INFORME DE AUDITORÍA TI-21-16

21 de junio de 2021

Departamento de Salud

Oficina de Informática y Avances Tecnológicos

(Unidad 5290 - Auditoría 14435)

Período auditado: 1 de octubre de 2019 al 16 de septiembre de 2020

CONTENIDO

Página

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

21 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 de la Oficina de Informática y Avances Tecnológicos (Oficina de Informática) del Departamento de Salud. 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 del Departamento se efectuaron de acuerdo con la ley y la reglamentación aplicables.

Objetivos específicos

1. Determinar si se han establecido las políticas de cuentas de acceso y seguridad, en el dominio principal y los subdominios de la red del Departamento, y las políticas de seguridad locales en los servidores principales donde están configurados estos dominios, de acuerdo con las políticas establecidas en la *Orden Administrativa 153*, *Para establecer las normas y controles para el uso de equipos y/o sistemas computadorizados de información, correo electrónico, sistemas on-line e internet*, aprobada el 19 de junio de 2000 por la entonces secretaria de Salud; y 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, entre otros.

2. Determinar si se documentan las autorizaciones de acceso de los usuarios del dominio principal y los subdominios de la red del Departamento, si los accesos son otorgados conforme a las autorizaciones, y si se inactivan las cuentas de los exempleados de acuerdo con las políticas establecidas en la *Carta Circular 140-16*, entre otros.

3. Determinar si el Departamento cuenta con una herramienta para el monitoreo de las actividades de la red y si se revisan con regularidad estas actividades de acuerdo con lo establecido en la *Orden Administrativa 153* y la *Carta Circular 140-16*, entre otros.

CONTENIDO DEL INFORME

Este es el segundo informe, y contiene dos hallazgos del resultado del examen que realizamos de los objetivos indicados. El informe de auditoría anterior es el *TI-20-07* del 12 de mayo de 2020, el cual contiene el resultado del examen de los cambios a los sueldos de los empleados regulares, registrados en el sistema de Recursos Humanos Mecanizados (RHUM) por el personal de la División de Nombramientos y Cambios de la Secretaría Auxiliar de Recursos Humanos y Relaciones Laborales del Departamento. Ambos informes están disponibles en nuestra página en Internet: www.ocpr.gov.pr.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 1 de octubre de 2019 al 16 de septiembre de 2020. En algunos aspectos examinamos operaciones de fechas anteriores. El examen lo efectuamos de acuerdo con las normas de auditoría gubernamental generalmente aceptadas contenidas en el *Government Auditing Stardards* 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 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; 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.

Para realizar esta auditoría utilizamos la *Orden Administrativa 153* y las políticas establecidas en 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 Systems Controls Audit Manual* (*FISCAM*)[1], emitido por el GAO. Aunque al Departamento 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

El Departamento de Salud se creó en virtud de la *Ley Núm. 81 del 14 de marzo de 1912*, según enmendada, y fue elevado a rango constitucional por disposición del Artículo IV, Sección 6 de la Constitución. Es el organismo de carácter normativo en la prestación de servicios de salud en Puerto Rico. Su misión es propiciar y conservar la salud para que cada ser humano cuente con un bienestar físico, emocional y social que le permita el pleno disfrute de la vida, y contribuir así al esfuerzo productivo y creador de la sociedad.

El Departamento es dirigido por un secretario nombrado por el gobernador con el consejo y el consentimiento del Senado de Puerto Rico. Mediante la *Orden Administrativa 240*, aprobada el 4 de septiembre de 2008 por la

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

entonces secretaria de Salud, se reorganizó la estructura organizacional conforme a la política pública del Estado Libre Asociado de Puerto Rico, y la misión y visión del Departamento.

La Oficina de Informática del Departamento, cuenta con 1 director, quien funge como principal oficial de informática; 1 director de operaciones y control; 1 supervisor de apoyo técnico; 1 supervisora del área de administración; 1 especialista de sistemas de información; 1 desarrollador; 3 programadores; 1 asistente administrativa; 1 contador; 1 ayudante del área de administración; 4 técnicos y 2 técnicos/chofer.

Dicha Oficina es responsable de la red de comunicación del Departamento, en la que se interconectan 127 servidores físicos y 77 servidores virtuales, entre otros equipos.

Los recursos para financiar las actividades administrativas, operacionales y funcionales del Departamento provienen de resoluciones conjuntas del Fondo General, asignaciones especiales de la Asamblea Legislativa, fondos especiales estatales, fondos federales e ingresos propios. El presupuesto consolidado estimado del Departamento para los años fiscales 2018-19 al 2020-21 fue $899,858,000, $1,010,889,000, y $1,115,384,000, respectivamente.

La Oficina de Informática no cuenta con un presupuesto propio. Sus gastos operacionales son sufragados del presupuesto asignado a la Secretaría Auxiliar de Planificación del Departamento.

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

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

COMUNICACIÓN CON LA GERENCIA

Mediante correo electrónico del 7 de abril de 2021, remitimos el borrador de este *Informe* para comentarios del Hon. Carlos Mellado López, secretario de Salud; y el borrador de los **hallazgos** de este *Informe* para comentarios de los Dres. Lorenzo González Feliciano y Rafael Rodríguez Mercado, exsecretarios de Salud.

El secretario contestó mediante carta del 29 de abril de 2021. En los **hallazgos** se incluyeron algunos de sus comentarios.

Mediante correo electrónico del 23 de abril de 2021, el doctor Rodríguez Mercado nos informó que, al revisar los documentos recibidos, no tenía comentarios. El doctor González Feliciano no contestó.

CONTROL INTERNO

La gerencia del Departamento 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 del Departamento.

En los **hallazgos** se comentan 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 de la Oficina de Informática del Departamento, 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** que se comentan a continuación.

Hallazgo 1 - Deficiencias relacionadas con las políticas de contraseñas y de auditoría configuradas en los servidores principales del Departamento

Situaciones

a. Cada entidad 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; y requerir que estas sean cambiadas. Además, deben implementar procesos que permitan revisar las actividades de los usuarios en aquellos activos sensitivos que lo ameriten, y detectar incidentes de seguridad.

   Para proteger y garantizar la seguridad de los sistemas y su utilización para fines autorizados, el Departamento estableció mediante la *Orden Administrativa 153*, que las contraseñas deberán incluir, al menos, ocho caracteres y deberán cambiarse cada seis meses o cuando el administrador de la red lo estime necesario.

   El Departamento cuenta con nueve servidores principales en los que están configurados el dominio[2] principal y dos subdominios[3].

[2] Un dominio es un grupo de computadoras y dispositivos en una red que se administran como una unidad con reglas y procedimientos comunes. En Internet, los dominios están definidos por la dirección IP.

[3] Un subdominio es un dominio que forma parte de un dominio principal.

Mediante estos dominios, un consultor ofrecía servicios para la administración de la seguridad y la actualización de los servidores, entre otros.

Al 13 de noviembre de 2019, en el dominio principal y en los 2 subdominios de los servidores principales del Departamento existían un total de 5,606 cuentas de acceso activas.

El examen realizado a las políticas de seguridad de las cuentas de acceso activas, y del dominio principal y los dos subdominios, establecidas mediante los sistemas operativos de estos, reveló las siguientes deficiencias:

1) Al 13 de noviembre de 2019, la política de las contraseñas en los perfiles de las cuentas de acceso activas contaba con los siguientes errores:

    a) No permitía realizar un cambio de contraseñas (*PswdCanBeChanged: No*) a los usuarios de 221 cuentas de acceso del dominio principal y de 4 cuentas de acceso de un subdominio. Esto, contrario al cambio de contraseña requerido, al menos, cada 6 meses en la *Orden Administrativa 153*.

    b) No requería que expiraran las contraseñas de 215[4] cuentas de acceso del dominio principal, de 28[5] cuentas de uno de los subdominios y de 16 cuentas del otro subdominio. (*PswdExpires: No*)

2) Al 5 de diciembre de 2019, la política establecida en el dominio principal y los subdominios, para establecer el largo de las contraseñas (*minimum password lengh*) de las cuentas de usuarios, no requería los ocho caracteres establecidos mediante

[4] Ciento cincuenta y dos de estas cuentas de acceso se comentan en el **apartado a.1)**.

[5] Dos de estas cuentas de acceso se comentan en el **apartado a.1)**.

la *Orden Administrativa 153* y la *Política ATI-003, Seguridad de los Sistemas de Información*, de la *Carta Circular 140-16*. Esta política estaba configurada para requerir solo siete caracteres.

3) Al 5 de diciembre de 2019, no se habían definido las políticas, en el dominio principal y los subdominios, de auditoría (*Audit Policy*) para que el sistema produjera, al menos, un registro de los siguientes eventos:

   a) 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*)

   b) El acceso al servicio de directorio[6] (*Audit directory service access*)

   c) El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*Audit system events*).

   Además, en el dominio principal y uno de los subdominios no se habían definido las políticas para producir un registro de las solicitudes al servidor para validar las cuentas de usuario (*Audit account logon events*) y los cambios efectuados a las opciones de seguridad, los privilegios de los usuarios y las políticas de auditoría (*Audit policy change*). Tampoco se había configurado en este subdominio la política para la activación y desactivación de las cuentas de acceso (*Audit logon events*).

Criterios

Las situaciones comentadas en el **apartado a.1) y 2)** se apartan de lo establecido en el Apartado A.3 de la *Orden Administrativa 153*. Además, las situaciones comentadas son contrarias a lo establecido en las secciones C.1, E.4,.5 y .7 y F.1 de la *Política ATI-003* de la *Carta Circular 140-16*.

[6] El servicio de directorio almacena y organiza la información de los objetos de la red (impresoras, equipos, usuarios) y permite que estén disponibles para los usuarios y administradores.

Efectos

Las situaciones comentadas en el **apartado a.1) y 2)** pueden 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. Además, lo comentado en el **apartado a.3)** impide al Departamento mantener un registro de los eventos inusuales o los problemas ocurridos en la red, que le permita al consultor encargado de administrar la seguridad tomar a tiempo las medidas correctivas o preventivas necesarias.

Causas

Las situaciones comentadas se debían a que el entonces director de la Oficina de Informática[7] no se aseguró de que el consultor encargado de la administrar la seguridad configurara las políticas de contraseñas y de auditoría conforme a lo establecido en la *Orden Administrativa 153* y en la *Política ATI-003*. Además, se debían a que el Departamento no contaba con normas y procedimientos que incluyeran directrices para establecer las políticas de expiración de contraseñas y auditoría necesarias para asegurar el dominio principal y los subdominios. **[Apartado a.1)b) y 3)]**

Comentarios de la Gerencia

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

> Como parte de las iniciativas ya comenzadas se completó la redacción de nuestras políticas y procedimientos, basadas en los nuevos requerimientos de controles establecidos a nivel Estatal y Federal. Dichas políticas y procedimientos atienden específicamente los hallazgos señalados en cuanto a los cambios de contraseñas. Esperamos poder iniciar la implementación de las mismas en los próximos treinta (30) días. [*sic*]

Véase la Recomendación 1.a. y b.1).

[7] El entonces director de la Oficina de Informática fungió hasta el 30 de junio de 2020.

Hallazgo 2 - Deficiencias relacionadas con el proceso de desactivar las cuentas de acceso de los exempleados y las cuentas de acceso que no han sido utilizadas

Situaciones

a. Las entidades gubernamentales deben implementar controles de accesos para la utilización de la información y los programas de aplicación, de forma que estos sean utilizados solo por el personal autorizado. Entre estos controles, la entidad debe asegurarse de que los privilegios de accesos de los usuarios sean evaluados regularmente. Las cuentas de los sistemas de información deben administrarse para controlar eficazmente las cuentas de los usuarios e identificar y autenticar a los usuarios. También se deben revisar periódicamente las listas de autorizaciones de las cuentas de accesos a los sistemas de información para determinar si son apropiadas. Además, la entidad debe asegurarse de que los administradores de cuentas reciban una notificación cuando los usuarios de los sistemas de información cesan funciones o se transfieren para que se eliminen, inactiven o aseguren las cuentas de acceso asignadas.

   La Oficina de Informática utiliza la *Solicitud de Acceso a Sistemas de Información*[8] (*Solicitud de Acceso*) para documentar la creación, modificación y cancelación de las cuentas de acceso a los sistemas de información. Dicha *Solicitud* debe ser completada por el solicitante (información del usuario y firma) y su supervisor (espacios para identificar las aplicaciones, los accesos y firma). Luego, se debe digitalizar y registrar en la aplicación *OTAC Ticket System*, para ser entregado al especialista de sistemas de información responsable de crear, modificar o cancelar las cuentas de acceso. Además, para la cancelación de las cuentas, la directora de Nombramientos y Cambios de la Secretaría Auxiliar de Recursos Humanos y Relaciones Laborales debe enviar, por correo electrónico, la información de las terminaciones de los empleados a la Oficina de Informática para que se deshabiliten las cuentas de acceso.

[8] Revisado en abril de 2014.

Del 1 de octubre de 2016 al 1 de octubre de 2019, en el Departamento cesaron funciones 1,089 empleados.

El examen realizado del estatus, al 13 de noviembre de 2019, de las cuentas de acceso otorgadas a 459 de los exempleados y de las 5,606 cuentas activas en el dominio principal y los 2 subdominios, reveló que no se realizaba un mantenimiento adecuado de las cuentas, según se indica:

1) No se habían desactivado 87 cuentas de acceso asignadas a exempleados que cesaron funciones, entre el 1 de noviembre de 2016 y el 16 de junio de 2019. De estas, 37 cuentas permanecían activas en el dominio principal, 24 en 1 de los subdominios y 26 en el otro subdominio. Al 13 de noviembre de 2019, habían transcurrido de 150 a 1,107 días desde la separación de estos exempleados. Además, 38 de estas cuentas[9] fueron utilizadas entre 5 y 1,041 días luego de la fecha separación.

2) Se mantenían activas 786 cuentas de acceso que no se habían utilizado en, al menos, 6 meses. De estas, 452 cuentas permanecían activas en el dominio principal, 252 en 1 de los subdominios y 82 en el otro subdominio. Al 13 de noviembre de 2019, habían transcurrido entre 181 y 5,284 días desde el último acceso (*LastLogonTime*).

3) Se mantenían activas 755 cuentas de acceso que nunca habían sido utilizadas (*LastLogonTime: NEVER*). De estas, 670 cuentas permanecían activas en el dominio principal, 74 en 1 de los subdominios y 11 en el otro subdominio.

Criterios

Las situaciones comentadas son contrarias a lo establecido en las secciones E.3 y .6 de la *Política ATI-003* de la *Carta Circular 140-16* y en el Capítulo 3.2, *Access Control*, del *FISCAM*.

[9] De estas, 13 cuentas permanecían activas en el dominio principal, 19 en uno de los subdominios y 6 en el otro subdominio.

Efectos

Las situaciones comentadas impiden al Departamento mantener un control adecuado sobre la administración de las cuentas de acceso. Además, propicia que personas no autorizadas puedan utilizar estas cuentas para lograr acceso 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 dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causas

Las situaciones comentadas se debían, en parte, a que el Departamento no contaba con un procedimiento escrito para la creación, la modificación, la cancelación y el mantenimiento de las cuentas de acceso. Esto, para requerir, a la Secretaría Auxiliar de Recursos Humanos la notificación inmediata a la Oficina de Informática de los traslados, las licencias prolongadas y la separación del personal con acceso a los sistemas de información. También para requerir a dicha Oficina la revisión periódica de las cuentas no utilizadas. Además, el especialista de sistemas de información nos informó que en muchas ocasiones los supervisores de cada área no entregaban las solicitudes de acceso a la Oficina de Informática para requerir que el especialista de sistemas de información deshabilitara las cuentas de acceso de estos usuarios.

Comentarios de la Gerencia

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

> […] Se comenzó un proceso de evaluación de políticas y procedimientos de la Secretaria Auxiliar de Recursos Humanos y Relaciones Laborales para enmendar las políticas actuales en cuanto a las renuncias y desactivación de cuentas de exempleados del Departamento. De igual forma, se estará comenzando el proceso de desactivar aquellas cuentas señaladas e incluidas en los Anejos 3-7. [*sic*]

Véanse las recomendaciones 1.b.2) y c., y 2.

RECOMENDACIONES

Al secretario de Salud

1. Asegurarse de que el director de la Oficina de Informática cumpla con lo siguiente:

    a. Imparta instrucciones al encargado de administrar la seguridad para asegurarse de que:

        1) Modifique las políticas de las contraseñas establecidas en las cuentas de acceso, en el dominio principal y los subdominios, para que se requieran el uso de contraseñas de, al menos, ocho caracteres y estas se cambien cada seis meses, conforme a lo requerido en la *Orden Administrativa 153*. **[Hallazgo 1-a.1) y 2)]**

        2) Evalúe las políticas de auditoría que provee el sistema operativo y las configure conforme a los riesgos existentes y la capacidad de sus servidores. Una vez configurados, mantenga respaldos de los registros de auditoría y los revise con regularidad para identificar actividades irregulares e implementar medidas preventivas y correctivas. **[Hallazgo 1-a.3)]**

    b. Prepare y remita para su aprobación un procedimiento para:

        1) La configuración de las políticas de seguridad en los dominios y subdominios del Departamento que incluya, entre otras, las políticas para requerir la expiración de las contraseñas y de auditoría. **[Hallazgo 1-a.1)b) y 3)]**

        2) La creación, la modificación, la cancelación y el mantenimiento de las cuentas de acceso que requiera, entre otras cosas, notificar a la Oficina de Informática los traslados, las licencias prolongadas y la separación del personal con acceso a los sistemas de información y la revisión periódica de las cuentas no utilizadas. **[Hallazgo 2]**

c. Imparta instrucciones al especialista de sistemas de información para asegurarse de que desactiven las cuentas de acceso de los exempleados, las que nunca se han utilizado y las que no se han utilizado en seis meses o por períodos prolongados. Además, se asegure de que, en lo sucesivo, se verifiquen y desactiven estas cuentas de acceso. **[Hallazgo 2]**

2. Impartir instrucciones a la secretaria auxiliar de Recursos Humanos y Relaciones Laborales para que, en coordinación con el director de la Oficina de Informática, prepare y remita, para la aprobación del secretario, normas o procedimientos que requieran la notificación inmediata a dicha Oficina de la terminación, las licencias prolongadas, el traslado o la reclasificación de empleados y la desactivación de las cuentas de acceso asignadas a estos. **[Hallazgo 2-a.1)]**

APROBACIÓN

A los funcionarios y a los empleados del Departamento, 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

DEPARTAMENTO DE SALUD
OFICINA DE INFORMÁTICA Y AVANCES TECNOLÓGICOS

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Dr. Lorenzo González Feliciano	Secretario	27 mar. 20	16 sep. 20
Dra. Concepción Quiñones de Longo	Secretaria Interina	14 mar. 20	26 mar. 20
Dr. Rafael Rodríguez Mercado	Secretario	1 oct. 19	13 mar. 20
Dra. Iris Cardona Gerena	Subsecretaria	8 jun. 20	16 sep. 20
Dra. Concepción Quiñones de Longo	"	1 oct. 19	13 mar. 20[10]
Sra. Celia Pérez Sepúlveda	Secretaria Auxiliar Interina de Recursos Humanos y Relaciones Laborales	1 jun. 20	16 sep. 20
Sra. Azalia Rivera Gómez	Secretaria Auxiliar de Recursos Humanos y Relaciones Laborales	1 oct. 19	31 may. 20
Sr. Jose M. Irizarry Figueroa	Director de la Oficina de Informática	1 jul. 20	16 sep. 20
Sr. Alexander Quevedo Pagán	"	1 oct. 19	30 jun. 20

[10] El puesto de subsecretario estuvo vacante del 14 de marzo al 7 de junio de 2020.

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