INFORME DE AUDITORÍA TI-20-09

2 de junio de 2020

Municipio de Cayey

Oficina de Informática

(Unidad 5430 - Auditoría 14355)

Período auditado: 13 de marzo al 2 de agosto de 2019

CONTENIDO

Página

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

2 de junio 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 Informática del Municipio de Cayey (Municipio). 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 Oficina de Informática del Municipio se efectuaron de acuerdo con las normas y la reglamentación aplicables.

Objetivo específico

Determinar si las operaciones de la Oficina de Informática; en lo que concierne a los controles para la administración de la seguridad, la continuidad del servicio y el acceso lógico; se efectuaron, en todos los aspectos significativos, de acuerdo con 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 entonces director de la Oficina de Gerencia y Presupuesto; y si dichos controles eran efectivos.

CONTENIDO DEL INFORME

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 13 de marzo al 2 de agosto 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, a base de muestras y de acuerdo con las circunstancias, según nuestros objetivos de auditoría. Realizamos pruebas, tales como: entrevistas a funcionarios, empleados y contratistas; inspecciones físicas; exámenes y análisis de informes y de documentos generados por la unidad auditada; y pruebas y análisis de procedimientos de control interno y de otros procesos.

Al realizar esta auditoría, utilizamos como mejores prácticas las políticas establecidas en la *Carta Circular 140-16* y las guías establecidas en el *Federal Information Systems Controls Audit Manual* (FISCAM)[1], emitido por el GAO. Aunque al Municipio no se le requiere cumplir con dichas políticas y guías, entendemos que estas representan las mejores prácticas en el campo de la tecnología de información, a falta de reglamentación interna para las áreas consideradas en esta auditoría.

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

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

El Municipio es una entidad del Gobierno del Estado Libre Asociado de Puerto Rico con personalidad jurídica. Sus operaciones se rigen por la *Ley 81-1991, Ley de Municipios Autónomos de Puerto Rico*,

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

según enmendada, y por el *Reglamento para la Administración Municipal de 2016*. Este fue aprobado el 19 de diciembre de 2016 por el entonces comisionado de Asuntos Municipales, y comenzó a regir el 17 de enero de 2017[2].

El Municipio tiene plenas facultades ejecutivas y legislativas en cuanto a su jurisdicción. Es una entidad jurídica con carácter permanente. Además, tiene existencia y personalidad legal independiente de las del Gobierno Estatal. La finalidad de este es el bien común local y, dentro de este y en forma primordial, la atención de asuntos, problemas y necesidades colectivas de sus habitantes.

El sistema gubernamental del Municipio está constituido por 2 poderes: el Ejecutivo y el Legislativo. El alcalde, como funcionario ejecutivo, ejerce las funciones administrativas y es electo cada 4 años en las elecciones generales de Puerto Rico. La Legislatura Municipal ejerce las funciones legislativas y está compuesta por 16 miembros, quienes también son electos en dichas elecciones. Los **anejos 1 y 2** contienen una relación de los funcionarios principales del Municipio y de la Legislatura Municipal que actuaron durante el período auditado.

El Municipio, para ofrecer sus servicios en el área operacional, cuenta con las siguientes dependencias: Obras Públicas, Control Ambiental, Mejoramiento Urbano, Ornato y Embellecimiento, Recreación y Deportes, Escuela de Bellas Artes, Policía Municipal, Manejo de Emergencias, Oficina de Recaudaciones, Hospital Municipal, Asuntos a la Vejez, Oficina de Permisos, Programa Head Start, Child Care y Asuntos Culturales e Históricos. La estructura organizacional del Municipio está compuesta por Auditoría Interna, Secretaría Municipal, Recursos Humanos, Finanzas Municipal, Ordenación Territorial, Asuntos Legales, Programas Federales y Comunicaciones y Relaciones Públicas.

---

[2] Este derogó el *Reglamento para la Administración Municipal* del 18 de julio de 2008. Además, mediante la *Ley 81-2017*, se transfirieron las funciones de la Oficina del Comisionado de Asuntos Municipales a la Oficina de Gerencia y Presupuesto.

A la fecha de nuestra auditoría, la Oficina de Informática contaba con una programadora de sistemas de información, la cual era supervisada por la directora de Recursos Humanos. La programadora de sistemas de información se encargaba de la administración y la seguridad de la red de comunicación, y de ofrecer apoyo técnico a los usuarios de la red de área local (LAN) del Municipio. Un consultor privado la asistía en estas funciones. Este personal otorgaba los accesos a la red y al Internet.

El Municipio tenía una infraestructura tecnológica que constaba de 3 servidores: 2 físicos y 1 virtual, 187 computadoras de escritorio y 41 portátiles. Además, contaba con el sistema financiero de contabilidad Rock Solid y con la aplicación ABS para el manejo de los registros de asistencia y los balances de licencias acumuladas de los empleados del Municipio.

El presupuesto del Municipio proviene de impuestos locales, contribuciones sobre la propiedad, ingresos intergubernamentales e ingresos por servicios. Para los años fiscales del 2016-17 al 2018-19, el presupuesto asignado ascendió a $30,778,263, $28,964,451 y $27,057,792, respectivamente. La Oficina de Informática no cuenta con un presupuesto propio. Sus gastos están contemplados dentro del presupuesto operacional del Municipio.

COMUNICACIÓN CON LA GERENCIA

Las situaciones determinadas durante la auditoría fueron remitidas al Hon. Rolando Ortiz Velázquez, alcalde, mediante carta del 3 de septiembre de 2019. En la referida carta se incluyó un anejo con detalles sobre las situaciones comentadas.

El 20 de septiembre de 2019 el alcalde remitió sus comentarios. Estos se consideraron al redactar el borrador de este *Informe*.

El borrador de este *Informe* se remitió mediante carta del 28 de febrero de 2020 para comentarios del alcalde. Sin embargo, este no contestó.

CONTROL INTERNO

La gerencia del Municipio de Cayey 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 del Municipio.

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 Oficina de Informática del Municipio 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 4**, que se comentan a continuación.

Hallazgo 1 - Falta de un informe del análisis de riesgos de los sistemas de información computadorizados, y de un plan o procedimiento escrito para el manejo de incidentes

Situaciones

a. El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información computadorizados existentes en una 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. Mediante este proceso se 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 22 de abril de 2019, en el Municipio no se había preparado un informe de análisis de riesgos de los sistemas de información computadorizados. En su lugar, se nos suministró el *Plan para el Manejo de Emergencias e Incidentes de la Oficina de Informática 2019-2020* (*Plan para el Manejo de Emergencias e Incidentes*). En el *Estudio de Riesgos de la Oficina de Informática (Tabla-1)* de dicho *Plan* se incluían los eventos que pudieran resultar en amenazas para los sistemas de información del Municipio, su frecuencia y la probabilidad de que ocurrieran. Sin embargo, determinamos que en dicha tabla no se consideraban los aspectos básicos necesarios para un análisis de riesgos, tales como: el inventario de los activos existentes del Municipio, con su clasificación de acuerdo con el nivel de importancia para la continuidad de las operaciones y, en el caso de los datos, su nivel de confidencialidad; las amenazas a las que están expuestos; y las conclusiones de la gerencia en respuesta a su evaluación del riesgo (aceptación, transferencia, reducción o asumir el riesgo).

b. Las entidades gubernamentales deben desarrollar procedimientos para identificar, informar y responder a incidentes de seguridad, incluidos aquellos que causen interrupción en la prestación de sus servicios. Estos procedimientos deben identificar el personal asignado para responder a los incidentes de seguridad e incluir sus límites en términos de tiempo máximo y mínimo de respuesta.

   Al 5 de agosto de 2019, el Municipio no contaba con un plan o procedimiento escrito para el manejo de incidentes que estableciera, entre otras cosas, una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos.

Criterios

Las situaciones comentadas se apartan de lo establecido en las secciones A y F de la *Política ATI-003, Seguridad de los Sistemas de Información*; y en las secciones C y E de la *Política ATI-015, Programa de Continuidad Gubernamental*, de la *Carta Circular 140-16*.

Efectos

La situación comentada en el **apartado a.** le impide al Municipio estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas principales utilizados en sus dependencias, y considerar cómo protegerlos para reducir los riesgos de daños materiales y pérdida de información.

Lo comentado en el **apartado b.** puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno. Además, impide al Municipio tener un control documentado sobre el manejo de incidentes, que permita implementar acciones correctivas y preventivas oportunas en casos similares que puedan presentarse en el futuro.

Causas

La situación comentada en el **apartado a.** se atribuye a la falta de conocimiento que tenía el personal de la Oficina de Informática sobre lo que debía contener un análisis de riesgos.

Lo comentado en el **aparatado b.** se atribuye a que el Municipio se encontraba en proceso de evaluar las políticas y normas que regirán su nuevo reglamento, el cual incluirá un plan y procedimientos escritos para el manejo de incidentes.

Véanse las recomendaciones de la 1 a la 3.a.

Hallazgo 2 - Falta de un plan de contingencias

Situación

a. Toda entidad gubernamental debe contar con un plan de contingencias, para restablecer sus operaciones más importantes en caso de que surja una emergencia. El mismo debe ser evaluado periódicamente, al menos, cuando existan cambios significativos en la misión de la entidad, la organización, los procesos de negocio y la infraestructura de tecnología de información, incluidos los equipos, los programas y el personal. Además, debe ser distribuido al personal correspondiente.

   Al 11 de julio de 2019, el Municipio carecía de un plan de contingencias. En su lugar se nos suministró el *Plan para el Manejo de Emergencias e Incidentes* como plan de contingencias. El mismo incluía procedimientos y recomendaciones para proteger y salvaguardar la propiedad en las instalaciones del Municipio, pero no las tareas que debe efectuar la Oficina de Informática del Municipio ni los requisitos necesarios para atender las situaciones de emergencia que se indican a continuación:

   - La identificación del centro de procesamiento de datos alterno y de respaldo de información.

- Los procedimientos a seguir cuando el centro de cómputos no pueda recibir ni transmitir información de los usuarios que acceden mediante conexiones remotas a los sistemas de información.
- La identificación de los archivos críticos del Municipio.
- El inventario actualizado de los equipos, los sistemas operativos y las aplicaciones.
- El detalle de la configuración de los equipos críticos (equipo de comunicación y servidores) y del contenido de los respaldos y archivos.
- El itinerario de restauración que incluya el orden de las aplicaciones a restablecer y los procedimientos para restaurar los respaldos.
- La lista de los proveedores principales que incluya el número de teléfono y el nombre del personal de enlace con el Municipio.

Criterio

La situación comentada se aparta de lo establecido en el Capítulo 3.5, *Contingency Planning*, del FISCAM.

Efecto

Lo comentado puede 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 computadorizados del Municipio.

Causa

Lo comentado se atribuye a que el personal de la Oficina de Informática del Municipio no tenía el conocimiento para determinar lo que debía incluir

el *Plan para el Manejo de Emergencias e Incidentes*, con respecto a las contingencias que debe considerar el Municipio para garantizar la continuidad de sus operaciones.

Véanse las recomendaciones 1 y 3.b.

Hallazgo 3 - Deficiencias relacionadas con los parámetros de seguridad configurados y la documentación relacionada con la autorización y la justificación de los privilegios otorgados a los usuarios del servidor principal

Situaciones

a. Los controles de acceso limitan y detectan los accesos inapropiados a los recursos de tecnología (datos, equipos e instalaciones), y los protege de modificación no autorizada, pérdida y divulgación. Estos controles incluyen tanto los lógicos como los físicos. Los controles de acceso lógico requieren que los usuarios se autentiquen, mediante el uso de contraseñas secretas u otros identificadores, y limitan los archivos y otros recursos a los que pueden acceder y las acciones que pueden realizar. Las entidades gubernamentales son responsables de diseñar y mantener la seguridad de sus sistemas de información, por lo que deben asegurarse de lo siguiente:

   - Establecer formalmente políticas de cuentas (políticas de las contraseñas y de control de cuentas) basadas en riesgos, y requerir su cumplimiento.
   - Limitar los intentos para acceder al sistema con una contraseña errónea, para asegurar que esta no pueda ser descifrada.
   - Establecer, en las políticas y los procedimientos de la entidad, criterios para identificar los eventos significativos del sistema que se deben registrar.
   - Establecer procesos que permitan examinar las actividades de los usuarios en aquellos activos sensitivos que lo ameriten.

Para llevar a cabo las operaciones y brindar sus servicios, el Municipio contaba con tres servidores, entre estos, el servidor principal. Mediante este se controlaba el acceso a los recursos de la red y se le permitía el acceso a Internet a los usuarios autorizados.

El examen efectuado el 29 de julio de 2019, sobre los parámetros de seguridad definidos en el sistema operativo de dicho servidor, reveló lo siguiente:

1) La política para requerir que las contraseñas de las cuentas de acceso tuvieran, al menos, ocho caracteres y unas combinaciones alfanuméricas (*Password must meet complexity requirements*) estaba inhabilitada.

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 creación, modificación o eliminación de una cuenta o grupo de usuarios; el cambio de nombre o contraseña; y la activación o desactivación de una cuenta o grupo de usuarios (*Audit* account *management*)
   - El acceso al directorio de servicio (*Audit directory service access*)
   - La activación y desactivación de las cuentas (*Audit logon events*)
   - Los accesos a los archivos, fólders e impresoras (*Audit object access*)
   - Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Audit policy change*)

- El uso de los privilegios asignados a los usuarios (*Audit privilege use*)
- 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*).

3) Las políticas sobre los privilegios asignados a los usuarios (*User Rights Assignment*) no estaban definidas.

4) La opción de seguridad para desactivar automáticamente del sistema al usuario, una vez venciera el término de acceso a los recursos de la red, previamente establecido (*Force logoff when logon hours expire*), estaba inhabilitada. Las restantes opciones de seguridad (*Security Options*) no estaban definidas.

b. Las entidades gubernamentales deben implementar controles de acceso para la utilización de la información y los programas, de forma que estos sean accedidos solo por el personal autorizado. Entre estos controles, se sugiere mantener la documentación de las solicitudes de acceso a los sistemas de información computadorizados.

Al 29 de julio de 2019, el Municipio contaba con 127 cuentas activas de acceso al servidor principal. Una programadora de sistemas y un consultor privado contratado por el Municipio eran los responsables de crear y efectuar el mantenimiento de estas cuentas y de documentar la creación, modificación y eliminación de los usuarios.

El examen efectuado el 5 de agosto de 2019 sobre el proceso para documentar la autorización y justificación de los privilegios otorgados a 10 de las 127 cuentas de accesos asignadas al personal del Municipio para acceder a su servidor principal, reveló que en el Municipio no contaban con documentación para nueve de estas.

Criterios

Las situaciones comentadas son contrarias a lo establecido en las secciones C y E de la *Política ATI-003* de la *Carta Circular 140-16*. Además, las situaciones comentadas se apartan de lo sugerido en el Capítulo 3.2, *Access Control*, del FISCAM.

Efectos

Lo comentado puede propiciar que personas no autorizadas accedan a información confidencial mantenida en los sistemas computadorizados del Municipio y puedan hacer uso indebido de esta. También pueden 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. Además, lo comentado en el **apartado b.** impide al Municipio mantener la evidencia requerida de las autorizaciones para otorgar, modificar o cancelar los accesos y privilegios a los usuarios.

Causa

Las situaciones comentadas se debían a que el Municipio no contaba con normas, políticas o procedimientos para configurar las políticas de seguridad en el servidor principal, ni para documentar por escrito la creación, modificación y cancelación de las cuentas de acceso a la red y los privilegios otorgados a sus usuarios.

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

Hallazgo 4 - Falta de respaldos periódicos de la información computadorizada, y de almacenamiento fuera de los predios de la Oficina de Recursos Humanos

Situaciones

a. Las entidades gubernamentales deben establecer procedimientos para respaldar periódicamente la información y los programas computadorizados, y almacenarlos en un lugar seguro y distante de sus predios. De ocurrir una emergencia o desastre que afecte las instalaciones principales de la entidad, los respaldos estarán disponibles para que se pueda recuperar la mayor cantidad de información.

El Municipio contaba con un servidor principal y un servidor de archivos (*file server*) para darle acceso a los sistemas de información y guardar los documentos de los usuarios. Además, contaba con una computadora donde estaba instalada la aplicación ABS, en donde se mantenía la asistencia y la acumulación de licencias de los empleados del Municipio.

La documentación e información obtenida relacionada con dichas operaciones reveló lo siguiente:

1) Al 2 de julio de 2019, en el Municipio no se realizaban respaldos periódicos de la información almacenada en el servidor de archivos ni de la configuración del servidor principal.

2) Al 20 de agosto de 2019, la directora de Recursos Humanos nos indicó que el respaldo de la aplicación ABS se grababa en un medio de almacenamiento externo (*pen drive*) que se guardaba en un archivo bajo llave en la Oficina de Recursos Humanos, y no se mantenía una copia fuera de los predios de dicha Oficina.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la Sección B.2 y 3 de la *Política ATI-003* de la *Carta Circular 140-16*. Además, lo comentado es contrario a lo sugerido en el Capítulo 3.5 del FISCAM.

Efectos

La situación comentada en el **apartado a.1)** podría ocasionar la pérdida permanente de información importante, sin la posibilidad de poder recuperarla, lo que afectaría adversamente las operaciones del Municipio. Además, ocasionó que, luego del paso del huracán María cuando el servidor principal se dañó, tuvieran que configurarlo desde cero por no existir un respaldo de la configuración de este.

Lo comentado en el **apartado a.2)** puede ocasionar que, en casos de emergencias, el Municipio no pueda disponer de los respaldos de información necesarios para la continuidad de las operaciones de la Oficina de Recursos Humanos.

Causa

Lo comentado se atribuye a que en el Municipio no contaban con un procedimiento para crear los respaldos de información.

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

RECOMENDACIONES

A la directora de la Oficina de Gerencia y Presupuesto

1. Ver que la Oficina de Gerencia Municipal se asegure de que el Municipio cumpla con el *Plan de Acción Correctiva* de esta Oficina. **[Hallazgos del 1 al 4]**

Al alcalde

2. Asegurarse de que se realice y documente un informe de análisis de riesgos que considere todos los sistemas de información computadorizados del Municipio, y que esté de acuerdo con la estructura organizacional y el ambiente operacional del mismo. El análisis preparado debe ser remitido para su aprobación. Una vez aprobado, ver que se revise cada vez que ocurra un cambio significativo dentro de la infraestructura operacional y tecnológica del Municipio para asegurarse de que se mantenga actualizado. **[Hallazgo 1-a.]**

3. Ejercer una supervisión efectiva sobre la directora de Recursos Humanos para que esta se asegure de lo siguiente:

    a. Se prepare y remita para su aprobación, un procedimiento o plan para el manejo de incidentes. Como parte de este, debe identificarse el personal asignado al equipo de respuesta, el tiempo mínimo y máximo de respuesta, y la documentación de todos los incidentes y la metodología utilizada para resolverlos. Esto, de manera que, cuando dichos incidentes se repitan, se puedan

resolver en el menor tiempo posible sin afectar los sistemas de información computadorizados y la continuidad de las operaciones del Municipio. **[Hallazgo 1-b.]**

b. Se revise y actualice el *Plan para el Manejo de Emergencias e Incidentes*, para que incluya los aspectos comentados en el **Hallazgo 2**, y lo remita para su aprobación. Una vez aprobado, debe asegurarse de que se distribuya a los funcionarios y a los empleados concernientes, se mantenga actualizado, se realicen pruebas periódicas para garantizar su efectividad y se conserve copia en un lugar seguro fuera de los predios del Municipio.

c. Se impartan instrucciones al personal de la Oficina de Informática para que evalúe las opciones correspondientes a las políticas de las contraseñas de las cuentas de acceso (*Password Policy*) y de auditorías (*Audit Policy*), los parámetros de seguridad (*Security Options*) y los privilegios a los usuarios (*User Rights Assignment*), y defina las que considere necesarias de acuerdo con los riesgos y las amenazas de los sistemas de información del Municipio. **[Hallazgo 3-a.]**

d. Se prepare y remita para su aprobación, normas o procedimientos para reglamentar las operaciones de los sistemas de información del Municipio, que incluyan las directrices que permitan documentar por escrito la creación, modificación y cancelación de las cuentas de acceso a la red y de los privilegios otorgados a sus usuarios. **[Hallazgo 3-b.]** Además, estas normas o procedimientos deben incluir instrucciones específicas para la creación y el almacenamiento de los respaldos de información. **[Hallazgo 4]**

e. Se identifiquen alternativas costo-efectivas, para que el personal de la Oficina de Informática prepare copias recurrentes de la información contenida en los servidores, y almacene una copia de los respaldos en un lugar seguro fuera del Municipio. Dicho lugar no debe estar expuesto a las mismas amenazas de desastre que la

Oficina de Informática, en donde se encuentran ubicados los servidores; y la Oficina de Recursos Humanos, en donde está ubicada la computadora de la aplicación ABS. **[Hallazgo 4]**

APROBACIÓN

A los funcionarios y a los empleados del Municipio, 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

MUNICIPIO DE CAYEY
OFICINA DE INFORMÁTICA

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Rolando Ortiz Velázquez	Alcalde	13 mar. 19	2 ago. 19
Sra. Mildred Rivera Ruiz	Secretaria Municipal	13 mar. 19	2 ago. 19
Sr. Edwin Quiles Rosario	Director de Finanzas	13 mar. 19	2 ago. 19
Sra. Johannie Z. Ortiz Huertas	Directora de Recursos Humanos	13 mar. 19	2 ago. 19
Sr. Ángel L. Tolentino Feliciano	Auditor Interno	13 mar. 19	2 ago. 19
Sra. Celeniz Rosado Malavé	Programadora de Sistemas de Información[3]	13 mar. 19	3 jul. 19

[3] El puesto estuvo vacante del 4 de julio al 2 de agosto de 2019.

ANEJO 2

MUNICIPIO DE CAYEY
OFICINA DE INFORMÁTICA

FUNCIONARIOS PRINCIPALES DE LA LEGISLATURA MUNICPAL DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Lyda M. Rivera Rivera	Presidenta	13 mar. 19	2 ago. 19
Sra. Nelly V. Cruz López	Secretaria	13 mar. 19	2 ago. 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

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr