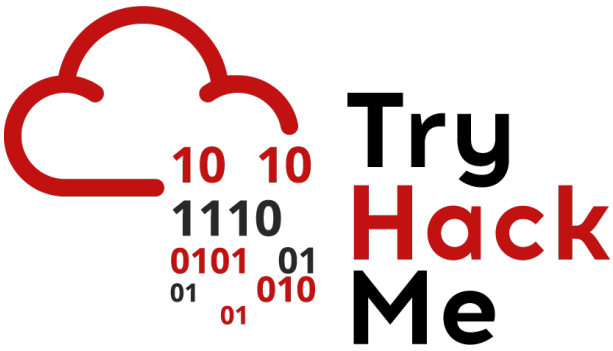
Writeup: Sala *Common Attacks*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

En la sala Common Attacks aprenderemos sobre los ataques más comunes utilizados por cibercriminales, como la **ingeniería social**, el **phishing**, los **ataques de red** y las amenazas basadas en **archivos maliciosos**. El objetivo de la sala es ayudar a identificar cómo funcionan estas técnicas y qué medidas tomar para protegernos, tanto a nivel personal como organizacional.

2. Sala

2.1. Tarea 1 - Introducción

Entramos en contexto para el aprendizaje sobre técnicas comunes utilizadas por atacantes en línea. Esta tarea destaca la importancia de la conciencia en seguridad cibernética y la comprensión de las amenazas digitales para protegerse eficazmente.

Pregunta: Let's get started!
Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Ingeniería Social

Nos introducimos en el concepto de ingeniería social como una técnica de ataque que se centra en manipular a las personas para obtener información confidencial, en lugar de explotar vulnerabilidades técnicas.

La tarea destaca la importancia de la concienciación y la educación en seguridad para prevenir estos ataques. Se presentan ejemplos reales, como el caso del **malware Stuxnet**, que fue diseñado para sabotear el programa nuclear de Irán, demostrando cómo la ingeniería social puede ser parte de ataques cibernéticos complejos.

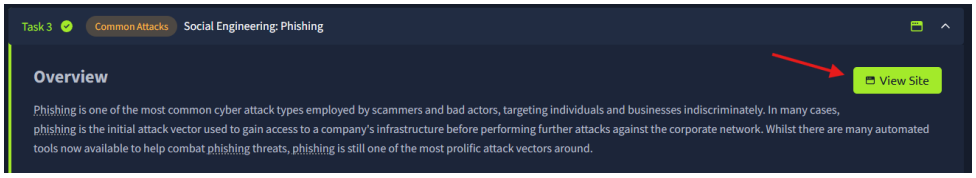
Pregunta: Read the task information and watch the attached videos
Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

Pregunta: What was the original target of Stuxnet?
Respuesta: **The Iran Nuclear Programme**

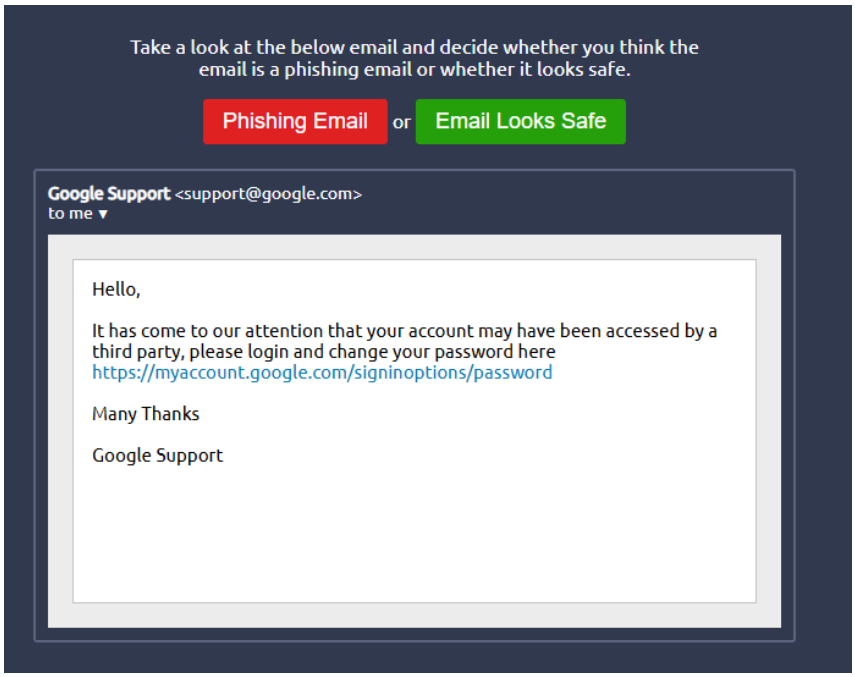
2.3. Tarea 3 - Ingeniería Social: Phishing

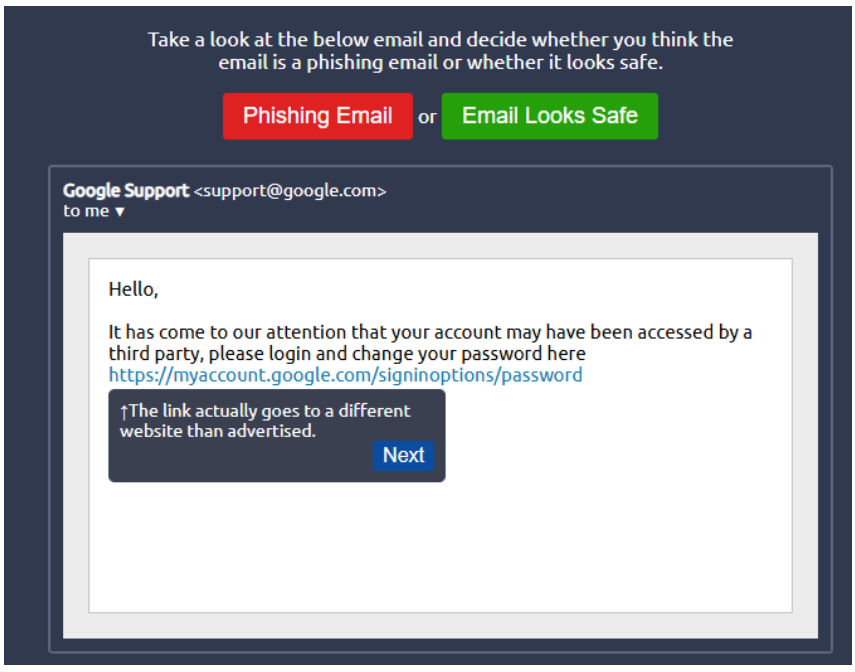
Aquí nos centramos en el análisis y detección de correos electrónicos de phishing, una técnica común de ingeniería social utilizada por atacantes para obtener información confidencial.

Para completar esta tarea debemos realizar un ejercicio, para comenzar a resolverlo debemos desplegar el sitio estático haciendo clic en **View Site** que se encuentra en la zona superior.

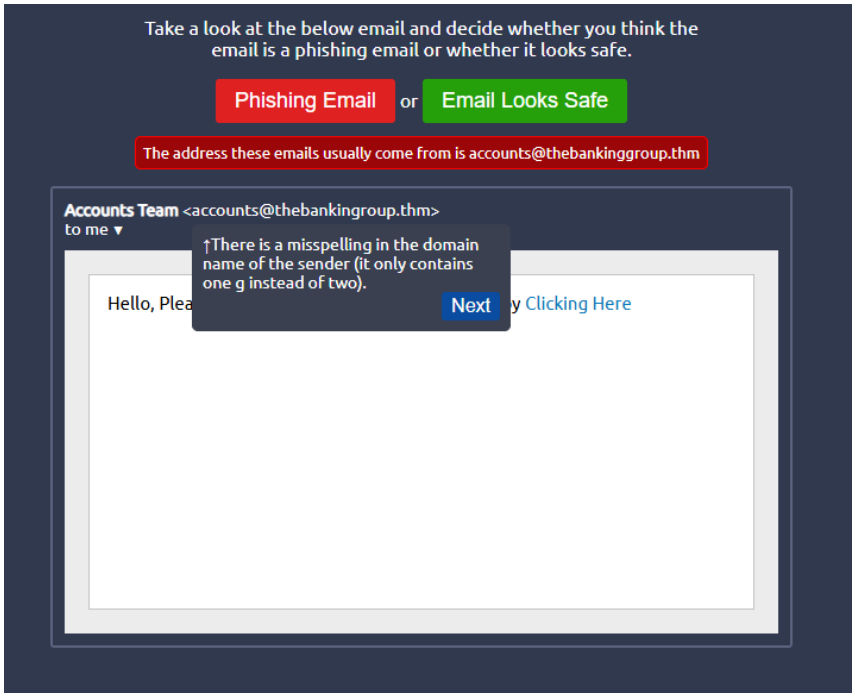


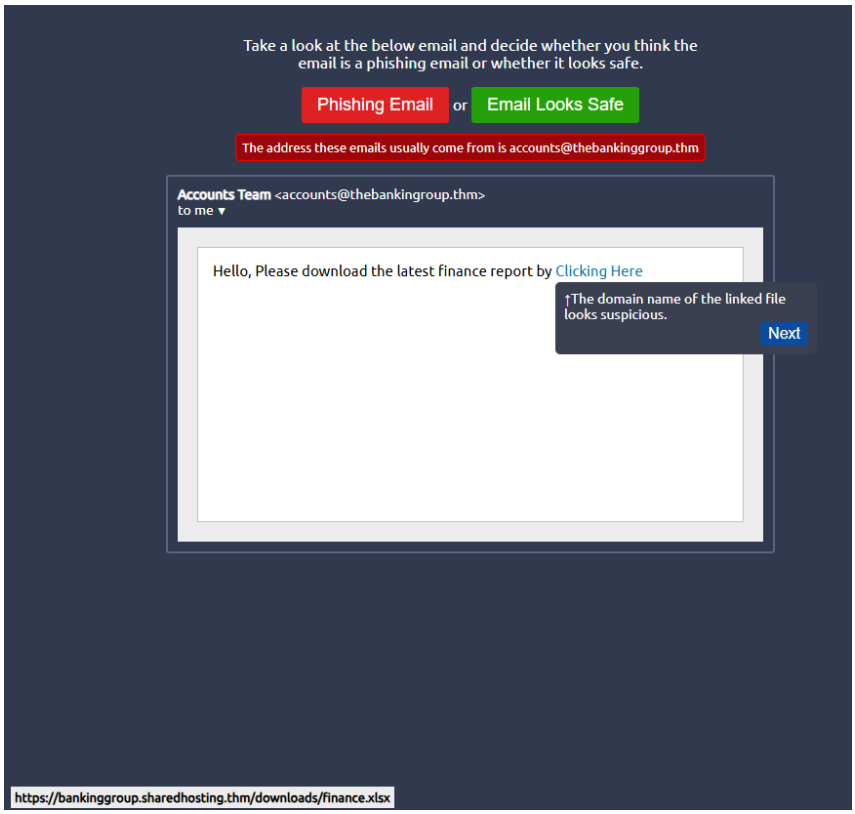
Una vez desplegado el sitio empezamos a responder correctamente las preguntas identificando cuales son ataques de phishing y cuales no.



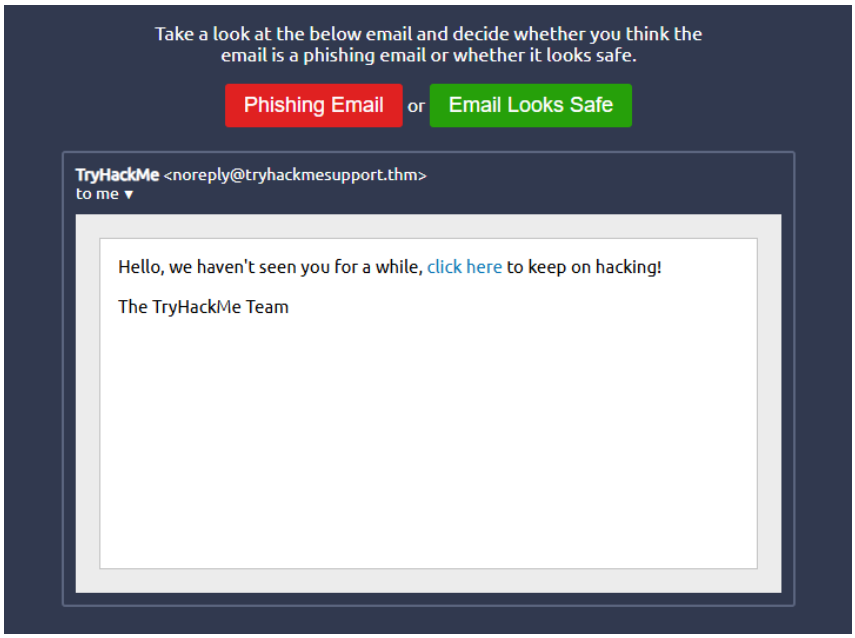


Respuesta: **Phishing Email**

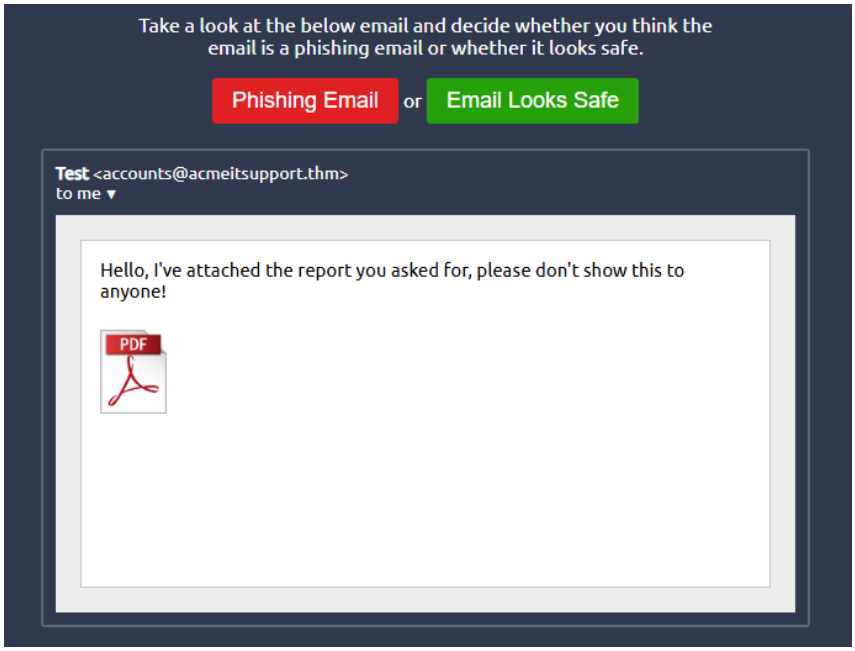


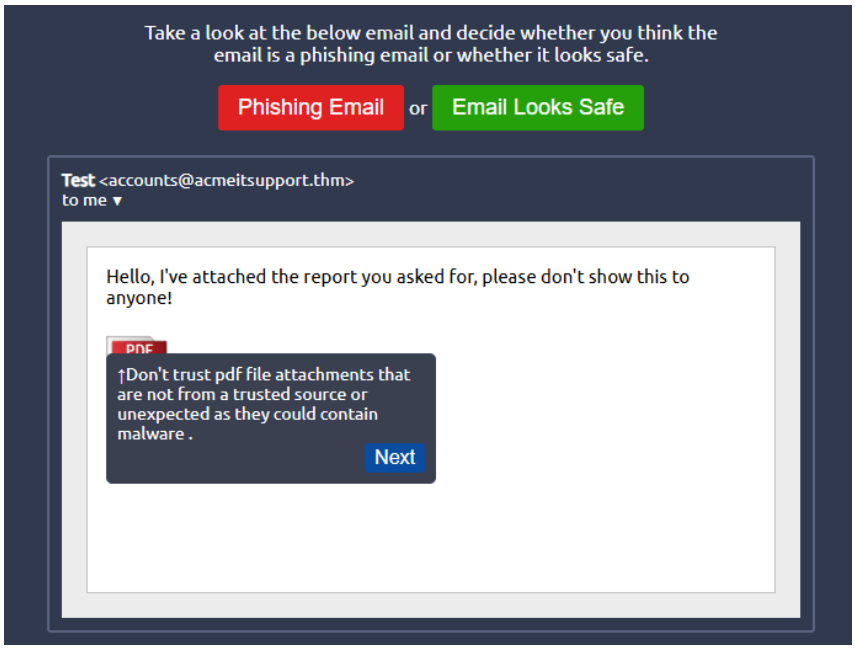


Respuesta: **Phishing Email**



Respuesta: **Email Looks Safe**





Respuesta: **Phishing Email**

Una vez que completamos este ejercicio nos proporcionara la flag para completar la tarea.

Respuesta: THM{I_CAUGHT_ALL_THE_PHISH}

2.4. Tarea 4 - Malware y Ransomware

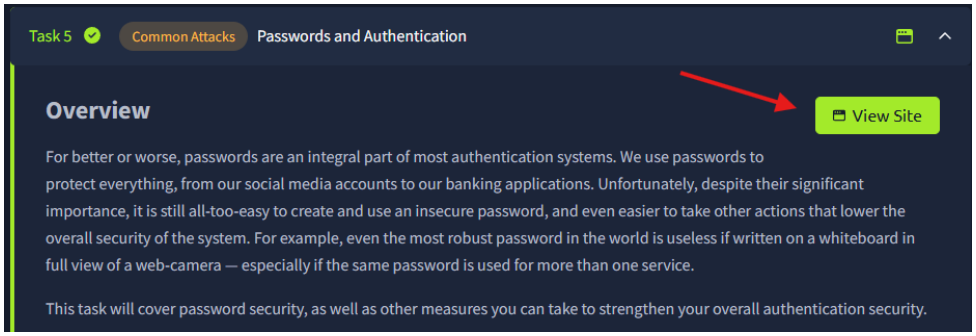
En esta tarea vamos a enfocarnos en comprender cómo el software malicioso puede comprometer sistemas y datos. Aquí se destaca el caso del ransomware **WannaCry**, que en mayo de 2017 afectó a más de 200,000 computadoras en más de 150 países y exigía un rescate en Bitcoin para desbloquear los archivos cifrados.

Pregunta: What currency did the Wannacry attackers request payment in?
Respuesta: Bitcoin

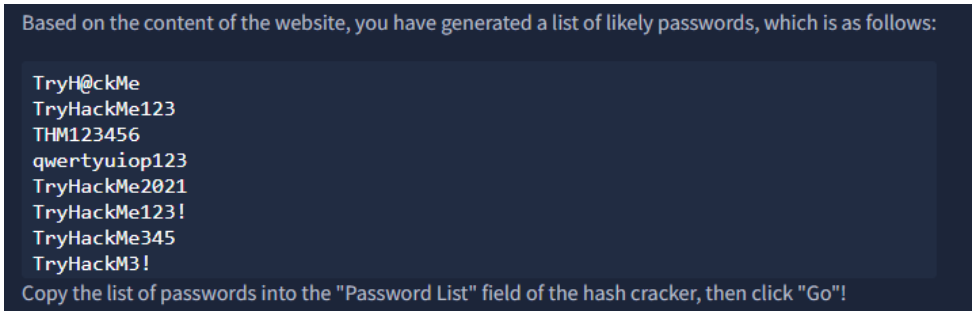
2.5. Tarea 5 - Contraseñas y autenticación

Aprenderemos en esta tarea las vulnerabilidades asociadas al uso de contraseñas débiles y la importancia de implementar prácticas de autenticación seguras. Para completar la tarea se debe realizar un ejercicio práctico en el cualse utiliza una herramienta interactiva de fuerza bruta para descifrar una contraseña a partir de su hash se utiliza una herramienta interactiva de fuerza bruta para descifrar una contraseña a partir de su hash.

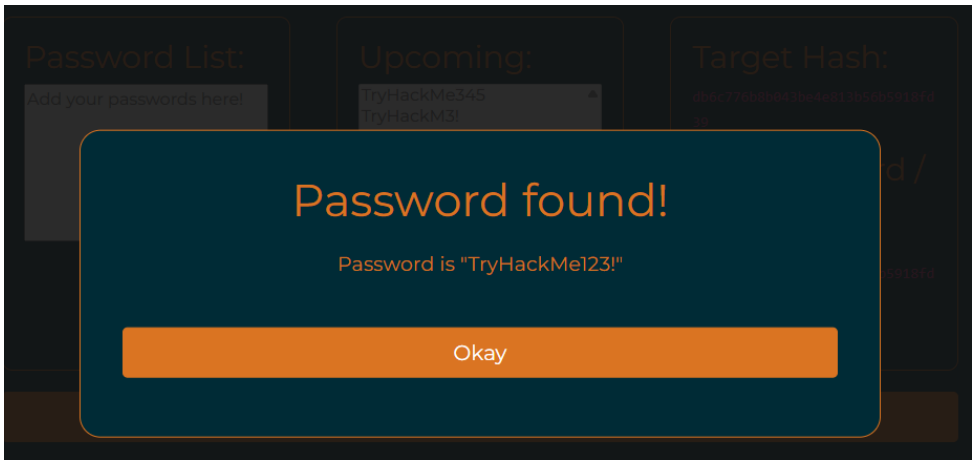
Para comenzar a utilizar la herramienta debemos desplegar el sitio estático haciendo clic en **View Site** que se encuentra en la zona superior.



Una vez se despliega el sitio debemos copiar la serie de contraseñas que nos proporciona TryHackMe en la tarea y pegarlas en el **Password List**.



Después procederemos a darle a **Go!** y obtendremos la contraseña de respuesta.



Respuesta: TryHackMe123!

2.6. Tarea 6 - Autenticación multifactor y administradores de contraseñas

Aprenderemos cómo la autenticación **multifactor (MFA)** añade una capa extra de seguridad al requerir un segundo factor (como una app de autenticación) además de la contraseña. Se recomienda usar aplicaciones en lugar de SMS, ya que son más seguras. También se destacan los administradores de contraseñas, herramientas que permiten generar y guardar contraseñas fuertes y únicas para cada cuenta.

Pregunta: Where you have the option, which should you use as a second authentication factor between SMS based TOTPs or Authenticator App based TOTPs (SMS or App)?

Respuesta: App

2.7. Tarea 7 - Seguridad de la red pública

Esta tarea aborda los riesgos asociados al uso de redes Wi-Fi públicas y cómo protegerse al conectarse a ellas. Algunas medidas de protección que se mencionan son:

- **Utilizar un VPN**
- **No conectarse a redes no confiables**
- **Evitar acceder a información sensible**

Pregunta: The interactive content for this task demonstrates what can happen if information is sent over a potentially unsafe network with various types of encryption (or lack thereof).

Respuesta: No requiere respuesta (Hacemos clic en Submit).

2.8. Tarea 8 - Copias de seguridad

Aprenderemos sobre Copias de Seguridad donde resalta la importancia de realizar respaldos regulares para proteger tus datos contra pérdidas accidentales, ataques de ransomware u otros incidentes.

Algunas recomendaciones claves en esta tarea son:

- **Cantidad mínima de copias de seguridad actualizadas: 3**
- **Número mínimo que deben almacenarse en una ubicación diferente: 1**

Una vez que aprendimos sobre las copias de seguridad podemos pasar a responder las siguientes preguntas.

Pregnta: What is the minimum number of up-to-date backups you should make?
Respusta: 3

Pregnta: Of these, how many (at minimum) should be stored in another location?
Respusta: 1

2.9. Tarea 9 - Actualizaciones y parches

En esta tarea veremos la importancia de mantener los sistemas actualizados para protegerse contra vulnerabilidades conocidas.

También se destaca el caso del exploit **EternalBlue**, que aprovechó una vulnerabilidad en el protocolo SMB de Windows. A pesar de que Microsoft lanzó el parche **MS17-010** para corregir esta falla, muchos sistemas no actualizados fueron afectados por el ransomware **WannaCry**.

Respuesta: No requiere respuesta (Hacemos clic en Submit).

2.10. Tarea 10 - Conclusión

En esta tarea se resume los conocimientos adquiridos sobre ataques comunes y las mejores prácticas para prevenirlos. Enfatiza la importancia de la concienciación en ciberseguridad y la aplicación de medidas proactivas para protegerse en el entorno digital.

Respuesta: No requiere respuesta (Hacemos clic en Submit).

3. Conclusión sobre la Sala

Esta sala nos enseñó los métodos más comunes que utilizan los atacantes para comprometer sistemas y usuarios, como la ingeniería social, el phishing, el malware, y el uso de contraseñas débiles. También aprendimos buenas prácticas de defensa como usar autenticación multifactor, administradores de contraseñas, VPNs, copias de seguridad y mantener los sistemas actualizados.