PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

9 de noviembre de 2026

VIA CORREO ELECTRÓNICO

Hon. Thomas Rivera Schatz
Presidente
Senado de Puerto Rico

Hon. Carlos "Johnny" Méndez Núñez
Presidente
Cámara de Representantes de Puerto Rico

Estimados señores Presidentes:

En cumplimiento con lo establecido en la Ley Núm. 40-2024, conocida como la "Ley de Ciberseguridad del Gobierno de Puerto Rico", la Oficina para la Evaluación de Incidentes Cibernéticos ("OEIC") presenta su Informe Trimestral, correspondiente al período del 1 de julio de 2026 al 30 de septiembre de 2026.[1]

Este informe ofrece una divulgación de las ejecutorias de la OEIC, con relación a los resultados de las gestiones e investigaciones realizadas durante el periodo correspondiente.

Nos mantenemos a su disposición para ampliar cualquier información o discutir iniciativas adicionales que contribuyan a fortalecer la resiliencia digital del Gobierno de Puerto Rico.

Atentamente,

Poincaré Díaz Peña
Principal Oficial de Innovación e Información
Puerto Rico Innovation and Technology Service

[1] De conformidad con el último ¶ del Art. 8 de la Ley 40-2024, 3 L.P.R.A. § 10128.

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

PRITS-CSREP-009

Informe Trimestral

Oficina para la Evaluación de Incidentes Cibernéticos

- Para el periodo comprendido entre el 1 de julio de 2026 al 30 de septiembre de 2026

Tabla de Contenido

1. Introducción 2
2. Detecciones 2
3. Incidentes e investigaciones 4
4. Gobernanza y cumplimiento 4
5. Comunicaciones y alertas 5
7. Conclusión 8
8. Aprobación y Firma 9
Apéndice I: Resumen del informe 10

1. Introducción

En cumplimiento con las disposiciones de la Ley Núm. 40-2024, conocida como la "Ley de Ciberseguridad del Gobierno de Puerto Rico", la Oficina para la Evaluación de Incidentes Cibernéticos ("OEIC") presenta su informe trimestral a ser remitido a la Asamblea Legislativa de Puerto Rico y publicado en las páginas cibernéticas del Puerto Rico Innovation and Technology Service ("PRITS") y del Instituto de Estadísticas de Puerto Rico.

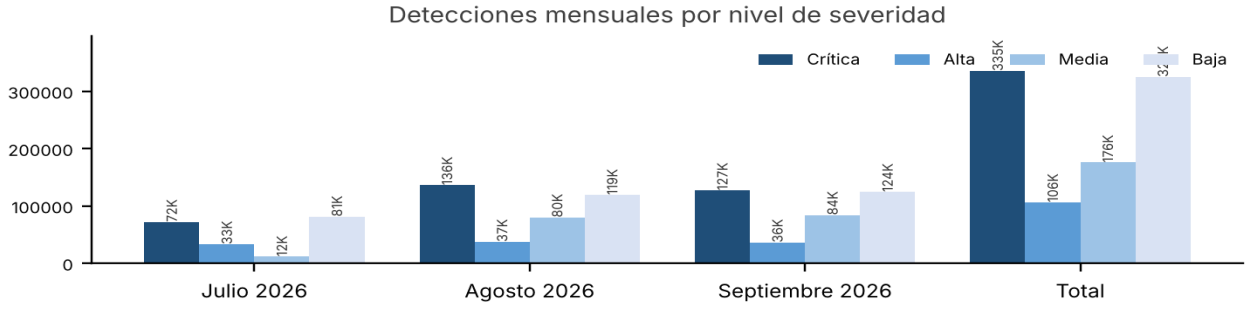
Este informe ofrece comprende los resultados de las gestiones e investigaciones publicables que pudieran haberse llevado a cabo por la OEIC durante el periodo comprendido entre el 1 de julio de 2026 al 30 de septiembre de 2026, inclusive.[2]

2. Detecciones

Como parte del esfuerzo continuo para proteger la infraestructura tecnológica del Gobierno de Puerto Rico, la OEIC mantuvo operaciones de monitoreo constante durante el trimestre julio a septiembre de 2026. Nuestros sistemas de vigilancia y análisis en tiempo real permitieron identificar un total de 942,423 detecciones, clasificadas según su nivel de severidad, lo que evidencia la importancia de contar con capacidades robustas de ciberdefensa en todo momento.

Julio registró el menor volumen del trimestre (197,978 detecciones); agosto casi duplicó esa cifra (372,655, un aumento de 88%), con un incremento en las detecciones críticas (136,235), y septiembre se mantuvo en un nivel similar (371,790). Este comportamiento refleja el monitoreo continuo y la capacidad de detección de las plataformas de seguridad del Gobierno, que permitieron identificar y atender oportunamente la actividad registrada.

Esta vigilancia es clave para la protección de los activos digitales, garantizando una respuesta rápida y efectiva ante posibles ataques.



[2] De conformidad con el último del Art. 8 de la Ley 40-2024, 3 L.P.R.A. § 10128, sobre las obligaciones correspondientes a la OEIC dispuestas en los incisos 1 al 15 del Art. 8, *id*.

Ilustración 1 Gráfica de la distribución de detecciones por nivel de severidad a lo largo del primer trimestre del año fiscal 2026-2027.

Mes	Crítica	Alta	Media	Baja	Total
Julio 2026	71,919	32,979	11,695	81,385	197,978
Agosto 2026	136,235	37,270	79,920	119,230	372,655
Septiembre 2026	127,187	36,129	84,063	124,411	371,790
Total	**335,341**	**106,378**	**175,678**	**325,026**	**942,423**

Tabla 1 Descripción de severidad de las amenazas detectadas.

SEVERIDAD	DESCRIPCIÓN
Crítica	Representan un riesgo inminente y grave para la ciberseguridad de una agencia. Estas amenazas son altamente sofisticadas y pueden causar daños significativos, lo que puede causar sistemas comprometidos, brechas de datos o interrupciones de servicios. Se requiere una acción inmediata y decisiva para mitigar estas amenazas. Estas detecciones son serias y deben ser abordadas de inmediato.
Alta	Representan un riesgo sustancial para la ciberseguridad. Aunque no son tan urgentes como las amenazas críticas, las detecciones con alta severidad exigen acción inmediata. Pueden explotar vulnerabilidades o debilidades en el sistema, lo que puede resultar en graves consecuencias si no se abordan rápidamente.
Media	Indican riesgos potenciales que son de moderada preocupación. Aunque pueden no representan un peligro inmediato, estas detecciones no deben pasarse por alto. Es importante abordarlas para evitar que se escalen a problemas más críticos.
Baja	Se consideran riesgos menores que pueden tener un impacto limitado en la ciberseguridad. Aunque pueden no representar un peligro inmediato, es esencial monitorear y abordar las amenazas de baja gravedad para mantener una postura de seguridad integral y evitar que evolucionen hacia problemas más significativos.

Al considerar el volumen de detecciones en conjunto con los incidentes atendidos durante el trimestre, se observa que agosto 2026 registró el mayor número de detecciones (372,655), mientras que Julio 2026 cerró con el nivel más bajo (197,978) a nivel de trimestre, se registró un total de 942,423 detecciones, una disminución (5%) en comparación con el trimestre anterior (995,462). En este contexto, el incidente atendido fue gestionado conforme al Plan de Respuesta a Incidentes Cibernéticos del Gobierno de Puerto Rico. La OEIC continuará monitoreando de cerca esta tendencia en los

próximos trimestres para fortalecer continuamente las estrategias de prevención y respuesta.

Vulnerabilidades Destacadas durante el trimestre julio a septiembre

Most prevalent vulnerability IDs

Vulnerabilidad	Cantidad	Notas
CVE-2026-62897	Medium — 46.2K	89 días desde primera detección
CVE-2026-70354	Medium — 46.2K	89 días desde primera detección
CVE-2026-47304	Medium — 45.5K	116 días desde primera detección
CVE-2026-50525	Low — 45.5K	117 días desde primera detección
CVE-2026-50646	Medium — 45.5K	117 días desde primera detección

3. Incidentes e investigaciones

La OEIC, a través del CSIRT-PRITS, atendió un incidente de ciberseguridad el 23 de septiembre, activando el Plan de Respuesta a Incidentes Cibernéticos del Gobierno de Puerto Rico. Fue gestionado conforme a los protocolos establecidos; los detalles específicos no se divulgan en este informe público, conforme a la naturaleza sensible de la información.

4. Gobernanza y cumplimiento

4.1 PRITS-POL-0016 Política de Gestión de Terceros (Third-Party Management internal Policy)

Con la aprobación y publicación de PRITS-POL-0016 Política de Gestión de Terceros (Third-Party Management Policy) el 11 de septiembre de 2026, el Gobierno de Puerto Rico fortaleció su marco normativo de ciberseguridad. Fortalece la gestión de los riesgos de ciberseguridad asociados a terceros.

Adicionalmente, durante el trimestre también se generaron las siguientes políticas: PRITS-SOP-0014-OPE Procedimiento de Notificación y Reporte de Incidentes de Ciberseguridad para Sistemas de Certificados mDL, PRITS-SOP-0025-OPE Procedimiento de Gestión de Terceros.

4.2 Evaluación de vulnerabilidades web

Como parte de los esfuerzos continuos para fortalecer la postura de ciberseguridad del Gobierno de Puerto Rico, se llevaron a cabo evaluaciones de seguridad, incluyendo pruebas de penetración y análisis de vulnerabilidades en páginas web, aplicaciones y componentes críticos de infraestructura, como sistemas de claves, a través de distintos dominios gubernamentales. Estas evaluaciones permitieron identificar debilidades técnicas que facilitaron la toma de acciones preventivas e iniciaron procesos de mitigación dirigidos a proteger los datos de los ciudadanos.

Adicionalmente, se continúa con el análisis activo de las vulnerabilidades previamente detectadas mediante el uso de una plataforma centralizada de gestión de vulnerabilidades. Varias agencias ya han comenzado a implementar medidas correctivas como resultado de estos hallazgos, fortaleciendo sus plataformas tecnológicas y reduciendo los riesgos asociados. La OEIC mantiene el monitoreo de estos esfuerzos y provee el acompañamiento técnico necesario para asegurar la resiliencia de la infraestructura digital del Gobierno.

Se destaca también la realización de evaluaciones de seguridad, incluyendo evaluaciones de vulnerabilidades web y evaluaciones de preparación ante ransomware (Ransomware Readiness Assessment, RRA), en agencias del Gobierno de Puerto Rico.

Adicionalmente, durante el trimestre la OEIC adelantó 15 documentos de gobernanza en distintas etapas de elaboración, revisión y aprobación, entre ellos la Política de Ciberseguridad y los Estándares de Ciberseguridad, además de las políticas de Clasificación de Datos, Respuesta a Incidentes y Gestión de Vulnerabilidades y Parches, y la actualización de la Política de Inteligencia Artificial publicada en septiembre de 2025, y ofreció adiestramientos de cumplimiento a su personal sobre las políticas vigentes.

5. Comunicaciones y alertas

Durante este trimestre se emitieron 5 alertas (ilustración 2) a los Oficiales Principales de Informática de las agencias (“OPIs”). Estas alertas incluyeron detalles sobre las cuentas reportadas, así como las recomendaciones para mitigar el riesgo.

El *phishing* es una técnica de ingeniería social mediante la cual los ciberdelincuentes se hacen pasar por personas u organizaciones de confianza para inducir a sus víctimas a divulgar información confidencial, abrir enlaces o archivos maliciosos, o autorizar transacciones fraudulentas. Estas campañas pueden llegar por correo electrónico, mensajes de texto (*smishing*), llamadas o mensajes de voz (*vishing*) y plataformas de mensajería. También pueden utilizar códigos QR que dirigen a páginas falsas para capturar credenciales.

La inteligencia artificial generativa facilita la automatización de la redacción, traducción y personalización de mensajes a gran escala. Los atacantes pueden adaptar sus comunicaciones al cargo de la persona, a sus funciones o a trámites que realiza habitualmente. También pueden clonar voces o generar imágenes y videos para suplantar a funcionarios, compañeros de trabajo o proveedores. Estas capacidades permiten producir campañas más convincentes y reducen la utilidad de señales tradicionales, como los errores de redacción, para identificar un fraude.
La detección y el reporte oportunos ayudan a limitar el impacto de estas campañas sobre los datos, los sistemas y la continuidad de los servicios gubernamentales. Se recomienda a las agencias adoptar las siguientes medidas.

- Fortalecer la cultura de ciberseguridad mediante adiestramientos y ejercicios periódicos que incluyan correos dirigidos, mensajes de texto, códigos QR y llamadas con voces generadas por IA.
- Mantener actualizados los sistemas y las herramientas de seguridad, reforzar los filtros de correo electrónico y priorizar la autenticación multifactor resistente al *phishing* en cuentas privilegiadas y sistemas críticos.
- Verificar por un canal independiente las solicitudes de información sensible, cambios de cuentas bancarias, pagos o restablecimiento de accesos. Utilizar un número de teléfono o contacto institucional previamente validado.
- Reportar de inmediato a la OEIC los intentos de *phishing* y las comunicaciones sospechosas, aunque la persona no haya interactuado con el mensaje. Si abrió un archivo, ingresó credenciales o autorizó una transacción, debe indicarlo en el reporte para facilitar la respuesta.

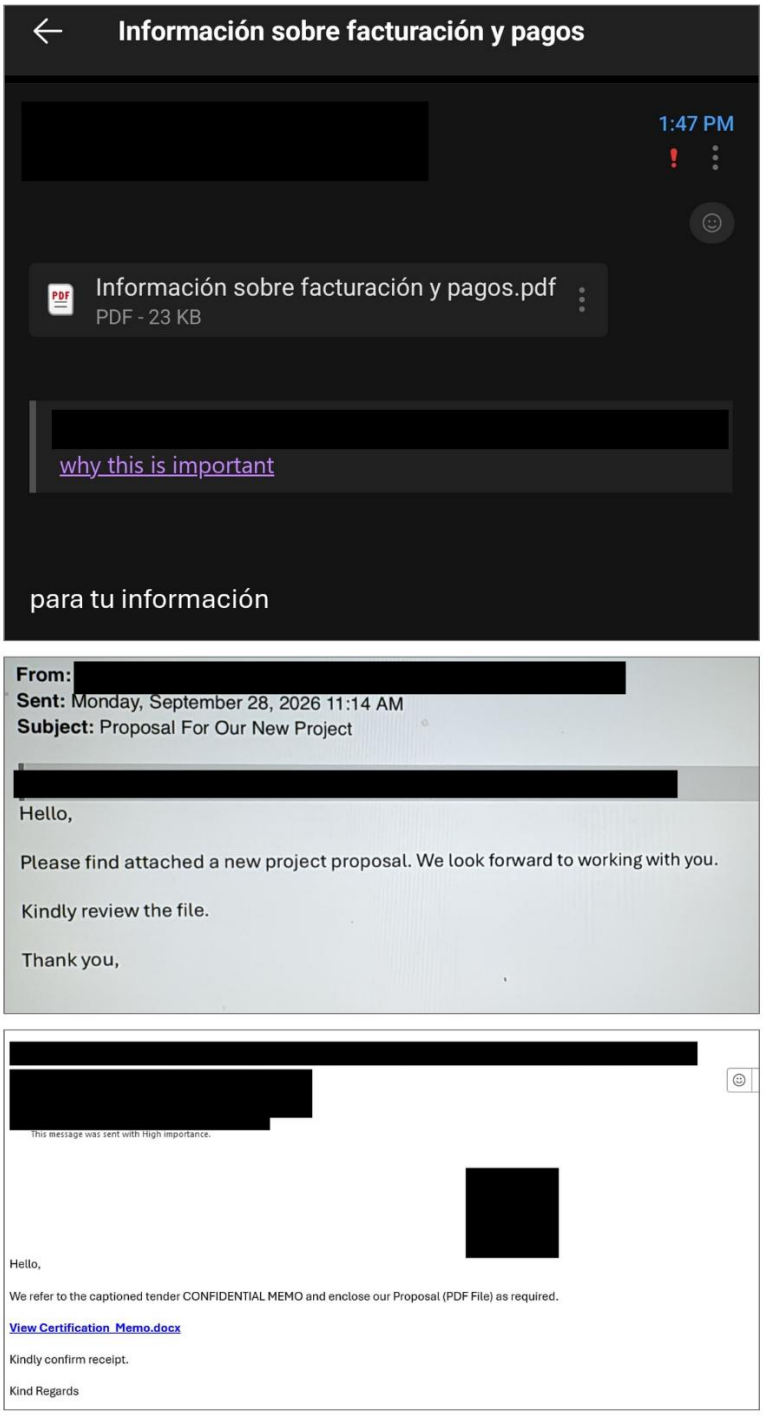


Ilustración 2 Ejemplos de correos de phishing reportados durante el trimestre (información identificable ocultada).

6. Educación, concienciación y adiestramientos

6.1 Concienciación sobre ciberseguridad

Como parte de los esfuerzos continuos para fortalecer la cultura de ciberseguridad en el Gobierno de Puerto Rico, durante los meses de Julio, Agosto y Septiembre de 2026 se llevaron a cabo 10 actividades educativas dirigidas a personal de PRITS y estudiantes, incluyendo 9 adiestramientos de cumplimiento sobre políticas de PRITS, Charla Concienciación en Ciberseguridad.

En total, 197 participantes fueron impactados a través de estas iniciativas educativas durante el trimestre, reflejando el compromiso del Gobierno de Puerto Rico con la capacitación continua y la concienciación en ciberseguridad.

7. Conclusión

El fortalecimiento de la ciberseguridad en el Gobierno de Puerto Rico es un proceso continuo que requiere vigilancia constante, capacitación técnica y colaboración efectiva entre todas las entidades públicas. Durante este trimestre, la OEIC ha mantenido su enfoque proactivo en la identificación y mitigación de amenazas, así como en la respuesta a incidentes críticos que podrían haber comprometido la operación de agencias gubernamentales.

Se destaca la activación efectiva de los protocolos de respuesta ante incidentes cibernéticos durante este trimestre, en el marco del incidente atendido, lo que permitió una respuesta coordinada y conforme a los protocolos establecidos. Esto representa una reducción frente a los 5 incidentes del trimestre anterior, reforzando la efectividad de las estrategias de prevención implementadas. Estas acciones han demostrado la capacidad del equipo del CSIRT-PRITS para responder con agilidad ante los hallazgos identificados.

De igual forma, la publicación de PRITS-POL-0016 Política de Gestión de Terceros (Third-Party Management Policy), PRITS-SOP-0014-OPE Procedimiento de Notificación y Reporte de Incidentes de Ciberseguridad para Sistemas de Certificados mDL, PRITS-SOP-0025-OPE Procedimiento de Gestión de Terceros; la realización de evaluaciones de seguridad, incluyendo evaluaciones de vulnerabilidades web y evaluaciones de preparación ante ransomware (Ransomware Readiness Assessment, RRA), en agencias del Gobierno de Puerto Rico; el apoyo continuo brindado a las agencias en la

implementación de herramientas de seguridad, estrategias de protección de ambientes tecnológicos, y atención de solicitudes a través de la plataforma de Service Desk, representan avances importantes en materia de gobernanza, cumplimiento normativo y madurez tecnológica. Estas iniciativas son consistentes con los marcos de referencia internacionales y las obligaciones legales establecidas en la Ley Núm. 40-2024.

Las 10 actividades de educación, concienciación y adiestramiento ofrecidas durante el trimestre, que impactaron a 197 participantes, han sido fundamentales para fortalecer la resiliencia institucional, equipando a servidores públicos con herramientas prácticas para identificar, reportar y actuar ante amenazas cibernéticas. Esto representa un aumento frente a las 4 actividades del trimestre anterior.

De cara a los próximos trimestres, la OEIC continuará desarrollando y ejecutando estrategias robustas de prevención, detección y respuesta, al tiempo que promoverá una cultura de ciberseguridad sólida y sostenible en toda la administración pública. Nuestro compromiso permanece firme: proteger la infraestructura digital del Gobierno y salvaguardar la información de todos los ciudadanos del Gobierno de Puerto Rico.

8. Aprobación y Firma

Aprobado y autorizado para publicación hoy 9 de noviembre de 2026, en San Juan, Puerto Rico.

Poincaré Díaz Peña
Principal Oficial de Innovación e Información
Puerto Rico Innovation and Technology Service

Apéndice I: Resumen del informe

