Estado Libre Asociado de Puerto Rico
Oficina del Contralor

(B)

14862
PRESIDENCIA DEL SENADO
RECIBIDO MAR21'19 PM 4:08

Yesmín M. Valdivieso
Contralora

21 de marzo de 2019

#14302
SECRETARIA DEL SENADO
RECIBIDO MAR21'19 PM 2:08

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

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

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-19-05* de la Oficina de Sistemas de Información de la Defensoría de las Personas con Impedimento del Estado Libre Asociado de Puerto Rico, aprobado por esta Oficina el 18 de marzo de 2019. Publicaremos dicho *Informe* en nuestra página en Internet: 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: www.ocpr.gov.pr
www.facebook.com/ocpronline *www.twitter.com/ocpronline*

INFORME DE AUDITORÍA TI-19-05

18 de marzo de 2019

Defensoría de las Personas con Impedimentos del Estado Libre Asociado de Puerto Rico

Oficina de Sistemas de Información

(Unidad 5366 - Auditoría 14190)

Período auditado: 1 de marzo al 8 de diciembre de 2017

CONTENIDO

Página

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

18 de marzo de 2019

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

Incluimos los resultados de la auditoría de tecnología de información que realizamos a la Oficina de Sistemas de Información (OSI) de la Defensoría de las Personas con Impedimentos del Estado Libre Asociado de Puerto Rico (Defensoría). 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; y en cumplimiento de nuestro *Plan Anual de Auditorías*.

OBJETIVOS DE AUDITORÍA

Objetivo general

Determinar si las operaciones de la OSI de la Defensoría se realizaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

1. Determinar si las operaciones de la OSI de la Defensoría, en lo que concierne a los controles internos para la administración de la seguridad y la continuidad del servicio, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

2. Determinar si las operaciones de la OSI de la Defensoría, en lo que concierne a los controles para el acceso lógico, y la entrada y salida de datos para el Sistema de Manejo de Casos, se efectuaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

Este informe contiene cinco hallazgos del resultado del examen que realizamos de los objetivos indicados en la sección anterior. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de marzo al 8 de diciembre de 2017. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Standards*, emitido por la Oficina de Rendición de Cuentas del Gobierno de Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a las auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos la auditoría para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de la auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas tales como: entrevistas a funcionarios y empleados; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la entidad auditada; pruebas y análisis de procedimientos de control interno, y de otros procesos; y confirmaciones de información pertinente.

Al realizar esta auditoría, utilizamos el *Procedimiento Operacional de la Oficina de Sistemas de Información* (*Procedimiento Operacional)*, aprobado el 21 de marzo de 2005 por el procurador de las personas con impedimentos. Además, utilizamos las políticas establecidas en la *Carta Circular 140-16, Normas Generales sobre la Implantación de Sistemas, Compra de Equipos y Programas y Uso de la Tecnología de Información para los Organismos Gubernamentales*, aprobada el 7 de noviembre de 2016 por el director de la Oficina de Gerencia y Presupuesto. Para las áreas relacionadas con el plan de contingencia, el centro alterno y el almacenamiento de los respaldos en un lugar distante y seguro, que no estaban consideradas en el *Procedimiento Operacional* y las políticas, utilizamos como mejor práctica las guías establecidas en el

Federal Information System Controls Audit Manual (*FISCAM*)[1], emitido por el GAO. Esto, porque aunque a la Defensoría no se le requiere cumplir con dichas guías, entendemos que estas representan las mejores prácticas en el campo de la tecnología de información, al examinar los sistemas computadorizados de las entidades gubernamentales.

Consideramos que la evidencia obtenida proporciona una base razonable para nuestra opinión y hallazgos.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Defensoría fue creada mediante la *Ley 158-2015*, *Ley de la Defensoría de las Personas con Impedimentos del Estado Libre Asociado de Puerto Rico*, según enmendada. Esta *Ley* derogó la *Ley 78-2013*, *Ley del Procurador de las Personas con Impedimentos del Estado Libre Asociado de Puerto Rico,* según enmendada, que creó la Oficina del Procurador de Personas con Impedimentos (OPPI)[2].

La Defensoría es una entidad jurídica independiente y separada, con autonomía fiscal, programática y administrativa, que tiene entre sus funciones fiscalizar y promover la defensa de los derechos de las personas con impedimentos[3]. Mediante procesos educativos y fiscalizadores, la Defensoría vela por la erradicación del discrimen por razón de impedimento físico o mental; toma acciones en contra del abuso o negligencia u otras formas de negación de derechos; y garantiza que se establezcan e implanten prácticas y condiciones idóneas en instituciones, hospitales o programas para personas con impedimentos. Además, es el

[1] El *FISCAM* está de acuerdo con las guías emitidas por el *National Institute of Standards and Technology*, entre estas, la publicación especial 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* y 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*.

[2] La OPPI se creó mediante la *Ley Núm. 2 del 27 de septiembre de 1985, Ley de la Oficina del Procurador de las Personas con Impedimentos*, según enmendada. Dicha *Ley* fue derogada por el *Plan de Reorganización 1-2011, Plan de Reorganización de las Procuradurías*. Este creó la Oficina de Administración de las Procuradurías y consolidó las oficinas del procurador de la Salud, las Personas Pensionadas y de la Tercera Edad, los Veteranos y las Personas con Impedimentos. La *Ley 78-2013* creó nuevamente la OPPI como un ente jurídico de forma independiente de cualquier otra agencia o entidad pública.

[3] Toda persona que tiene un impedimento físico, cognitivo, mental o sensorial que limita sustancialmente una o más actividades esenciales de su vida; o que tiene un historial o récord médico de impedimento físico, mental o sensorial; o es considerada que tiene un impedimento físico, mental o sensorial.

ente encargado de fiscalizar la implementación y el cumplimiento, por las agencias y entidades privadas, de la política pública dispuesta en la *Ley 238-2004, La Carta de Derechos de las Personas con Impedimentos*, según enmendada.

La Defensoría cuenta con el Consejo Directivo para la Defensa de las Personas con Impedimentos (Consejo Directivo) que está compuesto por 9 personas. De estas, 3 son nombradas por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico, y 6 son nombradas por organizaciones no gubernamentales que están relacionadas con la defensa de los derechos de las personas con impedimentos. El Consejo Directivo es responsable de nombrar al defensor de las Personas con Impedimentos (defensor); fiscalizar su desempeño y el cumplimiento con la política pública relacionada con los derechos de las personas con impedimentos; y velar por la gobernanza, autonomía, transparencia y rendición de cuentas de la Defensoría. Además, junto con el defensor, establece las políticas internas y los planes estratégicos relativos a la defensa de los derechos de las personas con impedimentos.

El defensor es nombrado por un término de seis años y es responsable de dirigir y supervisar la operación de la Defensoría; aprobar los reglamentos que rigen las funciones de esta; fiscalizar la implementación y el cumplimiento de la política pública en torno a las personas con impedimentos; elaborar informes anuales sobre el estado de los derechos de las personas con impedimentos; y remitir al Consejo Directivo informes trimestrales con respecto al progreso de su ejecución y la implementación del plan integral establecido, entre otros.

A la fecha de nuestra auditoría, la estructura organizacional de la Defensoría estaba compuesta por el área de Administración[4]; el programa de Carta de Derechos de las Personas con Impedimentos; y las oficinas de Asuntos Legales, Oficiales Examinadores y Sistemas de Información.

[4] El Área de Administración la componían las oficinas de Recursos Humanos, Finanzas, Presupuesto, y Servicios Generales.

Además, contaba con 1 Oficina Central ubicada en San Juan y 4 oficinas regionales en Arecibo, Humacao, Mayagüez y Ponce. También estaba adscrita a la Defensoría, la División para la Protección y la Defensa de las Personas con Impedimentos que tenía independencia administrativa y fiscal, y respondía directamente al Consejo Directivo. Esta División era dirigida por 1 director ejecutivo, quien era nombrado por el Consejo Directivo y ofrecía asistencia legal, administrativa y de cualquier otro remedio a la población de personas con impedimentos. Esto, mediante los siguientes 8 programas federales:

- Programa de Protección y Defensa de los Derechos de los Electores con Impedimentos (HAVA)
- Programa de Protección y Defensa del Usuario de Asistencia Tecnológica (PAAT)
- Programa de Asistencia al Cliente de Rehabilitación Vocacional (CAP)
- Programa de Protección y Defensa de los Derechos de las Personas con Lesión Cerebral Traumática (PATBI)
- Programa de Protección y Defensa de los Derechos de los Beneficiarios del Seguro Social por Incapacidad (PABSS)
- Programa de Protección y Defensa de los Derechos de las Personas con Impedimentos (PAIR)
- Programa de Protección de los Derechos de las Personas con Deficiencias en el Desarrollo (PADD)
- Programa de Protección y Defensa de las Personas con Condiciones Mentales (PAIMI).

La OSI contaba con un director de sistemas de información, quien le respondía al defensor. La OSI tenía vacantes los puestos de especialista de sistemas de información y administradora de sistemas de oficina.

La infraestructura tecnológica de la Defensoría estaba compuesta por 4 redes de comunicación de área local (*LAN*, por sus siglas en inglés) que funcionaban de forma independiente y estaban ubicadas en la Oficina Central de San Juan y en las oficinas regionales de Humacao, Mayagüez y Ponce. Además, al 5 de abril de 2017, la Defensoría contaba con 20 servidores físicos, y tenía 83 usuarios de la red, Internet y el correo electrónico. Para realizar sus funciones principales, la Defensoría contaba con 2 sistemas de información computadorizados:

- Sistema de Manejo de Casos - Diseñado para el registro y manejo de la información de las personas con impedimentos, las orientaciones, y los casos y las estadísticas internas relacionadas con los servicios ofrecidos. Esta información era utilizada para la redacción de los informes federales preparados en la Defensoría.

- Sistema de Manejo de la *Ley 238* - Diseñado para el registro y manejo de información de las agencias, los servicios que estos han prestados a las personas con impedimentos y los acomodos que han ofrecido a sus empleados. Este sistema era utilizado por los empleados asignados como enlace en cada agencia del gobierno y un empleado de la Defensoría asignado a esta área.

Además, utilizaba el *Puerto Rico Integrated Financial Accounting System (PRIFAS)* y el Sistema de Recursos Humanos Mecanizados (RHUM) del Departamento de Hacienda para el registro de las operaciones financieras y el procesamiento de la nómina.

Los recursos para financiar las actividades operacionales de la Defensoría provienen de asignaciones especiales, fondos federales y la resolución conjunta del presupuesto general. Los gastos operacionales de la OSI son sufragados del presupuesto operacional de la Defensoría que, para los años fiscales del 2015-16 al 2017-18, ascendió a $3,663,000, $3,503,000 y $2,721,000, respectivamente.

Los **anejos 1 y 2** contienen una relación de los funcionarios principales que actuaron durante el período auditado.

La Defensoría cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: www.dpi.pr.gov. Esta página provee información acerca de los servicios que presta dicha entidad.

COMUNICACIÓN CON LA GERENCIA

El borrador de este *Informe* se remitió para comentarios, por carta del 23 de enero de 2019, al Sr. Gabriel E. Corchado Méndez, defensor interino. En el mismo se indicaron datos específicos, tales como los nombres de las oficinas regionales.

Con el mismo propósito, remitimos el borrador de los hallazgos de este *Informe* al Sr. Frank Pérez Concepción, exdefensor; y del **Hallazgo 4**, a la Sra. Carmen J. Collazo Fernández, entonces defensora interina y directora ejecutiva, mediante cartas del 23 de enero de 2019. Además, el 6 de febrero de 2019, le remitimos el borrador del **Hallazgo 4** al Sr. Ivan Díaz Carrasquillo, exprocurador.

Los señores Pérez Concepción y Díaz Carrasquillo contestaron el borrador de este *Informe* mediante cartas del 14 y 17 de febrero de 2019. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

El defensor interino y la entonces defensora interina y directora ejecutiva, no contestaron.

CONTROL INTERNO

La gerencia de la Defensoría es responsable de establecer y mantener una estructura del control interno efectiva para proveer una seguridad razonable en el logro de:

- la eficiencia y eficacia de las operaciones
- la confiabilidad de la información financiera
- el cumplimiento de las leyes y la reglamentación aplicables.

Nuestro trabajo incluyó la comprensión y evaluación de los controles significativos para los objetivos de este *Informe*. Utilizamos dicha

evaluación como base para establecer los procedimientos de auditoría apropiados a las circunstancias; pero no con el propósito de expresar una opinión sobre la efectividad de la estructura del control interno de la Defensoría.

En los **hallazgos** de este *Informe* se comentan las deficiencias de controles internos significativas, dentro del contexto de los objetivos de nuestra auditoría, identificadas a base del trabajo realizado.

Las deficiencias comentadas no contienen necesariamente todos los aspectos de control interno que pudieran ser situaciones objeto de hallazgo. Esto, debido a que dichas deficiencias fueron identificadas como resultado de la evaluación de las operaciones, los procesos, las actividades y los sistemas relacionados con los objetivos de la auditoría.

OPINIÓN Y HALLAZGOS

Opinión cualificada

Las pruebas efectuadas y la evidencia en nuestro poder revelaron que las operaciones de la OSI de la Defensoría, en lo que concierne a los controles objeto de este *Informe*, se realizaron, en todos los aspectos significativos, de acuerdo con las normas y la reglamentación aplicables; y que dichos controles eran efectivos. Esto, excepto por los **hallazgos del 1 al 5** que se comentan a continuación.

Hallazgo 1 - Falta de un informe de análisis de riesgos de los sistemas de información computadorizados

Situación

a. El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información computadorizados existentes en la entidad, sus vulnerabilidades y las amenazas a las que se encuentran expuestos, así como la probabilidad de ocurrencia y el impacto de las mismas. Esto, con el fin de determinar las medidas de seguridad y los controles adecuados a ser implementados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo, y

proteger dichos activos, de manera que no se afecten adversamente las operaciones de la entidad. Este proceso asegura que las medidas de seguridad y los controles a ser implementados sean costo-efectivos, pertinentes a las operaciones de la entidad y que respondan a las posibles amenazas identificadas.

Al 5 de abril de 2017, en la Defensoría no se había preparado un análisis de riesgos de los sistemas de información computadorizados.

Criterios

La situación comentada se aparta de lo establecido en las políticas *ATI-003, Seguridad de los Sistemas de Información*, y *ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*.

Efectos

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

Causa

La situación comentada se atribuye a que el director de sistemas de información no había recibido adiestramientos relacionados con la preparación de un análisis de riesgos.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Plan de Contingencia ante Situaciones de Emergencia no actualizado y falta de un centro alterno para la recuperación de los sistemas de información

Situaciones

a. El 21 de marzo de 2005 el procurador de la OPPI aprobó el *Procedimiento Operacional* que incluía como anejo el *Plan de Contingencia ante Situaciones de Emergencia* (*Plan*). El *Plan* tenía como objetivo garantizar la continuidad de las operaciones de los servicios brindados mediante los sistemas de información, ante eventualidades que pudieran afectar su funcionamiento.

El examen realizado el 20 de abril de 2017 al *Plan* reveló que no estaba actualizado. Este no incluía los cambios organizacionales, de infraestructura tecnológica y de personal ocurridos en la Defensoría, según se indica:

1) En el Apartado II, Trasfondo, y IV, Orden de Instalación y Configuración de los Equipos, se incluían los requerimientos y procesos de restauración para equipos que tenían instalados sistemas operativos *Windows 2000 Server, Windows 98, XP y 2000*. A la fecha de nuestro examen, estos sistemas operativos no eran los utilizados en los servidores y en las computadoras de la Defensoría.

2) En el Apartado II.B, Resguardo de Información (*Backup*), se requería el cumplimiento con el procedimiento establecido en el Documento 7, Disposición de Resguardos y Documentos de Sistemas de Información del *Procedimiento Operacional*. Sin embargo, en este *Procedimiento* y en el *Plan* no se consideraban los respaldos que realizaba el director de sistemas de información en un disco externo y la necesidad de mantener copia de estos en un lugar distante de la Defensoría. Estos respaldos incluían una copia del Sistema de Manejo de Casos, de los servidores de archivo que incluían los documentos preparados en las diferentes oficinas de la Defensoría y del servidor de la página en Internet.

3) En el Anejo I, OPPI-Inventario de Sistemas, no se incluían los servidores, las computadoras, las impresoras y los equipos de comunicación que fueron adquiridos entre el 11 de septiembre de 2014 y el 30 de septiembre de 2016. Además, no se había actualizado la información de los equipos de la Oficina Regional de Aguada que, desde el 21 de junio de 2016, había sido trasladada a la Oficina Regional de Mayagüez.

4) En el Anejo IV, Grupos de Trabajo; en la Hoja de Participación del Anejo VI, Procedimiento de Prueba del Plan de

Contingencia; y en Anejo VII, Forma de Recibo de Plan de Contingencia; se incluía la información de contacto de 12 empleados que, a la fecha de la auditoría, no laboraban en la Defensoría. Además, el defensor estaba incluido como director de la Oficina Regional de Arecibo, y la directora de la Oficina Regional de Humacao, como especialista de sistemas de información.

5) En el *Plan* se hacía referencia a la agencia como la OPPI en vez de la Defensoría.

b. Al 5 de abril de 2017, la Defensoría no contaba con un centro alterno para restaurar las operaciones del Sistema de Manejo de Casos y del Sistema de Manejo de la *Ley 238,* en casos de emergencias que afectaran los servidores y las bases de datos ubicados en la Oficina Central y en tres de las oficinas regionales.

Situaciones similares a las de los **apartados a. del 2) al 4) y b.** fueron comentadas en el *Informe de Auditoría TI-05-05*.

Criterios

Las situaciones comentadas en el **apartado a.** son contrarias a lo establecido en el *Procedimiento Operacional*. En este se establece que los procedimientos y formularios incluidos en el mismo estarán sujetos a revisión continua por parte del equipo de trabajo de la OSI, quien referirá cualquier enmienda para ser considerada.

Además, las situaciones comentadas son contrarias a lo sugerido en el Capítulo 3.5, *Contingency Planning* del *FISCAM*. En este se sugiere que el plan de contingencia debe estar actualizado e incluir toda la información y los procesos necesarios para recuperar las operaciones de los sistemas de información computadorizados. **[Apartado a.]** También sugiere que, como parte integral del plan de continuidad de negocios, deban existir convenios donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. En dichos convenios debe incluirse una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. **[Apartado b.]**

Efectos

La situación comentada en el **apartado a.** podría propiciar la improvisación, y que, en casos de emergencia, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios a los usuarios de la Defensoría.

Lo comentado en el **apartado b.** podría afectar las operaciones de la Defensoría, ya que no tendrían disponibles unas instalaciones para operar sus sistemas principales después de una emergencia o evento que afecte su funcionamiento. Esto, podría atrasar o impedir el proceso de restauración de los archivos y el pronto restablecimiento de las operaciones normales de la Defensoría.

Causas

La situación comentada en el **apartado a.** se atribuye a que el director de sistemas de información desconocía de la existencia del *Plan*.

Lo comentado en el **apartado b.** se atribuye a la disminución de presupuesto operacional y disponibilidad de fondos para adquirir la infraestructura o servicios necesarios para establecer un centro alterno.

Véanse las recomendaciones 1, y 3.a. y b.

Hallazgo 3 - Deficiencias relacionadas con la documentación de las cuentas de acceso de los sistemas computadorizados y la administración de las cuentas de acceso activas del Sistema de Manejo de Casos

Situaciones

a. El director de sistemas de información era el responsable de la creación y eliminación de las cuentas de acceso a los sistemas computadorizados de la Defensoría. Para obtener acceso a estos sistemas, el usuario debía completar el *Formulario para Solicitar, Renovar, Cambiar o Retirar Cuentas* (*Formulario*), requerido en el Documento I, Procedimiento de Seguridad, del *Procedimiento Operacional.* El *Formulario* requería el nombre de usuario, el programa al que fue asignado, el tipo de acceso, y los directorios,

sistemas y horarios de acceso solicitados. Además, requería la fecha de aprobación, y la firma del supervisor del empleado y del director de sistemas de información.

El examen realizado el 19 de abril de 2017 sobre el proceso de la solicitud, creación, modificación y cancelación de las cuentas de acceso reveló que el director de sistemas de información no requería el *Formulario* para documentar la creación de las cuentas de acceso. En su lugar, las solicitudes eran realizadas mediante llamada telefónica o correos electrónicos enviados por el administrador de sistemas de oficina de Recursos Humanos. Los correos electrónicos carecían de información relacionada con el nombre del programa a donde fue asignado el empleado, los privilegios de acceso solicitados, y la aprobación del supervisor inmediato y del director de sistemas de información.

b. Al 23 junio 2017, el Sistema de Manejo de Casos tenía 55 cuentas de acceso activas. A estas, se les asignaban privilegios para acceder a toda la información (*Full*), a la de más de un área (*Medium*) o acceder solo a la del área o programa al que estaba asignado (*Basic*).

El examen realizado el 12 de julio de 2017 de estas cuentas de acceso reveló que no se habían desactivado 4 cuentas que estaban asignadas a un exconsultor que no ofrecía servicios en la Defensoría desde el 2016. De estas, 3 tenían privilegios de acceso *Full* a la información de 3 oficinas regionales y 1 tenía privilegio de acceso *Medium* a la información de una oficina regional.

Criterios

La situación comentada en el **apartado a.** es contraria a lo establecido en el Documento I del *Procedimiento Operacional*. En este se establece que los directores y coordinadores de las áreas de trabajo determinan y recomiendan por escrito el acceso que se le dará a sus subalternos. Los mismos solicitarán el nivel de acceso mediante el *Formulario* y el acceso o privilegio concedido estará limitado al propósito indicado en este.

La situación comentada en el **apartado b.** es contraria a lo establecido en la *Política ATI-003* de la *Carta Circular 140-16*.

Efectos

Las situaciones comentadas impiden a la Defensoría mantener un control adecuado sobre la administración de las cuentas. Además, propicia que personas puedan utilizar estas cuentas para lograr accesos no autorizados a información confidencial mantenida en los sistemas de información y hacer uso indebido de esta. También propicia la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información computadorizados sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causas

Las situaciones comentadas se atribuyen a que el director de sistemas de información desconocía sobre la existencia del *Formulario*, y utilizaba las cuentas asignadas al exconsultor para administrar el Sistema de Manejo de Casos y la red.

Comentarios de la Gerencia

El exdefensor nos indicó, entre otras cosas, lo siguiente:

> Como Defensor de las Personas con Impedimentos, nos consta que existían formularios para designar cuentas a los empleados. Por ende, era responsabilidad del Director de Sistemas utilizar los formularios al momento de crear cuentas a los usuarios con los privilegios correspondientes según sus funciones. [*sic*] **[Apartado a.]**

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

Hallazgo 4 - Deficiencias relacionadas con la utilización del Sistema de Manejo de Casos

Situaciones

a. Los coordinadores de los ocho programas federales de la División para la Protección y Defensa de las Personas con Impedimentos y los directores de las oficinas regionales de la Defensoría debían preparar y remitir los informes estadísticos estatales mensualmente a la coordinadora interagencial de la Defensoría. Estos informes incluían

información sobre los casos nuevos y los cerrados en la Defensoría, la asistencia técnica provista a los clientes, los referidos gestionados con otras agencias gubernamentales o entidades sin fines de lucro, y las orientaciones y actividades educativas ofrecidas. Además, los coordinadores debían preparar y enviar a la coordinadora interagencial un informe estadístico federal para la preparación de propuestas y la medición de la ejecución de los programas. Estos informes contenían información general de la agencia, los servicios provistos a los individuos, los programas y las actividades relacionadas con los litigios, y ejemplos de casos atendidos.

Desde el 2004, la Defensoría utilizaba el Sistema de Manejo de Casos. Este era un registro automatizado que mantenía información de sus clientes y un historial de los servicios ofrecidos. Además, contaba con tres secciones para producir informes de los casos por región, orientaciones ofrecidas y estadísticas de servicios, entre otros.

El examen efectuado sobre la utilización del Sistema reveló las siguientes deficiencias:

1) Al 31 de mayo de 2017, los empleados de una oficina regional de la Defensoría no utilizaban el Sistema para registrar la información de las personas con impedimentos y los servicios ofrecidos mediante los programas administrados por la Defensoría.

2) Al 1 de diciembre de 2017, la información en el Sistema contenía errores y estaba incompleta, por lo que no se utilizaba para preparar los informes requeridos por el gobierno estatal y federal.

Una situación similar al **apartado a.1)** fue comentada en el *Informe de Auditoría TI-05-09*.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política ATI-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular 140-16.*

Efectos

Las situaciones comentadas ocasionaban que los coordinadores tuvieran que preparar manualmente los informes estadísticos de cada programa para referirlos a la coordinadora interagencial. Además, ocasionaba que la coordinadora interagencial tuviera que utilizar hojas de trabajo creadas en *MS Word* y *MS Excel* para preparar los informes estadísticos requeridos a la Defensoría. Esto, retrasaba la preparación de los informes requeridos.

También, la situación comentada en el **apartado a.1)** privó a la Defensoría de un registro computadorizado que incluyera la información de las personas con impedimentos y los servicios ofrecidos en la oficina regional comentada. Esto provocó que, en septiembre de 2017, la Defensoría no pudiera recuperar la información de los expedientes físicos que perdió como resultado de los daños ocasionados por el huracán María.

Causas

La situación comentada en el **apartado a.1)** se debía a que, desde el 2010, se había dañado el servidor donde residía localmente el Sistema de Manejo de Casos en la oficina regional. Además, los fondos para adquirir un servidor nuevo se obtuvieron en el 2016 y, desde esa fecha, el director de sistemas de información no había instalado el servidor adquirido.

La situación comentada en el **apartado a.2)** se debía a que la directora ejecutiva de la División para la Protección y Defensa de las Personas con Impedimentos no había realizado un estudio sobre las necesidades de adiestramientos de los funcionarios y empleados responsables de registrar la información en el Sistema de Manejo de Casos. Esto, para corregir las deficiencias identificadas en el registro de la información. Además, se debía a que el Sistema no incluía la información de la oficina regional.

Comentarios de la Gerencia

El exdefensor de la Defensoría nos indicó, entre otras cosas, lo siguiente:

> En el 2016 como Defensor se identificaron fondos y se adquirieron seis (6) servidores nuevos para reemplazar los existentes y a su vez crear una copia de seguridad. Debido a la situación crítica de (…), era nuestra prioridad instalar uno en dicha región. Al momento de cesar funciones, por diferencias con el Consejo Directivo y la poca experiencia de la Directora Ejecutiva

> no se lograron instalar. Cabe señalar, que todas las irregularidades en el área de programas es responsabilidad de la Directora Ejecutiva. En el día de hoy todavía la Oficina Regional de (…) opera con altas deficiencias. [*sic*]

Véanse las recomendaciones 1, 3.e. y 4.

Hallazgo 5 - Deficiencia en el almacenamiento de los respaldos de los servidores de la Defensoría

Situación

a. El director de sistemas de información realizaba los respaldos diarios y mensuales del Sistema de Manejo de Casos, y mensuales de dos servidores de archivos y del servidor de la página en Internet de la Defensoría. El examen efectuado el 1 de junio de 2017 reveló que no se protegían adecuadamente los respaldos de los servidores de la Defensoría. El director de sistemas de información mantenía estos respaldos grabados en un disco duro externo ubicado en la OSI y no producía una copia adicional para mantenerla en un lugar seguro y distante de la Oficina Central de la Defensoría.

Criterio

La situación comentada es contraria a lo sugerido en el Capítulo 3.5, *Contingency Planning* del *FISCAM*. En este se sugiere que las copias de la información que sean necesarias para mantener las operaciones deben mantenerse en lugares distantes de la entidad. Esto, con el propósito de que no estén expuestos a las mismas amenazas y estén disponibles en caso de una emergencia o desastre.

Efecto

La situación comentada puede ocasionar que, en casos de desastre, la Defensoría no pueda disponer de los respaldos de información necesarios para la continuidad de las operaciones.

Causa

La situación comentada se debía a que, hasta el 17 de mayo de 2017, el director de sistemas de información no tuvo acceso a la caja de seguridad que la Defensoría tenía arrendada en una institución bancaria ubicada

frente a la Oficina Central. Además, el edificio donde se mantenía dicha caja estaba expuesto a las mismas amenazas de desastre que la Oficina Central en la que estaban los servidores y los respaldos.

Véanse las recomendaciones 1 y 3.f.

RECOMENDACIONES

Al Consejo Directivo de la Defensoría de las Personas con Impedimentos

1. Ver que el defensor interino cumpla con las **recomendaciones 2 y 3**, de manera que se corrijan y no se repitan las situaciones comentadas en este *Informe*. **[Hallazgos del 1 al 5]**

Al defensor interino de la Defensoría de las Personas con Impedimentos

2. Se asegure de que se prepare un análisis de riesgos, según se establecen en las políticas *ATI-003* y *ATI-015* de la *Carta Circular 140-16*. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. Una vez aprobado, ver que se revise cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica de la Defensoría para asegurarse de que se mantenga actualizado. **[Hallazgo 1]**

3. Ejercer una supervisión efectiva sobre el director de sistemas de información para asegurarse de que:

    a. Revise y remita, para su aprobación, el *Plan* y se asegure de que incluya información actualizada de los aspectos comentados en el **Hallazgo 2-a.** Además, se asegure de que se efectúen pruebas o simulacros a dicho plan que certifiquen su efectividad, y se mantenga la documentación de las estrategias utilizadas y los resultados de las mismas.

    b. Identifique alternativas costo-efectivas para la preparación de un centro alterno que no esté expuesto a los mismos riesgos que la OSI y el área de los servidores en las oficinas regionales. Además, se asegure de que el lugar identificado cuente con la infraestructura y los equipos necesarios para restaurar

las operaciones críticas computadorizadas de la Defensoría en caso de emergencia, y de que sea considerado en el *Plan*. **[Hallazgo 2-b.]**

c. Requiera el *Formulario* para documentar la creación, modificación y eliminación de las cuentas de accesos y de los privilegios otorgados a los usuarios. **[Hallazgo 3-a.]**

d. Evalúe si las cuentas del exconsultor comentadas en el **Hallazgo 3-b.** pueden ser desactivadas y los privilegios transferidos a las cuentas asignadas al director de sistemas de información. De no poder desactivar estas cuentas, se asegure de implementar controles adicionales para evitar el uso no autorizado de las mismas.

e. Realice las gestiones necesarias para que se instale y configure el servidor necesario para instalar el Sistema de Manejo de Casos en la Oficina Regional. **[Hallazgo 4-a.1)]**

f. Almacene una copia de los respaldos del Sistema de Manejo de Casos, de la información de los usuarios y de la página en Internet en un lugar seguro. Dicho lugar no debe estar expuesto a las mismas amenazas de desastre que la Oficina Central, en donde se encuentran los servidores ubicados en la OSI y el disco duro en donde se graban los respaldos de la Defensoría. **[Hallazgo 5]**

4. Coordine con la directora ejecutiva de la División para la Protección y Defensa de las Personas con Impedimentos para que, con la asistencia de la coordinadora interagencial y los coordinadores de los programas, realice un estudio sobre las necesidades de adiestramiento de los funcionarios y empleados responsables de registrar la información en el Sistema de Manejo de Casos. Además, se asegure de que se ofrezcan estos adiestramientos necesarios para corregir la situación comentada en el **Hallazgo 4-a.2)**.

APROBACIÓN

A los funcionarios y a los empleados de la Defensoría, les exhortamos a velar por el cumplimiento de la ley y la reglamentación aplicables, y a promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo. Les agradecemos la cooperación que nos prestaron durante nuestra auditoría.

Oficina del Contralor de Puerto Rico

Aprobado por: 

ANEJO 1

DEFENSORÍA DE LAS PERSONAS CON IMPEDIMENTOS
DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO

**MIEMBROS PRINCIPALES DEL CONSEJO DIRECTIVO
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Jorge Jiménez Sánchez	Presidente	1 mar. 17	8 dic. 17
Sr. Erlyn Pagán Santiago	Vicepresidente	1 mar. 17	8 dic. 17
Sra. Ramonita Pérez González	Secretaria	1 mar. 17	8 dic. 17

ANEJO 2

DEFENSORÍA DE LAS PERSONAS CON IMPEDIMENTOS
DEL ESTADO LIBRE ASOCIADO DE PUERTO RICO

**FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sra. Carmen J. Collazo Fernández	Defensora Interina	19 jul. 17	8 dic. 17
Sr. Frank Pérez Concepción	Defensor	1 mar. 17	19 jul. 17
Sra. Carmen J. Collazo Fernández	Directora Ejecutiva	1 mar. 17	8 dic. 17
Sr. Luis Capré Martínez	Director de Sistemas de Información	1 mar. 17	8 dic. 17

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-18-19* del 27 de abril de 2018, 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, extensiones 2801 o 2805, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

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

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 787-754-3030, extensión 3400.

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:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr