 - e. Redacte las normas y los procedimientos necesarios para reglamentar los procesos que se comentan en el **Hallazgo 5** y los remita para su revisión y la aprobación de la Junta de Síndicos.
 - f. Mantenga un registro de los programas adquiridos e instalados en las computadoras de la Administración que contenga, entre otra información, el número de la licencia y el costo de los programas instalados, el nombre del usuario, el número de propiedad y la descripción de la computadora donde están instalados los mismos. Esto, con el fin de mantener un inventario de los programas y prevenir la instalación de programas no autorizados. **[Hallazgo 6]**
4. Realizar un análisis para determinar el personal clave de la Administración que requiera tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. Luego de efectuado el análisis, remitir la lista del personal clave a la OTI. **[Hallazgo 4-a.]**

AGRADECIMIENTO

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

Por:

Ugicoria del Contralor
Fernán Maldonado

ANEJO 1

ADMINISTRACIÓN DE LOS SISTEMAS DE RETIRO
DE LOS EMPLEADOS DEL GOBIERNO Y LA JUDICATURA
OFICINA DE TECNOLOGÍA DE INFORMACIÓN
**MIEMBROS PRINCIPALES DE LA JUNTA DE SÍNDICOS
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Carlos M. García Rodríguez	Presidente	15 mar. 10	31 ag. 10
Sr. Omar Negrón Judice	Vicepresidente	15 mar. 10	31 ag. 10
Sr. Juan C. Puig Morales	Secretario	15 mar. 10	31 ag. 10

ANEJO 2

ADMINISTRACIÓN DE LOS SISTEMAS DE RETIRO
DE LOS EMPLEADOS DEL GOBIERNO Y LA JUDICATURA
OFICINA DE TECNOLOGÍA DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Héctor M. Mayol Kauffmann	Administrador	15 mar. 10	31 ag. 10
Sr. Manuel Iglesias Beléndez	Subadministrador	15 mar. 10	31 ag. 10
Sr. José L. Villafañe Ramos	Administrador Auxiliar de Administración	15 mar. 10	31 ag. 10
Sr. Fernando L. Arroyo Ortiz	Director de la Oficina de Servicios Administrativos	15 mar. 10	31 ag. 10
Sr. Daniel Casas Meléndez	Director de la Oficina de Tecnología de Información	15 mar. 10	31 ag. 10
Sr. Edwin Mercado Brignoni	Director de la Oficina de Auditoría Interna	15 mar. 10	31 ag. 10

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

**PRINCIPIOS PARA
LOGRAR UNA
ADMINISTRACIÓN
PÚBLICA DE
EXCELENCIA**

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-08-32* del 27 de junio de 2008, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensión 2124, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico Querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

**INFORMACIÓN SOBRE
LOS INFORMES DE
AUDITORÍA**

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el Administrador de Documentos al (787) 294-0625 o (787) 200-7253, extensión 536.

**INFORMACIÓN DE
CONTACTO***Dirección física:*

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Internet:

<http://www.ocpr.gov.pr>

Correo electrónico:

ocpr@ocpr.gov.pr

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069