PUERTO RICO INNOVATION
& TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

VIA CORREO ELECTRÓNICO

16 de mayo de 2025

A: 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 Estado Libre Asociado de Puerto Rico”, la Oficina para la Evaluación de Incidentes Cibernéticos (OEIC) presenta el Informe Trimestral de Ciberseguridad, correspondiente al período del 1 de enero al 31 de marzo de 2025.

Este informe ofrece una visión integral de los esfuerzos realizados para fortalecer la ciberseguridad del Gobierno de Puerto Rico, abarcando aspectos clave como la detección de amenazas, la gestión de incidentes, el cumplimiento normativo, la capacitación del personal gubernamental y la concienciación en ciberseguridad. A través de iniciativas estratégicas y un enfoque proactivo, continuamos trabajando para salvaguardar la infraestructura tecnológica del Gobierno y proteger la información de nuestros ciudadanos.

Confiamos en que este informe proporcionará un panorama detallado de las acciones implementadas y los desafíos que enfrentamos en el ámbito de la ciberseguridad. Nos mantenemos a su disposición para ampliar cualquier información o discutir iniciativas adicionales que contribuyan a fortalecer la resiliencia digital del Gobierno. Para ello, se pueden comunicarse con nosotros a través del correo electrónico cybersec@prits.pr.gov. Asimismo, estamos preparados para presentar estos hallazgos en persona si lo consideran necesario.

Atentamente,

Rubén M. Quiñonez Millan
Principal Oficial de Tecnología
Puerto Rico Innovation and Technology Service

Poincaré Díaz Peña
Principal Oficial de Seguridad Cibernética
Puerto Rico Innovation and Technology Service

PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

PRITS-CSREP-003

Informe Trimestral de Ciberseguridad

Oficina para la Evaluación de Incidentes Cibernéticos

- Enero a Marzo 2025

Tabla de Contenido

1. Introducción

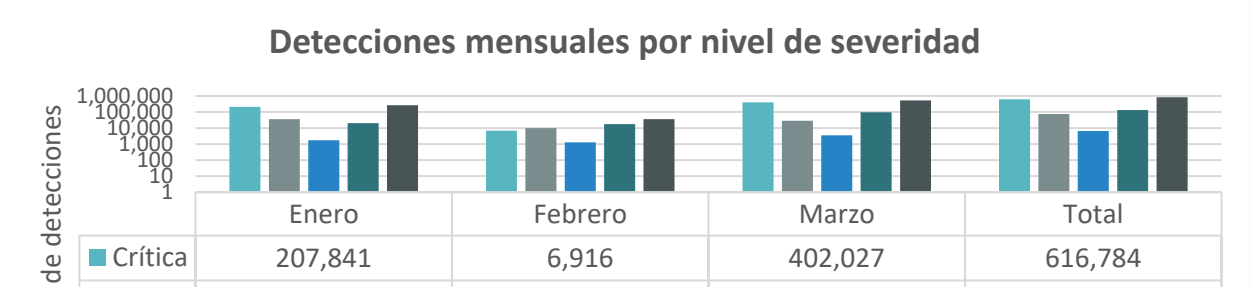
En cumplimiento con la Ley Núm. 40-2024, conocida como la "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", la Oficina para la Evaluación de Incidentes Cibernéticos (OEIC) presenta el informe trimestral de ciberseguridad correspondiente al periodo del 1 de enero al 31 de marzo de 2025. Este documento detalla las iniciativas y esfuerzos realizados para fortalecer la seguridad digital del Gobierno de Puerto Rico y proteger la información de los ciudadanos ante un panorama de amenazas que cambian constantemente.

A lo largo del trimestre, se han implementado medidas clave en materia de detección y respuesta a incidentes, gobernanza y cumplimiento normativo, concienciación en ciberseguridad y comunicación estratégica con las agencias gubernamentales. Además, se han llevado a cabo entrenamientos especializados y simulaciones de ciberataques para mejorar la preparación y capacidad de respuesta ante posibles amenazas.

2. Detecciones

Como parte del esfuerzo continuo para resguardar la infraestructura tecnológica, se han identificado y gestionado diversas amenazas cibernéticas mediante un monitoreo constante. Nuestros sistemas de detección analizan grandes volúmenes de datos en tiempo real, permitiendo reconocer patrones anómalos y tomar medidas preventivas para evitar incidentes de seguridad.

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



	Enero	Febrero	Marzo	Total
Crítica	207,841	6,916	402,027	616,784
Alta	36,139	9,818	28,447	74,404
Media	1,724	1,269	3,527	6,520
Baja	19,975	17,590	96,139	133,704
Total	265,679	35,593	530,140	831,412

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

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.

3. Incidentes e investigaciones

El 18 de enero de 2025, se detectó un acceso no autorizado a una infraestructura gubernamental. En respuesta inmediata, se activó el Equipo de Respuesta a Incidentes de Seguridad Cibernética del Puerto Rico Innovation and Technology Service (CSIRT-PRITS), conforme a los protocolos establecidos. El CSIRT-PRITS inició de forma inmediata las labores de contención, análisis y erradicación de los artefactos maliciosos identificados. Gracias a la rápida intervención del equipo, el incidente fue mitigado eficazmente, evitando que se concretara un ataque mayor, como la ejecución de ransomware o la exfiltración de datos sensibles.

El 26 de marzo de 2025, se recibió notificación sobre un incidente cibernético que afectó a una entidad gubernamental. De forma inmediata, se activó el protocolo de respuesta a incidentes cibernéticos, incluyendo la movilización del equipo del CSIRT-PRITS para apoyar las labores de mitigación.

El incidente comprometió una porción significativa de la infraestructura tecnológica de la entidad, resultando en la interrupción de sus operaciones por un período de dos días. No obstante, los servicios dirigidos a la ciudadanía no se vieron afectados, ya que la entidad contaba con un plan de continuidad operacional debidamente establecido, el cual permitió mantener la prestación de servicios esenciales.

Gracias a la experiencia del equipo de respuesta y la implementación de buenas prácticas en ciberseguridad y recuperación ante incidentes, los sistemas afectados fueron restaurados en un periodo razonable, garantizando la integridad de la información y restableciendo la operatividad institucional.

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 refuerza su compromiso con la protección de los datos personales al establecer un marco claro y estandarizado para el manejo responsable de la información. Esta 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 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 Oficina Estatal de Innovación y Ciberseguridad (OEIC) mantiene el monitoreo de estos esfuerzos y provee el acompañamiento técnico necesario para asegurar la resiliencia de la infraestructura digital del Gobierno.

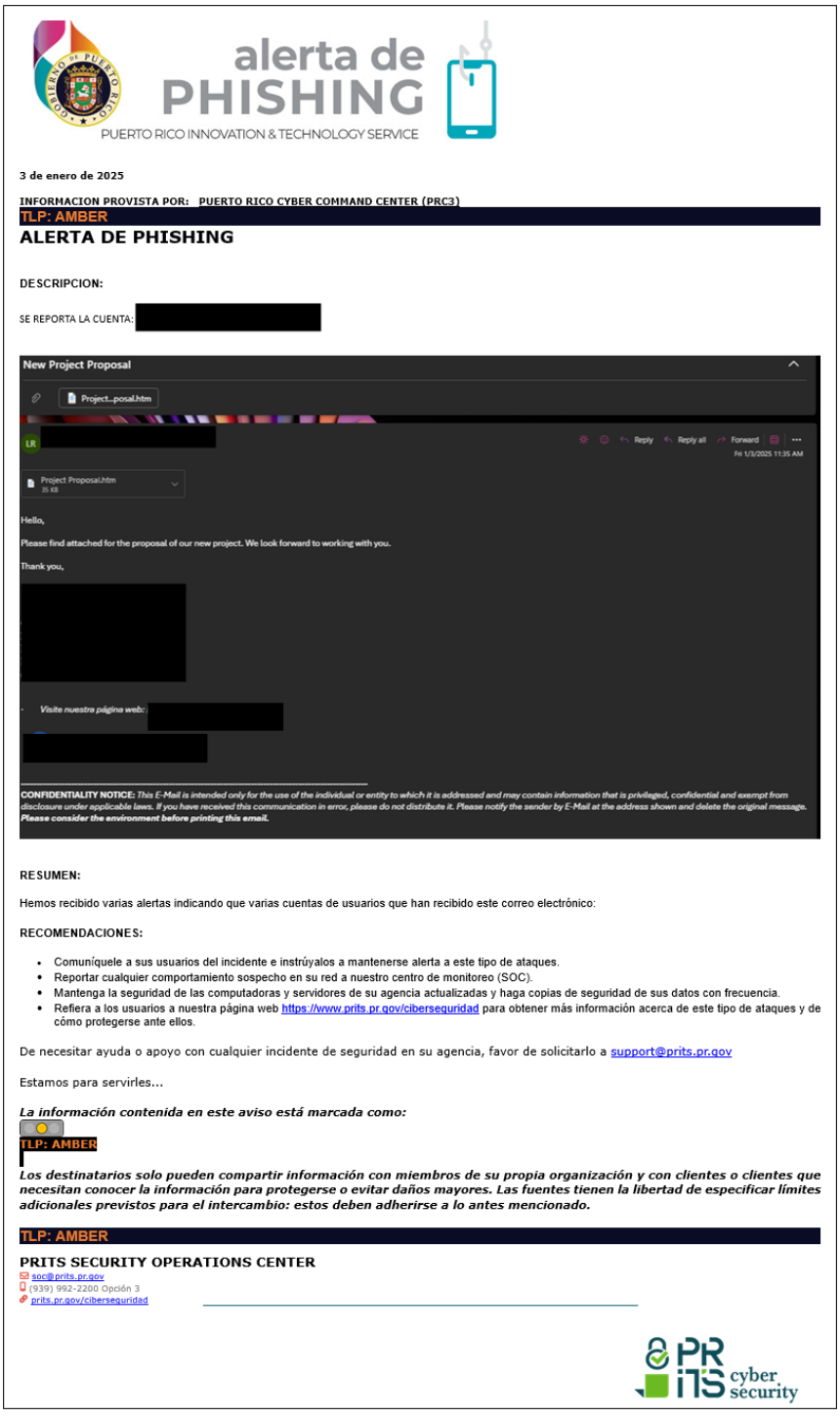
5. Comunicaciones y alertas

Durante este trimestre se emitieron 10 alertas de *phishing* (ilustración 2) a los Oficiales Principales de Informática (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

LR [redacted]

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]

[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

Durante los días 14, 28 y 29 de enero, así como el 7 de febrero de 2025, personal de la Oficina para la Evaluación de Incidentes Cibernéticos ofreció charlas de concienciación en ciberseguridad a empleados públicos de tres agencias gubernamentales, impactando a más de 150 servidores públicos.

Estas sesiones forman parte de los esfuerzos continuos del Gobierno de Puerto Rico para fortalecer la cultura de seguridad digital en el servicio público. Entre los temas abordados durante las orientaciones se incluyen:

- Phishing: ¿Qué es?, ¿cómo reconocerlo?, ¿qué hacer si se recibe un intento?, y las principales estrategias utilizadas para su propagación.
- Ransomware: Tipos de ataques, cómo identificar si se es víctima y cuáles son las acciones recomendadas ante un incidente de este tipo.
- Autenticación multifactor (MFA): Definición, beneficios para los usuarios y su importancia dentro de una estrategia de protección de cuentas y sistemas.
- Deepfakes: Qué son, cómo reconocerlos y cuáles son las estrategias comúnmente utilizadas para su difusión.

Estas charlas refuerzan el compromiso de la OEIC con la capacitación continua del recurso humano en el sector público para fortalecer la resiliencia cibernética del gobierno.

Ilustración 3 Charla de concienciación de ciberseguridad ofrecida al personal gubernamental.

6.2 Adiestramiento Tenable

El 10 y 12 de marzo, PRITS organizó una capacitación virtual para las agencias que participan de la primera fase de la implementación de la herramienta de manejo de vulnerabilidades Tenable. Esta herramienta es utilizada para la gestión de vulnerabilidades en sistemas, redes y aplicaciones. Permite identificar, evaluar y priorizar riesgos de seguridad en infraestructuras tecnológicas del gobierno. A través de escaneos automatizados, la plataforma facilita la detección de configuraciones inseguras, parches faltantes y otros puntos críticos, permitiendo a las agencias tomar acciones correctivas para fortalecer su postura de ciberseguridad.

Durante esta sesión se cubrieron:

- instalación y configuración.
- operaciones
- descripción general de la tecnología que incluye discusiones sobre la arquitectura y el diseño para entornos típicos.
- instrucciones detalladas de escaneo y análisis.

6.3 Adiestramiento de OKTA

Durante los días 31 de enero, 20 y 21 de marzo de 2025, se llevaron a cabo talleres básicos sobre la administración de la plataforma de Manejo de Identidad y Credenciales OKTA, dirigidos a personal técnico de agencias gubernamentales.

OKTA es una solución de gestión de identidad y acceso (IAM) que permite controlar de manera segura el acceso de los usuarios a sistemas, aplicaciones y datos. Entre sus funcionalidades principales se destacan la autenticación multifactor (MFA), el inicio de sesión único (SSO) y la gestión centralizada de usuarios. Esta plataforma fortalece la postura de ciberseguridad institucional al garantizar que únicamente personal autorizado acceda a los recursos, reduciendo así los riesgos de accesos no autorizados y suplantaciones de identidad.

Estos talleres apoyan los esfuerzos del Gobierno de Puerto Rico por implementar herramientas modernas y seguras en cumplimiento con la Ley 40-2024 y la Política de Identidad, Credenciales y Acceso

- Introducción a la alianza PRITS & OKTA
    - Descripción de funcionalidades clave de OKTA.

  - Beneficios del soporte y la comunidad de usuarios de OKTA.
  - Enfoque “Customer First” y rol del Customer Success Manager.
- Visión general de administración de OKTA
  - Uso del panel de administración (Admin Dashboard).
  - Descripción de los roles estándar de administrador.
  - Responsabilidades clave del rol de Super Admin.
  - Información general sobre la certificación de administradores OKTA.
- Integraciones con aplicaciones en el entorno PRITS
  - Integración con Active Directory.
  - Integración con Microsoft Office 365.
- Presentación del Roadmap de integraciones OKTA para 2025.
  - Nuevas funcionalidades y noticias destacadas
  - Cambios en el acceso y visibilidad de casos de soporte.
  - Discusión de temas relevantes y noticias recientes sobre OKTA.



6.4 Capacitación sobre Clasificación de datos a través de Microsoft Purview

En febrero de 2025, PRITS organizó una sesión dirigida a los directores de informática de las agencias gubernamentales con el objetivo de destacar la importancia de la clasificación de datos como paso fundamental para avanzar hacia la implementación efectiva de soluciones de inteligencia artificial en el entorno gubernamental.

Durante la sesión, se enfatizó que una adecuada categorización de la información permite aplicar controles de seguridad más precisos, garantizar la privacidad de los datos ciudadanos y facilitar su uso responsable para análisis avanzados. Esta práctica, además de mejorar la eficiencia operativa, es esencial para cumplir con la Ley Núm. 122-2019, conocida como la Ley de Datos Abiertos de Puerto Rico, la cual establece directrices para el acceso y la reutilización de información gubernamental de forma transparente y segura.

En este evento, se contó con la participación de personal especializado de Microsoft, quienes ofrecieron orientación sobre el uso de Microsoft Purview, la plataforma de

Microsoft diseñada para la gobernanza, clasificación y protección de datos. Purview permite identificar y etiquetar automáticamente datos sensibles, aplicar políticas de protección según su nivel de confidencialidad y monitorear el uso de la información en todo el entorno digital. Esta herramienta resulta clave para fortalecer la postura de seguridad, cumplir con requisitos regulatorios y habilitar el uso ético de la inteligencia artificial en el gobierno.

6.5 Capacitación sobre Respuesta a Incidentes y Análisis Forense Digital

Como parte de los esfuerzos para cerrar el trimestre con iniciativas de fortalecimiento institucional, los días 18 y 28 de marzo se llevaron a cabo dos adiestramientos dirigidos a personal técnico de agencias gubernamentales.

El primero de estos adiestramientos se centró en los procesos de respuesta ante incidentes cibernéticos, incluyendo la identificación, contención, erradicación y recuperación ante eventos de seguridad.

El segundo adiestramiento estuvo enfocado en proporcionar herramientas y metodologías para la recolección de evidencia digital y análisis forense, elementos clave para la investigación y documentación adecuada de incidentes.

Ambas sesiones contribuyen al fortalecimiento de las capacidades del gobierno en ciberseguridad, promoviendo una postura más resiliente ante amenazas digitales y apoyando el cumplimiento de las políticas de respuesta a incidentes vigentes.

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 Oficina para la Evaluación de Incidentes Cibernéticos (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, que permitió la contención y recuperación ante accesos no autorizados y ataques dirigidos a infraestructuras críticas. Estas acciones han demostrado la capacidad del equipo del CSIRT-PRITS para responder con agilidad, minimizando el impacto y preservando la integridad operativa de las agencias afectadas.

De igual forma, la publicación de la Política de Privacidad (PRITS-POL-0009), las evaluaciones de vulnerabilidades técnicas en múltiples entidades, y la implementación de herramientas como Tenable y OKTA, 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.

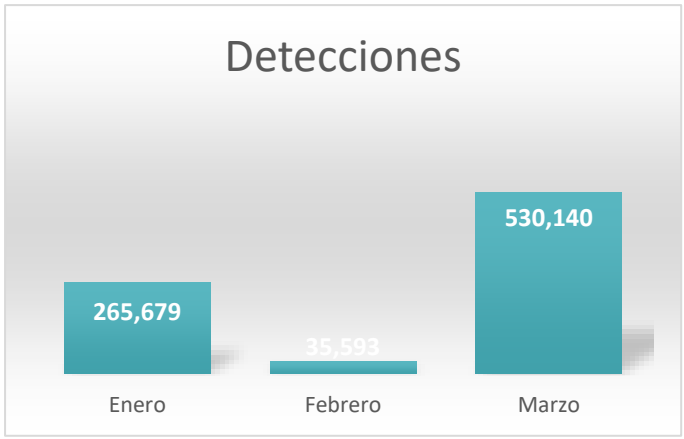
Las actividades de educación, concienciación y adiestramiento que incluyeron capacitaciones sobre phishing, ransomware, clasificación de datos con Microsoft Purview, y análisis forense digital han sido fundamentales para fortalecer la resiliencia institucional. Estas acciones han impactado positivamente a cientos de servidores públicos, equipándolos con herramientas prácticas para identificar, reportar y actuar ante amenazas cibernéticas.

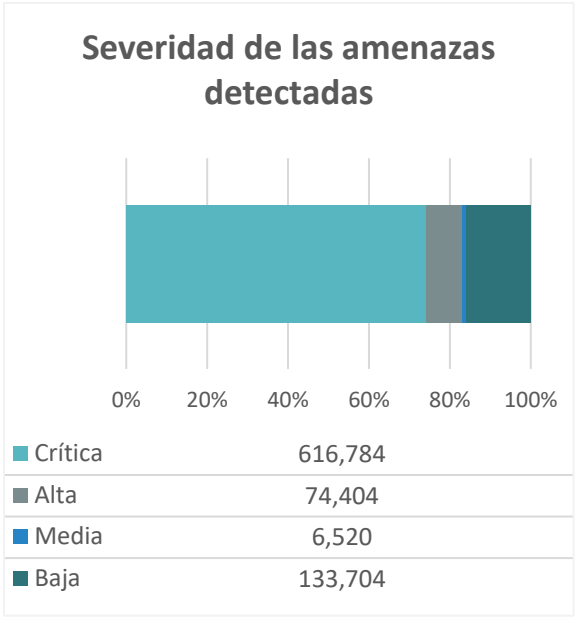
De cara a los próximos trimestres, la OEIC continuará desarrollando y ejecutando estrategias robustas de prevención, detección y respuesta, al tiempo que promoverá una

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.

Apéndice I: Resumen del informe

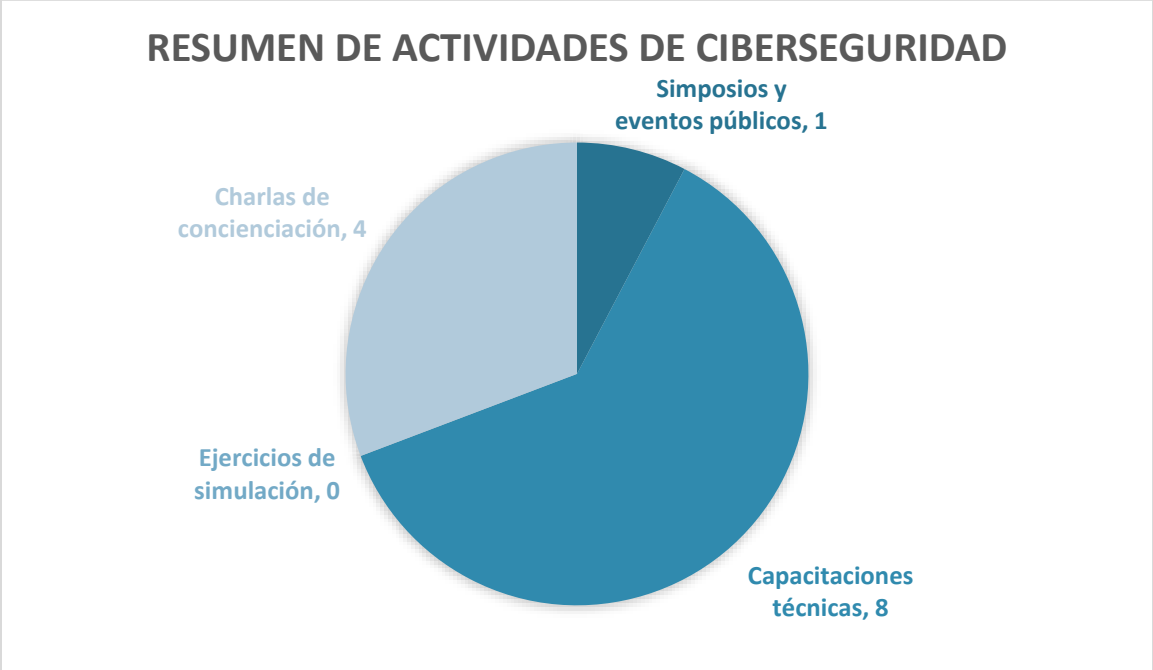
Ciberseguridad en números





Incidentes significativos	2	Investigaciones en curso	0	Publicación de gobernanza	1	Alertas de *phishing* emitidas	10

831,412
Detecciones en el trimestre


RESUMEN DE ACTIVIDADES DE CIBERSEGURIDAD
Simposios y eventos públicos, 1
Charlas de concienciación, 4
Ejercicios de simulación, 0
Capacitaciones técnicas, 8