

INFORME DE AUDITORÍA TI-21-05

1 de diciembre de 2020

Asamblea Legislativa de Puerto Rico

Cámara de Representantes de Puerto Rico

Oficina de Tecnología e Informática

(Unidad 5195 - Auditoría 14361)

Período auditado: 28 de febrero al 18 de septiembre de 2019

CONTENIDO

	Página
OBJETIVOS DE AUDITORÍA.....	2
CONTENIDO DEL INFORME.....	3
ALCANCE Y METODOLOGÍA.....	3
INFORMACIÓN SOBRE LA UNIDAD AUDITADA	3
COMUNICACIÓN CON LA GERENCIA.....	5
CONTROL INTERNO	6
OPINIÓN Y HALLAZGOS.....	6
1 - Falta de revisiones periódicas de los registros de eventos de seguridad del sistema operativo del servidor principal	7
2 - Falta de inactivación de las cuentas de acceso del servidor principal.....	8
RECOMENDACIONES.....	10
APROBACIÓN	11
ANEJO - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO	12

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

1 de diciembre de 2020

A la Gobernadora, 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 de la Oficina de Tecnología e Informática (OTI) de la Cámara de Representantes de Puerto Rico (Cámara). 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 OTI de la Cámara se efectuaron de acuerdo con las normas y la reglamentación aplicables.

Objetivos específicos

Determinar si las operaciones de la OTI, en lo que concierne a los controles para la administración de la seguridad, el acceso lógico y la continuidad del servicio; se efectuaron, en todos los aspectos significativos, de acuerdo con la *Orden Administrativa 2005-15, para Adoptar el Reglamento de Normas y Controles para la Administración y Uso de los Sistemas Computadorizados de la Cámara de Representantes de Puerto Rico; Derogar la Orden Administrativa Núm. 04-09, según enmendada; y para Otros Fines*, aprobada el 28 de junio de 2005 por el entonces presidente de la Cámara; y con el *OTI-SOP-09, Normas y Procedimientos para Mantenimiento Preventivo de los Sistemas*, aprobado el 30 de octubre de 2007, y el *OTI-SOP-4, Normas y Procedimientos para el Control de Accesos Físicos y Lógicos de los*

Sistemas de Información, aprobado el 25 de enero de 2008, por la entonces administradora de la Cámara, entre otros; y si dichos controles eran efectivos.

**CONTENIDO DEL
INFORME**

Este *Informe* contiene dos hallazgos sobre el 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 28 de febrero al 18 de septiembre de 2019. 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 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 la auditoría. En consecuencia, realizamos las pruebas que consideramos necesarias, 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 unidad auditada; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

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

**INFORMACIÓN SOBRE
LA UNIDAD AUDITADA**

En el Artículo III de la Constitución, se establece que el poder legislativo se ejerce por la Asamblea Legislativa que se compone de la Cámara de Representantes y el Senado de Puerto Rico, cuyos miembros son elegidos

por votación directa en cada elección general. Se establece, además, que la Cámara se compone de 51 representantes: 40 por distrito y 11 por acumulación¹.

La Cámara es dirigida por un presidente, quien tiene entre sus facultades y obligaciones, que coordinar los asuntos administrativos de esta. En tal capacidad, debe organizar las actividades relacionadas con los funcionarios de dicho cuerpo legislativo. Además, promulgar los reglamentos y las órdenes administrativas que regulan las operaciones fiscales de este.

Mediante la *Ley 140-2004*, se autorizó a la Asamblea Legislativa a ejercer la custodia y el control de su propiedad y fondos públicos; diseñar y establecer su propia organización fiscal, y los sistemas y procedimientos de contabilidad para llevar a cabo las transacciones financieras; aclarar el alcance de las disposiciones de ley aplicables a ambos cuerpos legislativos; y aprobar la reglamentación necesaria para llevar a cabo los propósitos de dicha *Ley*.

A la fecha de nuestra auditoría, la estructura administrativa de la Cámara se dividía en cuatro áreas: Administración, Sargento de Armas, Secretaría y Presidencia. La OTI le respondía al administrador de la Cámara y contaba con 1 director, 1 ayudante ejecutiva, 1 administrador de la red, 3 técnicos de sistemas de información, 1 técnico audiovisual, 1 supervisora de cuadro telefónico, 3 operadoras de cuadro telefónico y 1 secretaria.

El centro de cómputos de la Cámara operaba bajo un contrato, mediante el cual se proveía el servicio de alojamiento de servidores virtuales.

¹ En caso de que en una elección general resulten electos más de dos terceras partes de los miembros de la Cámara por un solo partido o bajo una sola candidatura, se aumenta el número de los miembros de la Cámara en representación del partido o partidos de minoría hasta un total de 17 representantes.

Este contrato de infraestructura como servicio (*IaaS*², por sus siglas en inglés) fue formalizado entre la Oficina de Servicios Legislativos (OSL)³ y la compañía contratada.

El presupuesto asignado a la Cámara proviene de resoluciones conjuntas del presupuesto general y de asignaciones especiales. El presupuesto asignado para los años fiscales del 2017-18 al 2019-20, ascendió a \$45,949,000, \$35,658,000 y \$29,599,500, respectivamente. En los años fiscales del 2017-18 al 2019-20, la Cámara asignó a la OTI un presupuesto de \$831,433, \$717,476 y \$137,515⁴, respectivamente.

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

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

COMUNICACIÓN CON LA GERENCIA

El 23 de julio de 2020 se remitió el borrador de este *Informe*, que incluía tres hallazgos, para comentarios del Hon. Carlos J. Méndez Núñez, Presidente de la Cámara. Este contestó el 15 de septiembre de 2020.

Luego de evaluar los comentarios y la evidencia suministrada, determinamos que el Presidente tomó las medidas pertinentes para corregir varias situaciones, por lo que determinamos eliminarlas. Las restantes prevalecieron y se incluyen en este *Informe*, al igual que algunos de los comentarios del Presidente.

² Infraestructura como servicio (*Infrastructure as a Service*) proporciona soluciones informáticas en un entorno virtualizado en la nube que le permite al cliente crear soluciones informáticas económicas y fáciles de ampliar.

³ La OSL le brinda servicios de asesoría y apoyo directo a los miembros de la Asamblea Legislativa y sus dependencias, y sirve de apoyo a los centros de cómputos de la Cámara, el Senado y la Superintendencia del Capitolio.

⁴ Hasta el 19 de septiembre de 2019.

CONTROL INTERNO

La gerencia de la Cámara 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 Cámara.

En los **hallazgos** 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 Cámara, 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 1 y 2** que se comentan a continuación.

Hallazgo 1 - Falta de revisiones periódicas de los registros de eventos de seguridad del sistema operativo del servidor principal

Situación

- a. Las entidades deben contar con procesos que permitan revisar las actividades de los usuarios en aquellos activos sensitivos que así lo ameriten. El administrador de la red tiene la responsabilidad de revisarla diariamente para prevenir y detectar accesos no autorizados.

Nuestro examen reveló que, al 15 de mayo de 2019, el administrador de la red no revisaba periódicamente los registros de seguridad (*security event log*⁵) provistos por el sistema operativo del servidor principal. Esto es necesario para conocer las posibles violaciones de seguridad que pudieran ocurrir en el servidor y en la red, y tomar prontamente las medidas preventivas y correctivas necesarias. El administrador solo examinaba dichos registros en el caso de que ocurriera alguna eventualidad con los sistemas de información.

Criterio

Lo comentado es contrario a lo establecido en las secciones 2.d y 3.g del *OTI-SOP-09, Normas y Procedimientos para Mantenimiento Preventivo de los Sistemas*.

Efectos

La situación comentada puede propiciar que personas no autorizadas accedan a información confidencial mantenida en los sistemas computadorizados y puedan 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. También priva a la Cámara de las herramientas necesarias para detectar irregularidades y alteraciones de los datos contenidos en los sistemas computadorizados, sin que se puedan detectar a tiempo para fijar

⁵ El registro de seguridad contiene sucesos como los intentos válidos y no válidos de inicio de sesión. También contiene sucesos relacionados con el uso de los recursos.

responsabilidades. Como ocurrió con la cuenta de acceso correspondiente a una exempleada que fue utilizada 23 días posteriores a su fecha de separación. La transacción realizada mediante la cuenta no se pudo examinar, debido a que en la OTI no pudieron proveernos el registro de eventos de seguridad de esta fecha.

Causa

La situación comentada se atribuye a que el administrador de la red no cumplió con las disposiciones citadas. De acuerdo con lo indicado por el administrador de la red, al ser el único empleado de la OTI que realizaba todas las funciones relacionadas con la administración de los sistemas de información computadorizados, se le hacía difícil realizar la revisión periódica y preventiva de los registros de seguridad disponibles en los sistemas de información.

Comentarios de la Gerencia

El Presidente de la Cámara nos indicó, entre otras cosas, que le solicitaron al director de la OTI que impartiera instrucciones al administrador de la red para que realice revisiones periódicas a los registros de seguridad, documente las mismas y, de ser necesario, tome de inmediato las medidas preventivas y correctivas.

Véase la Recomendación 1.a.

Hallazgo 2 - Falta de inactivación de las cuentas de acceso del servidor principal

Situación

- a. En la *Orden Administrativa 2005-15*, se establece que el representante o director de oficina es responsable de la integridad de la información que se mantiene en los directorios asignados a las oficinas que dirigen. Esta responsabilidad conlleva, entre otras cosas, notificar inmediatamente al director de la OTI, por medio electrónico, del uso prolongado de licencia, o el traslado, relevo o cese de funciones de algún usuario. Esto, para que se inactive la cuenta de acceso, según corresponda.

El examen realizado sobre el mantenimiento de las cuentas de acceso a los recursos de la red reveló que, al 17 de mayo de 2019, permanecían activas en el servidor principal:

- 1) Dos cuentas con privilegios de conexión remota⁶ asignadas a exconsultores. Esto, a pesar de que habían transcurrido 321 y 929 días desde la fecha de terminación de sus contratos.
- 2) Cinco cuentas de acceso asignadas a empleados que cesaron en sus funciones, entre el 31 de diciembre de 2016 y el 20 de febrero de 2019. Esto, luego de transcurridos entre 86 y 867 días, desde la fecha de separación de estos exempleados. Dos de estas cuentas nunca se conectaron a la red. La Oficina de Capital Humano le notificó a la OTI la separación de este personal el 10 de septiembre de 2019, entre 202 y 983 días posteriores a su separación y luego de que nuestros auditores requirieran la evidencia de la notificación.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la Sección T.2) del Artículo V de la *Orden Administrativa 2005-15*.

Efectos

Las situaciones comentadas impiden mantener un control de los usuarios autorizados a acceder los sistemas de información computadorizados y de los privilegios asignados a estos para fijar responsabilidades en caso de errores o irregularidades. Además, pueden propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta, la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información. Esto, sin que puedan ser detectados a tiempo para fijar responsabilidades.

⁶ Los privilegios otorgados a estas cuentas les permitían a estos consultores, entre otras cosas, acceder y utilizar información de una entidad gubernamental desde un lugar remoto o distinto de donde está guardada la misma.

Causa

Lo comentado se debió, en parte, a que el personal de la OTI desconocía que una vez al año tenía que solicitar a las oficinas de Capital Humano y de Contratos, una lista de empleados y de contratos activos para compararla con los usuarios existentes en el sistema, según establecido en el *OTI-SOP-4*. Esto, para eliminar del sistema las cuentas de los empleados y contratistas que no estuvieran activos en las listas.

Comentarios de la Gerencia

El Presidente de la Cámara nos indicó, entre otras cosas, que se impartieron instrucciones al director de la OTI para que solicite las listas de empleados y contratos activos a las oficinas de Capital Humano y de Contratos, y se asegure de que se realice la comparación con la lista de usuarios activos del sistema. Esto, de manera que se cumplan las directrices establecidas en las *Normas y Procedimientos para el Control de Accesos Físicos y Lógicos de los Sistemas de Información* de la Cámara. Además, le solicitaron a la directora de la Oficina de Capital Humano que se asegure de notificar a la OTI el cese de empleados en sus funciones, para la cancelación inmediata de las cuentas de acceso de estos.

Véase la Recomendación 1.b. y c.

RECOMENDACIONES**Al Presidente de la Cámara**

1. Asegurarse de que el administrador de la Cámara ejerza una supervisión efectiva para lo que se cumpla con lo siguiente:
 - a. El director de la OTI realice revisiones periódicas a los registros de seguridad (*Security Event Log*), documente las mismas y, de ser necesario, tome de inmediato las medidas preventivas y correctivas. **[Hallazgo 1]**
 - b. El director de la OTI solicite las listas de empleados y contratos activos a las oficinas de Capital Humano y de Contratos, y se asegure de que en la OTI se realice la comparación con la lista de usuarios activos del sistema. Esto, de manera que se cumplan

las directrices establecidas en el OTI-SOP-4, *Normas y Procedimientos para el Control de Accesos Físicos y Lógicos de los Sistemas de Información*. **[Hallazgo 2]**

- c. La directora de Capital Humano notifique a la OTI el cese de los empleados en sus funciones, para la cancelación inmediata de las cuentas de acceso de estos. **[Hallazgo 2-a.2)]**

APROBACIÓN

A los funcionarios y a los empleados de la Cámara, 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

**ASAMBLEA LEGISLATIVA DE PUERTO RICO
CÁMARA DE REPRESENTANTES DE PUERTO RICO
OFICINA DE TECNOLOGÍA E INFORMÁTICA
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO**

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Carlos J. Méndez Núñez	Presidente	28 feb. 19	18 sep. 19
Sr. Moisés D. Cortés Rosado	Administrador	28 feb. 19	18 sep. 19
Sr. Ismael San Antonio Beauchamp	Director de la Oficina de Tecnología e Informática	28 feb. 19	18 sep. 19
Sra. Karen Torres De La Torre	Directora de Capital Humano	28 feb. 19	18 sep. 19

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

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069