INFORME DE EXAMEN

OIG-E-26-002

Oficina del Inspector General
Gobierno de Puerto Rico

Departamento de Salud

Registro Demográfico

Examen del manejo y los controles internos del sistema digital relacionados con las solicitudes de los certificados de eventos vitales y la evaluación de los procesos subsiguientes hasta que los ciudadanos reciben los certificados luego de efectuar los pagos correspondientes.

3 de octubre de 2025

TABLA DE CONTENIDO

PÁGINA

RESUMEN EJECUTIVO

La Oficina del Inspector General de Puerto Rico (OIG), mediante su Área de Pre-Intervención y Exámenes, llevó a cabo un examen en el Registro Demográfico, del Departamento de Salud. El propósito fue evaluar el manejo de las solicitudes de certificados de eventos vitales, los controles internos del sistema digital y los procesos hasta la entrega de los certificados a los ciudadanos luego de realizar sus pagos. El examen reveló deficiencias significativas en controles internos e incumplimientos con leyes y reglamentos aplicables, que afectan la transparencia, la confiabilidad y la eficiencia de los procesos. Los hallazgos principales fueron los siguientes:

- Cobro en exceso de derechos - el Registro Demográfico cobró más de **$2,904,445.00** en exceso a lo aprobado en el Reglamento 5961, en 487,559 certificaciones emitidas entre el 1 de julio de 2022 y el 28 de febrero de 2025. Esta práctica ocurre desde el noviembre de 2015, cuando se preparó una enmienda de emergencia al Reglamento 5961 que nunca fue radicada ni aprobada por el Departamento de Estado, a pesar de que afectaba derechos de terceros. Desde entonces, el Registro Demográfico ha continuado cobrando tarifas no autorizadas.
- Deficiencias en la expedición de certificados de eventos vitales- problemas en los procesos de entrega y confiabilidad en la expedición de certificados de nacimiento, matrimonio, defunción y otros.
- Controles de acceso deficientes- fallas en la administración de usuarios y accesos al sistema que maneja los registros de eventos vitales, lo que representa un riesgo para la seguridad y confidencialidad de la información.
- Contratos sin radicar a tiempo- acuerdos colaborativos y sus enmiendas no fueron radicados o se radicaron con tardanza en el Registro de Contratos de la Oficina del Contralor de Puerto Rico.
- Reglamentos y procedimientos sin actualizar- documentos normativos desactualizados que limitan la efectividad de la gestión administrativa.
- Deficiencias en el diagrama de red de comunicaciones- el diagrama estaba incompleto o inexistente, lo que impide un control efectivo de la infraestructura tecnológica.
- Ausencia de un Plan Estratégico de Tecnología de Información- no se han definido metas claras ni estrategias de largo plazo para la administración tecnológica del Registro Demográfico.
- Fallas en el análisis de riesgos- no se realizan análisis adecuados de riesgos en los sistemas de información, lo que aumenta la vulnerabilidad institucional.
- Planes de continuidad y contingencia incompletos- el Plan de Continuidad de Operaciones presenta deficiencias y el Registro Demográfico carece de un Plan de Contingencias formal para manejar situaciones de emergencia tecnológica.

- Deficiencias en inventario de sistemas- informes incompletos y falta de controles adecuados para mantener actualizado el inventario de sistemas de información.
- Falta de adiestramientos: el personal no recibe capacitaciones suficientes sobre normas y procedimientos de seguridad en sistemas de información.
- Problemas de infraestructura física: desorganización en el cableado de equipos de comunicación, lo que dificulta el manejo y mantenimiento de la red.

El 9 de noviembre de 2015, se realizó una enmienda al Reglamento 5961 donde se establecían nuevos costos para la emisión de los eventos vitales, la cual tuvo la aprobación por el entonces gobernador de Puerto Rico. Esta enmienda fue preparada como un reglamento de emergencia, conforme con la petición del Registro Demográfico. Sin embargo, no fue radicada ante el Departamento de Estado porque no se culminó el procedimiento para la aprobación expedita que requiere y exige la *Ley de Procedimiento Administrativo Uniforme* al ser uno que afecta derechos de terceros.

Posterior a esto tampoco se radicaron y aprobaron enmiendas al Reglamento 5961 para aumentar los derechos a cobrar. El Registro Demográfico ha seguido hasta este momento cobrando por servicios no aprobados por reglamentación.

Conforme con lo establecido en el Reglamento Núm. 9229, *Reglamento para la Administración del Plan de Acción Correctiva de la Oficina del Inspector General de Puerto Rico*, del 13 de noviembre de 2020, y las disposiciones del Artículo 17 de la citada Ley Núm. 15-2017, la OIG remite el presente informe a la autoridad nominadora para que tome las medidas correctivas necesarias y notifique a la OIG las acciones tomadas para garantizar el fiel cumplimiento de las leyes y reglamentos aplicables.

La OIG está comprometida en fomentar niveles óptimos de integridad, honestidad, transparencia, efectividad y eficiencia en el servicio público. De igual forma rechaza todo acto, conducta o indicio de corrupción por parte de funcionarios o empleados públicos que inflija sobre la credibilidad del Gobierno de Puerto Rico y sus entidades.

De conocer sobre actos que podrían poner en peligro el buen uso de fondos públicos, así como actos que podrían constituir corrupción, puede comunicarse con la línea confidencial de la OIG al 787-679-7979, a través del correo electrónico informa@oig.pr.gov o a través de la página electrónica www.oig.pr.gov/informa.

El presente informe se hace público conforme con lo establecido en la citada Ley 15-2017, según enmendada, y otras normativas aplicables.

INFORMACIÓN SOBRE LA ENTIDAD EXAMINADA

El RD de Puerto Rico fue creado en virtud de la Ley Núm. 24 de 22 de abril de 1931, según enmendada, conocida como *Ley del Registro Demográfico de Puerto Rico* (en adelante, "Ley Núm. 24 de 1931"). Dicha ley encomienda como funciones principales la inscripción de los eventos vitales y la recopilación de datos, entiéndase nacimientos, defunciones (muertes) y matrimonios. También concede la expedición de certificaciones de los eventos mencionados, la custodia y conservación de los libros civiles (1885-1931) y la producción de estadísticas vitales.

Además, el Artículo 3-A de la Ley Núm. 24 de 1931 faculta al secretario de Salud a establecer, mediante reglamentación, los importes de los derechos a ser cobrados por los servicios que presta el RD y disponer que los fondos recaudados sean depositados en un Fondo Especial en el Departamento de Hacienda. Los fondos recaudados se destinan al presupuesto del RD para sufragar los gastos de funcionamiento. Mediante el Reglamento 5961, se establecen los procedimientos para que el RD cobre los derechos por los servicios de expedición de los certificados y otros servicios, tales como: adopciones, emancipaciones, correcciones judiciales y administrativas, legitimaciones, reconocimientos, inscripciones tardías, permisos de traslado y enterramientos, licencias de matrimonios, certificación de divorcio, certificaciones negativas y certificación de inscripción tardía.

Mediante la Orden Administrativa 578, conocida como *Orden Administrativa del Secretario de Salud para reorganizar la estructura organizacional del Departamento de Salud de conformidad con la política pública del Gobierno de Puerto Rico y definir las funciones de las unidades que compone el departamento y derogar las órdenes administrativas [sic] 569 y 573*, emitida el 1 de septiembre de 2023 por el entonces secretario de Salud, se reorganizó la estructura organizacional del Departamento de conformidad con la política pública del Gobierno de Puerto Rico. Además, se definieron las funciones de las unidades que componen el Departamento. En esta Orden se presenta el documento *Transformación Organizacional del DSPR 2023*, que describe en detalle las unidades y sus funciones. El Registro Demográfico pasó a ser una División dentro de la Secretaría Auxiliar para la Coordinación de Servicios y Asistencia en Salud. En esta Secretaría se agruparon los servicios y procesos relacionados con la coordinación de la asistencia de salud a la población.

El director del RD es nombrado por el secretario de Salud y ejerce sus funciones desde la Oficina Central. Las oficinas regionales están a cargo de un supervisor Regional, quien le responde al director. El RD tiene 57 oficinas locales que están a cargo de un registrador, quien le responde al supervisor de la Oficina Regional correspondiente. El registrador es responsable de la corrección, custodia y protección de las inscripciones de todos los eventos vitales que ocurren en la jurisdicción. Además, tiene la responsabilidad de preparar las instrucciones, formas, impresos, y libros necesarios para obtener la información de cada evento.

Dentro de la función de velar por el proceso de evaluación y calidad de información, el RD utiliza los estándares de calidad de la *National Association of Public Health Statistics Information System* (NAPHSIS). Esta entidad establece los parámetros de ejecución para el funcionamiento y operación de una oficina de registros vitales; recomendando la publicación anual de los datos para hacerlos accesibles al público, agencias, organizaciones, y otras entidades interesadas.

El público en general puede solicitar sus documentos mediante las siguientes opciones:

- Plataformas electrónicas y digitales: RenovacionesOnline[1], PR.GOV[2], VitalChek[3].
- Ordenar por teléfono a través de VitalChek.
- Visita a una oficina local.
- Solicitud por correo postal.

En el siguiente enlace de la página web del Departamento https://www.salud.pr.gov/CMS/36 se provee información acerca de los servicios que presta el RD.

BASE LEGAL

El presente informe se emite en virtud de los Artículos 7, 8, 9 y 17 de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico*.

OBJETIVOS

El examen estuvo dirigido a evaluar el manejo y los controles internos del sistema digital relacionados con las solicitudes de los certificados de eventos vitales y la evaluación de los procesos subsiguientes hasta que los ciudadanos reciben los certificados luego de efectuar los pagos correspondientes en el RD del Departamento.

Esto, de acuerdo con lo establecido en las siguientes regulaciones:

- Ley Núm. 24 de 22 de abril de 1931, según enmendada, conocida como *Ley del Registro General Demográfico de Puerto Rico.*
- Ley Núm. 230 de 23 de julio de 1974, según enmendada, conocida como *Ley de Contabilidad del Gobierno de Puerto Rico.*

[1] RenovacionesOnline es un sistema para que los ciudadanos y empresarios puedan hacer múltiples tramites de forma digital.

[2] El portal de internet con información centralizada del Gobierno de Puerto Rico es una herramienta en línea diseñada para brindar a los ciudadanos acceso a información relevante y actualizada sobre los servicios y actividades gubernamentales.

[3] A través de esta plataforma tiene la opción de ordenar su certificación de un evento vital de manera online, por teléfono o por correo.

- Ley Núm. 18 de 30 de octubre de 1975, según enmendada, conocida como *Ley de Registros de Contratos.*

- Ley Núm. 170 de 12 de agosto de 1988, según enmendada, conocida como *Ley de Procedimiento Administrativo Uniforme del Estado Libre Asociado de Puerto Rico*[4].

- Ley Núm. 38-2017, según enmendada, conocida como *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico.*

- Ley Núm. 75-2019, conocida como *Ley de la Puerto Rico Innovation and Technology Service (PRITS).*

- Reglamento Núm. 5961 de 7 de mayo de 1999, conocido como *Reglamento del Procedimiento para el Cobro de los Derechos del Registro Demográfico Correspondientes a la Expedición de Certificados de Nacimiento, Matrimonio, Defunción y Natimuerto, y Además de Otros Servicios*.

- Carta Circular Núm. 2-17 (RD), *Para establecer Administrativamente el Procedimiento Uniforme para la Expedición de Certificados de Eventos Vitales*, emitida el 30 de junio de 2017.

- Procedimiento RDS2, *Procedimiento para creación, modificación, reactivación o cancelación de acceso al sistema del Registro Demográfico (RegDem)*, revisado en septiembre de 2019.

- Procedimiento RD-02-2020, *Para establecer administrativamente los requisitos e instrucciones para solicitar una certificación de un evento vital mediante el correo postal*, del 26 de febrero de 2020.

ALCANCE Y METODOLOGÍA DEL EXAMEN

El examen cubrió el período del 1 de julio de 2022 hasta el 28 de febrero de 2025. Fue realizado conforme con las leyes, normas, reglamentos y procedimientos aplicables al RD relacionados con el manejo y los controles internos del sistema digital. Esto en relación con las solicitudes de los certificados de eventos vitales y la evaluación de los procesos subsiguientes hasta que los ciudadanos reciben los certificados luego de efectuar los pagos correspondientes.

Se efectuaron las pruebas que se consideraron necesarias, basado en muestras y de acuerdo con las circunstancias.

La metodología utilizada para el examen fue la siguiente:

[4] La Ley Núm. 170 de 1988 fue derogada por la Ley Núm. 38-2017, según enmendada, *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico*, que contiene disposiciones similares.

1. Realizar un estudio preliminar de leyes, reglamentos y procedimientos relacionados con el cobro de derechos para la emisión de eventos vitales.

2. Determinar la existencia de controles internos adecuados relacionados con las aplicaciones que maneja el RD en la expedición de eventos vitales.

3. Evaluar el cumplimiento con las leyes y reglamentos aplicables en la aprobación de acuerdos colaborativos entre el RD, el Gobierno y las empresas privadas.

4. Determinar si el procedimiento para la emisión de eventos vitales se llevó a cabo de acuerdo con la reglamentación aprobada.

5. Entrevistas a funcionarios y empleados del RD.

6. Examen de expedientes de los acuerdos colaborativos e información relacionada que se almacena en los sistemas de información que administra el RD.

7. Evaluación de los controles internos adoptados por el RD referente a los sistemas de información.

8. Análisis de informes, certificaciones y documentos provistos por el RD.

En algunos aspectos, se examinaron transacciones, documentos y operaciones de fechas anteriores y posteriores.

HALLAZGOS

En esta sección se detallan los hallazgos relacionados con las situaciones detectadas durante el transcurso del presente examen.

Hallazgo 1 – Cobro de derechos bajo el concepto de la emisión de eventos vitales en exceso a lo aprobado en el Reglamento 5961

Situación

El RD tiene entre sus funciones principales emitir las correspondientes certificaciones de eventos vitales[5] a las partes interesadas[6]. La emisión de certificados de eventos vitales conlleva unos costos establecidos en el Anejo A del Reglamento Núm. 5961 (Reglamento 5961), aprobado el 7 de mayo de 1999, por el Departamento de Estado, conocido como *Reglamento del procedimiento para el cobro de los derechos del Registro Demográfico correspondientes a la expedición de certificados*

[5] Significa los eventos de la vida humana, que incluyen los nacimientos, muertes, muertes fetales, terminaciones inducidas de embarazos, matrimonios y divorcios.

[6] De acuerdo con el Artículo 2 (12) de la citada Ley Núm. 24 de 1931 se define la parte interesada como: *significará el inscrito, si es de dieciocho (18) años de edad o mayor, su padre, su madre, su representante legal, custodio legal o tutor, o los herederos del inscrito. Será, además, cualquier menor que a su vez sea padre o madre de un menor para lo cual se autoriza la expedición de actas relacionadas tanto para su persona como para su hijo(a). "Parte interesada" será además, la señalada mediante orden del Tribunal.*

de nacimiento, matrimonio, defunción y natimuerto además de otros servicios enumerados a continuación:

- *Adopciones*
- *Emancipaciones*
- *Correcciones Judiciales*
- *Correcciones Administrativas*
- *Legitimaciones*
- *Reconocimientos*
  - *Dentro de 90 días*
  - *Después de 90 días*
- *Inscripciones Tardías (Nacimiento, Matrimonio, Defunción y Natimuerto)*
  - *Después de diez (10) días y hasta el año*
  - *Después del año*
- *Permisos de Traslado y Enterramiento*
- *Licencias de Matrimonio*
- *Certificación de Divorcio*
- *Certificaciones Negativas*
- *Certificación Inscripción Tardía*

Según la información divulgada al público en general en las páginas web del RD, https://www.salud.pr.gov/CMS/36 y https://www.salud.pr.gov/CMS/341, los costos por la obtención de las certificaciones de eventos vitales aumentaron en comparación con los costos establecidos en el Reglamento 5961.

En vista del aumento en los costos sobre la expedición de eventos vitales y de otros servicios relacionados, se le solicitó a la directora ejecutiva del RD que suministrara una certificación donde indicara las fechas en la que inició el cobro de las nuevas tarifas de la expedición de eventos vitales y quién lo autorizó. Además, que proveyera cualquier documento que estuviera relacionado.

De acuerdo con la información, los documentos suministrados y las certificaciones de la directora ejecutiva del RD, el 9 de noviembre de 2015, se realizó una enmienda al Reglamento 5961, bajo la aprobación del entonces gobernador de Puerto Rico, donde se establecían nuevos costos para la emisión de los eventos vitales. Esta enmienda fue preparada como un reglamento de emergencia, conforme con la petición del RD. Sin embargo, el documento titulado *Enmienda al Reglamento 5961* no fue presentado ante el Departamento de Estado.

La directora del RD certificó que la Oficina de Asesores Legales del Departamento informó que la enmienda al Reglamento 5961 no fue radicada ante el Departamento de Estado porque no se culminó el procedimiento para la aprobación expedita que permitía la Sección 2.13 de la Ley Núm. 170 de 12 de agosto de 1988, *Ley de Procedimiento Administrativo Uniforme* (Ley Núm. 170 de 1988), vigente en el año 2015.

La tabla que se presenta a continuación muestra una comparativa de los costos establecidos en el Reglamento 5961 versus los costos propuestos en la enmienda no registrada en el Departamento de Estado y los costos presentados en las páginas web del RD:

Tabla 1: Comparativa de costos en el Reglamento 5961 versus los costos propuestos en la enmienda no aprobada en el Departamento de Estado, y los costos presentados en las páginas web del RD

Tipo de Servicio	Costo del servicio en el Anejo del Reglamento 5961	Costos propuestos en la Enmienda no aprobada en el Departamento de Estado	Costo del servicio en las Páginas web del RD https://www.salud.pr.gov/ CMS/36 CMS/341	Cambios al Anejo del Reglamento 5961
Expedición de Certificados				
Nacimientos	$5.00	$5.00	$5.00	
Copias adicionales		$10.00	$10.00	$10.00 por copias adicionales.
Matrimonios	$5.00	$10.00	$10.00	$10.00 por cada copia.
Defunciones	$5.00	$10.00	$10.00	$10.00 por cada copia.
Otros Servicios				
Emancipaciones	$25.00	$40.00	$40.00	Dos sellos de $20 cada uno.
Legitimaciones	$5.00	$10.00	$10.00	
Reconocimientos				
Dentro de 90 días	$5.00	$20.00	$20.00	
Después de 90 días	$10.00	$35.00	$35.00	
Certificación de paternidad literal, para enmendar el seguro social.			$20.00	
Literal de paternidad		$20.00		
Eliminar Ley #104 si aplica.			$20.00	

Tipo de Servicio	Costo del servicio en el Anejo del Reglamento 5961	Costos propuestos en la Enmienda no aprobada en el Departamento de Estado	Costo del servicio en las Páginas web del RD https://www.salud.pr.gov/ CMS/36 CMS/341	Cambios al Anejo del Reglamento 5961
Inscripciones Tardías de Nacimientos				
Después de 10 días hasta el año	$10.00	$25.00	$25.00	Después de los primeros 30 días hasta el año.
Después del año	$25.00	$150.00	$150.00	Nacimiento en PR no registrado oficialmente dentro del primer año: Un sello de $30, un sello de $25, dos sellos de $10, y un sello de $75, para un total de $150.
Autorización para Realizar Estudios Genealógicos	$5.00	$100.00	$100.00	Sello de Rentas Internas o giro postal por la solicitud o búsqueda realizada.

El examen relacionado con la información suministrada por la directora del RD y con los cobros realizados a los ciudadanos por concepto de emisión de eventos vitales reveló lo siguiente:

a. No aparece una enmienda al Reglamento 5961 en la página web del Departamento de Estado ni en el Registro de Reglamentos.

b. La directora del RD certificó que desconocía que la enmienda no fue aprobada por el Departamento de Estado.

c. No se presentó evidencia que se culminó el procedimiento para la aprobación expedita que permitía la Sección 2.13 de la precitada Ley Núm. 170 de 1988, *Ley de Procedimiento Administrativo Uniforme*, vigente en ese momento.

d. No se proporcionó evidencia que se haya presentado al Departamento de Estado la referida enmienda de emergencia al Reglamento 5961, debidamente firmada por la secretaria del Departamento y autorizada por el entonces gobernador de Puerto Rico, según certificado por la directora del RD. Posteriormente, no se presentaron enmiendas al Reglamento 5961 para aumentar los derechos a cobrar.

e. El 5 de noviembre de 2015, el RD envió un correo electrónico dirigido a 14 empleados donde se les notificó y se les enviaron los nuevos costos de servicios en oficinas locales.

f. El 6 de noviembre de 2015, el RD envió un correo electrónico a 20 empleados del RD sobre los nuevos Costos de Servicios Comparación – Locales.

Criterio

Las situaciones comentadas son contrarias a las siguientes disposiciones:

La Sección 2.7(a) y la Sección 2.13, de la citada Ley Núm. 170 de 1988, según enmendada, conocida como *Ley de Procedimiento Administrativo Uniforme del Estado Libre Asociado de Puerto Rico*[7], disponen lo siguiente:

> ***Sección 2.7 — Nulidad de las Reglas o Reglamentos y Término para Radicar la Acción. (3 LPRA § 9617)***
>
> ***(a)*** *Una regla o reglamento aprobado después de la fecha de efectividad de esta Ley será nulo si no cumpliera sustancialmente con las disposiciones de esta Ley.*
>
> ***Sección 2.13 — Emergencias que Exigen Vigencia sin Previa Publicación. (3 LPRA § 9623)***
>
> *Las disposiciones de las Secciones 2.1, 2.2, 2.3 y 2.8 de esta ley, (3 L.P.R.A. §§ 2121, 2122, 2123 y 2128) podrán obviarse en todos aquellos casos en que el Gobernador certifique que, debido a una emergencia o a cualquier otra circunstancia que lo exija, los intereses públicos requieren que el reglamento o enmienda al mismo empiece a regir sin la dilación que requieren las Secciones 2.1, 2.2, 2.3 y 2.8 de esta ley (3 L.P.R.A §§ 2121, 2122, 2123 y 2128). En todos estos casos, el reglamento o la enmienda al mismo, junto con la copia de la certificación del Gobernador, serán radicados por el Secretario. Una vez así radicado el reglamento, o la enmienda al mismo, la agencia dará cumplimiento a lo dispuesto en las Secciones 2.1, 2.2 y 2.3 (3 L.P.R.A. §§ 2121, 2122 y 2123), y, de determinar modificaciones o enmiendas al reglamento radicado al amparo de esta sección, radicará las mismas en la oficina del Secretario de Estado, y se le dará cumplimiento a lo dispuesto en la Sección 2.8 de esta ley (3 L.P.R.A. § 2128).*[8]

El Artículo 3-A.[9] de la Ley Núm. 24 de 22 de abril de 1931, según enmendada, conocida como *Ley del Registro General Demográfico de Puerto Rico* (Ley Núm. 24 de 1931), que dispone lo siguiente:

[7] Ley Núm. 170 de 1988, *supra,* fue derogada por la Ley Núm. 38-2017, según enmendada, *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico*, la cual contiene disposiciones análogas.

[8] La Sección 1.3. — Definiciones, establece en el inciso (o) que Secretario significa el Secretario de Estado.

[9] Artículo adicionado por la Ley Núm. 220-1998.

> ***Artículo 3-A. (24 LPRA § 1071a)***
>
> *Se faculta al Secretario de Salud a establecer,* ***mediante reglamentación*** *al efecto, las cantidades a ser pagadas por concepto de cualquier certificado, documento o servicio que ofrece el Registro Demográfico de Puerto Rico, sus subregistros o registros subalternos. . . .* **[énfasis suplido]**

El Artículo 2, incisos (f) y (g), de la Ley Núm. 230 de 23 de julio de 1974, según enmendada, conocida como *Ley de Contabilidad del Gobierno de Puerto Rico* (Ley Núm. 230 de 1974), requiere lo siguiente:

> ***Artículo 2. — Declaración de Política. (3 LPRA § 283a)***
>
> *La política pública del Gobierno de Puerto Rico con relación al control y la contabilidad de los fondos y propiedad públicos será:*
>
> *[. . .]*
>
> ***(f)*** *que exista el control previo de todas las operaciones del gobierno; que dicho control previo se desarrolle dentro de cada dependencia, entidad corporativa o Cuerpo Legislativo para que así sirva de arma efectiva al jefe de la dependencia, entidad corporativa o Cuerpo Legislativo en el desarrollo del programa o programas cuya dirección se le ha encomendado. Tal control interno funcionará en forma independiente del control previo general que se establezca para todas las operaciones de cada rama de gobierno;*
>
> ***(g)*** *que independientemente del control previo general que se establezca para todas las operaciones de cada rama del gobierno, los jefes de dependencia, entidades corporativas y Cuerpos Legislativos sean en primera instancia responsables de la legalidad, corrección, exactitud, necesidad y propiedad de las operaciones fiscales que sean necesarias para llevar a cabo sus respectivos programas.*

Efecto

Las situaciones comentadas tienen el efecto de lo siguiente:

1. Durante el período de julio de 2022 a febrero de 2025 el RD cobró aproximadamente $2,904,445.00 en exceso a los costos aprobados en el Reglamento 5961. Lo anterior surge de las 487,559 certificaciones de eventos vitales que otorgó. Esta cantidad no incluye el período de noviembre de 2015 a junio de 2022 que el RD estuvo cobrando los derechos de la emisión de eventos vitales en exceso a lo permitido por el Reglamento 5961.

2. Incumplimiento con las disposiciones de las leyes citadas.

3. Se pierde la transparencia en las operaciones del RD.

4. Propicia que se cometan irregularidades en los cobros de derechos sobre la emisión de las certificaciones de eventos vitales sin que se puedan detectar a tiempo para fijar responsabilidades.

Causa

Las situaciones comentadas se atribuyen a lo siguiente:

1. Los directores ejecutivos que actuaron en el RD y los secretarios del Departamento en funciones desde el año 2015 hasta el 2024 no realizaron las acciones correspondientes para lograr que se enmendara el Reglamento 5961 conforme con los costos que se estuvieron cobrando durante esos años.

2. Los directores ejecutivos que actuaron en el RD no se aseguraron de que las operaciones relacionadas con los cobros de derechos por concepto de la emisión de eventos vitales estuvieran en armonía con la reglamentación aprobada.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *... Aceptamos los hallazgos identificados en dicho borrador ...*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 1.

Hallazgo 2 – Deficiencias en la expedición de certificados de eventos o registros vitales

Situación

Los registros vitales constituyen documentación oficial de eventos de la vida que se conservan bajo autoridad gubernamental, incluidos los certificados de nacimiento, las licencias de

matrimonio (o certificados de matrimonio), los acuerdos de separación, los certificados de divorcio o los certificados de defunción y de parte divorciada.

El RD cuenta con dos programas que recopilan la información de los eventos vitales para cada individuo: RegDem, donde se encuentran los datos de nacimientos, matrimonios y muertes fetales, y Vita donde se encuentran las defunciones. Ambas plataformas se utilizan para verificar y expedir certificados. El RD cuenta con diferentes alternativas para solicitar los certificados de estos eventos vitales:

1. Registros locales – El RD mantiene 57 registros locales alrededor de todo Puerto Rico, y 2 oficinas en los Estados Unidos, donde el ciudadano puede visitar y solicitar su certificado.

2. Correo postal – El solicitante envía una solicitud por correo postal firmada y completada en todas sus partes. Debe acompañarla con copia de identificación vigente con los aranceles correspondientes.

3. PR.GOV – Se ordena en línea a través del enlace PR.GOV, página oficial del Gobierno de Puerto Rico.

4. Renovaciones Online – Plataforma electrónica por la cual se tramitan los certificados de eventos vitales. El Registro Demográfico recibe y trabaja los documentos mediante la misma plataforma. Completado el proceso, establece la fecha de visita para la entrega de los documentos en la oficina local más cercana a la dirección informada en la solicitud.

5. VitalChek – Plataforma que provee para solicitar los certificados de un evento vital de forma electrónica o telefónica.

El examen del proceso de expedición de los certificados reveló lo siguiente:

a. PR.GOV Certificados en proceso

El examen de las solicitudes de certificados de eventos vitales que permanecen en proceso en la página electrónica PR.GOV reveló lo siguiente:

1. Había 4,987 solicitudes de eventos vitales en proceso al 30 de junio de 2024. De estas, 4,589 solicitudes (92%) tenían estatus en proceso al 30 de junio de 2022. Estas solicitudes debieron haber sido trabajadas o canceladas en 30 días o menos.

2. El RD no cuenta con procedimientos internos para determinar el tiempo que deben permanecer las solicitudes de certificados de eventos vitales en proceso.

b. PR.GOV Cancelaciones

El examen de las solicitudes de certificados de eventos vitales mediante la página electrónica PR.GOV que fueron canceladas reveló lo siguiente:

1. Cancelaron 4,514 solicitudes (91%) después de los 30 días que indicó la supervisora de PR.GOV que es el tiempo establecido para cancelar una solicitud.

2. El RD no cuenta con procedimientos internos para la cancelación de solicitudes de certificados de eventos vitales.

c. PR.GOV

El examen de 750 solicitudes y expediciones de certificados de eventos vitales mediante la página electrónica de PR.GOV reflejó lo siguiente:

1. En 55 solicitudes (7.34%) se excedieron de los 30 días establecidos para la emisión de los certificados.

2. En 12 solicitudes (1.60%) el solicitante pagó una cantidad incorrecta.

3. En 9 solicitudes (1.2%) se emitió un certificado a un solicitante que no es parte interesada.

4. En 7 solicitudes (.93%) el solicitante presentó una identificación expirada.

d. Registros locales y Renovaciones Online

El examen de 252 solicitudes y expediciones de certificados de eventos vitales mediante Renovaciones Online y registros locales reflejó lo siguiente:

1. En 129 solicitudes (51%) no se incluyó el número del sello de rentas internas en el encasillado provisto por el formulario.

2. En 13 solicitudes (5%) no se puede identificar si el solicitante era parte interesada.

3. En 7 solicitudes (3%) no se incluyó en el formulario la fecha o firma del expedidor.

4. En 7 solicitudes (3%) los documentos no fueron entregados debido a que se dañaron, según certificó la directora del RD.

5. En 2 solicitudes (0.79%) la información no concuerda con el sistema RegDem.

6. En una solicitud (0.39%) el número de control en RegDem no concuerda con el número de la solicitud.

e. Correo postal

El examen de 300 solicitudes y expediciones de certificados de eventos vitales mediante correo postal reflejó que en 4 solicitudes (1.33%) los certificados se expidieron en exceso de los 30 días laborables.

Criterio

Las situaciones comentadas en los **apartados a.** y **b.** son contrarias a la Sección 1.2 de la Ley Núm. 38-2017, según enmendada, conocida como *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico*, que dispone lo siguiente:

> ***Sección 1.2. — Política Pública.***
>
> *Las agencias establecerán las reglas y procedimientos que permitan la solución informal de los asuntos sometidos ante su consideración sin menoscabar los derechos garantizados por esta Ley. . .*

Las situaciones comentadas en los **apartados a.1, b.1**, **c.1** y **e.** son contrarias al Procedimiento RD-02-2020, *Para establecer administrativamente los requisitos e instrucciones para solicitar una certificación de un evento vital mediante el correo postal*, firmado el 26 de febrero de 2020, por la directora ejecutiva del RD, donde establece lo siguiente:

- *El tiempo aproximado de procesamiento de una solicitud es de **15 a 30 días laborales**. . .* **[énfasis en el procedimiento]**

Las situaciones comentadas en los **apartados c.3** y **d.2** son contrarias al Artículo 2, inciso (12), de la citada Ley Núm. 24 de 1931, que dispone lo siguiente:

> ***Artículo 2.***
>
> *Cuando en esta Ley se use:*
>
> ***(12) Parte interesada. —** Significará el inscrito, si es de dieciocho (18) años o mayor, su padre, su madre, su representante legal, custodio legal o tutor, o los herederos del inscrito. Será, además, cualquier menor que a su vez sea padre o madre de un menor para lo cual se autoriza la expedición de actas relacionadas tanto para su persona como para su hijo(a). "Parte interesada" será además la señalada mediante orden del Tribunal.*

Las situaciones comentadas en los **apartados c.4, d.1, d.3, d.5 y d.6** son contrarias a las siguientes disposiciones:

El Artículo 2(f) de la Ley Núm. 230 de 1974, el cual dispone lo siguiente:

> ***Artículo 2. — Declaración de Política.***
>
> *La política pública del Gobierno de Puerto Rico con relación al control y la contabilidad de los fondos y propiedad públicos será:*
>
> *[. . .]*

> ***(f)*** *que exista el control previo de todas las operaciones del gobierno; que dicho control previo se desarrolle dentro de cada dependencia, entidad corporativa o Cuerpo Legislativo para que así sirva de arma efectiva al jefe de la dependencia, entidad corporativa o Cuerpo Legislativo en el desarrollo del programa o programas cuya dirección se le ha encomendado. Tal control interno funcionará en forma independiente del control previo general que se establezca para todas las operaciones de cada rama de gobierno. . ..*

De acuerdo con dicha política pública y como medida de sana administración el RD debe establecer controles internos que impidan y dificulten que se cometan irregularidades. Entre estos, los formularios de las solicitudes de certificados de eventos vitales deben completarse en todas sus partes. Además, deben estar firmados por los empleados y funcionarios autorizados. Esto con el propósito de poder identificar fácilmente a los empleados que participan en estos procesos y poder fijar responsabilidades, de surgir alguna irregularidad.

La Carta Circular Núm. 2-17 (RD), *Para establecer Administrativamente el Procedimiento Uniforme para la Expedición de Certificados de Eventos Vitales*, emitida el 30 de junio de 2017, por la directora ejecutiva del RD. Este procedimiento establece que sus directrices *tienen que ser observadas al pie de la letra por todo el personal que labore o haga algún trabajo de expedición para el Registro Demográfico*.

La situación comentada en el **apartado d.4** es contraria al Artículo VIII-D del Reglamento 23, conocido como *Para la Conservación de Documentos de Naturaleza Fiscal o Necesarios para el Examen y Comprobación de Cuentas y Operaciones Fiscales*, según enmendado, aprobado el 15 de agosto de 1988, por el secretario de Hacienda, que establece lo siguiente:

> *Artículo VIII – <u>Disposiciones Generales</u>*
>
> *D – Los documentos fiscales deben conservarse, clasificarse y archivarse en forma tal que se puedan localizar, identificar y poner a la disposición del Contralor de Puerto Rico y del Secretario de Hacienda, o de cualquier otro funcionario autorizado por ley, con prontitud y en la forma deseada.*

Efecto

Las situaciones comentadas tienen el efecto de lo siguiente:

1. Impiden verificar y determinar la validez y corrección de las transacciones presentadas en los documentos fiscales solicitados.

2. Demuestra la ausencia de controles en la administración de los documentos relacionados con la expedición de certificados de eventos vitales.

3. Propicia la falta de transparencia y confianza en relación con los procesos que el RD realiza para la expedición de certificados. Estos documentos son de naturaleza legal y fiscal, y pueden ser requeridos ante los distintos foros gubernamentales y de justicia con los consiguientes efectos adversos para el RD al no tenerlos disponibles.

4. Limita el alcance del examen.

5. Propicia que se cometan errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades.

Causa

Las situaciones comentadas se atribuyen a lo siguiente:

1. Falta de un procedimiento escrito de cancelación que establezca, entre otras cosas, que todo trámite en proceso debe ser atendido en o antes de 30 días, de lo contrario cancelarlo al día siguiente del término de 30 días.

2. Falta de supervisión efectiva de los empleados para que se aseguren que las solicitudes se completen en todas sus partes, correctamente y de acuerdo con los requisitos.

3. Las situaciones comentadas son indicativas de que los servidores públicos a cargo de la expedición de certificados de eventos vitales se apartaron de los procesos establecidos y requeridos en el Reglamento 23. Además, son indicativas de que los servidores públicos que actuaron como directores del RD no ejercieron una supervisión eficaz para asegurarse del cumplimiento de dichos requerimientos.

4. El RD no tomó las medidas necesarias ni utilizó la tecnología disponible para salvaguardar la información y los documentos. Además, los directores del RD en funciones no cumplieron con sus responsabilidades y se apartaron de las disposiciones del Reglamento mencionado.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *... Aceptamos los hallazgos identificados en dicho borrador ...*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *... Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro*

Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 2.

Hallazgo 3 – Fallas relacionadas con los controles de acceso al sistema del RD que administra los registros de los eventos vitales

Situación

a. Toda entidad gubernamental, independientemente de su tamaño, tiene que implementar controles rígidos de acceso a la información y a las aplicaciones que se limite únicamente el personal autorizado. Como parte de estos controles, las entidades gubernamentales deben mantener toda la documentación necesaria para la otorgación de accesos o privilegios a los sistemas de información computadorizados.

   El Sistema RegDem es utilizado por los empleados, el personal contratado (usuarios internos) del RD y por representantes autorizados de las entidades gubernamentales y entidades del sector privado (usuarios externos) que solicitan acceso para consultar asuntos relacionados con los eventos vitales.

   El RD utiliza la *Certificación de Acuerdo de Confidencialidad y No Divulgación* para documentar las solicitudes de acceso y creación a los usuarios internos y externos al RegDem. Para la creación de las cuentas de acceso tienen que completar en todas sus partes los siguientes formularios:

   1. *Solicitud de Creación, Modificación, Reactivación o Cancelación de Acceso al Sistema Electrónico del Registro Demográfico de Puerto Rico* (RegDem).

   2. *Solicitud de Acceso a Sistemas de Información del Departamento de Salud – OIAT*.

   Estos formularios luego de ser procesados por la Oficina de Informática y Avances Tecnológicos (OIAT) del Departamento se mantienen archivados en las oficinas administrativas del RD.

   El sistema RegDem tenía 233 usuarios para el período de examen según la información provista por el RD. Sin embargo, al evaluar los formularios de los Acuerdos de Confidencialidad se observaron 304 adicionales que no fueron sometidos por el RD, para un total de 537 usuarios internos y externos activos para el período de examen.

Se realizó un examen a los Acuerdos de Confidencialidad de los 537 usuarios activos para los años 2022 al 2024. El examen reveló que el RD no tenía los *Acuerdos de Confidencialidad y No Divulgación* de los siguientes usuarios que les aplicaba:

1. Para el año 2023, 34 de 309 usuarios (11%) no tenían el acuerdo.

2. Para el año 2024, 20 de 378 usuarios (5%) no tenían el acuerdo.

3. Para el año 2022, 13 de 431 usuarios (3%) no tenían el acuerdo.

b. Las entidades gubernamentales que otorgan y comparten privilegios de accesos a los sistemas de información computadorizados mediante formularios provistos para ello, deben completarse en todas sus partes para mantener unos controles adecuados.

   El examen a los Acuerdos de Confidencialidad mencionados en el **apartado a.** reveló fallas en la cumplimentación de la información solicitada en ellos, según se indica:

   1. Entre los 418 usuarios que en el año 2022 completaron el acuerdo de confidencialidad, 69 (17%) no incluyeron la fecha de la firma del representante o supervisor, 57 (14%) no incluyeron su nombre, 28 (7%) no incluyeron el nombre del representante o supervisor, 18 (4%) no incluyeron su firma, 8 (2%) no incluyeron la firma del representante o supervisor, y 2 (0.5%) no incluyeron la fecha cuando firmaron el formulario.

   2. Entre los 275 usuarios que en el año 2023 completaron el acuerdo de confidencialidad, 22 (8%) no incluyeron su nombre, 15 (5%) no incluyeron su firma, 12 (4%) no incluyeron la fecha de la firma del representante o supervisor, 3 (1%) no incluyeron la fecha en que el usuario firmó el formulario, 2 (1%) no incluyeron el nombre del representante o supervisor, y 1 (0.4%) no incluyó la firma del representante o supervisor.

   3. Entre los 358 usuarios que en el año 2024 completaron el acuerdo de confidencialidad, 44 (12%) no incluyeron la fecha de la firma del representante o supervisor, 9 (3%) no incluyeron el nombre del representante o supervisor, 9 (3%) no incluyeron la firma del representante o supervisor, 7 (2%) no incluyeron la fecha cuando firmaron el formulario, 6 (2%) no incluyeron su nombre, y 3 (0.8%) no incluyeron su firma.

c. Todo organismo gubernamental que comparte información con entidades del gobierno estatal, federal o privadas debe establecer acuerdos por escrito para asegurarse que estas conozcan cuán sensitiva es la información y la responsabilidad que tienen de protegerla.

   Existían 23 acuerdos de colaboración firmados por el Departamento que otorgaban acceso a los registros de los eventos vitales del RD (acuerdos de colaboración). Los acuerdos, firmados entre el 13 de septiembre de 2019 al 1 de enero de 2024, incluían cláusulas del período de vigencia y requerían un compromiso para garantizar la confidencialidad de la información.

Las entidades podían acceder a los registros de los eventos vitales mediante el uso de cuentas de acceso remoto otorgado por el personal de la OIAT. El examen a los acuerdos de colaboración reveló que había 7 acuerdos con los períodos de vigencia expirados. Sin embargo, los usuarios de estos acuerdos continuaban activos según la información provista por el RD.[10]

Tabla 2: Acuerdos Colaborativos

#	Entidad	Acuerdos de Colaboración	Fecha de Vigencia
1.	A	Original	13 sep. 2019 al 30 jun. 2024
2.	B	Original Enmienda A	15 oct. 2019 al 30 jun. 2024 1 jul. 2022 al 30 jun. 2024
3.	C	Original Enmienda A Enmienda B	12 ago. 2020 al 30 jun. 2022 30 jun. 2022 al 30 jun. 2024 26 jul. 2022 al 30 jun. 2024
4.	D	Original	18 dic. 2020 al 30 jun. 2024
5.	E	Original	25 ene. 2021 al 30 jun. 2024
6.	F	Original Enmienda A	24 ago. 2021 al 31 dic. 2023 20 feb. 2023 al 31 dic. 2023
7.	G	Original	1 jul. 2023 al 30 jun. 2024

Criterio

Las situaciones comentadas en los **apartados a.** y **b.** son contrarias a las siguientes disposiciones:

El Procedimiento RDS2, *Procedimiento para creación, modificación, reactivación o cancelación de acceso al sistema del Registro Demográfico (RegDem)*, revisado en septiembre de 2019, que establece lo siguiente:

> *Toda solicitud de creación o cancelación de acceso al Sistema de Portal del Registro Demográfico debe de ser iniciada por el/la Enlace de Recursos Humanos, en ausencia de éste(a), puede iniciarla el/la supervisor(a) del empleado(a) que se le completa el documento. Toda creación, modificación o reactivación solicitud debe de estar acompañada por* ***los siguientes documentos completados y firmados: Acuerdo de Confidencialidad del Registro Demográfico****, Solicitud de Acceso a Sistemas de Información del Departamento de Salud – OIAT (SEG_DoH_FT_001) y Solicitud de Acceso en Aplicación al Portal (RDS1). Cabe señalar, que el Acuerdo de Confidencialidad del Registro Demográfico y Solicitud*

[10] El número de los 7 acuerdos colaborativos se le proveyó al Departamento con los nombres de las entidades correspondientes.

de Acceso a Sistemas de Información del Departamento de Salud – OIAT (SEG_DoH_FT_001) se continuarán completando anualmente. **[énfasis añadido]**

La Sección E, inciso 3, de la Política Núm. ATI-003, *Seguridad de los Sistemas de Información*, de la Carta Circular 140-16 de la Oficina de Gerencia y Presupuesto (OGP) revisada el 7 de noviembre de 2016, que establece lo siguiente:

E. Controles Generales

3. La información y los programas de aplicación en las operaciones de la agencia deberán tener controles de acceso para su utilización de tal manera que solamente el personal autorizado pueda ver los datos o acceder a las aplicaciones (o la parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.

La Política TI-PRITS-007, *Política de gestión de acceso, identidad y credenciales*, aprobada el 24 de enero de 2024 por la *Puerto Rico Innovation and Technology Service* (PRITS), que en la Sección 7, incisos 7.1, y 7.1.1 al 7.1.5, establece lo siguiente:

7. Procesos Requeridos

7.1 Control de Acceso

El acceso a información se basará en el principio de la "necesidad de conocer" y el privilegio mínimo. Los usuarios tendrán el nivel mínimo requerido para sus funciones gubernamentales legítimas luego de obtener las autorizaciones correspondientes.

7.1.1 Los controles de acceso se implementarán cuando el propietario de un recurso tecnológico (por ejemplo, sistemas, aplicaciones, datos) requiera restringir el acceso a un grupo limitado de usuarios o asignar diferentes niveles de acceso. Recursos ampliamente disponibles (por ejemplo, acceso a Internet, software de oficina, etc.) podrán no necesitar controles de acceso.

7.1.2 Los derechos de acceso se otorgarán a los usuarios en roles y responsabilidades. Si estas cambian, se modificarán los accesos de forma inmediata y prioritaria.

7.1.3 El acceso a datos confidenciales deberá ser documentado adecuadamente.

7.1.4 Los controles de acceso podrán utilizarse para separar funciones y limitar el nivel de acceso y acciones de un usuario.

7.1.5 Los controles de acceso podrán ser proporcionados por el sistema operativo, integrados al recurso o en una solución de un proveedor de servicios.

El Capítulo 3.2 del *Federal Information System Controls Audit Manual* (FISCAM), promulgado en febrero de 2009 (GAO-09-232G) por la *U.S. Government Accountability Office* (GAO)[11], que establece lo siguiente:

3.2 Access Controls (AC)

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical controls. Logical access controls require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they can execute. …

La situación comentada en el **apartado c.** es contraria a la *Cláusula Ultravires* incluida en los Acuerdos de Colaboración, que establece lo siguiente:

Conforme a derecho y las normas que rigen la contratación de servicios, los comparecientes en este acuerdo toman conocimiento de que no se prestara servicio alguno bajo este acuerdo hasta tanto sea firmado por ambas partes. ***De la misma forma, no se continuará dando servicios bajo este acuerdo a partir de su fecha de expiración, excepto que a la fecha de expiración exista ya una enmienda firmada por ambas partes.*** **[énfasis añadido]**

Efecto

Las situaciones comentadas en los **apartados a. y b.** imposibilitan al RD mantener la certeza requerida de las autorizaciones para otorgar los accesos y los privilegios a los usuarios del sistema RegDem, y del compromiso de estos para mantener la confidencialidad de la información de los eventos vitales.

La situación comentada en el **apartado c.** despoja al RD de aquellas herramientas que son necesarias para mantener la protección y asegurar la confidencialidad de los registros de los eventos vitales, exponiéndolos a controversia en caso de que la información se divulgue o se utilice para propósitos distintos a los autorizados. Además, se debió al incumplimiento con el acuerdo firmado.

[11] El FISCAM fue revisado en septiembre de 2024 (GAO-24-107026) y sustituyó la revisión realizada en el año 2009. El FISCAM revisado en el año 2024 contiene recomendaciones similares a las del año 2009.

Estas situaciones exponen al RD a riesgos legales, de privacidad, reputación, y al uso no autorizado de los datos.

Causa

Las situaciones comentadas en los **apartados a. y b.** se debieron a que los administradores del sistema RegDem, no verificaron que los usuarios internos y externos tuvieran un Acuerdo de Confidencialidad y completado en todas sus partes.

La situación comentada en el **apartado c.** se debió a que el RD no adoptó controles internos para la supervisión y la verificación, en coordinación con el Departamento, de la vigencia y todos los asuntos que envuelve la administración de los acuerdos de colaboración firmados. Esto es esencial para la protección y la seguridad de mantener la confidencialidad de los registros de los eventos vitales.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico una carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . . .*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 3.

Hallazgo 4 – Acuerdos Colaborativos y enmiendas no radicados o radicados con tardanza en el Registro de Contratos de la Oficina del Contralor de Puerto Rico

Situación

Toda entidad gubernamental debe registrar y remitir a la Oficina del Contralor de Puerto Rico (OCPR) copias de los contratos y las enmiendas a estos, dentro de los 15 días siguientes a la fecha

de su otorgamiento. Esto, porque ninguna prestación[12] o contraprestación[13] objeto de un contrato, podrá exigirse hasta que este se haya registrado y remitido a la OCPR, según dispone la Ley Núm. 18 de 30 de octubre de 1975, según enmendada, y en el Reglamento 9239, *Reglamento 33, Registro de Contratos de la Oficina del Contralor del Estado Libre Asociado de Puerto Rico*, aprobado el 9 de diciembre de 2020 por el Departamento de Estado.

El Departamento, por medio de la directora de la Oficina de Contratos, se encarga de registrar y remitir a la OCPR los contratos y las enmiendas debidamente formalizados para el RD. Según la información suministrada por el RD, del 13 de septiembre de 2019 al 1 de enero de 2024, se otorgaron 23 acuerdos colaborativos y 6 enmiendas.

El examen realizado a los 23 acuerdos colaborativos y a las 6 enmiendas que el Departamento formalizó para servicios con el RD reveló las siguientes deficiencias:[14]

a. El acuerdo colaborativo A y su enmienda A con la Entidad 1 no aparecían registrados en el Registro de Contratos de la OCPR. Tampoco indicaban que ninguna prestación o contraprestación objeto de estos acuerdos podría exigirse hasta que se haya presentado para su registro en la OCPR. Al acuerdo colaborativo A le faltaba la firma del entonces secretario del Departamento y no tenía número de contrato ni fecha. Además, estipula que estará vigente hasta el 30 de junio de 2028. La enmienda A está firmada por ambas partes el 15 de julio de 2023.

b. El acuerdo colaborativo B con la Entidad 2 fue registrado en el Registro de Contratos de la OCPR 28 días consecutivos después de su formalización.

c. La enmienda A del acuerdo colaborativo C con la Entidad 3 fue registrada en el Registro de Contratos de la OCPR 32 días consecutivos después de su formalización.

d. El acuerdo colaborativo D con la Entidad 4 fue registrado en el Registro de Contratos de la OCPR 20 días consecutivos después de su formalización.

e. La enmienda B del acuerdo colaborativo E con la Entidad 5 fue registrada en el Registro de Contratos de la OCPR 16 días consecutivos después de su formalización.

f. El acuerdo colaborativo F con la Entidad 6 fue registrado en el Registro de Contratos de la OCPR 16 días consecutivos después de su formalización.

Criterio

Las situaciones comentadas son contrarias a las siguientes disposiciones:

[12] Prestación – Es la obligación o compromiso que una parte asume en el contrato. Puede ser dar algo (como un bien), hacer algo (como un servicio) o incluso no hacer algo (una abstención).

[13] Contraprestación – Es lo que recibe a cambio la otra parte por esa prestación. Es la "recompensa" o beneficio que justifica el acuerdo.

[14] El número de los acuerdos colaborativos con deficiencias se le proveyó al Departamento con los nombres de las entidades correspondientes.

El Artículo 1, incisos (a) y (e), de la Ley Núm. 18 de 30 de octubre de 1975 (Ley Núm. 18 de 1975), según enmendada, conocida como *Ley de Registros de Contratos,* que disponen lo siguiente:

> ***Artículo 1. — Copias de contratos, escritos y documentos.***
>
> ***(a)*** *Las entidades gubernamentales y las entidades municipales del Estado Libre Asociado de Puerto Rico, sin excepción alguna, mantendrán un registro de todos los contratos que otorguen, incluyendo enmiendas a los mismos, y deberán remitir copia de éstos a la Oficina del Contralor dentro de los quince (15) días siguientes a la fecha de otorgamiento del contrato o la enmienda. …*
>
> ***(e)*** *En todo contrato sujeto a registro conforme el Artículo 1 de esta Ley se consignará en forma clara y conspicua un aviso que leerá como sigue:* ***"Ninguna prestación o contraprestación objeto de este contrato podrá exigirse hasta tanto el mismo se haya presentado para registro en la Oficina del Contralor a tenor con lo dispuesto en la Ley Núm. 18 de 30 de octubre de 1975, según enmendada"****.* **[énfasis en la ley]**

El Artículo 8, inciso 8.2, y los Artículos 9 y 15, del Reglamento 9239[15], *Reglamento 33 Registro de Contratos de la Oficina del Contralor del Estado Libre Asociado de Puerto Rico*, aprobado el 9 de diciembre de 2020 por el Departamento de Estado, que establecen lo siguiente:

> ***Artículo 8. Registro de Contratos***
>
> *8.2 Documentos a Registrar y Remitir*
>
> *Todo contrato, sin excepción alguna, y toda enmienda, acuerdo, determinación, constancia o acción que los rescinda, tiene que registrarse en el Registro de Contratos de la entidad. Esto incluye los contratos exentos de remitirse a la Oficina enumerados en este Reglamento.*
>
> *El Registro de Contratos debe ser un reflejo del Registro de Contratos de la entidad. Las entidades remiten copia fiel y exacta de todos los contratos, en los cuales tienen que aparecer las firmas de las partes. Los contratos que se otorguen deben estar redactados en su totalidad en un programa de procesador de texto, salvo en situaciones extraordinarias que la Contralora determine. Además, el contrato a remitir tiene que estar digitalizado en formato PDF con OCR.*
>
> ***Artículo 9. Término para Registro y Remisión de los Contratos***

[15] El Reglamento 9239 fue derogado por el Reglamento 9571 aprobado por el Departamento de Estado el 3 de julio de 2024, el cual contine disposiciones similares.

> *El registro* y *la remisión se realiza dentro de los 15 días consecutivos*, siguientes a la *fecha de otorgamiento del contrato o la enmienda, ...*

Artículo 15. Contratos Interagenciales[16]

> *La entidad responsable de realizar un desembolso de fondos está obligada a registrar y remitir el contrato a la Oficina. Si el contrato no conlleva un desembolso de fondos, es responsabilidad de quien comparece como primera parte en el contrato registrarlo en el Registro de Contratos, conforme se dispone en este Reglamento. Ambas entidades deben registrar el contrato en el registro interno de su entidad. . .*

Efecto

La situación comentada tiene como efecto lo siguiente:

1. Imposibilita que estos acuerdos y enmiendas estuvieran disponibles a la ciudadanía en calidad de documentos públicos.

2. Incumplimiento con la citada Ley Núm. 18 de 1975.

Causa

Las situaciones comentadas se atribuyen a que el secretario del Departamento y la directora ejecutiva del RD no velaron el cumplimiento con la ley y el reglamento mencionado.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . . .*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

[16] Según definido en el Artículo 4 del Reglamento 9239 se refieren a contratos entre entidades donde consienten en dar alguna cosa o proveer algún servicio relacionado con fondos o propiedad pública.

Ver la Recomendación 4.

Hallazgo 5 – Reglamentos y procedimientos sin actualizar

Situación

La reglamentación y los procedimientos son importantes para lograr una administración exitosa, enmarcada en una estructura de control interno, garantizar la consistencia, la uniformidad y la calidad de las operaciones de la entidad y fijar las responsabilidades para cada área de trabajo. De esta manera, cada servidor público puede conocer de antemano cómo es el proceso del cual es responsable, su participación, y la acción a tomar o seguir, entre otros aspectos.

a. El examen realizado a la reglamentación que rige las operaciones del RD en cuanto al control y manejo de los asuntos relacionados con los Registros Vitales[17], reveló que no se habían revisado los siguientes reglamentos con una vigencia mayor de 5 años:

    1. El Reglamento Núm. 318, *Reglamento para los Registros Demográficos*, aprobado por el Departamento de Estado el 19 de septiembre de 1957. Este Reglamento no había sido actualizado y conformado a los cambios en la legislación y administración del RD. Esto a pesar de haber transcurrido 67 años luego de la fecha de su aprobación.

    2. El Reglamento Núm. 5961, *Reglamento del Procedimiento para el Cobro de los Derechos del Registro Demográfico Correspondientes a la Expedición de Certificados de Nacimiento, Matrimonio, Defunción y Natimuerto, y Además de Otros Servicios*, aprobado por el Departamento de Estado el 7 de mayo de 1999. Esto a pesar de haber transcurrido 25 años luego de la fecha de su aprobación.

b. El examen reflejó que los siguientes procedimientos del RD tiene más de 5 años de aprobado:

Tabla 3: Procedimientos no actualizados

Núm. del procedimiento	Título del Procedimiento	Fecha de aprobación	Años de aprobado
2017	*Procedimiento para llevar a cabo una corrección administrativa de un evento vital*	1 jun. 2017	7
1-2018	*Celebrantes de matrimonios*	1 oct. 2018	6
02-2018	*Procedimiento para realizar correcciones administrativas desde una oficina local*	1 oct. 2018	6
03-2018	*Procedimiento para la expedición de la certificación de muerte fetal por medio del sistema del Registro Demográfico*	1 oct. 2018	6

[17] Significará certificados o informes de nacimientos, defunciones, casamientos, divorcios, disolución o anulación de casamientos e informes relacionados con ellos.

Núm. del procedimiento	Título del Procedimiento	Fecha de aprobación	Años de aprobado
04-2018	*Procedimiento para reportar problemas con las expediciones realizadas en el sistema*	9 oct. 2018	6
05-2018	*Procedimiento para solicitar servicios a la división de libros en Bayamón*	9 oct. 2018	6
06-2018	*Procedimiento para documentar en sistema, las orientaciones y otros asuntos concernientes a los eventos vitales custodiados por el Registro Demográfico*	9 oct. 2018	6
07-2018	*Procedimiento para atender las inscripciones de infantes por padres menores de edad*	9 oct. 2018	6
08-2018	*Procedimiento para marcar las expediciones del sistema en papel en blanco*	26 dic. 2018	6
09-2018	*Procedimiento para la anotación en sistema de los números de formas de seguridad dejadas en blanco*	26 dic. 2018	6
10-2018 Enmendado	*Procedimiento para documentar las formas de seguridad "NULA"*	28 may. 2019	5
RDS2 *Rev. Sept. 2019*	*Procedimiento para creación, modificación, reactivación o cancelación de acceso al sistema del Registro Demográfico*	sep. 2019	5

Criterio

La situación comentada en el **apartado a.** es contraria a las siguientes disposiciones:

El Artículo 3 de la citada Ley Núm. 24 de 1931, según enmendada, conocida como *Ley del Registro General Demográfico de Puerto Rico* que dispone, entre otras cosas, lo siguiente:

> ***Artículo 3.***
>
> *El Secretario de Salud cuidará de que esta Ley sea observada y aplicada uniformemente en todo el Estado Libre Asociado de Puerto Rico, incluyendo las islas adyacentes de Culebra y Vieques; recomendará de tiempo en tiempo la legislación adicional que sea necesaria a este propósito y dictará aquellas reglas y reglamentos que no estén en conflicto con las disposiciones de esta Ley y que sean necesarios para complementar las disposiciones de la misma. Dichos reglamentos luego de aprobados y promulgados por el Gobernador de Puerto Rico tomarán fuerza de ley.*

La Sección 2.19 de la Ley Núm. 38-2017, según enmendada, conocida como *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico,* que dispone lo siguiente*:*

> ***Sección 2.19. — Deber de Revisión Periódica de Reglamentos.***

Será deber de todas las agencias revisar cada cinco (5) años sus reglamentos para evaluar si los mismos efectivamente adelantan la política pública de la agencia o de la legislación bajo el cual fue aprobado el reglamento.

La situación comentada en el **apartado b.** es contraria a las siguientes disposiciones:

El Artículo 178 de la *Ley del Código Político de Puerto Rico de 1902*, según enmendado, dispone lo siguiente:

Artículo 178. — [Reglamentos de los departamentos]

Será atribución de cada jefe de departamento bajo el Gobierno Estatal, dictar reglamentos compatibles con la ley para el régimen interior de su departamento y gobierno de sus funcionarios y empleados, la distribución y despacho de sus asuntos y conservación de sus archivos, papeles y demás pertenencias.

El Artículo 2, inciso (f), de la citada Ley Núm. 230 de 1974, que dispone lo siguiente:

Artículo 2. — Declaración de Política.

La política pública del Gobierno de Puerto Rico con relación al control y la contabilidad de los fondos y propiedad públicos será:

(f) *que exista el control previo de todas las operaciones del gobierno; que dicho control previo se desarrolle dentro de cada dependencia, entidad corporativa o Cuerpo Legislativo para que así sirva de arma efectiva al jefe de la dependencia, entidad corporativa o Cuerpo Legislativo en el desarrollo del programa o programas cuya dirección se le ha encomendado. Tal control interno funcionará en forma independiente del control previo general que se establezca para todas las operaciones de cada rama del gobierno;*

Cónsono con dicha política pública y para un control interno efectivo, el Departamento debe establecer formalmente la frecuencia con la que revisará y aprobará lo procedimientos internos del RD. Este período debe ser razonable y tener en cuenta la naturaleza de las actividades del RD, así como la rapidez con la que evolucionan los factores externos que podrían afectar los procedimientos.

Efecto

Las situaciones comentadas tienen el efecto de lo siguiente:

1. Impide a los empleados[18] y funcionarios[19] del RD y a la ciudadanía, de contar con reglamentación y procedimientos actualizados de acuerdo con los cambios en la legislación y en los procesos administrativos del RD.

2. Dificulta adjudicar responsabilidad, de forma oportuna, en caso de que ocurran errores o irregularidades en las operaciones.

Causa

Las situaciones comentadas se atribuyen a que los directores ejecutivos que actuaron en el RD y los secretarios del Departamento en funciones no realizaron las acciones afirmativas para mantener actualizada la reglamentación y los procedimientos conforme con los cambios administrativos, operacionales y organizacionales.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 5.

Hallazgo 6 – Fallas relacionadas con el diagrama esquemático de la red de comunicaciones

Situación

Un diagrama esquemático de la red de comunicaciones es una representación gráfica que muestra cómo están interconectados los diferentes componentes o dispositivos dentro de una red de

[18] Son aquellas personas que ocupan cargos o empleos en el Gobierno de Puerto Rico que no están investidos de parte de la soberanía del Estado y comprende los empleados públicos regulares e irregulares, los que prestan servicios por contrato que equivalen a un puesto o cargo regular, los de nombramiento transitorio y los que se encuentran en período probatorio.

[19] Son aquellas personas que ocupan cargos o empleos en el Gobierno de Puerto Rico que están investidos de parte de la soberanía del Estado, por lo que intervienen en la formulación e implantación de la política pública.

comunicaciones. En estos diagramas, se utilizan símbolos y líneas para ilustrar los elementos clave de la red, como *routers*, *switches*, servidores, estaciones de trabajo, enlaces de comunicación y otros equipos.

El objetivo de un diagrama esquemático es proporcionar una visión clara y simplificada de la infraestructura de la red, ayudando a entender cómo fluye la información entre los dispositivos y la organización de los recursos dentro de la red.

Estos diagramas no necesariamente muestran detalles precisos de la configuración, sino que se enfocan en mostrar las conexiones principales y la topología general de la red. Se utilizan comúnmente en la planificación, diseño, administración y resolución de problemas en redes de comunicaciones.

Las operaciones del RD Central se realizan desde San Juan que se componen por la dirección ejecutiva, administración y operaciones (estadísticas vitales y bases de datos) y procesos de registración de eventos vitales. El RD cuenta con 57 registros locales establecidos alrededor de Puerto Rico y 2 oficinas en los Estados Unidos.

La OIAT del Departamento presentó el Diagrama Esquemático de su Red de Comunicaciones. El examen del diagrama reveló lo siguiente:

a. El diagrama es una visión general de alto nivel que solo presenta una interconexión, en términos generales, de dos conexiones a la Internet y una interconexión a una de dos oficinas remotas, mediante una red multiservicios IP/MPSL[20] (*Multiprotocol Label Switching*).

b. El diagrama no presenta su última revisión, por lo que no estaba actualizado con los cambios en la infraestructura que se habían realizado.

c. No incluye la interconexión de los equipos (servidores, switches[21], firewall, entre otros) del Departamento y el RD y sus localidades, donde muestre el rango de las conexiones activas para identificar los puntos de acceso a los recursos de la red.

d. Al no incluir las interconexiones no presenta la descripción del equipo y su configuración básica (modelo, nombre, *IP Address*) y el sistema operativo de las computadoras conectadas a la red.

[20] Red de multiservicios de última generación, que permite incrementar en línea el ancho de banda, de acuerdo con las necesidades del Departamento.

[21] Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN, en inglés) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3).

Es fundamental que las rutas de acceso se identifiquen y documenten en un diagrama de ruta de acceso o un diagrama de red similar esquemático. Estos diagramas o esquemas identifican a los usuarios y el tipo de dispositivo desde el que pueden acceder al sistema.

Criterio

La situación comentada es contraria a la Sección 9, incisos 9.1 y 9.1.4, de la Política TI-PRITS-005, *Política sobre las Mejores Prácticas de Infraestructura Tecnológica*, incluida en la Carta Circular Núm. 2023-004 de PRITS, conocida como *Normas Generales que deben seguir las agencias al establecer sus controles y procedimientos, de manera que se atiendan adecuadamente los recursos, las adquisiciones e implementación de soluciones o tecnología nueva, así coma el uso y manejo de los sistemas de información y el manejo de cambios en los proyectos de tecnología*, del 30 de junio de 2023, que establecen lo siguiente:

> ***9. RED***
>
> *Al establecer una política del componente de Red se pretende que las agencias*[22] *adquieran e implementen una infraestructura de red segura, escalable, basada en estándares de dominio en la industria, la cual provee la comunicación necesaria para la distribución de servicios eficientemente.*
>
> *9.1* ***Política para el Componente de Red***
>
> *9.1.4 El diseño de la red debe estar documentado.*

Efecto

La situación comentada impide al Departamento y al RD de lo siguiente:

1. Obtener una comprensión clara de los componentes de la red para mantener un control eficiente y efectivo al administrar y efectuar su mantenimiento.

2. Atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

3. Visualizar todas las conexiones que componen la red del Departamento y del RD y otras agencias adscritas.

4. Identificar las áreas de mejora, como la resolución de errores, la optimización de las estructuras de red y la garantía de que la red cumple con los requisitos de seguridad.

5. Mantener la tecnología al día con la evolución y desarrollo del Departamento y del RD.

[22] Agencia – Significa cualquier junta, cuerpo, tribunal examinador, corporación pública, comisión, oficina independiente, división, administración, negociado, departamento, autoridad, funcionario, persona, entidad o cualquier instrumentalidad del Gobierno de Puerto Rico, según se dispone en la Sección 1.3, inciso (a) de la Ley Núm. 38-2017, según enmendada, *Ley de Procedimiento Administrativo Uniforme del Gobierno de Puerto Rico*.

6. Visualizar toda la arquitectura de la red, por lo que no se podrá planificar, organizar y controlar eficazmente la estructura del sistema.

7. Identificar las dependencias con posibles obstáculos para implementar las medidas correctivas y preventivas.

8. Identificar mejoras para garantizar que el sistema funcione correctamente.

9. Alinear equipos multifuncionales.

Causa

La situación comentada se atribuye al incumplimiento con las directrices impartidas por PRITS en su Carta Circular Núm. 2023-004, *Normas Generales que deben seguir las agencias al establecer sus controles y procedimientos, de manera que se atiendan adecuadamente los recursos, las adquisiciones e implementación de soluciones o tecnología nueva, así coma el uso y manejo de los sistemas de información y el manejo de cambios en los proyectos de tecnología***,** del 30 de junio de 2023.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *... Aceptamos los hallazgos identificados en dicho borrador ...*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *... Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos…*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 6.

Hallazgo 7 – Falta de un Plan Estratégico de Tecnología de Información

Situación

La planificación estratégica de Tecnología de Información y Comunicaciones o un Plan Estratégico de Tecnología de la Información (TI) es un documento que define la manera en que una organización utilizará la tecnología para alcanzar sus objetivos. Este plan establece las

acciones necesarias para alinear los recursos tecnológicos con la visión y misión de la empresa, mejorando su eficiencia, competitividad e innovación. Incluye aspectos como la infraestructura tecnológica, la seguridad de los sistemas, la capacitación del personal y la gestión de proyectos tecnológicos, entre otros. En resumen, es una hoja de ruta para el uso efectivo y estratégico de la tecnología en la organización.

En términos generales, un Plan Estratégico de Tecnología de Información es una herramienta para establecer los esfuerzos de incorporación de la TI. Establece las políticas para controlar la adquisición, el uso y la administración de los recursos de TI. Integra la perspectiva de entidad/organización con el enfoque de TI, estableciendo un desarrollo informático que responda a las necesidades de la entidad y contribuye al complimiento de los objetivos. Su desarrollo está relacionado con la creación de un plan de transformación, que va del estado actual en que se encuentra la entidad, a su estado final esperado de automatización, esto, en concordancia con el plan estratégico de la entidad.

De la misma manera, la Planificación Estratégica se utiliza para establecer prioridades, enfocar la energía y los recursos, fortalecer las operaciones, garantizar que los empleados y otras partes interesadas estén trabajando hacia objetivos comunes y evaluar y ajustar la dirección de la entidad a un entorno cambiante.

Se solicitó el Plan Estratégico de Tecnología de Información del Departamento con el fin de visualizar, si en este se consideraba al RD como parte de la planeación estratégica. El Departamento no suministró el Plan Estratégico de Tecnología de Información. La directora del RD certificó, entre otras cosas, que esto recae bajo la responsabilidad de la Oficina de Informática del Departamento.

Criterio

La situación comentada es contraria a las siguientes disposiciones:

El Artículo 12, inciso (c), y el Artículo 13, inciso (a), de la Ley Núm. 75-2019, *Ley de la Puerto Rico Innovation and Technology Service* (Ley Núm. 75-2019), que disponen lo siguiente:

> ***Artículo 12. — Deberes y Responsabilidades de las Agencias.***
>
> *Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, las agencias tendrán que cumplir con los siguientes deberes y responsabilidades:*
>
> ***(c)** Preparar y presentar a la Puerto Rico Innovation and Technology Service los planes estratégicos de las agencias y el presupuesto de éstas relativo, únicamente, a las tecnologías de información y comunicación, dentro del término establecido por la Puerto Rico Innovation and Technology Service.*

Artículo 13. — Oficial Principal de Informática de las agencias.

Para cumplir cabalmente con los objetivos y la política pública establecida en esta Ley, el Oficial Principal de Informática de cada agencia, o en su defecto, el director o directores de información y tecnología de toda agencia, tendrán que cumplir con las políticas, protocolos, guías operacionales dispuestas por el PEII y los siguientes deberes y responsabilidades:

***(a)** Establecer un plan estratégico y funcional para el desarrollo, la implantación y el mantenimiento del sistema de información de la agencia.*

La Orden Administrativa PRITS-2021-002, conocida como *Establecer reportes de información inicial, reportes periódicos de las tecnologías de información y comunicación de las agencias bajo la jurisdicción de Puerto Rico Innovation & Technology Service en cumplimiento con la Ley 75-2019,* emitida el 12 de abril de 2021 por la PRITS, que en el Por Tanto Primero establece lo siguiente:

Con el propósito de apoyar a las Agencias en dar fiel cumplimiento a las disposiciones de la Ley-75 y para que PRITS pueda encaminar una integración adecuada de las TIC, toda Agencia presentará de conformidad con las fechas establecidas en el acápite Segundo de la presente Orden Administrativa lo siguiente:

I. Plan Estratégico – Para evaluar lo relativo a la administración, uso e inversión de las TIC con el propósito de identificar la necesidad de apoyo en la ejecución y/o asistencia de recursos, y cerciorarse que las acciones de las Agencias sean cónsonas con la política pública establecida. Se Radicarán los siguientes informes:

1. Informe de Proyectos: Mediante la utilización de la SECCIÓN A del Formulario PRITS-003 PLAN ESTRATÉGICO, se habrá de proveer la siguiente información:

a. Descripción detallada

b. Progreso

c. Necesidades Especiales para su ejecución

d. Recursos Externos

e. Recursos Internos

f. Presupuesto

g. Fuente de los recursos

h. *Referencia al número de contrato y cualquier enmienda en la Oficina del Contralor (si aplica)*

Efecto

La situación comentada, podría tener, entre otros, los siguientes efectos:

1. El Departamento quien administra las aplicaciones del RD no pueda visualizar la situación actual de la entidad.
2. No crea una visión de tecnología alineada con la estrategia de la entidad.
3. No se puedan identificar las oportunidades de mejora, y el rol que la tecnología debe tener en el Departamento y el RD.
4. El Departamento y el RD no puedan minimizar los riesgos de una transformación tecnológica debido a la ausencia de la capacidad de cambios y los desafíos a enfrentar.
5. El Departamento y el RD no se puedan centrar en las áreas críticas para alcanzar sus misiones con éxito.
6. No se optimice el uso de los recursos.
7. Impide mejorar la flexibilidad.
8. No se reduzcan las repeticiones/redundancias.
9. No se puedan establecer prioridades.

Causa

La situación comentada se atribuye a que los secretarios del Departamento no habían requerido a la OIAT la realización, para su firma, de un Plan Estratégico de Tecnología de Información, que incluyera las instrucciones del Formulario PRITS – 003. Esto según se requiere en la Ley Núm. 75-2019, para la continuidad de las funciones esenciales aplicables al Departamento y a todas las dependencias adscritas, incluso el RD.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 7.

Hallazgo 8 – Fallas con el análisis de riesgos de los sistemas de información computadorizados

Situación

El análisis de riesgos es un proceso a través del cual se identifican los activos de los sistemas de información existentes en el Departamento y en el RD, sus vulnerabilidades y las amenazas a las que se encuentras expuestos, así como la probabilidad de ocurrencia y su impacto.

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 del Departamento y del RD. Mediante este proceso, se asegura que las medidas de seguridad y los controles a ser implementados sean costo-efectivos, pertinentes a las operaciones de ambas entidades y que respondan a las amenazas que puedan ser identificadas. Además, el análisis de riesgos debe realizarse, al menos, cada 12 meses o luego de un cambio significativo en la infraestructura operacional.

El examen del análisis de riesgos suministrado por la OIAT reveló lo siguiente:

a. El análisis de riesgos no estaba actualizado a la fecha del examen, su fecha de revisión fue al 24 de noviembre del 2021.

b. No se consideran los aspectos básicos necesarios para un análisis de riesgos, tales como: la identificación de todos los activos de sistemas de información (equipos, programas y datos) existentes en el Departamento, el RD y otras dependencias, con su valoración, 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; la identificación de las vulnerabilidades y amenazas, la probabilidad de ocurrencia y el impacto de cada una de estas.

c. No presenta las conclusiones de la gerencia en respuesta a su evaluación del riesgo (aceptación, transferencia, reducción o asumir el riesgo).

d. No presenta informes de seguimiento o monitoreo de las amenazas y vulnerabilidades.

e. El documento no presenta la firma de aceptación de la autoridad nominadora (entiéndase el secretario del Departamento) o su representante autorizado, por ende no está autorizado.

Criterio

La situación comentada es contraria a las siguientes disposiciones:

El último párrafo de la Sección 10 del *Análisis de Riesgo* del 24 de noviembre de 2021 presentado por la OIAT establece lo siguiente:

> *10. METODOLOGÍA*
>
> ***Revisión periódica de Evaluación de Riesgo***
>
> *De acuerdo con las mejores prácticas de la industria de IT y basado en las normas establecidas por DRII[23], ISACA[24] y NIST[25], recomiendan revisar la evaluación de riesgo al menos una vez al año. La revisión debe considerar los resultados del monitoreo continuo de los factores de riesgo y así crear un documento que aborde todos los procesos críticos identificados en OIAT.*

La *Política para la Seguridad Cibernética* aprobada el 29 de octubre de 2021 por la PRITS, que en la Sección 6, incisos 6.1.1, 6.1.3, 6.1.6 y 6.1.8, establece lo siguiente:

> *6. Política*
>
> *6.1 Requerimientos generales*
>
> *Las agencias deberán:*
>
> *6.1.1 Proteger y mantener la confidencialidad, integridad y disponibilidad de la información almacenada y/o administrada por los sistemas de información gubernamentales y los activos de infraestructura relacionados.*
>
> *6.1.3 Potenciar las capacidades y los esfuerzos para impedir, detectar, prevenir, proteger y responder a las amenazas contra los sistemas de información y los datos del gobierno.*
>
> *6.1.6 Monitorear, identificar, responder y administrar los riesgos y eventos que involucran irregularidades de seguridad, infracciones o comprometen los*

[23] *Disaster Recovery Institute International.*
[24] *Information Systems Audit and Control Association.*
[25] *National Institute of Standards and Technology.*

activos de información, incluyendo la pérdida, el uso indebido y el acceso o divulgación no autorizados.

6.1.8 Realizar evaluaciones periódicas del riesgo y la magnitud del daño que podría resultar del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados de la información y los sistemas de información que respaldan las operaciones y los activos de la agencia.

Las mejores prácticas en el campo de la tecnología de información indican que para proteger los activos de sistemas de información y garantizar la continuidad de las operaciones, las agencias deben implantar y realizar una evaluación de riesgos para identificar los activos y recursos que se deben proteger, y clasificarlos en términos de criticidad y sensibilidad. Como parte integral de la evaluación de riesgos, se deben identificar las posibles amenazas o riesgos a los cuales estos están expuestos y determinar la probabilidad de que las amenazas o los eventos ocurran y el impacto que tendrían sobre las operaciones del Departamento y el RD y otras dependencias adscritas.

Como ejemplo de ello, el *National Institute of Standards and Technology (NIST)* del U.S. Department of Commerce emitió en septiembre de 2012 la Publicación Especial *800-30* ***Guide for Conducting Risk Assessments***, que en el Capítulo 1, *Introduction* y Sección 1.2, y en el Capítulo 2, Sección 2.4, establece respectivamente lo siguiente:

CHAPTER ONE

INTRODUCTION

Risk assessment is one of the fundamental components of an organizational risk management process as described in NIST Special Publication 800-39. Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems. The purpose of risk assessments is to inform decision makers and support risk responses by identifying (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations;(iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. …

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of risk management professionals including:

- *Individuals with oversight responsibilities for risk management (e.g., heads of agencies, chief executive officers, chief operating officers, risk executive [function]);*

- *Individuals with responsibilities for conducting organizational missions/business functions (e.g., mission/business owners, information owners/stewards, authorizing officials);*

- *Individuals with responsibilities for acquiring information technology products, services, or information systems (e.g., acquisition officials, procurement officers, contracting officers);*

- *Individuals with information system/security design, development, and implementation responsibilities (e.g., program managers, enterprise architects, information security architects, information system/security engineers, information systems integrators);*

- *Individuals with information security oversight, management, and operational responsibilities (e.g., chief information officers, senior information security officers*[26]*, information security managers, information system owners, common control providers); and*

- *Individuals with information security/risk assessment and monitoring responsibilities (e.g., system evaluators, penetration testers, security control assessors, risk assessors, independent verifiers/validators, inspectors general, auditors).*

CHAPTER TWO

THE FUNDAMENTALS

2.4 APPLICATION OF RISK ASSESSMENTS

Risk assessments support risk response decisions at the different tiers of the risk management hierarchy. At Tier 1, risk assessments can affect, for example: (i) organization-wide information security programs, policies, procedures, and guidance; (ii) the types of appropriate risk responses (i.e., risk acceptance, avoidance, mitigation, sharing, or transfer); (iii) investment decisions for information technologies/systems; (iv) procurements; (v) minimum organization-wide security controls; (vi) conformance to enterprise/security architectures; and (vii) monitoring strategies and ongoing authorizations of information systems and

[26] *At the agency level, this position is known as the Senior Agency Information Security Officer. Organizations may also refer to this position as the Chief Information Security Officer.*

common controls. At Tier 2, risk assessments can affect, for example: (i) enterprise architecture/security architecture design decisions; (ii) the selection of common controls; (iii) the selection of suppliers, services, and contractors to support organizational missions/business functions; (iv) the development of risk-aware mission/business processes; and (v) the interpretation of information security policies with respect to organizational information systems and environments in which those systems operate. Finally, at Tier 3, risk assessments can affect, for example: (i) design decisions (including the selection, tailoring, and supplementation of security controls and the selection of information technology products for organizational information systems); (ii) implementation decisions (including whether specific information technology products or product configurations meet security control requirements); and (iii) operational decisions (including the requisite level of monitoring activity, the frequency of ongoing information system authorizations, and system maintenance decisions). ...

Efecto

La situación comentada le impide al Departamento y al RD, y otras dependencias adscritas, lo siguiente:

1. Estimar el impacto que los elementos de riesgos tendrían sobre los sistemas de información, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

2. Dificulta desarrollar un plan de continuidad de negocios para poder establecer aquellas medidas de control que minimicen, mitiguen o eliminen los riesgos identificados.

3. Impide que se establezcan los procedimientos para restablecer las operaciones del Departamento, como las del RD y otras dependencias adscritas, de surgir alguna eventualidad.

Causa

La situación comentada se debió a que el RD no realizó los trámites con la OIAT para realizar el análisis de riesgos.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

Aceptamos los hallazgos identificados en dicho borrador. . .

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos…

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 8.

Hallazgo 9 – Fallas relacionadas con el Plan de Continuidad de Operaciones y falta de un Plan de Contingencias

Situación

a. Un Plan de Continuidad de Operaciones (en adelante, Plan de Continuidad) es un plan para restablecer y continuar las operaciones en respuesta a emergencias, tales como fenómenos meteorológicos, apagones, ataques terroristas u otras interrupciones significativas a las operaciones de la agencia. El Plan de Continuidad ayuda a asegurar que todo el personal, las instalaciones y la información estén protegidos, de modo que las funciones necesarias y las operaciones normales puedan reanudarse rápidamente después de la emergencia. La norma **ISO/IEC 22301:2019**, titulada *Seguridad y Resiliencia, Sistemas de gestión de la continuidad del negocio - Requisitos*, establece un marco internacionalmente reconocido para desarrollar, implementar, mantener y mejorar un Plan de Continuidad. En ella presenta componentes claves que el Plan de Continuidad debe incluir, entre otras cosas, lo siguiente:

    - Las funciones claves que la entidad debe realizar, independientemente de la emergencia.
    - El personal y los recursos necesarios para realizar estas funciones.
    - Los pasos que seguir si una entidad gubernamental no puede prestar sus servicios regulares.
    - Instrucciones para lograr el funcionamiento después de la emergencia.

    Los objetivos de continuidad de operaciones son, entre otros, los siguientes:

    - Asegurarse de que las funciones necesarias puedan realizarse después de un desastre.
    - Proteger la vida y reducir al mínimo las pérdidas y los daños materiales. Proteger al personal, las instalaciones, el equipo y demás activos fundamentales para las operaciones de las entidades.
    - Asegurar toda la información que resguarda la entidad.

- Establecer las responsabilidades del personal que estará ejecutando el BCP.
- Reducir al mínimo las interrupciones a las operaciones.
- Asegurarse de que existan centros alternos para reestablecer las operaciones de ser necesario.
- Lograr una recuperación oportuna y ordenada después de la emergencia.

Toda entidad gubernamental debe tener aprobado, implementado, ejercitado y probado (simulacros) un plan de recuperación de desastres, el cual debe ser actualizado cada vez que se incorporen sistemas y aplicaciones operacionales en la entidad o cuando se realice un cambio significativo dentro de la infraestructura operacional y de tecnología de información.

La directora del RD y el director de la OIAT del Departamento son los responsables de coordinar las tareas relacionadas con la preparación del plan de recuperación de desastres.

El examen realizado al Plan de Continuidad del Departamento/RD, del 4 de septiembre de 2023, reveló lo siguiente:

1. No contiene la elaboración de una evaluación de riesgo.
2. No contiene un análisis de impacto en el negocio.
3. No contiene un Plan de Contingencias.
4. No se realizan simulacros para probar el Plan de Continuidad.
5. No se ha capacitado a los empleados en lo relacionado con el Plan de Continuidad. (**Ver Hallazgo 11**)

b. Un Plan de Contingencias representa una amplia gama de actividades destinadas y dirigidas a mantener y recuperar los servicios críticos después de una emergencia; esta se ajusta a un entorno mucho más amplio de preparación para emergencias que incluye la organización, la continuidad de procesos y la planificación de la recuperación.

Un Plan de Contingencias engloba los procedimientos alternativos para facilitar el funcionamiento apropiado de las Tecnologías de Información, así como los riesgos operacionales u operativos[27], cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la entidad. Este Plan permite minimizar las consecuencias en caso de algún incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas de un evento:

[27] Los riesgos operativos u operacionales son, por ejemplo, los errores humanos, fraude, fallos tecnológicos, accidentes, pérdidas de información, caídas de la actividad, entre otros.

1. Antes, como un plan de prevención para mitigar los incidentes.
2. Durante, como un plan de emergencia o ejecución en el momento de presentarse el incidente.
3. Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

Las entidades gubernamentales, independiente de su tamaño y funciones, tienen que contar con un Plan de Contingencias, escrito y autorizado por el funcionario principal o el que este delegue, para restablecer sus operaciones más importantes y críticas en caso de que surja una emergencia. Dicho Plan debe estar actualizado e incluir toda la información y los procesos necesarios para recuperar las operaciones de sus sistemas de información computadorizados. Además, tiene que ser divulgado al personal responsable de los asuntos relacionados con la recuperación en casos de desastres y al personal responsable de la continuidad de las operaciones.

El Plan de Contingencias se genera para minimizar los riesgos operacionales u operativos y la recuperación oportuna de las operaciones relacionadas con los sistemas de información tecnológicos.

Se solicitó copia de la última versión del Plan de Continuidad y el Plan de Contingencias. El RD proveyó el Plan de Continuidad y presentó un Plan de Contingencias revisado en agosto de 2019 y por consiguiente no cuenta con un plan actualizado.

Criterio

La situación comentada en el **apartado a.** es contraria a las siguientes disposiciones:

La *Política para la Seguridad Cibernética* aprobada el 29 de octubre de 2021 por la PRITS, que en la Sección 7, incisos 7.2 y 7.2.10, establece lo siguiente:

> *7. Responsabilidades*
>
> *7.2 Equipo de manejo de riesgos y seguridad cibernética*
>
> *Cada jefe de la agencia debe designar a una persona o equipo que será responsable de la seguridad cibernética y el manejo de riesgo de la agencia. Las responsabilidades de este equipo incluyen, entre otras, las siguientes:*
>
> *7.2.10 Diseñar e implementar planes y procedimientos para la recuperación tras desastres y asegurar la continuidad de las operaciones de los sistemas de información que apoyan las operaciones y los activos de la agencia.*

La Política TI-PRITS-004, *Política sobre los Servicios de Tecnología*, aprobada el 30 de junio de 2024 por la PRITS, que en la Sección 7, incisos 7.2, 7.2.4, 7.2.4.1 y 7.2.4.2, establece lo siguiente:

7. Procedimiento

7.2 Responsabilidad de la Agencia

7.2.4 Recuperación de Desastres

7.2.4.1 La Agencia será responsable de asegurar la continuidad de sus operaciones mediante un Plan de Recuperación por Desastre desarrollado por la Agencia, de acuerdo con la Política para la Seguridad Cibernética promulgada por PRITS.

7.2.4.2 El Plan de Recuperación por Desastre abarcará todo lo relacionado a programación (software), equipo (hardware), datos y facilidades físicas de la Agencia.

La situación comentada en el **apartado b.** es contraria a las siguientes disposiciones:

El Artículo 7, inciso (18), de la Ley Núm. 40-2024, conocida como *Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico,* que dispone lo siguiente:

Artículo 7. — Estándares y principios mínimos de Ciberseguridad.

Toda Agencia y todo Proveedor de servicios contratados deberá cumplir y asegurarse que todo persona natural o jurídica que haga negocios o contrate con ellos cumpla con al menos los siguientes Estándares y principios mínimos de Ciberseguridad:

(*18*) *Establecer planes de resguardo y recuperación de datos que deben ser integrado al* ***plan de contingencia de la Agencia*** *para velar por la continuidad de las operaciones considerando sistemas mantenidos localmente y los sistemas mantenidos por suplidores o terceros tipo "cloud";* **[énfasis suplido]**

La Política TI-PRITS-005, *Política* sobre las *Mejores Prácticas de Infraestructura Tecnológica*, aprobada el 30 de junio de 2023 por la PRITS, que en la Sección 8, incisos 8.1 y 8.1.3, establece lo siguiente:

8. Datos/Información

8.1 Política para el Componente de Datos

8.1.3 Las agencias deben desarrollar un ***plan de contingencia*** *que contenga los elementos descritos en la Política de Seguridad Cibernética y los Estándares para la Seguridad Cibernética.* **[énfasis suplido]**

Las mejores prácticas en el campo de la tecnología de información que son utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información

computadorizados, recomiendan que como parte del *Plan de Continuidad de Negocios* (BCP, en inglés) se deberá preparar un *Plan de Contingencias*. Como ejemplo de ello, el Federal Information System Controls Audit Manual (FISCAM), promulgado en febrero de 2009 (GAO-09-232G) por la U.S. Government Accountability Office (GAO)[28], establece en su Capítulo 3.5 lo siguiente:

> ***3.5. Contingency Planning (CP)***
>
> *Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.*
>
> *Given these severe implications, it is critical that an entity have in place (1) procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. Such plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as those performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster-simulation exercises. …*

Según las mejores prácticas, los planes de contingencia deben actualizarse cada vez que se realicen cambios en los sistemas de información o en la infraestructura tecnológica.

Efecto

La situación comentada propicia, entre otras, lo siguiente:

1. Desorganización en casos de emergencias.
2. Improvisación por falta de guías.
3. Toma de decisiones inapropiadas.
4. Erogación innecesaria de fondos públicos.
5. Interrupciones prolongadas.
6. Ausencia de servicios a la ciudadanía.

[28] El FISCAM fue revisado en septiembre de 2024 (GAO-24-107026) y sustituyó la revisión realizada en el año 2009. El FISCAM revisado en el año 2024 contiene recomendaciones similares a las del año 2009.

Causa

Las situaciones comentadas se atribuyen en gran medida a que los servidores públicos que actuaron como directores de la OIAT para el período de examen, fechas anteriores y posteriores no se aseguraron de la verificación del Plan de Continuidad. Además, no incluyeron un Plan de Contingencias con los requisitos que son necesarios para atender las situaciones de emergencia.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 9.

Hallazgo 10 – Deficiencias relacionadas con el informe y toma de inventario de los sistemas de información

Situación

Los sistemas de información de las entidades gubernamentales, independientemente de su tamaño, incluidos los programas, las aplicaciones y todos los archivos electrónicos, deben constar en el inventario de las respectivas agencias y solo pueden utilizarse para fines estrictamente oficiales y legales. Dicho inventario debe revisarse anualmente y constatarse en un documento oficial.

a. La administradora del RD proveyó 2 inventarios físicos en hojas de Excel para el período de este examen. Una de las hojas presentaba 80 *routers*[29], distribuidos por todas las dependencias del RD. La otra hoja de Excel presentaba un inventario físico con 722 equipos computadorizados. El examen de estos inventarios reflejó lo siguiente:

[29] *Router* – Es un equipo (*hardware*) que conecta todos los dispositivos de una red para que puedan compartir una única conexión a Internet. Conecta ordenadores, impresoras y otros dispositivos finales entre sí mediante cables *Ethernet* o una conexión inalámbrica.

1) El inventario de los 80 *routers* no presentaba lo siguiente:

   a) En los 80 *routers* (100%) no incluyeron el modelo, el número de recibo, la fecha de adquisición para efectos de las garantías, y el suplidor.

   b) En 67 *routers* (84%) no incluyeron el número de serie.

2) En ambas listas de inventario no incluyeron los siguientes 52 ordenadores (computadoras portátiles):

Tabla 4: Ordenadores no incluidos en el inventario

#	Núm. de propiedad	#	Núm. de propiedad	#	Núm. de propiedad	#	Núm. de propiedad
1.	26760	2.	29019	3.	29023	4.	29025
5.	29035	6.	29042	7.	29050	8.	29054
9.	29056	10.	29059	11.	29178	12.	29189
13.	29212	14.	29246	15.	29255	16.	29259
17.	29269	18.	29271	19.	29276	20.	29301
21.	29303	22.	29333	23.	29342	24.	29367
25.	29371	26.	29379	27.	29391	28.	29393
29.	29399	30.	29406	31.	29413	32.	29421
33.	29430	34.	29433	33.	29439	36.	29440
37.	29441	38.	29447	39.	29448	40.	29454
41.	29456	42.	29473	43.	29482	44.	29484
45.	29485	46.	29637	47.	29644	48.	29743
49.	29745	50.	29824	51.	29827	52.	29848

Estas computadoras portátiles son parte del *Anexo D, Identificación de Personal de Continuidad, Asignación de Laptops*, incluido en el Plan de Continuidad Operacional del Registro Demográfico.

3) No se proveyó un registro de los programas adquiridos e instalados en las computadoras que incluyera, entre otras cosas: el número de la licencia del programa, el costo de los programas instalados, el nombre del proveedor, el nombre del usuario, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el número de propiedad asignado, la descripción de la computadora donde están instalados y el total de licencias adquiridas.

Criterio

La situación comentada es contraria a las siguientes disposiciones:

El Artículo 10, inciso (a), de la precitada Ley Núm. 230 de 1974, que dispone lo siguiente:

Artículo 10. — Custodia, control y contabilidad de propiedad pública.

(a) La custodia, cuidado y control físico de la propiedad pública será responsabilidad del jefe de la propia dependencia, Cuerpo Legislativo o entidad corporativa o su representante autorizado.

El Artículo XIV, incisos A y D, del Reglamento 7080, *Reglamento Núm. 11 Normas Básicas para el Control y Contabilidad de los Activos Fijos*, aprobado por el Departamento de Estado el 17 de enero de 2006, que establecen lo siguiente:

Artículo XIV – Inventario Físico

A. Los registros internos de las dependencias de inventario tienen que estar respaldados por los inventarios físicos.

[…]

D. Las agencias prepararán el inventario de forma mecanizada utilizando el Modelo SC 795, Inventario Físico de Activo Fijo.

Enviarán a la División de Cuentas de la Propiedad del Negociado de Cuentas del Departamento de Hacienda el Modelo SC 795 y SC 795.1, Certificación de Toma de Inventario Físico. El inventario debe incluir los siguientes datos:

1- Número de Propiedad

2- Costo

3- Clase de Propiedad

4- Descripción

5- Fecha de Adquisición

6- Fondo

La Política TI-PRITS-002, *Uso de los Sistemas de Información, de Internet y del Correo Electrónico*, aprobada el 17 de abril de 2023 por la PRITS, que en la Sección 6, incisos 6.2 y 6.2.2, establece lo siguiente:

6. Política

6.2. Normas generales aplicables al uso de los sistemas de información:

6.2.2. Los sistemas de información de las agencias, incluyendo los programas, aplicaciones y archivos electrónicos, son propiedad del Gobierno de Puerto Rico, por lo que deben constar en el inventario de las respectivas agencias y

solo pueden utilizarse para fines estrictamente oficiales y legales. Dicho inventario debe revisarse anualmente constatándolo en documento oficial.

La citada Orden Administrativa PRITS-2021-002, que en el Por Tanto Primero, incisos I. 3. a., establece lo siguiente:

I. Plan Estratégico

[…]

3. Informe de Infraestructura: Mediante la utilización de la SECCIÓN C del Formulario PRITS-003 PLAN ESTRATÉGICO se habrá [de] *proveer la siguiente información:*

a. Desglose de los equipos

El *Appendix XI – Glossary*, definición de *Inventario* del citado *Federal Information System Controls Audit Manual (FISCAM)* de febrero de 2009, que establece lo siguiente:

Inventory *FISMA*[30] *requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control. The inventory must include identification of the interfaces between agency systems and all other systems or networks, including interfaces not controlled by the agency.*

El Capítulo 3.1. del citado FISCAM, apartado *Security Management Critical Elements,* en el inciso SM-1.5 establece lo siguiente:

3.1. Security Management (SM)

SM-1.5. An inventory of systems is developed, documented, and kept up-to-date

To implement an effective security program, entities need to maintain a complete, accurate, and up-to-date inventory of their systems. Without one, the entity cannot effectively manage IS controls across the entity. For example, effective configuration management requires the entity to know what systems they have and whether the systems are configured as intended. Furthermore, the inventory is necessary for effective monitoring, testing, and evaluation of IS controls, and to support information technology planning, budgeting, acquisition, and management.

[30] Federal Information Security Management Act is United States legislation that defines a framework of guidelines and security standards to protect government information and operations. This risk management framework was signed into law as part of the Electronic Government Act of 2002 and later updated and amended.

> *FISMA requires that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or under its control.*
> ...

Con relación al **apartado a. 3)** las mejores prácticas de la tecnología de información sugieren como medida de control interno y en cumplimiento con la normativa aplicable que se mantenga un registro de todos los programas instalados en los ordenadores (computadoras), en el cual se indique, entre otras cosas, lo siguiente: el número de la licencia, nombre del proveedor, dueño de la licencia, fecha de adquisición, equipo donde está instalado (número de propiedad o de serie), ubicación física de la licencia y de sus manuales, el nombre del usuario, el número de propiedad asignado, y el costo.

Efecto

Las situaciones comentadas tienen el efecto de lo siguiente:

1. Impiden al Departamento y al RD mantener un control efectivo sobre el equipo y la propiedad bajo su custodia.

2. Propicia un ambiente para el uso indebido o la desaparición de la propiedad y otras situaciones adversas, como la protección y seguridad de la información[31] sin que se puedan detectar a tiempo para fijar responsabilidades.

3. Impide ejercer un control eficaz de los programas y de las licencias correspondientes.

4. Propicia la instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para el Departamento y el RD.

5. Limita a la PRITS de realizar un inventario general de las tecnologías de información y comunicación (TIC) existentes en el Gobierno, según se define en la citada Orden Administrativa PRITS-2021-002.

6. Dificulta y limita la gestión fiscalizadora.

Causa

Las situaciones comentadas se atribuyen a que los directores ejecutivos del RD no velaron que el personal encargado de la propiedad cumpliera con su responsabilidad de mantener un inventario de la propiedad del propio RD. Además, no tomaron las medidas necesarias para mantener un registro y un control adecuado de los programas adquiridos e instalados en los ordenadores

[31] La protección y seguridad de la información se refiere al conjunto de medidas y prácticas que se implementan para salvaguardar la confidencialidad, integridad y disponibilidad de la información. Su objetivo es evitar accesos no autorizados, alteraciones, pérdidas o daños a los datos, tanto en formato físico como digital.

(computadoras). Esto, con el fin de mantener un inventario de los programas adquiridos e instalados y detectar la instalación de programas no autorizados.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 10.

Hallazgo 11 – Ausencia de adiestramientos sobre las normas y los procedimientos para la seguridad de los sistemas de información

Situación

Para las entidades gubernamentales, independientemente de su tamaño, cada vez es más complejo proteger la información de la propia entidad, así como la de los ciudadanos que reciben servicios. A diferencia del pasado, hoy la ciberseguridad[32] es indispensable para garantizar las operaciones de las entidades, pues, los ataques cibernéticos son un riesgo real en cualquier tipo de actividad.

Si bien la fuerza laboral es el mayor activo que puede tener una entidad, no es menos cierto que también representan uno de los mayores riesgos en la seguridad de la información. Los delincuentes informáticos pueden vulnerar los sistemas informáticos de una entidad, al evitar ser detectados por los mecanismos de seguridad que las protegen. Sin embargo, hay una forma mucho

[32] La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos; también se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil y puede dividirse en algunas categorías comunes.

más sencilla y rápida, que es a través del *phishing*[33] o utilizando la ingeniería social[34], donde los atacantes usan a los empleados para que les faciliten involuntariamente el acceso a los sistemas de la organización.

Por lo antes mencionado, es de vital importancia para toda entidad gubernamental capacitar a sus empleados en los riesgos asociados con la seguridad informática. De esa forma, pueden evitar que cualquier atacante acceda a la información importante de la entidad, manteniéndola segura.

Como parte del examen se le solicitó a la directora del RD que suministrara lo siguiente:

1. Copia del programa de adiestramientos para el personal que incluya las orientaciones sobre las normas y los procedimientos relacionados con los sistemas de información computadorizados.

2. Certificación de los adiestramientos tomados por los empleados adscritos al Registro Demográfico con respecto a la seguridad de la información.

En respuesta a lo solicitado la directora del RD entregó lo siguiente:

1. Manual de Adiestramiento – Subsección Expedición de Certificaciones.
2. Manual de Adiestramiento – Subsección Registración de Eventos Vitales.
3. Guía para crear, registrar, expedir y enmendar un Registro de Defunción.
4. Hoja de Asistencia Adiestramientos Sección Procesos de Registración de Eventos Vitales.
5. Manual de Adiestramiento – Subsección Procesamiento de Datos.
6. Hoja de Asistencia Adiestramiento Readiestramiento Sistema Electrónico de Defunción (EDRS).

Sin embargo, no suministró la información solicitada. La directora del RD certificó que entregó copia de la información contenida en su carpeta con los adiestramientos de sistema ofrecidos al personal.

Criterio

La situación comentada es contraria a las siguientes disposiciones:

[33] Ciberataque dirigido a personas a través del correo electrónico, mensajes de texto, llamadas telefónicas u otras formas de comunicación. El término *phishing* se pronuncia igual que *fishing* y su traducción literal es "pescar". Un ataque de phishing tiene como objetivo engañar al destinatario para que realice la acción deseada por el atacante, como revelar información financiera, credenciales de acceso al sistema u otra información sensible.

[34] La ingeniería social es la práctica ilegítima de obtener información confidencial a través de la manipulación de usuarios legítimos. Es un conjunto de técnicas que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometido y es utilizado en diversas formas de estafas y suplantación de identidad. El principio que sustenta la ingeniería social es el de que, en cualquier sistema, los usuarios son el eslabón débil.

El Artículo 6, Sección 6.5, de la Ley Núm. 8-2017, según enmendada, conocida como *Ley para la Administración y Transformación de los Recursos Humanos en el Gobierno de Puerto Rico*, que dispone lo siguiente:

> ***Artículo 6. — Administración de los Recursos Humanos del Servicio Público.***
>
> ***Sección 6.5. — Disposiciones sobre Adiestramiento.***
>
> *El adiestramiento constituye parte esencial del principio de mérito. Es indispensable atemperar la política pública en materia de adiestramientos a las realidades de la Administración Pública del Siglo XXI . . .*

El Artículo 5, y el Artículo 7, inciso (17), de la Ley Núm. 40-2024, conocida como *Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico*, que dispone lo siguiente:

> ***Artículo 5. – Implementación de la política pública.***
>
> *[...]*
>
> *Toda Agencia, en colaboración con PRITS, deberá desarrollar, documentar e implementar un programa de Ciberseguridad de acorde con esta Ley. El programa, como mínimo, deberá incluir todos los activos de información de la Agencia, incluyendo servicios de informática provisto por terceros, una evaluación de riesgos de Ciberseguridad que la Agencia llevará a cabo por lo menos una vez al año,* ***un plan educativo*** *que vele por la educación del personal, contratistas, y clientes (la ciudadanía), incluyendo cursos especializados para desarrollo de los administradores de sistemas y tecnologías sobre las mejores prácticas de Ciberseguridad y una evaluación de vulnerabilidades de seguridad tanto interno como externo ("penetration test") para validar la efectividad de los controles que la agencia haya implementado. . . .* **[énfasis suplido]**
>
> ***Artículo 7. – Estándares y principios mínimos de Ciberseguridad.***
>
> ***(17)*** *Establecer y mantener un programa de educación de Ciberseguridad para el personal y para la ciudadanía, incluyendo personal de entidades que provean servicios al Gobierno. . .*

La Carta Circular Núm. 2021-007, *Establecimiento de la política para la seguridad cibernética*, emitida el 6 de diciembre de 2021, por la PRITS, que, en su *Propósito y Determinación*, inciso 5 establece lo siguiente:

> *La Política para la Seguridad Cibernética tiene como objetivo:*
>
> *5. Proporcionar orientación a empleados nuevos y existentes, personal temporero, contratistas, socios y terceros sobre la importancia de sus funciones y*

responsabilidades relacionadas con la seguridad cibernética y la protección de los activos de información del gobierno.

La *Política para la Seguridad Cibernética* aprobada el 29 de octubre de 2021 por la PRITS, que en la Sección 6, incisos 6.2.1 y 6.2.2, que establecen lo siguiente:

6. Política

6.2 Concienciación sobre la política, comunicación y capacitación

Las agencias serán responsables de la promoción continua y concienciación sobre la seguridad cibernética a través de capacitaciones, talleres u orientaciones periódicas. Para mitigar el riesgo de eventos de ciberseguridad y la divulgación involuntaria de información confidencial por parte de los empleados y proveedores de servicios externos, se tomarán las siguientes medidas.

6.2.1 Empleados nuevos

Durante el proceso de incorporación, el personal de Recursos Humanos deberá:

- *Proporcionar a todos los empleados nuevos acceso a la **Guía para empleados sobre seguridad cibernética** y asegurarse de que todos reconozcan formalmente que han recibido, leído y cumplirán con los todos los requisitos en este documento que se aplican a sus áreas de responsabilidad.*[35]

- *Asegurarse de que todos los empleados completen las actividades de capacitación y concienciación sobre ciberseguridad, según su disponibilidad.*

6.2.2 Empleados existentes

- *Al menos una vez al año, todos los empleados que hayan estado laborando por más de doce (12) meses, deberán completar una sesión anual de capacitación y concientización sobre ciberseguridad y reconocer formalmente la finalización de estos requisitos anuales.*

La Carta Circular OC-24-03, *Recomendaciones para la protección de los sistemas de información contra ataques cibernéticos*, emitida el 25 de agosto de 2023 por la Contralora de Puerto Rico, en el Anejo *Aspectos para considerar al momento de desarrollar, implementar y promover un programa de ciberseguridad*, inciso 8 c. establece lo siguiente:

[35] (Énfasis suplido).

8. *Promover una cultura de ciberseguridad dirigida a proteger la información confidencial de la entidad, sus proveedores y ciudadanos; y a reducir los errores o las fallas humanas que pueden afectar la seguridad. Como parte de las acciones que fomentan el desarrollo de esta cultura, recomendamos lo siguiente:*

    c. *Proveer adiestramientos continuos al encargado de la seguridad de los sistemas y a todos los empleados para que puedan identificar y responder a las posibles amenazas cibernéticas.*

Como medida de control interno y como parte de una sana administración y transparencia gubernamental toda entidad deberá garantizar el buen uso, manejo, integridad, exactitud y preservación de la información del gobierno y protegerla contra la modificación, divulgación y manipulación. Las agencias mantendrán al día un programa de concienciación sobre seguridad de información dirigida a todos los usuarios en todos los niveles.

Efecto

La situación comentada tiene el efecto de lo siguiente:

1. Aumenta el riesgo de pérdida y divulgación no autorizada de la información y propicia el uso indebido de los sistemas de información y el acceso no autorizado a los programas o datos del Departamento y el RD.

2. La falta de conocimiento de las normas de seguridad relacionadas con los sistemas de información ocasiona el incumplimiento de estas con los consiguientes efectos adversos en cuanto a la protección de la información y del equipo.

Causa

La situación comentada se atribuye a que la directora del RD no cumplió con su deber de informar a las Oficinas de Recursos Humanos del Departamento la necesidad de adiestramientos para los usuarios u operadores, a los fines de mantenerse al día en los conocimientos relacionados con las funciones y en el manejo de la seguridad de los sistemas a su cargo. Además, no había identificado las necesidades de adiestramiento en la seguridad de la información para los empleados del RD.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 11.

Hallazgo 12 – Falta de organización de los cables que se conectaban a los equipos de comunicación del RD

Situación

a. La extensión de la red de comunicaciones del Departamento en el RD contaba con 2 cuartos de distribución de cableado, entre los pisos 4 y 9 del edificio, que alberga las oficinas centrales del RD. En estas áreas se habían instalado 2 estantes o paneles de conexiones (*patch panel*[36]), también denominado bahía de rutas, para organizar y proteger los equipos de comunicación que mantenían las conexiones necesarias para interconectar las computadoras que recibían servicio de la red del Departamento.

El examen efectuado sobre los controles físicos y ambientales existentes para los 2 cuartos de distribución de cableado reveló lo siguiente:

1) Ambos (100%) no mantenían organizados, identificados ni amarrados los cables que se conectaban a los equipos. Esto es necesario para identificar las conexiones autorizadas y facilitar el mantenimiento de la red en caso de interrupciones. **[Ver Anejos 1 y 2]**

2) No contaban (100%) con un diagrama esquemático ni un diagrama de los *drops*[37] que ilustrara las conexiones establecidas con los equipos.

3) Los armarios con el cableado estaban abiertos en los 2 cuartos (100%).

4) El equipo de comunicación y el panel de los cables del servicio telefónico aparentaba estar fuera de funcionamiento. Esto dificulta mantener un control de acceso adecuado a dichos cuartos.

5) Con relación a los controles ambientales examinados en los 2 cuartos de distribución de cableado se determinó lo siguiente:

[36] Un panel de parcheo o de conexión es un componente esencial que forma parte de los racks para servidores de datos o comunicación. Estos dispositivos de hardware son tan imprescindibles en la estructura de red, como los enrutadores o conmutadores. Los paneles de parcheo sirven para la gestión de los diversos cables que conforman la red, para asegurar que dentro del rack todo esté ordenado, identificado y accesible.

[37] Conector de pared para las instalaciones de redes.

a) Los equipos de telecomunicaciones instalados en ambos presentaban particulado de polvo acumulado, lo que denota la falta de mantenimiento.

b) No existen controles (100%) para asegurar la existencia de niveles adecuados de temperatura y humedad.

c) Ambos (100%) eran utilizados para almacenar materiales y otros equipos, tales como: cajas de cartón, una escalera de aluminio, una silla de espera y partes de un panel de conexiones de telefonía o panel de parcheo telefónico análogo.

d) Ninguno (100%) contaba con extintores de incendios.

Criterio

La situación comentada es contraria a las siguientes disposiciones:

La Sección AC.04.01.09 *Physical access to system distribution and transmission lines is appropriately controlled,* incluida en la Tabla del *Federal Information System Controls Audit Manual* (FISCAM) *September 2024* | GAO-24-107026, que en su *Note* del *Illustrative audit procedures* establece lo siguiente:

> *Note: Security controls are applied to system distribution and transmission lines to prevent accidental damage, disruption, and physical tampering. Such controls may also be necessary to prevent eavesdropping or modification of unencrypted transmissions. Security controls of physical access to system distribution and transmission lines include disconnected or* ***locked spare jacks, locked wiring closets****, protection of cabling by conduit or cable trays, and wiretapping sensors.*

Las mejores prácticas y estándares de la industria requieren que la gerencia sea responsable de desarrollar políticas específicas de seguridad de acuerdo con las características propias de sus ambientes de tecnología, particularmente sus sistemas críticos. Esto implica que, como parte de una sana administración, las agencias deberán tener los cuidados necesarios para proteger los equipos computadorizados contra daños y averías y para mantener el funcionamiento óptimo de estos. Es necesario que se mantengan organizados los cables que conectan los equipos de comunicación para garantizar razonablemente la seguridad de los equipos y de los sistemas computadorizados. Esto permite atender y corregir a tiempo los problemas de comunicación y detectar cualquier conexión no autorizada. Un sistema de cable bien organizado ofrece una gran cantidad de beneficios, siendo la seguridad el más importante.

Efecto

Las situaciones comentadas tienen el efecto de lo siguiente:

1. Dificulta al personal de la OIAT realizar los trabajos para atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

2. Obstaculiza el acceso fácil a los cables.

3. Complica las reparaciones y actualizaciones.

4. Solución de problemas menos rápida (los errores humanos son una de las principales razones del tiempo de inactividad).

5. Maximiza las posibilidades de desconectar el cable equivocado.

6. Aumenta el tiempo de inactividad de la red y el daño del cable.

7. Disminuye el flujo de aire y la refrigeración, lo que puede acortar la vida útil de los cables.

8. Disminuye el rendimiento de la red con menor velocidad, eficiencia y ancho de banda.

9. Impide a la OIAT obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de esta.

10. Afecta la calidad de la señal y la seguridad de la red al mantener la proximidad de los cables de datos a fuentes de interferencia electromagnética y no tener métodos de enrutamiento adecuados para evitar cruces y enredos.

11. Dificulta el manejo y los controles internos de los sistemas relacionados con las solicitudes para la emisión de eventos vitales.

Causa

La situación comentada se debió a que la OIAT no impartió instrucciones para que se organizaran los cables conectados a los equipos de comunicación y a la falta de supervisión continua de la conexión de estos.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

> *Aceptamos los hallazgos identificados en dicho borrador. . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 12.

Hallazgo 13 - Contrato de servicio de tecnología formalizado en incumplimiento con las normativas de la PRITS

Situación

La contratación gubernamental es esencial para garantizar servicios de calidad en Puerto Rico. El Gobierno observa normativas estrictas para realizar compras y contratar servicios, promoviendo la transparencia y el uso eficiente de los fondos públicos. En este contexto la citada Ley Núm. 75-2019, según enmendada, *Ley de la Puerto Rico Innovation and Technology Service (PRITS)*, faculta y requiere a las entidades gubernamentales que establezcan y promuevan la política pública relacionada con la elaboración, manejo, desarrollo, coordinación e integración interagencial efectiva de la innovación, así como de la infraestructura tecnológica e informática del Gobierno de Puerto Rico. Además, la Ley Núm.75-2019, en su Artículo 6(ff), dispone que la PRITS evalúe y apruebe, previo a la formalización de un contrato, cualquier proyecto de creación, implantación, modificación, migración y actualización de las bases de datos, innovación, información y tecnología a ser adoptadas por la agencia, para garantizar que los proyectos tecnológicos estén alineados con la política pública del gobierno.

El 29 de marzo de 2021, el Departamento formalizó un contrato con una Compañía con el propósito de utilizar página electrónica oficial https://www.vitalchek.com/v/vital-records/puerto-rico#agencies para ofrecer a los ciudadanos la capacidad de realizar solicitudes en línea de certificados de eventos vitales de nacimiento, matrimonio y defunción con acceso a la plataforma del RD.

El contrato tiene vigencia desde el 29 de marzo de 2021 hasta el 30 de junio de 2025. Bajo los términos y condiciones del contrato el Departamento no está obligado a pagar a la Compañía por los servicios prestados. No obstante, la Compañía tendrá derecho a cobrar al ciudadano cargos por servicios por cada transacción procesada a través de la plataforma.[38]

El examen realizado al proceso de contratación entre el Departamento y la Compañía evidenció que, en contraposición de las normativas vigentes, el contrato no fue sometido para la evaluación

[38] La SEGUNDA cláusula del contrato detalla los cargos por servicios que deberá pagar el ciudadano por el uso de la plataforma.

y autorización de la PRITS. El 28 de abril de 2025, la directora ejecutiva del RD certificó lo siguiente:

> *El Contrato suscrito entre el Registro Demográfico y la compañía, para la administración del sistema VitalChek, tiene una fecha de efectividad del 29 de marzo de 2021 hasta el 30 de junio de 2025.*
>
> *La Orden Administrativa PRITS-OA-2021-001, la cual establece la obligación de obtener autorización del Puerto Rico Innovation and Technology Service (PRITS) para toda contratación relacionada con sistemas de información y tecnología, fue emitida y entró en vigor el día 12 de abril de 2021. Previo a esta Orden Administrativa estaba vigente la Carta Circular 2020-003.*
>
> *Al momento de la formalización del contrato, el Registro Demográfico por error involuntario no sometió a la PRITS dicho contrato para su aprobación. Desconocemos si en algún momento durante el trámite ordinario del contrato la Oficina de Gerencia y Presupuesto (OGP) donde también son enviados para su evaluación, fue requerido o eximido de dicha aprobación de la PRITS.*

Criterio

La situación comentada es contraria a las siguientes disposiciones:

Los Artículos 6(ff), 12(h), 14 y el 15 de la precitada Ley Núm. 75-2019, disponen lo siguiente:

> ***Artículo 6. — Funciones, facultades y deberes de la Puerto Rico Innovation and Technology Service y del Principal Ejecutivo de Innovación e Información del Gobierno (PEII).***
>
> *[…]*
>
> ***ff)** Revisar, evaluar y aprobar cualquier proyecto de creación, implantación, modificación, migración y actualización de las bases de datos, innovación, información y tecnología a ser adoptadas por las agencias.*
>
> ***Artículo 12. — Deberes y Responsabilidades de las Agencias.***
>
> *[…]*
>
> ***(h)** Desarrollar y emitir todas aquellas medidas que sean necesarias para asegurar el cumplimiento fiel y estricto con esta Ley. Asimismo, las políticas gerenciales de manejo de información y las guías sobre el uso y el mantenimiento de las tecnologías de información y comunicación que emita la Puerto Rico Innovation and Technology Service deberán ser comunicadas por los jefes de agencia de manera rápida y efectiva al personal correspondiente.*

Artículo 14. — Colaboración con la Oficina de Gerencia y Presupuesto.

[…]

Ninguna propuesta de desarrollo de las tecnologías de información y comunicación o contrato para la prestación de servicios de las tecnologías de información y comunicación por cualquier Agencia será otorgada sin la revisión y los comentarios previos de la Puerto Rico Innovation and Technology Service.

Artículo 15. — Proyectos de base de datos, innovación, información y tecnología de las agencias.

La Puerto Rico Innovation and Technology Service tendrá la facultad de revisar, evaluar y aprobar cualquier proyecto de creación, implantación, modificación, migración y actualización de las bases de datos, innovación, información y tecnología a ser adoptadas por las agencias. La Puerto Rico Innovation and Technology Service emitirá por escrito las recomendaciones y los estándares que correspondan, según sea el caso, para que los proyectos de bases de datos, innovación, información y tecnología de las agencias cumplan con los propósitos de esta Ley y remitirá dicha comunicación al jefe de agencia y al Oficial Principal de Informática de ésta. Las agencias tendrán que diseñar, desarrollar, adoptar e implantar sus proyectos de base de datos, innovación, información y tecnología a tenor con los parámetros y las especificaciones que establezca la Puerto Rico Innovation and Technology Service. Asimismo, dicha Oficina deberá evaluar y aprobar cualquier contratación de servicios o compra de equipo por parte de las agencias a ser utilizado o destinado para un proyecto de base de datos, innovación, información y tecnología.

La Carta Circular Núm. 2020-03, conocida como *Directrices que regirán la evaluación, autorización, adquisición e implementación de los centros de datos ("data centers"), servicios de nube, sistemas de telefonía, infraestructura de redes, equipos y servicios de seguridad informática, digitalización de trámites y servicios, plataformas de datos, páginas y portales web, aplicaciones móviles, servicios, aplicaciones y sistemas de informática en general, entre otros*[39]. En esta carta se establecía, entre otras cosas, lo siguiente:

Base Legal

El cumplimiento con la presente Carta Circular y la Ley-75 es indispensable, pues una de las consecuencias de su incumplimiento es que: "[n]inguna propuesta de desarrollo de las tecnologías de información y comunicación o contrato para la prestación de servicios de las tecnologías de información y comunicación por

[39] Derogada por la Carta Circular Núm. 2021-06, *Derogación Carta Circular PRITS 2020-003*, emitida el 7 de mayo de 2021.

cualquier Agencia será otorgada sin la revisión y los comentarios previos de la Puerto Rico Innovation and Technology Service.". Véase, Ley-75 en su Artículo 14.

Efecto

La situación comentada tiene el efecto de lo siguiente:

1. Impidió a la PRITS evaluar y autorizar el contrato para proveer los servicios a través de la plataforma VitalChek y proteger los mejores intereses del gobierno según requerido en la Ley Núm. 75-2019.

2. Expone al Departamento al riesgo, entre otros, de que los servicios contratados no cumplan con los estándares tecnológicos relativos a las tecnologías de información y comunicación que adopta y promulga la PRITS, lo que pudiera resultar en posibles deficiencias en la seguridad de la información.

3. Impidió a la PRITS evaluar si el uso de la plataforma https://www.vitalchek.com/v/vital-records/puerto-rico#agencies cumplía con las normas establecidas sobre el dominio oficial que deben operar las páginas electrónicas de las entidades gubernamentales (pr.gov), según establecido en la Política Núm. ATI-006, sobre el *Desarrollo Integración y Publicación de Transacciones Electrónicas Gubernamentales* y en *Carta Circular Núm. 2021-004, sobre el Dominio oficial del gobierno de Puerto Rico (pr.gov)*. Esta omisión es un efecto directo de haber eludido la revisión de la PRITS en la referida contratación.

4. Pone en riesgo la información suministrada a través de la plataforma Vitalchek, toda vez que PRITS no tiene el alcance para intervenir en dominios fuera de pr.gov, lo que limita completamente su capacidad de respuesta en la eventualidad de ataques de ciberseguridad.

Causa

La situación mencionada se atribuye a la falta de supervisión y control adecuado por parte del personal del Departamento encargado de la preparación y revisión de la contratación gubernamental, así como a la falta de implementación de medidas efectivas para garantizar que todos los contratos cumplan con las normativas de la PRITS.

Comunicación Gerencial

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios al borrador de los hallazgos:

Aceptamos los hallazgos identificados en dicho borrador. . .

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. . .*

Determinación de la OIG

El Hallazgo prevalece, ya que fue aceptado por la gerencia.

Ver la Recomendación 13.

COMUNICACIÓN GERENCIAL

El borrador de los hallazgos de este examen se sometió para comentarios mediante carta enviada el 2 de mayo de 2025 al secretario del Departamento y a la directora ejecutiva del RD.

El 16 de mayo de 2025, se recibió por correo electrónico carta de la directora del RD fechada 9 de mayo de 2025, con los siguientes comentarios:

> *Aceptamos los hallazgos identificados en dicho borrador, reconociendo que varios de ellos corresponden a otras divisiones o áreas de apoyo del Departamento de Salud, tales como la Oficina de Contratos y la Oficina de Informática y Avances Tecnológicos. . .*

El 4 de junio de 2025, se recibió por correo electrónico carta del secretario del Departamento fechada 29 de mayo de 2025, con los siguientes comentarios:

> *Sirva la presente como contestación a la solicitud de referencia. En ella solicita nuestra posición sobre hallazgos de la Oficina del Inspector General de Puerto Rico respecto al Registro Demográfico, la Oficina de Informática y Avances Tecnológicos y la Oficina de Contratos del Departamento de Salud sobre procesos de reglamentación y control interno.*
>
> *Hemos tenido la oportunidad de evaluar el borrador de informe comunicado por la OIG. En esa dirección, informamos que la directora del Registro Demográfico emitió comentarios al borrador de informe el pasado 9 de mayo de 2025, los cuales suscribimos y endosamos. Luego de haber examinado ambos documentos quedamos pendientes a la publicación del informe final y sus recomendaciones, a fin de proceder con la implementación del plan de trabajo que permita corregir los hallazgos señalados. . .*

La OIG está comprometida con velar que las recomendaciones sean debidamente cumplimentadas e implantadas y continuará trabajando con el Departamento y el RD en aras de continuar promoviendo una sana administración.

RECOMENDACIONES

Núm. Rec.	Acción Correctiva Recomendada	Descripción del Hallazgo	Responsable
1	Cumplir con la Orden emitida por la OIG; revisar y radicar el Reglamento 5961 conforme la Ley Núm. 38-2017, asegurando publicación, aprobación y notificación oficial.	Cobro en exceso de derechos (Hallazgo 1)	Secretario del Departamento / Directora RD
2	Diseñar protocolo de control de calidad y métricas de tiempo de expedición; supervisión semanal de casos atrasados.	Deficiencias en expedición de certificados (Hallazgo 2)	Directora RD
3	Implementar autenticación multifactor; revisión semestral de accesos y baja de usuarios inactivos.	Fallas en controles de acceso al sistema (Hallazgo 3)	Directora RD
4	Remitir acuerdos y enmiendas; incluir certificación de causas y medidas preventivas.	Contratos no radicados en OCPR (Hallazgo 4)	Secretario del Departamento
5	Revisar y actualizar Reglamentos 318 y 5961; establecer calendario de revisión periódica cada 3 años.	Reglamentos y procedimientos sin actualizar (Hallazgo 5)	Secretario del Departamento / Oficina Asesores Legales
6	Actualizar y conservar vigente el diagrama de la red.	Deficiencias en diagrama de red (Hallazgo 6)	Directora RD / OIAT
7	Elaborar Plan Estratégico de Tecnología alineado con metas del Departamento.	Ausencia de Plan Estratégico de TI (Hallazgo 7)	Directora RD / OIAT
8	Realizar análisis anual de riesgos con apoyo de OIAT.	Fallas en análisis de riesgos (Hallazgo 8)	Directora RD / OIAT
9	Completar planes y realizar simulacros anuales.	Deficiencias en Plan de Continuidad y Contingencia (Hallazgo 9)	Directora RD / OIAT
10	Establecer sistema automatizado para inventario de hardware y software.	Deficiencias en inventario de sistemas (Hallazgo 10)	Directora RD
11	Implementar programa de adiestramientos anuales en ciberseguridad, con pruebas de phishing y módulos de actualización.	Ausencia de adiestramientos de seguridad (Hallazgo 11)	Directora RD / Recursos Humanos

Núm. Rec.	Acción Correctiva Recomendada	Descripción del Hallazgo	Responsable
12	Reorganizar y rotular cableado de equipos de comunicación.	Falta de organización en cableado (Hallazgo 12)	Directora RD / OIAT
13	Validar cumplimiento de PRITS antes de firmar cualquier contrato; solicitar asistencia técnica especializada.	Contrato de tecnología en incumplimiento PRITS (Hallazgo 13)	Directora RD

CONCLUSIÓN

La evaluación realizada a los documentos y la información recopilada durante el examen reflejó incumplimiento con leyes y reglamentos aplicables al Departamento y al RD respecto al manejo y los controles en los sistemas digitales, particularmente de aquellos relacionados con las solicitudes de los certificados de eventos vitales y la evaluación de los procesos subsiguientes hasta que los ciudadanos reciban los certificados luego de efectuar los pagos correspondientes.

Será responsabilidad de la gerencia corregir las deficiencias presentadas para evitar que situaciones como las comentadas en los hallazgos se repitan.

Conforme con lo establecido en el Artículo 17 de la precitada Ley Núm. 15-2017 se remite el presente informe a la autoridad nominadora para que inicie las medidas correctivas pertinentes al incumplimiento de procedimientos internos por parte de sus empleados y notifique a la OIG las acciones tomadas para garantizar el fiel cumplimiento con las leyes y reglamentos aplicables. El incumplimiento con tomar medidas correctivas ante las situaciones aquí señaladas podría ocasionar la imposición de multas y procesos administrativos.

APROBACIÓN

El presente informe es aprobado en virtud de los poderes conferidos por la Ley Núm. 15-2017. Será responsabilidad de los funcionarios, empleados o cuerpo rector del gobierno de cada entidad, observar y procurar por que se cumpla cabalmente con la política pública. De la misma manera, establecer los controles y mecanismos adecuados para garantizar su cumplimiento. Será el deber, además, de cada uno de éstos, de los demás funcionarios y servidores públicos, el poner en vigor las normas, prácticas y estándares que promulgue la OIG, así como de las recomendaciones, medidas y planes de acción correctiva que surjan de las evaluaciones.

Hoy, 3 de octubre de 2025, en San Juan, Puerto Rico.

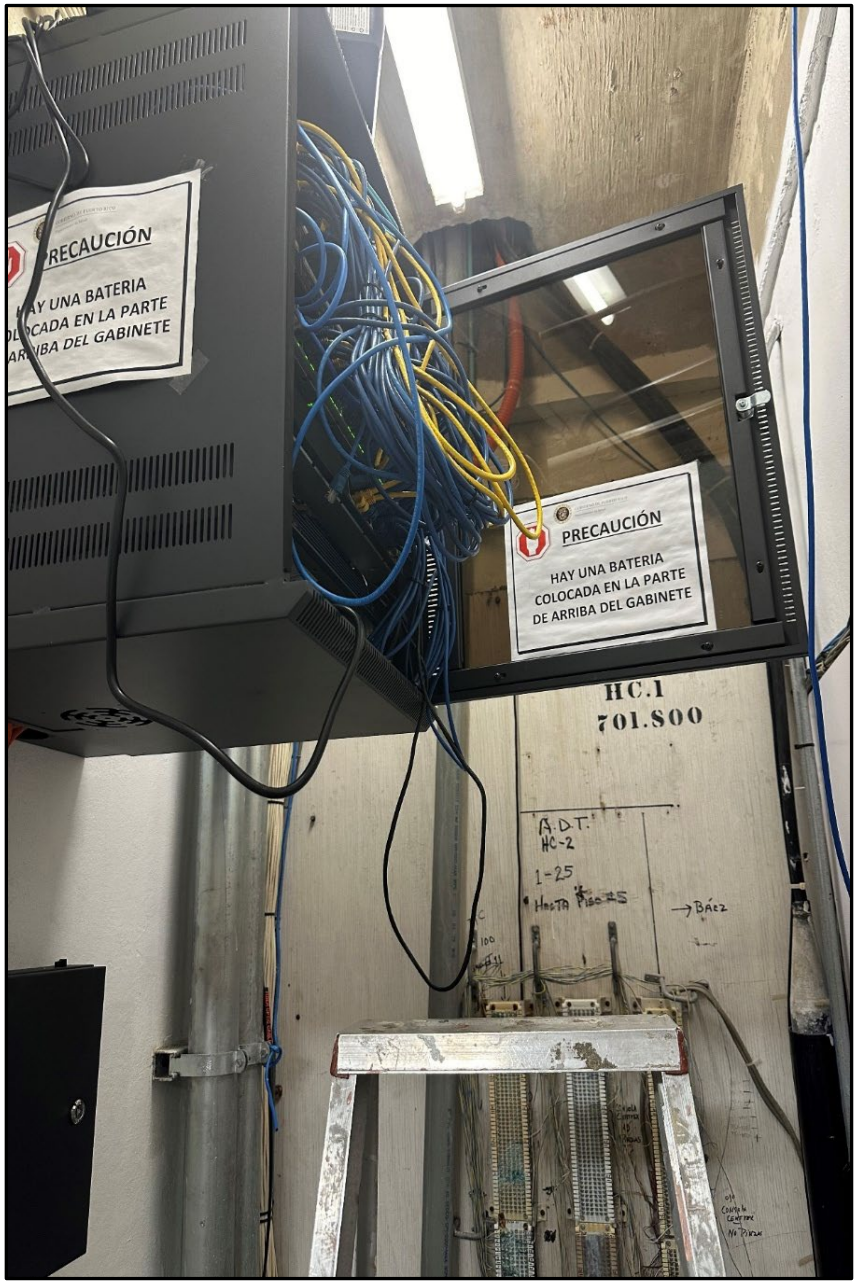
Ivelisse Torres Rivera, CIG, CIA, CFE, CICA
Inspectora General

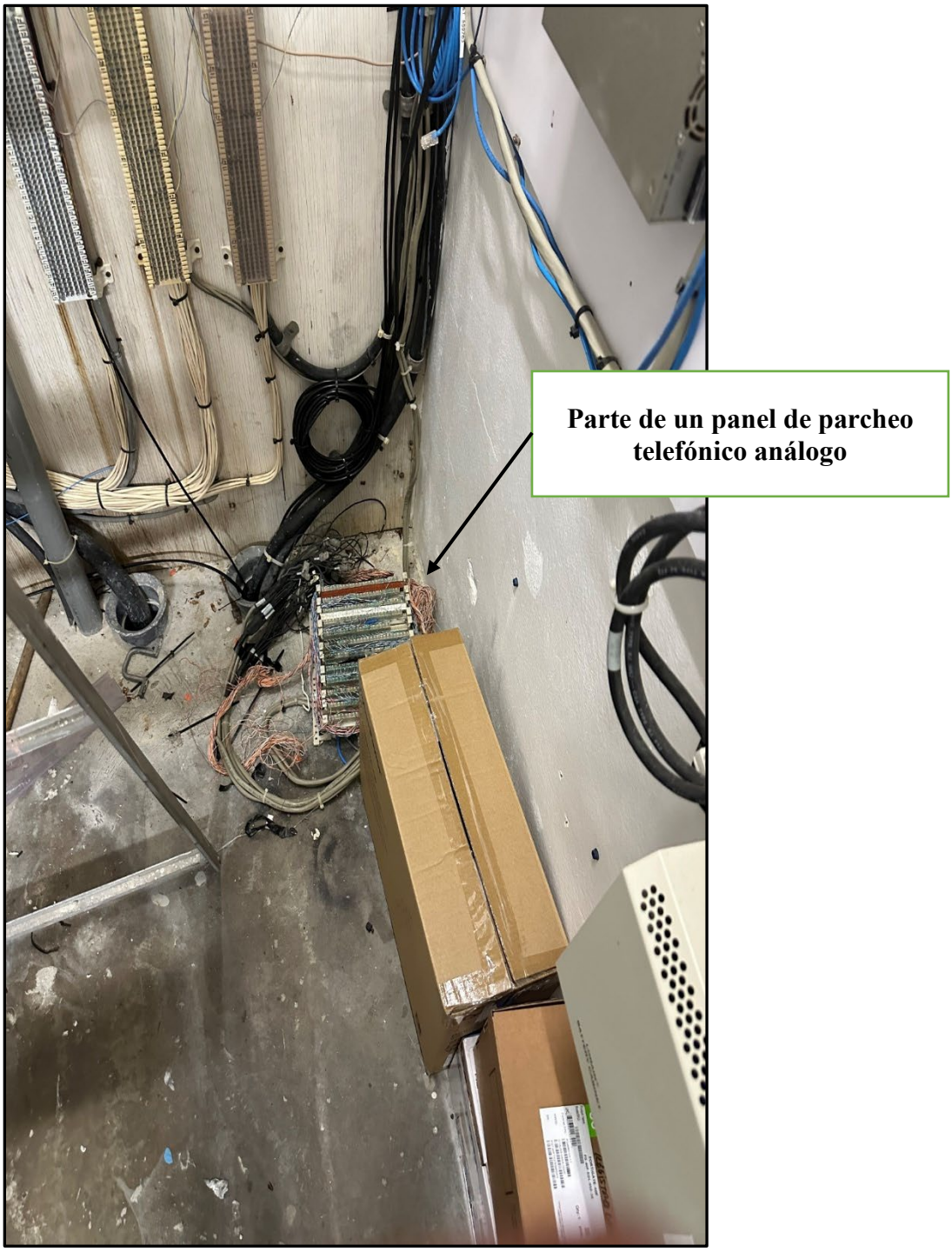
Dayanette Faisca Montalvo, CIGA, CAMS
Directora Área de Pre-Intervención y Exámenes

ANEJO 1

Edificio Oficina Central del RD

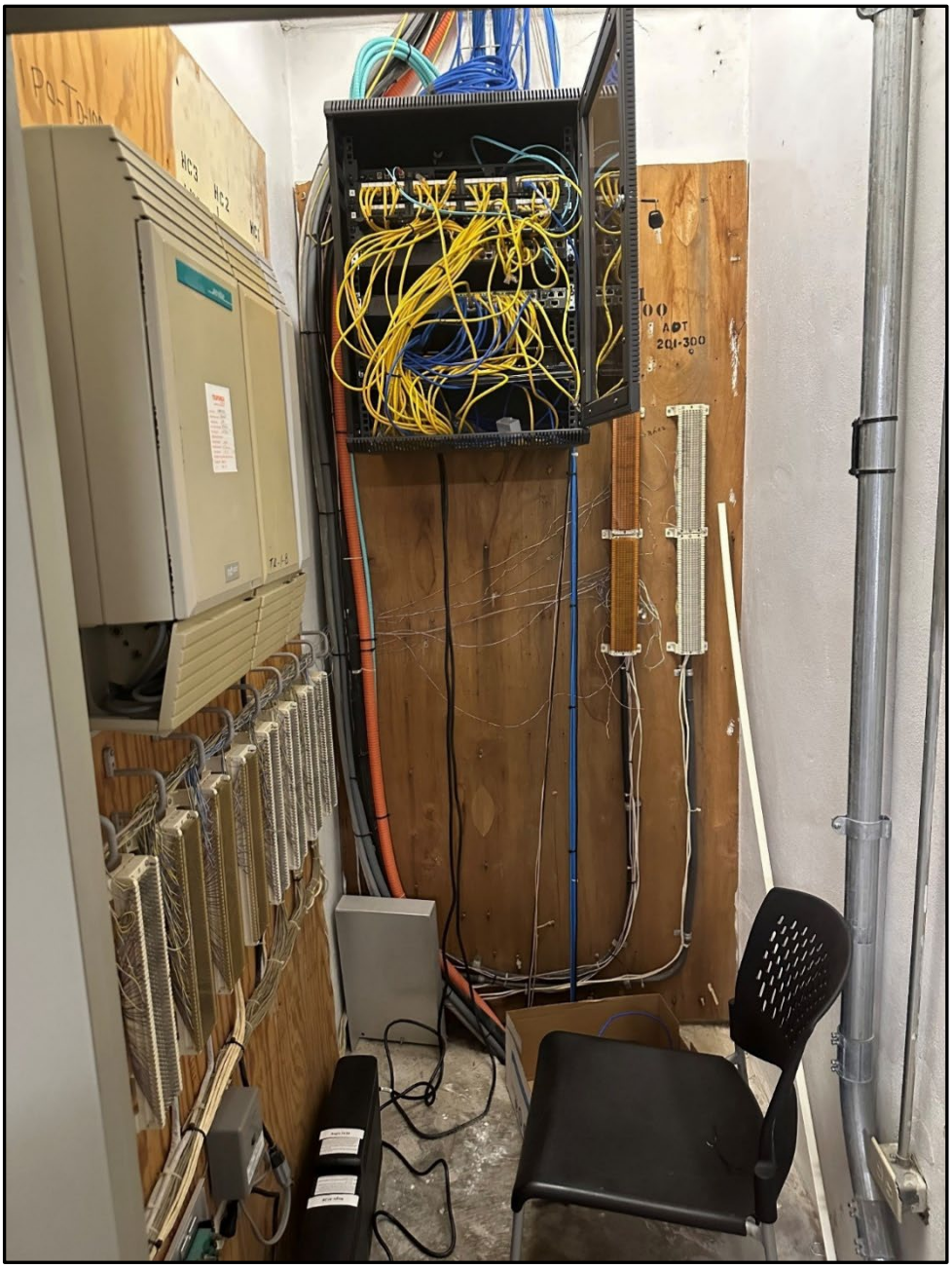
Piso 4




Parte de un panel de parcheo telefónico análogo

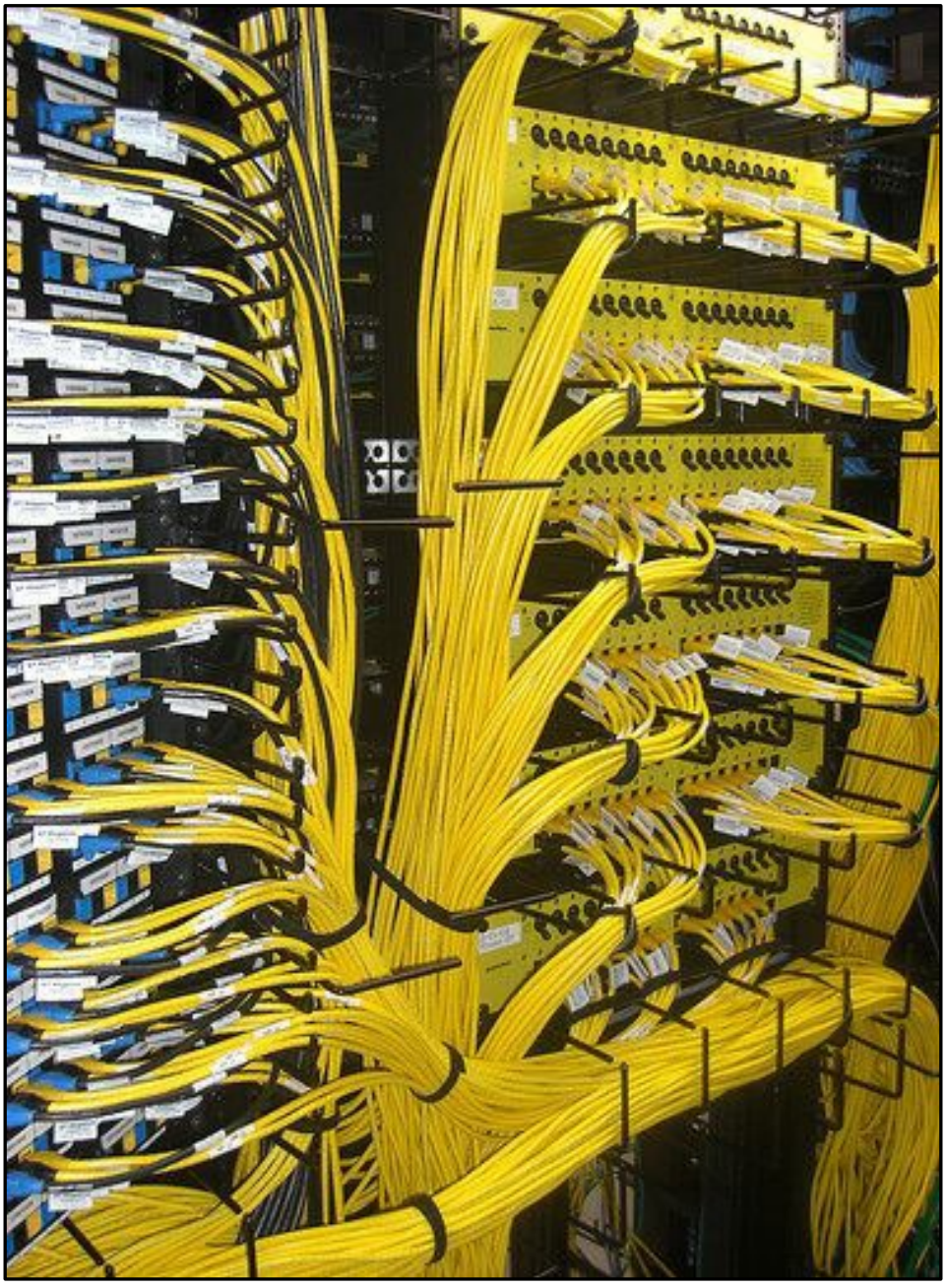

A.D.T.
HC-2
BÁEZ

Piso 9



ANEJO 2

Ejemplo de un panel de conexión con el cableado organizado



INFORMACIÓN GENERAL

Oficina del Inspector General
Gobierno de Puerto Rico

MISIÓN

Ejecutar nuestras funciones de manera objetiva, independiente y oportuna promoviendo mejorar la eficiencia, eficacia e integridad de las entidades bajo nuestra jurisdicción y el servicio público.

VISIÓN

Fomentar una cultura de excelencia mediante la capacitación, observación, fiscalización y desarrollo de sanas prácticas administrativas. Mantener los acuerdos con entidades locales e internacionales para fomentar acciones preventivas en el monitoreo continuo de los fondos del Gobierno de Puerto Rico.

INFORMA

La Oficina del Inspector General tiene el compromiso de promover una sana administración pública. Por lo que, cualquier persona que tenga información sobre un acto irregular o falta de controles internos en las operaciones de la Rama Ejecutiva, puede comunicarse a la OIG a través de:

Línea confidencial: 787-679-7979
Correo electrónico: informa@oig.pr.gov
Página electrónica: www.oig.pr.gov/informa

CONTACTOS

PO Box 191733
San Juan, Puerto Rico
00919-1733

787-679-7997

Ave Arterial Hostos 249
Esquina Chardón Edificio ACAA
Piso 7, San Juan, Puerto Rico

consultas@oig.pr.gov

www.oig.pr.gov