PUERTO RICO INNOVATION & TECHNOLOGY SERVICE

PRITS

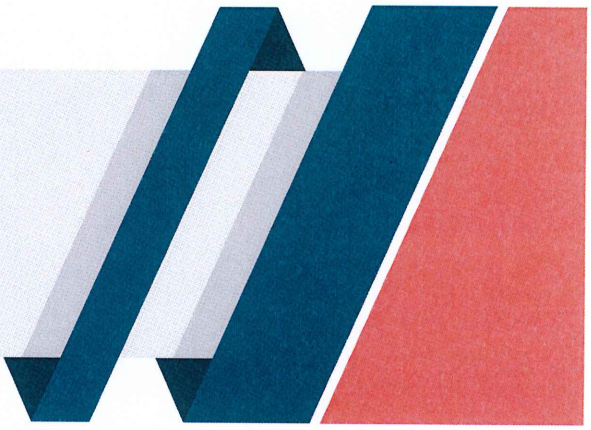
GOBIERNO DE PUERTO RICO

**PRITS-CSREP-004**

# Informe Trimestral

## *Oficina para la Evaluación de Incidentes Cibernéticos*

- Para el periodo comprendido entre el 1 de octubre de 2025 al 31 de diciembre 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 octubre de 2025 al 31 de diciembre 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 octubre a diciembre de 2025. Nuestros sistemas de vigilancia y análisis en tiempo real permitieron identificar un total de 2,369,643 detecciones, clasificadas según su nivel de severidad, lo que evidencia la importancia de contar con capacidades robustas de ciberdefensa en todo momento.

El análisis mensual reflejó un comportamiento irregular con un volumen significativamente alto de detecciones críticas durante octubre, seguido por una disminución en noviembre y un repunte moderado en diciembre. Esta fluctuación responde, en parte, a campañas dirigidas identificadas y neutralizadas oportunamente.

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

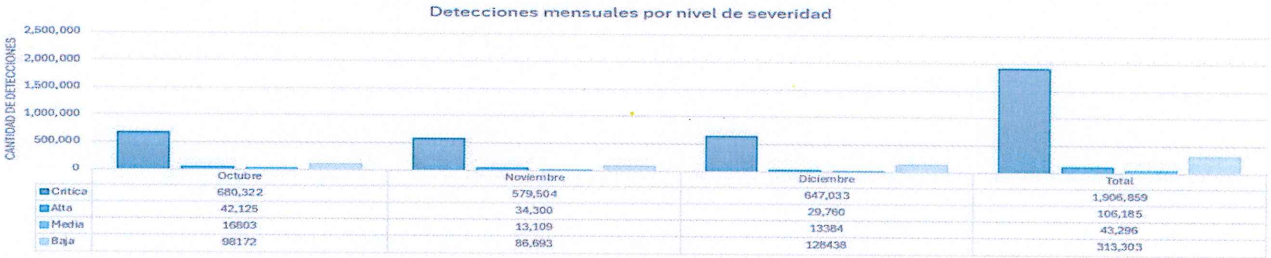



*Ilustración 1 Gráfica de la distribución de detecciones por nivel de severidad a lo largo del tercer trimestre del año fiscal 2024-2025.*

[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.*

*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 octubre a diciembre

Most prevalent vulnerability IDs

| ExPRT rating | Vulnerability ID | Vulnerabilities | First seen on your hosts |
|---|---|---|---|
| Medium | CVE-2025-55248 | 33.2K | 117 days |
| Medium | CVE-2025-14322 | 28.3K | 61 days |
| Medium | CVE-2025-14325 | 28.3K | 61 days |
| Medium | CVE-2025-14324 | 28.3K | 61 days |
| Low | CVE-2025-14331 | 28.3K | 61 days |

Most vulnerable hosts

| Hostname | Count | First seen on this host |
|---|---|---|
| UPRRPSMTXWV1 | 7.2K | 104 days |
| lb2dro | 6.1K | 132 days |
| selha | 6.1K | 132 days |
| saicgdtm | 6K | 132 days |
| lb2vrd | 6K | 132 days |

## 3. Incidentes e investigaciones

El 25 de noviembre de 2025, la OEIC recibió múltiples notificaciones por parte de varias agencias gubernamentales que reportaron haber sido víctimas de un ataque tipo *ransomware,* por lo que se activó de inmediato el Equipo de Respuesta a Incidentes Cibernéticos del Gobierno de Puerto Rico (CSIRT-PRITS), conforme a los protocolos establecidos en la Política de Respuesta a Incidentes.

El equipo técnico se organizó y se dividió para trasladarse físicamente a las jurisdicciones afectadas, con el fin de brindar apoyo especializado en todas las fases del manejo del incidente, incluyendo la identificación, contención, erradicación, recuperación (de ser necesario) y el análisis forense preliminar. La oportuna intervención permitió mitigar el impacto del ataque, confirmar que solo tres de las múltiples agencias notificadas resultaron afectadas, iniciar el restablecimiento completo de las operaciones esenciales en dichas agencias y definir medidas correctivas orientadas a prevenir incidentes similares en el futuro.

Es importante destacar que, al momento del incidente, las agencias afectadas contaban con servicios de monitoreo activo provistos por PRITS y la OEIC. No obstante, los ambientes comprometidos correspondían a infraestructuras fuera de soporte, tanto a nivel de sistemas operativos como del agente de detección utilizado por la OEIC, lo que limitó la capacidad de detección temprana y de respuesta automatizada en dichos entornos. En contraste, los sistemas que sí contaban con el agente de detección debidamente soportado no fueron impactados por el ataque.

Como resultado del incidente, se inició un proceso de actualización de los ambientes afectados, incluyendo la modernización de los sistemas operativos y la instalación del agente de detección correspondiente, con el objetivo de fortalecer las capacidades de monitoreo y respuesta ante amenazas futuras.

Este evento evidenció la importancia de contar con capacidades técnicas avanzadas, infraestructuras actualizadas y una coordinación interagencial efectiva para responder de manera adecuada a incidentes que afecten infraestructuras críticas del Gobierno. A raíz del incidente, se comenzó una revisión integral de la arquitectura tecnológica, las políticas de respaldo, la segmentación de redes y los controles de acceso de los sistemas impactados, con el propósito de reducir riesgos y fortalecer la continuidad operativa de los servicios gubernamentales.

## 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.

## 5. Comunicaciones y alertas

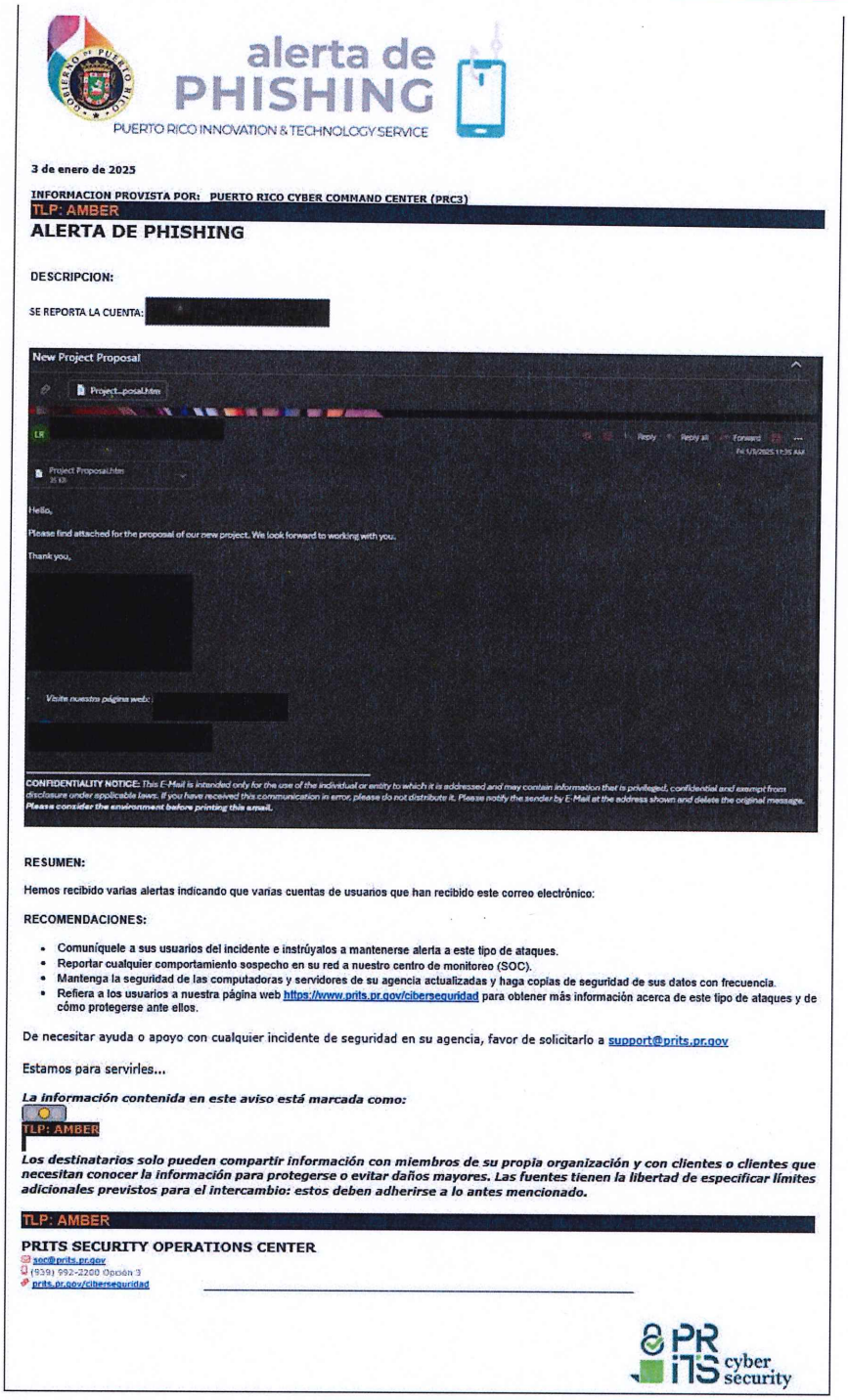
Durante este trimestre se emitieron 2 alertas de *phishing* (ilustración 2) a los Oficiales Principales de Informática de las agencias ("OPIs"). Estas alertas incluyeron detalles sobre las cuentas reportadas, así como las recomendaciones para mitigar el riesgo.

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

Project Proposal.htm

Hello,

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

Thank you,

Visite nuestra página web:

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) 992-2260 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 y el uso responsable de tecnologías emergentes en el Gobierno de Puerto Rico, durante los meses de octubre y noviembre de 2025 se llevaron a cabo múltiples adiestramientos y charlas educativas dirigidas tanto a empleados públicos como a estudiantes.

Durante este período se ofrecieron adiestramientos especializados a los OPIs, personal técnico y municipios, enfocados en temas críticos como la protección de la información bajo la nueva política de inteligencia artificial, ejercicios de mesa sobre *ransomware* impulsado por inteligencia artificial, arquitecturas y soluciones de seguridad de Fortinet, operaciones de Centros de Operaciones de Seguridad ("SOC"), modelos de Zero Trust y programas efectivos de manejo de vulnerabilidades en el entorno gubernamental. Estas iniciativas permitieron reforzar las capacidades técnicas, operacionales y estratégicas del personal responsable de la seguridad de los sistemas de información del Gobierno.

De manera complementaria, se realizaron charlas de concienciación en ciberseguridad dirigidas a estudiantes, impactando comunidades escolares mediante orientaciones sobre riesgos cibernéticos, buenas prácticas digitales y prevención de amenazas. Entre estas se incluyen charlas ofrecidas a estudiantes de escuelas públicas y privadas, contribuyendo a la formación temprana de una ciudadanía digital más informada y resiliente.

Adicionalmente, se ofreció un adiestramiento de alto impacto sobre el Portal de Transparencia del Gobierno de Puerto Rico, con una participación significativa de servidores públicos, reforzando los principios de acceso a la información, cumplimiento y uso seguro de plataformas digitales gubernamentales. También se brindaron adiestramientos internos al personal de PRITS como parte del fortalecimiento institucional continuo.

En total, más de 860 participantes fueron impactados a través de estas iniciativas educativas durante los meses de octubre y noviembre de 2025, reflejando el compromiso del Gobierno de Puerto Rico con la capacitación continua, la concienciación en ciberseguridad y la preparación ante los riesgos asociados al entorno digital actual.

Como parte de la continuidad de estos esfuerzos, el 1 de diciembre de 2025 se llevó a cabo la mesa redonda "Adultos Mayores Frente al Fraude y los Riesgos Cibernéticos", dirigida a promover la prevención, educación y protección de poblaciones vulnerables ante amenazas digitales y esquemas de fraude.

## 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, 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.

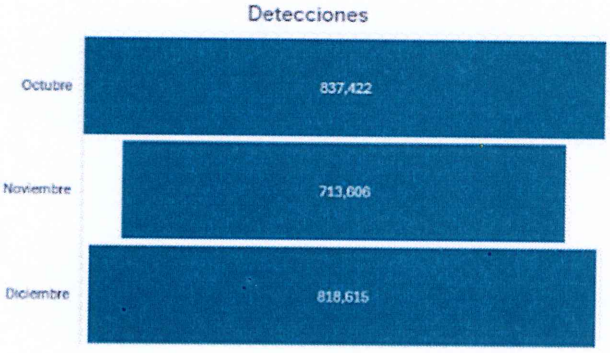
## 8. Aprobación y Firma

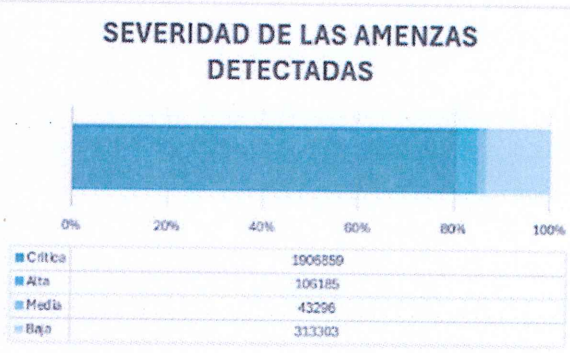
Aprobado y autorizado para publicación hoy 10 de febrero de 2025, en San Juan, Puerto Rico.

Poincaré Díaz Peña
Principal Oficial de Innovación e Información
Puerto Rico Innovation and Technology Service

## Apéndice I: Resumen del informe

### Ciberseguridad en números




| Incidentes significativos | 3 | Investigaciones en curso | 0 | Publicación de gobernanza | 1 | Alertas de *phishing* emitidas | 2 |
|---|---|---|---|---|---|---|---|