INFORME DE AUDITORÍA TI-21-17

23 de junio de 2021

Comisión de Derechos Civiles

Sistemas de Información Computadorizados

(Unidad 5191 - Auditoría 14454)

Período auditado: 9 de diciembre de 2019 al 31 de agosto de 2020

CONTENIDO

Página

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

23 de junio de 2021

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 los sistemas de información computadorizados de la Comisión de Derechos Civiles (Comisión). 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 los sistemas de información computadorizados de la Comisión se realizaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

Determinar si la Comisión cumplió con las políticas establecidas en el memorando *Medidas de Seguridad y Normas para la Utilización del Sistema de Computadoras*, aprobado el 20 de noviembre de 2003 por la entonces directora ejecutiva (*Memorando* del 20 de noviembre de 2003), el *Memorando Interno 2009-06, Medidas de Seguridad y Normas para la Utilización del Sistema de Computadoras*, aprobado el 19 de marzo de 2009 por el entonces director ejecutivo; la *Carta Circular 2013-004, Política para el Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, y la *Carta Circular 2016-001, Normas Complementarias sobre el Uso de Sistemas Electrónicos de la Comisión de Derechos Civiles*, aprobados el 29 de agosto de 2013 y el 1 de julio de 2016 por el director ejecutivo; y 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 entonces director de la Oficina de Gerencia y Presupuesto, entre otros, para lo siguiente:

1. Desarrollar, documentar y aprobar un plan de contingencia que incluya los requisitos que son necesarios para atender situaciones de emergencia.
2. Establecer las políticas para controlar el acceso a las cuentas del servidor principal; y producir y revisar los registros de estos accesos.
3. Documentar la justificación y autorización de los accesos remotos e inactivar las cuentas de acceso de usuarios de la red que ya no están relacionados con la Comisión.
4. Utilizar una herramienta para el monitoreo de las actividades en el uso del correo electrónico y revisar con regularidad estas actividades.

CONTENIDO DEL INFORME

Este *Informe* contiene dos hallazgos del resultado del examen que realizamos de los objetivos indicados. El mismo está disponible en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 9 de diciembre de 2019 al 31 de agosto de 2020. 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 los Estados Unidos (GAO, por sus siglas en inglés), en lo concerniente a auditorías de tecnología de información. Estas normas requieren que planifiquemos y realicemos auditorías para obtener evidencia suficiente y apropiada que proporcione una base razonable para nuestra opinión y hallazgos relacionados con los objetivos de 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,

empleados y consultores; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada o por fuentes externas; y pruebas y análisis de procedimientos de control interno y de otros procesos.

Para realizar esta auditoría, utilizamos el *Memorando* del 20 de noviembre de 2003, el *Memorando Interno 2009-06*, las cartas circulares *2013-004* y *2016-001*; y la *Política ATI-003, Seguridad de los Sistemas de Información*[1], de la *Carta Circular 140-16*. Para las áreas que no estaban consideradas en la reglamentación mencionada, utilizamos como mejor práctica las guías establecidas en el *Federal Information System Controls Audit Manual* (*FISCAM*)[2], emitido por el GAO. Aunque a la Comisión no se le requiere cumplir con dichas guías, entendemos que estas representan las mejores prácticas en el campo de la tecnología de información.

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

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Comisión fue creada en virtud de la *Ley Núm. 102 del 28 de junio del 1965*, según enmendada, y está adscrita a la Rama Legislativa[3], pero sin ser parte de la misma y usando sus servicios administrativos únicamente hasta donde sea necesario para facilitar su labor.

La función principal de la Comisión es educar al Pueblo en cuanto al significado de los derechos fundamentales y los medios de respetarlos, protegerlos y enaltecerlos. Además, gestionar, ante los individuos y las autoridades gubernamentales, la protección de los derechos humanos y el cumplimiento de las leyes que amparan tales derechos. También realizar estudios e investigaciones sobre la vigencia de los derechos fundamentales y sobre quejas o querellas presentadas por cualquier ciudadano relacionadas

[1] En la sección Política de *Política ATI-003*, se establece que los usuarios de los servicios de la Red Interagencial que no son agencias están sujetos al cumplimiento de las secciones E., Controles Generales; J., Internet; y K., Servicios Suministrados por Contratistas.

[2] El *FISCAM* utiliza las guías emitidas por el National Institute of Standards and Technology.

[3] Inicialmente estuvo adscrita al Departamento de Justicia.

con la violación de esos derechos. Por otro lado, evalúa las leyes, normas y actuaciones de los gobiernos estatal y municipal relacionados con los derechos civiles.

La Comisión está integrada por 5 miembros nombrados por el gobernador, con el consejo y consentimiento del Senado de Puerto Rico. Los comisionados son nombrados por un término de 6 años. Estos prestan sus servicios *ad honorem*. Una vez constituida la Comisión, los comisionados eligen, entre ellos, 1 presidente, 1 vicepresidente y 1 secretario. También nombran 1 director ejecutivo para organizar y dirigir las labores de esta. Con la aprobación de los comisionados, el director ejecutivo selecciona al personal, el cual no está sujeto a las disposiciones de las leyes de personal del Gobierno de Puerto Rico y sus reglamentos.

A la fecha de nuestra auditoría, la Comisión no contaba con una oficina de sistemas de información. La Comisión había contratado una compañía (Compañía) para que ofreciera los servicios de administración, configuración, mantenimiento, apoyo técnico y consultoría de los sistemas de información de la Comisión. Además, la Comisión tenía una red local de área (LAN, por sus siglas en inglés) que interconectaba 18 usuarios y contaba con 3 servidores físicos y 5 servidores virtuales, 21 computadoras de escritorio, 6 computadoras portátiles y 2 unidades de almacenamiento. También utilizaba la aplicación Kronos para el registro de las asistencias de los empleados y los servicios de correo electrónico, licencias y publicación de la página en Internet que eran ofrecidos por el Puerto Rico Innovation and Technology Service (PRITS)[4].

Los recursos para financiar las operaciones de la Comisión provienen de resoluciones conjuntas del Fondo General del Estado Libre Asociado de Puerto Rico. Además, la Comisión está autorizada para recibir y administrar fondos provenientes de asignaciones legislativas, transferencias de fondos de otras agencias o dependencias del Gobierno y de donativos de cualquier

[4] El PRITS administra la Red Interagencial, mediante la cual se proveen los servicios de correo electrónico y publicación de las páginas en Internet de las agencias del Estado Libre Asociado de Puerto Rico.

clase. El presupuesto aprobado de la Comisión, para los años fiscales 2017-18, 2018-19 y 2019-20, ascendió a $982,000, $944,000 y $821,000 respectivamente.

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

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

COMUNICACIÓN CON LA GERENCIA

Mediante correo electrónico del 23 de abril de 2021, remitimos el borrador de este *Informe* para comentarios del Lcdo. Ever Padilla Ruiz, director ejecutivo de la Comisión.

El director ejecutivo contestó mediante carta el 7 de mayo de 2021 y algunos de sus comentarios se incluyen en la sección **OPINIÓN Y HALLAZGOS**.

CONTROL INTERNO

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

- 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 esta auditoría. 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 Comisión.

En los **hallazgos** se comentan las deficiencias de control interno 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 relacionadas con los sistemas de información computadorizados de la Comisión objeto de este *Informe* se realizaron, en todos los aspectos significativos, de acuerdo con las normas y reglamentación aplicables; y que los controles establecidos, relacionados con dichas operaciones, eran efectivos. Esto, excepto por los **hallazgos 1 y 2** que se comentan a continuación:

Hallazgo 1 - Deficiencias relacionadas con el Plan de Respuesta ante una Emergencia

Situación

a. Toda entidad gubernamental debe contar con un plan de contingencia documentado y aprobado para restablecer sus operaciones más importantes en caso de una emergencia. El mismo debe incluir toda la información actualizada de los sistemas de información computadorizados y los procesos necesarios para recuperar sus operaciones. Además, este plan debe ser comunicado al personal responsable de las actividades de recuperación y debe identificar los riesgos y las prioridades operacionales de la agencia, los recursos de apoyo necesarios, los roles y las responsabilidades del personal asignado a las actividades de recuperación, los números de contacto, los archivos críticos, las computadoras y los equipos de telecomunicaciones compatibles con las necesidades de la entidad, entre otros.

Al 17 de agosto de 2020, la Comisión contaba con el *Plan de Respuesta ante una Emergencia* (*Plan*)[5], para mantener la continuidad de sus servicios. El examen realizado el 3 de septiembre de 2020, reveló que este *Plan* no incluía la información de contacto del proveedor primario del servicio de Internet; una lista de los equipos, los sistemas operativos, las aplicaciones y los archivos críticos de la Comisión; y el itinerario de restauración que debía seguir la Compañía para restaurar los respaldos.

Criterio

La situación comentada es contraria a lo sugerido en el Capítulo 3.5, Contingency Planning, del *FISCAM*.

Efectos

La situación comentada puede propiciar la improvisación y que, en casos de emergencias, 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 de la Comisión.

Causas

Lo comentado se atribuye a que la Comisión no cuenta con personal de sistemas de información que oriente al director ejecutivo sobre el contenido del *Plan* y, debido a limitaciones de presupuesto, no había requerido estos servicios a la Compañía.

Comentarios de la Gerencia

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

> […] Es importante puntualizar que durante las emergencias ocasionadas por los Huracanes Irma y María (el peor evento atmosférico de nuestra historia), la Comisión de Derechos Civiles continuó trabajando adherido a los planes de emergencia. Igual sucedió con los apagones generales registrados y con los terremotos

[5] El *Plan* fue provisto a nuestros auditores el 17 de agosto de 2020 por el director ejecutivo; y fue distribuido a los empleados de la Comisión mediante correo electrónico del 27 de febrero de 2020, pero no incluía fecha de aprobación.

> de diciembre de 2019 y enero 2020. En todas estas ocurrencias los protocolos establecidos permitieron mantener la continuidad de nuestros trabajos de manera apropiada, responsable y sistemática. [*sic*]
>
> […] El 19 de marzo de 2021, se revisó y aprobó el Plan de Respuestas Ante Emergencias actualizando toda la información e insertando las nuevas normas establecidas hasta esa fecha […]. [*sic*]

Evaluamos el *Plan* revisado el 10 de marzo de 2021y este aún carece de la información mencionada en el **Hallazgo**.

Véanse las recomendaciones 1 y 2.

Hallazgo 2 - Deficiencias relacionadas con los parámetros de contraseñas y auditoría, y el mantenimiento de las cuentas de los usuarios del servidor principal

Situaciones

a. Toda entidad gubernamental es responsable de diseñar y mantener la seguridad de sus sistemas de información. Los mecanismos de autenticación para acceder a estos sistemas deben incluir, entre otros, una contraseña combinada de números, letras y caracteres especiales, no menor de ocho caracteres. Además, todas las contraseñas a nivel administrativo se deben cambiar, como mínimo, cada 4 meses y las de los usuarios, cada 6 meses. También las entidades gubernamentales deben implementar procesos que permitan revisar las actividades de los usuarios en aquellos activos sensitivos que lo ameriten.

   Mediante las cartas circulares *2013-004* y *2016-001*, la Comisión requiere a los usuarios de sus sistemas computadorizados que establezcan y cambien de tiempo en tiempo sus contraseñas. Además, les informa que el uso de estos sistemas puede ser auditado periódicamente.

   La Comisión cuenta con un servidor principal, administrado por la Compañía, mediante el cual se controla el acceso a los recursos de la red y se le permite el acceso a Internet a los usuarios autorizados.

El examen sobre los parámetros de seguridad configurados en el servidor al 30 de enero de 2020, y las políticas de auditoría configuradas al 5 de marzo de 2020, reveló lo siguiente:

1) En el servidor principal no se habían definido las políticas de contraseñas (*password policy*) para requerir:

   a) El uso de contraseñas de un mínimo de ocho caracteres en combinaciones de números, letras y caracteres especiales. Las políticas estaban configuradas para requerir 0 caracteres no complejos (*minimum password length:0* y *password must meet complexity requirements: disabled*).

   b) El cambio de las contraseñas de cuentas administrativas, al menos, cada 4 meses y las de los usuarios cada 6 meses. La política estaba configurada para un mínimo y máximo de 0 días (*minimum/maximum password age: 0*)

2) Las políticas de auditoría (*audit policy*) no estaban definidas para requerir que el sistema produjera un registro de los siguientes eventos:

   - La solicitud al servidor para validar las cuentas de usuario (*audit account logon events*)
   - La activación y desactivación de las cuentas (*audit logon events*)
   - Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*audit policy change*)
   - Las acciones ejecutadas por algún programa (*audit process tracking*)
   - El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*audit system events*).

b. Toda entidad gubernamental debe implementar controles que minimicen los riesgos de que la información sea accedida de forma no autorizada. Además, los privilegios de acceso de los usuarios deben ser reevaluados regularmente para asegurarse de que solo el personal autorizado acceda a las aplicaciones y los datos que necesita utilizar.

El director ejecutivo debe solicitar a la Compañía la configuración de las cuentas de accesos a los sistemas de información de la Comisión. Una vez recibida esta solicitud, la Compañía se debe encargar de crear, modificar y desactivar las cuentas de acceso.

Al 29 de julio de 2020, en el servidor principal había 53 cuentas de usuarios activas para acceder a la red. El examen de estas cuentas reveló que 11 cuentas (21%) nunca habían sido utilizadas por sus usuarios.

Criterio

Las situaciones comentadas son contrarias a lo dispuesto en la *Carta Circular 2013-004* y la sección E. de la *Política ATI-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 140-16*.

Efectos

Las situaciones comentadas en los **apartados a.1) y b.** pueden propiciar que personas no autorizadas logren acceso a información confidencial y hagan uso indebido de esta; y la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas, sin que puedan detectarse a tiempo para fijar responsabilidades.

Lo comentado en el **apartado a.2)** impide a la Comisión mantener un registro de los eventos inusuales o problemas ocurridos en la red que le permita a la Compañía tomar a tiempo las medidas correctivas o preventivas necesarias.

Causas

Las situaciones comentadas se deben principalmente a que el director ejecutivo de la Comisión no requirió que en el contrato otorgado a la Compañía se incluyeran algunas de las tareas relacionadas con la administración de las cuentas, los servicios de configuración y la revisión de los accesos, que eran necesarios para cumplir con la *Política ATI-003*.

Además, el director ejecutivo indicó que, por ser temas altamente técnicos, él no dominaba los mismos y tampoco contaba con las herramientas suficientes para tener un criterio apropiado para implementar las políticas de seguridad y auditoría a los sistemas de información de la red.

Comentarios de la Gerencia

El director ejecutivo nos indicó en su carta, entre otras cosas, que el 4 de noviembre de 2020 aprobó la *Carta Circular 2020-12, Procesos Internos para la Evaluación Continua de los Sistemas de Información*, que incluye procedimientos internos para la evaluación continua de los sistemas de información. Como parte de estos, se han producido informes trimestrales que incluyen recomendaciones de la Compañía para efectuar mejoras en los controles de acceso. Además, nos informó que aprobó la *Carta Circular 2020-13, Normas Complementarias para la Seguridad de los Sistemas de Información*, el 10 de noviembre de 2020, que incluye normas relacionadas con la definición de las políticas de contraseña y la actualización de estas.

Sin embargo, no nos proveyó evidencia de que se hayan realizado cambios a la configuración del servidor para atender las deficiencias comentadas en el **Hallazgo 2-a.** ni de acciones efectuadas para restringir el acceso de las 11 cuentas no utilizadas, según comentado en el **Hallazgo 2-b.**

Véanse las recomendaciones 1 y 3.

RECOMENDACIONES

A los comisionados

1. Tomar las medidas necesarias y establecer mecanismos de supervisión adecuados para asegurarse de que el director ejecutivo cumpla con las **recomendaciones 2 y 3**.

Al director ejecutivo de la Comisión

2. Revisar y aprobar el *Plan de Respuesta ante una Emergencia*, para que incluya los aspectos comentados en el **Hallazgo 1**. Una vez actualizado, debe asegurarse de que se distribuya a los funcionarios y a los empleados concernientes, se revise y realicen pruebas periódicas para garantizar su efectividad y se conserve copia en un lugar seguro fuera de los predios de la Comisión.

3. Requerir lo siguiente a la Compañía o al empleado designado por la Comisión:

    a. Efectúe las modificaciones en los parámetros de seguridad del sistema operativo de los servidores de la red para:

        1) Requerir que las contraseñas tengan, al menos, un mínimo de ocho caracteres y una combinación de caracteres alfanuméricos (letras, símbolos y números). **[Hallazgo 2-a.1)a)]**

        2) Establecer un término para que las contraseñas de las cuentas de acceso expiren y se les requiera a los usuarios cambiar las mismas como lo requiere la *Política ATI-003*. **[Hallazgo 2-a.1)b)]**

    b. Evalúe las políticas de auditoría (*audit policy*), y active las que considere necesarias de acuerdo con los riesgos y las amenazas de los sistemas de información de la Comisión, según lo establecido en la *Política ATI-003*. **[Hallazgo 2-a.2)]**

    c. Evalúe los accesos de las cuentas comentadas en el **Hallazgo 2-b.** para determinar cuáles de estas no son necesarias para las operaciones de la Comisión y sus sistemas de información, y las inhabilite.

APROBACIÓN

A los funcionarios y a los empleados de la Comisión de Derechos Civiles, 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

COMISIÓN DE DERECHOS CIVILES
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

MIEMBROS DE LA COMISIÓN
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dra. Nieve de los Ángeles Vázquez Lazo	Presidenta	9 dic. 19	31 ago. 20
Dr. Hiram Meléndez Juarbe	Comisionado	9 dic. 19	31 ago. 20
Lcda. Patricia Otón Oliveri	"	9 dic. 19	31 ago. 20
Lcdo. Andrés Córdova Phelps	"	9 dic. 19	31 ago. 20

ANEJO 2

COMISIÓN DE DERECHOS CIVILES
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. Ever Padilla Ruiz	Director Ejecutivo	9 dic. 19	31 ago. 20
Sra. Alexa Torres Vicente	Ayudante Especial	9 dic. 19	31 ago. 20

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