Secretaría

Lcda. Tania Barbarossa Ortiz

- ☐ Ver al dorso
- ☐ Para su información
- ☐ Notas
- ☐ Para mantenerle al día
- ☐ Expediente
- ☑ Dar Cuenta
- ☐ Registrar y Procesar
- ☐ Archivar
- ☐ Preparar Carta

Senado
DE PUERTO RICO

El Capitolio
PO Box 9023431
San Juan, Puerto Rico
00902-3431

T: 787.722.3460
787.722.4012
F: 787.723.5413
W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

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

COMISIONES ESPECIALES

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

COMISIONES CONJUNTAS

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

#861

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

RECIBIDO SECRETARIA SENADO DE P.R.
2013 AUG -1 AM 9:58

2 de abril de 2013

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Eduardo A. Bhatia Gautier
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-13-18* de la Oficina de Sistemas de Información LAN del Secretariado del Departamento de la Familia (Departamento) y la Oficina de Sistemas de Información del Departamento, aprobado por esta Oficina el 22 de marzo de 2013. Publicaremos dicho *Informe* en nuestra página en Internet: http://www.ocpr.gov.pr para conocimiento de los medios de comunicación y de otras partes interesadas.

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

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,

Yesmín M. Valdivieso

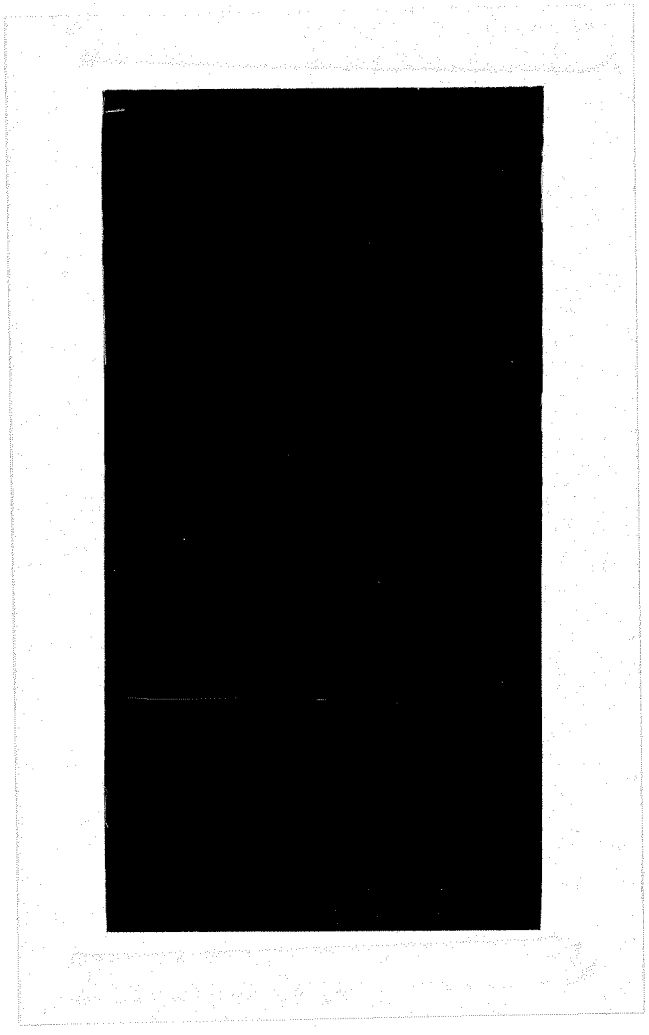
Anejo

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

#841

[redacted]

Estado Libre Asociado de Puerto Rico
Oficina del Contralor
San Juan, Puerto Rico



INFORME DE AUDITORÍA TI-13-18

22 de marzo de 2013

Departamento de la Familia

Oficina de Sistemas de Información LAN del Secretariado y la Oficina de Sistemas de Información del Departamento

(Unidad 5300 - Auditoría 13484)

Período auditado: 12 de julio de 2010 al 29 de abril de 2011

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **6**

OPINIÓN Y HALLAZGOS **7**

1 - Deficiencias relacionadas con el Avalúo de Riesgos Sistemas de Información Secretariado 2010 7

2 - Deficiencias en el Plan de Seguridad de los Sistemas de Información de la Agencia 2011 (OSI Secretariado) y en el Plan de Seguridad de la OSI Minillas 10

3 - Deficiencias en el Plan de Continuidad de Servicios Sistemas de Información Secretariado 2011 y en el Plan de Recuperación de Desastres de la OSI Minillas, y falta de documentación de los resultados de las pruebas efectuadas para certificar la efectividad del Plan de Continuidad, de almacenamiento de documentación fuera de la OSI Minillas y, de un centro alterno para la recuperación de los sistemas de información de la OSI Minillas 12

4 - Deficiencias relacionadas con la producción y el almacenamiento de los respaldos diarios de los archivos computadorizados de información mantenidos en los servidores principales de la OSI Secretariado 16

5 - Deficiencias relacionadas con los parámetros de seguridad del servidor primario de la OSI Minillas 18

6 - Documentos no suministrados para examen relacionados con la justificación y la autorización de los accesos a las cuentas con privilegios de administrador y de conexión remota a los sistemas de información 21

RECOMENDACIONES **23**

AGRADECIMIENTO **25**

ANEJO - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **26**

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

22 de marzo de 2013

Al Gobernador, y a los presidentes del Senado
y de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información LAN del Secretariado (OSI Secretariado) del Departamento de la Familia (Departamento) y la Oficina de Sistemas de Información del Departamento (OSI Minillas) para determinar si las mismas se efectuaron 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. Hicimos la misma a base de la facultad que se nos confiere en el Artículo III, Sección 22 de la Constitución del Estado Libre Asociado de Puerto Rico y, en la *Ley Núm. 9 del 24 de julio de 1952*, según enmendada.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 12 de julio de 2010 al 29 de abril de 2011. El examen lo efectuamos de acuerdo con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este *Informe* contiene seis hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, la continuidad de servicio y el acceso lógico a los sistemas de información computadorizados. El mismo está disponible en nuestra página en Internet: http://www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Departamento de Servicios Sociales se creó por virtud de la *Ley Núm. 171 del 30 de junio de 1968, Ley Orgánica del Departamento de Servicios Sociales*, según enmendada.

Mediante el *Plan de Reorganización 1* del 28 de julio de 1995, según enmendado, se redenominó y se reorganizó el Departamento de Servicios Sociales como el Departamento de la Familia, integrado por un Secretariado y cuatro componentes organizacionales: la Administración de Desarrollo Socioeconómico de la Familia (ADSEF), la Administración de Familias y Niños (ADFAN), la Administración para el Sustento de Menores (ASUME) y la Administración para el Cuidado y Desarrollo Integral de la Niñez (ACUDEN). Además, mediante este *Plan*, se adscribió al Departamento la Corporación de Industrias de Ciegos, Personas Mentalmente Retardadas y Otras Personas Incapacitadas de Puerto Rico[1].

El Departamento se creó para, entre otras funciones, promover el desarrollo de una organización dinámica que facilite, sea instrumento de cambio, y estimule al desarrollo social y económico de la familia y de la comunidad. La misión del Departamento va dirigida a facilitar y proveer oportunidades de desarrollo económico y social, de forma ágil y coherente, a las personas en desventaja social y económica. Esto, con el propósito de que las familias alcancen la autosuficiencia, la integración al desarrollo socioeconómico de manera productiva, y se fomente la buena convivencia familiar y comunitaria.

La estructura programática del Secretariado consta de tres programas:

- Programa de Determinación de Elegibilidad para Servicios de Incapacidad del Seguro Social - Este programa documenta, evalúa y adjudica toda reclamación de incapacidad que se haga al Seguro Social por trabajadores asegurados, sus viudas si tienen entre 50 y 59 años, y

[1] Esta Corporación fue creada mediante la *Ley Núm. 207 del 14 de mayo de 1948*, según enmendada.

los dependientes incapacitados de 18 años en adelante. También facilita los procedimientos de obtención de información y orienta a los reclamantes.

- Dirección y Administración General - Este programa desarrolla, integra y coordina la política pública, las normas y la reglamentación del área de familia, a ser implantadas a nivel intra e interagencial, y a través de las organizaciones comunitarias y de base de fe. Además, formula los planes y los programas, y prepara e integra el presupuesto de todo el Departamento. Finalmente, evalúa la efectividad y eficiencia de las operaciones.

- Programa de Licenciamiento de Lugares para el Cuido de Niños y Personas de Edad Avanzada - Este programa evalúa, expide licencias y supervisa los establecimientos que se dedican al cuido de niños y personas envejecientes, a tono con las leyes y los reglamentos aplicables. También licencia y supervisa personas que se dediquen a ubicar menores en centros de adopción. Su prioridad es que dicha población no sea explotada, abandonada, maltratada o expuesta a daños físicos, emocionales y sociales, de cualquier persona que intervenga directa o indirectamente con estos; además de garantizarles una mejor calidad de vida y un desarrollo pleno.

El Departamento es administrado por un Secretario nombrado por el Gobernador con el consejo y el consentimiento del Senado de Puerto Rico. Para realizar sus funciones, el Departamento cuenta con el Secretariado que es dirigido por el Secretario. El Secretariado cuenta con las secretarías auxiliares de Administración, de Planificación e Informática, y de Recursos Humanos y Relaciones Laborales; la Oficina de Auditoría Interna; la Oficina de Asesoramiento Legal; el Instituto de Educación y Adiestramiento; la Oficina del Programa de Licenciamiento; y la Oficina del Programa de Determinación de Incapacidad. Con el mismo propósito, los administradores de la ADSEF, la ADFAN, la ASUME y la ACUDEN son responsables de ejecutar la política pública establecida por el Secretario y le responden a este por el funcionamiento de los organismos

a su cargo. Además, el Departamento ofrece sus servicios a través de 10 oficinas regionales[2] y 103 oficinas locales, y cuenta con una Junta Adjudicativa que tiene la autoridad legal para considerar y resolver controversias en apelaciones iniciadas por solicitantes y participantes de servicios bajo los programas del Departamento, o cualquier otro asunto dispuesto por ley o reglamento.

A la fecha de nuestra auditoría, el Departamento cuenta con la OSI Secretariado y con la OSI Minillas, las cuales le respondían a la Secretaria Auxiliar de Planificación. La OSI Secretariado cuenta con un Ayudante Especial II que fungía como Director Interino y un Programador de Sistemas Electrónicos III. En la OSI Secretariado se mantenían ocho servidores que controlaban el acceso a la red de comunicaciones (red), y al correo electrónico, y en los que se mantenían los datos de las aplicaciones administrativas utilizadas por el personal del Secretariado. La OSI Minillas cuenta con un Director de la Oficina de Sistemas de Información, una División de Administración, una División de Apoyo Técnico OSI, una División de Control, una División de Proyectos Especiales, una División de Seguridad, un Área de Programación, un Área de Operaciones y un Área de Redes. La OSI Minillas es responsable de ofrecer el servicio de red a las oficinas locales y regionales del Departamento, y de mantener en operación las aplicaciones del Secretariado, de la ADSEF y de la ADFAN. Entre estas aplicaciones se incluyen las relacionadas con la emisión de beneficios de los programas de Asistencia Nutricional (PAN) y Ayuda Temporal para Familias Necesitadas (TANF), administrados por la ADSEF. Además, la aplicación utilizada por la ADFAN para el pago de beneficios a hogares de crianza, sustitutos y diurnos, y las aplicaciones utilizadas por el Secretariado para controlar la correspondencia, la impresión de cheques de finanzas, el inventario de alimentos, el registro de millaje y de los boletos de pago de gasolina de los vehículos oficiales, y la determinación de incapacidad, entre otras.

---

[2] Las oficinas regionales del Departamento están localizadas en Aguadilla, Arecibo, Bayamón, Caguas, Carolina, Guayama, Humacao, Mayagüez, Ponce y San Juan.

Para los años fiscales 2009-10 y 2010-11, el presupuesto del Departamento ascendió a $78,690,000 y $75,883,000. Los gastos de la OSI Secretariado eran sufragados con el presupuesto general del Secretariado y los de la OSI Minillas eran sufragados por fondos del presupuesto de la ADSEF y del Secretariado[3].

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

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

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos del 1 al 3-a. y del 3-c. al 6** de este *Informe* y varias situaciones determinadas durante la auditoría, relacionadas con los controles internos establecidos para la administración del programa de seguridad, la evaluación de la continuidad de las operaciones, el control de acceso lógico y físico, los controles de las computadoras, los procedimientos administrativos de la OSI Secretariado y la OSI Minillas, y la participación de la Oficina de Auditoría Interna del Departamento en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información fueron remitidas a la Lcda. Yanitzia Irrizarry Méndez, entonces Secretaria de la Familia, mediante carta de nuestros auditores, del 20 de mayo de 2011. En la referida carta se incluyó un anejo con detalles sobre las situaciones comentadas.

Mediante carta del 13 de junio de 2011, la entonces Secretaria de la Familia remitió sus comentarios a dichos **hallazgos**. Sus comentarios fueron considerados al redactar el borrador de este *Informe*.

---

[3] El detalle de la aportación anual del Secretariado y de la ADSEF para cubrir los gastos de OSI Minillas no pudo ser obtenido durante la auditoría. Este incluye pagos de nóminas, equipos, renta y contratos, entre otros.

El borrador de los **hallazgos** de este *Informe* se remitió a la entonces Secretaria de la Familia para comentarios, por carta del 5 de diciembre de 2012. En este se indicaron datos específicos, tales como: nombres, cuentas de acceso y localizaciones, que por seguridad no se incluyen en este *Informe*.

La Sra. Glyssette Rodríguez Cabrera, entonces Secretaria Auxiliar de Planificación del Departamento, contestó el borrador de los **hallazgos 1, 2-a., 3 del a. al c., 4-a.1), 5 y 6-a.2)** de este *Informe* mediante carta del 21 de diciembre de 2012. Sus comentarios se consideraron en la redacción final de este *Informe*, y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas revelaron que las operaciones de la OSI Secretariado y de la OSI Minillas del Departamento en lo que concierne a los controles internos para la administración del programa de seguridad, la continuidad del servicio, el control de acceso lógico y físico, la segregación de deberes, los controles de las computadoras, los procedimientos administrativos de la OSI Secretariado y de la OSI Minillas, y la participación de la Oficina de Auditoría Interna del Departamento en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 6** que se comentan a continuación.

Hallazgo 1 - Deficiencias relacionadas con el Avalúo de Riesgos Sistemas de Información Secretariado 2010

Situación

a. Un avalúo de riesgos de los sistemas de información computadorizados es un método para identificar las vulnerabilidades y las amenazas a los recursos de dichos sistemas. Mediante este se identifican los posibles daños para determinar dónde implantar las medidas de seguridad para proteger dichos recursos, de manera que no se afecten adversamente las operaciones. Este método se utiliza

para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y que respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.
- Identificar las vulnerabilidades y las amenazas de los recursos de sistemas de información.
- Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad gubernamental.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 29 de diciembre de 2010, el *Avalúo de Riesgos Sistemas de Información Secretariado 2010 (Avalúo de Riesgos 2010)*, aprobado por la Secretaria Auxiliar de Planificación y el Ayudante Especial II que fungía como Director Interino de la OSI Secretariado carecía de lo siguiente:

- La fecha de aprobación.
- Un inventario de todos los activos de sistemas de información que detallara los equipos, los programas y los datos; y la valoración y la clasificación de acuerdo con la misión y los servicios del Departamento.
- La identificación de las posibles amenazas naturales (huracanes y terremotos, entre otras) que podrían afectar los activos de sistemas de información del Secretariado.
- La documentación del análisis de impacto sobre las operaciones del Departamento en caso de que se materialice alguna amenaza. Este análisis debía considerar las vulnerabilidades existentes, los controles establecidos para proteger los activos y la probabilidad de que ocurran las amenazas identificadas en el informe.

- El plan de acción para garantizar el funcionamiento del sistema (compuesto por la OSI Secretariado y las demás oficinas de este), el cual era requerido en la sección Impacto del *Avalúo de Riesgos 2010*.
- Las conclusiones de la gerencia en respuesta a su evaluación del riesgo (aceptación, transferencia, reducción o asumir el riesgo).

Criterio

Esta situación es contraria a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular 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.

Efecto

La situación comentada impide al Secretariado estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

Causa

La situación comentada se atribuye a que la Secretaria Auxiliar de Planificación no se aseguró de que el Ayudante Especial II preparara el *Avalúo de Riesgos 2010* conforme a lo establecido en la *Carta Circular 77-05.*

Comentarios de la Gerencia

En la carta de la entonces Secretaria Auxiliar de Planificación, esta nos indicó, entre otras cosas, lo siguiente:

> La Oficina de Sistemas de Información del Secretariado (OSI-Secretariado) tomará la iniciativa de mejorar el alcance del Avalúo de Riesgos. [...] OSI-Secretariado reiniciará este proceso para lograr el cumplimiento efectivo de las actividades

> relacionadas a la contingencia y continuidad del negocio ante la eventualidad de algún desastre, accidente, acto criminal o robo que impacte adversamente las operaciones tecnológicas. [...] [*sic*]

Véase la Recomendación 1.a.

Hallazgo 2 - Deficiencias en el Plan de Seguridad de los Sistemas de Información de la Agencia 2011 (OSI Secretariado) y en el Plan de Seguridad de la OSI Minillas

Situaciones

a. Al 24 de febrero de 2011, el Secretariado del Departamento contaba con el *Plan de Seguridad de los Sistemas de Información de la Agencia 2011* (*Plan de Seguridad 2011*) aprobado el 28 de enero de 2011 por la Secretaria Auxiliar de Planificación. El examen del *Plan de Seguridad 2011* reveló que este carecía de la siguiente información que debe ser parte esencial de un plan de seguridad:

- La documentación de la validación de las normas de seguridad[4]
- La responsabilidad de la gerencia y de los demás componentes de la unidad; tales como: los dueños y los usuarios de los recursos de información, el personal a cargo del procesamiento de los datos y los administradores de la seguridad, entre otros
- Un programa de adiestramiento especializado al equipo clave de seguridad
- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, los contratistas, el personal de sistemas de información y los usuarios, y el cual 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).

---

[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.

b. Al 3 de marzo de 2011, la OSI Minillas contaba con el *Manual de Seguridad de Acceso a la Red*, aprobado el 24 de febrero de 2011 por el Director de la OSI Minillas. El examen del *Manual de Seguridad* reveló que este carecía de la siguiente información que debe ser parte esencial de un plan de seguridad:

- La documentación de la validación de las normas de seguridad
- La responsabilidad de la gerencia y de los demás componentes de la unidad; tales como: los dueños y los usuarios de los recursos de información, el personal a cargo del procesamiento de los datos y los administradores de la seguridad, entre otros
- La documentación de la interconexión de los sistemas
- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros).

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta 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.

Efectos

Las situaciones comentadas podrían provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos.

Causa

Las situaciones comentadas se atribuyen a que la Secretaria Auxiliar de Planificación no había requerido al Ayudante Especial II y al Director de la OSI Minillas que incluyera en los planes de seguridad la información que se indica en este **Hallazgo**.

Comentarios de la Gerencia

En la carta de la entonces Secretaria Auxiliar de Planificación, esta nos indicó, entre otras cosas, lo siguiente:

> En visitas hechas por los auditores del contralor se proveyó evidencia de la validación de normas de seguridad de osi-secretariado. [...] Sin embargo, estaremos considerando las recomendaciones de mejoras presentadas en éste señalamiento para mejorar el Plan de Seguridad de los Sistemas de Información aprobado recientemente. Las mejoras a ser incorporadas estarán enfocadas en proteger la información y los activos del Departamento [...]. [*sic*] **[Apartado a.]**

Consideramos las alegaciones de la entonces Secretaria Auxiliar de Planificación, pero determinamos que el **Hallazgo** prevalece. Esto, debido a que los documentos provistos por el Departamento a los auditores y los enviados con la contestación no incluían las disposiciones indicadas en el **Hallazgo**. Además, no incluían información sobre las pruebas de los controles para eliminar o mitigar las amenazas y las vulnerabilidades, y de la validación de estos mediante simulacros que permitan verificar la efectividad del plan de seguridad.

Véase la Recomendación 1.b.

Hallazgo 3 - Deficiencias en el Plan de Continuidad de Servicios Sistemas de Información Secretariado 2011 y en el Plan de Recuperación de Desastres de la OSI Minillas, y falta de documentación de los resultados de las pruebas efectuadas para certificar la efectividad del Plan de Continuidad, de almacenamiento de documentación fuera de la OSI Minillas y, de un centro alterno para la recuperación de los sistemas de información de la OSI Minillas

Situaciones

a. El examen efectuado el 10 de marzo de 2011 al *Plan de Continuidad de Servicios Sistemas de Información Secretariado 2011*, aprobado el 27 de enero de 2011 por la Secretaria Auxiliar de Planificación y el Ayudante Especial II, reveló que el mismo no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:

   - El detalle de la configuración de los equipos críticos, de las aplicaciones y del contenido de los respaldos, así como los nombres de las librerías y de los archivos

- Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar
- Los procedimientos para efectuar pruebas en el centro alterno
- Una hoja de cotejo para verificar los daños ocasionados por la contingencia.

b. El examen efectuado el 8 de marzo de 2011 al *Plan de Recuperación de Desastres* de la OSI Minillas, aprobado el 28 de diciembre de 2010 por la Secretaria de la Familia, reveló que el mismo no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:

- El detalle de la configuración de los equipos críticos, de las aplicaciones y del contenido de los respaldos, así como los nombres de las librerías y de los archivos
- Una lista del personal al cual se le distribuyó el *Plan*.

c. En la Parte IV- Procesos para desastre total de las facilidades del *Plan de Continuidad* se indicaba el uso de los servidores mantenidos en el centro alterno para restaurar las operaciones de la OSI Secretariado. Al 10 de marzo de 2011, el Ayudante Especial II no mantenía documentación sobre los resultados de las pruebas o simulacros efectuados en el centro alterno que certificaran la efectividad del *Plan de Continuidad*.

d. Al 1 de febrero de 2011, no se mantenía una copia del *Plan de Recuperación* ni de la documentación de las aplicaciones y de los equipos computadorizados en un lugar seguro fuera de las instalaciones de la OSI Minillas.

e. Al 2 de marzo de 2011, el Departamento no contaba con un centro alterno para restaurar las operaciones críticas computadorizadas de la OSI Minillas en caso de emergencia. Tampoco había formalizado acuerdos con otra entidad para establecer un centro alterno en las instalaciones de esta.

Criterios

Las situaciones comentadas en los **apartados a. y b.** son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

Las mejores prácticas en el campo de la tecnología de información establecen que se deben efectuar pruebas o simulacros de forma periódica, de acuerdo con la frecuencia requerida por el *Plan de Continuidad de Negocios*, para certificar la efectividad de este. Además, se debe mantener documentación de las estrategias utilizadas y los resultados de las pruebas realizadas. **[Apartado c.]**

Además, se requiere que las entidades gubernamentales mantengan una copia actualizada del *Plan de Continuidad de Negocios* y de la documentación de sus aplicaciones y equipos computadorizados 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. **[Apartado d.]**

También 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: **[Apartado e.]**

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

Efectos

Las situaciones comentadas en los **apartados del a. al c.** pueden propiciar la improvisación, y que en casos de emergencia se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos, e interrupciones prolongadas de los servicios ofrecidos a los usuarios de los sistemas de información y los ciudadanos que reciben beneficios del Departamento.

La situación comentada en el **apartado d.** podría ocasionar que, de ocurrir una emergencia que impida entrar a las instalaciones de la OSI Minillas, el encargado de activar el *Plan de Recuperación* no tenga acceso a este 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.

La situación comentada en el **apartado e.** podría afectar las funciones del Departamento y los servicios de la OSI Minillas, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o de un 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 OSI Minillas.

Causas

Las situaciones comentadas en los **apartados a. y b.** se debían, en parte, a que la Secretaria Auxiliar de Planificación del Departamento, no había impartido instrucciones al Ayudante Especial II ni al Director de la OSI Minillas para que consideraran los aspectos indicados. Además, no les había impartido instrucciones para que estos documentaran las pruebas de simulacro efectuadas en el centro alterno y las efectuadas al *Plan de Recuperación*. **[Apartado c.]** Tampoco había efectuado las gestiones necesarias para mantener copia del *Plan de Recuperación* y de la documentación de las aplicaciones y los equipos computadorizados en un lugar seguro fuera de los predios de la OSI Minillas. **[Apartado d.]**

La situación comentada en el **apartado e.** se atribuye a que en el Departamento no se había concluido el proceso de evaluación de estrategias para el servicio de un centro alterno.

Comentarios de la Gerencia

En la carta de la entonces Secretaria Auxiliar de Planificación, esta nos indicó, entre otras cosas, lo siguiente:

> OSI-Secretariado y OSI- Minillas poseen sus respectivos Planes de Contingencia y Continuidad del Negocio en caso de desastre [...]. Sin embargo, estaremos revisando ambos planes para lograr mayor nivel de efectividad en la ejecución de resultar algún

> evento que así lo amerite. Consideramos brindar mayores recursos al Área de Documentación de Sistemas para armonizar la documentación de los sistemas mantenidos al igual que los procedimientos de continuidad de negocio ante desastre [...]. [*sic*] **[Apartados a. y b.]**
>
> [...] Se incorporará el cuestionario de validación y aceptación de las pruebas a realizar en la activación de los planes de contingencias [...]. [*sic*] **[Apartado c.]**

Véanse las recomendaciones 1.c. y d., y 2.

Hallazgo 4 - Deficiencias relacionadas con la producción y el almacenamiento de los respaldos diarios de los archivos computadorizados de información mantenidos en los servidores principales de la OSI Secretariado

Situaciones

a. Los respaldos de dos servidores de la OSI Secretariado eran preparados de forma automatizada mediante una aplicación que mantenía un registro electrónico de los respaldos producidos. Estos respaldos incluían toda la información (*full backup*) de los correos electrónicos y los datos de las aplicaciones, de las bases de datos y de los usuarios mantenidos en los servidores. Una vez realizados, los respaldos debían ser enviados diariamente a una bóveda ubicada en el Área de Operaciones y Control de la OSI Minillas con el propósito de mantenerlos en un lugar seguro fuera de los predios donde están ubicados los servidores de la OSI Secretariado.

   El examen realizado el 10 de marzo de 2011 relacionado con los procedimientos efectuados para la producción y el almacenamiento de los respaldos de archivos computadorizados de información mantenidos en los servidores principales de la OSI Secretariado, reveló las siguientes deficiencias:

   1) El registro electrónico de los respaldos generados entre el 28 de diciembre de 2010 y el 10 de marzo de 2011 mediante la aplicación y el formulario *Registro de Cambio de Tapes de Backups* no incluían información sobre los respaldos diarios

del 29 y 30 de diciembre de 2010, del 19 y 21 de enero de 2011, del 9, 10, 11, 14, 22 y 25 de febrero de 2011, y del 1, 8 y 9 de marzo de 2011.

2) Al 9 de marzo de 2011, los respaldos diarios de archivos computadorizados de información no se mantenían en la bóveda ni en otro lugar seguro fuera de los predios de la OSI Secretariado.

Criterio

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, que deberán existir procedimientos para tener y mantener un respaldo recurrente de la información y de los programas de aplicación y de sistemas esenciales e importantes para las operaciones. En consonancia con dicha política pública, se requiere producir respaldos de la información crítica del Departamento y mantener una copia de estos 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.

Efecto

Las situaciones comentadas pueden ocasionar que en casos de emergencias el Departamento no pueda disponer de los respaldos de información necesarios para la continuidad de sus operaciones.

Causas

Las situaciones comentadas se debían a que la Secretaria Auxiliar de Planificación no se aseguró de que el Ayudante Especial II revisara diariamente el registro de los respaldos producidos por la aplicación, mantuviera un registro de las razones y las medidas tomadas en los casos en que estos respaldos no fueron realizados, y tramitara el envío de los respaldos a la caja de seguridad. Tampoco había establecido métodos alternos para efectuar el traslado de los respaldos cuando el personal que los transportaba estaba ausente y no había desarrollado un procedimiento

detallado sobre la preparación, el manejo y el almacenamiento de los respaldos de la información mantenida en los servidores de la OSI Secretariado.

Comentarios de la Gerencia

En la carta de la entonces Secretaria Auxiliar de Planificación, esta nos indicó, entre otras cosas, lo siguiente:

> [...] En OSI-Secretariado se realizan diariamente los resguardos de datos conforme a las políticas y procedimientos establecidos. [...] Reconocemos que la Data es el recurso de mayor importancia luego de los recursos humanos en el Departamento. Existen altas vulnerabilidades en las operaciones por las cuales es necesario la adquisición e implantación de un sistema de resguardo seguro, confiable y automatizado. [...] se inició un proceso de evaluación de las cotizaciones y sus respectivos ofrecimientos en cuanto a solución, configuración y costos. [...] Sin embargo, a causa de la veda electoral y el cambio de administración la orden de compra se ha quedado en espera de su final aprobación. [...] [*sic*] **[Apartado a.1)]**

Consideramos las alegaciones de la entonces Secretaria Auxiliar de Planificación respecto al **apartado a.1)** del **Hallazgo**, pero determinamos que el mismo prevalece. Esto, debido a que los documentos provistos por el Departamento a los auditores y los enviados con la contestación no incluían evidencia de los respaldos generados en las fechas comentadas ni una justificación razonable para que estos no se realizaran.

Véase la Recomendación 1.e. y f.

Hallazgo 5 - Deficiencias relacionadas con los parámetros de seguridad del servidor primario de la OSI Minillas

Situaciones

a. Al 23 de septiembre de 2010, la OSI Minillas tenía en operación un servidor para controlar la seguridad de las cuentas de los usuarios de la red, ubicados en las oficinas locales y regionales del Departamento, en la ADSEF, la ADFAN, la ACUDEN y el Secretariado.

   El examen efectuado sobre los parámetros de control de acceso y de seguridad definidos al 23 de septiembre de 2010 en el sistema

operativo de dicho servidor reveló las siguientes deficiencias en la utilización de las opciones que permiten controlar la seguridad de las cuentas de los usuarios:

1) Existían deficiencias en la activación de las políticas relacionadas con las contraseñas de las cuentas de acceso (*Account Password Policy*), según se indica:

   a) No se requería a los usuarios que utilizaran una contraseña de un mínimo de ocho caracteres. Los usuarios podían utilizar contraseñas de hasta un mínimo de seis caracteres (*Min password length: 6 chrs*).

   b) No se requería a los usuarios que cambiaran la contraseña de su cuenta de acceso al menos cada 180 días. Los usuarios podían utilizar la misma contraseña indefinidamente (*Max Password Age: 0*).

   c) No se requería un mínimo de días para que el sistema le permitiera a los usuarios cambiar la contraseña nuevamente (*Minimum Password Age: 0*). El día del cambio de la contraseña, los usuarios podían cambiarla nuevamente, lo que permitía reutilizar la contraseña anterior.

   d) No se requería a los usuarios que utilizara, al menos, un mínimo de cinco contraseñas diferentes antes de repetir una utilizada anteriormente (*Enforce Password History: 0*).

2) En la opción *Account Lockout Policy* no se había definido un término fijo de intentos de acceso sin éxito a los recursos de la red para que el sistema deshabilitara automáticamente las cuentas de acceso (*Account Lockout Not define*).

Criterios

Las situaciones comentadas en el **apartado a.1)a), b) y d)** son contrarias a lo establecido en el Artículo VII, Normas Aplicables a la Instalación de Programas, Confidencialidad y Seguridad de la Información, del *Manual de Normas sobre el uso de Tecnología de Información*, aprobado

el 3 de mayo de 2010 por la Secretaria de la Familia. En el *Manual* se establece, entre otras cosas, que las claves de acceso serán regidas por los siguientes parámetros de seguridad:

- La contraseña del usuario deberá ser de un mínimo de ocho caracteres. **[Apartado a.1)a)]**
- La contraseña deberá ser cambiada en un plazo menor a 180 días y no podrá repetir las últimas cinco contraseñas utilizadas en el sistema. **[Apartado a.1)b) y d)]**

Las situaciones comentadas en el **apartado a.1)c) y 2)** son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, 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. Esta norma se instrumenta, en parte, mediante el uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos.

Efectos

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

Causa

Las situaciones comentadas se debían, en parte, a que el Director de la OSI Minillas no había impartido instrucciones para que se pusieran en vigor, conforme a la reglamentación aplicable, las opciones de seguridad que los sistemas operativos proveen.

Comentarios de la Gerencia

En la carta de la entonces Secretaria Auxiliar de Planificación, esta nos indicó, entre otras cosas, lo siguiente:

> [...] Conforme a la magnitud de usuarios mantenidos en la plataforma de sistemas tecnológicos y la cantidad de usuarios relacionados a clientes externos y consultores de diversos proyectos de impacto en el Departamento, estaremos considerando la adquisición de una solución para el manejo y administración de las cuentas de acceso [...]. Reconocemos la importancia del control de cuentas de usuario y el aspecto de cumplimiento con la seguridad delos sistemas y la Data mantenida. Estaremos revisando la política y procedimiento para la administración y mantenimiento de las cuentas de acceso a los sistemas tecnológicos del Departamento. [*sic*]

Véase la Recomendación 1.g.

Hallazgo 6 - Documentos no suministrados para examen relacionados con la justificación y la autorización de los accesos a las cuentas con privilegios de administrador y de conexión remota a los sistemas de información

Situación

a. Al 2 de diciembre del 2010, el Director de la OSI Minillas no suministró para examen lo siguiente:

   1) Los documentos justificantes autorizados para otorgar privilegios de administrador del dominio a 56 cuentas de acceso. Una cuenta como esta tiene amplios privilegios que permiten, entre otras cosas, realizar cambios a la configuración del sistema, instalar programas y equipos, acceder a todos los archivos de la computadora, y realizar cambios a las cuentas de otros usuarios.

   2) Los documentos justificantes autorizados para proveerle a un Programador de Sistemas Electrónicos II y a un Supervisor de Sistemas de Información III el privilegio de conexión remota. Este tipo de privilegio permite acceder y utilizar la información computadorizada de una entidad desde un lugar remoto o distinto de donde se mantiene la misma.

Criterios

Las situaciones comentadas se apartan de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece que:

- La información y los programas de aplicación utilizados en las operaciones de la entidad gubernamental deberán tener controles de acceso para su utilización, de manera que solamente el personal autorizado pueda ver los datos necesarios, o usar las aplicaciones (o la parte de las aplicaciones) que necesita. Estos controles deberán incluir mecanismos de autenticación y autorización. **[Apartado a.1)]**

- Si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la entidad gubernamental (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información. **[Apartado a.2)]**

Efectos

Las situaciones comentadas impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y los privilegios a los usuarios. También propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, puede propiciar 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.

Causa

Las situaciones comentadas se debieron a que el Director de la OSI Minillas entendía que no contaba con suficientes recursos y herramientas de seguridad que facilitaran la administración de estos tipos de acceso.

Comentarios de la Gerencia

En la carta de la entonces Secretaria Auxiliar de Planificación, esta nos indicó, entre otras cosas, lo siguiente:

> [...] OSI-Minillas durante el año 2010 sufrió baja de recursos asignados a puestos de impacto en las operaciones diarias [...].

> La baja en recursos ha sido causada por retiro relacionado a cumplimiento con años de servicios, imposiciones de mejoramiento fiscal, entre otros. Como consecuencia, la segregación de las funciones se vio afectada para lograr cumplir con el control y salvaguarda requerida en la otorgación y administración de los privilegios de las cuentas de acceso a los sistemas de manera remota. Además, durante el año 2012 en la restructuración de la oficina se adquirió un Firewall de alta capacidad para manejar los accesos a los sistemas de información. [*sic*] **[Apartado a.2)]**

Consideramos las alegaciones de la entonces Secretaria Auxiliar de Planificación respecto al **apartado a.2)** del **Hallazgo**, pero determinamos que el mismo prevalece. Esto, debido a que las medidas implantadas por el Departamento no son suficientes para asegurar que se documente la justificación y la autorización para otorgar cuentas de acceso con privilegios de administrador del dominio y con privilegio de conexión remota a sus sistemas computadorizados.

Véase la Recomendación 1.h.

RECOMENDACIONES

A la Secretaria de la Familia

1. Ejercer una supervisión efectiva sobre la Secretaria Auxiliar de Planificación para asegurarse de que:

    a. Se incluyan en el avalúo de riesgos los elementos mencionados en el **Hallazgo 1**. El informe producto de este avalúo de riesgos debe ser remitido para su aprobación.

    b. Revise y actualice el *Plan de Seguridad 2011* y el *Manual de Seguridad* para que se incluyan los criterios descritos en el **Hallazgo 2** y los remita para su aprobación. Una vez aprobado, se asegure de que se divulgue a los funcionarios y a los empleados, y se revise periódicamente.

    c. Revise y actualice el *Plan de Continuidad* y el *Plan de Recuperación* para que se incluyan los aspectos comentados en el **Hallazgo 3-a. y b.** y los remita para su aprobación. Además, se asegure de que se efectúen, si aún no se ha hecho, pruebas o

simulacros al *Plan de Continuidad* que certifiquen su efectividad, y se mantenga la documentación de las estrategias utilizadas y los resultados de las pruebas. **[Hallazgo 3-c.]**

d. Efectúe las gestiones necesarias para mantener copia del *Plan de Recuperación*, y de la documentación de las aplicaciones y de los equipos computadorizados en un lugar seguro fuera de los predios donde están instalados los equipos computadorizados. **[Hallazgo 3-d.]**

e. Imparta instrucciones al Ayudante Especial II para que revise diariamente el registro de los respaldos producidos, mantenga un registro de las razones y medidas tomadas en los casos en que estos respaldos no sean realizados, y tramite el envío de los respaldos a un lugar seguro fuera de las instalaciones del Secretariado. Además, establezca métodos alternos para efectuar el traslado de los respaldos cuando el personal de transporte se ausente. **[Hallazgo 4]**

f. Desarrolle un procedimiento detallado sobre la preparación, el manejo y el almacenamiento de los respaldos de la información mantenida en los servidores de la OSI Secretariado y lo remita para aprobación. **[Hallazgo 4]**

g. El personal encargado de administrar los sistemas de la OSI Minillas efectúe las modificaciones en los parámetros de seguridad del sistema operativo para:

1) Requerir a los usuarios que utilicen una contraseña de un mínimo de ocho caracteres y que cambien la misma cada 180 días, según requerido en el *Manual*. **[Hallazgo 5-a.1)a) y b)]**

2) Establecer un tiempo mayor al actualmente definido para efectuar los cambios de contraseñas nuevas y aumentar la cantidad de contraseñas diferentes antes de poder repetir una utilizada anteriormente. **[Hallazgo 5-a.1)c) y d)]** Además, establecer un número razonable de intentos de

acceso sin éxito permitidos a los usuarios antes de inactivar la cuenta. **[Hallazgo 5-a.2)]** Esto, de manera que se reduzcan las posibilidades de que personas no autorizadas puedan acceder indebidamente los sistemas de información.

h. Los accesos con privilegios de administrador del dominio y de conexión remota estén debidamente justificados, autorizados y documentados. **[Hallazgo 6]**

2. Formalizar un acuerdo escrito con un centro alterno que acepte la utilización de sus respectivos equipos en caso de desastres o emergencias en el lugar donde están instalados los equipos computadorizados, o considerar establecer su propio centro alterno en alguna instalación que no esté expuesta a los mismos riesgos que dicho lugar. **[Hallazgo 3-e.]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yesmín M. Valdivieso

ANEJO

DEPARTAMENTO DE LA FAMILIA

OFICINA DE SISTEMAS DE INFORMACIÓN LAN DEL SECRETARIADO
Y OFICINA DE SISTEMAS DE INFORMACIÓN DEL DEPARTAMENTO

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD

DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcda. Yanitzia Irizarry Méndez	Secretaria	12 jul. 10	29 abr.11
Sra. Glyssette Rodríguez Cabrera	Secretaria Auxiliar de Planificación	12 jul. 10	29 abr. 11
Sr. Jesús A. Cruz Morales	Director de la Oficina de Sistemas Información	12 jul. 10	29 abr. 11
Sr. Rafael Cruz Acevedo	Ayudante Especial II	12 jul. 10	29 abr. 11

MISIÓN

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

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

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

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

QUERELLAS

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

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

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

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

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

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

http://www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr