

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 de la Montaña
- Asuntos de la Mujer
- Asuntos Internos
- Reglas y Calendario

COMISIONES ESPECIALES

- Puerto de las Américas
- Derecho de Autodeterminación del Pueblo de Puerto Rico

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



Secretaría

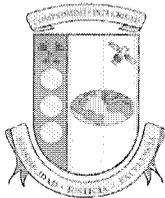
MANUEL A. TORRES NIEVES
Secretario del Senado

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

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



Estado Libre Asociado de Puerto Rico
Oficina del Contralor

RECIBIDO
OFIC. PRESIDENTE SENADO PR
THOMAS RIVERA SCHATZ

2009 AUG 19 AM 11:10

Manuel Díaz Saldaña
Contralor

19 de agosto de 2009

PRIVILEGIADA Y CONFIDENCIAL

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

Estimado señor Presidente:

Le incluimos copia del **Informe de Auditoría TI-10-04** de la Oficina de Sistemas de Información de la Oficina de Servicios con Antelación al Juicio, adscrita al Departamento de Corrección y Rehabilitación, emitido por esta Oficina el 14 de agosto de 2009. Publicaremos dicho **Informe** en nuestra página de Internet: <http://www.ocpr.gov.pr> para conocimiento de los medios de comunicación y de otras partes interesadas.

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

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

Cordialmente,

Manuel Díaz Saldaña

Anejo

RECIBIDO OFICINA
PRESIDENTE SENADO
2009 AUG 19 PM 3:56

PO_5484

INFORME DE AUDITORÍA TI-10-04
14 de agosto de 2009
**DEPARTAMENTO DE CORRECCIÓN
Y REHABILITACIÓN**
**OFICINA DE SERVICIOS CON
ANTELACIÓN AL JUICIO**
OFICINA DE SISTEMAS DE INFORMACIÓN
(Unidad 5378 - Auditoría 13043)

Período auditado: 6 de junio de 2007 al 15 de abril de 2008

CONTENIDO

	Página
INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....	3
RESPONSABILIDAD DE LA GERENCIA	5
ALCANCE Y METODOLOGÍA.....	6
OPINIÓN.....	7
RECOMENDACIONES	7
AL SECRETARIO DE CORRECCIÓN Y REHABILITACIÓN	7
AL DIRECTOR EJECUTIVO DE LA OFICINA DE SERVICIOS CON ANTELACIÓN AL JUICIO	7
CARTAS A LA GERENCIA.....	12
COMENTARIOS DE LA GERENCIA.....	13
AGRADECIMIENTO.....	14
RELACIÓN DETALLADA DE HALLAZGOS.....	15
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO.....	15
HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA OFICINA DE SERVICIOS CON ANTELACIÓN AL JUICIO, ADSCRITA AL DEPARTAMENTO DE CORRECCIÓN Y REHABILITACIÓN	16
1 - Cuentas para acceder a Internet y al correo electrónico utilizadas para fines ajenos a la gestión pública, y falta de controles de los mensajes de correo electrónico recibidos y enviados de fuentes externas a la OSAJ	16
2 - Falta de un Plan de Seguridad y de un procedimiento para el manejo de incidentes	19
3 - Falta de un Plan de Continuidad de Negocios, deficiencias en el Plan de Contingencias, falta de pruebas o simulacros que certificaran la efectividad del Plan y de documentación fuera de la OSI.....	22
4 - Falta de acuerdos para mantener los respaldos fuera del Centro y de un centro alternativo de recuperación de sistemas de información.....	26

5 - Falta de normas y de procedimientos escritos para la administración, la seguridad y el uso de los sistemas computadorizados.....	28
6 - Deficiencia relacionada con el formulario utilizado para solicitar la creación, la modificación y la cancelación de las cuentas de acceso de los usuarios	30
7 - Deficiencias relacionadas con la configuración y la estructura de seguridad para acceder a la Red	32
8 - Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de la Red, y falta de revisiones periódicas de las bitácoras (<i>logs</i>) de eventos de estos servidores	34
9 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información	38
10 - Falta de controles en el reclutamiento de personal de la OSI y de procedimientos para el traslado y la separación del personal que tiene acceso a los sistemas de información de la OSAJ	40
11 - Falta de adiestramientos periódicos a la OPI y al Administrador de la Red sobre sus funciones y la seguridad de los sistemas, y a los funcionarios y empleados sobre el uso y el control de los equipos y sistemas computadorizados, y falta de un registro de los adiestramientos recibidos por el personal de la OSI	42
ANEJO - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO	47

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

14 de agosto de 2009

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 Sistemas de Información (OSI) de la Oficina de Servicios con Antelación al Juicio (OSAJ), adscrita al Departamento de Corrección y Rehabilitación (Departamento), 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 la **Sección 22 del Artículo III de la Constitución del Estado Libre Asociado de Puerto Rico** y en la **Ley Núm. 9 del 24 de julio de 1952**, según enmendada.

Determinamos emitir dos informes de esta auditoría. Este es el primer informe y contiene el resultado de nuestro examen sobre la administración del programa de seguridad, los controles de acceso y la evaluación de la continuidad del servicio establecidos en la OSI, y la función de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La OSAJ se creó mediante la **Ley Núm. 177 del 12 de agosto de 1995, Ley de la Oficina de Servicios con Antelación al Juicio**, según enmendada, y comenzó operaciones el 15 de noviembre de 1995. Es una entidad autónoma adscrita al Departamento de Corrección y Rehabilitación. Su misión es propiciar que se eliminen los efectos de la desigualdad económica en la concesión de la libertad provisional al imputado de un delito y reducir el uso innecesario

de las cárceles, y de esa manera ayudar a reducir el hacinamiento en éstas. En el cumplimiento de su función, la OSAJ se encarga de investigar y evaluar a todo imputado de delito y de ofrecer sus recomendaciones en cuanto a la posibilidad de decretar la libertad provisional del imputado, en la alternativa o adicionalmente a la imposición de fianza. Además, en la OSAJ se preparan informes escritos que se presentan en los tribunales en la vista para la imposición de fianza. El Juez, luego de considerar los informes escritos presentados por la OSAJ, puede imponer o modificar fianzas monetarias o conceder la libertad provisional. Si el Juez le concede al imputado libertad provisional sujeto a condiciones, con o sin fianza, éste es supervisado por la OSAJ hasta la emisión de un fallo o veredicto, o hasta que termine el proceso judicial. La OSAJ supervisa el cumplimiento de las condiciones de libertad provisional que le fueron impuestas al imputado e informa con premura a los tribunales y a cualquier otro funcionario pertinente de cualquier incumplimiento de dichas condiciones.

La OSAJ es un Administrador Individual para fines de la **Ley Núm. 184 del 3 de agosto de 2004, Ley para la Administración de los Recursos Humanos en el Servicio Público del Estado Libre Asociado de Puerto Rico**, según enmendada. Ésta promulga su reglamentación, la cual es aprobada por el Secretario de Corrección y Rehabilitación. El Secretario establece la política pública de la OSAJ para implantar las disposiciones de la **Ley Núm. 177**. La OSAJ es administrada por un Director Ejecutivo, quien es nombrado por el Gobernador. Entre sus funciones está la de reclutar y nombrar el personal, preparar informes al Secretario sobre la labor realizada por la OSAJ, y adoptar y promulgar los reglamentos que sean necesarios para implantar las disposiciones de la **Ley Núm. 177**.

Para llevar a cabo sus funciones la OSAJ cuenta con la siguiente estructura organizacional: Oficina del Director, Oficina del Subdirector, Oficina de Administración, Oficina de Recursos Humanos, OSI, Oficina de Supervisión y Seguimiento, y la Unidad Especializada de Investigaciones y Arrestos.

La OSI era dirigida por un Oficial Principal de Informática (OPI) y contaba con un Administrador de Redes¹ y una Administradora de Sistemas de Oficina.

La OSAJ brinda sus servicios a través de 14 centros regionales de servicios localizados en las regiones judiciales de: Aguadilla, Aibonito, Arecibo, Bayamón, Caguas, Carolina, Fajardo, Guayama, Humacao, Mayagüez, Ponce, Río Grande, San Juan y Utuado.

Los gastos operacionales de la OSI eran sufragados del presupuesto operacional de la OSAJ, que para los años fiscales 2006-07 y 2007-08 fue de \$7,627,000 y \$7,422,000, respectivamente.

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

La OSAJ cuenta con una página de Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.osaj.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.

¹ La OSAJ contaba con un Administrador de Redes del 6 de junio de 2007 al 31 de enero de 2008.

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**, 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**. Ambas **cartas circulares** se pueden acceder a través de nuestra página de Internet: <http://www.ocpr.gov.pr>.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 6 de junio de 2007 al 15 de abril de 2008. En algunos aspectos examinamos 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
- Análisis de información suministrada por fuentes externas
- Pruebas y análisis de información financiera, de procedimientos de control interno y de otros procesos
- Confirmaciones de información pertinente

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne a la administración del programa de seguridad, los controles de acceso, la evaluación de la continuidad del servicio y la función de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados no se realizaron conforme a las normas generalmente aceptadas en este campo, según los **hallazgos del 1 al 11** de este **Informe**, clasificados como principales.

En la parte de este **Informe** titulada **RELACIÓN DETALLADA DE HALLAZGOS** se presentan dichos **hallazgos**.

RECOMENDACIONES

AL SECRETARIO DE CORRECCIÓN Y REHABILITACIÓN

1. Ver que el Director Ejecutivo de la OSAJ cumpla con las **recomendaciones de la 3 a la 9** de este **Informe**. [**Hallazgos del 1 al 8, 10 y 11**]
2. Asegurarse de que la Secretaría Auxiliar de Auditoría: [**Hallazgo 9**]
 - a. Establezca un programa de adiestramiento continuo para capacitar a los auditores internos del Departamento en las técnicas de auditoría de sistemas de información computadorizados.
 - b. Realice las gestiones necesarias para que se examinen periódicamente los controles y las operaciones de los sistemas de información computadorizados del Departamento y de las entidades adscritas.

AL DIRECTOR EJECUTIVO DE LA OFICINA DE SERVICIOS CON ANTELACIÓN AL JUICIO

3. Realizar un análisis para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado para acceder a Internet. Luego de efectuado el análisis, someter la lista de las páginas autorizadas a la OSI. [**Hallazgo 1-a.**]

4. Realizar un análisis para determinar el personal clave de la OSAJ que requiera tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. Luego de efectuado el análisis, someter la lista del personal clave a la OSI. **[Hallazgo 1-b.]**
5. Ejercer una supervisión efectiva sobre el OPI para asegurarse de que:
 - a. Realice las inspecciones periódicas necesarias para verificar el uso adecuado de las cuentas de acceso a Internet y correo electrónico. **[Hallazgo 1]**
 - b. Colabore con la persona encargada de ofrecer los adiestramientos durante las orientaciones a los usuarios sobre las normas y los procedimientos de los sistemas computadorizados. **[Hallazgo 1]**
 - c. El encargado de administrar la red de comunicaciones (Red) limite el acceso a las páginas electrónicas que son necesarias para cumplir con los deberes y las responsabilidades del personal autorizado para acceder a Internet, según el análisis realizado por la gerencia. **[Hallazgo 1-a.]**
 - d. Restrinja los derechos y privilegios para que solamente el personal clave de la OSAJ pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis realizado por la gerencia. **[Hallazgo 1-b.]**
 - e. Prepare y someta para aprobación el **Plan de Seguridad** en el que se establezcan los proyectos, las tareas y las actividades requeridos para proteger al personal y a los activos del sistema de información. **[Hallazgo 2-a.]**
 - f. Prepare y someta para aprobación el procedimiento para el manejo de incidentes no esperados. Como parte del procedimiento, se debe requerir que se documenten todos los incidentes y cómo se resolvieron, de manera que, cuando se repitan los mismos, se puedan resolver en el menor tiempo posible sin afectar los sistemas de información y la continuidad de las operaciones. **[Hallazgo 2-b.]**

- g. Revise el **Plan de Contingencia de Emergencia** para que incluya los aspectos comentados en el **Hallazgo 3-b.** y lo someta para aprobación.
- h. Prepare los procedimientos de prueba o simulacros necesarios para verificar la efectividad del **Plan de Contingencia de Emergencia** y los someta para aprobación. **[Hallazgo 3-c.]**
- i. Efectúe pruebas o simulacros del **Plan de Contingencia de Emergencia**, por lo menos, dos veces al año y mantenga la documentación de las estrategias utilizadas y los resultados de las pruebas. **[Hallazgo 3-c.]**
- j. Mantenga una copia del **Plan de Contingencia de Emergencia** aprobado, en un lugar seguro fuera de los predios de la OSAJ. **[Hallazgo 3-d.]**
- k. Prepare y someta para aprobación los procedimientos para preparar y mantener los respaldos (*backups*) de los datos y de la documentación de los programas y las aplicaciones que incluya un acuerdo, por escrito, para almacenar los mismos en un lugar seguro fuera de los predios de la Oficina Central de la OSAJ. **[Hallazgo 4-a.]**
- l. Prepare y someta para aprobación las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el **Hallazgo 5.**
- m. Incluya en el formulario **Registro de Acceso** la información necesaria de acuerdo con lo comentado en el **Hallazgo 6** y someta el mismo para aprobación.
- n. Establezca una configuración que incluya una Zona Desmilitarizada (*DMZ*, por sus siglas en inglés)² que limite el acceso desde Internet a los servidores de la Red de la OSAJ y viceversa. Esto es necesario para proteger la Red de ataques cibernéticos y

² En seguridad informática, una zona desmilitarizada (*DMZ*, por sus siglas en inglés) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una *DMZ* es que las conexiones desde la red interna y la externa a la *DMZ* estén permitidas, mientras que las conexiones desde la *DMZ* sólo se permitan a la red externa. La *DMZ* se utiliza para ubicar servidores que son necesarios que sean accedidos desde fuera, como servidores de *E-mail*, *Web* y *DNS (Domain Name Service)*.

- para evitar que personas externas y no autorizadas puedan acceder a ésta y comprometer la seguridad de sus sistemas. **[Hallazgo 7-a.]**
- o. Configure un servidor para que sólo provea el servicio de mensajería y transfiera el servicio ofrecido para la página *Web* a otro servidor dedicado para dicho propósito. **[Hallazgo 7-b.]**
- p. Supervise las funciones del personal encargado de administrar los sistemas para que configure las opciones de seguridad que proveen los sistemas operativos para:
- 1) Restringir el horario de acceso a los recursos de la Red, según las funciones y las responsabilidades de cada usuario, y activar en los servidores la opción para desconectar automáticamente las cuentas de acceso cuando éstas son utilizadas para acceder los recursos de la Red fuera de horas laborables. **[Hallazgo 8-a.1)a]**
 - 2) Activar las opciones correspondientes en la pantalla de políticas de auditorías (*Audit Policies*) que se mencionan en el **Hallazgo 8-a.1)b** y **2)**, de manera que se pueda mantener un rastro de las actividades realizadas en los servidores de la OSAJ.
- q. Realice las gestiones necesarias para eliminar las cuentas de acceso de los usuarios que hayan cesado sus funciones en la OSAJ. **[Hallazgo 8-a.1)c]**
- r. Prepare para aprobación los procedimientos para la administración de la Red en los cuales se establezcan, entre otras cosas, las directrices para que el personal encargado de administrar los sistemas: **[Hallazgo 8-b.]**
- 1) Configure las pantallas correspondientes para que se mantengan las bitácoras (*logs*) de auditoría y no se eliminen los eventos registrados del servidor principal de la Red.

- 2) Revise periódicamente los eventos registrados en los servidores principales de la Red y, de ser necesario, tome de inmediato las medidas preventivas y correctivas correspondientes.
 - 3) Grabe el contenido del registro en un medio de almacenamiento alternativo antes de que se complete la capacidad de almacenamiento del mismo en el Sistema.
- s. Establezca, en coordinación con la Directora de Recursos Humanos, un plan para ofrecer adiestramientos técnicos periódicos al personal a cargo de administrar los sistemas de información de la OSAJ y un programa de adiestramiento por escrito, para ofrecer orientaciones periódicas a los empleados de la OSAJ sobre la seguridad de los sistemas de información. En el mismo se debe ofrecer información sobre la seguridad de acceso lógico y físico, el manejo y el control de las contraseñas, la producción de respaldos, y las normas de uso de los equipos y sistemas de información computadorizados. Además, se deben ofrecer orientaciones periódicas a todo el personal de la OSAJ sobre los planes establecidos de seguridad y de contingencia. **[Hallazgo 11-a. y b.]**
6. Realizar las gestiones pertinentes para asegurarse de que se prepare un **Plan de Continuidad de Negocios**, que incluya un **Plan para la Recuperación de Desastres** y un **Plan para la Continuidad de las Operaciones**. Este **Plan** debe ser sometido para revisión y aprobación. Una vez éste sea aprobado, tomar las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la OSAJ. Además, asegurarse de que sea distribuido a los funcionarios y empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 3-a.]**
 7. Formalizar un acuerdo escrito con un centro alternativo que acepte la utilización de sus respectivos equipos en casos de desastres o emergencias en la OSAJ, o considerar establecer su propio centro alternativo en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OSI. **[Hallazgo 4-b.]**

8. Ver que los supervisores de las oficinas y unidades de la OSAJ cumplan con lo dispuesto en los **artículos VI y VII del Reglamento Interno sobre Normas y Procedimientos sobre el Uso de los Sistemas Electrónicos (Reglamento Interno)**, aprobado el 15 de noviembre de 2006 por el Secretario de Corrección y Rehabilitación para el Departamento y sus agencias componentes. [**Hallazgo 8-a.1)c)**]

9. Ejercer una supervisión eficaz sobre la Directora de Recursos Humanos para asegurarse de que:
 - a. Refiera a la Unidad Especializada de Investigaciones y Arrestos para consideración e investigación el historial personal de todo candidato a ocupar un puesto en la OSAJ. [**Hallazgo 10-a.**]

 - b. Prepare y refiera para aprobación las normas y los procedimientos necesarios para establecer acuerdos de confidencialidad con los empleados y los consultores de la OSAJ. [**Hallazgo 10-a.**]

 - c. Prepare y refiera para aprobación las normas y los procedimientos necesarios para el manejo de las transferencias y la separación de empleados. [**Hallazgo 10-b.**]

 - d. Cumpla con las disposiciones establecidas en la **Sección 6.5 de la Ley Núm. 184** para proveer los adiestramientos requeridos y necesarios a sus recursos humanos, y mantener evidencia y un historial de los adiestramientos recibidos por cada empleado. [**Hallazgo 11-c.**]

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este **Informe** se sometió para comentarios al Secretario de Corrección y Rehabilitación, Hon. Carlos M. Molina Rodríguez, al Director Ejecutivo de la OSAJ, Lic. Rolando Rivera Guevárez, al ex Secretario de Corrección y Rehabilitación, Lic. Miguel A. Pereira Castillo, y a la ex Directora Ejecutiva de la OSAJ, Lic. Waleska Casiano Matos, en cartas del 11 de mayo de 2009. La carta del licenciado Pereira Castillo fue tramitada por correo certificado con acuse de recibo, a una dirección provista por el Departamento.

El 28 de mayo de 2009 se envió una carta de seguimiento al ex Secretario de Corrección y Rehabilitación y al Director Ejecutivo de la OSAJ y se les concedió hasta el 5 de junio de 2009 para someter los comentarios al borrador de los **hallazgos** de este **Informe**.

El 4 de junio de 2009 el ex Secretario de Corrección y Rehabilitación envió un mensaje por correo electrónico para informar que no había recibido el informe al que se hace referencia en la carta del 28 de mayo de 2009.

El 5 de junio de 2009 nuestra Oficina se comunicó con el ex Secretario de Corrección y Rehabilitación para verificar su dirección. Éste nos indicó que la dirección a la cual enviamos el borrador de los **hallazgos** del **Informe**, en carta del 11 de mayo de 2009, era la correcta. Para esa misma fecha, se le envió una carta con el borrador de los **hallazgos** de este **Informe** y se le concedió hasta el 22 de junio de 2009 para someter los comentarios al mismo.

El 5 y 24 de junio de 2009 se recibieron en la Oficina, devueltas por el correo, las cartas del 11 de mayo y 5 de junio de 2009 con el borrador de los **hallazgos** de este **Informe** que le fue referido al ex Secretario de Corrección y Rehabilitación debido a que las mismas no fueron reclamadas.

COMENTARIOS DE LA GERENCIA

El Director Ejecutivo contestó el borrador de los **hallazgos** de este **Informe** mediante carta del 4 de junio de 2009. Además, la ex Directora Ejecutiva y el Secretario de Corrección y Rehabilitación contestaron el mismo mediante cartas del 26 de mayo de 2009. Las observaciones sometidas por dichos funcionarios fueron consideradas en la redacción final del informe. Algunas de sus observaciones se incluyen en la parte de este **Informe** titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección **HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA OFICINA DE SERVICIOS CON ANTELACIÓN AL JUICIO, ADSCRITA AL DEPARTAMENTO DE CORRECCIÓN Y REHABILITACIÓN**.

AGRADECIMIENTO

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

Oficina del Contralor
Por: 

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, 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.

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

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

Al final de cada hallazgo se hace referencia a las recomendaciones que se incluyen en el informe para que se tomen las medidas necesarias sobre los errores, irregularidades o actos ilegales señalados.

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

correspondiente en la sección de HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA OFICINA DE SERVICIOS CON ANTELACIÓN AL JUICIO, ADSCRITA AL DEPARTAMENTO DE CORRECCIÓN Y REHABILITACIÓN, 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 OFICINA DE SISTEMAS DE INFORMACIÓN DE LA OFICINA DE SERVICIOS CON ANTELACIÓN AL JUICIO, ADSCRITA AL DEPARTAMENTO DE CORRECCIÓN Y REHABILITACIÓN

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

Hallazgo 1 - Cuentas para acceder a Internet y al correo electrónico utilizadas para fines ajenos a la gestión pública, y falta de controles de los mensajes de correo electrónico recibidos y enviados de fuentes externas a la OSAJ

- a. La OSAJ mantenía un servidor³ en la Red que permitía acceso a Internet a los usuarios autorizados. Dicho servidor 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. Al 11 de diciembre de 2007 la OSAJ tenía 172 cuentas para acceder a Internet mediante dicho servidor. Nuestro examen sobre el registro de direcciones de Internet visitadas por los usuarios y registradas en el servidor del 6 al 12 de febrero de 2008 reveló que 10 cuentas se utilizaron para examinar páginas de Internet con contenidos ajenos a los intereses y a la gestión pública.
- b. La OSAJ mantenía un servidor³ en la Red que permitía a los empleados el envío y el recibo de mensajes de correo electrónico. Dicho servidor producía 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 60 registros del correo electrónico correspondientes al 1, 12, 19 y 26 de noviembre de 2007 reveló que los usuarios podían recibir y enviar

³ El nombre del servidor se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al Secretario y al ex Secretario de Corrección y Rehabilitación, y al Director Ejecutivo y a la ex Directora Ejecutiva de la OSAJ.

mensajes de correo electrónico de fuentes externas a la OSAJ sin ningún tipo de restricción. Además, identificamos tres cuentas que se utilizaron para enviar mensajes de correo electrónico con contenidos ajenos a los intereses y a la gestión pública.

En la **Sección 9 del Artículo VI de la Constitución del Estado Libre Asociado de Puerto Rico** se establece que sólo se dispondrá de las propiedades y de los fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado y en todo caso por autoridad de ley.

En el **Artículo 3.2(c) de la Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental**, según enmendada, se dispone, entre otras cosas, que ningún funcionario o empleado público utilizará propiedad pública para obtener directa o indirectamente ventajas, beneficios o privilegios que no estén permitidos por ley.

En las **Normas sobre el Uso de los Sistemas Electrónicos**, emitidas el 29 de junio de 2007 por la Directora Ejecutiva, se establece, entre otras cosas, que la información contenida en las computadoras, los servicios asociados tanto internos como externos, los mensajes de correspondencia electrónica (*e-mails*), información de Intranet o Internet y los documentos y programas existentes, no podrán reproducirse o utilizarse para fines ajenos a las funciones y poderes de la Institución.

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, 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, se establece, entre otras cosas, lo siguiente:

- Los sistemas de información y las herramientas asociadas, como el correo electrónico y la Internet, sólo podrán ser utilizados por personal debidamente autorizado. Será responsabilidad de cada entidad gubernamental definir las tareas que conllevan acceso a tal herramienta. El uso de tales recursos constituye un privilegio otorgado con el propósito de agilizar los trabajos de la entidad gubernamental y no es un derecho.

- Los sistemas de comunicación y acceso a Internet son propiedad de la entidad gubernamental y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la entidad y nunca con fines no oficiales o para actividades personales o con fines de lucro.
- El correo electrónico podrá utilizarse únicamente para propósitos oficiales relativos a las funciones de la agencia. Se prohíbe el uso del mismo para asuntos no oficiales o actividades personales con fines de lucro o en menoscabo de la imagen de la entidad gubernamental o sus empleados.

El uso de las cuentas para acceder a Internet y al correo electrónico pertenecientes a la OSAJ para procesar documentos y examinar archivos de carácter privado es contrario al interés público y desvirtúa los propósitos para los cuales fueron creadas y asignadas. Además, provee al funcionario o empleado que indebidamente los utiliza unas ventajas, beneficios y privilegios que no están permitidos por ley.

Por otro lado, el acceso a páginas de Internet y a mensajes de correo electrónico ajenos al fin público expone a los equipos y a la información sensible almacenada en los sistemas a riesgos innecesarios como son la propagación de virus, *spyware*⁴, *phishing*⁵, *spoofing*⁶, *spamming*⁷ y ataques de negación de servicios⁸, entre otros, que pudieran afectar la continuidad de las operaciones.

⁴ Es un programa que se instala inadvertidamente en una computadora y que propaga sin autorización información sobre el usuario de la computadora y sus hábitos de utilización de Internet.

⁵ Es un tipo de ataque de correo electrónico que trata de convencer a un usuario de que el originador es auténtico, pero con la intención de obtener información.

⁶ Es un ataque activo en el que el intruso presenta una identidad que no es la identidad original. En este ataque el propósito es obtener acceso a los datos sensibles o a los recursos de los sistemas de información computadorizados a los que no se permite el acceso bajo la identidad original.

⁷ Es el envío de correspondencia electrónica a cientos o a miles de usuarios.

⁸ Ocurren cuando una computadora conectada a Internet es inundada con datos y solicitudes que deben ser atendidas. La máquina se dedica exclusivamente a atender estos mensajes y queda imposibilitada de realizar otras actividades.

Las situaciones comentadas se debían, en parte, a la falta de:

- Orientaciones periódicas a los usuarios de los sistemas de información computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso y manejo de las cuentas para acceder a Internet y al correo electrónico.
- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento de las normas establecidas para el uso oficial de las cuentas para acceder a Internet y al correo electrónico.
- Análisis para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado a acceder a Internet. Esto, para que el encargado de administrar la Red limite el acceso a las páginas autorizadas.
- Análisis para determinar los funcionarios y los empleados a quienes debían otorgarse los privilegios para recibir y enviar mensajes de correo electrónico de fuentes externas, de acuerdo con las necesidades de la OSAJ y con los deberes y las responsabilidades de sus puestos. Esto, para que el encargado de administrar la Red configure las cuentas de los usuarios.

Véanse las recomendaciones 1 y de la 3 a la 5.d.

Hallazgo 2 - Falta de un Plan de Seguridad y de un procedimiento para el manejo de incidentes

- a. Al 30 de diciembre de 2007 la OSAJ no tenía un **Plan de Seguridad** aprobado por la Directora Ejecutiva que incluyera, entre otras cosas, disposiciones en cuanto a:
 - La documentación de la validación de las normas de seguridad⁹
 - La evidencia de un análisis de riesgos actualizado, que sea la base del **Plan**

⁹ 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**.

- La responsabilidad de la gerencia y de los demás componentes de la unidad
- Un programa de adiestramiento especializado al equipo clave de seguridad
- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, contratistas, personal de sistemas de información y usuarios, y que permita mantener los conocimientos actualizados
- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros)
- La documentación de la interconexión de los sistemas.

En la **Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05**, se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. También se establece que las entidades gubernamentales son responsables de:

- Proveer adiestramientos a toda la gerencia y a los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- Proveer adiestramientos al personal de sistemas de información y telecomunicaciones y de que se le transmitan conocimientos actualizados sobre los aspectos de seguridad de sus áreas.
- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

De ocurrir una emergencia, la falta de un **Plan de Seguridad** y de los correspondientes adiestramientos y simulacros podría dar lugar a:

- Pérdidas irreparables de vidas humanas

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

La situación comentada se atribuye a que la Directora Ejecutiva no había promulgado una directriz para el desarrollo, la implantación y la actualización continua del **Plan de Seguridad**, según lo establecido en la **Carta Circular Núm. 77-05**.

- b. Al 30 de septiembre de 2005 la OSI no tenía un procedimiento o plan para el manejo de incidentes que estableciera, entre otras cosas, una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece, entre otras cosas, que las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad, incluidos los límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta. Además, se establece que todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.

La situación comentada le impide a la OSI tener un control eficaz y documentado sobre el manejo de incidentes. Además, puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

La situación comentada obedece, principalmente, a que la Directora Ejecutiva no le había requerido a la OPI que desarrollara y sometiera para su consideración y aprobación las normas y los procedimientos escritos necesarios para establecer el procedimiento o plan para el manejo de incidentes.

La ex Directora Ejecutiva, en la carta que nos envió, informó, entre otras cosas, que el **Avalúo de Riesgo** y el **Plan de Seguridad** se prepararon durante el 2008. Los mismos fueron completados en diciembre de 2008, y aprobados y firmados en febrero de 2009.
[Apartado a.]

Consideramos las alegaciones de la ex Directora Ejecutiva de la OSAJ en relación con el **Apartado a. del Hallazgo**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones 1 y 5.e. y f.

Hallazgo 3 - Falta de un Plan de Continuidad de Negocios, deficiencias en el Plan de Contingencias, falta de pruebas o simulacros que certificaran la efectividad del Plan y de documentación fuera de la OSI

- a. Al 31 de diciembre de 2007 la OSAJ carecía de un **Plan de Continuidad de Negocios** que incluyera los planes específicos, completos y actualizados de la OSI. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la OSI, en caso de riesgos como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que las entidades gubernamentales deberán desarrollar un **Plan de Continuidad de Negocios** que incluya un **Plan para la Recuperación de Desastres** y un **Plan para la Continuidad de las Operaciones**. Además, en la **Política Núm. TIG-004, Servicios de Tecnología** de dicha **Carta Circular** se establece que la Agencia será responsable de asegurar la continuidad de sus operaciones mediante un Plan de Recuperación por Desastre desarrollado de acuerdo a la **Política de Seguridad (TIG-003)**. El Plan de Recuperación por Desastre abarcará todo lo relacionado a programación, equipo, datos e instalaciones físicas de la Agencia.

- b. La **Revisión al Plan de Contingencia de Emergencia (Plan)**, aprobado el 25 de enero de 2008 por la Directora Ejecutiva y la Directora de la OSI, que nos fue provisto como el Plan de Contingencias de la OSI, no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:
- La asignación clara de responsabilidades para la recuperación
 - Los procedimientos a seguir cuando el centro de cómputos (Centro) no puede recibir ni transmitir información
 - El inventario de los equipos, de los sistemas operativos y de las aplicaciones
 - La identificación de los archivos críticos de la OSI
 - Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos
 - El detalle de la configuración de los equipos críticos (equipos de comunicaciones y servidores) y del contenido de los respaldos, así como los nombres de las librerías y de los archivos
 - El nombre del encargado de activar el **Plan** y del personal de reserva, de forma tal que pueda ser ejecutado sin depender de individuos específicos
 - Una hoja de cotejo para verificar los daños ocasionados
 - Una lista de los números de teléfonos de los miembros de cada grupo de recuperación
 - Una lista de los proveedores principales, que incluya el número de teléfono y el nombre del personal de enlace con la entidad.
- c. La OSI no había efectuado procedimientos de prueba o simulacros que certificaran la efectividad del **Plan**.

Las mejores prácticas en el campo de la tecnología de información utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que como parte del **Plan de Continuidad de Negocios** se deberá preparar un **Plan de Contingencias**. Éste es una guía que garantiza la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afectan su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la entidad y deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del Centro o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. Además, se deben efectuar procedimientos para realizar pruebas o simulacros por lo menos dos veces al año, revisar el **Plan** en una base trimestral y darlo a conocer a todo el personal que llevará a cabo los procesos del mismo.

- d. No se mantenía una copia del **Plan** fuera de las instalaciones de la OSI.

Como norma de sana administración y de control interno se requiere que las entidades gubernamentales mantengan copia actualizada del **Plan de Continuidad de Negocios**, que incluye el **Plan de Contingencias**, en un lugar seguro fuera del edificio donde radica el Centro. Esto es necesario para garantizar la continuidad de las operaciones prontamente en caso de que ocurra un evento inesperado.

Las situaciones comentadas podrían 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 a los usuarios de la OSAJ.

Además, la situación comentada en el **Apartado d.** podría ocasionar que, de ocurrir una emergencia que impida el acceso a la OSAJ, el encargado de activar el **Plan de Contingencias** no tuviera acceso a éste para iniciar el proceso de reconstrucción de archivos y programas, y el restablecimiento y la continuidad de las operaciones normales de los sistemas de información en un tiempo razonable.

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a que al 15 de abril de 2008 la Directora Ejecutiva no había requerido la preparación de un **Plan para la Continuidad de Negocios** basado en el avalúo de riesgos realizado. Éste debe contener un **Plan para la Continuidad de las Operaciones** y un **Plan para la Recuperación de Desastres**, a fin de que sirvan como herramientas para responder ante cualquier desastre que ocurra.

La situación comentada en el **Apartado c.** se atribuye a que la Directora Ejecutiva no veló ni le requirió a la OPI que desarrollara para su aprobación las normas y los procedimientos escritos para efectuar las pruebas al **Plan** y coordinara las pruebas y los simulacros correspondientes que aseguren que éste cumple con su propósito de garantizar la continuidad de los servicios en la OSI.

La situación comentada en el **Apartado d.** se atribuye, en parte, a que la OPI no se había percatado de la importancia de mantener una copia del **Plan** fuera de las instalaciones de la OSAJ.

La ex Directora Ejecutiva, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Esta información se incluyó en el Plan de Avalúo de Riesgo que se aprobó en febrero de 2009. [**Apartado a.**]

Si el interés era lograr el cumplimiento, se nos debió informar las deficiencias para poder corregirlo y cumplir dentro del término. [**Apartado b.**]

En cuanto a la realización de simulacros, admitimos que los mismos no se realizaron dentro del período auditado. [**Apartado c.**]

La que suscribe hizo las gestiones para guardar la información en la... Estamos en el proceso de guardar la información en la bóveda de la..., ya que se acordó cedernos el espacio para el resguardo (sic). [**Apartado d.**]

Consideramos las alegaciones de la ex Directora Ejecutiva en relación con el **Apartado a. del Hallazgo**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones 1, de la 5.g. a la j. y 6.

Hallazgo 4 - Falta de acuerdos para mantener los respaldos fuera del Centro y de un centro alternativo de recuperación de sistemas de información

- a. Al 10 de enero de 2008 la OSAJ no había formalizado acuerdos escritos para mantener una copia de los respaldos (*backups*) diarios y mensuales de la información de los sistemas computadorizados y de la documentación de las instalaciones, las configuraciones, los programas de aplicaciones y las actualizaciones realizadas a los sistemas de información, en un lugar fuera de los predios de la Oficina Central de la OSAJ. Dichos acuerdos son necesarios para proteger la información y poder restaurar prontamente las operaciones computadorizadas en casos de desastres o emergencia.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece que deberán existir procedimientos para tener y mantener una copia de respaldo recurrente de la información y de los programas de aplicación y de sistemas esenciales e importantes para las operaciones de la agencia. En consonancia con dicha política pública se requiere mantener una copia de los respaldos almacenada en un lugar seguro fuera de los predios de la entidad y que sea una localidad que ofrezca las condiciones ambientales y de seguridad necesarias. Esto, con el propósito de poder recuperar la mayor cantidad de información posible en caso de una emergencia o desastre.

La situación comentada podría ocasionar la pérdida permanente de información importante, sin la posibilidad de recuperarla, lo que afectaría adversamente las operaciones de la OSI y, por consiguiente, de la OSAJ en caso de surgir una emergencia.

La situación comentada se atribuye a que los funcionarios que se han desempeñado en el cargo de Director Ejecutivo no le requirieron al personal gerencial de la OSI que preparara directrices específicas y detalladas para producir y preparar las copias de respaldos de datos [Véase el Hallazgo 5] y de la documentación de programas, y para mantener las mismas en un lugar seguro fuera de los predios de la Oficina Central de la OSAJ.

- b. Al 31 de diciembre de 2007 la OSAJ no había formalizado acuerdos con otra entidad para establecer, en las instalaciones de ésta, un centro alternativo de sistemas de información que permita restaurar las operaciones computadorizadas en casos de emergencia.

Las mejores prácticas en el campo de la tecnología de información sugieren que como parte integral del **Plan de Continuidad de Negocios** deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. Debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la agencia, podrían ser los siguientes:

- Una entidad pública o privada de similar configuración y tamaño
- Una compañía dedicada a servicios de restauración
- Un centro alternativo de la propia agencia.

La situación comentada podría afectar las funciones de la OSAJ, así como los servicios de las aplicaciones que ésta utiliza para verificar el historial delictivo y prestar vigilancia a los imputados. Esto, porque no tendría disponible unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento.

La situación comentada se atribuye a que la Directora Ejecutiva de la OSAJ no se había percatado de la importancia de identificar un lugar disponible y adecuado como centro alternativo y de formalizar los acuerdos escritos necesarios para la utilización del mismo en casos de emergencia.

El Director Ejecutivo, en la carta que nos envió informó, entre otras cosas, lo siguiente:

...deseamos puntualizar que en la actualidad se ha establecido un acuerdo por escrito con la... para almacenar nuestras cintas de resguardo en la referida entidad (sic). La agencia se encuentra en el proceso de adquirir una caja fuerte y cumplir con este hallazgo. **[Apartado a.]**

Se acepta el hallazgo número 4, dado que en el mismo informe se indica que la Ex Directora Ejecutiva de la agencia para ese entonces, no se había percatado de la necesidad de identificar un lugar adecuado como centro alternativo e igualmente formalizar acuerdos por escrito necesarios para la utilización en caso de emergencia. *[Sic]* **[Apartado b.]**

La ex Directora Ejecutiva, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Para el mes de octubre de 2008 se solicitó a la... el acceso a sus facilidades para guardar nuestros files ya que no se nos recomendó guardar la información en el... porque estamos en la misma red. Las gestiones rindieron fruto y actualmente se está haciendo la gestión con... para mover los resguardos. [Sic] [Apartado a.]

Véanse las recomendaciones 1, 5.k. y 7.

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

a. Al 31 de diciembre de 2007 no se habían promulgado las normas ni los procedimientos escritos necesarios para reglamentar los siguientes procesos relacionados con la administración, la seguridad y el uso de los sistemas computadorizados:

- El establecimiento de un itinerario para el mantenimiento preventivo del equipo de acuerdo con las especificaciones del proveedor
- El establecimiento de un registro de todos los programas instalados en la Red en el cual se indique, entre otras cosas, el número de la licencia, el nombre del proveedor, la fecha de adquisición, el equipo donde está instalado (número de propiedad o de serie), el nombre del usuario y el costo
- El mantenimiento del equipo y la administración de problemas y cambios relacionados con los sistemas de información
- La atención y respuesta de emergencias
- La administración, configuración, control de cambios e informes de la Red
- La preparación, la identificación, la retención y la protección de los respaldos (*backups*) de información mantenida en los servidores y en las computadoras
- La identificación, la selección, la instalación y la modificación de las aplicaciones del sistema operativo

- La disposición de información sensible y de programas, antes de transferir o disponer de los equipos computadorizados y los medios de almacenamiento de información.

En el **Artículo 6 (f) de la Ley Núm. 177** se establece como funciones y deberes del Director Ejecutivo, entre otras responsabilidades, el adoptar y promulgar los reglamentos que sean necesarios o convenientes para implantar las disposiciones de esta **Ley**.

En el **Artículo VIII, Normas Aplicables a la Oficina de Sistemas de Información, del Reglamento Interno** se establece, entre otras cosas, que la OSI mantendrá un procedimiento de respaldos y plan de contingencias para proteger las computadoras, sus periferales y archivos de información en casos de desastres.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establecen las directrices generales que permiten a las agencias establecer controles adecuados en sus sistemas de información computadorizados para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Será responsabilidad de cada entidad gubernamental desarrollar normas específicas que consideren las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Esto implica que, como norma de sana administración, se deben establecer por escrito políticas, normas y procedimientos de control interno eficaces que reglamenten las operaciones computadorizadas y estén aprobados por la alta gerencia. Mediante los mismos se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en casos de renunciaciones o ausencias del personal de mayor experiencia y facilitan la labor de adiestramiento.

La situación comentada podría ocasionar que las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias. Además, podría exponer al personal de la OSI, a los equipos y a la información a riesgos innecesarios que pudieran afectar la continuidad de las operaciones y a otras situaciones adversas.

La situación comentada se atribuye a que la Directora Ejecutiva no veló ni le requirió a la OPI que desarrollara para su aprobación las normas y los procedimientos escritos de las operaciones de los sistemas computadorizados.

La ex Directora Ejecutiva, en la carta que nos envió, informó lo siguiente:

Refiérase al informe sobre Avalúo de Riesgos incluido como anejo a este informe.

Consideramos las alegaciones de la ex Directora Ejecutiva de la OSAJ, pero determinamos que el **Hallazgo** prevalece.

Véanse las recomendaciones 1 y 5.1.

Hallazgo 6 - Deficiencia relacionada con el formulario utilizado para solicitar la creación, la modificación y la cancelación de las cuentas de acceso de los usuarios

a. En la OSAJ se utilizaba el formulario **Registro de Acceso** para solicitar la creación, la modificación y la cancelación de las cuentas de acceso de los usuarios. En el examen realizado a este formulario encontramos que el mismo no requería lo siguiente:

- La aprobación del acceso por parte del supervisor inmediato
- La justificación del otorgamiento del acceso basado en las responsabilidades del usuario
- La justificación del cambio en los accesos de las cuentas a los usuarios
- La solicitud de acceso de conexión remota y la justificación del mismo basado en las responsabilidades del usuario
- La solicitud de cuentas con privilegios de administrador de los sistemas operativos
- La cancelación de acceso por parte de la OSI.

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 los sistemas de información dejen de funcionar correctamente y de que la información sea

accedida de forma no autorizada. Se establece, además, que la información y los programas de aplicación utilizados 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, o usar las aplicaciones (o parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización. Esta norma se instrumenta, en parte, mediante:

- 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.

La situación comentada impide mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y los privilegios a los usuarios. Esto, a su vez, puede propiciar que personas no autorizadas accedan a información confidencial y la utilicen indebidamente. Además, puede propiciar la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada se debió a que la OPI no se había percatado de la importancia de mantener un control adecuado de los accesos otorgados, cancelados, modificados y de documentar claramente la justificación de los mismos.

La ex Directora Ejecutiva, en la carta que nos envió, informó lo siguiente:

El formulario de Registro de Acceso contiene las firmas del personal necesario para autorizar el uso. No se incluyó la firma del supervisor inmediato ya que siendo ésta una agencia tan pequeña se entendió que con la firma del Director de Recursos Humanos y el de sistemas de información es suficiente ya que en esta agencia son pocas las clases de puestos y todos los empleados que ostentan una clase hacen lo mismo. En cuanto a los cambios de acceso, se incluyó un apartado al final del documento para cancelar los accesos a las cuentas o las aplicaciones a utilizar. En cuanto a la conexión remota, se le incluye la evidencia de las autorizaciones de accesos. [*Sic*]

Consideramos las alegaciones de la ex Directora Ejecutiva, pero determinamos que el **Hallazgo** prevalece.

Véanse las recomendaciones 1 y 5.m.

Hallazgo 7 - Deficiencias relacionadas con la configuración y la estructura de seguridad para acceder a la Red

- a. El examen realizado el 22 de febrero de 2008 a la configuración y a la estructura de seguridad establecida para acceder a la Red de la OSAJ, a través de Internet, reveló que no se había establecido como medida de seguridad una Zona Desmilitarizada (*DMZ*, por sus siglas en inglés). Esto, para brindar a la Red interna de la OSAJ una protección que minimice los riesgos de que la información sea accedida de forma no autorizada.
- b. Al 14 de noviembre de 2007 la OSAJ tenía un servidor¹⁰ el cual, además de estar definido como un servidor de mensajería, estaba configurado para proveer los servicios del *Web Server*. Por esto, ambos servicios eran ofrecidos en un solo servidor contrario a la práctica adecuada que requiere que los servicios de mensajería y los de la página *Web* estén configurados en servidores distintos, cada uno dedicado para cada servicio.

¹⁰ Véase la nota al calce 3.

En el **Artículo I, Introducción, del Reglamento Interno** se establece, entre otras cosas, que la OSI o unidad a cargo, es responsable de asegurar la integridad y exactitud de la información del Estado Libre Asociado de Puerto Rico, protegiéndola contra la divulgación, manipulación y destrucción no autorizada o accidental.

En la **Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular Núm. 77-05**, se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar e implantar una infraestructura de Red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientemente. Además, en la **Política Núm. TIG-003** de dicha **Carta Circular** se establece, entre otras cosas, que cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Esta política se instrumenta, en parte, mediante la configuración de los servidores que proveen los servicios de página *Web*, correo electrónico y *DNS* Externo que estén dedicados para proveer únicamente dichos servicios.

Las situaciones comentadas propician que personas no autorizadas puedan lograr acceso mediante Internet a información confidencial y, a la vez, comprometan la seguridad de los equipos de la Red por el uso indebido de ésta.

La situación comentada en el **Apartado a.** se debía, en parte, a que la OPI no había ejercido una supervisión eficaz sobre la persona encargada de administrar los sistemas para que configurara la Red de la OSAJ con los criterios básicos de una arquitectura de seguridad.

La situación comentada en el **Apartado b.** se atribuye a que la OPI no se percató del daño potencial que tendría la Red de la OSAJ por configurar dos servicios en un mismo servidor.

El Director Ejecutivo, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Al presente, nos encontramos en el proceso de identificación de fondos para adquirir el equipo necesario y establecer la **zona desmilitarizada (DMZ)**. [**Apartado a.**]

...posterior ha haber revisado este hallazgo, los servicios de publicación de la página electrónica de la OSAJ fueron transferidos a la Oficina de Administración de la Red Interagencial. [Sic] [Apartado b.]

La ex Directora Ejecutiva, en la carta que nos envió, informó lo siguiente:

Se acepta parcialmente el hallazgo por falta de acceso al personal técnico para contestar el mismo. No obstante, se le incluye la evidencia que pudimos localizar en nuestros archivos.

Véanse las recomendaciones 1, y 5.n. y o.

Hallazgo 8 - Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de la Red, y falta de revisiones periódicas de las bitácoras (logs) de eventos de estos servidores

a. El examen realizado el 22 de octubre de 2007 sobre los parámetros de los controles de acceso y de seguridad definidos en el sistema operativo de los 26 servidores de la Red de la OSAJ, reveló las siguientes deficiencias:

1) En el servidor configurado como *Primary Domain Controller (PDC)*:

- a) No se había restringido el tiempo de acceso a la Red de la OSAJ a 47 usuarios conforme a las responsabilidades y las necesidades de servicio de éstos. Los mismos tenían acceso a la Red las 24 horas y los 7 días de la semana.
- b) No se había definido la política de auditoría (*Audit Policy*) para que el sistema produjera un registro cuando ocurrieran los siguientes eventos:
 - La conexión y desconexión de las cuentas de los usuarios (*Logon and Logoff*)
 - El uso de los privilegios asignados a los usuarios (*Use of User Right*)
 - El seguimiento de los procesos (*Process Tracking*)
 - Los cambios a la política de seguridad (*Security Policy Changes*)
 - La administración de usuarios o grupos (*User/Group Management*)

- El acceso al directorio de servicio (*Directory Service Access*)
 - La conexión de cuentas privilegiadas (*Privileged Account Logon*)
- c) No se habían eliminado las cuentas de acceso de 11 empleados que habían cesado sus funciones entre el 15 de mayo y el 10 de octubre de 2007. A la fecha de nuestro examen dichas cuentas permanecían activas en el sistema.
- 2) En los restantes 25 servidores¹¹, no se habían activado las siguientes opciones correspondientes a las políticas de auditoría (*Audit Policies*):
- a) En los 25 servidores no se había activado la opción para auditar el uso de los privilegios asignados a los usuarios (*Use of User Right*), los cambios a la política de seguridad (*Security Policy Changes*), el seguimiento de los procesos (*Process Tracking*) y el acceso al directorio de servicio (*Directory Service Access*).
 - b) En 14 servidores no se había activado la opción para auditar la administración de usuarios o grupos (*User/Group Management*), la conexión y desconexión de las cuentas de los usuarios (*Logon and Logoff*), y la conexión de cuentas privilegiadas (*Privileged Account Logon*).
- b. Al 14 de noviembre de 2007 el personal encargado de administrar los sistemas no realizaba verificaciones periódicas de las bitácoras (*logs*) de eventos provistas por el sistema operativo. Esto, para conocer las posibles violaciones de seguridad que pudieran ocurrir en el servidor y en la Red, y tomar prontamente las medidas preventivas y correctivas necesarias.

En el **Artículo VI, Normas Generales, del Reglamento Interno** se establece, entre otras cosas, que el supervisor de todo usuario que cese en sus funciones o por cualquier otra razón deje de ser usuario de las computadoras será responsable de notificar a la OSI para que éstos procedan a eliminar su contraseña del sistema o procedan a mover los archivos, como sea

¹¹ Véase la nota al calce 3.

pertinente. Además, en el **Artículo VII, Normas Específicas** se establece, entre otras cosas, que en el caso de la eliminación de acceso de algún empleado debe ser notificado a la OSI con no menos de una semana de anticipación, para permitir la protección adecuada de la información del Departamento o agencia a la cancelación del acceso.

Por otro lado, en el **Artículo VIII** se establece, entre otras cosas, que como el equipo de computadoras es propiedad pública y los servicios ofrecidos son sufragados por el Estado Libre Asociado de Puerto Rico, se realizarán auditorías y monitorías en cuanto al uso y manejo de dichos componentes del sistema computadorizado de información. Se mantendrá un registro en cuanto al uso y manejo de cada uno de los usuarios del equipo de computadoras que se le asigne para realizar sus labores.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política pública 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. También se establece que 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 uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos
- La impresión y el examen continuo de las bitácoras (*logs*) que detallan los eventos inusuales del sistema
- 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.

La situación comentada en el **Apartado a.** propicia que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. Además, propicia 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 b.** 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 uso indebido de los sistemas computadorizados.

La situación comentada en el **Apartado a.1)a) y b), y 2)** se debía, en parte, a que el personal encargado de administrar los sistemas no había puesto en vigor todas las opciones de seguridad de acceso lógico que proveen los sistemas operativos ni había establecido controles adecuados para el mantenimiento de las cuentas de acceso a la Red.

La situación comentada en el **Apartado a.1)c)** se debía, en parte, a que los supervisores de las diferentes oficinas y unidades de la OSAJ no habían velado por el cumplimiento de las normas establecidas en el **Reglamento Interno.**

La situación comentada en el **Apartado b.** se debía, en parte, a que la OPI no había preparado, para la aprobación de la Directora Ejecutiva, los procedimientos necesarios para administrar la Red [**Véase el Hallazgo 5**] en donde, entre otras cosas, se impartieran las instrucciones para que el personal encargado de administrar los sistemas configure la pantalla de mantenimiento de las bitácoras de eventos y las revise periódicamente.

La ex Directora Ejecutiva, en la carta que nos envió, informó lo siguiente:

Se acepta parcialmente el hallazgo por falta de acceso al personal técnico para contestar el mismo. No obstante, se le incluye la evidencia que pudimos localizar en nuestros archivos que entendemos que es de utilidad.

Véanse las recomendaciones 1, de la 5.p. a la r. y 8.

Hallazgo 9 - Falta de participación de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información

- a. La Oficina de Auditoría Interna del Departamento se encarga de auditar las operaciones de la OSAJ. Al 27 de junio de 2007 la Oficina de Auditoría Interna del Departamento no había efectuado auditorías de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados de la OSAJ.

En la **Sección 2110 de las Normas para el Ejercicio Profesional de la Auditoría Interna** emitida por el Instituto de Auditores Internos se establece, entre otras cosas, que la actividad de auditoría interna debe asistir a la organización mediante la identificación y evaluación de las exposiciones de los riesgos y contribuir al mejoramiento de los sistemas de gestión de riesgos y control.

En la **Sección 2110.A2** de dichas **Normas** se establece, además, que la actividad de auditoría interna debe evaluar las exposiciones de riesgo referidas a gobierno, operaciones y sistemas de información con relación a lo siguiente:

- Confiabilidad e integridad de la información financiera y operativa
- Eficacia y eficiencia de las operaciones
- Protección de activos
- Cumplimiento de las leyes, los reglamentos y los contratos.

La falta de fiscalización y de recomendaciones sobre los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados por parte de los auditores

internos, puede propiciar que se cometan errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades. También priva a la gerencia de información necesaria sobre el funcionamiento de los sistemas, los controles y demás operaciones de la OSAJ. Además, existe la posibilidad de que en los sistemas de información no se incluyan los controles básicos necesarios para evitar incurrir en errores, irregularidades y otras situaciones adversas.

Esta situación se debía a que la Oficina de Auditoría Interna no contaba con personal suficiente y adiestrado en el área de auditoría de sistemas de información.

El Secretario de Corrección y Rehabilitación, en la carta que nos envió informó, entre otras cosas, lo siguiente:

Al respecto le indicamos que la Secretaria Auxiliar de Auditoría, realizó una monitoria el 22 de octubre de 2007 a los controles de Sistema de información de la Oficina Central de OSAJ. El resultado de esta monitoria fue informada el 23 de enero de 2008 a la... Directora Ejecutiva de OSAJ para entonces. El 27 de marzo de 2008 la... sometió a la Secretaría Auxiliar de Auditoría del Departamento de Corrección, el plan de acción correctiva para atender las deficiencias encontradas. [Sic]

El Director Ejecutivo, en la carta que nos envió informó, entre otras cosas, lo siguiente:

...la Oficina de Auditoría Interna del Departamento de Corrección y Rehabilitación (DCR) realizó una auditoría a nuestra agencia. La misma se realizó para el año 2007 e impactó a la Oficina de Sistemas de Información.

La ex Directora Ejecutiva, en la carta que nos envió informó, entre otras cosas, lo siguiente:

...la Oficina de Auditoría Interna del Departamento de Corrección y Rehabilitación realizó una auditoría al Área de Sistemas de Información de la Agencia a petición nuestra. Se incluye copia de la evidencia de la Auditoría. Consta en poder de la Oficina de Auditoría del DCR la evidencia de cumplimiento con el Plan de Acción Correctiva.

Consideramos las alegaciones del Secretario de Corrección y Rehabilitación, el Director Ejecutivo de la OSAJ y la ex Directora Ejecutiva, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 2.

Hallazgo 10 - Falta de controles en el reclutamiento de personal de la OSI y de procedimientos para el traslado y la separación del personal que tiene acceso a los sistemas de información de la OSAJ

- a. El 25 de enero de 2006 la OSAJ solicitó autorización a la Administración de Instituciones Juveniles (AIJ) para un destaque administrativo del Administrador de Redes. La OSAJ no le requirió a este empleado, previo a ocupar el puesto de Administrador de Redes el 6 de febrero de 2006, información personal necesaria para realizar una investigación sobre su carácter, hábitos, conducta, conocimiento en el área técnica y reputación en el área profesional. Debido a que la OSAJ no había establecido acuerdos de confidencialidad con los empleados ni con los consultores, a este empleado tampoco se le requirió firmar acuerdos escritos de no divulgación antes de exponerlo a datos confidenciales u otros activos sensitivos de la entidad.
- b. Al 5 de septiembre de 2007 la OSAJ no había establecido procedimientos escritos para el manejo del traslado y la separación del personal que tiene acceso a los sistemas de información. Estos procedimientos deben considerar, entre otras cosas, los procesos a realizarse para la entrevista final, la devolución de la propiedad y de las tarjetas de identificación, la notificación al Oficial de Seguridad, con el fin de que se efectúe el cambio correspondiente o la revocación inmediata de las cuentas de acceso, y la identificación del período durante el cual los acuerdos de no divulgación son efectivos.

En el **Artículo 6 C. del Reglamento Núm. 6635, Reglamento de la Unidad Especializada de Investigaciones y Arrestos, adscrita a la Oficina de Servicios con Antelación al Juicio**, se establece que los agentes adscritos a la Unidad Especializada de Investigaciones y Arrestos tendrán, entre otros deberes y responsabilidades, el practicar investigaciones en la

comunidad y en el ambiente de trabajo sobre el carácter, reputación, hábitos y conducta en general de los solicitantes a empleo en la OSAJ.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece, entre otras cosas, que las agencias establecerán controles en el reclutamiento del personal de sistemas de información, especialmente para el área de seguridad, de tal manera que se verifique su conocimiento en el área técnica y su reputación en el área profesional y que este personal firmará acuerdos por escrito de no divulgación antes de ser expuesto a datos confidenciales y a otros activos sensitivos.

La situación comentada en el **Apartado a.** podría dar lugar al reclutamiento de personal no apto para ejercer las funciones de seguridad asignadas y al uso indebido de información privilegiada sin que pueda detectarse a tiempo para fijar responsabilidades y tomar las medidas correctivas necesarias. Esto, a su vez, resultaría en otras consecuencias adversas para la OSAJ.

La situación comentada en el **Apartado b.** propicia que no existan mecanismos de control para evitar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. Esto puede propiciar la comisión de irregularidades sin que puedan ser detectadas a tiempo para fijar responsabilidades.

La situación comentada en el **Apartado a.** obedece, principalmente, a que los funcionarios que actuaron como Director de Recursos Humanos no le solicitaron al empleado la información necesaria para someterla a la Unidad Especializada de Investigaciones y Arrestos para su consideración e investigación. Además, la Directora Ejecutiva no les había requerido a estos directores que desarrollaran y sometieran para su consideración y aprobación las normas y los procedimientos escritos necesarios para establecer acuerdos de confidencialidad con los empleados y consultores de la OSAJ.

La situación comentada en el **Apartado b.** obedece a que la Directora Ejecutiva no le había requerido a los funcionarios que actuaron como Director de Recursos Humanos durante el período auditado, que desarrollaran y sometieran para su consideración y aprobación las

normas y los procedimientos escritos necesarios para el traslado y la separación del personal que tiene acceso a los sistemas de información de la OSAJ.

El Director Ejecutivo, en la carta que nos envió, informó lo siguiente:

Actualmente, se han creado especificaciones de clase con requerimientos más técnicos y la Oficina de Recursos Humanos ha creado las posiciones de: (1) **Técnico de Sistemas de Información** y (2) **Administrador de Redes**, con el propósito de separar las tareas y proporcionar integridad, confidencialidad y disponibilidad de la información. [Apartado a.]

La ex Directora Ejecutiva, en la carta que nos envió, informó lo siguiente:

Al tomar conocimiento de la misma, se ordenó a la Unidad de Investigaciones y Arrestos la realización de la Investigación. Posteriormente el se determinó no renovar el destaque del Empleado de la AIJ. Este fue devuelto a su Agencia de Origen. [Sic] [Apartado a.]

Véanse las recomendaciones 1 y de la 9.a. a la c.

Hallazgo 11 - Falta de adiestramientos periódicos a la OPI y al Administrador de la Red sobre sus funciones y la seguridad de los sistemas, y a los funcionarios y empleados sobre el uso y el control de los equipos y sistemas computadorizados, y falta de un registro de los adiestramientos recibidos por el personal de la OSI

a. Durante los años fiscales del 2004-05 al 2006-07 la OPI y el Administrador de la Red de la OSAJ no recibieron adiestramientos continuos sobre los temas relacionados con sus funciones y con la seguridad de los sistemas de información, tales como:

- Protocolos de la Red
- Diseño, instalación, configuración y mantenimiento de la Red
- Monitoreo de la Red, herramientas para la autoevaluación de la misma y detección de intrusos
- Análisis de problemas
- Novedades, actualizaciones o mejoras en los sistemas

- Nuevas amenazas y posibles soluciones
 - Seguridad y confidencialidad de la información y de las leyes de derecho de autor de los programas computadorizados
 - Técnicas para prevenir incendios y manejar los equipos de extinción instalados en el Centro
 - Administración del Plan de Contingencias para el desalojo de los empleados.
- b. La OSAJ no ofrecía adiestramientos sobre el uso y el control de los equipos y de los sistemas de información. Esto, para orientar a los funcionarios y a los empleados en cuanto a la seguridad de acceso lógico y físico, el manejo y el control de las contraseñas y las normas de uso de los equipos y sistemas de computadorizados, entre otros. Las entrevistas realizadas del 10 de octubre al 1 de noviembre de 2007 a 30 usuarios de computadoras revelaron lo siguiente:
- Veintinueve de los usuarios (97 por ciento) indicaron no haber recibido adiestramientos relacionados con las amenazas y la seguridad de Internet.
 - Veintinueve de los usuarios indicaron no haber recibido adiestramientos u orientaciones relacionados con las características, el cambio y la protección de las contraseñas.
 - Veintinueve de los usuarios indicaron no haber recibido adiestramientos u orientaciones relacionados con la Ingeniería Social.
 - Veintisiete de los usuarios (90 por ciento) indicaron no haber recibido adiestramientos u orientaciones sobre la seguridad de acceso lógico y físico.
 - Diez de los usuarios (33 por ciento) indicaron no haber recibido adiestramientos u orientaciones sobre las medidas correctivas y disciplinarias por violaciones al uso de los sistemas de información.

- Quince de los usuarios (50 por ciento) indicaron no haber recibido adiestramientos u orientaciones sobre las normas de uso de los equipos y los sistemas de información.
 - Veintitrés de los usuarios (77 por ciento) indicaron no haber recibido adiestramientos u orientaciones sobre el Plan de Seguridad para el Desalojo de Empleados y Control de Emergencia.
 - Veinticinco de los usuarios (83 por ciento) indicaron no haber recibido adiestramientos sobre el Plan de Contingencias.
 - Veintiocho de los usuarios (93 por ciento) indicaron no haber recibido adiestramientos sobre el Plan de Continuidad de los Servicios y recuperación de desastres.
 - Trece de los usuarios (43 por ciento) no habían recibido adiestramiento sobre la utilización de las computadoras y de los programas instalados en las mismas. De los 17 usuarios que indicaron haber recibido adiestramientos, 16 sólo habían sido adiestrados y readiestrados en el sistema que se utilizaba para verificar el historial delictivo del imputado.
- c. La OSAJ no mantenía un registro de los adiestramientos tomados por el personal de sistemas de información. La OSI coordinaba los adiestramientos para las necesidades particulares de su personal, pero no le informaba sobre los mismos a la Oficina de Recursos Humanos para la evaluación y el registro de éstos.

En la **Sección 6.5 de la Ley Núm. 184** se establece, entre otras cosas, como concepto básico en administración que, para que una agencia cumpla a cabalidad su misión, debe desarrollar al máximo sus recursos humanos y proveer los instrumentos administrativos para su mejor utilización. Además, se indica que cada agencia mantendrá un historial por cada empleado de los adiestramientos recibidos, de modo que puedan utilizarse para tomar decisiones relativas a ascensos, traslados, asignaciones de trabajo, evaluaciones y otras acciones de personal compatibles con el principio de mérito.

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

- La agencia es responsable de proveer adiestramientos a toda la gerencia y a los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimiento actualizado sobre los aspectos de seguridad de sus áreas.
- La agencia es responsable de crear mecanismos de capacitación para todos los empleados conozcan los procedimientos de seguridad que le apliquen.

En la **Política Núm. TIG-011 de la Carta Circular Núm. 77-05** se establece que los datos y la información que las agencias mantienen son vitales para la toma de decisiones tanto para la agencia como para el desarrollo de estrategias que benefician los servicios ofrecidos por el Gobierno del Estado Libre Asociado de Puerto Rico. Las agencias deben establecer metodologías para asegurar la integridad y la confiabilidad de los datos producidos y almacenados. Dicha política se instrumenta, en parte, mediante el adiestramiento ordenado y continuo a los usuarios de computadoras sobre el uso de éstas y de los programas instalados en las mismas.

La situación comentada en el **Apartado a.** podría reducir la efectividad de los sistemas computadorizados, y exponer los datos y al personal a riesgos innecesarios que afecten la continuidad de las operaciones de la OSAJ.

La situación comentada en el **Apartado b.** puede propiciar que no se utilicen al máximo los equipos y los programas computadorizados, se pierda información almacenada en las computadoras, se utilicen equipos y programas computadorizados sin la debida autorización, y se instalen programas que no estén debidamente autorizados por la OSAJ. Además, que se propaguen virus a los equipos computadorizados.

La situación comentada en el **Apartado c.** impide a la Oficina de Recursos Humanos tener un control eficaz y documentado sobre los adiestramientos recibidos por el personal de la OSI que sirva para identificar las necesidades de adiestramientos y para tomar decisiones relativas a ascensos, traslados, asignaciones de trabajo, evaluaciones y otras acciones de personal.

Las situaciones comentadas en los **apartados a. y b.** se atribuyen a que la OPI no cumplió con su deber de informar a la Oficina de Recursos Humanos sobre las necesidades de adiestramientos para ésta y para el Administrador de la Red a los fines de mantenerse al día en los conocimientos relacionados con sus funciones y el manejo de la seguridad de los sistemas a su cargo. Además, no había identificado las necesidades de adiestramiento de los usuarios sobre el uso de los sistemas computadorizados a los fines de planificar, coordinar e implantar un plan de adiestramiento y orientación sobre la seguridad de la información para los empleados de la OSAJ.

La situación comentada en el **Apartado c.** se atribuye a que los directores de Recursos Humanos que actuaron durante el período auditado no cumplieron con las disposiciones establecidas en la **Ley Núm. 184.**

La ex Directora Ejecutiva, en la carta que nos envió informó, entre otras cosas, lo siguiente:

El personal de la Oficina de Sistemas de Información de la OSAJ recibió adiestramientos de varios temas relacionados. Se incluyen las evidencias como anejo a la presente comunicación. [**Apartado a.**]

Consideramos las alegaciones de la ex Directora Ejecutiva en relación con el **Apartado a. del Hallazgo**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones **1, 5.s. y 9.d.**

ANEJO

DEPARTAMENTO DE CORRECCIÓN Y REHABILITACIÓN
OFICINA DE SERVICIOS CON ANTELACIÓN AL JUICIO
OFICINA DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES QUE ACTUARON
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lic. Miguel A. Pereira Castillo	Secretario de Corrección y Rehabilitación	6 jun. 07	15 abr. 08
Sra. Providencia Vales de Méndez	Secretaria Auxiliar de Auditoría	6 jun. 07	15 abr. 08
Lic. Waleska Casiano Matos	Directora Ejecutiva	6 jun. 07	15 abr. 08
Lic. Vanessa Jiménez Cuevas	Subdirectora Ejecutiva	6 jun. 07	15 abr. 08
Sr. Armando Villegas Ortiz	Ayudante Especial	6 jun. 07	15 abr. 08
Sr. Héctor Rivera Pastor	Supervisor General de Presupuesto y Finanzas	6 jun. 07	15 abr. 08
Sra. Leticia Picón Colón	Oficial Principal de Informática	6 jun. 07	15 abr. 08
Sr. José C. Vizcarrondo Magriz	Director de Investigaciones y Arrestos Interino	6 jun. 07	15 abr. 08
Sra. Isa-Nymari Santiago Aponte	Directora de Recursos Humanos Interina	3 ago. 07	15 abr. 08
Sr. Juan A. López Medina	Director de Recursos Humanos	6 jun. 07	2 ago. 07
Vacante	Director de Administración ¹²	6 jun. 07	15 abr. 08
"	Director de Supervisión y Seguimiento ¹²	6 jun. 07	15 abr. 08

¹² El Sr. Armando Villegas Ortiz, Ayudante Especial, ejercía las funciones de Director de Administración y la Lic. Vanessa Jiménez Cuevas, Subdirectora Ejecutiva, ejercía las funciones de Directora de Supervisión y Seguimiento.