PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

PRITS-CSREP-008

Informe Trimestral

Oficina para la Evaluación de Incidentes Cibernéticos

- Para el periodo comprendido entre el 1 de abril de 2026 al 30 de junio 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 6
8. Aprobación y Firma 7
Apéndice I: Resumen del informe 8

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 2026 al 30 de junio 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 abril a junio de 2026. Nuestros sistemas de vigilancia y análisis en tiempo real permitieron identificar un total de 995,462 detecciones, clasificadas según su nivel de severidad, lo que evidencia la importancia de contar con capacidades robustas de ciberdefensa en todo momento.

Abril registró un volumen alto de detecciones críticas; mayo mostró una disminución marcada; junio tuvo un repunte significativo, superando el nivel de abril e impulsado principalmente por detecciones críticas y altas.

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

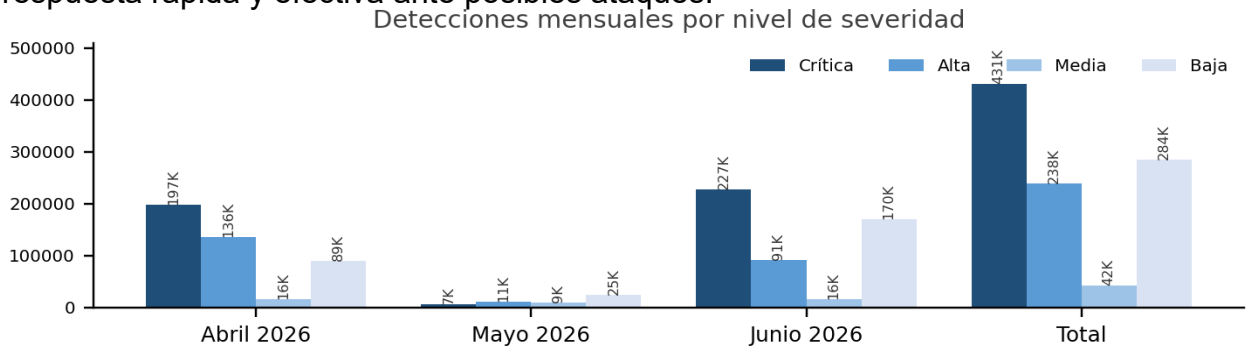


Ilustración 1 Gráfica de la distribución de detecciones por nivel de severidad a lo largo del cuarto trimestre del año fiscal 2025-2026.

Mes	Crítica	Alta	Media	Baja	Total
Abril 2026	197,403	135,751	16,340	89,270	438,764
Mayo 2026	6,597	11,332	9,104	24,630	51,663
Junio 2026	227,291	90,996	16,254	170,494	505,035
Total	**431,291**	**238,079**	**41,698**	**284,394**	**995,462**

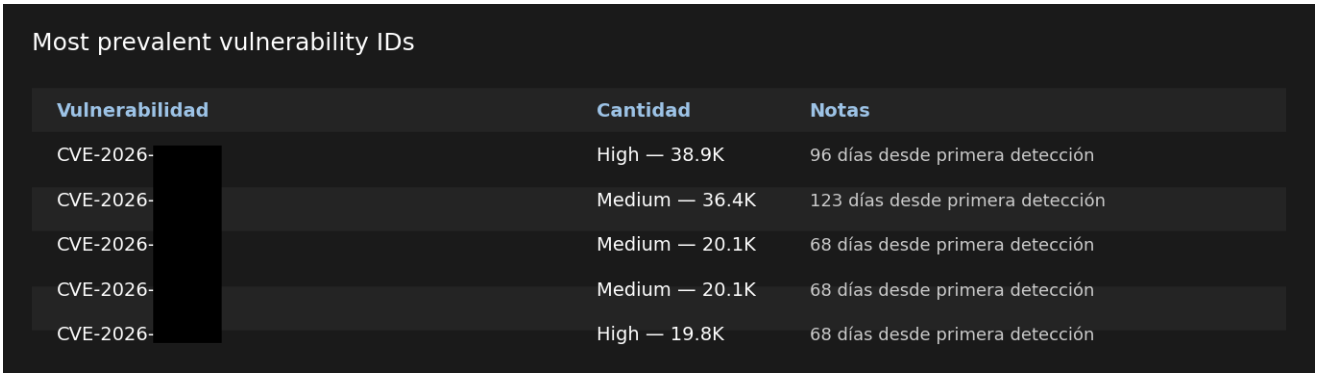
Tabla 1 Descripción de severidad de las amenazas detectadas.

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 junio 2026 registró el mayor número de detecciones (505,035), mientras que mayo 2026 cerró con el nivel más bajo (51,663). A nivel trimestral, se registró un total de 995,462 detecciones, una disminución (36%) en comparación con el trimestre anterior (1,551,828). Esta disminución es consistente con la implementación de las medidas correctivas adoptadas a raíz del incidente atendido medidas correctivas aplicadas conforme a los protocolos establecidos en el Plan de Respuesta a Incidentes Cibernéticos, 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.

Vulnerabilidades Destacadas durante el trimestre abril a junio



Most prevalent vulnerability IDs

Vulnerabilidad	Cantidad	Notas
CVE-2026-[redacted]	High — 38.9K	96 días desde primera detección
CVE-2026-[redacted]	Medium — 36.4K	123 días desde primera detección
CVE-2026-[redacted]	Medium — 20.1K	68 días desde primera detección
CVE-2026-[redacted]	Medium — 20.1K	68 días desde primera detección
CVE-2026-[redacted]	High — 19.8K	68 días desde primera detección

3. Incidentes e investigaciones

La OEIC, a través del CSIRT-PRITS, atendió 5 incidentes de ciberseguridad los días 7 de mayo, 22 de mayo, durante el mes de abril y durante el mes de junio (2 incidentes), activando en cada caso el Plan de Respuesta a Incidentes Cibernéticos del Gobierno de Puerto Rico. Todos fueron gestionados 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-REG-001 Reglamento para la Imposición de Multas por Violaciones a Estándares de Ciberseguridad

Con la aprobación y publicación de PRITS-REG-001 Reglamento para la Imposición de Multas por Violaciones a Estándares de Ciberseguridad el 26 de mayo de 2026, el Gobierno de Puerto Rico fortaleció su marco normativo de ciberseguridad. Establece el procedimiento de PRITS para investigar, procesar y adjudicar querellas por violaciones a los principios de ciberseguridad de la Ley Núm. 40-2024, incluyendo la imposición de multas administrativas como medida disuasiva.

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.

5. Comunicaciones y alertas

Durante este trimestre no se emitieron alertas de phishing a los Oficiales Principales de Informática de las agencias (“OPIs”). La OEIC continúa monitoreando activamente posibles campañas de phishing dirigidas a entidades del Gobierno de Puerto Rico.

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.

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 2026 se llevaron a cabo 2 actividades educativas dirigidas a OPIs, personal técnico, municipios, empleados públicos y jefes de agencias, como Government Tech Summit 2026 en donde se hablaron temas de Innovación, ciberseguridad, Zero trust, Inteligencia artificial y otra de estas actividades lo fue Okta Workflows Workshop herramienta para la administración y manejo de identidad para todo el gobierno.

Cerca de 450 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 de los 5 incidentes atendidos, lo que permitió la contención y recuperación oportuna, minimizando el impacto y preservando la integridad operativa de las entidades afectadas. Si bien esto representa un aumento frente al trimestre anterior (2 incidentes), cada caso fue atendido con activación oportuna de los protocolos correspondientes. 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-REG-001 Reglamento para la Imposición de Multas por Violaciones a Estándares de Ciberseguridad, representa 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 2 actividades de educación, concienciación y adiestramiento ofrecidas durante el trimestre, que impactaron cerca de 450 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 de participación frente a las 2 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 Puerto Rico.

8. Aprobación y Firma

Aprobado y autorizado para publicación hoy 17 de agosto 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