INFORME DE AUDITORÍA TI-09-14

6 de febrero de 2009

DEPARTAMENTO DEL TRABAJO
Y RECURSOS HUMANOS
OFICINA DE CÓMPUTOS Y
SISTEMAS DE INFORMACIÓN

(Unidad 5310 - Auditoría 12956)

Período auditado: 11 de agosto de 2006 al 10 de octubre de 2007

CONTENIDO

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

6 de febrero 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 Cómputos y Sistemas de Información (OCSI) del Departamento del Trabajo y Recursos Humanos (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, la segregación de deberes, 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.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Departamento se creó en virtud de la **Ley Núm. 15 del 14 de abril de 1931**, **Ley Orgánica del Departamento del Trabajo**, según enmendada. En el **Artículo IV de la Constitución** se reiteró su creación como uno de los departamentos principales de la Rama Ejecutiva del Gobierno del Estado Libre Asociado de Puerto Rico. La **Ley Núm. 100 del 23 de junio de 1977** redenomina esta agencia como Departamento del Trabajo y Recursos Humanos.

Posteriormente, el **Plan de Reorganización Núm. 2 de 1994** reestructura el Departamento. Este **Plan** reorganizó el Departamento a base de los siguientes componentes operacionales:

- Administración del Derecho al Trabajo
- Programas vigentes en el Departamento
- Consejo de Desarrollo Ocupacional y Recursos Humanos
- Cuerpo de Voluntarios al Servicio de Puerto Rico[1]

El Departamento, además de las funciones y las responsabilidades que le encomiendan las leyes protectoras del trabajo y otras leyes en beneficio de la paz laboral y el bienestar de los trabajadores, es la agencia de la Rama Ejecutiva que se encarga de implantar, desarrollar y coordinar la política pública y los programas dirigidos a la formación y la capacitación de los recursos humanos indispensables para cubrir las necesidades del sector del trabajo.

El Departamento lo dirige un Secretario nombrado por el Gobernador con el consejo y consentimiento del Senado de Puerto Rico. Para lograr sus objetivos, el Departamento cuenta con las oficinas del Secretario y Subsecretario, las secretarías auxiliares, los negociados, los programas y las oficinas locales.

El Departamento cuenta con un Área Administrativa y de Asesoramiento compuesta por: la Secretaría Auxiliar de Asuntos Gerenciales, la Secretaría Auxiliar de Planificación, Investigación y Desarrollo, la Secretaría Auxiliar de Recursos Humanos, la Oficina del Procurador del Trabajo y la Oficina de Auditoría Interna. Además, cuenta con el Área Programática compuesta por: la Secretaría de Asuntos Legales y Normas, la Secretaría Auxiliar de Beneficios y Desarrollo de la Fuerza Trabajadora, la Secretaría de Seguridad y Salud en el Trabajo, el Negociado de Seguridad de Empleo, el Negociado de Fomento del Trabajo, la Unidad de Investigaciones y Determinación de Sobrepagos, y la Oficina de Mediación y

---

[1] Mediante la **Ley Núm. 224 del 6 de agosto de 1999** se enmendó la **Ley Núm. 1 del 23 de junio de 1985, Ley del Cuerpo de Voluntarios al Servicio de Puerto Rico**, con nueva nominación: **Administración para el Adiestramiento de Futuros Empresarios y Trabajadores**, y se enmendó sustancialmente su ley orgánica.

Adjudicación. Según el diagrama organizacional a octubre de 2006, la OCSI estaba adscrita a la Secretaría Auxiliar de Planificación, Investigación y Desarrollo.

La OCSI era dirigida por un Oficial Principal de Informática (OPI) y contaba con cuatro unidades de trabajo: Unidad de Control, Unidad de Entrada de Datos, Unidad de Programación y Unidad de Comunicaciones. Al 31 de julio de 2006 la OCSI tenía 30 empleados.

El **ANEJO** contiene una relación de los funcionarios principales del Departamento que actuaron en el período auditado.

El Departamento contaba con un contrato por servicios profesionales y consultivos para los servicios de mantenimiento de aplicaciones y corridas diarias de servicios (*outsourcing*) y de apoyo técnico para el proceso continuo de las aplicaciones de *mainframe*: **Sistema Automatizado de Beneficios (SABEN)**, Contribuciones, Estadísticas, Sistema de Seguro por Incapacidad No Ocupacional Temporera **(SINOT)**, **CPI**, *Call Center* y Sistema Automatizado de Voz (IVR) del Negociado de Seguridad de Empleo (NSE), y Módulo de la Distribución del Tiempo (Finanzas) del Departamento. Además, contaba con 13 servidores y 2 redes de comunicaciones (*LAN* y *WAN*, por sus siglas en inglés) que conectaban al Departamento con sus oficinas locales y con la compañía contratada.

La OCSI no contaba con un presupuesto propio, ya que la misma le brinda servicios de apoyo a todos los programas adscritos al Departamento, por lo que sus gastos eran prorrateados entre todos los programas o de acuerdo con las necesidades de éstos al momento de solicitar el servicio.

El Departamento cuenta con una página de Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.dtrh.gobierno.pr. Esta página provee información acerca de la entidad y de los servicios que presta.

RESPONSABILIDAD DE LA GERENCIA

La gerencia de todo organismo gubernamental debe considerar los siguientes **Diez Principios para Lograr una Administración Pública de Excelencia**. Éstos se rigen por principios de calidad y por los valores institucionales:

1. Adoptar normas y procedimientos escritos que contengan controles internos de administración y de contabilidad eficaces, y observar que se cumpla con los mismos.

2. Mantener una oficina de auditoría interna competente.

3. Cumplir con los requisitos impuestos por las agencias reguladoras.

4. Adoptar un plan estratégico para las operaciones.

5. Mantener el control presupuestario.

6. Mantenerse al día con los avances tecnológicos.

7. Mantener sistemas adecuados de archivo y de control de documentos.

8. Cumplir con el **Plan de Acción Correctiva** de la Oficina del Contralor de Puerto Rico, y atender las recomendaciones de los auditores externos.

9. Mantener un sistema adecuado de administración de personal que incluya la evaluación del desempeño, y un programa de educación continua para todo el personal.

10. Cumplir con la **Ley de Ética Gubernamental**, 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 11 de agosto de 2006 al 10 de octubre de 2007. 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 procedimientos de control interno y de otros procesos
- Confirmaciones de información pertinente

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OCSI en lo que concierne a la administración del programa de seguridad, los controles de acceso, la segregación de deberes, 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 16** de este **Informe**, clasificados como principales.

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

RECOMENDACIONES

AL SECRETARIO DEL TRABAJO Y RECURSOS HUMANOS

1. Ejercer una supervisión eficaz sobre el Secretario Auxiliar de Planificación, Investigación y Desarrollo para asegurarse de que el OPI:

   a. Efectúe inspecciones periódicas para verificar el cumplimiento con las normas establecidas para el uso de las microcomputadoras y de las cuentas para acceder a Internet. **[Hallazgo 1]**

   b. Establezca los mecanismos de control necesarios en el servidor que permite el acceso a Internet para impedir que las cuentas de acceso con dicho privilegio puedan acceder a páginas de Internet con contenido ajeno a la gestión pública. **[Hallazgo 1]**

   c. Realice las gestiones pertinentes para la preparación de un plan de seguridad para la OCSI y someta el mismo para su consideración y aprobación. Una vez aprobado, asegurarse de que se realicen pruebas periódicas y, se divulgue a los empleados y funcionarios concernidos. **[Hallazgo 2-a.]**

   d. Desarrolle y someta para su consideración y aprobación las normas y los procedimientos escritos para el manejo de incidentes que establezca, entre otras cosas, una estrategia formal y documentada para el manejo de los incidentes, un equipo de respuesta y documentación de las actividades relacionadas con el manejo de los mismos. **[Hallazgo 2-b.]**

   e. Revise la **Guía Metodológica para el Plan de Manejo de Emergencias (Guía)** para que se incluya la información que se indica en el **Hallazgo 4-a.** Una vez revisada, someta la misma para su consideración y aprobación.

   f. Efectúe pruebas o simulacros de la **Guía**, por lo menos, dos veces al año y mantenga la documentación de las estrategias utilizadas y los resultados de las pruebas. **[Hallazgo 4-b.]**

g. Mantenga una copia de la **Guía** y de la documentación de los servidores y de las aplicaciones en un lugar seguro fuera de los predios del Departamento. **[Hallazgo 4-c.]**

h. Efectúe las modificaciones necesarias a las pantallas de políticas de control de contraseñas (*Account Policy*), de auditorías (*Audit Policy*) y de seguridad (*Security Options*), de manera que se corrijan las situaciones comentadas. **[Hallazgo 6-a.]**

i. Realice las gestiones necesarias para eliminar las 13 cuentas de acceso correspondientes a empleados que cesaron sus funciones en el Departamento y las 114 cuentas inactivas, y efectúe las modificaciones necesarias a los sistemas, de manera que se corrijan y no se repitan las situaciones comentadas en el **Hallazgo 6-b.**

j. Mantenga actualizada la lista de los usuarios con autorización para acceder a Internet. **[Hallazgo 6-c.]**

k. Enmiende el formulario **Hoja de Solicitud de Accesos a Sistemas** para que contenga la información que se indica en el **Hallazgo 7-a.**

l. Se asegure de que el personal a cargo de recibir los formularios **Hoja de Solicitud de Accesos a Sistemas** verifique que éstos se completen en todas sus partes por los usuarios, antes de entregarlo al personal encargado de crear la cuenta de acceso a los recursos de la red de comunicaciones (Red). Además, que los técnicos de la OCSI completen el referido formulario una vez brinden el servicio. **[Hallazgo 7-b.]**

m. Prepare por escrito las normas y los procedimientos necesarios para la producción y la protección de los respaldos de la información mantenida en los servidores del Departamento, y someta los mismos para su consideración y aprobación. **[Hallazgo 8-a.1)]**

n. Realice las gestiones para identificar un lugar para almacenar los respaldos realizados a la información mantenida en los servidores del Departamento que no

esté expuesto a las mismas posibles amenazas de desastres naturales que el edificio donde está localizado el Departamento. **[Hallazgo 8-a.2)]**

o. Realice las gestiones necesarias para que se identifiquen los cables, de manera que se pueda determinar con facilidad a qué computadora pertenecen y corregir a tiempo los problemas de comunicación. Además, para la actualización periódica del diagrama de la Red, y vea que se incluyan en el mismo los servidores, las computadoras y la manera en que estos equipos se interconectan. **[Hallazgo 9-a.2) y b.]**

p. Redacte y someta para su aprobación las normas y los procedimientos necesarios para reglamentar las operaciones que se comentan en el **Hallazgo 11-a.** Una vez aprobados, se asegure de que se oriente al personal sobre las disposiciones de los mismos.

q. Revise el inventario de programas instalados en la Red para que se incluya la cantidad de licencias existentes por programa. Además, realice revisiones periódicas del inventario de programas instalados para mantener actualizado el mismo y verificar que los programas instalados en las microcomputadoras sean únicamente los autorizados por el Departamento. **[Hallazgo 14]**

2. Asegurarse de que se realice y se documente el análisis de riesgos, según se establece en la **Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05, Normas sobre la Adquisición e Implantación de los Sistemas, Equipos y Programas de Información Tecnológica para los Organismos Gubernamentales**, aprobada el 8 de diciembre de 2004 por la Directora de la Oficina de Gerencia y Presupuesto (OGP), y que se sugieren en las mejores prácticas en el campo de la tecnología. **[Hallazgo 3]**

3. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus respectivos equipos en casos de desastres o emergencias en el Departamento, o considerar establecer su propio centro alterno en alguna de las instalaciones que no esté expuesta a los mismos riesgos que el lugar donde se encuentra la OCSI. **[Hallazgo 4-d.]**

4. Ver que el Coordinador de Manejo de Emergencias coordine y efectúe pruebas al **Plan Operacional de Emergencia**. **[Hallazgo 4-e.]**

5. Asegurarse de que se le requiera a la compañía contratada para brindar los servicios de mantenimiento de aplicaciones y corridas diarias de servicios (*outsourcing*) y de apoyo técnico para el proceso continuo de las aplicaciones de *mainframe* del Departamento, que lleve a cabo el simulacro de prueba de recuperación de datos para asegurar que tiene la capacidad de dar continuidad a dichos servicios. **[Hallazgo 5]**

6. Ejercer una supervisión eficaz sobre la Secretaria Auxiliar de Recursos Humanos para asegurarse de que:

    a. Los directores de cada área soliciten, por escrito al OPI, la cancelación de la cuenta de acceso tan pronto un empleado cese en sus funciones. **[Hallazgo 6-b.1)]**

    b. Se revise el **Plan de Clasificación** del Departamento para que se integren al mismo los puestos que ocupan el personal de la OCSI. **[Hallazgo 10-a.1)]**

    c. Se prepare el formulario **Descripción de Puesto** y se le entregue copia del mismo a los empleados, según se establece en la **Ley Núm. 184 del 3 de agosto de 2004, Ley para la Administración de los Recursos Humanos en el Servicio Público**, según enmendada, y se actualicen los mismos de acuerdo con los cambios en los títulos de clasificación de puesto, y las tareas y funciones adicionales asignadas a los empleados. **[Hallazgo 10-a.2) y 3), y b.]**

    d. Revise el borrador del Reglamento de Personal y lo someta a la Oficina de Recursos Humanos del Estado Libre Asociado de Puerto Rico para su revisión y aprobación. **[Hallazgo 11-b.]**

e. Supervise efectivamente el proceso de evaluación de desempeño del personal del Departamento conforme a lo establecido en el **Sistema de Evaluación del Desempeño del DTRH**. **[Hallazgo 13]**

7. Asegurarse de que el Director de Seguridad y Planta Física imparta las instrucciones necesarias para que los cuartos de distribución de cableado se mantengan organizados y no se almacenen materiales inflamables. **[Hallazgo 9-a.1)]**

8. Ver que se cumpla con el **Reglamento Núm. 4284, Reglamento para la Administración de Documentos Públicos en la Rama Ejecutiva**, emitido el 19 de julio de 1990 por el Administrador de Servicios Generales, y con el **Reglamento Núm. 23, Para la Conservación de Documentos de Naturaleza Fiscal o Necesarios para el Examen y Comprobación de Cuentas y Operaciones Fiscales del 15 de agosto de 1988**, según enmendado, aprobado por el Secretario de Hacienda. **[Hallazgo 12]**

9. Asegurarse de que el Director de la Oficina de Auditoría Interna: **[Hallazgo 15]**

   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. Se asegure de que se examinen periódicamente los controles y las operaciones de los sistemas de información computadorizados del Departamento.

   c. Realice las gestiones necesarias para que se establezca comunicación directa sobre los procesos de autorización o acreditación a las aplicaciones.

10. Tomar las medidas correspondientes para que la OCSI responda a la alta gerencia del Departamento como una unidad independiente de sus usuarios. **[Hallazgo 16]**

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este **Informe** se sometió para comentarios, en carta del 4 de diciembre de 2008, al entonces Secretario del Trabajo y Recursos Humanos, Sr. Román M. Velasco González.

COMENTARIOS DE LA GERENCIA

El 18 de diciembre de 2008 el entonces Secretario del Trabajo y Recursos Humanos contestó el borrador de los **hallazgos** de este **Informe**. Sus comentarios fueron considerados en la redacción final del **Informe**. Algunas de las observaciones se incluyen en la parte de este **Informe** titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección HALLAZGOS EN LA OFICINA DE CÓMPUTOS Y SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS.

AGRADECIMIENTO

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

Por: Oficina del Contralor
Natanael Agrait Cruz

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 CÓMPUTOS Y SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS, 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 CÓMPUTOS Y SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

Los **hallazgos del 1 al 16** se clasifican como principales.

Hallazgo 1 - Accesos a Internet con fines ajenos a la gestión pública

a. El examen del registro de direcciones de Internet (*Log* del servidor configurado para el servicio de Internet) visitadas por los usuarios del Departamento el 3 de abril de 2007 reveló que, entre las 9:56 a.m. y la 1:58 p.m., 4 cuentas de acceso de usuarios[2] accedieron 34 páginas de Internet con contenido ajeno a la gestión pública[3].

   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 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.

---

[2] La relación de las cuentas de acceso de los usuarios se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al entonces Secretario del Trabajo y Recursos Humanos.

[3] Dicha información se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al entonces Secretario del Trabajo y Recursos Humanos.

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** se establece como política pública, que los sistemas de comunicación y el 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 uso de las cuentas para acceder a Internet para asuntos 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 las utiliza ventajas, beneficios y privilegios que no están permitidos por ley.

La situación comentada se debía a la falta de inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento por los usuarios de las normas establecidas sobre el uso oficial de los equipos computadorizados y de las cuentas para acceder a Internet.

El entonces Secretario, en la carta que nos envió, informó lo siguiente:

> Se está estableciendo una política a nivel del ISA Server donde se restringe los accesos a páginas de web pre-identificadas y sólo para uso laboral. En el active directory se identifican las páginas de navegación para las cuales el usuario está autorizado. Todo Director que solicite acceso a la Internet para algún empleado deberá acompañar en la hoja de solicitud los URL a los que se estarán accesando y la justificación para los mismos. [*Sic*]
>
> Esta política del ISA Server se inició el pasado mes de septiembre de 2008 y se espera que sea finalizada en marzo de 2009.
>
> En la actualización de la Política General de Administración de Sistemas de Información Tecnológica, firmada por el Secretario del Trabajo en el 2008, se establecen los usos y prohibiciones con respecto al uso de Internet y el correo electrónico.

Véase la Recomendación 1.a. y b.

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

a. Al 10 de abril de 2007 el Departamento tenía la **Guía Metodológica para Plan de Manejo de Emergencias**. Sin embargo, en el examen de la **Guía** identificamos que carecía de la siguiente información, que debe ser parte esencial de un plan de seguridad:

- Documentación de la validación de las normas de seguridad[4]
- Evidencia de la existencia de un análisis de riesgo, en el cual se basa el plan de seguridad
- Responsabilidad de la gerencia y los demás componentes de la unidad
- Identificación de las instituciones y operaciones críticas
- Programa de adiestramiento especializado al equipo clave de seguridad
- Programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, contratistas y usuarios, y que permita mantener los conocimientos actualizados
- Documentación para incidentes no esperados y la conclusión de la Gerencia en cuanto a determinar la capacidad de respuesta a dichos incidentes
- Participación del equipo de seguridad en el plan de contingencias
- Documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programas, equipos y personal, entre otros)
- Documentación de la interconexión de los sistemas.

[4] La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el **Avalúo de Riesgos**. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del **Plan de Seguridad**.

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

- Proveer adiestramientos a toda la gerencia y a los supervisores de la 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 para 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

- Atraso en el proceso de reconstrucción de datos y programas, y en el restablecimiento y la continuidad de las operaciones normales y otras situaciones adversas.

La situación comentada se atribuye a que el Secretario en funciones no había promulgado una directriz sobre la implantación y la continua actualización del **Plan**.

b. Al 10 de abril de 2007 la OCSI 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 tendrán la responsabilidad de desarrollar procedimientos para detectar, informar 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 OCSI 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 se atribuye a que, según el OPI, la OCSI utilizaba el plan para el manejo de incidentes de la OGP, el cual no se nos suministró para examen.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, que la OCSI cuenta con un Plan de Seguridad completo y probado en circunstancias reales como huracanes, inundaciones y el cierre operacional del Gobierno. **[Apartado a.]**

Consideramos las alegaciones del entonces Secretario respecto al **Apartado a. del Hallazgo**, pero determinamos que el mismo prevalece.

Véase la Recomendación 1.c. y d.

Hallazgo 3 - Deficiencias en el Análisis de Riesgo en las Operaciones

a. Al 10 de abril de 2007 el Departamento tenía el **Análisis de Riesgo en las Operaciones (Análisis)** de la OCSI de mayo de 2001. El examen del **Análisis** reveló las siguientes deficiencias:

1) No estaba aprobado por el Secretario.

2) Luego de su preparación en el 2001 no se había actualizado, de modo que se consideraran los cambios ocurridos en los equipos y los sistemas computadorizados.

3) La valorización de los activos que aparecía en el **Análisis** fue estimada, basada en el costo de los equipos adquiridos para establecer o implantar la Red en el Departamento. Esto no representaba una valorización real de los activos de la OCSI.

4) Se efectuó un examen cuantitativo de las posibles amenazas, pero los hallazgos que aparecían en el **Análisis** no se efectuaron ni se presentaron de acuerdo con un orden de prioridades. Para el OPI todos los hallazgos tenían la misma prioridad.

5) No se encontró evidencia sobre las conclusiones de la gerencia en respuesta al **Análisis**.

6) El **Análisis** incluía recomendaciones dirigidas a proteger los activos, pero no había documentación de que éstas se hubiesen cumplimentado.

7) El **Análisis** fue preparado por el OPI y no se nos presentó evidencia de la participación de representantes de otras áreas operacionales del Departamento en la preparación del mismo.

8) La revisión del **Análisis** no estaba documentada.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política pública, que cada entidad deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Para esto deberá llevar a cabo un análisis de riesgo que incluya:

- Un inventario de activos de sistemas de información que incluya el equipo, los programas y los datos. Todos los activos deberán ser clasificados de acuerdo con el nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.

- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido a los datos, entre otros) junto con un análisis del impacto

en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

Las mejores prácticas en el campo de la tecnología sugieren que para proteger los activos de sistemas de información y garantizar la continuidad de las operaciones la agencia deberá desarrollar e implantar un programa de avalúo y administración de riesgos para identificar los activos y recursos que se deben proteger, y clasificar los mismos en términos de criticidad y sensitividad. Como parte del avalúo de riesgos, se deben identificar las posibles amenazas o los riesgos a los cuales éstos están expuestos, y determinar la probabilidad de que las amenazas o los eventos ocurran y el impacto que tendrían sobre las operaciones. De esta manera, se pueden tomar las decisiones apropiadas con relación a los riesgos que se pueden aceptar y cuáles se pueden mitigar a través de controles de seguridad. El informe de avalúo de riesgos, producto de este análisis, deberá someterse a la gerencia de la entidad para su revisión y aprobación.

La situación comentada impide al Departamento evaluar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de ésta y de considerar cómo protegerlos para reducir los riesgos de daños materiales y pérdida de información. Además, impide el desarrollo de un **Plan de Continuidad de Negocios** donde se establezcan las medidas de control que minimizarían los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones del Departamento en caso de que surja alguna eventualidad. **[Véase el Hallazgo 4-a.]**

La situación comentada se atribuye a que el Secretario en funciones no había requerido que se efectuara el análisis de riesgos según lo establecido en la **Carta Circular Núm. 77-05**. El **Análisis** que se nos proveyó para examen fue realizado por iniciativa del OPI.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, lo siguiente:

> La Oficina de Cómputos y Sistemas cuenta con un Análisis de Riesgo en las Operaciones realizado por su Director en el año 2001. El único análisis hecho anterior data de 1986 y nunca había sido actualizado. Los Análisis de Riesgo en las Operaciones se realizan en períodos de cada 10 años o según sean actualizadas y/o modificadas las operaciones transaccionales de la agencia.
>
> El Departamento se encuentra al presente en un proceso de reingeniería de los procesos operacionales de todas las oficinas y Negociados que han añadido el uso de tecnología de sistemas a sus funciones. De éstas se destacan las del NSE y que a la fecha de este informe no están concluidas, por lo que un análisis actualizado de riesgos no puede ser realizado hasta tanto se concluyan los procesos de reingeniería operacional que se llevan en el NSE.

Consideramos las alegaciones del entonces Secretario respecto al **Hallazgo**, pero determinamos que el mismo prevalece.

Véase la Recomendación 2.

Hallazgo 4 - Deficiencias relacionadas con el Plan de Continuidad de Negocios, y falta de pruebas o simulacros que certificaran la efectividad de la Guía, de documentación fuera de la OCSI, de acuerdos escritos para mantener un centro alterno y, de cumplimiento con el Plan Operacional de Emergencia

a. El 11 de agosto de 2006 el OPI nos entregó la **Guía** como el **Plan de Continuidad de Negocios** y como el **Plan de Recuperación de Desastres**. El examen de la **Guía** reveló las siguientes deficiencias:

   1) No se había sometido al Secretario para su aprobación.

   2) No incluía la fecha de preparación o de su última revisión.

   3) Carecía de los siguientes requisitos que son necesarios para atender situaciones de emergencia:

      - Identificación de los procesos críticos de la OCSI

- Identificación de la información y las operaciones críticas del Departamento y su clasificación en orden de prioridad

- Identificación de los recursos que darán apoyo a las operaciones críticas de la OCSI en caso de emergencia, específicamente las relacionadas con las aplicaciones que se encuentran en el Departamento

- Prioridades para los procesamientos de emergencia llevados a cabo por la OCSI

- Políticas y procedimientos sobre el mantenimiento efectivo de los equipos

- Políticas y procedimientos para el registro de los problemas de los equipos

- Detalle de la configuración de los sistemas utilizados en la OCSI requeridos para el centro de sistemas de información alterno

- Inventario de equipos, sistemas operativos, de aplicaciones y archivos críticos de la OCSI

- Itinerario de restauración que incluya el orden de las aplicaciones a restaurar y procedimientos para restaurar los respaldos.

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**.

Las mejores prácticas en el campo de la tecnología utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que el **Plan de Continuidad de las Operaciones** debe incluir todas las medidas preventivas específicas para continuar con sus operaciones en caso de riesgos como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros. El

Plan de Continuidad de Operaciones deberá estar actualizado y aprobado por el funcionario de máxima autoridad de la agencia.

b. Al 18 de septiembre de 2007 la OCSI no había efectuado procedimientos de prueba o simulacros que certificaran la efectividad de la **Guía**.

Las mejores prácticas en el campo de la tecnología utilizadas para garantizar la confiabilidad, integridad y disponibilidad de los sistemas de información computadorizados sugieren que como parte del **Plan de Continuidad de Negocios**, se deben efectuar procedimientos para realizar pruebas o simulacros de forma periódica, de acuerdo con la frecuencia requerida por éste.

c. No se mantenía una copia de la **Guía** ni de la documentación de los servidores y de las aplicaciones del Departamento en un lugar seguro fuera de las instalaciones de la OCSI.

Como norma de sana administración y de control interno se requiere que las entidades gubernamentales mantengan una copia actualizada del **Plan de Continuidad de Negocios** y de la documentación de sus servidores y aplicaciones 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 en forma desordenada. Esto afectaría 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 se debieron a que el OPI:

- No le había sometido la **Guía** al Secretario en funciones para su aprobación. **[Apartado a.1)]**

- No había considerado la importancia de mantener actualizada la **Guía [Apartado a.2)]**, de incluir los requisitos mencionados en la **Guía [Apartado a.3)]**, de efectuar

procedimientos de pruebas **[Apartado b.]** y de mantener una copia de la **Guía** y de la documentación de los servidores y de las aplicaciones fuera de las instalaciones del Departamento **[Apartado c.]**.

d. Al 5 de octubre de 2007 el Departamento no había formalizado un acuerdo con otros centros de sistemas de información para restaurar, en casos de emergencia, el procesamiento de las aplicaciones que se encontraban en los servidores.

Como norma generalmente aceptada en el campo de la informática se requiere que como parte integral del **Plan de Continuidad de Negocios**, deben existir convenios 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 alterno de la propia entidad.

La falta de acuerdos escritos con un centro alterno podría afectar las funciones del Departamento y los servicios de la OCSI, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones normales de la OCSI.

La situación comentada se debía a que el OPI no había realizado las gestiones de identificar un lugar disponible y adecuado como centro alterno para formalizar los acuerdos escritos necesarios.

e. El Departamento desarrolló un **Plan Operacional de Emergencias (Plan Operacional)** a base de las guías establecidas por el Departamento de Seguridad Nacional y la Agencia Federal para el Manejo de Emergencias, y en colaboración con la Agencia Estatal para el Manejo de Emergencias y Administración de Desastres de Puerto Rico (AEMEAD). El **Plan Operacional** fue aprobado el 25 de mayo de 2007 por el Secretario.

Como parte del **Plan Operacional** se estableció un Comité de Emergencias constituido por varios comités de seguridad. El Comité de Seguridad de la OCSI (Comité) estaba compuesto por tres integrantes. En el examen realizado el 12 de septiembre de 2007 se encontró que la Oficina de Manejo de Emergencias del Departamento no había efectuado pruebas al **Plan Operacional**.

En la **Sección VI, Desarrollo y Mantenimiento del Plan**, del **Plan Operacional de Emergencias**, aprobado el 25 de mayo de 2007 por el Secretario del Trabajo y Recursos Humanos, se establece, entre otras cosas, que el contenido de este **Plan** debe ser entendido, discutido y conocido por todo el personal del Departamento, especialmente por el personal que integra el Comité de Emergencia, quienes tienen la responsabilidad de apoyar o ejecutar el mismo. Este **Plan** se evaluará mediante ejercicios o simulacros.

De ocurrir una emergencia, las situaciones comentadas podrían dar lugar a que el equipo no se proteja adecuadamente y sufra daños materiales, así como la pérdida de información importante.

La situación comentada se debía a que el Coordinador Interagencial de Manejo de Emergencias no había coordinado las pruebas y los simulacros correspondientes.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, lo siguiente:

> Se someterá para la firma del Secretario del Trabajo, la versión actualizada de la Guía Metodológica para el Plan de Manejo de Emergencias, según sugerencia. **[Apartado a.1)]**
>
> Se actualizará la Guía Metodológica para el Plan de Manejo de Emergencias y se le incluirá la fecha de su revisión. **[Apartado a.2)]**

> Se le incluirá a dicha Guía un inventario de equipos y activos de la OCSI. **[Apartado a.3)]**
>
> El señalamiento incluye que a septiembre de 2007 no se había llevado a cabo el simulacro de restauración de sistemas, pero dicha prueba se realizó y se concluyó exitosamente en octubre de 2007, para lo cual está evidenciado en las carpetas de evaluación y certificación de transacciones disponibles para la revisión de los auditores. **[Apartado b.]**
>
> Copia de dicha Guía se mantendrá en el Centro Alterno de Recuperación de Desastres de … y en el área de resguardo de "back ups" en el NSE. **[Apartado c.]**

Consideramos las alegaciones del entonces Secretario respecto al **Apartado b. del Hallazgo**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones de la 1.e. a la g., 3 y 4.

Hallazgo 5 - Falta de simulacro de prueba de recuperación de datos por una compañía contratada

a. El 19 de julio de 2006 el Departamento formalizó el **Contrato Núm. 2007-000062**[5] con una compañía para los servicios de mantenimiento de aplicaciones y corridas diarias de servicios (*outsourcing*) y de apoyo técnico para el proceso continuo de las aplicaciones de *mainframe*: **SABEN**, Contribuciones, Estadísticas, **SINOT**, **CPI** y Módulo de la Distribución del Tiempo (Finanzas) del Departamento. El **Contrato** tenía vigencia del 1 de julio de 2006 al 30 de junio de 2007.

   Por virtud del **Contrato**, la compañía sería responsable, entre otras cosas, de asegurar la capacidad de recuperación de desastres en su centro de recuperación de negocios con un simulacro de prueba de recuperación de datos para el Departamento, durante la vigencia del **Contrato**. Al 3 de julio de 2007 y luego de concluida la vigencia del **Contrato**, no se había realizado el simulacro de prueba que se establecía en el mismo.

   En la **Ley Núm. 230 del 23 de julio de 1974**, **Ley de Contabilidad del Gobierno de Puerto Rico**, según enmendada, se establece que cada dependencia o entidad corporativa

[5] Según la Certificación de Contratos sometida a la Oficina del Contralor de Puerto Rico. Para propósitos del registro interno de contratos del Departamento, este contrato correspondía al número 067070062.

deberá mantener un control previo de todas sus operaciones para que sirva de arma efectiva al jefe de la entidad en el desarrollo del programa o programas cuya dirección se le ha encomendado. En consonancia con este principio, y como norma de sana administración y de control interno, los funcionarios que dirigen agencias gubernamentales tienen la obligación de ver que se cumplan las cláusulas establecidas en los contratos, de modo que se protejan adecuadamente los mejores intereses del Gobierno.

La situación comentada impidió al Departamento evaluar la continuidad de los servicios ante la posibilidad de un desastre natural o cualquier otro evento que impidiese al Departamento dar continuidad a sus servicios desde sus instalaciones.

La situación comentada se debió, en parte, a que el OPI no veló por el cumplimiento del contrato.

Véase la Recomendación 5.

Hallazgo 6 - Deficiencias en los parámetros de seguridad y en otros controles de acceso lógico de los servidores de la Red

a. Al 20 de abril de 2007 la OCSI tenía en operación 13 servidores. El examen de los parámetros de control de acceso y de seguridad definidos en el sistema operativo de nueve servidores[6] reveló las siguientes deficiencias en la utilización de las opciones que permiten controlar la seguridad de las cuentas de los usuarios:

1) En la pantalla *Account Policies* de dos servidores[6] se habían activado las opciones de seguridad para requerir lo siguiente:

a) Al menos, un mínimo de cinco contraseñas diferentes antes de volver a utilizar la misma (*Enforce Password History*)

b) Que las contraseñas utilizadas fueran combinaciones alfanuméricas (*Password Must Meet Complexity Requirements*)

[6] Una relación de los servidores se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al entonces Secretario del Trabajo y Recursos Humanos.

2) En la pantalla *Audit Policy* no se habían activado las siguientes opciones de seguridad correspondientes al registro de auditoría (*Audit Log*):

   a) En tres servidores[7] no se había activado la opción para auditar los eventos de acceso de las cuentas (*Audit account logon events*) y los eventos de acceso (*Audit logon events*).

   b) En seis servidores[7] no se había activado la opción para auditar el uso de los privilegios de los usuarios (*Audit privilege use*), y el reinicio, apagado y los eventos que afectan el sistema de seguridad (*Audit system events*).

   c) En siete servidores[7] no se había activado la opción para auditar la administración de las cuentas de los usuarios y los grupos (*Audit account management*).

   d) En ocho servidores[7] no se había activado la opción para auditar el acceso de servicio al directorio (*Audit directory services access*), el acceso a los archivos y a los objetos (*Audit Object Access*), los cambios efectuados a las políticas de auditoría (*Audit Policy Change*) y el rastro de los procesos (*Audit process tracking*).

   e) En un servidor[7] no se había activado la opción para el registro de auditoría (*All auditing disabled*).

3) En la pantalla *Security Options* de cuatro servidores[7] no se habían configurado 18 políticas de seguridad[8] de acuerdo con la recomendación de la industria.

---

[7] Véase la nota al calce 6.

[8] La relación de las políticas de seguridad se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al entonces Secretario del Trabajo y Recursos Humanos.

b. El examen realizado a un servidor[9] reveló que al 20 de abril de 2007 el Departamento tenía 1,863 cuentas de usuarios para acceder a la Red. De éstas, 1,749 estaban activas y 114 inactivas. El examen efectuado del control y el mantenimiento de estas cuentas reveló las siguientes deficiencias:

1) Seiscientas veinticinco cuentas permanecían activas a pesar de que 151 de éstas no se utilizaron por un período de entre 91 y 927 días, y 474 nunca se utilizaron. Trece de las 625 cuentas correspondían a empleados que dejaron de trabajar para el Departamento entre el 1 de enero de 2006 y el 29 de marzo de 2007.

2) Las 114 cuentas que estaban inactivas para acceder a la Red (*Account Disabled*) no habían sido eliminadas del sistema. De éstas, 91 cuentas nunca se utilizaron.

c. Existían 29 usuarios que tenían acceso a Internet y no estaban incluidos en la lista provista por el OPI que contenía los empleados autorizados a acceder a Internet.

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

[9] Véase la nota al calce 6.

- La asignación de códigos y contraseñas únicas y confidenciales para cada usuario que garantice un nivel óptimo de seguridad en los sistemas computadorizados

- La notificación inmediata al encargado de la seguridad de datos del cese de un usuario en sus funciones por motivo de renuncia, separación o traslado para la cancelación de su cuenta de acceso

- La renovación periódica de la contraseña de cada usuario, según las necesidades de la entidad gubernamental y los procedimientos establecidos

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

En la **Carta Circular Núm. OC-98-11 del 18 de mayo de 1998, Sugerencias sobre Normas y Controles para el Uso de los Sistemas Computadorizados**, promulgada por el Contralor de Puerto Rico, se establece que para tener acceso al sistema, el usuario deberá registrar una contraseña (*password*) de por lo menos ocho caracteres, deberá ser una combinación de caracteres alfanuméricos (letras, números y símbolos) en cualquier proporción y arreglo, y que sólo será de su conocimiento.

Las situaciones comentadas en el **Apartado a.1)** ponen en riesgo la seguridad de las cuentas de los usuarios al permitir que éstos puedan repetir la misma contraseña cuando se le requiera cambiarla luego de dos contraseñas diferentes o utilizar una contraseña que no requiera caracteres alfanuméricos (letras, números y símbolos).

Las situaciones comentadas en el **Apartado a.2) y 3)** impedían a la OCSI mantener un registro de los eventos inusuales o problemas ocurridos en el sistema que le permitiera tomar a tiempo las medidas correctivas o preventivas necesarias.

La situación comentada en el **Apartado b.** propició que las cuentas de dos ex empleados del Departamento fuesen utilizadas y que a la de otro se le cambiara la contraseña luego de la fecha de terminación de éstos. Además, podría propiciar que personas no autorizadas tengan acceso a los sistemas de información del Departamento y puedan obtener información

confidencial, cometer irregularidades o alterar, por error o deliberadamente, los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada en el **Apartado c.** le impedía al Departamento cumplir con el objetivo de asegurar la utilización de Internet de acuerdo con los estándares y las normas que protejan la integridad de los datos, la seguridad y la transferencia a través de los sistemas computadorizados. Además, impide la detección temprana de posibles situaciones irregulares en el uso de Internet y del equipo computadorizado.

Las situaciones comentadas en los **apartados a.**, **b.2) y c.** se debían, en parte, a que el OPI no puso en vigor las opciones de seguridad de acceso lógico que se comentan ni los controles adecuados sobre el mantenimiento de las cuentas provistos por el sistema operativo. Además, no mantenía actualizada la lista de usuarios con autorización para acceder a Internet.

La situación comentada en el **Apartado b.1)** se debía, en parte, a que no existía una comunicación directa por parte de la Secretaría Auxiliar de Recursos Humanos con la OCSI para la cancelación de la cuenta de acceso tan pronto un empleado cese sus funciones.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en el **Hallazgo**.

Véanse las recomendaciones de la 1.h. a la j. y 6.a.

Hallazgo 7 - Deficiencias relacionadas con los formularios para la solicitud de acceso a la Red y a las aplicaciones del Departamento

a. El acceso a la Red y a las aplicaciones **SABEN** e **Interempleo** del Departamento era solicitado y aprobado mediante el formulario **Hoja de Solicitud de Accesos a Sistemas**. En el examen realizado a este formulario encontramos que el mismo no incluía lo siguiente, según requerido en su política interna:

- Un área para indicar el nivel de acceso necesario para llevar a cabo la tarea del usuario (leer, escribir, borrar, ejecutar o editar archivos)
- El período de uso de las claves de acceso
- La política referente a los medios de seguridad y el uso de las claves de acceso.

b. El examen efectuado a las solicitudes de acceso a la Red y a las aplicaciones del Departamento de 50 usuarios, emitidas entre el 14 de noviembre de 2006 y el 3 de abril de 2007, reveló las siguientes deficiencias:

1) No se encontró ni le fue suministrada a nuestros auditores evidencia de que se hubiera utilizado el formulario **Hoja de Solicitud de Accesos a Sistemas** para la solicitud y la aprobación de las cuentas de acceso de 14 usuarios[10]. La evidencia provista para la solicitud de creación de estas cuentas fue 2 cartas (1 solicitud en cada una), 2 correos electrónicos (3 solicitudes en cada uno) y 1 orden de trabajo (*Special Job Ticket*) con 6 solicitudes.

[10] La relación de los usuarios para los que no se utilizó este formulario se incluyó en el borrador de los **hallazgos** del **Informe** sometido para comentarios al entonces Secretario del Trabajo y Recursos Humanos.

2) Para la solicitud y aprobación de las cuentas de acceso de los restantes 36 usuarios se utilizó el formulario **Hoja de Solicitud de Accesos a Sistemas**. El examen de estos formularios reveló que les faltaba parte de la información requerida, según se indica:

INFORMACIÓN REQUERIDA	CANTIDAD DE FORMULARIOS
Justificación para otorgar el acceso solicitado	27
Persona que procesó la solicitud y la fecha en que se realizó	26
El *username* y el *password* asignado para la Red, SABEN o Interempleo	25
Fecha en que el Supervisor aprobó la solicitud	19
Nombre del Supervisor	18
Firma del Supervisor	17
Fecha de la solicitud	15
Si el usuario era empleado del Departamento o de una compañía externa	9
Acción requerida (Usuario nuevo, Modificar usuario o Eliminar usuario)	4
Tipo de acceso solicitado (Red, SABEN, Interempleo)	1
Fecha en que el solicitante firmó la solicitud	1

En la **Sección C, Solicitud de Acceso, de la Política General sobre la Administración, Manejo y Seguridad de Información Computadorizada, Internet y Mensajería Electrónica (Política General)**, aprobada el 15 de octubre de 2001 por el Secretario del Trabajo y Recursos Humanos, se establece, entre otras cosas, que será política del Departamento y sus componentes que la OCSI establezca los controles de solicitud de acceso a sus sistemas electrónicos, de acuerdo con sus necesidades. La solicitud deberá indicar el nivel de acceso necesario para llevar a cabo la tarea. Esta solicitud será autorizada por el supervisor del empleado y enviada al encargado de los sistemas de información. Además, en la **Sección E, Renovación Periódica de las Claves de Acceso Secretas** de la **Política General** se establece, entre otras cosas, que la OCSI tiene la responsabilidad de

crear y mantener un documento oficial que describa la asignación, el uso, el cambio y el control de las claves de acceso para la operación del centro. El documento debe incluir, entre otras cosas:

- La política referente a los medios de seguridad y uso de las claves de acceso
- El período de uso de las claves de acceso

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

- Las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada.
- La información y los programas de aplicación utilizados en las operaciones de 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.

Las situaciones que se comentan impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos a los usuarios. Esto, a su vez, puede propiciar que personas no autorizadas accedan a información confidencial y la utilicen indebidamente. 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.** se debía a que el OPI no había ejercido el debido cuidado para cumplir con lo establecido en la **Política General**.

La situación comentada en el **Apartado b.** denota falta de supervisión al personal de la OCSI que recibía las solicitudes de acceso por no requerir el formulario **Hoja de Solicitud de Accesos a Sistemas** antes de otorgar el acceso, y no verificar que los formularios estuvieran debidamente completados por los usuarios y los técnicos de la OCSI que brindaban el servicio.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 1.k. y l.

Hallazgo 8 - Deficiencias en la preparación y el almacenamiento de los respaldos de información de los servidores del Departamento

a. El examen realizado de la preparación y el almacenamiento de los respaldos de la información contenida en los servidores del Departamento reveló lo siguiente:

1) Al 18 de septiembre de 2007 el Departamento no contaba con normas ni procedimientos escritos para documentar los respaldos de la información mantenida en 12 servidores[11].

2) Los respaldos realizados a la información mantenida en los servidores del Departamento no se protegían adecuadamente. Estos respaldos se almacenaban en el NSE, el cual estaba localizado en un edificio cerca del Departamento, por lo que estaban expuestos a las mismas posibles amenazas de desastres que la información almacenada en los servidores.

[11] Véase la nota al calce 6.

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, entre otras cosas, personal adiestrado para dichas funciones y que toda información almacenada en medios electrónicos, que se utilice como parte de la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar seguro fuera de los predios de la entidad, en donde la información no se vea afectada por las mismas posibles amenazas de desastres naturales. Esto, con el propósito de poder recuperar la mayor cantidad de información posible en caso de una emergencia o desastre.

Las situaciones comentadas podrían afectar la continuidad de las operaciones normales de la OCSI si ocurriera alguna eventualidad que afectara las instalaciones de ésta y destruyera toda la información que allí se almacena. Además, el mantener almacenados los respaldos de información en un lugar cercano a donde se encuentra el centro principal del Departamento, expone la información a las mismas amenazas de desastres naturales lo que podría ocasionar la pérdida permanente de información importante sin la posibilidad de poder restaurarla, lo que afectaría adversamente las operaciones del Departamento.

La situación comentada en el **Apartado a.1)** se debía a que el OPI entendía que la documentación de los respaldos no era necesaria porque:

- Cinco[12] de los servidores tenían información que no requería ser respaldada porque la misma no sufría cambios.
- Uno[12] de los servidores sólo contenía datos informativos.
- Uno[12] de los servidores era respaldado automáticamente.

Además, el OPI no había considerado necesario respaldar la información de otros dos servidores[12].

[12] Véase la nota al calce 6.

La situación comentada en el **Apartado a.2)** se debía a que el OPI no había considerado el que el NSE estuviera expuesto a las mismas posibles amenazas de desastres naturales que el edificio donde estaba localizado el Departamento.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, que como parte de los servicios de *outsourcing*, el Departamento tiene contratadas las labores de respaldo de todos los procesos de los sistemas **SABEN**, **TAXES**, **SINOT** y Modelo de Costo, los cuales se almacenan en una bóveda de seguridad de la compañía contratada. Además, informa que internamente se realizan dos tipos de respaldo, a través de cartuchos, los cuales se realizan diariamente fuera del edificio central y se mantienen en un archivo externo en el edificio del NSE frente al Departamento.

Consideramos las alegaciones del entonces Secretario, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.m. y n.

Hallazgo 9 - Deficiencias en los cuartos de distribución del cableado (*wiring closets*) de la Red y en el diagrama esquemático

a. El examen efectuado el 3 de abril de 2007 a nueve cuartos de distribución del cableado (*wiring closets*) de la Red reveló lo siguiente:

   1) El cuarto de distribución del cableado de uno de los pisos no cumplía con las condiciones ambientales adecuadas para proteger el equipo de telecomunicaciones. En el referido cuarto se habían almacenado materiales inflamables, tales como: pintura, tela y papel de traza.

2) En los nueve cuartos de cableado no se había identificado la cablería utilizada en los cuartos de distribución para la conexión entre los *hubs*[13] y los *switches*[14], lo cual es necesario para identificar cada cable y la estación de trabajo a la que corresponde.

En la **Política Núm. TIG-003 de la Carta Circular Núm. 77-05** se establece como política pública, que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas y directrices generales que permitirán a la agencia establecer controles adecuados en sus sistemas electrónicos de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Esto implica que, para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- No se almacenen materiales que entorpezcan el libre movimiento en las referidas áreas y puedan causar daños a los equipos

- Se mantenga la documentación e identificación adecuada del cableado de conexión a la Red de forma que permita corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada.

b. Al 2 de abril de 2007 el diagrama esquemático de la Red y sus respectivos equipos de comunicación no estaba actualizado, según se indica:

1) No incluía el detalle del cableado dentro de cada *wiring closet* y las computadoras a que pertenecen no estaban representadas en el mismo

2) No incluía los servidores de los programas de Estadísticas y Normas.

En la **Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular Núm. 77-05** se establece como política pública, que las entidades

[13] Dispositivo de comunicación central para líneas de comunicaciones en una topología de estrella. Se utiliza para ampliar una red y dividir el ancho de banda entre las estaciones de trabajo conectadas.

[14] Dispositivo de comunicación central para líneas de comunicaciones de red que permite que ocurran transmisiones simultáneas, y aumenta el ancho de banda de la red.

gubernamentales tendrán la responsabilidad de adquirir, desarrollar e implementar 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, incluye como política que el diseño de la Red debe estar documentado.

Las mejores prácticas en el campo de la tecnología de información sugieren que para mantener en funciones aceptables la Red es necesario establecer controles adecuados sobre los inventarios, la ubicación, y las conexiones entre sus componentes. Esto se logra mediante la documentación detallada y actualizada de las conexiones que permita corregir, a tiempo, problemas de comunicación de la Red y detectar cualquier conexión no autorizada.

La situación que se comenta en el **Apartado a.1)** puede ocasionar daños y deterioros prematuros a los equipos de la Red y los equipos de computadoras, lo que dificultaría obtener el rendimiento máximo en términos de los servicios que ofrecen estos equipos.

Las situaciones comentadas en los **apartados a.2) y b.** impedían al Departamento controlar, administrar y efectuar un mantenimiento rápido, eficiente y efectivo de los equipos que componen su Red. Además, impide resolver problemas de conexión en un tiempo razonable y efectuar una planificación efectiva para realizar mejoras a la Red, según el crecimiento de sus sistemas.

La situación comentada en el **Apartado a.1)** se debía, en parte, a que el Director de Seguridad y Planta Física no realizó las gestiones necesarias para remover el material inflamable y otros desperdicios del cuarto de distribución del cableado.

Las situaciones comentadas en los **apartados a.2) y b.** se debían, en parte, a que el OPI no consideró la necesidad de identificar adecuadamente la cablería de la Red y no había realizado las gestiones necesarias para mantener un diagrama esquemático actualizado.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en el **Hallazgo**.

Véanse las recomendaciones 1.o. y 7.

Hallazgo 10 - Deficiencias en los formularios Descripción de Puesto del personal que laboraba en la OCSI e inexistencia de dos formularios

a. El examen realizado en junio de 2007 de los formularios **Descripción de Puesto (DTRH/16)** del personal que laboraba en la OCSI reveló lo siguiente:

1) Los formularios de cuatro programadores de Sistemas de Información y de un Oficinista III de la OCSI tenían títulos de clasificación de puesto que no existían en el **Plan de Clasificación de Puestos del Departamento**.

2) Las funciones incluidas en los formularios no eran consistentes con las realizadas por el personal, según se indica:

a) En el formulario de una Funcionaria Administrativa III no se detallaban las siguientes funciones que realizaba al momento de nuestro examen:

- Dirigir y supervisar las actividades que se llevaban a cabo en la Unidad de Control.

- Registrar los salarios trimestrales en el sistema.

- Gestionar solicitudes de informes, de otras áreas del Departamento, con la compañía que realizaba el procesamiento externo de varias aplicaciones del Departamento.

- Recibir los cheques emitidos por la compañía externa y cotejar que la secuencia de los mismos fuese correcta.

- Realizar los cambios correspondientes a la información entrada incorrectamente en las aplicaciones **Salarios Online** y **Salarios Trimestrales**.

b) En el formulario de una Auxiliar Administrativa II y el de un Oficial de Adiestramiento de Servicio de Empleo y Desempleo I no se detallaban las siguientes funciones que realizaban al momento de nuestro examen:

- Instalación de aplicaciones
- Configuración de impresoras
- Asistencia técnica a los usuarios de la Red.

c) En el formulario del OPI no se indicaba que éste estaba a cargo de administrar la seguridad de los sistemas de información.

3) En los formularios de ocho operadores de Equipo de Entrada de Información se indicaban, en las funciones marginales del puesto, que este personal estaba bajo la supervisión de un Supervisor de Equipo de Perforar y Verificar Datos, a pesar de que al momento del examen en el Departamento no se utilizaban equipos de perforar datos. Además, estos formularios indicaban que el Supervisor Inmediato era una Funcionaria Administrativo I que al momento del examen estaba retirada.

b. Al 8 de marzo de 2007 los formularios **Descripción de Puesto (DTRH/16)** de dos técnicos de la Red no constaban en los expedientes de personal del Departamento.

En el **Apartado 2 de la Sección 6.2 del Artículo 6 de la Ley Num. 184** se establece que cada Autoridad Nominadora será responsable de establecer y mantener una estructura racional de funciones que propenda a la mayor uniformidad posible y que sirva de base para las acciones de personal. Para ello, entre otras disposiciones, preparará una descripción por escrito de cada puesto, copia de la cual será entregada a cada empleado. La descripción del puesto será de tal naturaleza que oriente al empleado respecto a las funciones generales,

esenciales y marginales que debe realizar, sobre el propósito de cada función, que permita a la Autoridad Nominadora cumplir adecuadamente su gestión pública.

Las situaciones comentadas pueden ocasionar, entre otras cosas, que los empleados de la OCSI desconozcan los límites y el alcance de las tareas inherentes a sus puestos y que se dificulte la evaluación del desempeño de sus funciones, al carecer de mecanismos formales actualizados para evaluar el desempeño del personal. Además, podrían ocasionar que los empleados realicen o se les requiera realizar tareas de naturaleza incompatible, lo cual podría afectar la confiabilidad de la información que provee el Departamento y puede tener consecuencias adversas en caso de que algún empleado se querelle en cuanto a las funciones que desempeña.

La situación comentada en el **Apartado a.1)** se debía a que los formularios **Descripción de Puesto** correspondían al **Plan de Clasificación de la Administración del Derecho al Trabajo** (ADT). Al 22 de junio de 2007 el Departamento utilizaba dos planes de clasificaciones, el de la ADT y el propio, debido a que no se había revisado el **Plan de Clasificación** del Departamento para integrar nuevos puestos.

Las situaciones comentadas en el **Apartado a.2) y 3)** se debían a que la Secretaria Auxiliar de Recursos Humanos no había actualizado los formularios **Descripción de Puesto (DTRH/16)** para incluir las funciones adicionales que realizaba el personal de la OCSI.

La situación comentada en el **Apartado b.** se debía a que la Secretaria Auxiliar de Recursos Humanos no cumplió con la disposición legal de preparar los formularios **Descripción de Puesto** mencionados.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, lo siguiente:

> Se actualizarán los deberes de la Funcionaria Administrativa III, según recomendado, para la revisión de la Secretaría Auxiliar de Recursos Humanos. **[Apartado a.2)b)]**

Se actualizarán los deberes de la Auxiliar Administrativa II, según recomendado, para la revisión de la Secretaría Auxiliar de Recursos Humanos. **[Apartado a.2)c)]**

Se añadirán a los deberes del OPI, las recomendaciones del auditor. **[Apartado a.2)d)]**

Además, indicó que el título del personal de entrada de datos es Operador de Equipo de Entrada de Información y no Operador de Equipo de Perforar y Verificar Datos. **[Apartado a.3)]**

Consideramos las alegaciones del Secretario respecto al **Apartado a.3) del Hallazgo**, pero determinamos que el mismo prevalece.

Véase la Recomendación 6.b. y c.

Hallazgo 11 - Falta de procedimientos escritos para la administración, seguridad y reglamentar las operaciones de la OCSI y ausencia de reglamentación para la administración de los recursos humanos

a. Al 2 de abril de 2007 no se habían promulgado las normas ni los procedimientos necesarios para establecer y documentar los siguientes procesos relacionados con la administración, la seguridad y el uso de los sistemas computadorizados, y para reglamentar y controlar eficazmente las siguientes operaciones de la OCSI, entre otras:

- Disposición de la información sensitiva y de los programas antes de transferir o dar de baja los equipos computadorizados y medios de almacenamiento de información
- Accesos remotos a través de *Virtual Private Network* otorgados a los usuarios
- Clasificación de los archivos de acuerdo con su importancia y con las funciones que realiza la OCSI
- Notificación del cese de un usuario en sus funciones, por motivo de renuncia, separación o traslado, a la persona encargada de la seguridad de los sistemas de información para cancelar su cuenta de acceso

- Solicitud, autorización y aprobación de los cambios a los programas y archivos en producción

- Seguridad y control de acceso a la OCSI y al área de los servidores

- Acceso a las aplicaciones del sistema operativo

- Evaluación de las funciones de los empleados para determinar el riesgo de funciones incompatibles.

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 normas, procedimientos y políticas de control interno eficaces que reglamenten las operaciones computadorizadas y estén aprobadas por la alta gerencia. Mediante las mismas se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuye a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia y facilita la labor de adiestramiento.

La situación comentada propicia que las medidas de control y las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme, lo que podría reducir su eficacia, afectar la continuidad de las operaciones y exponer la información a riesgos innecesarios. 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.

La falta de un procedimiento sobre la notificación del cese de los usuarios propició que al 20 de abril de 2007 se mantuviesen activas 13 cuentas de acceso que correspondían a empleados que dejaron de trabajar para el Departamento entre el 1 de enero de 2006 al 29 de marzo de 2007. **[Véase el Hallazgo 6-b.1)]**

La situación comentada denota que el OPI no veló por que se desarrollaran normas, procedimientos escritos y documentación sobre los procesos de borrar información sensitiva y programas antes de transferir o disponer de un equipo, accesos remotos y clasificación de archivos de la OCSI del Departamento. Además, se debía a que el Secretario en funciones no le requirió al OPI que desarrollara y sometiera a su aprobación las normas y los procedimientos necesarios para que se le informara del cese en sus funciones de los usuarios. En relación con el procedimiento para el manejo de incidentes, según el OPI, la OCSI utilizaba el plan para el manejo de incidentes de la OGP, el cual no se nos entregó para examen.

b. Al 21 de junio de 2007 el Departamento no contaba con un reglamento para la administración de los recursos humanos del servicio de carrera y de confianza.

En el **Apartado 1 de la Sección 5.4. del Artículo 5 de la Ley Núm. 184** se establece que todos los Administradores Individuales, cubiertos o no por la **Ley Núm. 45 del 25 de febrero de 1998, Ley de Relaciones del Trabajo para el Servicio Público**, deberán adoptar para sí un reglamento con relación a las áreas esenciales al principio de mérito, el cual deberá estar en armonía con las disposiciones de esta **Ley**.

La situación comentada puede ocasionar que no se administren efectivamente los asuntos relacionados con el personal de carrera y de confianza, lo cual puede tener consecuencias adversas para el Departamento.

La situación comentada se debía a que el Secretario en funciones no efectuó las gestiones necesarias dirigidas a la aprobación de un reglamento para regular la administración de los recursos humanos del Departamento.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en el **Apartado a. del Hallazgo**.

Véanse las recomendaciones 1.p. y 6.d.

Hallazgo 12 - Documentos no suministrados para examen

a. Al 3 de octubre de 2007 el OPI no nos suministró para examen los siguientes documentos o informes:

- **Plan de Contingencias** de la OCSI
- Informe sobre las pruebas realizadas a las operaciones críticas que se llevaban a cabo en la OCSI
- Inventario de los archivos de respaldos localizados en el centro alterno contratado y en el NSE
- Código de Ética de la Agencia para el Uso y Resguardo de Equipo, Programas y Datos establecido en la **Política General**.

En el **Artículo 18 del Reglamento Núm. 4284** se dispone que la documentación de una transacción oficial en una dependencia debe completarse según requerido para, entre otras cosas: facilitar información a la Rama Legislativa y a otras dependencias autorizadas sobre la manera que se llevan a cabo las transacciones del Gobierno; para proteger los derechos fiscales, legales y otros derechos del Gobierno y de personas afectadas por las transacciones del Gobierno. Se dispone, además, que al formular y llevar a cabo la política pública del Gobierno, los funcionarios del Gobierno son responsables de incluir en la documentación de sus organismos toda la información esencial de sus actividades importantes.

En el **Reglamento Núm. 23** se incluyeron las normas que rigen el archivo y la disposición de documentos fiscales del Gobierno. En dicho **Reglamento** se dispone que los documentos fiscales deben conservarse y archivarse en forma tal que se puedan localizar, identificar, y

poner a disposición del Contralor de Puerto Rico, o de cualquier otro funcionario autorizado por ley, con prontitud y en la forma deseada.

La situación comentada limitó el alcance de nuestro examen, ya que nos impidió realizar una evaluación completa de todos los documentos relacionados con la continuidad de las operaciones en el Departamento. Además, la falta de un plan de contingencias disponible podría propiciar la improvisación, y que en casos de emergencia, se tomen medidas inapropiadas y en forma desordenada. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios a los usuarios del Departamento.

Atribuimos esta situación a que el OPI no cumplió con su responsabilidad de ejercer un control del **Plan** y de los otros documentos mencionados, ni tomar las medidas necesarias para proteger adecuadamente los mejores intereses del Departamento.

El entonces Secretario, en la carta que nos envió informó, que los documentos que se indican que no fueron entregados son los mismos que se discuten en el **Hallazgo 4** de este **Informe**.

Consideramos las alegaciones del entonces Secretario respecto al **Hallazgo**, pero determinamos que el mismo prevalece.

Véase la Recomendación 8.

Hallazgo 13 - Falta de evidencia de evaluaciones periódicas al personal de la OCSI

a. Examinamos los expedientes de personal de 13 de los 30 empleados de la OCSI. Al 14 de junio de 2007 seis de estos expedientes no incluían evidencia de que se hubiesen realizado las evaluaciones periódicas correspondientes a estos empleados. Las fechas de las evaluaciones más recientes incluidas en los seis expedientes fluctuaban entre el 30 de junio de 2003 y el 10 de marzo de 2006.

   En el **Manual del Sistema de Evaluación de Desempeño** del Departamento, aprobado el 21 de julio de 2000 por la Secretaria del Departamento y la Administradora de la Oficina

Central de Asesoramiento Laboral y Administración de Recursos Humanos[15], se establece, entre otras cosas, que el ciclo de evaluación es el período de doce meses que se inicia a partir del aniversario de la fecha de nombramiento del empleado.

La ausencia de un proceso de evaluación periódico para el personal de la OCSI priva a la gerencia de una herramienta efectiva para medir las ejecutorias de sus empleados. Esto es importante para conocer las áreas en que el empleado debe mejorar y en las que sobresale con el objetivo de ofrecerle adiestramiento o compensarle por las labores realizadas.

Esta situación se debía a que la Secretaria Auxiliar de Recursos Humanos no supervisó adecuadamente el proceso de evaluación del desempeño del personal que laboraba en la OCSI, según lo establecido en el **Manual del Sistema de Evaluación de Desempeño** del Departamento.

Véase la Recomendación 6.e.

Hallazgo 14 - Inventario incompleto de programas instalados en la Red

a. Al 30 de marzo de 2007 el informe de inventario de programas instalados en la Red no incluía la cantidad de licencias existentes por cada programa instalado.

En la **Política General** se establece, entre otras cosas, que todo programa adquirido por el Departamento y sus componentes para la utilización en sus sistemas de información computadorizados, debe ser registrado propiamente e inmediatamente al ser recibido según las indicaciones en su contenido. La OCSI deberá mantener un registro de todos los programas y componentes. Además, se establece que las instalaciones de programas a nivel de redes de telecomunicaciones deberán ser controladas por el Administrador de la Red. Todos los requisitos legales, de protección, acceso, almacenamiento y seguridad de estos programas deberán ser implantados por el Administrador de la Red. El número total de licencias adquiridas deberá coincidir con el registro (inventario) en el servidor principal.

[15] Ahora Oficina de Recursos Humanos del Estado Libre Asociado de Puerto Rico (ORHELA).

La situación comentada impide ejercer un control eficaz sobre los programas y las licencias de éstos. Además, propicia la instalación y el uso de programas no autorizados, sin que esto se pueda detectar a tiempo para fijar responsabilidades, con los consiguientes efectos adversos.

La situación comentada se debía a que el OPI estableció como informe de inventario de programas el que proveía la OGP.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, que el control de inventario de programas de todas las agencias del Gobierno se lleva a través de la OGP.

Consideramos las alegaciones del entonces Secretario, pero determinamos que el **Hallazgo** prevalece.

Véase la Recomendación 1.q.

Hallazgo 15 - Falta de auditorías internas de la seguridad, los controles y las operaciones de los sistemas de información y de los procesos de autorización y acreditación de aplicaciones

a. Al 1 de mayo de 2007 la Oficina de Auditoría Interna no había efectuado evaluaciones o auditorías sobre lo siguiente:

- Los controles y las operaciones de los sistemas de información
- La seguridad de las aplicaciones más importantes del Departamento
- El proceso de autorización y acreditación de las aplicaciones antes de que se llevaran a producción.

En la **Sección 2110 de las Normas para el Ejercicio Profesional de la Auditoría Interna**, emitidas por el Instituto de Auditores Internos, se establece, entre otras cosas, que la actividad de auditoría interna debe asistir a la organización mediante la identificación y 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 las Normas para el Ejercicio Profesional de la Auditoría Interna** se establece, entre otras cosas, 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.

Es norma generalmente aceptada en el campo de los sistemas de información que durante las diferentes etapas del desarrollo y la implantación de los sistemas se requiera la participación de los auditores internos. Esta norma se fundamenta en la aportación que pueden hacer éstos en la implantación de controles adecuados. En consonancia con esta norma, la Oficina de Auditoría Interna tiene la responsabilidad de examinar las operaciones de los sistemas de información e informar a la gerencia sobre cualquier desviación de las normas establecidas.

La falta de fiscalización y de recomendaciones sobre los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados de la OCSI 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 las demás operaciones del Departamento. 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, y puede ser parte de las causas de los **hallazgos** que se comentan en este **Informe**.

Estas situaciones se debían a que la Oficina de Auditoría Interna del Departamento no contaba con personal suficiente y adiestrado en el área de auditoría de sistemas de

información. Además, no existía comunicación por parte de la gerencia de las áreas operacionales y la Oficina de Auditoría Interna sobre los procesos de autorización y acreditación de las aplicaciones.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 9.

Hallazgo 16 - Falta de independencia organizacional en las operaciones de la OCSI

a. La OCSI no tenía independencia organizacional con respecto a los usuarios que servía. Ésta le respondía a la Secretaría Auxiliar de Planificación, Investigación y Desarrollo, que era uno de sus usuarios. Dicha estructura no proveía para mantener un sistema de control administrativo adecuado y ofrecer servicios a base de las necesidades de las distintas dependencias del Departamento.

   Toda unidad de sistemas de información se debe reconocer como una unidad de servicios para todas las dependencias. Ésta debe ser independiente de las oficinas a las que sirve y solamente responder al nivel gerencial más alto de la entidad. Esto es necesario para garantizar un servicio equitativo a todos los usuarios de la OCSI.

   La situación comentada puede propiciar el uso inadecuado de los recursos computadorizados y que la utilización de los mismos se concentre en las áreas del usuario que tiene autoridad en las decisiones de la OCSI. Además, puede afectar el desarrollo de aplicaciones, y ocasionar el estancamiento en el desarrollo y la implantación de los sistemas de los demás usuarios.

   Dicha situación se debía, en parte, a que el Secretario en funciones no había clasificado a la OCSI como una unidad independiente de sus usuarios.

El entonces Secretario, en la carta que nos envió informó, entre otras cosas, que como medida correctiva se estarán realizando las gestiones pertinentes para separar la OCSI de la Secretaría Auxiliar de Planificación, y promover el reordenamiento operacional según el modelo funcional anterior.

Véase la Recomendación 10.

ANEJO

DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

OFICINA DE CÓMPUTOS Y SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Sr. Román M. Velasco González	Secretario del Trabajo y Recursos Humanos	11 ago. 06	10 oct. 07
Sra. Myrna Torres Correa	Secretaria Auxiliar de Asuntos Gerenciales	16 mar. 07	10 oct. 07
Sr. Edwin Colón Pagán	Secretario Auxiliar de Asuntos Gerenciales	11 ago. 06	15 mar. 07
Sr. Eugenio Almedina Rodríguez	Secretario Auxiliar de Planificación, Investigación y Desarrollo	11 ago. 06	10 oct. 07
Sra. Sandra Arroyo Dávila	Secretaria Auxiliar de Recursos Humanos	11 ago. 06	10 oct. 07
Sr. José A. Ríos Rivera	Oficial Principal de Informática	11 ago. 06	10 oct. 07
Sr. Juan J. Rosa Méndez	Auditor Ejecutivo	18 sep. 06	10 oct. 07