INFORME DE EXAMEN OIG-E-26-009

Oficina del Inspector General
Gobierno de Puerto Rico

Registro Inmobiliario Digital de PR

Adscrito al Departamento de Justicia

Examen sobre evaluación de los controles internos relacionados al sistema *Karibe* y registro inmobiliario.

3 de junio de 2026

TABLA DE CONTENIDO

PÁGINA

RESUMEN EJECUTIVO

El Área de Pre-Intervención y Exámenes (Área de PIE) de la Oficina del Inspector General de Puerto Rico (OIG) realizó un examen en el Registro Inmobiliario Digital de Puerto Rico (Registro), adscrito al Departamento de Justicia para evaluar los controles internos del sistema *Karibe*.

El examen realizado reveló deficiencias en controles internos e incumplimientos con leyes y reglamentos aplicables, que afectan la confiabilidad y la eficiencia de los procesos. Los hallazgos principales fueron los siguientes:

- Deficiencias en la expedición, uso y manejo de las cartas de crédito.
- Deficiencias relacionadas con la creación, mantenimiento y cancelación de accesos a los sistemas de información del Departamento de Justicia.
- Falta de controles en la Oficina del *Helpdesk-Karibe*.
- Deficiencias en la seguridad del sistema *Karibe.*
- Ausencia de mecanismos de cifrado de datos en reposo.
- Ausencia de un software o aplicación para manejo de cambios al sistema *Karibe.*

Conforme con lo establecido en el Artículo 17 de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (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 Núm. 15-2017, según enmendada, y otras normativas aplicables.

INFORMACIÓN SOBRE LA ENTIDAD EXAMINADA

En el Artículo 34 de la Ley Núm. 205-2004, *Ley Orgánica del Departamento de Justicia*, según enmendada, se faculta al secretario para establecer la organización y estructura interna del Departamento para el mejor cumplimiento de las funciones que le impone la ley, ello con sujeción a las normas y guías que apliquen sobre la organización de la Rama Ejecutiva. Además, de los que se establecen en esta Ley, se incorporan y se hacen formar parte funcional de la estructura administrativa del Departamento otros componentes como, el Registro de la Propiedad (Registro) creado por la Ley Núm. 198 de 8 de agosto de 1979, derogada y sustituida por la Ley Núm. 210-2015, según enmendada, conocida como *Ley del Registro de la Propiedad Inmobiliaria del Estado Libre Asociado de Puerto Rico*.

La Ley Núm. 210-2015 se crea con el propósito de establecer todos los procesos llevados a cabo en el Registro de manera telemática. Mediante esta Ley Núm. 210-2015, se crea el Registro Inmobiliario Digital del Estado Libre Asociado de Puerto Rico.

El Registro contiene un sistema de publicidad de títulos que incluye las adquisiciones, modificaciones y extinciones del dominio y de los demás derechos reales que recaen sobre dichos bienes. El Registro, además, provee para la inscripción o anotación de otros derechos sobre o relacionados a bienes inmuebles, conforme se indica en la Ley.

El Registro funciona bajo la dirección de un director administrativo nombrado por el secretario de Justicia. En consulta con el secretario, el director administrativo tendrá a su cargo la organización, formulación del presupuesto, administración y funcionamiento del Registro. Previa autorización por parte del secretario, el director podrá emitir reglas provisionales para la operación de modos alternos o experimentales o de procesos de transición en el Registro.

El Registro tiene como base la finca como unidad registral y está organizado en 14 oficinas regionales con 29 secciones. Cada sección estará a cargo de un registrador de la propiedad y en ella se inmatricularán las fincas que radiquen en su demarcación territorial.

Las funciones administrativas y fiscales de cada una de las secciones del Registro son realizadas por 1 registrador, 1 supervisor, 1 certificador y los técnicos de la sección.

Mediante la Orden Administrativa Núm. 2018-12 (OA-2018-12) aprobada el 21 de diciembre de 2018 por la secretaria de Justicia, se estableció la *Sede Metropolitana del Registro de la Propiedad* para integrar en una sola estructura la Oficina Administrativa, el *Helpdesk-Karibe*, y otras secciones del Registro, con el propósito de centralizar áreas y servicios. Conforme a dicha orden, la Oficina de *Helpdesk-Karibe* debía funcionar dentro de la estructura operacional de la Oficina Administrativa del Registro de la Propiedad y tener a su cargo brindar asistencia a los usuarios, al personal y a los registradores en el uso del sistema *Karibe*.

El 30 de octubre de 2025, la secretaria de Justicia promulgó la Orden Administrativa 2025-12 (OA-2025-12) a los fines de formalizar el funcionamiento de la Oficina del *Help Desk*, adscrita al Registro. Entre los objetivos principales del *Help Desk* se encuentran los siguientes: (1) el ofrecimiento de un servicio de apoyo y orientación relacionados a los asuntos registrales, (2) servicio de apoyo sobre el uso del sistema de información registral, y (3) la solución de incidencias tecnológicas para los usuarios internos y externos. A su vez, apoyar y mantener el sistema de información registral operacional.

DETALLES DE LA INTERVENCIÓN

Previo a la aprobación de la Ley Núm. 210-2015 existía un sistema llamado Ágora. Este era un sistema digital en el cual se realizaba todo el proceso relacionado a las transacciones que se llevan a cabo en el Registro. Aunque era un sistema digital tenían que imprimir todo lo que se realizaba a través de este sistema y encuadernar la información que surgía del mismo. No es hasta la creación de la Ley Núm. 210-2015 que se crea el sistema de informática llamado *Karibe*.

El sistema *Karibe*, implementado en marzo de 2016, contempla la facilitación y automatización de los procesos, así como el acceso a las constancias del Registro mediante la centralización de los datos. Esta permite a notarios y otros usuarios registrados realizar trámites relacionados con la propiedad, como la presentación de escrituras, estudios de títulos y búsqueda de propiedades, de forma digital.

El desarrollo, cambios y mantenimiento del sistema *Karibe* es gestionado por contratistas. El director de la Oficina de Informática del Departamento de Justicia es el custodio de los servidores donde reside la aplicación *Karibe* y responsable de otorgar los accesos necesarios para estos fines, una vez aprobados por el director administrativo del Registro. El director de la Oficina de Informática responde a un Principal Oficial de Tecnología e Informática (*Chief Information Officer – CIO*[1]) o en su lugar, al secretario de Justicia.

El servicio a los usuarios internos y externos está a cargo de la Oficina de *HelpDesk-Karibe*, cuyo personal responde directamente al director administrativo del Registro.

Este examen está dirigido a evaluar los controles internos y de cumplimiento relacionados con el sistema *Karibe.*

[1] Los secretarios de Justicia en funciones promulgaron las órdenes administrativas Núm. 2017-11 y Núm. 2025-10 para crear y denominar al *Principal Asesor en Tecnología* como *Principal Oficial de Tecnología e Informática (Chief Information Officer -CIO).* El 29 de octubre de 2025, el director administrativo del Registro certificó que el puesto de Funcionario de Tecnología de Información del Departamento de Justicia no ha sido designado. Según informó el Área de Recursos Humanos, el último CIO nombrado desempeñó tales funciones entre los años 2020 y 2021.

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 determinar el cumplimiento con las regulaciones aplicables, y determinar la efectividad de los controles internos implementados por el Registro y el Departamento de Justicia relacionados con el sistema *Karibe*.

Las regulaciones aplicables durante el período examinado son las siguientes:

1. Ley Núm. 205 de 9 de agosto de 2004, según enmendada, conocida como *Ley Orgánica del Departamento de Justicia.*

2. Ley Núm. 209 de 8 de diciembre de 2015, según enmendada, conocida como *Ley de Aranceles.*

3. Ley Núm. 210 de 8 de diciembre de 2015, según enmendada, conocida como *Ley del Registro de la Propiedad Inmobiliaria del Estado Libre Asociado de Puerto Rico.*

4. Ley Núm. 216 de 27 de diciembre de 2010, según enmendada, conocida como *Ley para Agilizar el Registro de la Propiedad.*

5. Ley Núm. 230 de 23 de julio de 1974, según enmendada, conocida como *Ley de Contabilidad del Gobierno de Puerto Rico.*

6. Ley Núm. 75 de 25 de julio de 2019, según enmendada, conocida como *Ley de la Puerto Rico Innovation and Technology Service (PRITS).*

7. Ley Núm. 40 de 18 de enero de 2024, según enmendada, conocida como *Ley de Ciberseguridad del Estado Libre Asociado del Puerto Rico.*

8. Reglamento Núm. 8714 aprobado el 8 de marzo de 2016 por el secretario de Estado, conocido como *Reglamento General para la Aplicación de la Ley Núm. 209-2015.*

9. Reglamento Núm. 8814 aprobado el 14 de septiembre de 2016 por el secretario de Estado, *Reglamento General para la Ejecución de la Ley del Registro de la Propiedad Inmobiliaria.*

10. Orden Administrativa Núm. 2017-11 promulgada por la secretaria de Justicia el 27 de diciembre de 2017, *Para la Creación de la Figura del Principal Asesor en Tecnología (Chief Information Officer - CIO).*

11. Orden Administrativa Núm. 2018-10 promulgada por la secretaria de Justicia el 31 de octubre de 2018, *Para establecer las Políticas Aplicables a Servicios de Tecnología Administrados por el Departamento de Justicia.*

12. Orden Administrativa Núm. 2018-12 promulgada por la secretaria de Justicia el 31 de diciembre de 2018, *Para establecer la Sede Metropolitana del Registro de la Propiedad.*

13. Orden Administrativa Núm. 2025-10 promulgada por la secretaria de Justicia el 30 de septiembre de 2025, *Para denominar al Principal Asesor en Tecnología como Principal Oficial de Tecnología e Informática (Chief Information Officer -CIO) y delimitar y precisar sus funciones; y para reiterar las funciones y facultades de la oficina de informática del departamento de justicia y el sistema de información de justicia criminal.*

14. Política TI-PRITS-006 de 30 de junio de 2023, *Política para la Gestión* de *Cambios.*

15. Política TI-PRITS-007 de 24 de enero de 2024, *Política de gestión de acceso, identidad y credenciales*.

16. *Estándares para la Seguridad Cibernética* promulgados por PRITS el 15 de mayo de 2023.

17. GAO 24-107026 – September 2024, *Federal Information System Controls Audit Manual (FISCAM).*

18. NIST Special Publication 800-53 (Revision 5) – September 2020, *Security and Privacy Controls for Information Systems and Organizations.*

19. *Procedimiento para la Creación de la Cuenta de/ Usuario "username" y Contraseña "Password"* emitido por el Departamento de Justicia (sin fecha).

20. *Manual de las Normas, Procedimientos y Políticas de Seguridad,* aprobado por la secretaria de Justicia el 10 de octubre de 2019.

21. Memorando del Director Administrativo del Registro de la Propiedad de 22 de mayo de 2020, *Recibo en las Secciones de Cartas de Crédito, Comprobantes Físicos y Documentos Físicos para Corregir Asientos Durante el Cierre de las Operaciones en el Registro.*

ALCANCE Y METODOLOGÍA DEL EXAMEN

El examen cubrió el período del 1 de enero de 2023 al 21 de enero de 2026.

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:

1. Estudio de las leyes, reglamentos y procedimientos aplicables al objetivo del examen.
2. Evaluación de los controles internos adoptados y el cumplimiento con las normativas aplicables, relacionados con el sistema *Karibe*.
3. Evaluación de los procesos de expedición, uso y manejo de las cartas de crédito.
4. Entrevistas a contratistas, funcionarios y empleados del Departamento de Justicia y del Registro.
5. Análisis de informes, certificaciones y documentos provistos por el Departamento de Justicia y el Registro.
6. Validación de información obtenida.
7. Otros análisis dependiendo de las circunstancias.

En algunos aspectos, se examinaron transacciones, documentos y operaciones de fechas anteriores y posteriores, relacionados al objetivo de la intervención.

HALLAZGOS

A continuación, se detallan los hallazgos relacionados con las situaciones detectadas durante el transcurso del presente examen.

Hallazgo 1 – Deficiencias en la expedición, uso y manejo de las cartas de crédito

Situación

Las cartas de crédito de *Karibe* son aquellas que emite el sistema en ocasión del retiro de un documento o cuando se inscribe un documento con aranceles pagados en exceso. Una vez presentado un documento, los aranceles quedan cancelados.

La carta de crédito podrá utilizarse únicamente para el pago de aranceles de documentos presentados personalmente en el Registro Inmobiliario Digital (Registro) y podrá combinarse con otros comprobantes para completar los derechos de inscripción de documentos. La carta de crédito no podrá utilizarse por vía telemática[2] en la presentación de documentos o para la solicitud de certificaciones registrales. Tampoco se permitirá su uso para el pago de otros derechos requeridos por otras agencias o ramas de gobierno.

[2] Se refiere al uso de medios electrónicos para gestionar trámites, comunicaciones y servicios con las entidades gubernamentales. Esto incluye desde la presentación de solicitudes hasta la recepción de notificaciones, todo a través de plataformas digitales.

En aquellos casos en que el recipiente de la carta de crédito no tenga interés de utilizarla en el Registro, podrá solicitar el crédito correspondiente al secretario del Departamento de Hacienda de conformidad con lo establecido en el Artículo 6 de la Ley Núm. 209-2015.

El 20 de junio de 2025, el Registro proveyó un informe de cartas de crédito emitidas entre el 1 de julio de 2023 y el 6 de mayo de 2025, correspondiente al período de examen, según se indica a continuación:

Figura 1 – Universo de cartas de crédito emitidas durante el período de examen

Cartas de Crédito del Sistema *Karibe* 1 de julio de 2023 al 6 de mayo de 2025		
Cartas de Crédito	**Total**	**Importe**
Canceladas	35	$ 50,150.00
Redimidas	11,587	$ 3,001,484.10
Sin Redimir	22,452	$ 3,663,690.75
Total	**34,074**	**$ 6,715, 324.85**

El examen realizado a los procesos de expedición, uso y manejo de las cartas de crédito reveló lo siguiente:

a. El sistema *Karibe* está configurado de manera que, de generarse una carta de crédito el presentante indique a quién se notificará y enviará la carta. Al momento de realizar la presentación, el sistema ofrece al presentante seleccionar 1 de 3 opciones como destinatario de la carta de crédito. Estos son: (1) el notario, (2) el presentante, (3) otro. Esta selección se realiza dentro del módulo de presentación, y determina a quién se notificará y enviará la carta de crédito. El sistema envía una notificación al correo electrónico del destinatario seleccionado, indicando que se ha generado un crédito, y se adjunta la carta de crédito en formato PDF. No obstante, la carta de crédito generada no indica a favor de quién fue expedida, lo que permite que esta sea utilizada por una persona distinta a la indicada por el presentante en las opciones previamente mencionadas.

   Conforme a las entrevistas realizadas, el proceso de validación de una carta de crédito se limita a ingresar el número de serie y confirmar que la carta no haya sido previamente redimida, así como de verificar que el importe coincida con el registrado en el sistema. Sin embargo, no se valida la identidad del solicitante ni se requiere evidencia de autorización del presentante, lo que permite que la carta de crédito sea redimida por el portador.

   En una muestra de 47 cartas de crédito con importes entre $5,070 y $49,544 se observó que 2 cartas por un monto total de $26,850 fueron redimidas en nuevas presentaciones de documentos por un notario o presentante distinto al que se había designado originalmente para recibir la notificación de la carta de crédito.

b. Todo usuario, con credenciales de técnico, supervisor y registrador en el sistema *Karibe* tiene acceso al módulo que contiene las cartas de crédito redimidas y sin redimir. Dicho acceso permite la descarga e impresión de las cartas sin redimir, sin restricción alguna y sin requerir la aprobación de un nivel superior como medida de control. Para el período del 1 de julio de 2023 al 6 de mayo de 2025, se encontraban sin redimir 22,452 cartas de crédito por un total de $3,663,690.75.

Criterio

Las situaciones comentadas son contrarias al Artículo 2, incisos (f) y (g), de la Ley Núm. 230 del 23 de julio de 1974, según enmendada, conocida como *Ley de Contabilidad del Gobierno de Puerto Rico* (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 pública 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.*

Además, es contraria a la Regla 267.5 del Reglamento Núm. 8814, *Reglamento General Para la Ejecución de la Ley del Registro de la Propiedad Inmobiliaria,* aprobado el 14 de septiembre de 2016 por el Departamento de Estado, que establece lo siguiente:

> **Regla 267.5 – Carta de crédito; expedición; uso y prohibición**
>
> *La carta de crédito por el retiro de los documentos aplicará para todos los documentos pendientes de inscripción en el registro, independientemente de la fecha de su presentación.*

Toda carta de crédito se expedirá a favor del notario autorizante del documento presentado salvo que el notario presentante expresamente disponga en la sección de observaciones del módulo de presentación del sistema de informática registral que cualquier crédito relacionado con esa transacción se expida a su nombre o de otra persona.

El uso de la carta de crédito estará limitado para el pago de los derechos de inscripción de los documentos que se presenten por la vía presencial y podrá combinarse con otros comprobantes para completar los derechos de inscripción correspondientes. Se prohíbe su uso en la presentación por la vía telemática y para la solicitud de certificaciones registrales.

Efecto

Las situaciones comentadas tienen el *efecto* de lo siguiente:

1. Genera confusión sobre la titularidad del crédito, lo que facilita su uso indebido por personas no autorizadas y genera riesgo de redención por terceros sin autorización.

2. Exposición a reclamaciones legales y disputas, colocando al Registro en desventaja institucional ante controversias, especialmente si notarios o presentantes reclaman uso indebido.

3. Uso incorrecto de cartas de crédito y otras irregularidades operacionales, afectando la transparencia y credibilidad del proceso registral.

Causa

Las situaciones comentadas se atribuyen a lo siguiente:

1. Falta de una supervisión efectiva de las operaciones relacionadas con el control, manejo y uso de las cartas de crédito.

2. El director administrativo del Registro no había impartido las debidas instrucciones, de manera que la configuración del sistema *Karibe* provea para que la carta de crédito generada indique a favor de quién fue expedida, contrario a lo establecido en la Regla 267.5 del Reglamento 8814.

3. Ausencia de un mecanismo de validación que confirme a quién corresponde el crédito al momento de su redención.

Comunicación Gerencial

El 21 de enero de 2026 recibimos del director administrativo del Registro, previa aprobación de la secretaria de Justicia, los comentarios al borrador de los hallazgos, y citamos:

> *Se implementarán mecanismos para que las cartas de crédito se expidan con el nombre del notario u otra persona, según se disponga en la presentación, a tenor con la Regla 267.5 del Reglamento para la ejecución de la Ley 210-2015. Asimismo, se limitará la visualización de datos sensibles, como la numeración de las cartas de crédito, para controlar el acceso. La impresión y descarga se restringirá exclusivamente al rol de Registrador. Estos cambios requerirán de ajustes en la programación del Sistema Karibe, los cuales se trabajarán en coordinación con la compañía proveedora del servicio, garantizando la seguridad y funcionalidad del sistema.*

Determinación de la OIG

Se consideraron los comentarios del director administrativo del Registro; no obstante, la OIG determinó que el hallazgo prevalece. Se reconoce el compromiso del Registro de configurar el sistema *Karibe* para que la carta de crédito se expida a nombre del beneficiario que disponga la presentación y de restringir su impresión y descarga al rol de Registrador. Sin embargo, la propia respuesta gerencial admite que estas medidas requieren ajustes de programación aún pendientes, por lo que, a la fecha de emisión de este informe, se encuentran en etapa de planificación y sin evidencia de implementación ni efectividad, lo que confirma que subsiste el incumplimiento con la Regla 267.5 del Reglamento Núm. 8814.

Además, las acciones propuestas no atienden la ausencia de un mecanismo de validación de identidad al momento de la redención, deficiencia que permitió que dos cartas, por $26,850, fueran redimidas por un presentante distinto al designado, ni mitigan la exposición de las 22,452 cartas sin redimir por $3,663,690.75 que permanecen accesibles para descarga e impresión sin aprobación de un nivel superior. En ausencia de evidencia de controles implementados y operantes, persisten las debilidades que comprometen la corrección y propiedad de las operaciones fiscales del Registro, conforme al Artículo 2, incisos (f) y (g), de la Ley Núm. 230 de 1974, por lo que el hallazgo prevalece.

Ver la Recomendación 1.

Hallazgo 2 - Deficiencias relacionadas con la creación, mantenimiento y cancelación de accesos a los sistemas de información del Departamento de Justicia

Situación

Al 27 de junio de 2025, el Registro contaba con 333 cuentas de acceso activas en el sistema *Karibe* que incluían empleados, consultores o contratistas, cuentas de servicio o genéricas, entre otros.

De estas, 11 correspondían a cuentas con privilegios administrativos, incluyendo 4 cuentas con roles de superadministrador y 7 con roles de administrador del sistema *Karibe*. Una cuenta con privilegios administrativos es aquella con accesos completos destinada a realizar tareas de administración legítimas, tales como la instalación de programas y actualizaciones, administración de cuentas de usuario, modificación del sistema operativo ("OS", en inglés) y configuración de aplicaciones, entre otros.[3] Las cuentas administrativas correspondían a:

Figura 2 – Once (11) cuentas administrativas del sistema *Karibe*

Rol	Fecha de creación	Propósito o función	Usuarios
Superadministrador	28-abr-2015	Personal de la Oficina de *Helpdesk-Karibe.* Servicios de apoyo a usuarios internos y externos.	4
Administrador	28-abr-2015		2
Administrador	18-sep-2014	Cuenta genérica utilizada para la reasignación de casos.	1
Administrador	28-abr-2015	Director Administrativo del Registro.	1
Administrador	29-jun-2022 20-mar-2025	Contrato con compañía de Programación y mantenimiento de la base de datos. Desde 31-mar-2022 al 30-jun-2025.	2
Administrador	1-ago-2016	Contratista Oficina de Informática del DJ. Desde 1-ago-2016 hasta 31-dic-2024. Validación y Mantenimiento de Sistema *Karibe*.	1
		Total	**11**

[3] *TI-PRITS-007 Política de gestión de acceso, identidad y credenciales, 5. Definiciones, 5.9 Cuenta Administrativa*

El examen realizado a los procesos de creación, mantenimiento y cancelación de cuentas de acceso a los sistemas de información reveló lo siguiente:

a. El Registro no suministró la documentación ni instrucciones formales para la autorización y manejo de las 11 cuentas con privilegios administrativos. El 24 de septiembre de 2024, el director administrativo certificó lo siguiente:

> *Las solicitudes de creación u otorgación del rol de superadministrador o administrador de los usuarios incluidos en el Requerimiento […] no se incluyen debido a que se gestionaron directamente en la base de datos de la aplicación Karibe por los programadores, siguiendo las funciones del personal de Help Desk. Los roles de […] e […] fueron modificados tras su transferencia a la oficina del Help Desk.*

b. El usuario y contraseña de la cuenta administrativa genérica era compartida por 2 empleadas de la Oficina de *Helpdesk-Karibe* quienes a su vez tenían asignadas cuentas de superadministradores.

c. Las cuentas asignadas a 3 contratistas estaban vinculadas a sus correos electrónicos privados. La Oficina de Informática no les creó cuentas institucionales con el dominio *@justicia.pr.gov* para ser utilizadas durante los trabajos que requerían acceso al manejo de los sistemas de información del Gobierno.

d. Al 18 de junio de 2025, la cuenta de un consultor con privilegios de administrador del sistema *Karibe* permanecía activa en el perfil del usuario, a pesar de que su contrato había vencido el 31 de diciembre de 2024.

e. En la revisión de 44 cuentas correspondientes a exempleados adscritos al Registro que cesaron sus funciones entre el 1 de julio de 2023 y el 31 de mayo de 2025, se validó que la cuenta de un empleado cuyas funciones culminaron el 12 de septiembre de 2023, fue desactivada 292 días después de su salida. La Oficina de Informática, responsable de cancelar los accesos a la red del Departamento de Justicia, no proveyó el formulario *Certificación de Devolución de Propiedad*, utilizado para certificar la cancelación de accesos a los sistemas, redes y servicios institucionales, según lo establecido en el procedimiento aplicable.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la Política TI-PRITS-007, *Política de gestión de acceso, identidad y credenciales*, aprobada el 24 de enero de 2024, según se indica:

> ***7. PROCESOS REQUERIDOS***
>
> ***7.1 Control 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.

[…]

7.1.6 Se revisarán periódicamente las configuraciones y controles de acceso para garantizar su alineación con las necesidades y autorizaciones vigentes.

7.2 Gestión de cuentas

[…]

7.2.3 La creación de cuentas de usuarios y las modificaciones de accesos deberán documentarse y/o registrarse adecuadamente.

[…]

7.2.5 Las agencias deberán contar con documentación e instrucciones formales para la autorización y gestión de cuentas con privilegios de administrador o acceso especial. Esto incluye la creación, asignación, uso y eliminación de dichas cuentas con capacidades elevadas.

7.2.6 Las agencias deberán proporcionar una cuenta de usuario a cada persona que trabaje para el proveedor de servicios que requiera acceso para el manejo de los sistemas de información del Gobierno, incluyendo, pero sin limitarse a, manejo de bases de datos y servidores, configuración de aplicaciones, entre otros, según la normativa establecida por PRITS

7. PROCESOS REQUERIDOS

7.3 Cuentas

7.3.1 General

[…]

7.3.1.3 No se permitirán cuentas compartidas.

[…]

7.3.2 Administrativas

7.3.2.1 Las credenciales de cuentas administrativas o con privilegios elevados sólo podrán ser usadas por un (1) administrador en el ejercicio de sus funciones. No se

compartirán excepto en el estricto cumplimiento de procedimientos de cambio de control, recuperación ante desastres y/o continuidad de operaciones gubernamentales.

[…]

7.3.2.3 Las personas con cuentas administrativas deberán utilizar la cuenta con el mínimo nivel de privilegios necesario para realizar sus tareas (por ejemplo, cuenta de usuario en lugar de cuenta de administrador).

[…]

7.3.3 Proveedor de servicios

7.3.3.1 Los proveedores de servicios deberán utilizar la cuenta provista bajo el dominio del Gobierno para la prestación de los servicios a las agencias. No se aceptarán cuentas de entidades externas al Gobierno.

También, es contraria a los establecido en los *Estándares para la Seguridad Cibernética* promulgados por la PRITS el 15 de mayo de 2023, según se indica:

3.4 Servicios Contratados

[…]

3.4.5 La agencia será responsable de determinar cuándo un contratista o un tercero requiere acceso a una aplicación o sistema de información en particular, y cualquier otro aspecto del entorno de TI de la agencia. […] El acceso será limitado en alcance y tiempo, de acuerdo con los servicios a ser prestados por el contratista, ***y será modificado o revocado cuando corresponda****.* (Énfasis nuestro)

3.5 Controles Adicionales de TI

[…]

3.5.7 Los privilegios de acceso de los usuarios se reevaluarán periódicamente. El acceso empleará el principio de privilegio mínimo, permitiendo a los usuarios autorizados acceder solo a los datos y aplicaciones que son necesarios para realizar sus tareas y funciones.

El 31 de octubre de 2018, la secretaria de Justicia promulgó la Orden Administrativa Núm. 2018-10 (OA-2018-10) titulada, *Políticas Aplicables a Servicios de Tecnología Administrados por el Departamento de Justicia*, con el propósito de requerir al personal de la agencia el cumplimiento

estricto de las políticas promulgadas por la OGP[4] y las que futuramente emita el Principal Ejecutivo de Información (PEI) del Gobierno de Puerto Rico. La referida OA-2018-10 requiere, entre otras cosas, lo siguiente:

> *III. Disposiciones*
>
> *d. […] En cuanto a los programas con aplicaciones, estos deberán tener controles de acceso para que solamente personal autorizado pueda ver los datos o acceder a las aplicaciones que se necesiten. Los privilegios a usuarios se tienen que revisar regularmente […]*
>
> *Todas las divisiones y dependencias del Departamento de Justicia que administren proyectos de tecnología tienen el deber de mantenerse actualizados en torno a todas las políticas y normativas gubernamentales referentes a los mismos. Es imprescindible que todo proyecto gestionado cumpla con los requerimientos descritos en las políticas antes enumeradas* ***y cualquier otra aplicable que se promulgue en el futuro.*** (Énfasis nuestro)

Además, no es cónsono con las instrucciones impartidas en el *Procedimiento para eliminar la Cuenta del Usuario* del Departamento de Justicia, según se indica:

> *Todo empleado que sea separado de sus funciones conforme al inciso A, Sección Segunda de Razón de Salida, deberá tramitar la* ***Certificación de Devolución de Propiedad****. Este documento requiere la recolección de firmas de los directores, supervisores o empleados autorizados correspondientes, incluyendo la firma de la Oficina de Informática.*
>
> *El(la) Director(a) correspondiente deberá cumplimentar y firmar el Inciso I del mencionado documento […] Una vez se haya firmado y tramitado debidamente, la Oficina de Informática procederá a:*
>
> - *Cancelar todos los accesos del empleado a los sistemas, redes y servicios del Departamento de Justicia y sus componentes adscritos.*
> - *Efectuar dicha cancelación a la fecha de salida que se indique en el formulario.*
>
> *No obstante, la cuenta del empleado podrá prevalecer activa por un período máximo de 30 días a solicitud del supervisor inmediato, con el propósito de permitir el acceso a información relacionada con las tareas previamente*

[4] A la fecha de aprobación de la OA-2018-10, el Área de Tecnologías de Información (ATI) adscrita a la Oficina de Gerencia y Presupuesto era la responsable de promulgar las normas y los procedimientos relativos al uso de las tecnologías de información a nivel gubernamental. Con la aprobación de la Ley Núm. 75-2019 se crea la *Puerto Rico Innovation and Technology Service (PRITS)* con el mismo propósito.

asignadas. Esta extensión deberá ser solicitada formalmente por el supervisor y aprobada por la Oficina de Informática.

Efecto

Las situaciones mencionadas tienen el *efecto* de lo siguiente:

1. Incrementa el riesgo de accesos no autorizados.
2. Dificulta el seguimiento y el control sobre las actividades realizadas por cuentas privilegiadas.
3. Compromete el cumplimiento de políticas internas y estándares de seguridad establecidos.

Causa

Las situaciones comentadas se atribuyen a lo siguiente:

1. Falta de requerimiento de documentación e instrucciones formales para autorizar y manejar cuentas con privilegios administrativos.
2. Ausencia de revisión periódica para limitar el número de usuarios con privilegios, asegurando que los roles asignados correspondan a sus funciones y aplicando el principio de mínimo privilegio.
3. Incumplimiento de la política TI-PRITS-007 por parte del personal del *Helpdesk-Karibe* al compartir credenciales de una cuenta administrativa genérica.
4. Omisión en la provisión de cuentas bajo el dominio gubernamental para contratistas, lo que afecta la trazabilidad y control.
5. Falta de cancelación oportuna de cuentas administrativas de proveedores al vencimiento de contratos.

Comunicación Gerencial

El 21 de enero de 2026 recibimos del director administrativo del Registro, previa aprobación de la secretaria de Justicia, los comentarios al borrador de los hallazgos con evidencia de algunas de las medidas correctivas adoptadas, y citamos:

> *Se utilizarán los formularios para las solicitudes de accesos a la red del Departamento de Justicia y a la aplicación Karibe, para la creación de cuentas institucionales y de acceso a empleados y contratistas que permitirá documentar y controlar accesos y privilegios (Anejos 1 y 2). Se redactará y aprobará la normativa relacionada con la gestión de roles en las cuentas. La Oficina de Informática creó cuentas institucionales al personal de […], proveedor de*

servicios de programación y mantenimiento del Sistema Karibe (Anejo 3). Se canceló la cuenta de […] (Anejo 4). Se solicitó la inclusión de un renglón en la Certificación de Devolución de Propiedad para asegurar la cancelación de accesos a Karibe de los empleados (Anejo 5).

Determinación de la OIG

Se consideraron los comentarios del director administrativo del Registro y la evidencia que acompañó la respuesta gerencial; no obstante, la OIG determinó que el hallazgo prevalece. Se reconoce que el Registro adoptará formularios para las solicitudes de acceso, creará cuentas institucionales al personal del proveedor del sistema *Karibe* y cancelará la cuenta del consultor identificada. Sin embargo, estas acciones atienden de forma parcial las deficiencias señaladas y no se presentó evidencia que acredite su aplicación consistente ni la revisión periódica de privilegios; a ello se suma que la propia respuesta gerencial reconoce que aún está pendiente redactar y aprobar la normativa para la gestión de roles, lo que confirma que persiste la falta de documentación e instrucciones formales que exige la Política TI-PRITS-007.

Además, la respuesta gerencial no atiende la eliminación de la cuenta administrativa genérica compartida por dos empleadas que a su vez poseían roles de superadministrador, ni el establecimiento de un proceso recurrente y documentado de reevaluación de privilegios conforme al principio de privilegio mínimo. Asimismo, la solicitud de incorporar un renglón en la Certificación de Devolución de Propiedad constituye una gestión aún no acreditada como operante, insuficiente por sí sola para subsanar las fallas de cancelación oportuna evidenciadas, como la desactivación de la cuenta de un exempleado 292 días después de cesar sus funciones. En ausencia de evidencia de controles implementados y operantes, subsisten las debilidades en la creación, mantenimiento y cancelación de accesos, contrarias a la Política TI-PRITS-007 y a los Estándares para la Seguridad Cibernética de PRITS, por lo que el hallazgo prevalece.

Ver la Recomendación 2.

Hallazgo 3 – Falta de controles en la Oficina del *Helpdesk-Karibe*

Situación

Desde el 28 de abril de 2015, cuatro (4) usuarios con roles de superadministrador y dos (2) con roles de administrador brindaban asistencia técnica a usuarios internos y externos en el uso del sistema *Karibe*.

Del examen realizado a los procesos llevados a cabo por la Oficina de *Helpdesk-Karibe,* se validó lo siguiente:

a. Personal adscrito a la Oficina de *Helpdesk-Karibe* con credenciales ilimitadas de superadministradores del sistema *Karibe,* tenía a su vez funciones de técnicos del Registro

de la Propiedad, incluyendo el estudio y despacho de documentos variados de cancelaciones de hipotecas, compraventas, declaratorias de herederos, servidumbre, expropiaciones, particiones de bienes, entre otros.

b. Los mecanismos de asistencia técnica para usuarios internos y externos consistían exclusivamente en correo electrónico o llamada telefónica. La Oficina de *Helpdesk-Karibe* no cuenta con una aplicación o plataforma automatizada de gestión de servicios o software de servicio de asistencia técnica, diseñado para entre otros:

   1) Proporcionar un único punto de contacto para usuarios internos y externos.
   2) Brindar respuestas a las consultas de los usuarios mediante *tickets* u opciones de autoservicio.
   3) Automatización de tareas rutinarias.
   4) Proveer métricas y estadísticas de rendimiento.

Criterio

La situación comentada en el apartado **a.** no es cónsona con la Sección 550.01 del *Federal Information System Controls Audit Manual* (FISCAM[5]), promulgado por el *Government Accountability Office* (GAO), establece lo siguiente:

> ***550 FISCAM Framework for Segregation of Duties***
>
> *550.01 The segregation of duties (SD) category relates to the policies, procedures, and an organizational structure for managing who can control key aspects of computer-related operations and thereby prevent unauthorized actions or unauthorized access to assets or records. Segregation of duties involves segregating work responsibilities so that one individual does not control all critical stages of a process. Effective segregation of duties is achieved by splitting responsibilities between two or more individuals or organizational units. In addition, dividing duties this way diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.*
>
> ***Table 12 : FISCAM Framework for Segregation of Duties (SD)***
>
> ***Illustrative controls***

[5] *FISCAM (September 2024)*

SD.01 Management designs and implements general controls to appropriately segregate incompatible duties and mitigate risks resulting from incompatible duties that cannot be segregated.

SD.01.01 Incompatible duties are identified based on risk.

SD.01.01.01 Identify, document, and periodically review and update incompatible duties within and across business process (i.e., system user) functions that should not be performed by the same organizational unit or individual. Such duties may include

- *preparation of data for input into the system,*
- *approval of data for input into the system,*
- *data input,*
- *research and resolution of data input errors that the system identified,*
- *research and resolution of data processing errors that the system identified,*
- *reconciliation of interfaced data, and*
- *verification of output data.*

De igual forma, esta situación no es cónsona con el apartado 3.1 del *National Institute of Standard and Technology (NIST*[6]), en su *Special Publication 800-53*[7], *Security and Privacy Controls for Information Systems and Organizations,* que indica lo siguiente:

3.1 ACCESS CONTROL

AC-5 SEPARATION OF DUTIES

CONTROL:

Discussion: Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. […]

Además, es contraria con lo establecido en la parte V, apartado 2(b), 7 y 8 de la Orden Administrativa Núm. 2025-10, emitida el 30 de septiembre de 2025 por la secretaria de Justicia. En esta se dispone que la Oficina de Informática debe impulsar el desarrollo y adquisición de

[6] El NIST se estableció dentro del Departamento de Comercio de los E.U. como un laboratorio de ciencia, ingeniería, tecnología y medición, y tiene la función estatutaria de desarrollar normas y directrices para los sistemas de información federal.
[7] *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53, rev. 5 (Gaithersburg, Md.: September 2020). Proporciona un catálogo de controles de seguridad y privacidad para sistemas de información y organizaciones para proteger las operaciones y los activos de la organización, a las personas, a otras organizaciones y a los Estados Unidos de un conjunto diverso de amenazas y riesgos. (*FISCAM, 2024*).

aplicaciones que permitan automatizar y mantener procesos, fomentar la interoperabilidad y ofrecer servicios eficientes; evaluar y optimizar el uso de recursos tecnológicos adoptando medidas preventivas y correctivas; y planificar, en coordinación con todas las áreas, el diseño, implantación y mantenimiento integral del sistema de información para estandarizar y oficializar herramientas tecnológicas que optimicen los procesos institucionales.

Efecto

Las situaciones comentadas tienen el *efecto* de lo siguiente:

1. Permite que un mismo empleado controle etapas críticas del proceso registral y del sistema *Karibe*, lo que incrementa el riesgo de errores, irregularidades y uso indebido de privilegios sin detección oportuna.

2. Reduce la eficiencia del servicio, ocasionando retrasos, duplicidad de esfuerzos y pérdida de solicitudes; impide medir el rendimiento por ausencia de métricas (tiempo de respuesta, resolución, volumen de tickets); y obliga a aumentar el personal para tareas que podrían automatizarse, especialmente ante el crecimiento del volumen de solicitudes.

Causa

La situación se atribuye a que el director administrativo del Registro no garantizó que el personal del *Helpdesk-Karibe* limitara sus funciones únicamente a brindar apoyo a los usuarios, según lo dispuesto en la Orden Administrativa Núm. 2018-12. Además, los CIO y los directores en funciones de la Oficina de Informática incumplieron su responsabilidad de implementar una solución tecnológica para automatizar la gestión del servicio de asistencia técnica, tal como exige la Ley Núm. 75-2019 y la Orden Administrativa Núm. 2025-10.

Comunicación Gerencial

El 21 de enero de 2026 recibimos del director administrativo del Registro, previa aprobación de la secretaria de Justicia, los comentarios al borrador de los hallazgos con evidencia de algunas de las medidas correctivas adoptadas, y citamos:

> *Se reconoce que dos empleadas del Help Desk trabajaron simultáneamente roles de Administrador y Técnico debido a una necesidad extraordinaria para atender atrasos en documentos. Esta medida fue temporal y ya concluyó. Se tomarán acciones para garantizar el cumplimiento de la normativa y evitar que situaciones similares se repitan. Por otro lado, cabe destacar que mediante la Orden Administrativa Núm. 2025-12, aprobada el 30 de octubre de 2025, se creó oficialmente el Help Desk (Anejo 6). Se evaluarán mecanismos efectivos de asistencia automatizada para usuarios internos y externos, con la Oficina de Informática e […].*

Determinación de la OIG

Se consideraron los comentarios del director administrativo del Registro y la información presentada en la respuesta gerencial; no obstante, la OIG determinó que el hallazgo prevalece. Se reconoce que la gerencia formalizara el funcionamiento de la Oficina del *Help Desk* mediante la Orden Administrativa Núm. 2025-12 y que indicara que la asignación simultánea de roles de administrador y técnico respondió a una necesidad extraordinaria ya concluida. No obstante, dicha formalización es una medida organizativa que por sí sola no acredita el establecimiento de controles operantes de segregación de funciones, pues no se presentó evidencia de los mecanismos adoptados para impedir que un mismo empleado vuelva a controlar etapas críticas del proceso registral y de la administración del sistema *Karibe*, conforme exigen la Sección 550 del FISCAM y el control AC-5 del NIST SP 800-53.

En cuanto a la ausencia de una herramienta automatizada de gestión de servicios, la respuesta gerencial se limita a indicar que se evaluarán mecanismos de asistencia automatizada, acción prospectiva en etapa de planificación que no evidencia la adopción de una plataforma que provea un único punto de contacto, la gestión mediante *tickets* y las métricas de rendimiento requeridas por la Orden Administrativa Núm. 2025-10. En ausencia de evidencia de controles implementados y operantes, subsisten las debilidades en la segregación de funciones y en la gestión eficiente del servicio de asistencia técnica.

Ver la Recomendación 3.

Hallazgo 4 – Deficiencias en la seguridad del sistema *Karibe*

Situación

En entrevista realizada al contratista y programador del sistema *Karibe*, éste indicó que no se han realizado pruebas de vulnerabilidades a esta aplicación. Esta información fue confirmada por el director de la Oficina de Informática del Departamento de Justicia mediante entrevista y certificación del 18 de junio de 2025.

Criterio

La situación comentada es contraria a las siguientes disposiciones:

El Artículo 5 de la Ley Núm. 40-2024, *Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico*, según enmendada, dispone, entre otras cosas 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 […] una evaluación de vulnerabilidades de seguridad*

tanto interno como externo ("penetration test") para validar la efectividad de los controles que la agencia haya implementado.

En los apartados 3.2.1, 3.2.1.1 y 3.2.1.4 de los *Estándares para la Seguridad Cibernética* promulgados por la PRITS el 15 de mayo de 2023, se establece lo siguiente:

3.2 Software y Aplicaciones

3.2.1 Todo programa de aplicación desarrollado, por una agencia o ***mediante contrato con un tercero****, para brindar servicios a los ciudadanos a través de Internet o facilitar las operaciones internas de la agencia, deberá asegurar que considera los siguientes elementos mínimos de seguridad para su implementación.* (Énfasis suplido)

3.2.1.1 La integración de las mejores prácticas de seguridad para evitar accesos no autorizados y/o maliciosos a través del internet.

[…]

3.2.1.4 Se deberá realizar una evaluación de vulnerabilidad antes de que la aplicación se ponga en producción y su certificación se incluirá como parte de la entrega de los servicios o productos.

La parte IV de la Orden Administrativa Núm. 2017-11[8] emitida por la secretaria de Justicia el 27 de diciembre de 2017, establece que el CIO debe garantizar la integridad, confidencialidad y seguridad de la información y de los sistemas que la respaldan, implementando controles, protocolos y mecanismos internos adecuados. Además, debe velar por el cumplimiento de las normas de seguridad informática y control interno establecidas por OGP, PRITS y demás regulaciones aplicables.

La Oficina de Informática, bajo la supervisión del CIO, es responsable de administrar y supervisar los sistemas tecnológicos del Departamento, asegurando la consistencia y seguridad en los sistemas de computadoras.

Efecto

Las situaciones identificadas pueden generar exposición de datos sensibles, accesos no autorizados, interrupciones de servicio, incumplimiento normativo y daño reputacional significativo.

[8] *Creación de la figura del principal asesor en tecnología (Chief Information Officer-CIO)*. Vigente durante el período de examen; sustituida el 30-sep-2025 por la OA-2025-10.

Causa

La situación señalada se debe a que los *Chief Information Officers* (CIO) y los directores de la Oficina de Informática en funciones han incumplido con su deber de gestionar y realizar las pruebas de vulnerabilidades mandatorias al sistema *Karibe*.

Comunicación Gerencial

El 21 de enero de 2026 recibimos del director administrativo del Registro, previa aprobación de la secretaria de Justicia, los comentarios al borrador de los hallazgos con evidencia de algunas de las medidas correctivas adoptadas, y citamos:

> *El 15 de enero de 2026, el Registro de la Propiedad presentó la solicitud para enmendar el contrato con […], relacionado con los servicios de programación y mantenimiento del Sistema Karibe (Anejo 7). La enmienda propuesta integrará servicios especializados de ciberseguridad dirigidos a identificar y atender vulnerabilidades, además de implementar un mecanismo robusto de autenticación multifactor (MFA), que eleve significativamente los controles de acceso al sistema.*

Determinación de la OIG

Se consideraron los comentarios del Registro de la Propiedad y la información presentada en la respuesta gerencial; no obstante, la OIG determinó que el hallazgo prevalece. Se reconoce y valora que el Registro presentara, el 15 de enero de 2026, una solicitud para enmendar el contrato con el proveedor del sistema *Karibe* con el fin de integrar servicios especializados de ciberseguridad y un mecanismo de autenticación multifactorial. Sin embargo, se trata de una solicitud de enmienda aún no aprobada ni ejecutada, por lo que no se presentó evidencia de su perfeccionamiento ni de la realización de la evaluación de vulnerabilidades que exigen el Artículo 5 de la Ley Núm. 40-2024 y el apartado 3.2.1.4 de los Estándares para la Seguridad Cibernética de PRITS.

Asimismo, la incorporación de la autenticación multifactor (MFA), aunque fortalece los controles de acceso, no sustituye la evaluación de vulnerabilidades internas y externas (*penetration test*) que permanece sin efectuarse, según lo confirmó el director de la Oficina de Informática. Al continuar el sistema *Karibe* en producción sin dicha prueba, subsisten las deficiencias en la seguridad de la aplicación y en la gestión de riesgos tecnológicos que la Orden Administrativa Núm. 2017-11 encomienda al CIO.

Ver la Recomendación 4.

Hallazgo 5– Ausencia de mecanismos de cifrado de datos en reposo

Situación

En los sistemas de información, el término cifrado significa un procedimiento criptográfico en el que el texto sin formato se convierte a un formato de texto cifrado para evitar que cualquier persona, excepto el destinatario previsto, lea dichos datos[9].

Como resultado de las entrevistas realizadas, y del análisis de la información recibida, se evidenció que el sistema *Karibe* reside en un servidor cuyos datos en reposo[10] no cuentan con medidas de protección mediante cifrado. Aunque cuentan con mecanismos de inmutabilidad[11], esta herramienta no garantiza la confidencialidad y privacidad de los datos.

Criterio

La situación comentada es contraria a las siguientes disposiciones:

El Artículo 254 de la Ley Núm. 210-2015, *Ley del Registro de la Propiedad Inmobiliaria del Estado Libre Asociado de Puerto Rico*, según enmendada, establece lo siguiente:

> ***ARTÍCULO 254. - Seguridad y conservación del registro electrónico.***
>
> *Los libros, información y los sistemas para operar el Registro, serán diseñados con todas las precauciones para su conservación, evitación de fraude, falsedad, deterioro y extravío. […] Contará con todos los sistemas de seguridad, almacenaje y redundancia de la base de datos aplicables al Departamento de Justicia.*

Los Artículos 3 (3) y 7 (4) de la Ley Núm. 40-2024, según enmendada, *Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico*, establecen lo siguiente:

> ***Artículo 3.-Política Pública.***
>
> *Se establece como política pública en Puerto Rico lo siguiente:*
>
> *[…]*
>
> ***3.*** *Proteger y mantener la confidencialidad, integridad y disponibilidad de la información almacenada y/o administrada por los Recursos* [sic] *de información gubernamentales y los activos de infraestructura relacionados, ya sea que esté en*

[9] PRITS. (2023). *Estándares para la Seguridad Cibernética V1.2*, Sección 2.9 "Cifrado"

[10] Se refiere a la información que se encuentra almacenada en un medio físico o digital y que no está siendo transmitida ni procesada activamente.

[11] Es un principio o técnica que garantiza que una vez que un dato, archivo o registro ha sido creado o almacenado, **no pueda ser modificado, eliminado o alterado** sin dejar evidencia.

reposo (almacenada), que esté en movimiento (transmitida o recibida), o que está siendo creada o en proceso de transformación (procesada);

[…]

Artículo 7. - Estándares y principios mínimos de Ciberseguridad

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

[…]

***(4)** Establecer controles administrativos que hagan requisito en el uso de cifrados, basado en las mejores recomendaciones del National Institute of Standards and Technology (NIST) para reforzar la confidencialidad e integridad de la data en transporte y en almacén.*

La Regla 254.2 del Reglamento Núm. 8814 establece que toda la información en la base de datos registral debe ser fiel y exacta, y que la Oficina de Sistemas de Informática del Departamento de Justicia es responsable de instalar programas y sistemas de seguridad, redundancia y antivirus para proteger la integridad del sistema.

Por su parte, el apartado 3.1.5 de los Estándares de Seguridad Cibernética de PRITS dispone que se deben implementar controles técnicos, como cifrado, para garantizar la confidencialidad de datos sensibles tanto en reposo como en tránsito en redes no seguras.

La Orden Administrativa Núm. 2017-11 y su actualización en la Núm. 2025-10 establecen que el CIO es responsable de garantizar la integridad, confidencialidad y seguridad de la información y de los sistemas que la respaldan, mediante la implementación de controles, protocolos y mecanismos internos, cumpliendo con las normas de OGP, PRITS y demás regulaciones aplicables.

Asimismo, la Oficina de Informática, bajo la supervisión del CIO, debe administrar y supervisar los sistemas tecnológicos del Departamento, promover la incorporación de nuevas tecnologías, mantener uniformidad y consistencia en los datos, asegurar su confiabilidad y aplicar reglas de seguridad que impidan accesos no autorizados.

El Manual de Normas, Procedimientos y Políticas de Seguridad (10 de octubre de 2019) establece que todo acceso a las bases de datos del Departamento de Justicia debe contar con mecanismos adecuados y controlados que garanticen la seguridad, integridad y confidencialidad de la información almacenada.

Efecto

Las situaciones identificadas pueden ocasionar accesos no autorizados a información sensible, pérdida de confidencialidad de datos personales, financieros o institucionales, incumplimiento de normativas de protección de datos con posibles sanciones legales y un daño reputacional significativo ante la exposición pública de información no protegida.

Causa

La situación señalada se debe a que los CIO y los directores de la Oficina de Informática en funciones han incumplido con su deber de implementar medidas de protección adicionales y robustas mediante el cifrado de datos.

Comunicación Gerencial

El 21 de enero de 2026 recibimos del director administrativo del Registro, previa aprobación de la secretaria de Justicia, los comentarios al borrador de los hallazgos, los cuales citamos a continuación:

> *Se reconoce el hallazgo sobre la ausencia de cifrado de datos en reposo en el Sistema Karibe, por lo tanto, se realizará un análisis responsable del impacto de la implementación en el Registro de la Propiedad. Se advierte que el cifrado implicaría cambios en la infraestructura de Karibe y una inversión, afectando almacenamiento, procesamiento, latencia, capacidad, respaldos y flujo de datos en reposo, así como la gestión de claves. También, se reconoce que la información del Registro es de carácter público y su acceso público es esencial para los servicios que brindamos a la ciudadanía, por lo que un cifrado generalizado podría hacer más lento el sistema y las búsquedas externas. Por ello, antes de implantar esta medida se evaluará cómo equilibrar seguridad y rendimiento para no menoscabar la publicidad registral ni la eficiencia de las consultas de los usuarios.*

Determinación de la OIG

Se consideraron los comentarios del Registro de la Propiedad y la información presentada en la respuesta gerencial; no obstante, la OIG determinó que el hallazgo prevalece. Se reconoce y valora que la gerencia aceptara la deficiencia y se comprometiera a realizar un análisis responsable del impacto de implantar el cifrado, ponderando los efectos en infraestructura, costos y rendimiento del sistema. Sin embargo, dicho compromiso constituye una acción de evaluación en etapa preliminar y no equivale a la implantación de un control de cifrado, por lo que no se presentó evidencia de medidas concretas que protejan los datos en reposo conforme exigen los Artículos 3(3) y 7(4) de la Ley Núm. 40-2024 y el apartado 3.1.5 de los Estándares para la Seguridad Cibernética de PRITS.

Si bien la OIG reconoce la legítima preocupación por preservar la publicidad registral y la eficiencia de las consultas, el carácter público del Registro no exime de proteger la confidencialidad e integridad de los datos sensibles almacenados, entre ellos la información personal, financiera y la relacionada con las cartas de crédito. El mecanismo de inmutabilidad existente no garantiza dicha confidencialidad, y la obligación de cifrar la data en almacén no admite excepción por la función de publicidad del Registro. En ausencia de evidencia de controles de cifrado implantados, subsisten las deficiencias en la protección de la información, contrarias al Artículo 254 de la Ley Núm. 210-2015, a la Regla 254.2 del Reglamento Núm. 8814 y a las disposiciones antes citadas

Ver la Recomendación 4.

Hallazgo 6 – Ausencia de un software o aplicación para manejo de cambios al sistema *Karibe*

Situación

El examen realizado a los procesos implementados para documentar las solicitudes, manejo e implementación de cambios al sistema *Karibe* reflejó lo siguiente:

a. El contratista y el director de la Oficina de Informática del Departamento de Justicia certificaron la ausencia de una aplicación o herramienta dedicada a la documentación y manejo de cambios de versiones del sistema *Karibe.*

b. Las solicitudes de cambio a la base de datos y la aplicación se gestionaban mediante correos electrónicos enviados por el personal de la Oficina de *Helpdesk-Karibe* al contratista, en lugar de un sistema formal de registro y aprobación.

Criterio

Las situaciones comentadas son contrarias a las siguientes disposiciones:

La Política TI-PRITS-006 sobre gestión de cambios establece que todo cambio en hardware, red y aplicaciones debe seguir un procedimiento formal que incluya, como mínimo, información del solicitante, descripción del cambio, encargado, prioridad, tipo, impacto, sistemas afectados, especificaciones actualizadas, plazo, procedimiento detallado, plan de "rollback", riesgos y mitigación, plan de comunicación y funciones y responsabilidades. Además, se recomienda contar con un sistema o herramienta para registrar y gestionar todas las solicitudes de cambio, tanto programadas como no programadas.

La Orden Administrativa Núm. 2025-10 establece que la Oficina de Informática, bajo la supervisión del CIO, debe impulsar el desarrollo y adquisición de aplicaciones que automaticen procesos y fomenten interoperabilidad, evaluar y optimizar el uso de recursos tecnológicos

mediante acciones preventivas y correctivas, y planificar junto a todas las áreas el diseño, implantación y mantenimiento integral del sistema de información para estandarizar y modernizar los procesos institucionales.

Efecto

La falta de control y seguimiento sobre los cambios en el sistema *Karibe* genera ausencia de documentación, dificulta auditorías y la detección de modificaciones no autorizadas, incrementa errores operacionales por cambios mal coordinados, expone a incidentes de seguridad en sistemas críticos y provoca incumplimiento de políticas institucionales y normativas aplicables.

Causa

La situación comentada se debe a que, contrario a lo establecido en la Política TI-PRITS-006 y en la OA-2025-10, los CIO y los directores de la Oficina de Informática en funciones han incumplido con su deber de impulsar el desarrollo y la adquisición de programas que permitan automatizar los procesos del Departamento, en particular, la implementación de un sistema (software) de gestión de cambios del sistema *Karibe*.

Comunicación Gerencial

El 21 de enero de 2026 recibimos del director administrativo del Registro, previa aprobación de la secretaria de Justicia, los comentarios al borrador de los hallazgos con evidencia de algunas de las medidas correctivas adoptadas, y citamos:

> *En cumplimiento con la Política TI-PRITS-006 y los estándares ISO 9001:2015 e ISO/IEC 20000-1, se desarrolló un documento oficial para el Registro de Gestión de Cambio y Servicio del Sistema Karibe (Anejo 8). Con ello, se asegura la trazabilidad y control de cambios, alineando nuestras prácticas con los estándares internacionales y las disposiciones normativas aplicables.*

Determinación de la OIG

Se consideraron los comentarios del Registro de la Propiedad y la información presentada en la respuesta gerencial. No obstante, aunque se elaboró un documento para el Registro de Gestión de Cambio y Servicio del Sistema *Karibe*, no se evidenció su implementación efectiva ni la aplicación consistente de controles, por lo que el hallazgo prevalece.

Ver la Recomendación 5.

COMENTARIO ESPECIAL

En esta sección se comentan situaciones que no necesariamente están relacionadas al examen, pero que son significativas para asegurar la transparencia gubernamental y el acceso a la información pública.

Comentario Especial – Normativas de emergencia que permanecen vigentes a pesar del restablecimiento de las operaciones

Situación

El 22 de mayo de 2020, el director administrativo del Registro emitió una directriz para establecer un mecanismo que permitiera la recepción de cartas de crédito, comprobantes y otros documentos por correo electrónico. Esta medida, que entró en vigor el 26 de mayo de 2020, fue adoptada como respuesta a las limitaciones operacionales ocasionadas por la pandemia, con el propósito de garantizar la continuidad de los servicios al público.

Como parte de esta iniciativa, se autorizó específicamente a recibir cartas de crédito y documentos complementarios mediante correos electrónicos. No obstante, al momento de nuestra intervención, el Registro continúa aplicando esta directriz exclusivamente para las cartas de crédito, las cuales se utilizan para completar el pago de aranceles relacionados con la presentación de documentos.

Criterio

La situación comentada es contraria Artículo de la Regla 267.5 del Reglamento Núm. 8814 *Reglamento General para la Ejecución de la Ley del Registro de la Propiedad Inmobiliaria,* aprobado el 14 de septiembre de 2016 por el Departamento de Estado, que establece lo siguiente:

> **Regla 267.5 – Carta de crédito; expedición; uso y prohibición**
>
> *[...]*
>
> *El uso de la carta crédito estará limitado para el pago de los derechos de inscripción de los documentos que se presenten por la vía presencial y podrá combinarse con otros comprobantes para completar los derechos de inscripción correspondientes. Se prohíbe su uso en la presentación por la vía telemática y para la solicitud de certificaciones registrales.*

Cabe destacar que, de una evaluación a la Regla 267.5 del Reglamento Núm. 8814 y de las referidas directrices del 22 de mayo de 2020, se determinó que estas disposiciones fueron necesarias y justificadas ante las circunstancias excepcionales de cierre de las dependencias gubernamentales durante la emergencia de salud pública. No obstante, al haberse restablecido las

operaciones presenciales en el Registro, la continuidad de dicha práctica sin una enmienda reglamentaria formal resulta incongruente con la normativa vigente.

De entenderse necesario mantener el mecanismo electrónico para agilizar y facilitar la gestión al público, deberá promoverse la revisión o modificación del Reglamento Núm. 8814 y de las normas administrativas aplicables, a fin de armonizar los procedimientos operacionales con el marco regulatorio actual. Esta acción fortalecería la transparencia, la uniformidad en los procesos y la seguridad jurídica de las transacciones realizadas mediante el sistema *Karibe*.

La gerencia no emitió comentarios sobre esta situación en su comunicación del 21 de enero de 2026.

Ver la Recomendación 6.

COMUNICACIÓN GERENCIAL

El borrador de los hallazgos de este examen se sometió para comentarios mediante carta enviada el 12 de diciembre de 2025 a la secretaria de Justica con copia al director administrativo del Registro. En comunicación recibida el 21 de enero de 2026, el director administrativo, previa aprobación de la secretaria de Justicia, sometió la respuesta a los hallazgos y evidencia de varias de las medidas correctivas tomadas. Los comentarios y documentación recibidos se consideraron en la redacción final de este informe.

La OIG reconoce la colaboración del Registro durante el proceso de examen y reitera su compromiso de continuar trabajando de manera coordinada con la entidad para promover el fortalecimiento de los controles internos y la implantación de las recomendaciones incluidas en este informe, en apoyo a una sana administración pública.

RECOMENDACIONES

Con la contestación al borrador de los hallazgos recibida el 21 de enero de 2026, la gerencia incluyó evidencia de las medidas correctivas adoptadas hasta entonces. A continuación, se incluyen recomendaciones que la gerencia deberá implementar y presentar evidencia de las medidas tomadas, de manera que se corrijan en su totalidad las situaciones señaladas en los hallazgos.

Núm. Rec.	Acción Correctiva Recomendada	Descripción del Hallazgo	Responsable
1	Modificar formato de carta de crédito, implementar validación de identidad y restringir	Deficiencias en expedición, uso y manejo de cartas de crédito (Hallazgo 1).	Director Administrativo del Registro

Núm. Rec.	Acción Correctiva Recomendada	Descripción del Hallazgo	Responsable
	impresión/descarga solo al rol de Registrador.		
2	Adoptar normativa para asignar privilegios administrativos, limitar usuarios, eliminar cuentas genéricas y establecer revisión periódica automatizada.	Deficiencias en creación, mantenimiento y cancelación de accesos (Hallazgo 2).	Director Administrativo del Registro / Director de Oficina de Informática
3	Implementar software para gestión de asistencia técnica y garantizar segregación de funciones.	Falta de controles en la Oficina del *Helpdesk-Karibe* (Hallazgo 3).	Director de Oficina de Informática
4	Establecer programa anual de pruebas de penetración y escaneos de vulnerabilidades; implementar controles de cifrado para los datos en reposo.	Deficiencias en seguridad del sistema *Karibe* y ausencia de cifrado (Hallazgos 4 y 5).	Director de Oficina de Informática
5	Implementar software para manejo de cambios con registro, evaluación de impacto, flujos de aprobación y auditoría.	Ausencia de herramienta para manejo de cambios en el sistema *Karibe* (Hallazgo 6).	Director de Oficina de Informática
6	Ajustar reglamentación si se mantiene la práctica de recibir cartas de crédito por correo electrónico.	Normativas de emergencia que permanecen vigentes (Comentario Especial).	Director Administrativo del Registro

CONCLUSIÓN

La evaluación realizada a los documentos, y la información recopilada durante nuestro examen, revelaron los hallazgos y deficiencias de controles según detallados, para los cuales se emiten las correspondientes recomendaciones.

Los hallazgos identificados evidencian deficiencias en la expedición, uso y manejo de las cartas de crédito, así como debilidades en los controles y medidas de seguridad del sistema *Karibe*. Será responsabilidad de la gerencia corregir las deficiencias señaladas para evitar que situaciones como las comentadas en los hallazgos se repitan.

Conforme con lo establecido en el Artículo 17 de la Ley Núm. 15-2017, antes citada, 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

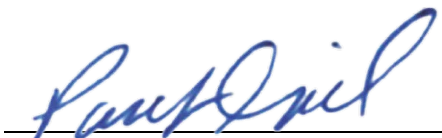
aplicables. El incumplimiento con tomar medidas correctivas ante las situaciones aquí señaladas podría ocasionar la imposición de multas y procesos administrativos.

APROBACIÓN

El presente informe es aprobado en virtud de los poderes conferidos por la Ley Núm. 15-2017, antes citada. 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 estos y 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 junio de 2026, en San Juan, Puerto Rico.

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



Pablo L. González Flores, CISA, CFE
Director del Área de Pre-Intervención y Exámenes

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