VIA CORREO ELECTRÓNICO

23 de octubre de 2024

A: Hon. José Luis Dalmau
Presidente
Senado de Puerto Rico

Hon. Rafael Hernández
Presidente
Cámara de Representantes de Puerto Rico

Estimados señores Presidentes:

Me dirijo a ustedes en cumplimiento con lo establecido en la Ley 40 del 18 de enero de 2024, conocida como "Ley de Ciberseguridad del Estado Libre Asociado de Puerto Rico", para presentarles el primer informe trimestral de la Oficina para la Evaluación de Incidentes Cibernéticos (OEIC).

Este informe resume las gestiones e investigaciones realizadas por nuestra Oficina durante el primer trimestre del año fiscal en curso. Como Principal Oficial de Seguridad Cibernética (CISO), es mi deber informarles sobre los avances y desafíos en materia de ciberseguridad que enfrenta el Gobierno.

El informe adjunto detalla nuestras actividades en las siguientes áreas clave:

- Detecciones realizadas de posibles amenazas cibernéticas.
- Notificaciones de *phishing* recibidas y gestionadas.
- Incidentes reportados directamente a nuestra Oficina.
- Investigaciones en curso sobre brechas de seguridad y ataques cibernéticos.
- Charlas de concienciación en ciberseguridad impartidas a empleados gubernamentales, publico general y jóvenes.

Estos datos proporcionan una visión general de nuestras operaciones y del panorama actual de la ciberseguridad en el Gobierno. Consideramos que esta información es crucial para la toma de decisiones informadas en futuras políticas y asignaciones de recursos en materia de seguridad cibernética.

Para cualquier aclaración o información adicional que requieran sobre el contenido de este informe, 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-001

Informe Trimestral

Oficina para la Evaluación de Incidentes Cibernéticos

- julio a septiembre 2024

PR ITS cyber security

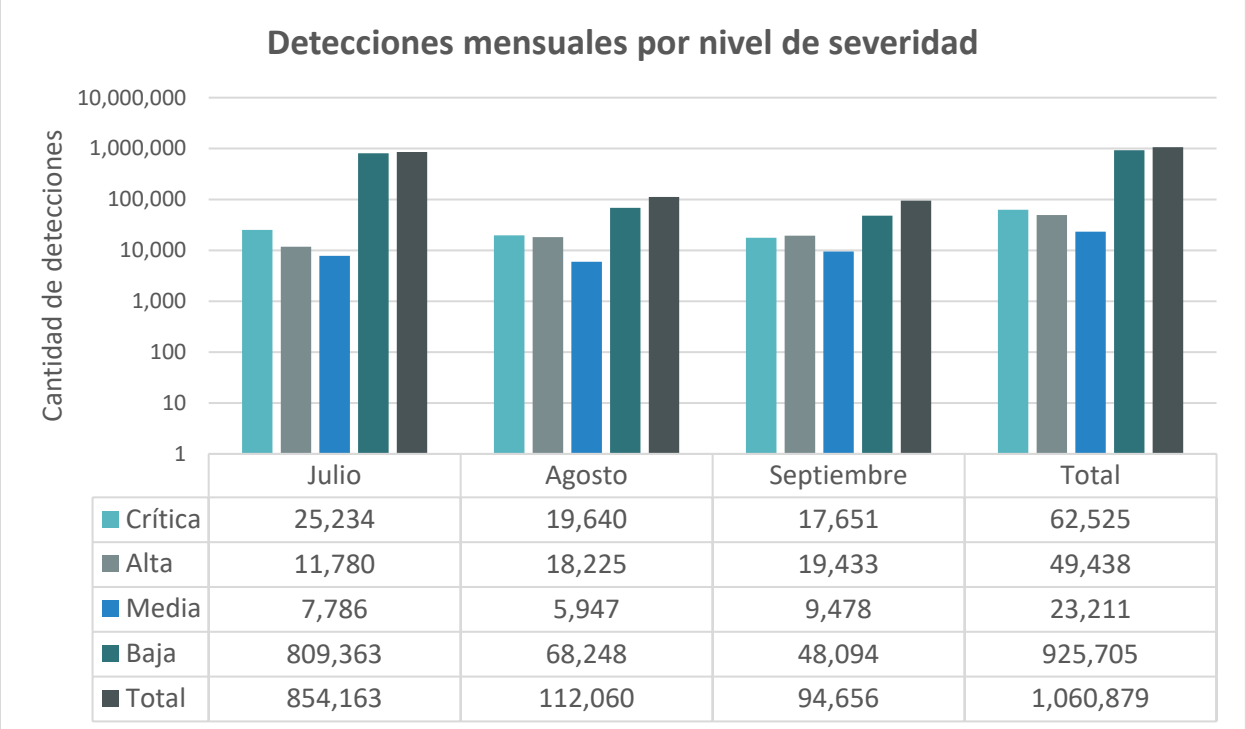
TABLA DE CONTENIDO

1. Introducción

En cumplimiento con las disposiciones de la Ley Núm. 40-2024, conocida como "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. Este documento ofrece una visión general de nuestras gestiones y logros en materia de seguridad cibernética durante el período que comprende del 1ro de julio al 30 de septiembre del año en curso. El informe abarca las detecciones realizadas, incidentes reportados, investigaciones en curso, iniciativas de gobernanza implementadas, comunicaciones y alertas emitidas a las agencias, así como las actividades de concienciación llevadas a cabo. A través de este informe, buscamos proporcionar una perspectiva clara y transparente de nuestros esfuerzos continuos para salvaguardar la infraestructura digital del Gobierno y proteger la información de nuestros ciudadanos.

2. Detecciones

Manteniendo una vigilancia constante sobre nuestra infraestructura, nuestros sistemas de detección han logrado identificar y responder a diversas amenazas cibernéticas de forma proactiva. A través de un monitoreo ininterrumpido y el análisis de grandes volúmenes de datos, hemos podido detectar patrones sospechosos y tomar las medidas necesarias para proteger nuestros activos digitales.



	Julio	Agosto	Septiembre	Total
Crítica	25,234	19,640	17,651	62,525
Alta	11,780	18,225	19,433	49,438
Media	7,786	5,947	9,478	23,211
Baja	809,363	68,248	48,094	925,705
Total	854,163	112,060	94,656	1,060,879

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

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.

Tabla 1: Descripción de severidad de las amenazas detectadas.

3. Incidentes e Investigaciones

Durante el pasado trimestre no se reportaron incidentes significativos que hayan afectado las operaciones gubernamentales o comprometido la integridad o confidencialidad de los sistemas. Como resultado, actualmente no hay ninguna investigación en curso relacionada con incidentes cibernéticos.

Gracias a la implementación de medidas de seguridad y a la vigilancia constante de nuestra infraestructura, hemos logrado mantener los sistemas de información a salvo de amenazas externas. Sin embargo, continuamos realizando evaluaciones para asegurar la protección continua de los sistemas gubernamentales.

4. Gobernanza y Cumplimiento

En el mes de agosto, se logró un avance en materia de gobernanza de datos con la aprobación y publicación de la Política de Clasificación de Datos del Gobierno de Puerto Rico. Esta nueva normativa representa un paso importante en nuestros esfuerzos continuos por fortalecer la seguridad de la información en el ámbito gubernamental.

El propósito fundamental de esta política es establecer un marco estandarizado para el manejo apropiado de la información gubernamental, tomando en cuenta los diversos niveles de sensibilidad y criticidad operacional de los datos. Con su implementación, se busca mitigar de manera efectiva los riesgos asociados al manejo inadecuado de información, asegurando que cada tipo de dato reciba los controles de seguridad y el tratamiento adecuado según su clasificación asignada.

La correcta clasificación de los datos y la aplicación de medidas de protección correspondientes permitirán a las agencias gubernamentales prevenir una serie de amenazas potenciales. Entre estas se incluyen los accesos no autorizados, las fugas de información confidencial y las modificaciones indebidas de datos críticos. Estas medidas son cruciales para salvaguardar la privacidad de los ciudadanos, mantener la integridad de las operaciones gubernamentales y, en última instancia, preservar la confianza pública en las agencias.

En esencia, esta política sienta las bases para una gestión responsable y segura de los datos gubernamentales. Lo logra a través de la estandarización de prácticas, la definición clara de roles y el establecimiento de responsabilidades específicas en torno a la clasificación y el manejo apropiado de la información. Este enfoque mejora nuestra postura de ciberseguridad, al tiempo que promueve una cultura de responsabilidad y conciencia en el manejo de datos sensibles en todo el aparato gubernamental.

En un esfuerzo por fortalecer la seguridad cibernética del Gobierno, se llevó a cabo una serie de evaluaciones exhaustivas de seguridad web. Estas evaluaciones tenían como objetivo principal identificar posibles vulnerabilidades en los sitios web gubernamentales que pudieran ser explotadas por actores malintencionados.
Para garantizar un enfoque sistemático y eficaz, el proceso comenzó con un análisis preliminar detallado de vulnerabilidades. Este análisis incluyó la identificación de direcciones IP públicas, el mapeo de subdominios asociados y la evaluación del estado de protección contra ataques de denegación de servicio (DoS). Esta fase preparatoria fue esencial para orientar nuestros esfuerzos hacia las áreas más críticas y optimizar el proceso de evaluación.

Las evaluaciones de seguridad se realizaron utilizando herramientas avanzadas de escaneo, abarcando más de 1,190 subdominios y páginas web pertenecientes a dominios pr.gov y servicios provistos por terceros. Este amplio alcance nos permitió obtener una visión integral de la postura de ciberseguridad de los sitios web gubernamentales evaluados.

Como parte de nuestro compromiso con la mejora continua, se enviaron comunicaciones detalladas a las agencias correspondientes. Estas cartas incluían un inventario completo de las vulnerabilidades detectadas, clasificadas según su nivel de criticidad. El objetivo de esta comunicación era doble: por un lado, informar a las agencias sobre los hallazgos específicos de sus sitios web, y por otro, proporcionar la base necesaria para que cada

agencia pueda desarrollar e implementar planes de acción para mitigar las vulnerabilidades identificadas.

De este modo, se estableció un canal de comunicación bidireccional con las agencias, permitiendo aclarar dudas, ofrecer apoyo y monitorear de cerca la implementación de las medidas de seguridad recomendadas. Este proceso no solo busca abordar las vulnerabilidades actuales, sino también fortalecer la capacidad general de las agencias para mantener altos estándares de seguridad web en el futuro.

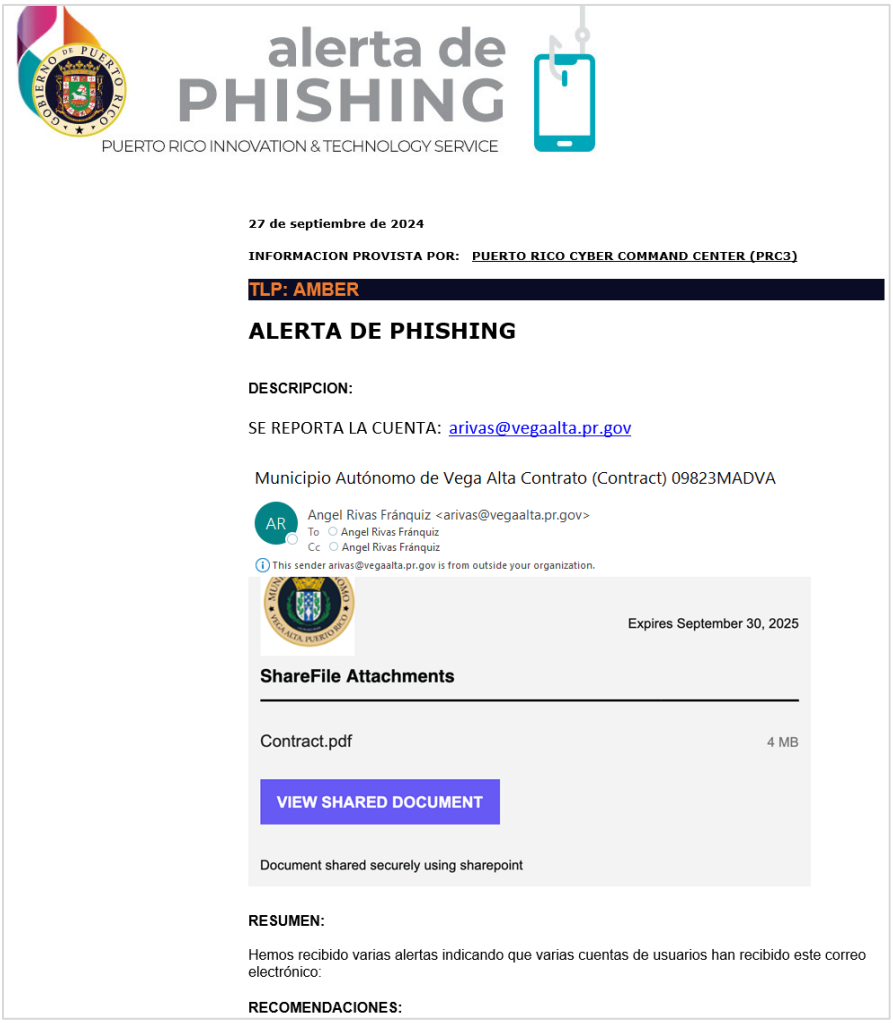
5. Comunicaciones y Alertas

Durante este trimestre se emitieron 42 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 con la formación en ciberseguridad 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

27 de septiembre de 2024

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

TLP: AMBER

ALERTA DE PHISHING

DESCRIPCION:

SE REPORTA LA CUENTA: arivas@vegaalta.pr.gov

Municipio Autónomo de Vega Alta Contrato (Contract) 09823MADVA

AR Angel Rivas Fránquiz <arivas@vegaalta.pr.gov>
To Angel Rivas Fránquiz
Cc Angel Rivas Fránquiz
This sender arivas@vegaalta.pr.gov is from outside your organization.

Expires September 30, 2025

ShareFile Attachments

Contract.pdf 4 MB

VIEW SHARED DOCUMENT

Document shared securely using sharepoint

RESUMEN:

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

RECOMENDACIONES:

6. CHARLAS Y CONCIENCIACIÓN

Durante el trimestre, se llevaron a cabo un total de 5 charlas en temas asociados a la ciberseguridad (ilustración 3). En agosto, se impartieron dos sesiones dirigidas a empleados de agencias gubernamentales, enfocándose en mejores prácticas y seguridad de la información. Asimismo, se realizó una charla de concienciación al público en general. En septiembre, se ofrecieron dos charlas a estudiantes, abordando el uso responsable de redes sociales y el ciberacoso.

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

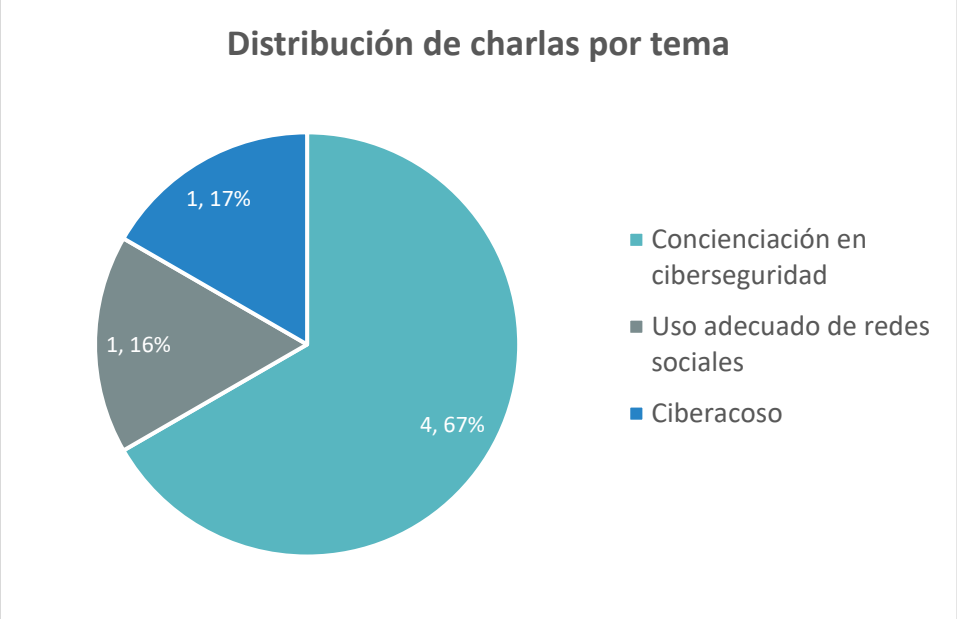


Ilustración 3: Gráfica de la distribución de charlas por tema en el trimestre.

Estas actividades de concienciación forman parte de nuestros esfuerzos continuos para educar y preparar a diversos sectores de la población en temas críticos de ciberseguridad. Las charlas han permitido llegar a un amplio espectro de la sociedad, desde funcionarios públicos hasta estudiantes, abordando temas relevantes para cada grupo.

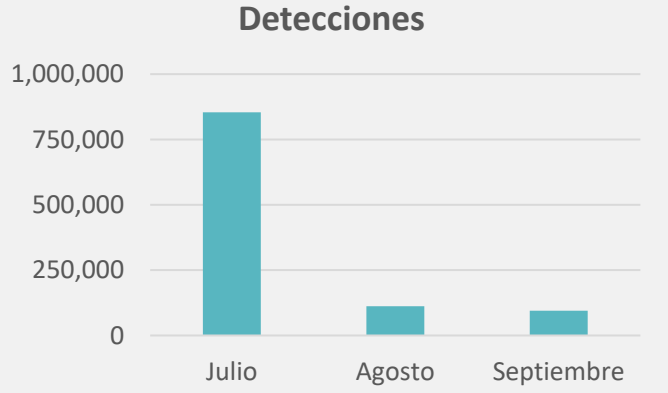
Estas iniciativas educativas contribuyen significativamente a la creación de un entorno digital más seguro para todos los ciudadanos, fomentando una cultura de responsabilidad y conciencia en el uso de tecnologías digitales.

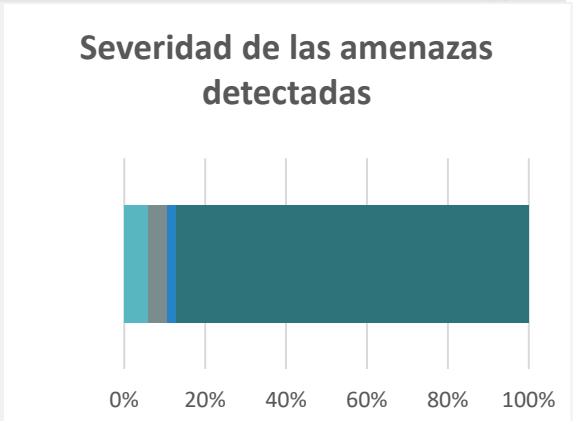
7. Conclusión

El trimestre reportado refleja el compromiso de la OEIC con la mejora de la postura de ciberseguridad del Gobierno. A través de las detecciones proactivas, el desarrollo de la Política de Clasificación de Datos, la emisión de alertas y las iniciativas de concienciación, continuamos fortaleciendo las defensas cibernéticas. La ausencia de incidentes reportados y la falta de investigaciones en curso durante este periodo son indicadores de la eficacia de nuestras estrategias. Sin embargo, reconocemos que la ciberseguridad es un desafío constante. Continuaremos adaptando nuestras prácticas, mejorando nuestras capacidades y colaborando estrechamente con las agencias y municipios para mantener un entorno digital seguro y resiliente.

8. Apéndice I: Resumen del Informe

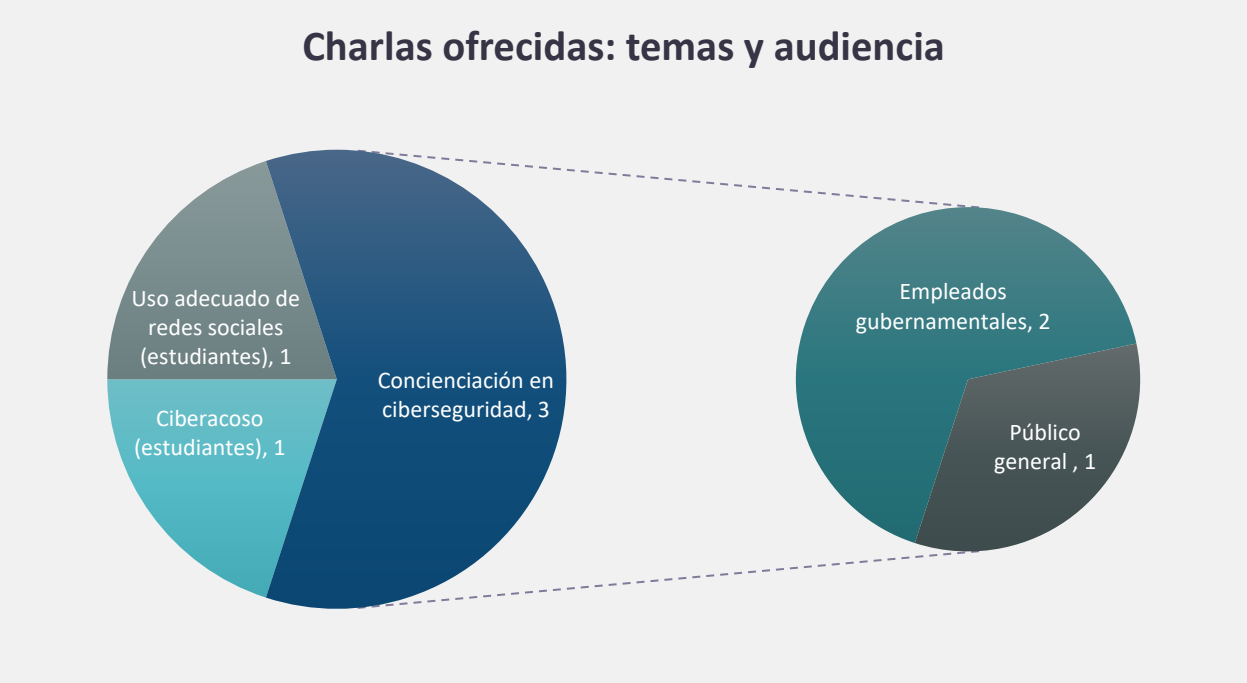
Ciberseguridad en números





Incidentes significativos	0	Investigaciones en curso	0	Publicación de gobernanza	1	Alertas de *phishing* emitidas	42

1,070,879
Detecciones en el trimestre


Charlas ofrecidas: temas y audiencia
Uso adecuado de redes sociales (estudiantes), 1
Ciberacoso (estudiantes), 1
Concienciación en ciberseguridad, 3
Empleados gubernamentales, 2
Público general , 1