PUERTO RICO INNOVATION
& TECHNOLOGY SERVICE

PRITS

GOBIERNO DE PUERTO RICO

VIA CORREO ELECTRÓNICO

27 de febrero 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 octubre al 31 de diciembre de 2024.

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,

Antonio J. Ramos Guardiola
Principal Ejecutivo de Innovación e Información
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-CSREP-002

Informe Trimestral de Ciberseguridad

Oficina para la Evaluación de Incidentes Cibernéticos

- Octubre a diciembre 2024

Tabla de Contenido

1. Introducción

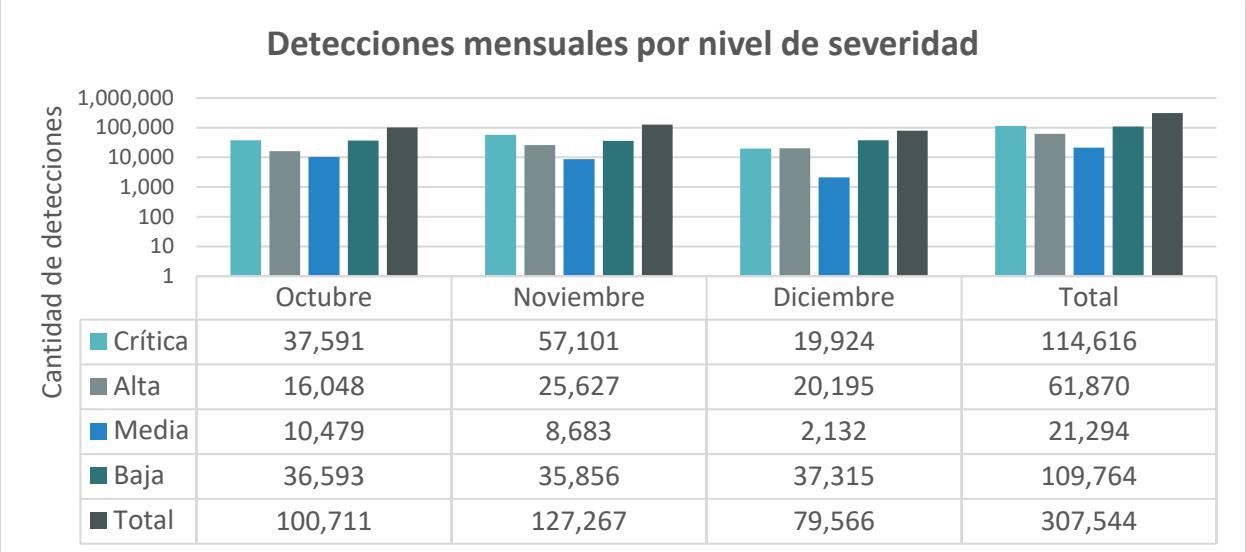
En cumplimiento con la Ley Núm. 40-2024, conocida como la "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", la Oficina para la Evaluación de Incidentes Cibernéticos (OEIC) presenta el informe trimestral de ciberseguridad correspondiente al periodo del 1 de octubre al 31 de diciembre de 2024. 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.



	Octubre	Noviembre	Diciembre	Total
Crítica	37,591	57,101	19,924	114,616
Alta	16,048	25,627	20,195	61,870
Media	10,479	8,683	2,132	21,294
Baja	36,593	35,856	37,315	109,764
Total	100,711	127,267	79,566	307,544

Ilustración 1 Gráfica de la distribución de detecciones por nivel de severidad a lo largo del segundo 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 1 de octubre de 2024, se detectó un ataque de ransomware que afectó varios servidores físicos, estaciones de trabajo y máquinas virtuales de una agencia. Tras identificar el incidente, el equipo de tecnología implementó medidas iniciales para contener y recuperar los sistemas comprometidos, a la espera de orientación especializada.

El 2 de octubre de 2024, se solicitó apoyo adicional para la respuesta al incidente y la determinación de la causa raíz. Como parte del análisis forense digital, se recopiló información clave, incluyendo diagramas de red, inventarios de sistemas, registros de firewall y datos de los sistemas impactados. Se llevaron a cabo procesos de adquisición y análisis de imágenes forenses con el fin de esclarecer el origen del ataque y evaluar posibles interacciones con los datos de la agencia.

Gracias a la aplicación de las mejores prácticas en materia de ciberseguridad y recuperación de incidentes, los sistemas fueron restaurados en un tiempo considerable, asegurando la integridad de la información y la continuidad operativa de la agencia.

Actualmente no hay investigación en curso relacionada con incidentes cibernéticos.

4. Gobernanza y cumplimiento

4.1 Política de Respuesta a Incidentes de Seguridad de la Información

Con la aprobación y publicación en noviembre de la Política de Respuesta a Incidentes de Seguridad de la Información, el Gobierno de Puerto Rico refuerza la seguridad digital al establecer un marco claro y estandarizado para la gestión de incidentes. Esto permite una respuesta más rápida y eficaz ante amenazas, minimizando el impacto en la continuidad operativa y la protección de datos gubernamentales.

Además, la política promueve la coordinación interagencial al definir responsabilidades específicas y procedimientos alineados con estándares internacionales como el Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST CSF). Esto facilita la interoperabilidad entre agencias y fortalece la resiliencia del ecosistema digital del gobierno.

Finalmente, su implementación impulsa una cultura de prevención y mejora continua, asegurando que las entidades gubernamentales cuenten con capacitaciones, herramientas y mecanismos de monitoreo para adaptarse a las amenazas emergentes y cumplir con los requisitos legales en ciberseguridad.

4.2 Procedimiento para informar incidentes de seguridad de la información

En cumplimiento con la Ley Núm. 40-2024, se aprobó y publicó el Procedimiento para informar incidentes de seguridad de la información, con el propósito de establecer un proceso estructurado y eficiente para la notificación de eventos que puedan comprometer la ciberseguridad de los sistemas gubernamentales. Este procedimiento garantiza una respuesta coordinada y oportuna ante incidentes de ciberseguridad, permitiendo la recopilación de información clave y la activación de medida de mitigación a través de la Oficina para la Evaluación de Incidentes Cibernéticos (OEIC), adscrita a PRITS.

Este procedimiento fortalece la ciberseguridad al definir claramente las responsabilidades de las agencias gubernamentales, empleados y proveedores de servicios contratados. Al permitir la notificación de incidentes a través de

correo electrónico y la herramienta Service Desk, se facilita la comunicación inmediata para atender incidentes, asegurando una mayor trazabilidad y eficiencia en la gestión de éstos. Además, el procedimiento establece plazos estrictos, como la obligación de los proveedores de reportar incidentes dentro de las primeras 48 horas, lo que refuerza la transparencia y el cumplimiento de estándares de seguridad.

Las implicaciones de este procedimiento son significativas, ya que establecen un marco normativo que impulsa la cultura de seguridad en el ecosistema gubernamental. Su aplicación no solo permite una mejor coordinación entre agencias y entidades federales, sino que también reduce el impacto de amenazas cibernéticas mediante la detección y respuesta temprana. A medida que se implemente este proceso, será crucial la capacitación continua de los empleados y la evaluación periódica de su efectividad para garantizar su éxito a largo plazo.

4.3 Evaluación de vulnerabilidades web

Como parte de los esfuerzos para fortalecer la ciberseguridad del Gobierno de Puerto Rico, se realizaron evaluaciones de seguridad web en diversos subdominios y páginas web gubernamentales. Estas evaluaciones permitieron identificar vulnerabilidades y notificar a las agencias correspondientes con recomendaciones para su mitigación.

Varias agencias ya han comenzado a tomar acciones correcticas, fortaleciendo sus plataformas y reduciendo riesgos de seguridad. La OEIC continúa monitoreando estos esfuerzos y brindando apoyo para asegurar la protección de la infraestructura digital gubernamental.

5. Comunicaciones y alertas

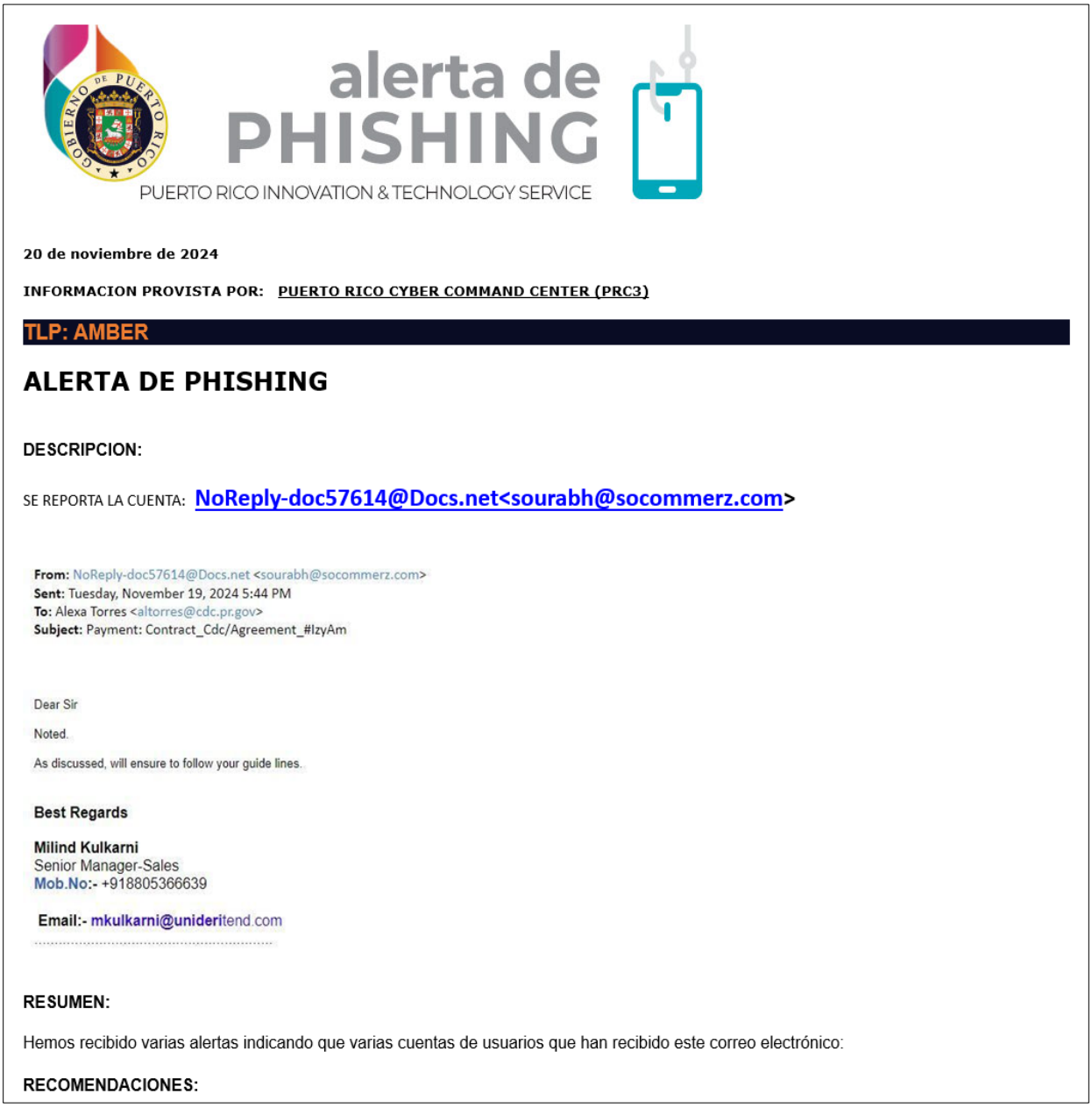
Durante este trimestre se emitieron 9 alertas de *phishing* (ilustración 2) a los Oficiales Principales de Informática (OPIs). Estas alertas incluyeron detalles sobre las cuentas reportadas, así como las recomendaciones para mitigar el riesgo.

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

20 de noviembre de 2024

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

TLP: AMBER

ALERTA DE PHISHING

DESCRIPCION:

SE REPORTA LA CUENTA: NoReply-doc57614@Docs.net<sourabh@socommerz.com>

From: NoReply-doc57614@Docs.net <sourabh@socommerz.com>
Sent: Tuesday, November 19, 2024 5:44 PM
To: Alexa Torres <altorres@cdc.pr.gov>
Subject: Payment: Contract_Cdc/Agreement_#IzyAm

Dear Sir

Noted.

As discussed, will ensure to follow your guide lines.

Best Regards

Milind Kulkarni
Senior Manager-Sales
Mob.No:- +918805366639

Email:- mkulkarni@unideritend.com

RESUMEN:

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

RECOMENDACIONES:

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

6. Educación, concienciación y adiestramientos

6.1 Primer Simposio Antiterrorismo Doméstico

Los días 8 y 9 de octubre, PRITS participó en el Primer Simposio Antiterrorismo Doméstico organizado por la Junta de Seguridad Pública de la Región Sur. Este

evento reunió a expertos y funcionarios de distintas áreas para discutir estrategias de seguridad, incluyendo la seguridad cibernética, un tema cada vez más relevante en la protección del gobierno y la ciudadanía.

Como parte de la participación de PRITS, se instaló una mesa informativa donde se explicaron:

- Los principales riesgos de seguridad en el mundo digital, como los ataques de hackers, el robo de información y el fraude en línea.
- El Plan de Ciberseguridad del Gobierno, que establece cómo se protege la información y los sistemas digitales de las agencias públicas.
- Las herramientas y servicios que PRITS ofrece a las agencias y municipios para ayudarlos a mejorar su seguridad digital.

Además, el Principal Oficial de Seguridad Cibernética tuvo la oportunidad de hablar ante el público sobre el rol de PRITS en la protección de los activos digitales gubernamentales y los servicios de ciberseguridad disponibles.

Ilustración 3 Personal de ciberseguridad de PRITS en la mesa informativa durante el Primer Simposio de Antiterrorismo Doméstico.

6.2 Adiestramiento Falcon CrowdStrike

El 15 de octubre, PRITS organizó una capacitación especial para los Oficiales Principales de Informática (OPIs) de las agencias gubernamentales. Los OPIs son los responsables de administrar y proteger los sistemas tecnológicos de cada agencia, por lo que es fundamental que estén actualizados en temas de ciberseguridad.

Durante esta sesión, se explicaron tres temas clave:

- Servicios del *Center for Internet Security* (CIS)
  Este centro ofrece herramientas para ayudar a las agencias a identificar y prevenir amenazas digitales, algunas de ellas sin costo.

- Descripción general del *Security Operation Center* (SOC)
  Es un centro especializado donde se monitorean constantemente las redes del gobierno para detectar actividades sospechosas o intentos de ciberataques.

- Uso de *Falcon CrowdStrike EDR*
  Es un sistema avanzado que detecta y responde rápidamente a posibles ataques informáticos antes de que causen daño.

Con esta capacitación, los OPIs aprendieron sobre nuevas herramientas y estrategias para fortalecer la seguridad digital de sus agencias.

Ilustración 4 Participantes del adiestramiento sobre Falcon CrowdStrike.

6.3 Capacitación en seguridad de redes con Fortinet

En octubre, PRITS organizó dos sesiones de adiestramiento técnico en colaboración con Fortinet, con el objetivo de fortalecer las capacidades de los participantes en la administración y seguridad de redes.

- 23 de octubre – Introducción a la Seguridad de Red con Fortinet

Este entrenamiento enseñó a los participantes a instalar y configurar un sistema de seguridad llamado FortiGate, que ayuda a controlar el tráfico de internet y prevenir accesos no autorizados. También se explicó cómo:

- Aplicar reglas de seguridad para proteger los datos.
- Detectar y bloquear posibles amenazas.
- Utilizar métodos seguros de conexión, como las redes privadas virtuales (VPNs).

- 24 de octubre – Fortalecimiento de la Red Empresarial
  En esta sesión más avanzada, los participantes aprendieron cómo hacer que las redes del gobierno sean más rápidas, seguras y eficientes. Se abordaron temas como:
  - Cómo reducir el impacto de los ataques cibernéticos con sistemas automatizados.
  - Cómo mejorar la visibilidad de amenazas en la red y responder a ellas rápidamente.
  - Cómo optimizar la conexión a internet en agencias con múltiples oficinas utilizando ADVPN (una tecnología que mejora la seguridad y velocidad de las redes).

Estos entrenamientos ayudaron a mejorar la protección de los sistemas informáticos del gobierno, reduciendo los riesgos de ataques y mejorando el acceso seguro a la información.

Ilustración 5 Principal Oficial de Seguridad Cibernética orientando a los participantes del adiestramiento para mejorar la seguridad de las redes gubernamentales.

6.4 Ejercicios de simulación de ciberataques (*Tabletop Exercises* – TTXs)

Para evaluar qué tan preparados están el gobierno y los municipios para enfrentar un ataque cibernético, PRITS organizó dos ejercicios de simulación los días 14 y 15 de noviembre.

Estos ejercicios se realizaron usando un método llamado *Tabletop Exercise* (TTX), en el que los participantes analizan distintos escenarios de ataques ficticios y deciden cómo responderían ante ellos. En esta ocasión, se practicó la respuesta ante un ataque de *ransomware*, un tipo de virus que bloquea el acceso a la información hasta que se pague un rescate.

- 14 de noviembre – Ejercicio con agencias grandes
  - Participaron 23 empleados correspondientes a 9 agencias.
  - Se practicó cómo detectar y responder rápidamente ante un ataque cibernético de gran escala.

- 15 de noviembre – Ejercicio con agencias pequeñas y municipios
  - Participaron 24 empleados de 9 agencias y 2 municipios.
  - Se enfocó en los desafíos que enfrentan las entidades con menos recursos y personal.

Ambos ejercicios contaron con la participación de expertos del sector privado y agencias federales, permitiendo la colaboración intersectorial y el intercambio de ideas y mejores prácticas.

Ilustración 6 Personal de las agencias durante el ejercicio de simulación de un ciberataque de ransomware.

6.5 Capacitación en Splunk

Los días 5 y 6 de diciembre, PRITS ofreció entrenamientos sobre Splunk, una herramienta utilizada para analizar grandes cantidades de información y detectar

amenazas de seguridad. Splunk ayuda a detectar patrones sospechosos en las redes del gobierno, permitiendo una respuesta más rápida ante posibles amenazas.

En este entrenamiento, se explicaron:

- Cómo funciona Splunk y su arquitectura.
- Cómo organizar y separar datos de manera segura.
- Cómo se configura Splunk en la nube para mejorar el monitoreo de seguridad.

Este entrenamiento permitió a los participantes optimizar el uso de Splunk para la gestión y análisis de datos de seguridad, mejorando la capacidad de monitoreo y detección de amenazas.

6.6 Charla de concienciación en ciberseguridad

Para cerrar el año, el 17 de diciembre, se ofreció una charla educativa sobre ciberseguridad al personal de la Junta de Planificación. El objetivo de esta charla fue aumentar la conciencia sobre los peligros en el mundo digital y enseñar buenas prácticas para proteger la información. Se abordaron temas como:

- Cómo identificar correos electrónicos fraudulentos (*phishing*) que intentan engañar a los usuarios para que entreguen su información.
- La importancia de crear contraseñas seguras y no compartirlas.
- Cómo proteger dispositivos personales y laborales ante ataques cibernéticos.

Estas charlas son fundamentales para que los empleados del gobierno adopten hábitos seguros y ayuden a prevenir incidentes de seguridad.

Ilustración 7 Charla de concienciación de ciberseguridad ofrecida al personal de la Junta de Planificación.

7. Conclusión

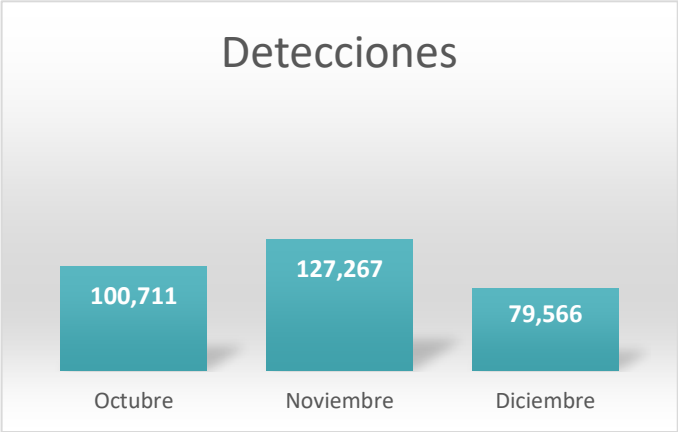
El fortalecimiento de la ciberseguridad en el Gobierno de Puerto Rico es un proceso continuo que requiere vigilancia, capacitación y colaboración entre todas las agencias. Durante este trimestre, la OEIC ha trabajado activamente en la detección y mitigación de amenazas, la respuesta a incidentes críticos y la implementación de políticas que refuercen la postura de seguridad digital a nivel gubernamental.

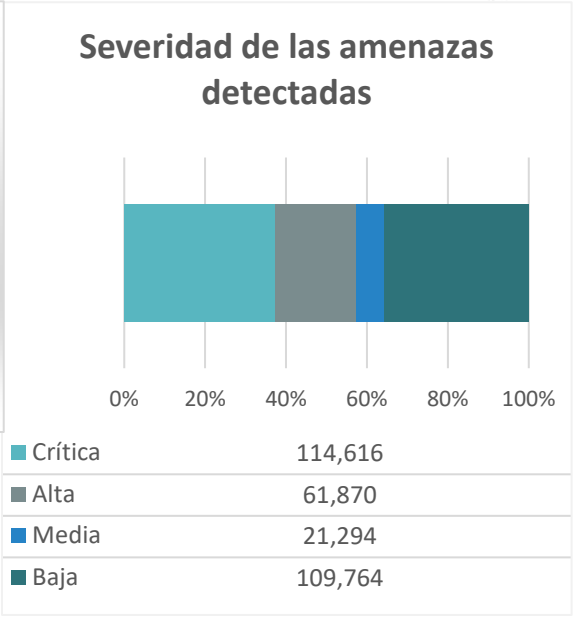
Las iniciativas de concienciación y capacitación han sido esenciales para dotar al personal de conocimientos y herramientas que permitan una respuesta más efectiva ante ataques cibernéticos. Asimismo, el desarrollo de procedimientos estandarizados y el fortalecimiento de la gobernanza han contribuido a mejorar la coordinación y resiliencia del ecosistema digital del Gobierno.

En los próximos trimestres, continuaremos reforzando nuestras estrategias de prevención y respuesta, adaptándonos a las nuevas amenazas y promoviendo una cultura de ciberseguridad en toda la administración pública. La protección de la infraestructura digital y la seguridad de la información de los ciudadanos seguirán siendo nuestra prioridad.

Apéndice I: Resumen del informe

Ciberseguridad en números





307,544
Detecciones en el trimestre

Incidentes significativos	1	Investigaciones en curso	0	Publicación de gobernanza	2	Alertas de *phishing* emitidas	9