PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

PRITS-CSREP-007

Informe Trimestral

Oficina para la Evaluación de Incidentes Cibernéticos

- Para el periodo comprendido entre el 1 de enero de 2026 al 31 de marzo de 2026

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 enero de 2026 al 31 de marzo 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 enero a marzo de 2026. Nuestros sistemas de vigilancia y análisis en tiempo real permitieron identificar un total de 1,551,828 detecciones, clasificadas según su nivel de severidad, lo que evidencia la importancia de contar con capacidades robustas de ciberdefensa en todo momento.

Enero registró un volumen excepcionalmente alto de detecciones, impulsado principalmente por detecciones de severidad crítica; febrero mostró una caída drástica a niveles mínimos; marzo tuvo un repunte moderado sin alcanzar los niveles observados en enero. Esta vigilancia es clave para la protección de los activos digitales, garantizando una respuesta rápida y efectiva ante posibles ataques.

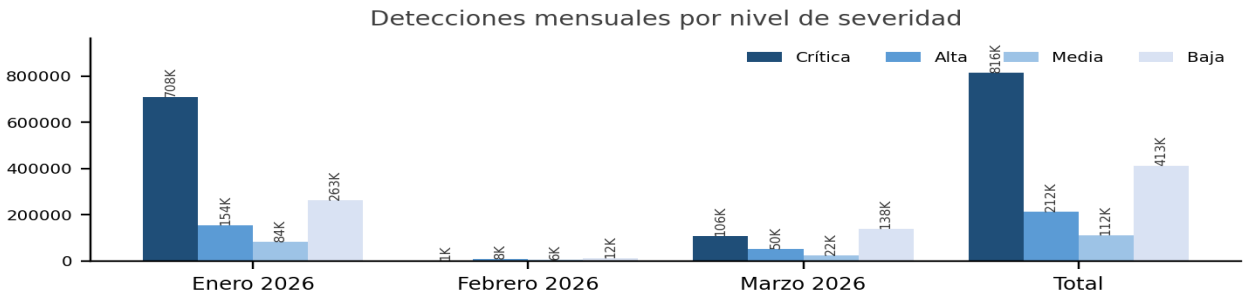


Ilustración 1 Gráfica de la distribución de detecciones por nivel de severidad a lo largo del tercer trimestre del año fiscal 2025-2026.

[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
Enero 2026	707,906	153,600	83,527	262,671	1,207,704
Febrero 2026	1,304	7,670	5,831	12,318	27,123
Marzo 2026	106,474	50,399	22,284	137,844	317,001
Total	**815,684**	**211,669**	**111,642**	**412,833**	**1,551,828**

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 enero a marzo

Most prevalent vulnerability IDs

Vulnerabilidad	Cantidad	Notas
CVE-2026-33116	Medium — 35.1K	91 días desde primera detección
CS-U25-F388142	Low — 23.4K	305 días desde primera detección
CVE-2025-55248	Medium — 22.9K	274 días desde primera detección
CVE-2026-23666	Medium — 18.7K	91 días desde primera detección
CVE-2026-32226	Medium — 18.7K	91 días desde primera detección

Al considerar el volumen de detecciones en conjunto con los incidentes atendidos durante el trimestre, se observa que enero 2026 registró el mayor número de detecciones (1,207,704), mientras que febrero 2026 cerró con el nivel más bajo (27,123). A nivel trimestral, se registró un total de 1,551,828 detecciones, un aumento (90%) en comparación con el trimestre anterior (817,957). 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.

3. Incidentes e investigaciones

La OEIC, a través del CSIRT-PRITS, atendió un incidente de ciberseguridad el 10 de marzo de 2026, activando el Plan de Respuesta a Incidentes Cibernéticos del Gobierno de Puerto Rico. El incidente 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.

La OEIC, a través del CSIRT-PRITS, atendió un incidente de ciberseguridad el 23 de marzo de 2026, activando el Plan de Respuesta a Incidentes Cibernéticos del Gobierno de Puerto Rico. El incidente 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 Políticas vigentes

Durante este trimestre no se publicaron políticas nuevas de ciberseguridad. El marco normativo de políticas y manuales de ciberseguridad previamente publicados por PRITS permanece en pleno efecto, y la OEIC continúa supervisando su cumplimiento en todas las entidades gubernamentales.

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 realizó 1 evaluación de seguridad adicional, 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.
Se destaca también el inicio de la implementación de OKTA como plataforma de inicio de sesión único (SSO) a nivel de todo el Gobierno de Puerto Rico, con un alcance planificado de 62 agencias; se llevaron a cabo reuniones de orientación

con los Oficiales Principales de Informática (OPIs) sobre el proyecto, así como adiestramientos para la administración de la plataforma.

5. Comunicaciones y alertas

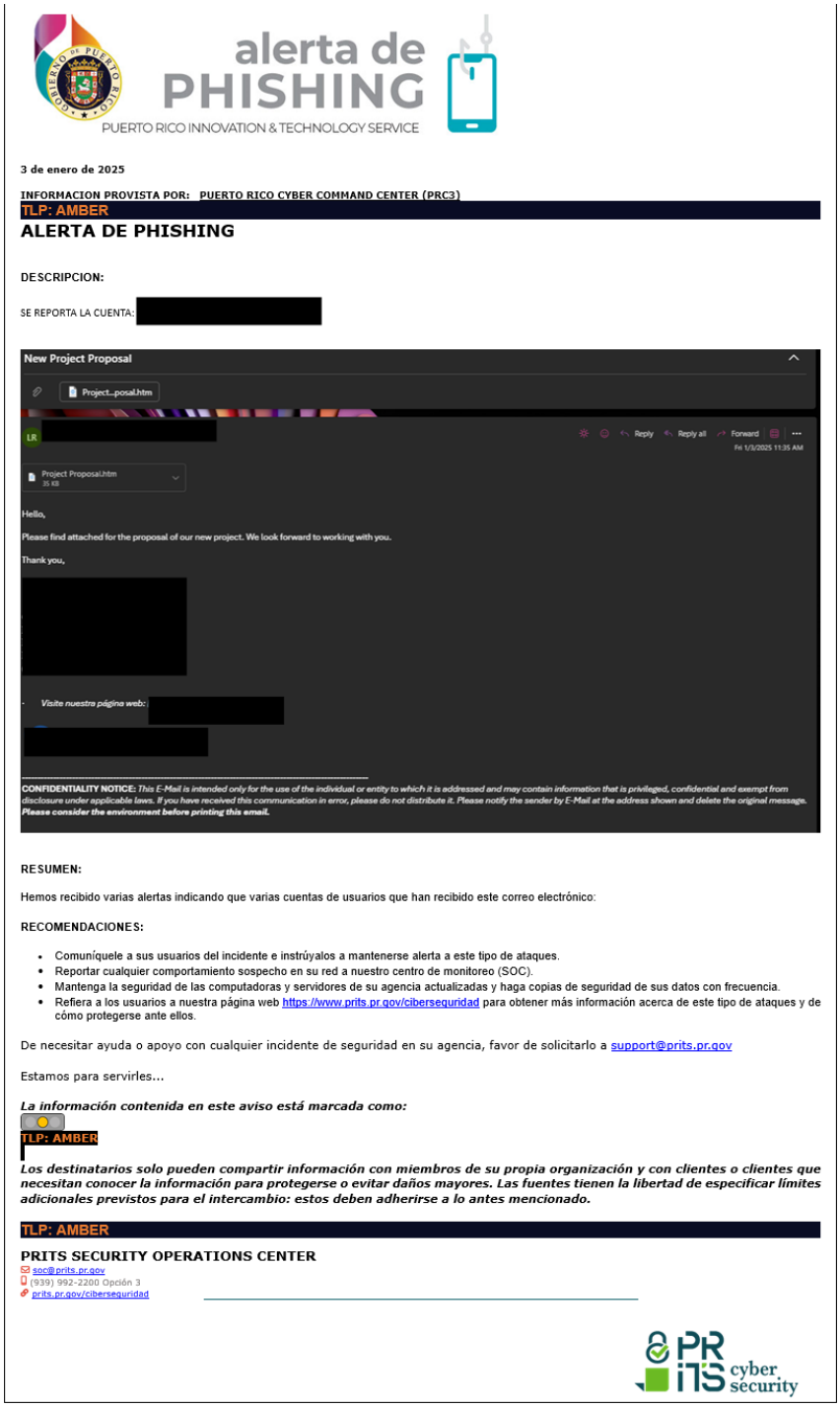
Durante este trimestre se emitieron 1 alerta(s) de *phishing* (ilustración 2) a los Oficiales Principales de Informática de las agencias ("OPIs"). Estas alertas incluyeron detalles sobre las cuentas reportadas, así como las recomendaciones para mitigar el riesgo.

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 35 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 enero, febrero y marzo de 2026 se llevaron a cabo 2 actividades educativas dirigidas a OPIs y personal técnico, incluyendo temas como Orientaciones y recomendaciones en estructurales, reuniones de orientación y adiestramiento.

En total, 45 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 2 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 (0 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, 1 evaluación de seguridad realizada en agencias del Gobierno de Puerto Rico; el inicio de la implementación de OKTA como plataforma de inicio de sesión único (SSO) a nivel de todo el Gobierno de Puerto Rico, con un alcance planificado de 62 agencias; se llevaron a cabo reuniones de orientación con los Oficiales Principales de Informática (OPIs) sobre el proyecto, así como adiestramientos para la administración de la plataforma, 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 2 actividades de educación, concienciación y adiestramiento ofrecidas durante el trimestre, que impactaron a 45 participantes, han sido fundamentales para fortalecer la resiliencia institucional, equipando a servidores públicos con herramientas prácticas para identificar, reportar y actuar ante amenazas cibernéticas. Aunque el número de actividades formales fue menor que en el trimestre anterior (15), la OEIC mantuvo su apoyo continuo a las agencias en temas de ciberseguridad a través de otros canales, según se detalla en la sección de Gobernanza.

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