PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

PRITS-CSREP-004

Informe Trimestral

Oficina para la Evaluación de Incidentes Cibernéticos

- Para el periodo comprendido entre el 1 de abril de 2025 al 30 de junio de 2025

Tabla de Contenido

1. Introducción

En cumplimiento con las disposiciones de la Ley Núm. 40-2024, conocida como la "Ley de Ciberseguridad del Estado Libre Asociado 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 abril de 2025 al 30 de junio de 2025, 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 abril a junio de 2025. Nuestros sistemas de vigilancia y análisis en tiempo real permitieron identificar un total de 716,705 detecciones, clasificadas según su nivel de severidad, lo que evidencia la importancia de contar con capacidades robustas de ciberdefensa en todo momento.

Abril registró el volumen más alto del trimestre, impulsado por detecciones críticas; mayo y junio reflejaron una disminución sostenida.

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

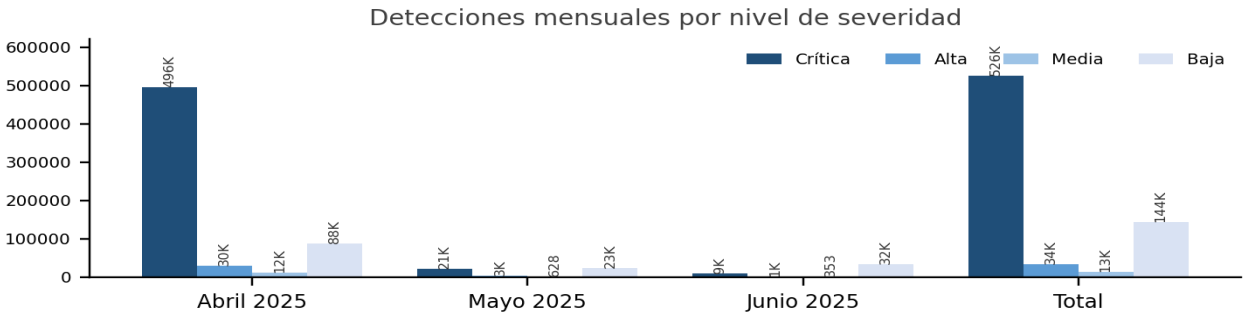


Ilustración 1 Gráfica de la distribución de detecciones por nivel de severidad a lo largo del cuarto trimestre del año fiscal 2024-2025.

[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*.

Mes	Crítica	Alta	Media	Baja	Total
Abril 2025	496,340	29,846	11,738	88,039	625,963
Mayo 2025	21,192	2,955	628	23,338	48,113
Junio 2025	8,588	1,337	353	32,351	42,629
Total	**526,120**	**34,138**	**12,719**	**143,728**	**716,705**

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.

Vulnerabilidades Destacadas durante el trimestre abril a junio

Cumplimiento de remediación por severidad

Severidad (ExPRT)	Plazo SLA	Cumplimiento
Crítica (ExPRT)	SLA: 7 días	97% en cumplimiento / 3% fuera de cumpli
Alta (ExPRT)	SLA: 14 días	50% en cumplimiento / 50% fuera de cumpl
Media (ExPRT)	SLA: 30 días	56% en cumplimiento / 44% fuera de cumpl
Baja (ExPRT)	SLA: 90 días	54% en cumplimiento / 46% fuera de cumpl

Al considerar el volumen de detecciones en conjunto con los incidentes atendidos durante el trimestre, se observa que abril 2025 registró el mayor número de detecciones (625,963), mientras que junio 2025 cerró con el nivel más bajo (42,629). Esta disminución es consistente con la implementación de las medidas correctivas adoptadas a raíz del incidente atendido capas adicionales de seguridad, monitoreo adicional de la base de datos, reingeniería para transmisión de datos más segura, lo que sugiere que las estrategias de mitigación en curso están rindiendo resultados positivos. No obstante, la OEIC continuará monitoreando de cerca esta tendencia en los próximos trimestres para confirmar su sostenibilidad.

3. Incidentes e investigaciones

El 30 de mayo de 2025, el Departamento de Justicia de Puerto Rico detectó un acceso no autorizado en el Sistema de Información de Justicia Criminal (SIJC-PR). Tan pronto se identificó la situación, se activaron los protocolos de seguridad establecidos y se inició un proceso coordinado de contención e investigación en conjunto con el Puerto Rico Innovation and Technology Service (PRITS) y su Oficina de Evaluación de Incidentes Cibernéticos (OEIC). Como medida preventiva, se suspendieron temporalmente algunos servicios del SIJC-PR, incluyendo la emisión de certificados de antecedentes penales, con el fin de proteger la integridad de la información y salvaguardar los datos personales de la ciudadanía. El Gobierno confirmó que la información de los ciudadanos no se vio comprometida. El sistema fue restablecido el 5 de junio de 2025, tras trabajo conjunto y continuo entre el Departamento de Justicia y PRITS. Durante las fases de recuperación y prueba, PRITS incorporó capas adicionales de seguridad, implementó medidas de monitoreo adicional sobre la base de datos, e inició un proceso de reingeniería orientado a fortalecer la transmisión segura de datos. La investigación del incidente, en

coordinación con las autoridades estatales y federales pertinentes, continuó incluso después del restablecimiento del sistema.

4. Gobernanza y cumplimiento

4.1 Política de Privacidad

Con la aprobación y publicación de la Política de Privacidad (PRITS-POL-0009) en marzo de 2025, el Gobierno de Puerto Rico estableció un marco claro y estandarizado para el manejo responsable de la información, teniendo como uno de sus objetivos principales la protección de los datos personales. La referida política define los principios y prácticas que rigen la recopilación, procesamiento, almacenamiento y divulgación de datos personales, asegurando su tratamiento justo, legal y transparente.

Asimismo, la política promueve la interoperabilidad y la responsabilidad interagencial al establecer lineamientos consistentes con marcos internacionales como ISO/IEC 27001 y 27701, así como el *National Institute of Standards and Technology* (*NIST*) *Privacy Framework*. Esto permite que todas las entidades alineen sus procesos con estándares reconocidos, fortaleciendo la protección de la privacidad en el ecosistema digital gubernamental.

Además, su implementación fomenta una cultura institucional orientada a la minimización de datos, la seguridad en el procesamiento, el respeto a los derechos de los titulares de datos y la preparación ante incidentes. Esto incluye controles como autenticación multifactorial, cifrado, acceso basado en roles y capacitación continua en privacidad y seguridad de la información.

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.

Durante este trimestre se realizaron 3 evaluaciones de seguridad adicionales, incluyendo pruebas de penetración y análisis de vulnerabilidades en agencias del Gobierno de Puerto Rico. Los hallazgos específicos de estas evaluaciones no se divulgan en este informe público, conforme a la naturaleza sensible de la información; las agencias correspondientes reciben el detalle técnico completo de forma directa para fines de remediación.

5. Comunicaciones y alertas

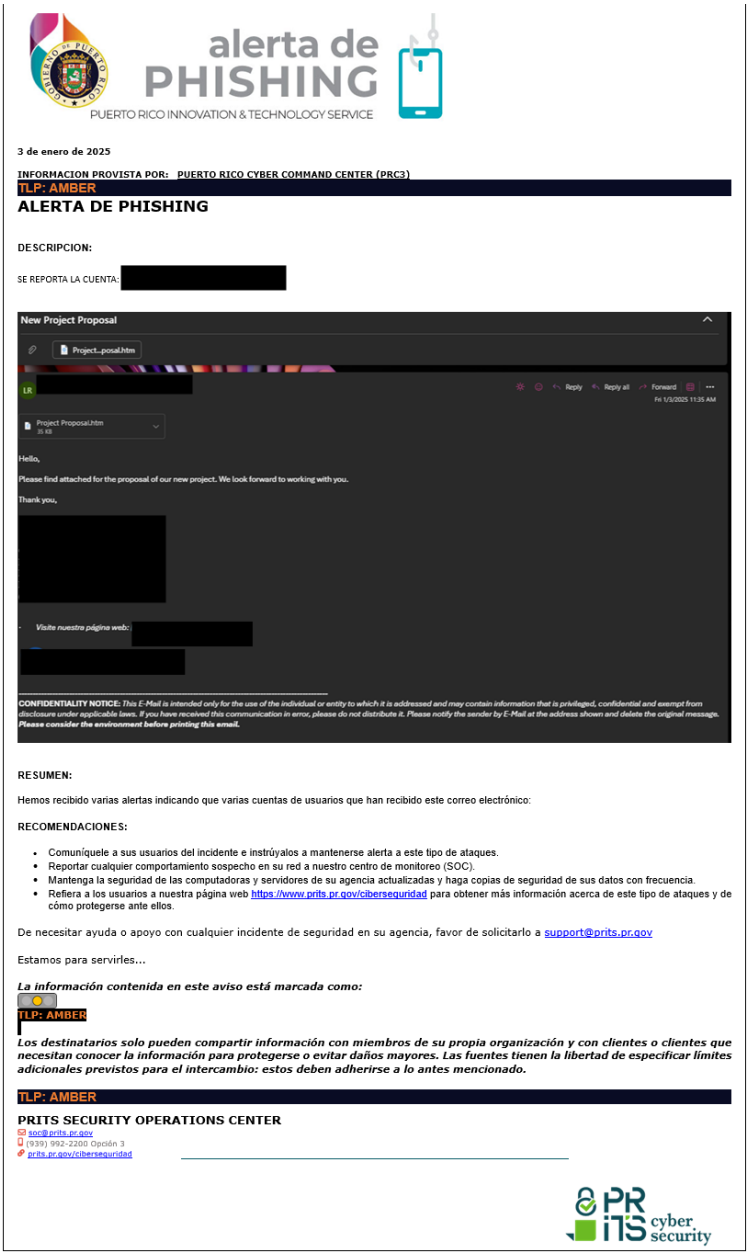
Durante este trimestre se emitió 1 alerta de ciberseguridad general no relacionada a phishing (ilustración 2) a los Oficiales Principales de Informática de las agencias (“OPIs”). Estas alertas incluyeron detalles sobre las cuentas reportadas, así como las recomendaciones para mitigar el riesgo.

El *phishing* es una técnica de ingeniería social utilizada por ciberdelincuentes para engañar a los usuarios y obtener información confidencial, como contraseñas, datos de tarjetas de crédito o información personal. Los atacantes suelen enviar correos electrónicos fraudulentos que parecen provenir de fuentes confiables, como bancos, empresas o instituciones gubernamentales, con el objetivo de inducir a los usuarios a hacer clic en enlaces maliciosos o descargar archivos infectados.

La detección oportuna de estas amenazas es crucial para proteger los activos de las agencias. Se recomienda a todas las agencias reforzar sus medidas de seguridad y mantenerse alerta ante nuevas variantes de *phishing*, incluyendo tomar las siguientes medidas:

- Continuar forjando una cultura de ciberseguridad mediante talleres y adiestramientos para identificar y evitar estas amenazas.
- Mantener actualizados los sistemas y software de seguridad.

- Verificar la autenticidad de cualquier solicitud de información antes de responder.
- Reportar cualquier comportamiento sospechoso a la OEIC.



alerta de PHISHING

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

3 de enero de 2025

INFORMACION PROVISTA POR: PUERTO RICO CYBER COMMAND CENTER (PRC3)

TLP: AMBER

ALERTA DE PHISHING

DESCRIPCION:

SE REPORTA LA CUENTA: [redacted]

New Project Proposal

Project...posal.htm

Reply Reply all Forward

Fri 1/3/2025 11:35 AM

Project Proposal.htm

25 KB

Hello,

Please find attached for the proposal of our new project. We look forward to working with you.

Thank you,

[redacted]

Visite nuestra página web: [redacted]

CONFIDENTIALITY NOTICE: *This E-Mail is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable laws. If you have received this communication in error, please do not distribute it. Please notify the sender by E-Mail at the address shown and delete the original message.* ***Please consider the environment before printing this email.***

RESUMEN:

Hemos recibido varias alertas indicando que varias cuentas de usuarios que han recibido este correo electrónico:

RECOMENDACIONES:

- Comuníquele a sus usuarios del incidente e instrúyalos a mantenerse alerta a este tipo de ataques.
- Reportar cualquier comportamiento sospecho en su red a nuestro centro de monitoreo (SOC).
- Mantenga la seguridad de las computadoras y servidores de su agencia actualizadas y haga copias de seguridad de sus datos con frecuencia.
- Refiera a los usuarios a nuestra página web https://www.prits.pr.gov/ciberseguridad para obtener más información acerca de este tipo de ataques y de cómo protegerse ante ellos.

De necesitar ayuda o apoyo con cualquier incidente de seguridad en su agencia, favor de solicitarlo a support@prits.pr.gov

Estamos para servirles...

La información contenida en este aviso está marcada como:

TLP: AMBER

Los destinatarios solo pueden compartir información con miembros de su propia organización y con clientes o clientes que necesitan conocer la información para protegerse o evitar daños mayores. Las fuentes tienen la libertad de especificar límites adicionales previstos para el intercambio: estos deben adherirse a lo antes mencionado.

TLP: AMBER

PRITS SECURITY OPERATIONS CENTER

soc@prits.pr.gov

(939) 992-2200 Opción 3

prits.pr.gov/ciberseguridad

PR ITS cyber security

Ilustración 2 Ejemplo (fragmento) de una alerta de phishing enviada a los OPIs.

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 Abril, Mayo y Junio de 2025 se llevaron a cabo 5 actividades educativas dirigidas a OPIs, personal técnico, municipios, empleados públicos y estudiantes, incluyendo temas como Tenable, Charla Cyber Awareness, How to Survive a Ransomware Attack, Digital Forensic Form Incident Managemen.

En total, 127 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 la contención y recuperación oportuna, minimizando el impacto y preservando la integridad operativa de las entidades afectadas. Estas acciones han demostrado la capacidad del equipo del CSIRT-PRITS para responder con agilidad ante los hallazgos identificados.

De igual forma, 3 evaluaciones de seguridad realizadas en agencias del Gobierno de Puerto Rico, 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.

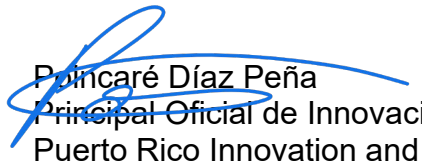
Las 5 actividades de educación, concienciación y adiestramiento ofrecidas durante el trimestre, que impactaron a 127 participantes, han sido fundamentales para fortalecer la

resiliencia institucional, equipando a servidores públicos con herramientas prácticas para identificar, reportar y actuar ante amenazas cibernéticas.

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 Estado Libre Asociado de Puerto Rico.

8. Aprobación y Firma

Aprobado y autorizado para publicación hoy 17 de julio 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