INFORME ESPECIAL

OIG-IE-26-005

Oficina del Inspector General
Gobierno de Puerto Rico

Estudio sobre el Cumplimiento de las Normativas de Gobernanza Tecnológica en las Entidades bajo Jurisdicción de la Oficina del Inspector General de Puerto Rico

25 de noviembre de 2025

TABLA DE CONTENIDO

RESUMEN EJECUTIVO

La Oficina del Inspector General de Puerto Rico (en adelante, OIG), llevó a cabo un estudio sobre el cumplimiento de las normativas de gobernanza tecnológica en las entidades bajo su jurisdicción. Ello, de conformidad con las directrices en la Carta Circular Conjunta OIG-CC-2024-02 y 2024-01[1] (en adelante, Carta Circular Conjunta), emitida el 25 de abril de 2024, por la OIG y la *Puerto Rico Innovation and Technology Service* (en adelante, *PRITS*). En esta se solicitó, a los jefes de las entidades bajo jurisdicción de la OIG, instruir a los oficiales principales de informática (en adelante, OPI) o a aquel empleado o funcionario que efectúe funciones similares, a completar un cuestionario denominado *Cuestionario de Gobernanza Tecnológica*.

El estudio se fundamenta en las disposiciones de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico* (en adelante, Ley Núm. 15-2017), la cual faculta a la OIG a llevar a cabo estudios y evaluaciones para mejorar la efectividad y eficiencia en el funcionamiento de las entidades gubernamentales. Esto incluye desarrollar estándares y políticas para guiar a las entidades en el establecimiento de controles adecuados y en la práctica de sana administración.

Asimismo, este esfuerzo se realizó en coordinación con *PRITS*, creada por virtud de la Ley Núm. 75-2019, conocida como *Ley de la Puerto Rico Innovation and Technology Service*, con el fin de establecer y promover la política pública sobre la elaboración, manejo, desarrollo, coordinación e integración interagencial efectiva de la innovación y de la infraestructura tecnológica e informática del Gobierno de Puerto Rico.

El cuestionario abordó los siguientes aspectos críticos:

- Información sobre el inventario de licencias de software y contratos maestros.
- Detalles sobre el inventario de equipos y la identificación de equipos obsoletos.
- Proyección de equipo a ser reemplazado o adquirido.
- Planes para proyectos tecnológicos a corto y largo plazo.

[1] Las disposiciones de esta Carta Circular se aplicaron a todas las entidades gubernamentales, agencias, departamentos, oficinas y corporaciones públicas de la Rama Ejecutiva, que se encuentran bajo la jurisdicción de la Oficina del Inspector General (en adelante, "OIG"), en virtud de la Ley Núm. 15- 2017; y de la Ley Núm. 75-2019, según enmendada, conocida como *Ley de la Puerto Rico Innovation and Technology Service*.

Se excluyeron de estos términos a los municipios, la Universidad de Puerto Rico, el Centro de Recaudación de Ingresos Municipales, la Oficina de Gerencia y Presupuesto, la Oficina de Ética Gubernamental, la Corporación del Proyecto Enlace del Caño Martín Peña y la Compañía para el Desarrollo Integral de la Península de Cantera, Municipios, Rama Legislativa; y Rama Judicial, por ser entes excluidos de la Ley Núm.15-2017, antes citada.

- Evaluación de la protección de la infraestructura y datos.
- Ciberseguridad.
- Procedimientos de respaldo y almacenamiento de datos.
- Uso de servicios en la nube y medidas de seguridad aplicadas.
- Información sobre contratistas, consultores, y personal de TI.
- Datos sobre el presupuesto asignado para tecnología.

Este estudio proporciona una perspectiva integral de la gestión tecnológica en las entidades gubernamentales a raíz de la política pública establecida mediante reglamentación.

El objetivo principal del estudio es facilitar la optimización del uso de los recursos tecnológicos en las entidades gubernamentales, mediante la identificación sistemática de fortalezas, deficiencias y áreas de oportunidad. A través del Cuestionario de Gobernanza Tecnológica, se recopiló información detallada que permite evaluar el grado de alineación de cada entidad con los principios de eficiencia operativa, cumplimiento normativo y buenas prácticas en la gestión de tecnología.

El instrumento permitió examinar aspectos como la existencia de inventarios actualizados de licencias y equipos, la identificación y reemplazo de tecnología obsoleta, la planificación de proyectos tecnológicos a corto y largo plazo, la implantación de controles en materia de ciberseguridad, los procedimientos de respaldo y almacenamiento de datos, el uso de servicios en la nube, así como la estructura organizacional del área de tecnología y el manejo de personal interno y externo.

Los resultados obtenidos revelan que, aunque algunas entidades cumplen satisfactoriamente con los criterios establecidos, también se identificaron múltiples áreas críticas con niveles importantes de incumplimiento o cumplimiento parcial. Entre estas se destacan la ausencia de políticas internas para el manejo de accesos, la falta de procesos sistemáticos para evaluar riesgos tecnológicos, el uso limitado de mecanismos para revocar accesos de forma oportuna y deficiencias en el versionamiento y documentación de *API* (Interfaz de Programación de Aplicaciones). En áreas como la protección de datos, el control de infraestructura física o la administración del presupuesto asignado a tecnología, se observaron diferencias notables entre entidades, reflejando un grado variable de madurez en sus prácticas de gobernanza.

Incluso en los componentes que presentaron niveles aceptables de cumplimiento, fue posible identificar oportunidades concretas de mejora. Estas incluyen la necesidad de revisar y actualizar

normativas internas, fortalecer los protocolos de seguridad, documentar adecuadamente los procedimientos operacionales y reforzar la supervisión de servicios tercerizados. La identificación de estas brechas permitirá el desarrollo de estrategias específicas para apoyar a las entidades en el fortalecimiento de su gobernanza tecnológica, en armonía con la política pública establecida por *PRITS* y la función fiscalizadora de la OIG.

Mediante el establecimiento y la promoción de la política pública liderada por *PRITS*, al amparo de la Ley Núm. 75-2019, las entidades tendrán la oportunidad de fortalecer su infraestructura tecnológica y optimizar la gobernanza, fomentando así la transparencia y la eficacia en la gestión pública

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 pudieran poner en peligro el buen uso de fondos públicos, así como 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.

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* y de los artículos 6, 7 y 9 de la Ley Núm. 75-2019 según enmendada, conocida como *Ley de la Puerto Rico Innovation and Technology Service*.

OBJETIVO

El estudio tuvo como objetivo evaluar el cumplimiento de la Ley Núm. 75-2019, las políticas específicas de *PRITS* y otras normativas relacionadas con la integración y gestión de la tecnología y de la infraestructura informática en el Gobierno de Puerto Rico. Esta evaluación se llevó a cabo siguiendo las directrices establecidas en la Carta Circular Conjunta, emitida el 25 de abril de 2024, por la OIG y PRITS.

El propósito de este esfuerzo es fortalecer la gestión tecnológica mediante la identificación de áreas de mejora, el aseguramiento del cumplimiento normativo, y la revisión de conformidad con

las políticas y la reglamentación vigente. Además, busca promover la transparencia y rendición de cuentas en la gestión de tecnologías, así como impulsar la innovación a través de la incorporación de nuevas tecnologías y proyectos que optimicen los servicios gubernamentales.

ALCANCE Y METODOLOGÍA

El estudio se basó en las respuestas suministradas por 90[2] entidades gubernamentales, según requerido en la Carta Circular Conjunta del 25 de abril de 2024. Como parte de su diseño metodológico, no se llevaron a cabo pruebas físicas ni visitas a las entidades para validar el cumplimiento, en tanto el alcance del análisis se concentró en evaluar el estado de cumplimiento según lo informado por las propias entidades en el instrumento provisto. La metodología empleada incluyó los siguientes pasos:

- **Recopilación y tabulación de datos**: Se recopiló todas las respuestas obtenidas del cuestionario y se organizó en tablas para facilitar su tabulación, análisis e interpretación.
- **Asignación de criterios y análisis**: Se asignó criterios específicos de evaluación para cada pregunta, de acuerdo con los objetivos del estudio.
- **Requerimiento de información:** Se solicitó a las entidades la presentación de documentos pertinentes, incluyendo reglamentación, procedimientos y normas vigentes aplicables a la disposición de *hardware* y medios de almacenamiento.
- **Evaluación de documentos:** Se revisó y analizó los documentos recibidos para obtener los resultados finales.

INFORMACIÓN SOBRE EL ESTUDIO

La Ley Núm. 75-2019, otorgó a *PRITS* la autoridad para establecer y promover la política pública sobre la elaboración, manejo, desarrollo, coordinación e integración interagencial efectiva de la innovación, la infraestructura tecnológica e informática del Gobierno de Puerto Rico. Entre sus facultades se incluye, desarrollar proyectos tecnológicos de forma ordenada para facilitar la integración efectiva de la tecnología a la gestión gubernamental.[3]

Igualmente, se le otorgó la facultad de emitir órdenes administrativas, opiniones y cartas circulares a petición de parte o *motu proprio* cuando lo estime necesario e investigar posibles violaciones a las disposiciones de su ley habilitadora y de los reglamentos que se promulguen al amparo de esta.[4] También, se le ha delegado la facultad para supervisar, orientar y colaborar en la implementación de

[2] Véase Anejo.
[3] Art. 6 de la Ley Núm. 75-2019, conocida como *Ley de la Puerto Rico Innovation and Technology Service.*
[4] *Id.* Art. 7. Sección (3) y (6)

la Ley Núm. 151-2004, según enmendada, conocida como *Ley de Gobierno Electrónico*,[5] y de la Ley Núm. 148-2006, según enmendada, conocida como *Ley de Transacciones Electrónicas*,[6] entre otras.

Para liderar la estrategia y el proceso de innovación y transformación en Puerto Rico el Artículo 6(s) de la Ley Núm. 75-2019 establece que *PRITS* trabajará en coordinación con las instrumentalidades del Gobierno de Puerto Rico, el gobierno federal y el sector privado. Su enfoque se centra en desarrollar iniciativas que promuevan la agenda de innovación, informática y tecnología.[7] Así también, los incisos (q) y (r) del citado artículo autorizan a *PRITS* a otorgar acuerdos colaborativos o aquellos contratos necesarios para la consecución de sus deberes estatutarios.[8]

Por su parte, la Ley Núm. 15-2017 estableció la OIG con el objetivo de promover óptimos niveles de integridad, honestidad, transparencia, efectividad y eficiencia en el servicio público.[9] Se le otorgaron funciones y facultades con el propósito de fortalecer los mecanismos de prevención, fiscalización, investigación y auditoría en la gestión gubernamental.[10]

La OIG interviene proactivamente con las entidades cubiertas para promover una sana administración pública. Entre sus responsabilidades se encuentran realizar estudios, exámenes y evaluaciones para medir, mejorar y optimizar la efectividad, eficacia y economía en el funcionamiento de estas entidades.[11] El cumplimiento de estas funciones representa una base fundamental para garantizar la integridad en la administración pública.

Además, la OIG tiene la responsabilidad de coordinar y fortalecer esfuerzos gubernamentales dirigidos a fomentar la integridad y la eficiencia operacional de los procesos, así como asistir en la implantación de medidas correctivas.[12]

Cónsono con lo antes expuesto y en cumplimiento con sus deberes ministeriales, resulta imperante que tanto *PRITS* como la OIG cuenten con información actualizada de las áreas críticas de la gestión tecnológica de las entidades bajo su alcance jurisdiccional.

Esta actualización de información representa un requisito necesario para el cumplimiento normativo, así como un elemento clave para fortalecer la gobernanza tecnológica, fomentar la transparencia y garantizar la rendición de cuentas en la administración gubernamental. Al contar con datos precisos y actualizados, tanto *PRITS* como la OIG podrán contribuir a la optimización de recursos, identificar

[5] Art. 4 de la Ley Núm. 151-2004, según enmendada, conocida como *Ley de Gobierno Electrónico*.
[6] Art. 20 de la Ley Núm. 148-2006, según enmendada, conocida como *Ley de Transacciones Electrónicas*.
[7] Art. 6 de la Ley Núm. 75-2019, conocida *como Ley de la Puerto Rico Innovation and Technology Service.*
[8] *Id.*
[9] Art. 2, de la Ley Núm. 15-2017, según enmendada, conocida como *Ley del Inspector General de Puerto Rico*.
[10] *Id.* Art. 4.
[11] *Id.* Art. 7.
[12] *Véase* el Art. 7 de la Ley Núm. 15-2017, para detalles adicionales sobre sus poderes y facultades.

áreas de mejora y fomentar la colaboración interinstitucional. Esto impulsará los objetivos compartidos de eficiencia, innovación y responsabilidad en el ámbito tecnológico gubernamental.

Para facilitar este proceso, la OIG y *PRITS* diseñaron un formulario electrónico para recopilar la información. Se evaluó las respuestas suministradas por 90 entidades en igual número de cuestionarios recibidos, considerando que para propósitos de este estudio una entidad podría estar compuesta por un departamento sombrilla y sus componentes. (**Anejo**).

A manera de ofrecer una visión detallada sobre la efectividad en la gestión tecnológica y de seguridad de las entidades, asegurando el cumplimiento normativo y la optimización de recursos, las preguntas incluidas en el cuestionario se clasificaron por temas.

A continuación, se presentan los **4 temas principales** en que fue clasificado el cuestionario:

1. **Cumplimiento con la Ley Núm. 75-2019**
    - **a.** Cumplimiento Normativo
    - **b.** Inventario de Equipos y Sistemas
    - **c.** Proyectos y Recursos Humanos
    - **d.** Seguridad en las Redes
    - **e.** Gestión de Privilegios de Acceso
    - **f.** Evaluación de Vulnerabilidad y Seguridad del Sistema
    - **g.** Control de Acceso Físico y Seguridad de las Instalaciones
    - **h.** Plan y Centro de Recuperación de Desastre
    - **i.** Interconexión de Sistemas
2. **Desarrollo de Interfaz de Programación de Aplicaciones (*API's*, *Application Programming Interface*)**
3. **Publicaciones Web**
4. **Ciberseguridad**

Fue necesario emitir un requerimiento adicional a todas las entidades para que nos suministraran información complementaria que nos permitiera continuar con la evaluación. En el análisis de las respuestas se observó que, en algunos casos, las respuestas no correspondían con la información solicitada o no contestaron.

La recopilación de los datos incluidos por las entidades en el cuestionario sirvió para determinar el grado de cumplimiento con las políticas y regulaciones establecidas. Los resultados se traducen en una puntuación que refleja el nivel de adecuación con respecto a los temas u áreas críticas. Las puntuaciones asignadas durante el estudio se limitaron a clasificar las respuestas proporcionadas por las entidades de acuerdo con la siguiente escala:

- **0 a 50:** Insuficiente

  Los criterios evaluados no se satisfacen en su totalidad, indicando áreas significativas de no conformidad y la necesidad de mejoras sustanciales.

- **51 a 75:** Moderado

  Se observan algunos niveles de adecuación, pero existen deficiencias notables que requieren atención para alcanzar un estándar aceptable de conformidad.

- **76 a 100:** Adecuado

  Los criterios evaluados se satisfacen de manera adecuada, reflejando un nivel de cumplimiento satisfactorio y conforme a los estándares establecidos

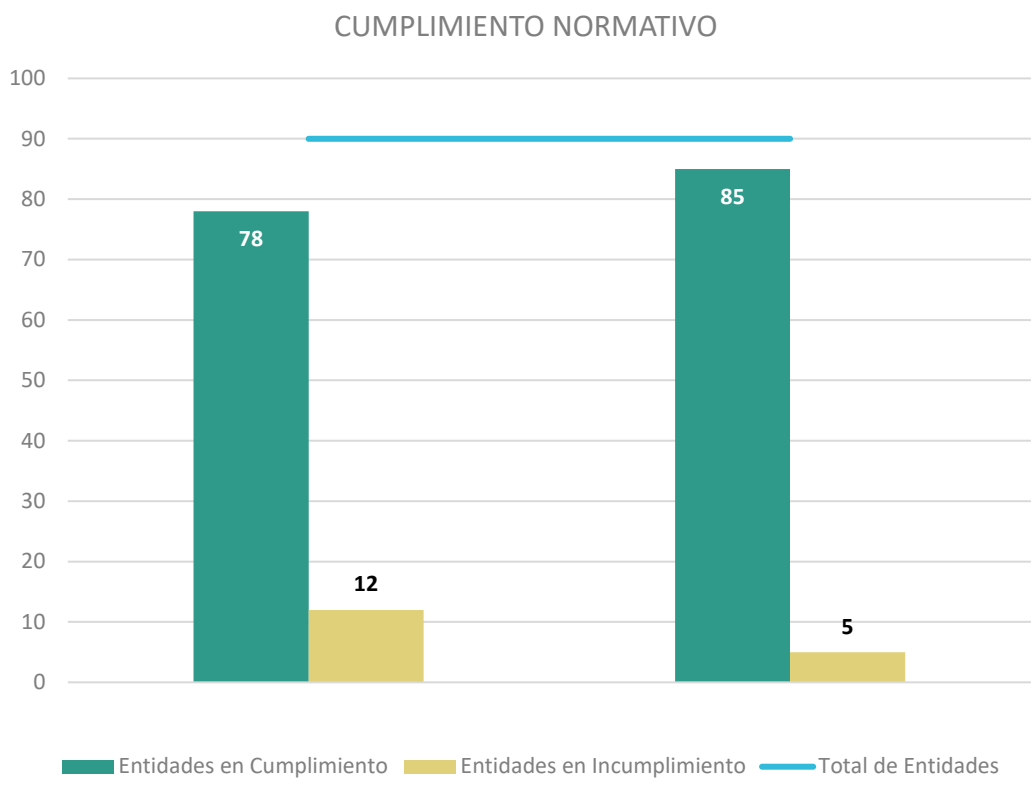
Además, de definir criterios específicos para identificar los incumplimientos de ciertas entidades, se detallaron los efectos asociados a dichas irregularidades y se presentaron propuestas de acciones correctivas dirigidas a las entidades que requieren atender estas áreas prioritarias.

RESULTADOS DEL ESTUDIO

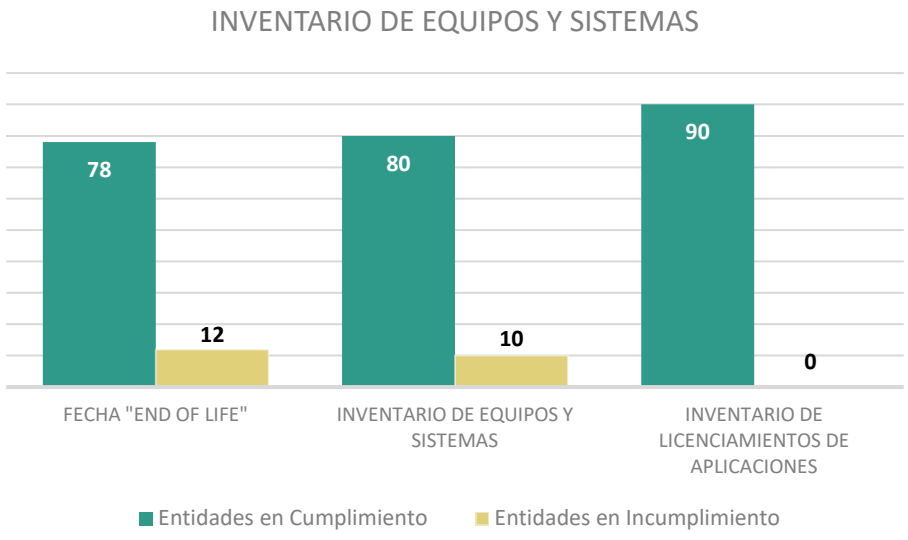
Con el propósito de presentar de forma clara y visual las respuestas obtenidas en el cuestionario, a continuación, se incluyen gráficos que ilustran los datos recopilados.

1. **CUMPLIMIENTO CON LA LEY 75-2019**

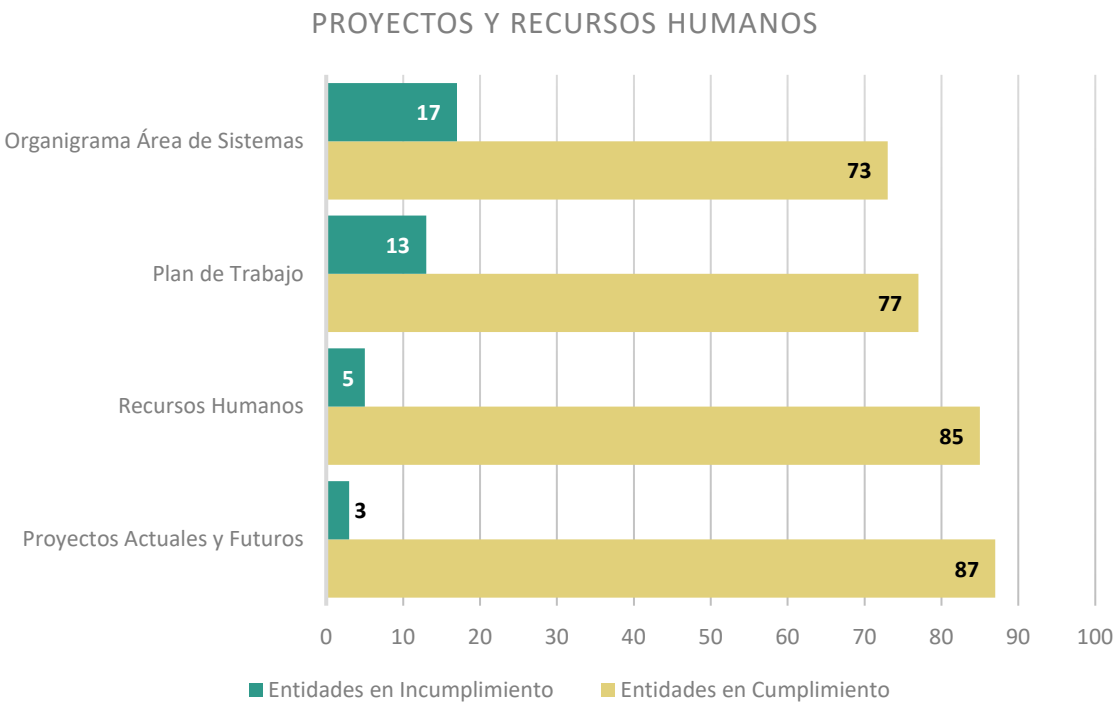
   a. **Cumplimiento Normativo -** Normas relacionadas con la gestión de sistemas de información, incluyendo la designación de un oficial principal de informática autorizado, la existencia de normas internas para la seguridad y el uso de los sistemas.



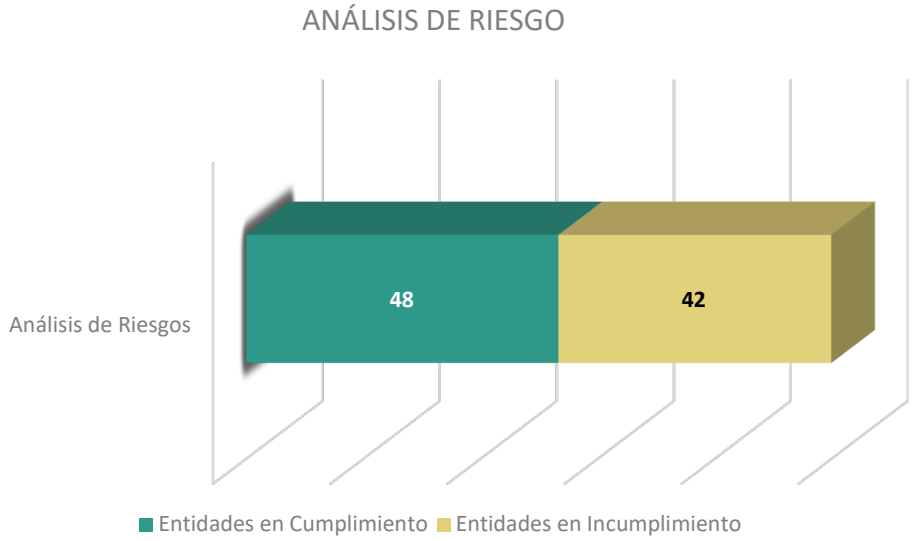
b. Inventario de Equipos y Sistemas - Manejo y seguimiento de los equipos y sistemas de información, incluyendo la existencia y actualización del inventario, así como la gestión del ciclo de vida de los equipos.

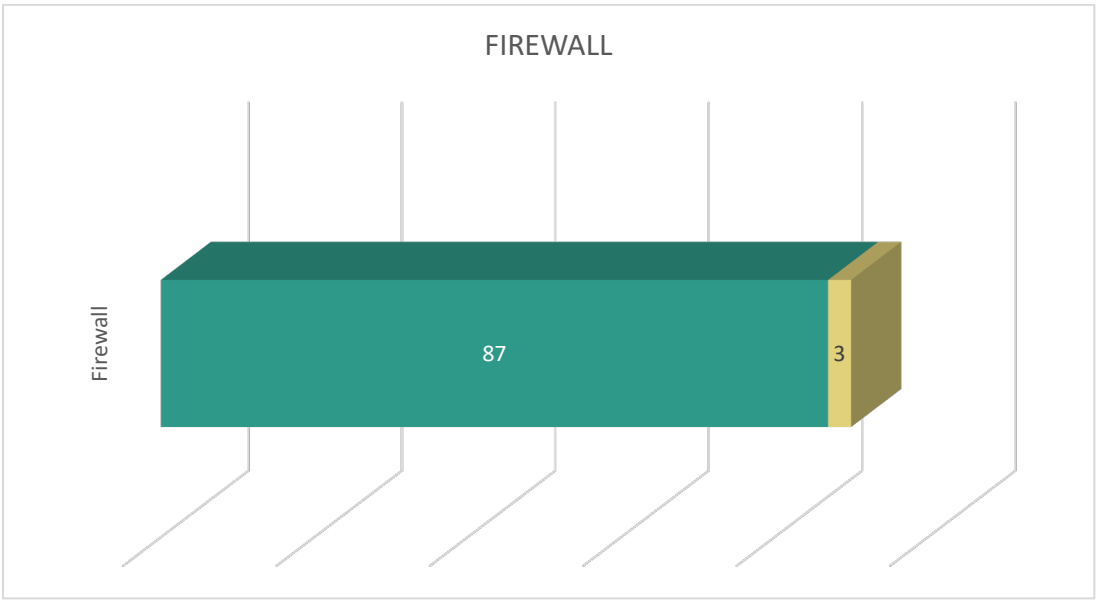


c. **Planificación y Recursos Humanos -** Planificación y gestión de los sistemas de información, los proyectos en curso y futuros, y su distribución. Incluye también los recursos humanos disponibles.



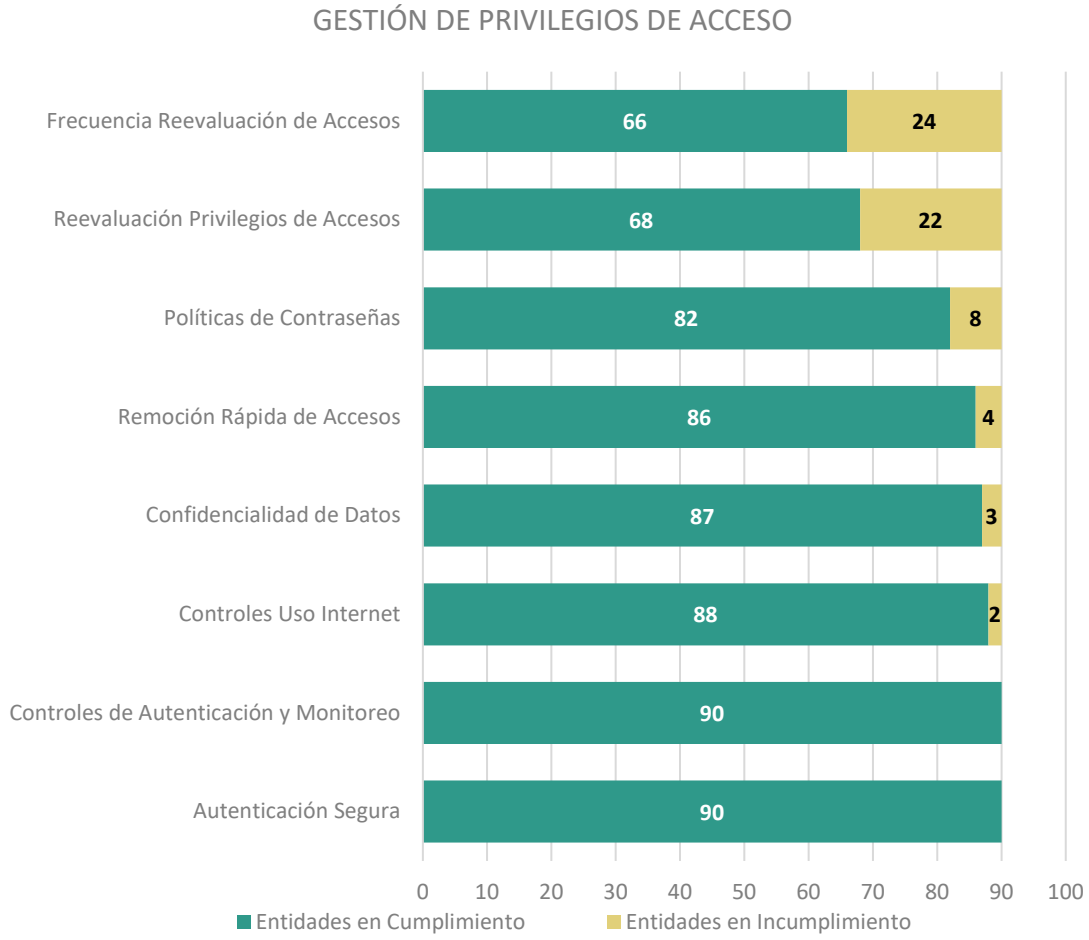
d. Seguridad en las Redes - Medidas de seguridad implementadas en las redes, como el análisis de riesgos realizado, la implementación y configuración de *firewalls*[13].



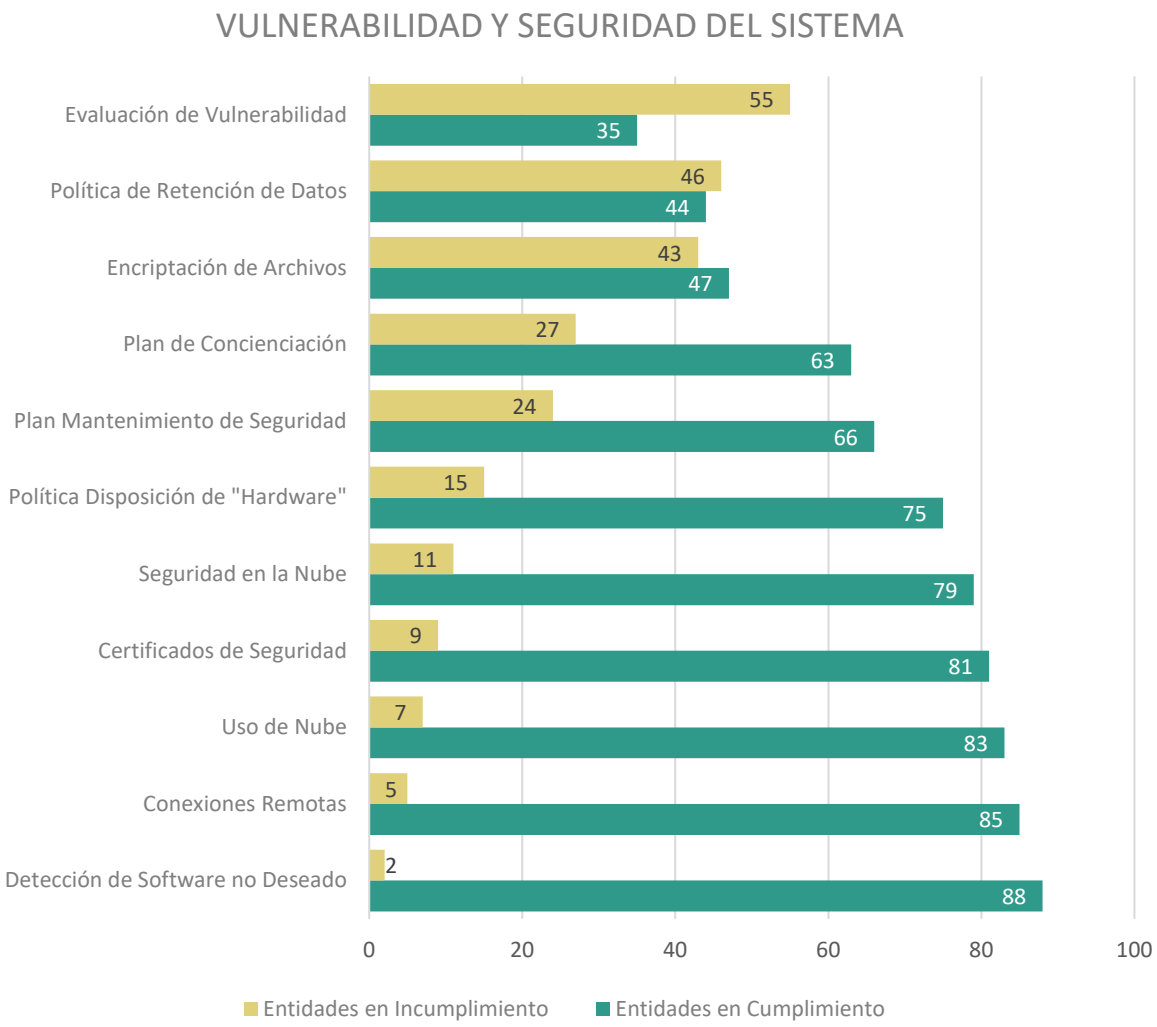


[13] Dispositivo de seguridad de red diseñado para monitorear, filtrar y controlar el tráfico de red entrante y saliente basado en reglas de seguridad predeterminadas.

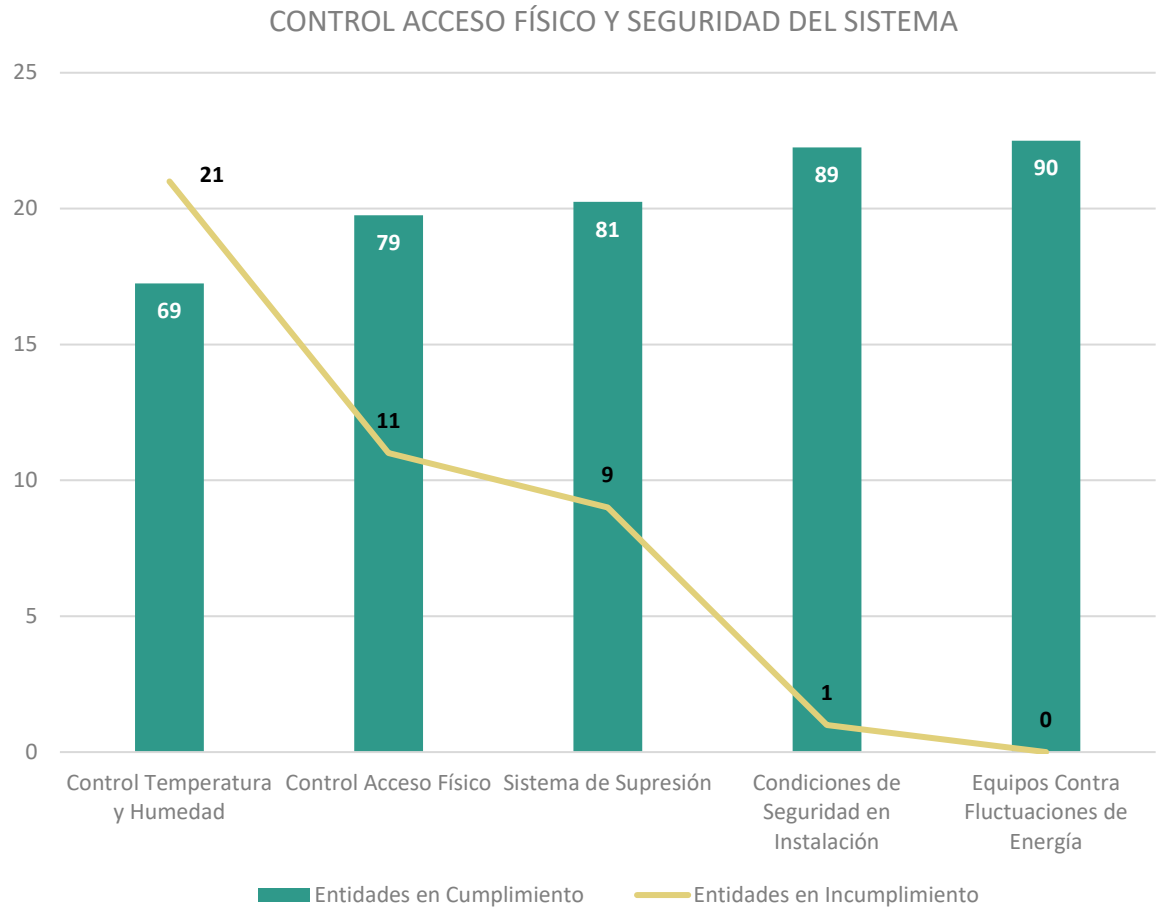
e. **Gestión de Privilegios de Acceso -** Políticas de cambio de contraseñas y los requisitos de autenticación, la administración de los privilegios de acceso, la reevaluación periódica de permisos, la remoción de accesos para empleados que se desvinculan del servicio, y los controles para gestionar el uso de Internet. También a la protección de la información en redes internas y externas.



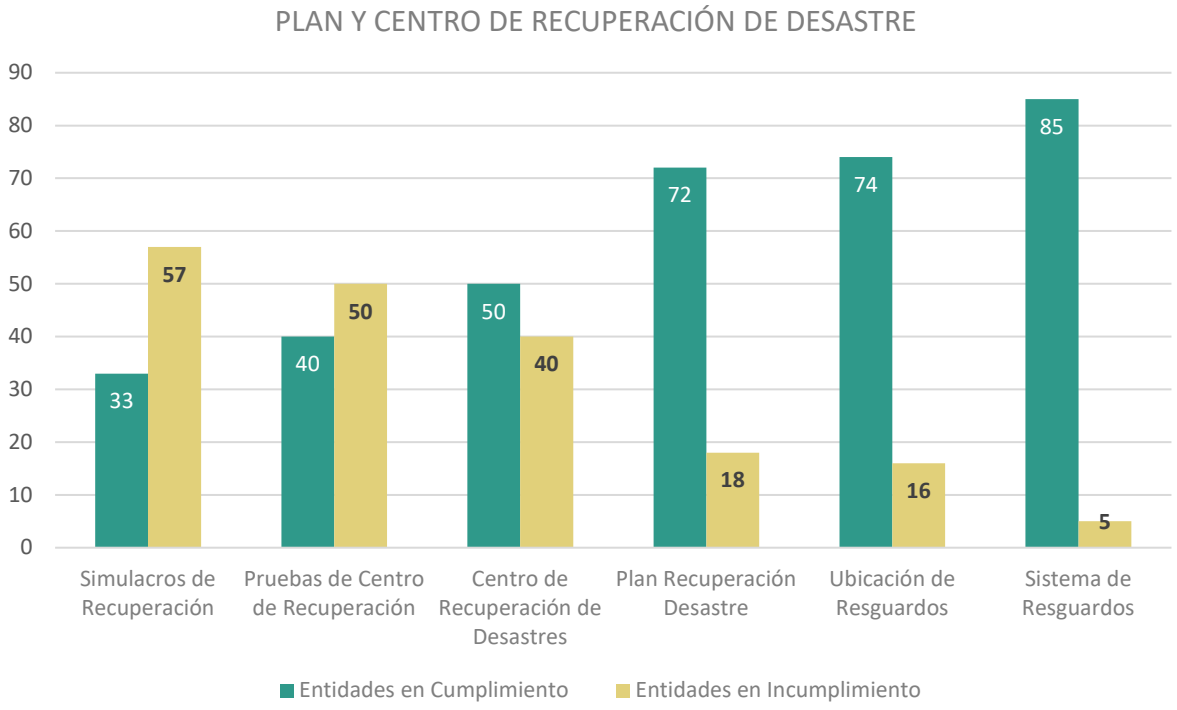
f. **Evaluación de Vulnerabilidad y Seguridad de los Sistemas -** Prácticas y medidas adoptadas para asegurar los sistemas de información, incluyendo la gestión de conexiones remotas, el mantenimiento de parches, el uso de tecnologías en la nube, la encriptación de archivos, las configuraciones de seguridad y la evaluación de vulnerabilidades. También a la instalación de controles de detección, la concienciación de los usuarios y las políticas relacionadas con la retención/destrucción de datos y la disposición de *hardware* y medios de almacenamiento.



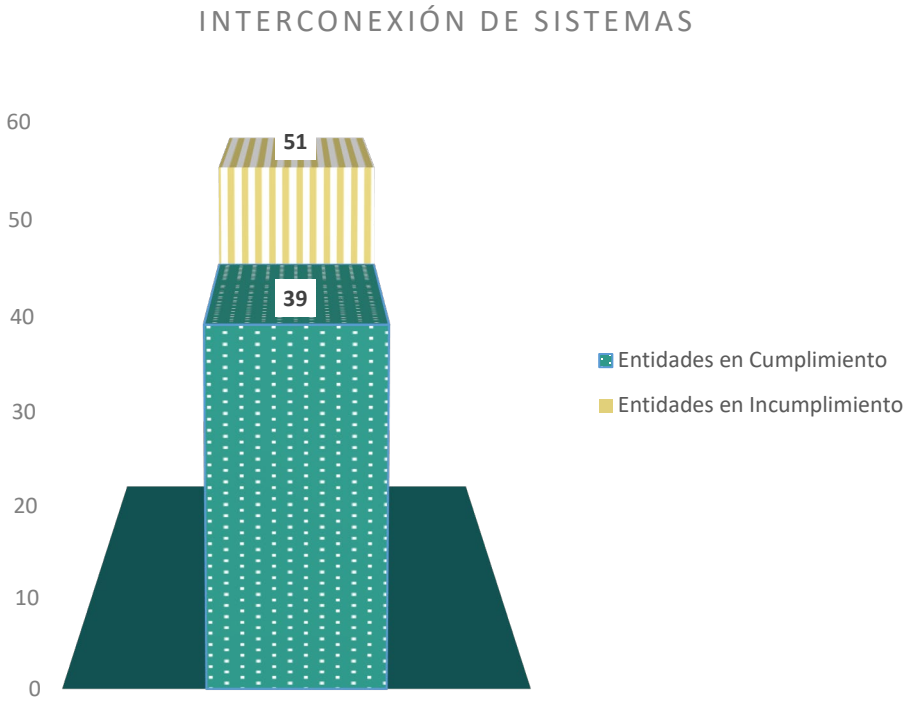
g. **Control de Acceso Físico y Seguridad de las Instalaciones -** Medidas de seguridad física para proteger las instalaciones de procesamiento, incluyendo el control de acceso, la protección contra incendios y el mantenimiento de condiciones ambientales adecuadas.



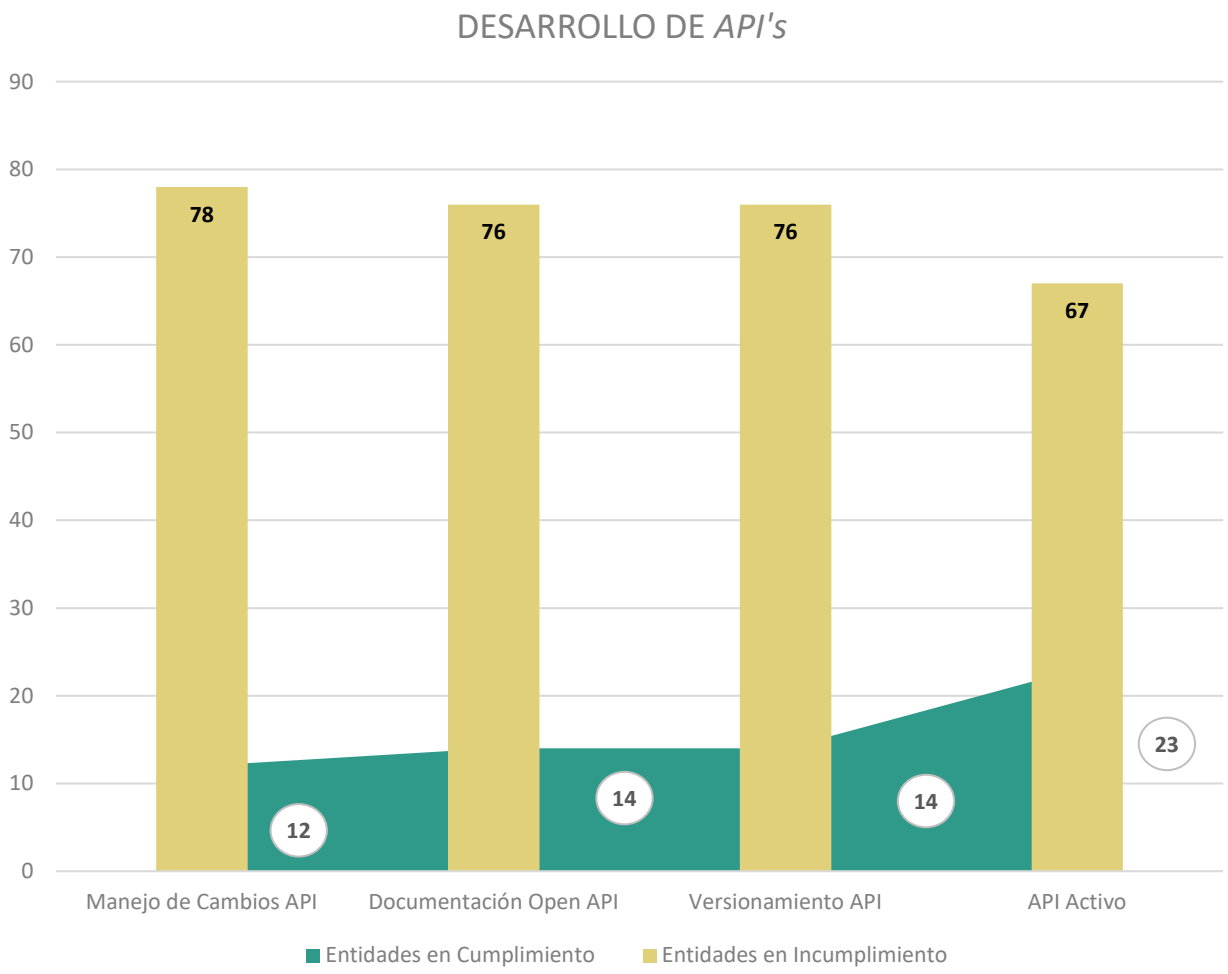
h. Plan y Centro de Recuperación de Desastre - Estrategias y recursos dedicados a la recuperación en caso de desastre, la ubicación y el mantenimiento de resguardos, la existencia y operación del centro de recuperación, y la frecuencia de los simulacros realizados para asegurar su eficacia.



i. **Interconexión de Sistemas -** Interconexión de los sistemas de información con otras agencias o entidades y la disponibilidad de los sistemas. También, a la gestión de contratos para servicios externos que facilitan certificaciones a los ciudadanos.

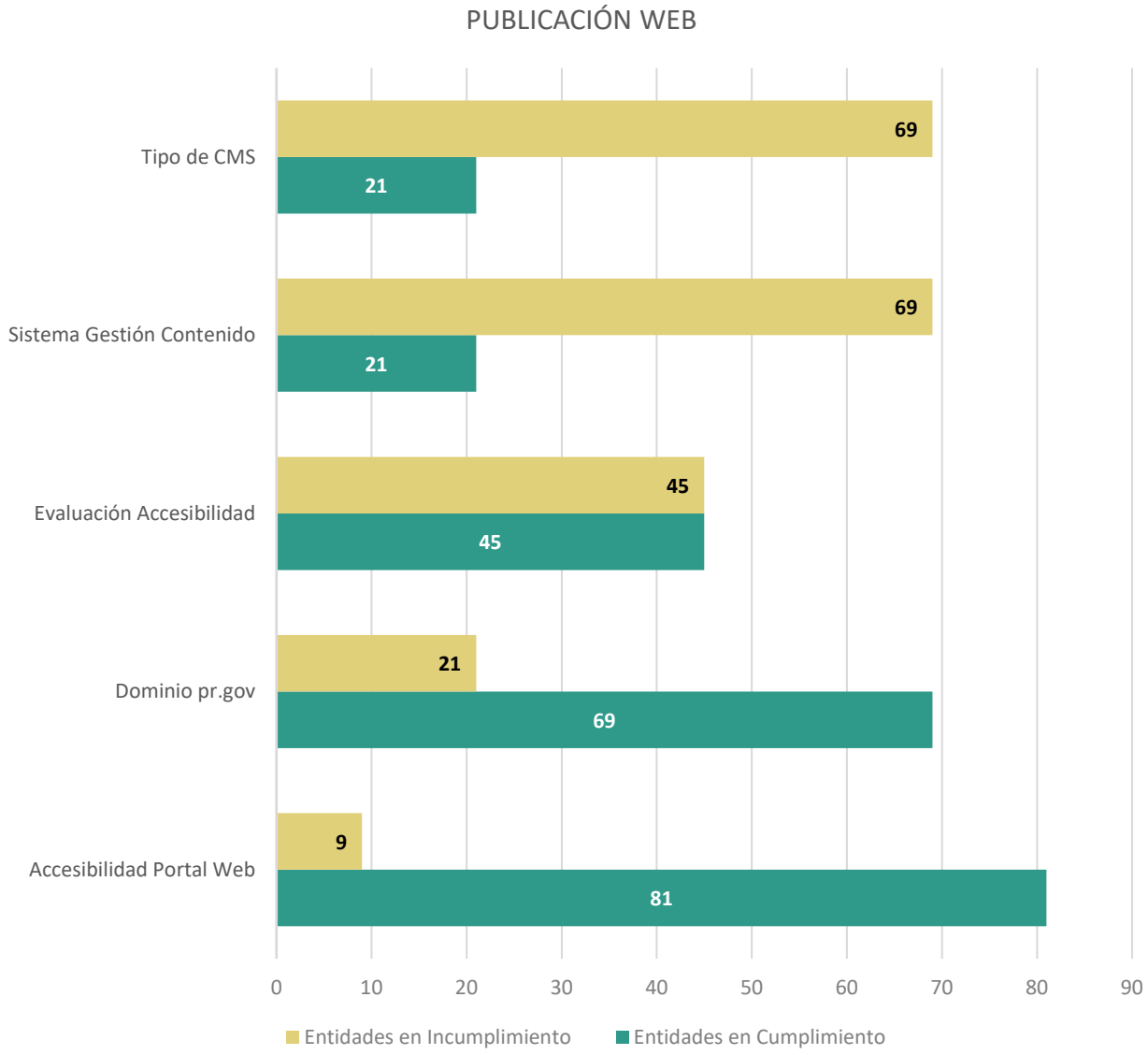


2. **DESARROLLO DE INTERFAZ DE PROGRAMACIÓN DE APLICACIONES[14] (*API'S, Application Programming Interface*) -** Revisión del desarrollo y la gestión de interfaces de programación (*API's*) para asegurar que cumplan con los estándares de documentación, versionamiento y manejo de cambios. Verificar que las *API's* estén implementadas correctamente y que sigan las mejores prácticas para su uso y mantenimiento.

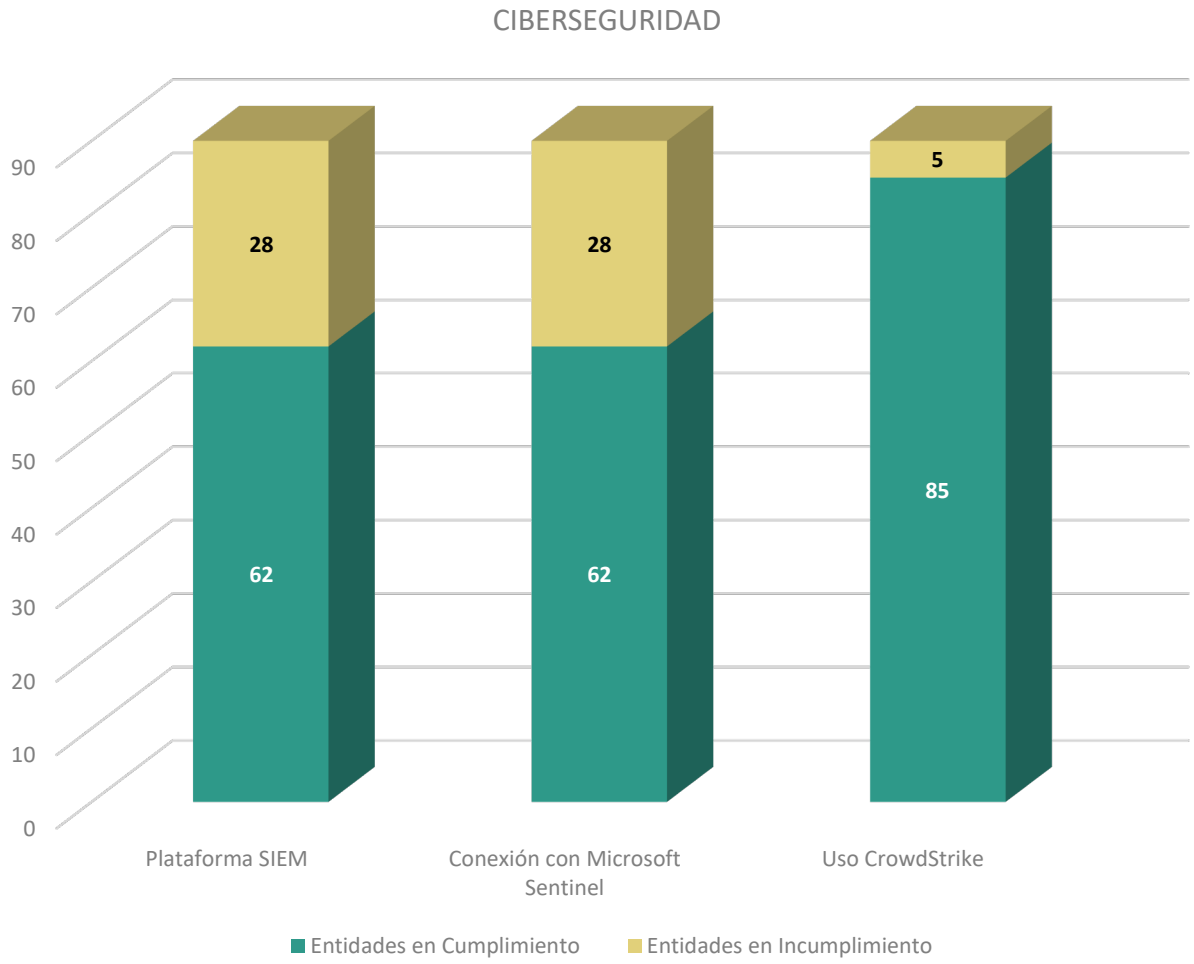


[14] Conjunto de herramientas, protocolos y definiciones que permite que diferentes sistemas o aplicaciones se comuniquen entre sí de manera eficiente.

3. **PUBLICACIONES WEB -** Identificación de la existencia de páginas o servicios web fuera del dominio pr.gov y la accesibilidad de los portales web. Aseguramiento de que los sitios web sean accesibles al ciudadano y cumplan con las evaluaciones de accesibilidad requeridas.



4. **CIBERSEGURIDAD -** Implementación de herramientas de seguridad destinadas a proteger la infraestructura tecnológica. Verificación del uso de soluciones adecuadas para la detección y gestión de incidentes de seguridad, asegurando además que la agencia esté integrada con plataformas de seguridad eficientes y efectivas.



A continuación, se presentan los resultados del cuestionario, organizados y clasificados en tres niveles de puntuación: Adecuado, Moderado e Insuficiente, en relación con las principales áreas evaluadas según la información proporcionada. La tabla destaca el desempeño basado en los criterios establecidos, mostrando el grado de cumplimiento en cada área. Estos resultados facilitan la identificación tanto de las fortalezas como de las áreas que requieren atención y mejoras para alcanzar un nivel óptimo de conformidad.

ÁREAS EVALUADAS	*Total Entidades*	*Entidades en Cumplimiento*	*RESULTADO*		*CRITERIO*	*ENTIDADES EN INCUMPLIMIENTO*	
			%	*Adecuado Moderado Insuficiente*		*EFECTO*	*ACCIÓN CORRECTIVA*
1. Cumplimiento con la Ley Núm. 75-2019 ***Evaluar la conformidad con la Ley Núm. 75-2019 en relación con la infraestructura tecnológica y los recursos necesarios***							
a. ***Cumplimiento Normativo: Conformidad con las normativas de gestión de sistemas de información, incluyendo la designación de un Oficial Principal de Informática autorizado, la existencia de normas internas para la seguridad y el uso de los sistemas.***							
¿La entidad cuenta con un Oficial Principal de Informática, autorizado por PRITS? (Arts. 12 y 13 de Ley Núm. 75-2019)	**90**	**78**	**87%**	**Adecuado**	**Ley Núm. 151-2004 Ley Gobierno Electrónico -** Art. 7 (g) **Ley Núm. 75-2019 Ley PRITS** - Arts. 12 (b), (d) y (j) **Orden Administrativa** PRITS 2021-003 **Boletín Informativo OE** - 2021-007	La ausencia de un oficial autorizado puede llevar a un manejo inadecuado de los sistemas de información y a incumplimientos legales o normativos.	Designar y capacitar a un oficial autorizado y asegurarse de que esté siempre disponible para gestionar los sistemas de información, garantizar el cumplimiento normativo y coordinar la seguridad tecnológica de la entidad.

ÁREAS EVALUADAS	*Total Entidades*	*Entidades en Cumplimiento*	*RESULTADO*		*CRITERIO*	*ENTIDADES EN INCUMPLIMIENTO*	
			%	*Adecuado Moderado Insuficiente*		*EFECTO*	*ACCIÓN CORRECTIVA*
¿Cuenta con normas internas para reglamentar el uso y la seguridad de las computadoras, los equipos de sistemas de información y las licencias de los programas computadorizados?	**90**	**85**	**94%**	**Adecuado**	**Ley Núm. 151-2004 Ley Gobierno Electrónico -** Art. 7 (g) **Ley Núm. 75-2019 Ley PRITS** - Arts. 12 (d), (h) y 13 (e) **Ley Núm. 40-2024 Ley Ciberseguridad**- Arts. 5, 7 y 9 **CC 2021-007 - Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021** - Art. 8.1 **CC 2023-004 -Para la Adopción de nueva Políticas PRITS Política ATI-015** Inciso A - 3. **Política TI-PRITS-002** - Arts. 6.2, 6.3 y 6.4 **Política TI-PRITS-007** - Secciones 6 y 7	Sin normas claras, puede haber uso inapropiado de sistemas y datos, aumentando el riesgo de brechas de seguridad.	Desarrollar y comunicar claramente normas internas para el uso y la seguridad de los sistemas. Realizar capacitaciones periódicas para asegurar que todos los usuarios comprendan y sigan estas normas.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
b. Inventario de Equipos y Sistemas: Manejo y seguimiento de los equipos y sistemas de información, incluyendo la existencia y actualización del inventario, así como la gestión del ciclo de vida de los equipos.							
¿Cuenta con un Inventario de Equipos y Sistemas de Información?	**90**	**80**	**89%**	**Adecuado**	**Ley Núm. 151-2004 Ley Gobierno Electrónico -** Art. 7 (g)**Ley Núm. 230-1974 Ley Contabilidad de Gobierno PR -** Art. 10, apartado (a) **Ley Núm. 75-2019 Ley PRITS -**Arts. 12 (b), (d) y 13 (k) **Reglamento Núm. 7080-2006,** Reglamento 11 Normas Básicas para el Control y la Contabilidad de los Activos Fijos, Art. XIV apartados A, D y E**CC 2023-004 -** Para la Adopción de nuevas Políticas PRITS **Política TI-PRITS-002 -** Art. 6.2.2 **Política TI-PRITS-003** -Art. 7 **Center for Internet Security "CIS"- Critical Security Controls, v8.1-2024** - Controles 1 y 2 **Federal Information System Controls Audit Manual (FISCAM)-Feb. 2009**, *Appendix I, IV. IS Business Process Application Level Controls*	Un inventario desactualizado puede resultar en pérdidas de equipos, dificultades en la gestión de activos y riesgos de seguridad.	Mantener un inventario actualizado de todos los equipos y sistemas. Realizar auditorías regulares del inventario para asegurar la precisión y la integridad de la información.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Tiene fecha de "end of life" de los servidores," switches" y "firewall"?	**90**	**78**	**87%**	**Adecuado**	**Ley Núm. 230-1974 Ley de Contabilidad de Gobierno PR -** Art. 10, apartado (a) **Ley Núm. 151-2004 Ley Gobierno Electrónico -** Art. 7 (g) **Ley Núm. 75-2019 Ley PRITS -** Arts. 12 (b), (d) y 13 (k) **Reglamento Núm. 7080-2006,** Reglamento 11 Normas Básicas para el Control y la Contabilidad de los Activos Fijos, Art. XIV apartados A, D y E **CC 2023-004 -** Para la Adopción de nuevas Políticas PRITS **Política TI-PRITS-002 -** Art. 6.2.2 **Política TI-PRITS-003** -Art. 7 **Center for Internet Security "CIS"- Critical Security Controls, v8.1-2024** - Controles 1 y 2 **Federal Information System Controls Audit Manual (FISCAM)-Feb. 2009**, *Appendix I, IV. IS Business Process Application Level Controls*	Equipos obsoletos pueden ser vulnerables a ataques y fallos, afectando la operación.	Establecer un sistema para monitorear y gestionar la fecha de *End of Life* de los equipos. Planificar la sustitución o actualización de equipos antes de que se vuelvan obsoletos.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Tiene un Inventario de licenciamiento de aplicaciones?	**90**	**90**	**100%**	**Adecuado**	**Ley Núm. 230-1974 Ley de Contabilidad del Gobierno PR - Art. 10, apartado (a) Ley Núm. 151-2004 Ley Gobierno Electrónico - Art. 7 (g) Ley Núm. 75-2019 Ley PRITS -Arts. 12 (b), (d) y 13 (k) Reglamento Núm. 7080-2006,** Reglamento 11 Normas Básicas para el Control y la Contabilidad de los Activos Fijos, Art. XIV apartados A, D y E **CC 2023-004 - Para la Adopción de nuevas Políticas PRITS Política TI-PRITS-002** - Art. 6.2.2 **Política TI-PRITS-003** -Art. 7 **Center for Internet Security "CIS"- Critical Security Controls, v8.1-2024** - Controles 1 y 2 **Federal Information System Controls Audit Manual (FISCAM)-Feb. 2009**, *Appendix I, IV. IS Business Process Application Level Controls* **CC 2024-004** - Directrices **Política ATI-013** - Adquisición Tecnológica **Estándares para la Seguridad Cibernética** - 3.7	El uso de *software* sin licencia puede resultar en sanciones y problemas legales. **Riesgos Legales y de Cumplimiento**: Sin un inventario, podrías estar usando *software* sin licencia adecuada, lo cual puede resultar en sanciones por incumplimiento de derechos de autor. **Riesgos Operativos**: Dificultad para rastrear qué *software* está en uso y para gestionar actualizaciones y soporte.	Mantener un inventario actualizado de todas las licencias de *software*. Asegurarse de que todos los *softwares* utilizados estén correctamente licenciados y realizar auditorías periódicas para cumplir con las normativas. Crear y mantiene un inventario centralizado de todas las licencias de *software*. Usar herramientas de gestión de activos de *software* (SAM) para automatizar y simplificar este proceso. Asegurarse de que el inventario se actualice regularmente para reflejar nuevas adquisiciones o bajas de *software*.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
c. Proyectos y Recursos Humanos: Planificación y gestión de los sistemas de información, los proyectos en curso y futuros, y su distribución. Incluye también los recursos humanos disponibles.							
¿Cuenta con un plan de trabajo para los sistemas de información?	**90**	**77**	**86%**	**Adecuado**	**Ley Núm. 151-2004 Ley de Gobierno Electrónico -** Art. 7 (g) **Ley 75-2019 Ley PRITS -** Arts. 12 (b), (c) y (d), 13 (a) y (k) **Ley Núm. 236-2010 Ley de Rendición de Cuentas Art. 4 a. (3) Orden Administrativa PRITS 2021-002** Para establecer reportes de información I 1. Sección A Formulario *PRITS* 003 Plan Estratégico **CC 2023-004** - **Para la Adopción de nuevas Políticas PRITS Política TI-PRITS-004** - Art. 7.2.1.4	La falta de un plan de trabajo puede llevar a una mala gestión de proyectos y recursos.	Desarrollar un plan de trabajo detallado para la gestión de sistemas de información. Incluir metas, plazos y responsables, y revisar y actualiza el plan regularmente.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
Se documenta todos los proyectos que se encuentran trabajando y futuros.	**90**	**87**	**97%**	**Adecuado**	**Ley Núm. 151-2004 Ley de Gobierno Electrónico -** Art. 7 (g) **Ley 75-2019 Ley PRITS -** Arts. 12 (b), (c) y (d), 13 (a) y (k) **Ley Núm. 236-2010 Ley de Rendición de Cuentas Art. 4 a. (3) Orden Administrativa PRITS 2021-002** Para establecer reportes de información I 1. Sección A Formulario *PRITS* 003 Plan Estratégico **CC 2023-004** - **Para la Adopción de nuevas Políticas PRITS Política TI-PRITS-004** - Art. 7.2.1.4	La falta de documentación de proyectos puede resultar en una planificación deficiente y en desalineación con los objetivos.	Documentar todos los proyectos en curso y futuros con detalles sobre los objetivos, cronogramas y recursos. Realizar revisiones periódicas para asegurar que los proyectos se alineen con los objetivos estratégicos.
¿Cuenta con un organigrama del área u oficina de sistemas?	**90**	**73**	**81%**	**Adecuado**	**Ley Núm. 230-1974 Ley de Contabilidad de Gobierno de PRLey Núm. 151-2004 Ley Gobierno Electrónico -** Art. 7 (g), (i) **Ley Núm. 75-2019 Ley PRITS** -Art. 12 (b), (d) **Orden Administrativa PRITS 2021-002** -Para establecer reportes de información Primero I (2) Sección B Formulario PRITS-003 Plan Estratégico **CC 93-11-OGP- Normas Administración Presupuestaria y Aspectos Organizacionales …**	Un organigrama desactualizado puede causar confusión sobre roles y responsabilidades.	Mantener un organigrama actualizado que refleje la estructura actual del área de sistemas. Revisar y ajustar el organigrama en función de cambios organizacionales y asegurar que todos los roles y responsabilidades estén claramente definidos.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
La descripción de los puestos de los empleados y funcionarios se mantiene actualizada.	**90**	**85**	**94%**	**Adecuado**	**Ley Núm. 230-1974** ***Ley de Contabilidad de Gobierno de PR*** **Ley Núm. 151-2004** ***Ley Gobierno Electrónico*** **-** Art. 7 (g), (i) **Ley Núm. 75-2019** ***Ley PRITS*** -Art. 12 (b), (d) **Orden Administrativa PRITS 2021-002** -Para establecer reportes de información Primero I (2) Sección B Formulario PRITS-003 Plan Estratégico **CC 93-11-OGP-*Normas Administración Presupuestaria y Aspectos Organizacionales …***	Descripciones de puestos inadecuadas pueden llevar a una falta de claridad en las responsabilidades y a una gestión deficiente.	Actualizar las descripciones de puestos regularmente para reflejar responsabilidades y competencias actuales. Asegurarse de que cada puesto tenga una descripción clara y revisar estas descripciones con frecuencia.
d. Seguridad en las Redes: Medidas de seguridad en redes, como firewalls.							
¿Cuenta con un análisis de riesgos preparado para los sistemas de información?	**90**	**48**	**53%**	**Moderado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** - Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** -Arts. 12 (b), (d) y 13 (k) **Ley Núm. 40-2024** ***Ley de Ciberseguridad*** -Art. 3 (6) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** **-** Art. 6.1.8 **Estándares para la Seguridad Cibernética - 3.7** **CC 2023-04** ***Adopción de Nuevas***	Sin un análisis de riesgo, las vulnerabilidades pueden quedar sin identificar, aumentando el riesgo de incidentes de seguridad.	Realizar análisis de riesgo periódicos para identificar y mitigar vulnerabilidades. Establecer un calendario de revisiones regulares y asegurar la participación de expertos en seguridad.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					Políticas PRITS ***Política ATI-015*** -Apartado C		
¿Cuenta con un "Firewall"?	**90**	**87**	**97%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** -Arts. 12 (b), (d) y 13 (k) **Ley Núm. 40-2024** ***Ley de Ciberseguridad*** - Art. 7 (13) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** **-** Art. 6.1.9 **Estándares para la Seguridad Cibernética** - 3.1.4 **CC 2023-04** ***Adopción de Nuevas Políticas PRITS*** ***Política TI-PRITS-002*** - 6.2 Normas Generales -6.2.14 **Política TI-PRITS-004** -7.2 Seguridad - 7.2.7.4 **Center for Internet Security "CIS"- Critical Security Contro**ls, v8.1-2024 - CIS Control 9 **Federal Information System Controls Audit Manual (FISCAM) - 2009**, (**FISCAM**) 2.1.4 **National Institute of Standard and Technology (NIST) Special Publication SP 800-41 r1 -** Guidelines on Firewalls and Firewall Policy	La falta de un *firewall* actualizado puede permitir accesos no autorizados y ataques.	Mantener el *firewall* actualizado y revisar sus configuraciones regularmente. Implementar reglas estrictas de acceso y realiza pruebas de seguridad para asegurar que proteja adecuadamente contra amenazas.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
e. Gestión de Privilegios de Acceso: Políticas de cambio de contraseñas y los requisitos de autenticación, la administración de los privilegios de acceso, la reevaluación periódica de permisos, la remoción de accesos para empleados que dejan la agencia, y los controles para gestionar el uso de Internet. También examina la protección de la información en redes internas y externas.							
¿Existen políticas establecidas para forzar cambio de contraseñas para los accesos de los sistemas de información ya sea en términos de 30, 60, 90 días a los usuarios?	**90**	**82**	**91%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-**Art. 7 (g) **Ley Núm. 75-2019 Ley PRITS** -Arts. 12 (d) y 13 (k) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Estándares para la Seguridad Cibernética*** **-** 3.5.9 y 3.5.10 **CC 2023-04** ***Adopción de Nuevas Políticas PRITS*** ***Política TI-PRITS-002*** **-**6.2 Normas Generales - 6.2.11, 6.4.5 **Política TI-PRITS-004** Apoyo y Mantenimiento a Sistemas Internos -7.2.3.2 **Política TI-PRITS-007** Cuentas... - 7.3.1.2, 7.3.2.4, 7.4.1 @ 7.4.11	Políticas inadecuadas pueden llevar a contraseñas débiles y vulnerabilidades de seguridad.	Establecer políticas estrictas de cambio de contraseñas, incluyendo requisitos de complejidad y frecuencia de cambio. Implementar controles para asegurar que las contraseñas se actualicen de manera segura y regular.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
Existen mecanismos de autenticación del dominio y las aplicaciones.	**90**	**90**	**100%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** **-**Arts. 12 (b), (d) y 13 (k) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Estándares para la Seguridad Cibernética*** **-**3.3 y 3.5.9	Mecanismos de autenticación débiles pueden permitir accesos no autorizados.	Implementar mecanismos de autenticación robustos, como autenticación multifactorial (MFA), para fortalecer la seguridad. Revisar y actualiza estos mecanismos regularmente para adaptarse a nuevas amenazas y tecnologías.
¿Los privilegios de acceso de los usuarios se reevalúan periódicamente?	**90**	**68**	**76%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** **-**Arts. 12 (b), (d) y 13 (k) ***Ley Núm. 40-2024 Ley de Ciberseguridad*** Art. 7 (14) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Estándares para la Seguridad Cibernética*** **-**Servicios Contratados Art. 3.4.5, Controles adicionales de TI -3.5.7 **CC 2023-04** ***Adopción de Nuevas Políticas PRITS*** ***Política TI-PRITS-002*** **-**6. Política - 6.1 General - 6.2.11 **Política TI-PRITS-007 -** Control de Acceso 7.1.6 -Gestiones de	La falta de reevaluación puede resultar en permisos excesivos y riesgos de abuso.	Reevaluar regularmente los privilegios de acceso para asegurarse de que cada usuario tenga solo los permisos necesarios. Implementar un proceso para revisar y ajustar estos permisos de manera periódica.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					Cuenta., Incisos 7.2.5 **Center for Internet Security "CIS"- Critical Security Controls, v8.1- 2024 -** CIS Control 4 y 14		
Tiempo que se reevalúan los privilegios de acceso de los usuarios.	**90**	**66**	**73%**	**Moderado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS*** -Arts. 12 (b), (d) y 13 (k) **Política TI-PRITS-007** - Control de Acceso 7.1.6 - Gestiones de Cuenta., Inciso 7.2.5	Intervalos inadecuados pueden llevar a una gestión ineficaz de accesos.	Establece un intervalo fijo para la reevaluación de privilegios, como trimestral o semestral. Ajusta el intervalo según el riesgo y la criticidad de los accesos para mantener una gestión efectiva.
¿Se remueve de manera expedita/rápida los permisos de acceso a empleados/as que dejan la agencia?	**90**	**86**	**96%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -**Art. 7 (g)**Ley Núm. 75-2019 *Ley PRITS*** -Arts. 12 (d) y 13 (k)**CC 2021-007 - Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021 -** Art. 6.2.3 y 6.2.4 **CC 2023-04 *Adopción de Nuevas Políticas PRITSPolítica TI-PRITS 007*** Art. 7.1.2, 7.1.4, 7.1.6, 7.7.3, 7.7.4 **Center for Internet Security "CIS"- Critical Security Controls**, v8.1-2024 - CIS Control 16	La falta de remoción rápida de permisos puede resultar en accesos no autorizados después de la salida de empleados.	Implementar un proceso para la remoción rápida de permisos cuando un empleado salga de la empresa o cambie de rol. Asegurarse de que este proceso sea automatizado si es posible para reducir el riesgo de accesos no autorizados.

ÁREAS EVALUADAS	*Total Entidades*	*Entidades en Cumplimiento*	*RESULTADO*		*CRITERIO*	*ENTIDADES EN INCUMPLIMIENTO*	
			%	*Adecuado Moderado Insuficiente*		*EFECTO*	*ACCIÓN CORRECTIVA*
Controles que utiliza la entidad para evitar el uso inadecuado del Internet de los usuarios.	**90**	**88**	**98%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** -Arts. 12 (d) y 13 (k) **Ley Núm. 40-*2024 Ley de Ciberseguridad*** -Art. 7 (1) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** **-** Art. 6.2.3 y 6.2.4 **Estándares para la Seguridad Cibernética** Arts. 3.1 y 3.2.1.2 **CC 2023-04** ***Adopción de Nuevas Políticas PRITS Política TI-PRITS-002*** Art. 6 - 6.1 y 6.3 **Política TI-PRITS 004** Art. 7.2.5.2 **Política TI-PRITS 007** Art. 7.1.1 y 7.7.4 ***Federal Information System Controls Audit Manual - 2009*****, (FISCAM)** Art. 3.5	Sin controles, el uso inadecuado de Internet puede llevar a problemas de seguridad y productividad.	Establecer políticas y controles para el uso de Internet, como filtrado de contenido y monitorización del tráfico web. Capacitar a los empleados sobre el uso seguro y responsable de Internet.
Controles de autenticación, autorización, confidencialidad, integridad y monitoreo para proteger la información y los sistemas en aquellos casos en los que sea necesario acceder a la red interna desde fuera de las instalaciones de la agencia.	**90**	**90**	**100%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** **-**Arts. 12 (d) y 13 (k) **Ley Núm. 40-2024** ***Ley de Ciberseguridad*** Art. 7 (2) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** **-** Art. 6.1 **Estándares para la Seguridad Cibernética** Art. 3.3	Sin controles adecuados, el acceso remoto puede ser vulnerable a ataques.	Implementar controles robustos para autenticación y autorización remota, como autenticación multifactorial (MFA) y *VPN* segura. Revisa y actualiza estos controles regularmente para proteger el acceso remoto.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					CC 2023-04 *Adopción de Nuevas Políticas PRITS* ***Política TI-PRITS-004*** - Servicios de Tecnologías 7.2.7.1 **Política TI-PRITS-005** - Art. 9.1.8 **Política TI-PRITS 007-** Art. 7.4 **Center for Internet Security "CIS"- Critical Security Controls, v8.1- 2024 -** CIS Control 4		
Controles necesarios para garantizar la confidencialidad de los datos sensibles en reposo y en tránsito en redes no seguras.	**90**	**87**	**97%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -**Arts. 12 (b), (d) y 13 (k) **Ley Núm. 40-2024 *Ley de Ciberseguridad*** Art. 3 (3) y 7 (2) y (4) **CC 2021-007 - *Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021* -** Art. 6.1.1 y 6.1.2 **Estándares para la Seguridad Cibernética** Art. Internet - 3.1.5 y Controles adicionales TI 3.5.5	Datos sin cifrar pueden ser interceptados o accedidos por personas no autorizadas.	Cifrar los datos tanto en reposo como en tránsito para proteger la confidencialidad. Utilizar algoritmos de cifrado fuertes y asegurarse de que los sistemas y redes soporten estas prácticas de cifrado.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
f. Evaluación de Vulnerabilidad y Seguridad del Sistema:Prácticas y medidas relacionadas con la seguridad de los sistemas, incluyendo conexiones remotas, parches, encriptación, y políticas de retención y disposición de hardware.							
¿Existen protocolos para conexiones remotas seguras en la agencia?	**90**	**85**	**94%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS*** - Arts. 12 (b), (d) y 13 (k) **Ley Núm. 40-2024 *Ley de Ciberseguridad*** Art. 7(4) (5) **Estándares para la Seguridad Cibernética** 3.1.6 **National Institute of Standard and Technology (NIST) Special Publication - SP 800-113 -** *Guide to SSL VPNs*	La falta de seguridad en las conexiones remotas puede exponer la red de la agencia a ataques cibernéticos, accesos no autorizados y robo de datos. Conexiones inseguras pueden servir como punto de entrada para *malware* y otras amenazas externas.	Implementar medidas de seguridad robustas para las conexiones remotas, como autenticación multifactorial (MFA), *VPNs* seguras, y cifrado de datos. Monitorear y auditar regularmente estas conexiones para detectar accesos no autorizados y amenazas.
¿Cuenta con un plan de mantenimiento de parches y certificaciones de seguridad del sistema?	**90**	**66**	**73%**	**Moderado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS*** - Art. 12 (b), (d), 13 (k) **Ley 40-2024 *Ley de Ciberseguridad*** Art. 7 (2) **CC 2023-004 *Para la Adopción de nuevas Políticas PRITS Estándares para la Seguridad Cibernética 3.1.6.2*** **Política TI-PRITS 004** Art. 7.2.1.6 **Federal Information System Controls Audit Manual - 2009, (FISCAM)** -Art. 2.5.1A	Sin mantenimiento de parches ni certificaciones, los sistemas quedan vulnerables a ataques y fallos de seguridad.	Desarrollar un plan de mantenimiento de parches y asegurar que todos los sistemas reciban actualizaciones de seguridad de manera oportuna. Obtener y mantener certificaciones de seguridad relevantes para asegurar la conformidad y la protección contra vulnerabilidades.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Se utilizan tecnologías de virtualización o servicios en la nube para el procesamiento y almacenamiento de datos?	**90**	**83**	**92%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -**Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -** Art. 12 (b), (d) y 13 (k) **CC 2023-004 - *Para la Adopción de nuevas políticas PRITS*** **Política TI-PRITS-004 - Solicitud Servicios -**Art. 6.9 **Orden Administrativa 2021-002** Para establecer reportes de información - Primero I 3. Sección C Formulario PRITS-003 del Plan Estratégico **Orden Administrativa 2023-001** Implantar Nuevas Directrices - Art. 9 **National Institute of Standard and Technology (NIST) Special Publication (SP) -** SP 800-210 *Guideline General Access Control Guidance for Cloud System-2020*	La falta de medidas de seguridad adecuadas para la virtualización y servicios en la nube puede resultar en la exposición de datos sensibles a amenazas, así como en problemas de cumplimiento normativo y pérdida de integridad de los datos.	Implementar medidas de seguridad específicas para la virtualización y servicios en la nube, como cifrado de datos, controles de acceso estrictos, y evaluaciones de riesgos. Asegurarse de cumplir con las normativas y estándares de seguridad aplicables.
¿Se aplican medidas de seguridad en entornos de nube?	**90**	**79**	**88%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -** Art. 12 (b) y (d), 13 (k) **Orden Administrativa PRITS-2023-001 -** Art. 8 **Política TI-PRITS-002** - 6.2.14 **National Institute of Standard and Technology (NIST) Special Publication (SP)** - *SP 800-210 Guideline General Access Control Guidance for Cloud System-2020*	La ausencia de medidas de seguridad específicas para entornos en la nube puede llevar a brechas de datos, accesos no autorizados, y la exposición de información confidencial a terceros no deseados.	Establecer medidas de seguridad adecuadas para entornos en la nube, incluyendo controles de acceso, cifrado de datos y auditorías regulares. Utilizar herramientas de seguridad y servicios proporcionados por el proveedor de la nube para proteger los datos sensibles.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Tiene configuraciones para encriptar los archivos confidenciales?	**90**	**47**	**52%**	**Moderado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** -Art. 7 (g)**Ley Núm. 75-2019** ***Ley PRITS*** - Art. 12 (b) y (d), 13 (k)**Ley 40-2024** ***Ley de Ciberseguridad*** Art. 7 (4) y (5) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Estándares para la Seguridad Cibernética*** **-** Art. 3.1.5 y 3.1.6 **CC 2023-004** ***Para la Adopción de Nuevas Políticas PRITS*** **Política TI-PRITS-002** Art. 6.4.4 **Política TI-PRITS-007** Art. 7.5.1	Sin cifrado para los archivos confidenciales, los datos pueden ser fácilmente interceptados y accedidos por actores maliciosos, poniendo en riesgo la privacidad y la seguridad de la información.	Configurar cifrado fuerte para todos los archivos confidenciales tanto en reposo como en tránsito. Utilizar algoritmos de cifrado robustos y asegurar que el cifrado sea implementado correctamente en todos los sistemas relevantes.
¿Cuenta con configuraciones y certificados de seguridad que controlan el acceso a programas desde el Internet?	**90**	**81**	**90%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** -Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** - Art. 12 (b) y (d), 13 (k) **Ley Núm. 40-2024** ***Ley de Ciberseguridad*** Art. 7 (2) y (5) **CC 2023-004** ***Para la Adopción de Nuevas Políticas PRITS Política*** **TI-PRITS-002** Art. 6.3	La falta de configuraciones y certificados de seguridad adecuados puede permitir accesos no autorizados y ataques dirigidos a los programas accesibles desde Internet, comprometiendo la seguridad del sistema.	Asegurar las configuraciones de seguridad y obtener certificados adecuados para controlar el acceso a programas accesibles desde Internet. Implementar medidas como *firewalls*, certificados *SSL/TLS*, y mecanismos de autenticación para proteger estos programas.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Existe una evaluación de vulnerabilidad de sus sistemas?	**90**	**35**	**39%**	**Insuficiente**	**Ley Núm. 75-2019 *Ley de PRITS* -** Art. 12 (b) y (d), 13 (k) **Ley Núm. 151-2004 *Ley Gobierno Electrónico* -** Art. 7 (g) **Ley Núm. 40-2024 *Ley de Ciberseguridad*** - Art. 3 (6) y Art. 5 párrafo 2 **Política ATI-015 -**Apartado C **CC 2021-007 - *Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021* -** Art. 7.2.7 **Estándares para la Seguridad Cibernética 2021 -** Art. *Software* y Aplicaciones 3.2.1.4 **Federal Information System Controls Audit Manual - 2009, (FISCAM) -** Art. 2.5.1 A	La falta de evaluaciones periódicas de vulnerabilidad puede dejar sistemas expuestos a riesgos no detectados, aumentando la probabilidad de explotación por parte de atacantes.	Realizar evaluaciones de vulnerabilidad periódicas para identificar y mitigar riesgos. Utilizar herramientas de escaneo de vulnerabilidades y realizar pruebas de penetración para detectar y corregir fallos de seguridad.
¿Tiene instalados controles de detección como detección de programas no deseados (por ejemplo, virus, adware, spyware, malware, ransomware) y la prevención de eventos o actividades de intrusión que puedan afectar la seguridad de la información?	**90**	**88**	**98%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -**Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -** Art. 12 (b) y (d), 13 (k) **Ley Núm. 40-2024 *Ley de Ciberseguridad* -** Art. 7 (13) **CC 2021-007 - *Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021* -** Art. 6.1.1 @ 6.1.13 **Estándares para la Seguridad Cibernética -** Informes 3.8.2 - Software y Aplicaciones 3.2.1.3 - Controles Adicionales de TI 3.5.1 -Dispositivos Móviles 3.6.1.4 **CC 2023-04 *Para la Adopción de***	La ausencia de controles de detección y prevención puede resultar en infecciones por *malware*, pérdida de datos, y actividades de intrusión que comprometan la seguridad de la información.	Implementar controles de detección y prevención de *malware*, como *software* antivirus y *anti- malware* actualizado. Realizar análisis de seguridad regulares y configurar alertas para detectar y responder a actividades sospechosas.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					Nuevas Políticas PRITS **Política TI-PRITS-002** Art. 6.2.14 **Política TI-PRITS-004** Art. 7.2.7.4 **Federal Information System Controls Audit Manual - 2009, (FISCAM)** - Art. 2.5.1A		
¿Cuenta con un plan de concienciación a los usuarios de la entidad?	**90**	**63**	**70%**	**Moderado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** - Art. 7 (g)**Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b), (d), (h) y 13 (i) y (k)**Ley Núm. 40-2024** ***Ley de Ciberseguridad*** **-** Art. 7 (17)**Política ATI-015** -Apartado H, I **CC 2021-007 -** ***Establecimiento Política CiberseguridadPolítica para la Seguridad Cibernética 2021*** - Arts. 6.2.1 y 7.3.13**CC 2023-004 - Para la Adopción de nuevas Políticas PRITS Política TI-PRITS-007 -**Art. 7.7 **Federal Information System Controls Audit Manual - 2009, (FISCAM) -** Art.3.1**Center for Internet Security "CIS"- Critical Security Controls,** v8.1-2024, CIS Control 17	La falta de un programa de concienciación puede llevar a que los usuarios no conozcan las mejores prácticas de seguridad, aumentando el riesgo de errores humanos y comportamientos inseguros que podrían comprometer la seguridad de la información.	Desarrollar e implementar un programa de concienciación en seguridad para los usuarios. Realizar capacitaciones regulares sobre las mejores prácticas de seguridad, amenazas comunes y cómo evitar errores que podrían comprometer la seguridad de la información.
¿Existe alguna política para retención/destrucción de datos?	**90**	**44**	**49%**	**Insuficiente**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **- Art. 7 (g) Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b), (d) y 13 (k) **Ley Núm. 40-2024** ***Ley de Ciberseguridad*** **-** Art. 7 (18) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad***	La ausencia de una política clara puede provocar la acumulación de datos innecesarios y aumentar el riesgo de exposición de información sensible por retención indebida.	Establecer y aplicar una política clara para la retención y destrucción de datos. Definir periodos de retención, métodos de destrucción segura y cumplir con las

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					Estándares para la Seguridad Cibernética **-**Controles Adicionales TI **-** 3.5.12 y 3.5.13 **Reglamento Núm. 7080-2006,** ***Reglamento 11 Normas Básicas para el Control y la Contabilidad de los Activos Fijos*****,** Art. XIV apartados A, D y E **CC 2023-004 -** ***Para la Adopción de Nuevas Políticas PRITS*** **Política TI-PRITS-002 -** Art. 6.2.7 **Política TI-PRITS-003 -** Art. 6, 7.2, 7.3 y 7.6 **Política TI-PRITS-007 -** Art. 7.7		Regulaciones y normativas pertinentes.
¿Cuál es la política de disposición de "hardware" y medios de almacenamiento? Explique y provea evidencia	**90**	**75**	**83%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b), (d) y 13 (k) **Ley Núm. 40-2024** ***Ley de Ciberseguridad*** **-** Art. 7 (18) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Estándares para la Seguridad Cibernética*** **-Controles Adicionales TI -** 3.5.12 y 3.5.13 **Reglamento 9157 -*Reglamento de la Propiedad Excedente de la ASG* -** Capítulos VI y VII **CC 2023-004 -** ***Para la Adopción de Nuevas Políticas PRITS*** **Política TI-PRITS-003 -**Art. 6, 7.1, 7.4, 7.5 y 7.6	Sin una política de disposición segura, los datos sensibles pueden ser expuestos y recuperados de dispositivos obsoletos.	Implementar una política de disposición segura para *hardware* y medios de almacenamiento. Asegurarse de que los dispositivos obsoletos sean destruidos de manera segura para evitar la exposición de datos sensibles. Utilizar métodos de destrucción aprobados y documentar el proceso.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
g. Control de Acceso Físico y Seguridad de las Instalaciones: Medidas de seguridad física en las instalaciones de procesamiento, como el control de acceso, protección contra incendios y condiciones ambientales.							
¿La instalación de procesamiento está ubicada en un lugar que provee condiciones apropiadas para evitar el acceso no autorizado (puertas, paredes, ventanas)? describa	**90**	**89**	**99%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** -Art. 7 (g)**Ley Núm. 75-2019** ***Ley PRITS*** - Art. 12 (b), (d) y 13 (k)**Ley Núm. 40-2024** ***Ley de Ciberseguridad*** - Art. 7 (15) **CC 2021-007 -** ***Establecimiento Política CiberseguridadPolítica para la Seguridad Cibernética 2021*** -Art. 1**Estándares para la Seguridad Cibernética** -Controles Adicionales TI 3.5.3**FISCAM** - 3.2	La falta de controles físicos puede permitir el acceso no autorizado a áreas sensibles.	Implementar sistemas de control de acceso como tarjetas magnéticas o biometría y llevar un registro detallado de todas las entradas y salidas. Establecer políticas claras de acceso y realizar auditorías periódicas para garantizar que solo el personal autorizado tenga acceso a áreas sensibles.
¿Se controla o restringe el acceso físico a la instalación de procesamiento mediante tarjetas, códigos o cualquier otro medio de autenticación y autorización?	**90**	**79**	**88%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-Art. 7 (g) Ley Núm. 75-2019** ***Ley PRITS*** - Art. 12 (b), (d) y 13 (k) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** -Art. 1 **Estándares para la Seguridad Cibernética** -Controles Adicionales TI 3.5.3 y 3.5.16 **CC 2023-004 -** ***Para la Adopción de Nuevas Políticas PRITS*** **Política TI-PRITS-007 -**	Sin un registro adecuado, puede ser difícil monitorear y gestionar el acceso.	Asegurar de revisar y actualizar regularmente los permisos de acceso, manteniendo una documentación precisa de quién tiene acceso a cada área. Capacitar al personal sobre las políticas de acceso y los procedimientos correspondientes para asegurar una gestión efectiva.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					Art. 7.4.12 **Federal Information System Controls Audit Manual - 2009, (FISCAM) -** 3.2 **Center for Internet Security "CIS"- Critical Security Controls, v8.1-2024,** Control CIS 15		
¿La instalación de procesamiento cuenta con supresores de incendio (detectores de humo y sistema de supresión)?	**90**	**81**	**90%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b), (d) y 13 (k) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** **-** Art. 1 **Estándares para la Seguridad Cibernética** -Controles Adicionales TI 3.5.3 **Federal Information System Controls Audit Manual - 2009, (FISCAM)** - 3.2	La falta de protección contra incendios puede resultar en daños significativos en caso de incendio.	Instalar y mantener sistemas de supresión de incendios adecuados, como detectores de humo y rociadores automáticos. Realizar mantenimientos periódicos para asegurar su funcionalidad y capacitar al personal en procedimientos de evacuación y manejo de incendios.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Existen controles para asegurar la existencia de niveles adecuados de temperatura y de humedad en la instalación de procesamiento?	**90**	**69**	**77%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b) y (d), 13 (k) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** - Art. 6.1.8 **Estándares para la Seguridad Cibernética 2021** - Controles Adicionales Art. 3.5.3 **Federal Information System Controls Audit Manual - 2009, (FISCAM)** - 3.2	La falta de control puede dañar equipos sensibles y afectar su funcionamiento.	Utilizar sistemas de climatización y deshumidificación para mantener condiciones ambientales óptimas. Implementar sensores de temperatura y humedad con alertas para monitorizar las condiciones en tiempo real y realiza mantenimientos regulares en estos sistemas.
¿Se utilizan equipos para mantener el funcionamiento de los sistemas y proteger los mismos contra interrupciones y fluctuaciones de energía eléctrica?	**90**	**90**	**100%**	**Adecuado**	**Ley Núm. 151-*2004 Ley de Gobierno Electrónico*** **-** Art. 7 (g)**Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b) y (d), 13 (k) **Orden Administrativa PRITS-2021-002 -** PRIMERO I. 3.**CC 2021-007 - Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021 -** Art. 1 **Estándares para la Seguridad Cibernética 2021 -** Controles Adicionales TI 3.5.3 **Política ATI - 015** Apartado E **Federal Information System Controls Audit Manual - 2009, (FISCAM)** - 3.2	Las interrupciones de energía pueden causar pérdidas de datos y fallos en los sistemas.	Instalar sistemas de alimentación ininterrumpida (*UPS*) y, si es necesario, generadores para proporcionar respaldo en caso de interrupciones prolongadas de energía. Desarrollar un plan de recuperación para garantizar la continuidad del negocio durante estos eventos.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
h. Centro de Recuperación de Desastre: ***Revisa las estrategias y recursos para la recuperación tras desastres, incluyendo la ubicación y mantenimiento de resguardos y la eficacia del centro de recuperación.***							
¿Cuenta con un plan de recuperación de desastres?	**90**	**72**	**80%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 12 (b) y (d) y 13 (k) **Ley Núm. 40-2024 *Ley de Ciberseguridad* -** Art. 7 (18) **Orden Administrativa PRITS-2023-001** Quinto Disposiciones Generales 4. **CC 2021-007 - *Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021* -** Art. 7.2 (7.2.10) **Política ATI-015** -Art. D. **CC 2023-004 -** Para la Adopción de nuevas Políticas PRITS **Política TI-PRITS-004** -Arts. 7.2.1.6, 7.2.4 **Política TI-PRITS-005** -Arts. 7.1.8, 8.1.3 y 9.1.3 **Federal Information System Controls Audit Manual (FISCAM)-Feb. 2009, (FISCAM)** 3.5	Sin un plan de recuperación, la entidad puede enfrentar largos tiempos de inactividad y pérdida de datos en caso de desastre.	Desarrollar y aprobar un plan de recuperación de desastres completos. Asegurarse de que todos los empleados estén familiarizados con el plan y realiza simulacros para garantizar la eficacia en caso de emergencia.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Cuenta con un sistema de resguardos?	**90**	**85**	**94%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -** Art. 12 (b) y (d), 13 (k) **Ley Núm. 40-2024 *Ley de Ciberseguridad*** - Art. 7 (18) **CC 2023-04 *Para la Adopción de Nuevas Políticas PRITS*** **CC 2024-005 *Recordatorio Preparación y Procedimientos para la Protección...*** **Política TI-PRITS-004 -** Secciones 7.2.4 y 7.2.7.1 **Política TI-PRITS -005 -** Art. 6.1.8 **Federal Information System Controls Audit Manual - 2009, (FISCAM) -** 3.5	Sin resguardos, la recuperación después de un fallo puede ser lenta y costosa.	Implementar un sistema de resguardos eficiente que garantice la recuperación rápida y económica después de un fallo. Asegurase de que los datos y sistemas críticos estén respaldados regularmente y almacenados de manera segura.
¿Los resguardos se mantienen fuera de las facilidades principales o de producción?	**90**	**74**	**82%**	**Adecuado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 7 (g)**Ley Núm. 75-2019 *Ley PRITS* -** Art. 12 (b), (d) y 13 (k) **CC 2023-04 *Para la Adopción de Nuevas Políticas PRITS...* Orden Administrativa 2021-002** I. (3)**Federal Information System Controls Audit Manual - 2009, (FISCAM)** - 3.5	Resguardos almacenados en las mismas instalaciones pueden perderse en un desastre.	Almacenar copias de seguridad en ubicaciones externas para protegerlas contra desastres que afecten las instalaciones principales. Utilizar servicios de almacenamiento en la nube o sitios de resguardos geográficamente separados.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
¿Tiene un centro de recuperación de desastres?	**90**	**50**	**56%**	**Moderado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **- Art. 7 (g)** **Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b), (d) y 13 (k) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** **-** Art. 7.2.10 **Política ATI-015 -** Apartado D **CC 2023-04** ***Para la Adopción de Nuevas Políticas PRITS Política TI-PRITS-004*** **-**7.2.4 **Federal Information System Controls Audit Manual - 2009, (FISCAM) -** 3.5 **Prácticas Profesionales para la Gestión de Continuidad del Negocio (DRII) - Práctica Profesional Uno:** Gestión de Programas	La falta de un centro puede resultar en una recuperación lenta y desorganizada después de un desastre.	Establecer un centro de recuperación de desastres para facilitar una respuesta rápida y organizada en caso de emergencia. Este centro debe estar equipado para gestionar la recuperación de sistemas y datos críticos.
¿Hace pruebas periódicas del centro?	**90**	**40**	**44%**	**Insuficiente**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 7 (g) **Ley Núm. 75-2019** ***Ley PRITS*** **-** Art. 12 (b), (d) y 13 (k) **CC 2021-007 -** ***Establecimiento Política Ciberseguridad Política para la Seguridad Cibernética 2021*** **-** Art. 7.2.7 **Política ATI-015 -** Apartado H.1 **CC 2023-04 Para la Adopción de Nuevas** ***Políticas PRITS Política TI-PRITS-004*** **-**7.2.3.3 **Prácticas Profesionales para la Gestión de Continuidad del Negocio (DRII)** - Práctica	Sin pruebas, es difícil asegurar que el centro funcionará correctamente en una emergencia.	Realizar pruebas periódicas del centro de recuperación de desastres para verificar su funcionalidad y eficacia en situaciones de emergencia. Estas pruebas deben incluir simulaciones completas para identificar y corregir posibles problemas antes de un desastre real.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					Profesional Uno: Gestión de Programas **Federal Information System Controls Audit Manual - 2009, (FISCAM) -** 3.5		
Para el Plan de recuperación de Desastres, ¿realiza simulacros para ejecución del Plan?	**90**	**33**	**37%**	**Insuficiente**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **Política ATI-015 -** Apartado D (1) **Federal Information System Controls Audit Manual - 2009, (FISCAM) -** 3.5 (test) **Prácticas Profesionales para la Gestión de Continuidad del Negocio (DRII) -** Práctica Profesional Uno: Gestión de Programas **Center for Internet Security "CIS"- Critical Security Controls, v8.1-2024**, Control CIS 15	La falta de simulacros puede llevar a una respuesta inadecuada durante un desastre real.	Realizar simulacros periódicos del plan de recuperación de desastres para garantizar que el personal esté preparado y el plan sea efectivo. Simular diferentes escenarios para identificar y corregir debilidades.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
i. Interconexión de Sistemas:Analiza la conexión de los sistemas con otras agencias, la disponibilidad de estos sistemas, los simulacros de recuperación y la gestión de contratos para servicios de certificación.							
¿Tiene sistemas que se interconectan con otros agencias o entidades?	**90**	**39**	**43%**	**Insuficiente**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 7 (g) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **Orden Administrativa PRITS - 2021-002** **Ordenes Ejecutivas 2021-007 y 2021-008** **Política ATI-006** Disposiciones Normativa A. 1.4 **Política ATI-013** Política **Política ATI-015** Apartado J	Las interconexiones no documentadas pueden resultar en brechas de seguridad y mala gestión de datos.	Documentar todas las interconexiones con otras agencias para prevenir brechas de seguridad y asegurar una gestión adecuada de datos. Establecer acuerdos claros sobre el manejo y protección de la información compartida.
2. Desarrollo de "API's" Revisar el desarrollo y la gestión de interfaces de programación (APIs) para asegurar que cumplan con los estándares de documentación, versionamiento y manejo de cambios. Verificar que las APIs estén implementadas correctamente y que sigan las mejores prácticas para su uso y mantenimiento.							
¿Ha desarrollado alguna Interfaz de Programación o "API" en su agencia y se encuentra activo?	**90**	**23**	**26%**	**Insuficiente**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **CC 2023-04 *Para la Adopción de Nuevas Políticas PRITS*** **Política TI-PRITS-001 -**1, 6.4, 7 y 8.2. **Carta General PRITS - Repositorios de Interfaces (*APIs*),** 9-sept-2020	La falta de *APIs* puede restringir la integración de sistemas y la automatización de procesos. Además, la falta de interoperabilidad puede dificultar la comunicación entre diferentes aplicaciones y servicios.	**Evaluar Necesidades**: Considerar desarrollar *APIs* para mejorar la integración y eficiencia de los sistemas. **Adoptar Mejores Prácticas**: Sigue las mejores prácticas de desarrollo de *APIs* para asegurar su

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
					OE-2013-013 Boletín Administrativo - Primero **Guía *PRITS*-004 Guías de Interfaz y Diseño (*GUIDI*)**		efectividad y mantenimiento.
Los APIs cuentan con documentación siguiendo el formato estándar OpenAPI	**90**	**14**	**16%**	**Insuficiente**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -**Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **CC 2023-04 *Para la Adopción de Nuevas Políticas PRITS* Política PRITS T-001 -** 1, 6.4, 7 y 8.2 **Carta General PRITS - Repositorios de Interfaces (APIs), 9**-sept-2020 **OE 2013-013 Boletín Administrativo** - Primero **Guía PRITS-004 Guías de Interfaz y Diseño (GUIDI)**	**Incompatibilidad**: No seguir el estándar Open *API* puede llevar a problemas de interoperabilidad con otras herramientas y sistemas. **Difícil Documentación**: La falta de estandarización puede hacer que la documentación sea menos clara y accesible.	**Adoptar Open *API***: Implementar el formato estándar Open *API* para asegurar la compatibilidad y mejorar la documentación.
Los API cuentan con versionamiento	**90**	**14**	**16%**	**Insuficiente**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **CC 2023-04 *Para la Adopción de Nuevas Políticas PRITS* Política TI- PRITS-001 -** 1, 6.4, 7 y 8.2**Carta General PRITS - 9/sept/2020 Repositorios de Interfaces (*APIs*) OE 2013-013 Boletín Administrativo - Primero Guía *PRITS*-004 Guías de Interfaz y Diseño (*GUIDI*)**	**Gestión Ineficiente**: La ausencia de versionamiento dificulta la gestión de cambios y el soporte para múltiples versiones. **Problemas de Compatibilidad**: Puede generar conflictos al actualizar o integrar nuevas versiones.	**Implementar Versionamiento**: Asegura que tus *APIs* cuenten con un sistema de versionamiento claro para facilitar el mantenimiento y las actualizaciones.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
Proceso de manejo de cambios al alterar y/o actualizar estos APIs.	**90**	**12**	**13%**	**Insuficiente**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **CC 2023-04 *Para la Adopción de Nuevas Políticas PRITS*** **Política TI- PRITS-001 -** 1, 6.4, 7 y 8.2 **Carta General PRITS - 9/sept/2020 Repositorios de Interfaces (*APIs*)** **OE 2013-013 Boletín Administrativo - Primero Guía *PRITS*-004 Guías de Interfaz y Diseño (*GUIDI*)**	**Riesgos en la Implementación**: La falta de un proceso definido para manejar cambios puede llevar a errores en la implementación y problemas operativos. **Dificultades en el Mantenimient**o: Sin un proceso claro, la gestión de cambios se vuelve desorganizada y propensa a fallos.	**Establecer un Proceso de Manejo de Cambios**: Definir y documentar un proceso para manejar alteraciones y actualizaciones de las *APIs* para asegurar una implementación fluida y controlada.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
3. Publicaciones Web ***Revisar la existencia de páginas o servicios web fuera del dominio pr.gov y la accesibilidad de los portales web.*** ***Asegurarse de que los sitios web sean accesibles al ciudadano y cumplan con las evaluaciones de accesibilidad requeridas.***							
La agencia tiene una página o servicio que no resida en el dominio pr.gov.	**90**	**69**	**77%**	**Adecuado**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019** ***Ley PRITS*** **-** Arts. 2, 12 (b), (d) y 13 (k) **Política Núm. ATI-006** (5) **CC 2021-004** ***Dominio Oficial del Gobierno de Puerto Rico (pr.gov)*** **CC 2023-004** ***Para la Adopción de Nuevas Políticas PRITS*** **Política TI -PRITS -** 7.3.3.1 **Carta Generales PRITS - Dominio PR.GOV,** 2-mayo-2020 **Guía PRITS-004 Guías de Interfaz y Diseño (GUIDI)**	**Consistencia y Control**: No tener páginas fuera del dominio pr.gov facilita la gestión y el control centralizado de las publicaciones web. **Cumplimiento de Políticas**: Asegura que todas las páginas cumplan con las políticas y estándares gubernamentales.	**Revisar Páginas Externas**: Si existen páginas fuera del dominio pr.gov, asegurarse de que haya una justificación válida y documentada. **Centralizar Contenidos**: Considera centralizar los servicios y páginas web en el dominio pr.gov para una mejor gestión y cumplimiento.
¿Su agencia cuenta con un Sistema de Gestión de Contenido (CMS)?	**90**	**21**	**23%**	**Insuficiente**	**Ley Núm. 151-2004** ***Ley de Gobierno Electrónico*** **-** Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019** ***Ley PRITS*** **-** Arts. 2, 12 (b), (d) y 13 (k) **CC 2023-006** ***Actualización Sistema Gestión de Contenidos (CMS)*** 23/oct/2023	**Dificultades en la Gestión de Contenidos**: Sin un *CMS*, la gestión y actualización de contenidos web puede ser más complicada y menos eficiente. **Mayor Riesgo de Errores**: La falta de un *CMS* puede llevar a errores y a una menor cohesión en la gestión de contenidos.	**Implementar un CMS**: Si no cuentas con un CMS, considera implementar uno para mejorar la gestión, actualización y organización del contenido web.

ÁREAS EVALUADAS	*Total Entidades*	*Entidades en Cumplimiento*	*RESULTADO*		*CRITERIO*	*ENTIDADES EN INCUMPLIMIENTO*	
			%	*Adecuado Moderado Insuficiente*		*EFECTO*	*ACCIÓN CORRECTIVA*
¿Su agencia cuenta con un portal web accesible al ciudadano?	**90**	**81**	**90%**	**Adecuado**	**Ley Núm. 229-2003** ***Para Garantizar el Acceso a la Información...*** - Art. 4 y 5 **Ley Núm. 151-2004** ***Ley Gobierno Electrónico*** **-** Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019** ***Ley PRITS*** **-** Arts. 2, 12 (b), (d) y 13 (c) (k) **CC 2023-006** ***Actualización de los Sistemas de Gestión de Contenidos (CMS)*** 23-oct-2023 **Política ATI -006 -** Política **OE 2013-013 Boletín Administrativo - Primero** **Guía PRITS-004 Guías de Interfaz y Diseño (*GUIDI*)**	**Exclusión de Usuarios**: La falta de accesibilidad puede excluir a ciertos ciudadanos de acceder a la información y servicios. **Problemas de Cumplimiento**: Puede haber incumplimiento con las normativas de accesibilidad web.	**Asegurar Accesibilidad**: Asegúrate de que el portal web cumpla con los estándares de accesibilidad para todos los ciudadanos

ÁREAS EVALUADAS	*Total Entidades*	*Entidades en Cumplimiento*	*RESULTADO*		*CRITERIO*	*ENTIDADES EN INCUMPLIMIENTO*	
			%	*Adecuado Moderado Insuficiente*		*EFECTO*	*ACCIÓN CORRECTIVA*
Cuenta con la evaluación de accesibilidad de PRITS	**90**	**45**	**50%**	**Insuficiente**	**Ley Núm. 229-*2003 Para Garantizar el Acceso a la Información...* -**Art. 4, 5 y 6 **Ley Núm. 151-2004 *Ley Gobierno Electrónico* -** Art. 5 (i) y (n), 7 (c), (g) y (h) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **Política ATI - 006** **CC 2023-004 - *Para la Adopción de nuevas políticas PRITS*** **CC 2023-006 *Actualización de los Sistemas de Gestión de Contenidos (CMS)*** 23-oct-2023 **Política TI-PRITS-004 -** 7.2.2.3 **OE 2013-013 *Boletín Administrativo* -** *Primero* ***Guía PRITS-004 Guías de Interfaz y Diseño (GUIDI)***	**Falta de Cumplimiento**: No tener una evaluación puede resultar en incumplimiento con los requisitos de accesibilidad. **Problemas de Accesibilidad**: Puede haber problemas de accesibilidad que no se han identificado ni corregido	**Obtener Evaluación**: Asegurarse de obtener y mantener una evaluación de accesibilidad para cumplir con los estándares y mejorar el acceso para todos los usuarios.

ÁREAS EVALUADAS	Total Entidades	Entidades en Cumplimiento	RESULTADO		CRITERIO	ENTIDADES EN INCUMPLIMIENTO	
			%	Adecuado Moderado Insuficiente		EFECTO	ACCIÓN CORRECTIVA
4. Ciberseguridad ***Evaluar la implementación de soluciones de seguridad avanzadas para proteger la infraestructura tecnológica. Asegurar que se utilicen herramientas especializadas para la detección y gestión de eventos de seguridad, garantizando además que la agencia esté integrada a plataformas de protección eficaces y confiables.***	**90**	**69**	**77%**	**Moderado**	**Ley Núm. 151-2004 *Ley de Gobierno Electrónico* -** Art. 5 (i) y (n), 7 (g) y (h) **Ley Núm. 75-2019 *Ley PRITS* -** Arts. 2, 12 (b), (d) y 13 (k) **Ley Núm. 40-2024 *Ley de Ciberseguridad* -** Art. 7 (13)	Sin estas herramientas, la entidad puede ser vulnerable y la protección contra amenazas puede ser insuficiente. Puede comprometer la capacidad para la detección y respuestas a eventos de seguridad.	Considerar la implementación de las herramientas necesarias para mejorar la protección contra amenazas y garantizar una seguridad robusta y un monitoreo efectivo.

En el contexto de este estudio, se recopilaron los **costos estimados** asociados a diversas áreas tecnológicas, según la información suministrada por las entidades. Estos incluyen gastos en licenciamiento de software, almacenamiento en la nube, compra de equipos de redes y adquisición de infraestructura tecnológica, entre otros. Los datos obtenidos ofrecen una perspectiva sobre las inversiones actuales en tecnología realizadas por las entidades gubernamentales, proporcionando así una base sólida para identificar áreas de mejora y optimizar la eficiencia del gasto.

Se distribuyeron los gastos por concepto, según las contestaciones suministradas por las entidades. Los parámetros para cada renglón surgieron al determinar la cantidad mínima y máxima estimada de la inversión.[15].

Concepto de Gasto	Cantidad Mínima Informada	Cantidad Máxima Informada
Contrato Maestro de Licenciamiento- *Software* de Productividad Organizacional (e.g., *Oracle, Microsoft, Adobe, CAD*, etc.)	$400	$7,000,000
Licenciamiento Plataformas de Servicio/ *Case Management (e.g., Service Desk)*	$800	$878,000
Licenciamiento de Resguardo	$950	$150,000
Licenciamiento Plataformas de Virtualización	$455	$1,017,031
Licenciamiento Plataformas de Recursos Humanos	$814	$3,986,640
Licenciamiento *SaaS (Software as a Service)*	$960	$70,898,957
Licenciamiento - Otro	$254	$6,885,445
Pago por líneas de telecomunicaciones dedicadas	$420	$15,615,443
Pago por servicios de telefonía	$105	$3,485,445
Pago por consumo de data	$620	$1,411,002

[15] Algunas entidades no proveyeron información sobre los costos estimados, relacionados a determinados conceptos, ya que informaron que el servicio o bien es a través de *PRITS*.

Concepto de Gasto	Cantidad Mínima Informada	Cantidad Máxima Informada
Almacenamiento en la Nube	$3,000	$5,697,678
Almacenamiento de Nube - Otros	$1,662	$370,696
Arrendamiento- Servicios de Colocación Centro de Datos	$950	$4,641,936
Arrendamiento- Facilidades *IT*	$800	$1,585,592
Compra de Infraestructura on *PREMISE* (*mainframes*, servidores)	$763	$5,000,000
Compra de Equipo de Redes	$499	$1,900,000
Compra de Equipo de Operación (*workstations*, multifuncionales, periferales)	$1,350	$4,252,875
Servicios Profesionales- Administración de Sistema, Mantenimiento y Servicios Manejados	$160	$28,219,029
Servicios Profesionales - Consultoría	$3,500	$12,433,842
Adiestramiento Profesional *IT*	$600	$250,000
Pólizas de Seguros Especializados	$6,500	$2,977,000
Conservación y Reparación de Equipo	$500	$3,746,691
Otros Gastos de Tecnología	$650	$59,363,546

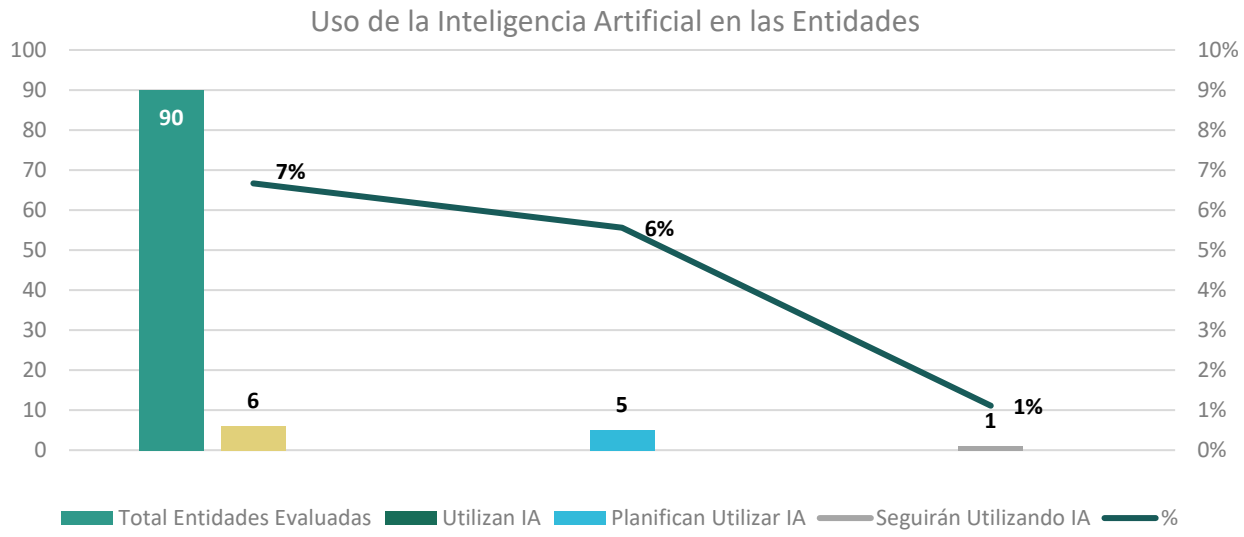
En el estudio, también se recopiló información sobre el **uso de inteligencia artificial (IA)** por las entidades. La IA está siendo cada vez más incorporada a diversas áreas operativas, tales como la automatización de procesos, el análisis predictivo, la gestión de datos y la optimización de decisiones estratégicas. La Inteligencia Artificial (IA) es un campo científico de la informática en el que, mediante la combinación de algoritmos[16], se crean programas y mecanismos que pretenden

[16] Conjunto de instrucciones o pasos definidos que se siguen para resolver un problema o realizar una tarea específica. Estos pasos están diseñados de manera lógica y estructurada para garantizar que se obtenga un resultado claro al final.

simular la inteligencia y los comportamientos propios del ser humano. En síntesis, podemos definir la IA como la potencial habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planificar.

A raíz del desarrollo y la facilidad para acceder a algoritmos de IA, las entidades gubernamentales y sus proveedores de servicio deben procurar maximizar los beneficios de la IA, mientras reducen los posibles riesgos. La IA en un ente gubernamental debe estar en primer orden al servicio de los intereses de los ciudadanos, y no limitarse su utilización al funcionamiento interno del Gobierno. Para cumplir con lo anterior, **resulta indispensable que *PRITS* regule, revise y apruebe cualquier uso actual o que en el futuro soliciten las entidades gubernamentales para el uso de laIA[17].**

Solo un 7% (6 de 90) entidades reportaron[18] el uso de soluciones basadas en IA tanto para mejorar la eficiencia de los servicios como para reducir costos operativos de la siguiente manera:



RECOMENDACIONES

La OIG recomienda que se continúe fortaleciendo la coordinación interagencial ente PRITS y la OIG, a fin de viabilizar la implantación uniforme de la política pública tecnológica y atender de manera integrada las áreas de mejora identificadas en este estudio. La colaboración sostenida entre ambas entidades resulta esencial para el desarrollo de estándares transversales, la alineación de procesos de gobernanza tecnológica, la supervisión del cumplimiento regulatorio,

[17] Véase Carta Circular CC-2023-002-Integración de la Inteligencia Artificial en la Tecnología Gubernamental del 12 de abril de 2023, promulgada por *PRITS*.
[18] Según información provista por las entidades.

la estandarización de criterios técnicos y la planificación estratégica de iniciativas tecnológicas a nivel gubernamental. Del mismo modo, la interacción continua permitirá armonizar esfuerzos de fiscalización, orientar a las entidades en la implementación de controles correctivos y promover capacidades institucionales que eleven la madurez tecnológica, la resiliencia operacional y la seguridad de los sistemas de información del Gobierno de Puerto Rico.

El director ejecutivo de *PRITS* o su designado autorizado, debe continuar los esfuerzos junto a la OIG para:

1. Monitorear que todas las entidades cumplan con la preparación anual de un análisis de riesgos y la ejecución de evaluaciones de vulnerabilidades trimestrales con informes sometidos a PRITS.
2. Establecer un formulario para solicitar la ejecución documentada de simulacros y pruebas de recuperación de respaldos off-site, al menos una vez al año para garantizar la continuidad de servicios.
3. Implementar lineamientos uniformes para la documentación, versionamiento y control de cambios de API's, junto con un plan de interconexión gradual de sistemas críticos.
4. Desarrollar proyectos piloto de uso de Inteligencia Artificial en procesos administrativos, bajo supervisión de PRITS y con informes de resultados y cumplimiento ético.

CONCLUSIÓN

El estudio realizado evidenció resultados diversos en los niveles de cumplimiento observados entre las entidades gubernamentales evaluadas. Los resultados se clasificaron en tres niveles — Insuficiente (0 a 50), Moderado (51 a 75) y Adecuado (76 a 100) — conforme al promedio obtenido por cada área temática principal evaluada.

Los resultados reflejan que las áreas con mayores deficiencias corresponden a la seguridad en las redes, la gestión de vulnerabilidades, los procesos de recuperación ante desastres y la interconexión de sistemas. Estas áreas alcanzaron un nivel insuficiente o moderado de cumplimiento, lo que evidencia la necesidad de establecer controles más rigurosos, actualizar las políticas internas y fortalecer las capacidades operativas de las entidades para mitigar riesgos tecnológicos y garantizar la continuidad de sus operaciones. En este esfuerzo, *PRITS*, como organismo rector en materia de política pública tecnológica, juega un rol fundamental para uniformar los estándares mínimos de cumplimiento y promover mejores prácticas en la gestión tecnológica gubernamental.

Por otro lado, se identificaron áreas donde las entidades gubernamentales mantienen los niveles de cumplimiento adecuados, tales como el cumplimiento normativo general, la gestión de inventarios tecnológicos, la planificación de proyectos y la administración de los recursos

humanos vinculados a la tecnología. No obstante, incluso en estas áreas, se observaron oportunidades de mejora dirigidas a reforzar la documentación de procesos, implementar evaluaciones periódicas de riesgos, fortalecer los mecanismos de respaldo y almacenamiento de información, y modernizar la infraestructura tecnológica, en alineación con las directrices establecidas por *PRITS.*

El análisis detallado de las respuestas recibidas permitió identificar áreas específicas de fortaleza y de oportunidad para cada tema evaluado, lo cual resulta esencial para orientar las acciones correctivas y los esfuerzos de fortalecimiento institucional, según las necesidades particulares de cada entidad gubernamental.

Cabe destacar que la Comisión Estatal de Elecciones no respondió al requerimiento de información emitido por la OIG, razón por la cual sus resultados fueron clasificados como incumplidos.

En este contexto, la Oficina del Inspector General de Puerto Rico reafirma su compromiso con la fiscalización efectiva y el fortalecimiento de los controles institucionales en las entidades gubernamentales. Los hallazgos de este estudio representan una oportunidad estratégica para que las entidades revisen y actualicen sus procesos, desarrollen planes de acción correctiva y adopten las mejores prácticas en materia de gobernanza tecnológica.

En resumen, se concluyó lo siguiente:

1. **Tema Principal: Cumplimiento con la Ley Núm. 75-2019**
    - **Nivel de Cumplimiento Promedio:** Moderado
    - **Fortalezas:**
        - Cumplimiento Normativo-Adecuado
        - Inventario de Equipo y Sistemas-Adecuado
        - Proyectos y Recursos Humanos-Adecuado
        - Gestión de Privilegios de Acceso-Adecuado
        - Control Acceso Físico y Seguridad del Sistema-Adecuado
    - **Áreas de Mejora:**
        - Seguridad en Redes-Moderado
        - Vulnerabilidad y Seguridad del Sistema-Moderado
        - Plan y Centro Recuperación de Desastre-Moderado
        - Interconexión de Sistemas-Insuficiente

2. **Tema Principal: Desarrollo de "*API's*" (*Application Programming Interface*)**
    - **Nivel de Cumplimiento Promedio:** Insuficiente
    - **Áreas de Mejora:**
        - *API* Activo-Insuficiente
        - Documentación Open API-Insuficiente
        - Versionamiento *API*-Insuficiente
        - Manejo de Cambios *API*-Insuficiente
3. **Tema Principal: Publicaciones Web**
    - **Nivel de Cumplimiento Promedio:** Moderado
    - **Fortalezas:**
        - Dominio pr.gov-Adecuado
        - Accesibilidad Portal Web-Adecuado
    - **Áreas de Mejora:**
        - Evaluación Accesibilidad (portal Web)-Moderado
        - Sistema Gestión de Contenido-Insuficiente
        - Tipo de CMS-Insuficiente
4. **Tema Principal: Ciberseguridad**
    - **Nivel de Cumplimiento Promedio:** Moderado

Estos resultados constituyen un insumo valioso para *PRITS*, en su función de establecer y promover la política pública sobre tecnología del Gobierno de Puerto Rico, conforme a la Ley Núm. 75-2019. Su integración con los esfuerzos de fiscalización de la OIG permitirá fortalecer la gobernanza, uniformar los controles, elevar los niveles de cumplimiento y promover la eficiencia, transparencia y seguridad en la prestación de servicios públicos.

APROBACIÓN

Este informe se aprueba en virtud de los poderes conferidos por la Ley Núm. 15-2017, según enmendada. Es responsabilidad de los funcionarios, empleados y cuerpos rectores de cada entidad gubernamental asegurar el cumplimiento riguroso de la política pública establecida. Cada entidad debe implementar los controles y mecanismos necesarios para garantizar este cumplimiento.

Además, corresponde a todos los funcionarios y servidores públicos adoptar y poner en práctica las normas, prácticas y estándares promulgados por la Oficina del Inspector General de Puerto

Rico, así como las recomendaciones, medidas y planes de acción correctiva derivados de las evaluaciones.

Hoy, 25 de noviembre de 2025, en San Juan, Puerto Rico.

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

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

ANEJO

#	Entidades Gubernamentales (Completaron el Cuestionario)	Siglas
1	Administración de Asuntos Federales de Puerto Rico en Washington	PRFAA
2	Administración de Compensaciones por Accidentes de Automóviles	ACAA
3	Administración de Seguros de Salud de Puerto Rico	ASES
4	Administración de Servicios Generales	ASG
5	Administración de Terrenos	AT
6	Autoridad de Acueductos y Alcantarillados	AAA
7	Autoridad de Asesoría Financiera y Agencia Fiscal de Puerto Rico	AAFAF
	Autoridad para el Financiamiento de Facilidades Industriales, Turísticas, Educativas, Médicas y de Control Ambiental	AFICA
	Autoridad para las Alianzas Público-Privadas	APP
	Corporación del Fondo de Interés Apremiante	COFINA
8	Autoridad de Edificios Públicos	AEP
9	Autoridad de Energía Eléctrica	AEE
10	Autoridad del Distrito del Centro de Convenciones de Puerto Rico	ADCCPR
11	Autoridad para el Financiamiento de la Infraestructura de PR	AFI
12	Autoridad para el Financiamiento de la Vivienda	AFV
13	Banco de Desarrollo Económico de Puerto Rico	BDE
14	Centro Comprensivo de Cáncer de la Universidad de PR	CCC
15	Centro de Investigaciones, Educación y Servicios Médicos para la Diabetes	CDPR
16	Comisión Apelativa del Servicio Público	CASP
17	Comisión de Desarrollo Cooperativo de Puerto Rico	CDCOOP
18	Comisión de Desarrollo Cooperativo de Puerto Rico – Corporación Pública para la Supervisión y Seguro de Cooperativas de PR	COSSEC
19	Comisión de Investigación, Procesamiento y Apelación (CIPA)	CIPA
20	Comisión de Juegos del Gobierno de PR	CJ
21	Comisión Estatal de Elecciones	CEE
22	Comisión Industrial de PR	CIPR
23	Corporación de las Artes Musicales	CAM
24	Corporación de Puerto Rico para la Difusión Pública	WIPR
25	Corporación del Centro de Bellas Artes Luis A. Ferré	CBA

#	Entidades Gubernamentales (Completaron el Cuestionario)	Siglas
26	Corporación del Conservatorio de Música de Puerto Rico	CCM
27	Corporación del Fondo del Seguro del Estado	CFSE
28	Defensoría de las Personas con Impedimentos	DPI
29	Departamento de Agricultura	DA
	Administración para el Desarrollo de Empresas Agropecuarias	ADEA
30	Autoridad de Tierras de Puerto Rico	ATPR
31	Autoridad de Tierras – Fondo de Innovación para el Desarrollo Agrícola	FIDA
32	Corporación de Seguros Agrícolas de Puerto Rico	CSA
33	Departamento de Asuntos del Consumidor	DACO
34	Departamento de Corrección y Rehabilitación	DCR
35	Junta de Libertad Bajo Palabra	JLBP
36	Departamento de Desarrollo Económico y Comercio	DDEC
	Programa de la Oficina de Exención Contributiva Industrial (DDEC)	OECI
37	Autoridad para el Redesarrollo de los Terrenos y Facilidades de la Estación Naval Roosevelt Roads (DDEC)	LRA
38	Compañía de Fomento Industrial (DDEC)	PRIDCO
39	Junta de Planificación de Puerto Rico (DDEC)	JP
40	Compañía de Turismo de Puerto Rico (DDEC)	CTPR
41	Programa de la Oficina de Gerencia de Permisos (DDEC)	OGPe
42	Programa de la Oficina Estatal de Política Pública Energética (DDEC)	OEPPE
43	Departamento de Educación	DE
44	Departamento de Estado	DEPR
45	Departamento de Hacienda	DH
46	Departamento de Justicia	DJ
47	Departamento de la Familia	DF
	Administración de Desarrollo Socioeconómico de la Familia	ADSEF
	Administración de Familias y Niños	ADFAN
	Administración para el Cuidado y Desarrollo Integral de la Niñez	ACUDEN
48	Administración para el Sustento de Menores (ASUME)	ASUME
49	Departamento de la Vivienda	DV
50	Departamento de la Vivienda – Administración de Vivienda Pública	AVP

#	Entidades Gubernamentales (Completaron el Cuestionario)	Siglas
51	Departamento de Recreación y Deportes	DRD
52	Departamento de Recursos Naturales y Ambientales	DRNA
	Autoridad de Desperdicios Sólidos de Puerto Rico	ADS
	Junta de Calidad Ambiental	JCA
	Programa de Parques Nacionales	PPN
53	Departamento de Salud	DS
54	Administración de Servicios de Salud Mental y Contra la Adicción	ASSMCA
55	Administración de Servicios Médicos de Puerto Rico	ASEM
56	Corporación del Centro Cardiovascular de Puerto Rico y del Caribe	CCCPRC
57	Departamento de Seguridad Pública	DSP
58	Negociado de Investigaciones Especiales	NIE
59	Negociado de la Policía de Puerto Rico	NPPR
60	Negociado de Sistemas de Emergencia 9-1-1	NSE911
61	Negociado del Cuerpo de Bomberos de Puerto Rico	NCBPR
62	Negociado del Cuerpo de Emergencias Médicas de PR	NCEM
63	Negociado para el Manejo de Emergencias y Adm. de Desastres	NMEAD
64	Departamento de Transportación y Obras Públicas	DTOP
65	Autoridad de los Puertos de Puerto Rico	APPR
66	Autoridad de Carreteras y Transportación	ACT
67	Autoridad de Transporte Integrado	ATI
	Autoridad de Transporte Marítimo de Puerto Rico y las Islas Municipio	ATM
68	Autoridad Metropolitana de Autobuses	AMA
69	Comisión para la Seguridad en el Tránsito	CST
70	Departamento del Trabajo y Recursos Humanos	DTRH
71	Administración de Rehabilitación Vocacional	ARV
72	Escuela de Artes Plásticas y Diseño de PR - Corporación Escuela Artes Plásticas y Diseño de PR	EAPD
73	Fideicomiso Institucional de la Guardia Nacional de PR	FIGNA
74	Guardia Nacional de Puerto Rico	GNPR
75	Instituto de Ciencias Forenses de Puerto Rico	ICF
76	Instituto de Cultura Puertorriqueña de PR	ICP

#	Entidades Gubernamentales (Completaron el Cuestionario)	Siglas
77	Instituto de Estadísticas de Puerto Rico	IEPR
78	Junta de Relaciones del Trabajo	JRT
79	Junta de Retiro del Gobierno de Puerto Rico (Antes Administración del Sistema de Retiro / Sistema Retiro Maestros)	JR
80	Junta Reglamentadora del Servicio Público de PR	JRSP
	Negociado de Energía de PR	NEPR
	Negociado de Telecomunicaciones de Puerto Rico	NTPR
	Oficina Independiente de Protección al Consumidor	OIPC
	Negociado de Transporte y Otros Servicios Públicos	NTSP
81	Oficina de Administración y Transformación de los Recursos Humanos del Gobierno de Puerto Rico	OATRH
82	Oficina de la Procuradora de las Mujeres	OPM
83	Oficina para el Desarrollo Socioeconómico y Comunitario (Comunidades Especiales)	ODSEC
84	Oficina del Comisionado de Instituciones Financieras	OCIF
85	Oficina del Comisionado de Seguros de PR	OCS
86	Oficina del Contralor Electoral	OCE
87	Oficina del Procurador de las Personas de Edad Avanzada	OPPEA
88	Oficina del Procurador del Paciente	OPP
89	Oficina del Procurador del Veterano de Puerto Rico	OPV
90	Oficina Estatal de Conservación Histórica	OECH

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