

Actividad Fundamental 4

Redes y Seguridad: Sistemas Distribuidos

Hernández González Grecia Damiani

1998444

Lucio Mireles Daniel

2004268

Arzola Gutierrez Gilberto Alejandro

2001061

Durán Ramírez Ana Laura

1969975

Frias Salinas Isaac Alessandro

2005483

Neaves Cisneros Karen Dennis

1946929

Rodriguez Escamilla Bryan Eduardo

1998529



INDICE

1 INTRODUCCION

2 SEGURIDAD

3 TIPOS DE AMENAZAS

4 TIPOS DE VIRUS

5 TIPOS DE INTRUSOS

6 TIPOS DE
AUTENTIFICADORES

7 NIVELES DE SEGURIDAD

8 ANALISIS DE PROBLEMAS Y
SOLUCIONES

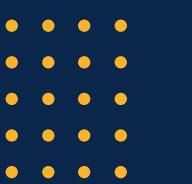
9 CONCLUSION

10 BIBLIOGRAFIAS

Introducción

Las mayoría de los usuarios que cuentan con un computador siempre tratan de proteger los datos que esta guarda y esto es logrado a través de métodos de seguridad que estos métodos varían dependiendo del tipo de protección requerida por el usuario, ya sea realizando un respaldo de los datos o creando contraseñas para restringir quien puede acceder a ellos.

Las cuestiones relacionadas con la seguridad de los sistemas operativos han cambiado de manera radical en las últimas dos décadas, esto debido a que en el paso de los años han existido mas amenazas relacionadas a los virus y malware que puede afectar al computador.



SEGURIDAD

La seguridad en el ámbito del software es esencial para proteger aplicaciones, sistemas y datos digitales contra amenazas cibernéticas y garantizar la integridad, confidencialidad y disponibilidad de la información. Esta área se enfoca en identificar y mitigar riesgos relacionados con el desarrollo, uso y mantenimiento del software.



Tipos de Autenticación

Mediante el uso de contraseñas

Requerir que el usuario escriba un nombre de inicio de sesión y una contraseña.

Mediante el uso de un objeto físico

Comprobar algún objeto físico que tengan, en vez de algo que sepan.

Mediante biométrica

Mide las características físicas del usuario que son difíciles de falsificar.

Autenticación mediante el uso de contraseñas

La autenticación más comúnmente utilizada implica que los usuarios ingresen un nombre de usuario y una contraseña. La contraseña se almacena en un archivo de contraseñas y se compara con la contraseña proporcionada por el usuario. Para garantizar la seguridad, las contraseñas deben mantenerse en secreto, y en sistemas como Windows o UNIX, no se muestran mientras se escriben.



Sin embargo, las contraseñas a menudo son vulnerables, ya que las personas tienden a elegir contraseñas débiles y predecibles. Los ataques de fuerza bruta, donde un atacante intenta adivinar las contraseñas probando muchas combinaciones, son una amenaza común. El uso de contraseñas de un solo uso o sistemas de autenticación más avanzados puede aumentar la seguridad.



Autenticación mediante el uso de un objeto físico



El segundo método de autenticación se basa en el uso de objetos físicos, como tarjetas de plástico, para verificar la identidad del usuario. Estas tarjetas pueden contener información en una tira magnética o un chip. Las tarjetas inteligentes, con un pequeño circuito integrado, son especialmente seguras y versátiles, utilizadas en diversas aplicaciones como compras en tiendas, teléfonos de pago y parquímetros. Además, las tarjetas inteligentes permiten la autenticación segura en línea, eliminando la necesidad de contraseñas.



Se pueden utilizar varios esquemas de autenticación, como el reto-respuesta, donde la tarjeta inteligente y el servidor intercambian información para verificar la identidad del usuario. Sin embargo, estas tarjetas pueden ser vulnerables a ataques de canal lateral, como el análisis de energía, y es posible actualizar los protocolos de autenticación en ellas a medida que surgen nuevas amenazas.

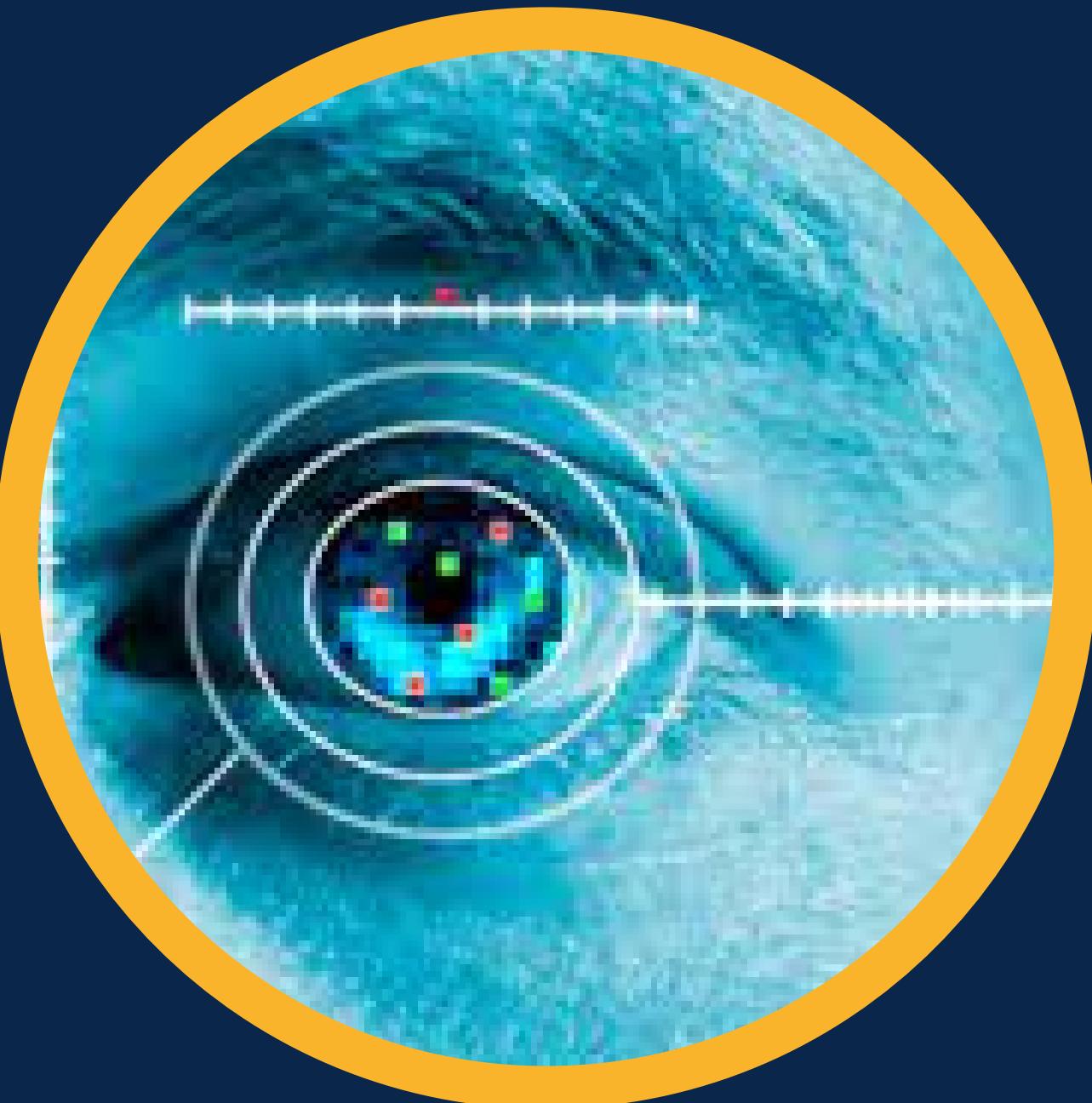
Autenticación mediante biométrica

El tercer método de autenticación se basa en características biométricas difíciles de falsificar, como huellas dactilares o el análisis del iris, que se miden durante la inscripción y se almacenan para verificar la identidad del usuario durante la identificación. Aunque existen técnicas como la longitud de los dedos, firmas y análisis de voz, algunos sistemas biométricos pueden ser vulnerables a la suplantación.

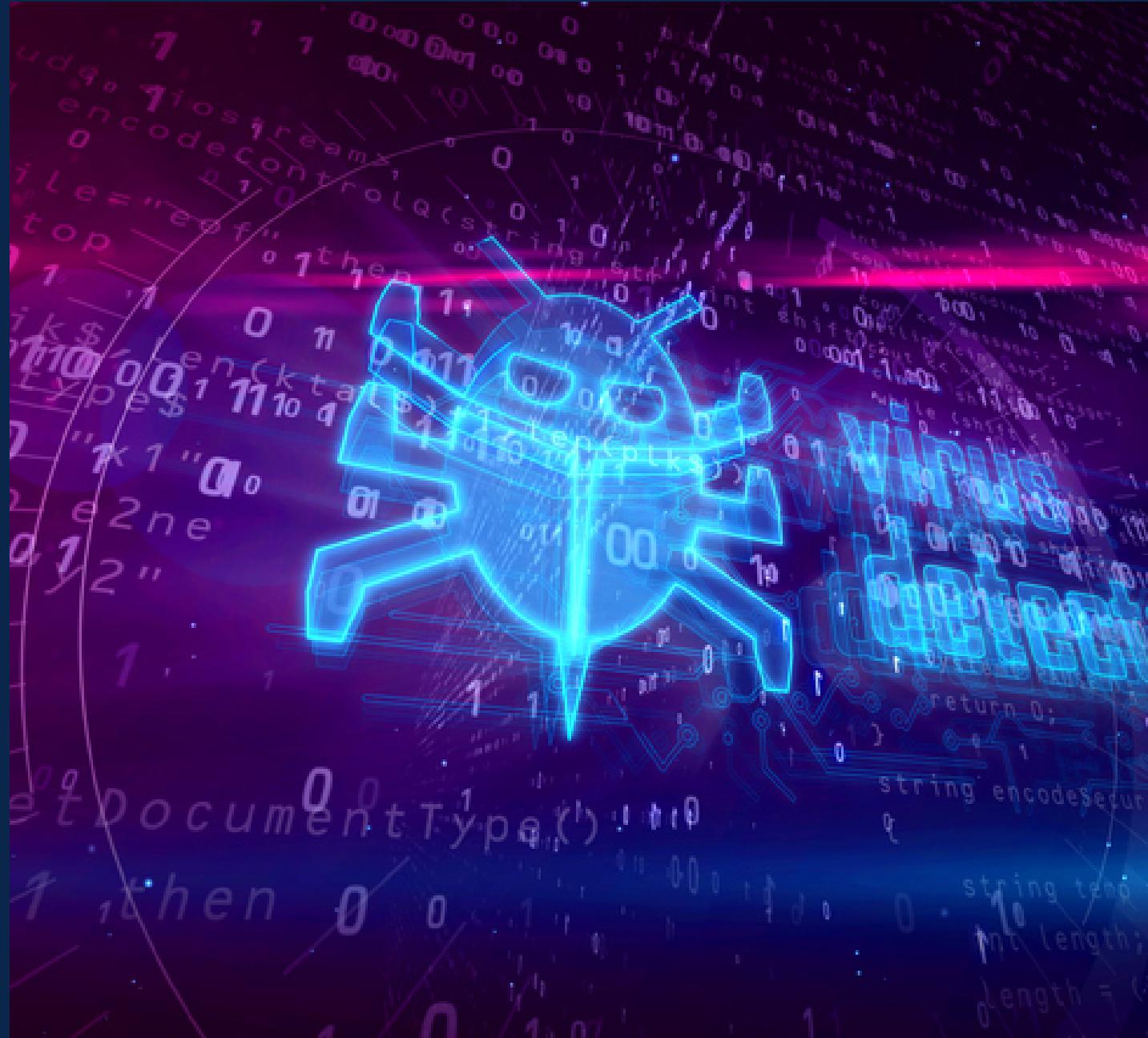


Autenticación mediante biométrica

La aceptación psicológica por parte de los usuarios es crucial, ya que incluso sistemas altamente seguros pueden no ser aceptados si resultan intrusivos o incómodos.



Tipos de amenazas



Existen diversos tipos de amenazas en el ámbito de la seguridad del software y la ciberseguridad. Estas amenazas pueden clasificarse en varias categorías según su origen y naturaleza. Entre ellas existen:

- Malware
- Ataques de Ingeniería Social
- Ataques de Fuerza Bruta
- Ataques de Inyección
- Ataques de Denegación de Servicio (DDoS)
- Ataques a la Red
- Ataques Zero-Day
- Ataques de Man-in-the-Middle (MitM)
- Ataques de Ransomware

Tipos de Autenticación

Mediante el uso de contraseñas

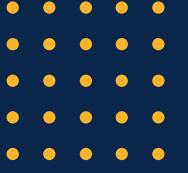
Requerir que el usuario escriba un nombre de inicio de sesión y una contraseña.

Mediante el uso de un objeto físico

Comprobar algún objeto físico que tengan, en vez de algo que sepan.

Mediante biométrica

Mide las características físicas del usuario que son difíciles de falsificar.



Tipos de Virus

Los virus informáticos son un software que se instala en un dispositivo con el fin de intervenir en el funcionamiento del mismo. Es necesaria la intervención de parte de un usuario para que el sistema sea infectado por un virus

Gusano

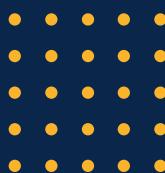
Troyano

Ransomware

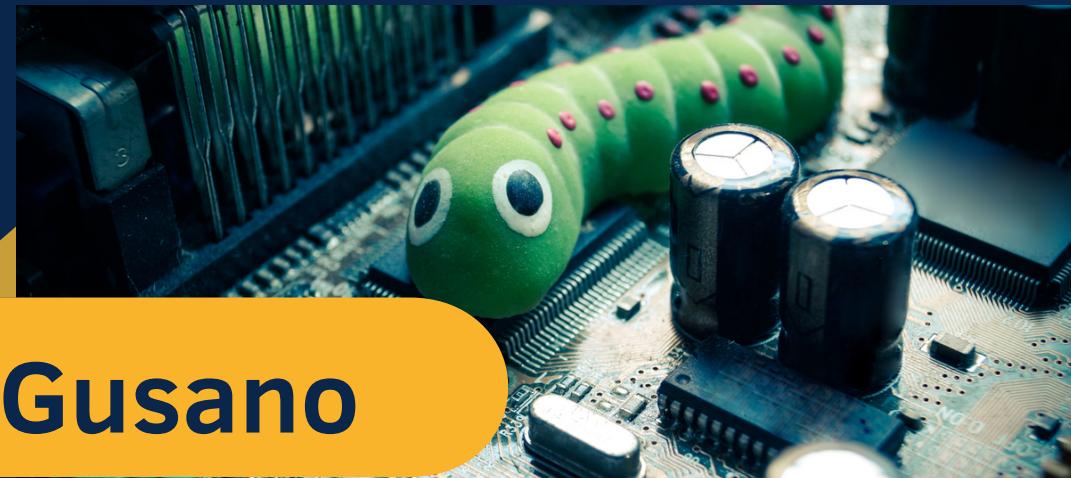
Spyware

Spyware

Troyano



VIRUS



Gusano

Es uno de los malware mas comunes , ya que no requieren de la intervención del usuario ni de la modificación de algún archivo para poder infectar un equipo

Su objetivo es el de replicarse e infectar el mayor numero de dispositivos posibles



Ransomware

Este se ha convertido en el mas temido en la actualidad. Consiste en encriptar toda la información de la empresa, impidiendo el acceso a los datos y los sistemas y se pide un rescate para poder liberar la información



Troyanos

Son programas que se instalan en un equipo y pasan desapercibidos para el usuario
Su objetivo es el de ir abriendo puertas para que otro tipo de malware se instale



Adware

Se trata de un software que secuestra el navegador u otras partes del sistema para inundarlo con anuncios no deseado
Suelen tener características y comportamientos diferentes

VIRUS

Keyloggers

Se instalan a través de troyanos y se encargan de robar datos de acceso a plataformas web, sitios bancarios y similares



Spyware

Es un malware que intenta mantenerse oculto mientras se registra información en secreto
Puede supervisar y copiar todo lo que escribe, carga, descarga y almacena



Tipos de intrusos

En este apartado hablaremos de 2 tipos diferentes de intrusos en la red, estos son:

HACKER

CRACKERS



HACKERS

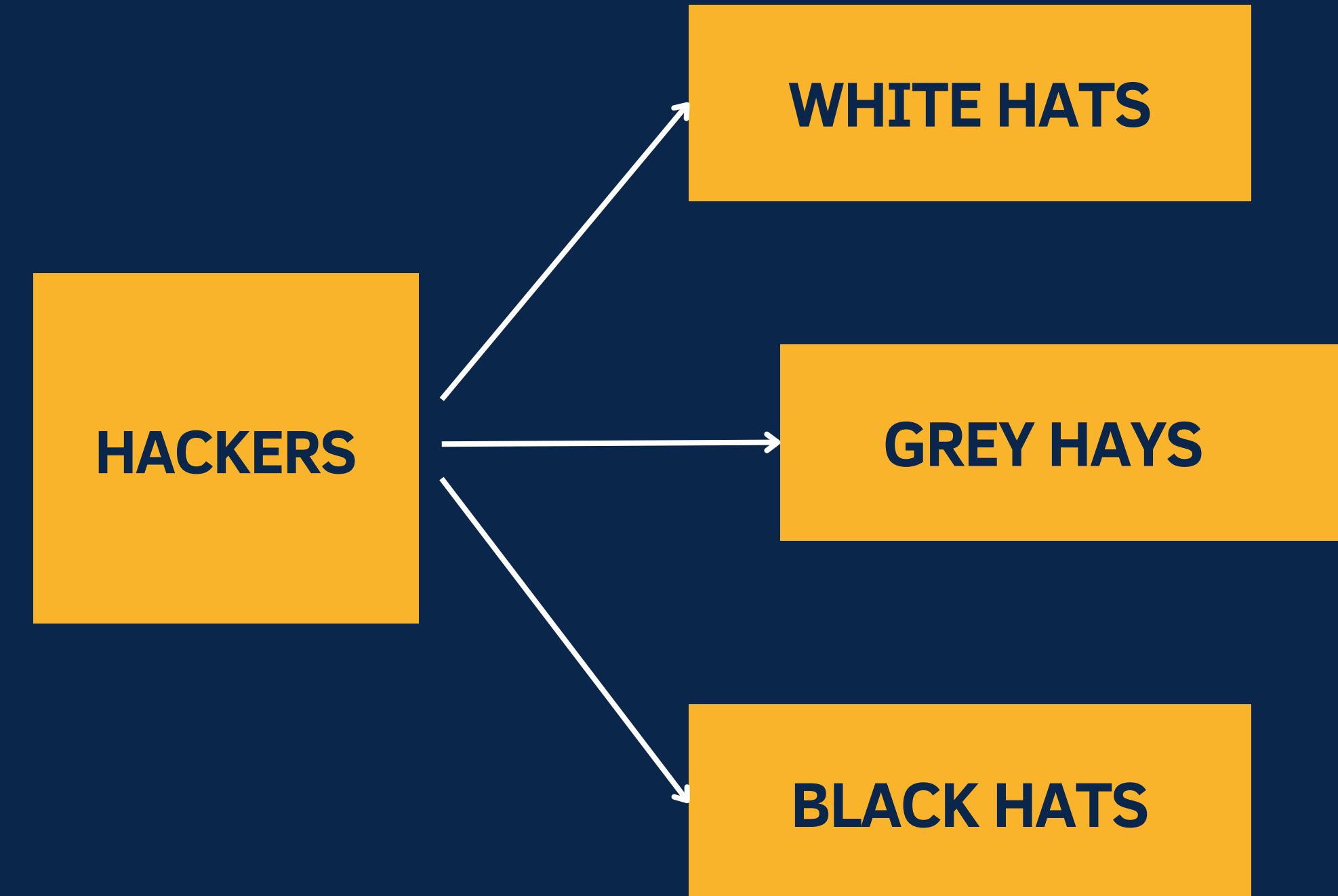
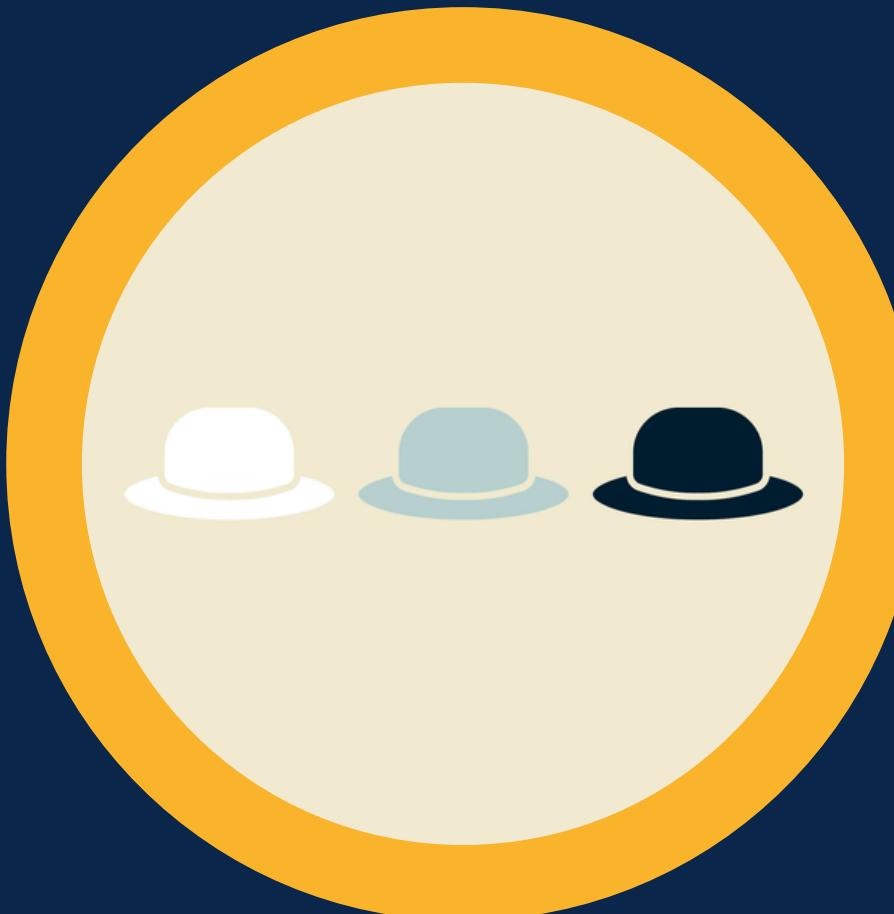
Destaca por su excelencia en programación y electrónica, un conocimiento avanzado en ordenadores y redes informáticas. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Buscan y descubren las debilidades de una computadora o red informática.





HACKERS

Una vez teniendo el conocimiento acerca de lo que es un hacker, de este concepto derivan 3 nuevas variantes o tipos de hackers que existen.



WHITE HATS



A los “WHITE HATS” también se les llama hackers éticos. Estos expertos en informática utilizan sus conocimientos para buscar vulnerabilidades y hacer tests de penetración, para estudiar y corregir fallos de seguridad y mejorar los sistemas en materia de seguridad. Alertan de un fallo en algún programa comercial, comunicándoselo al fabricante. Pueden formar parte de un equipo de seguridad empresarial o gubernamental.

GREY HATS

Suelen utilizar las mismas técnicas que los sombreros negros para encontrar vulnerabilidades y luego venderlas a quién este dispuesto a pagar por ellas. Su clientela abarca gobiernos, servicios militares y otros hackers. Además, se pueden presentar como expertos en seguridad para resolver los fallos encontrados. Su enfoque suele estar en el lucro más que en perjudicar a las empresas de manera directa.



BLACK HATS



Utilizan sus conocimientos para realizar actividades ilegales, normalmente con animo de lucro y para aumentar su reputación. Suelen ser creadores de tipo de malware.

CRACKERS

Ser un cracker es saber romper algo, en este caso sistemas y software. Tienen un conocimiento profundo de programación y electrónica. Siempre encuentran el modo de romper una protección y estas roturas se suelen filtrar o difundir en la red para el conocimiento de los demás.

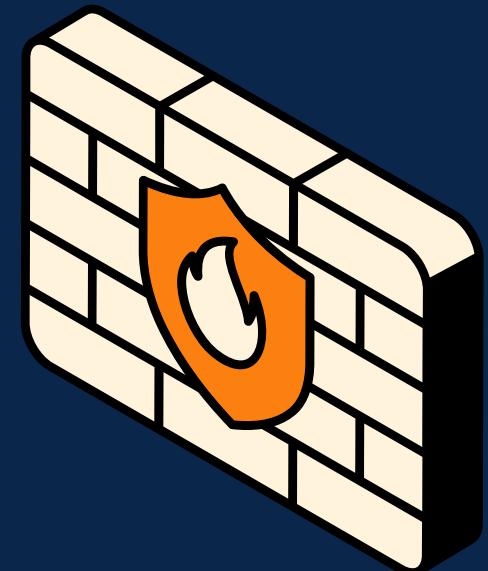


Niveles de seguridad

Para la Red:

- **Firewalls**

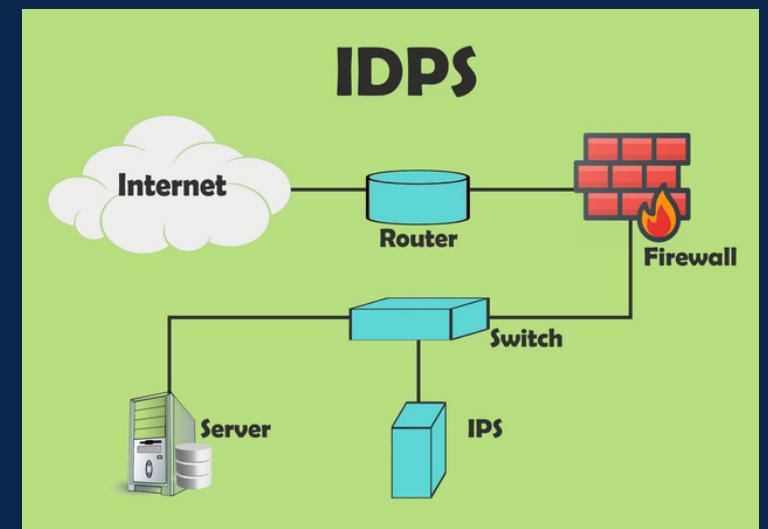
Son la medida de seguridad tradicional que se han añadido a las redes y los sistemas finales, donde el tráfico se divide en deseado y el no deseado

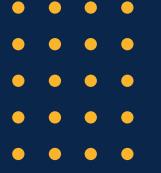


- **Sistema de detección y prevención de intrusiones**

Un IDPS supervisa la red en busca de actividad maliciosa, mediante la realización de informes y la respuesta a los incidentes de seguridad de red y a las posibles amenazas

Este se centra en encontrar el tráfico que provenga de un hacker o de otros agentes





- **Red privada virtual (VPN)**

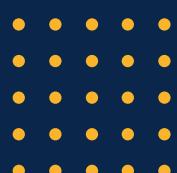
Protege la confidencialidad de los datos cuando atraviesan su red. El núcleo de una VPN es cifrado, aunque también utiliza la autenticación.

Existen tres opciones de cifrado

1. **IPSec**: Se puede utilizar en cualquier situación, ya que funciona en la capa 3 del modelo de interconexión de sistemas abiertos

2. **SSL/TLS** :Proporciona una opción de cifrado para las VPN, pero también para cualquier conexión con base en la web

3. **SSH** se utiliza principalmente para las conexiones remotas de un equipo a otro. Lo han utilizado los administradores de red para conectarse a servidores, enrutadores y conmutadores con fines administrativos



Para la Empresas:

- Seguridad interna

Establece medidas de seguridad a nivel local dentro de la misma red para proteger los sistemas ante un atacante local e incluso ante las acciones, voluntarias o involuntarias, de los usuarios

- Seguridad Externa

Integra elementos defensivos a todos los sistemas informáticos de la empresa para protegerlos frente a amenazas externas, procedentes mayormente de internet

- Seguridad perimetral

Se define como los elementos y dispositivos electrónicos para la protección física de los sistemas



Analisis de problemas y soluciones

Existen varias razones que son capaces de incrementar la inseguridad de los sistemas. Estos serian la compartición. La complejidad del sistema. Los puntos de ataque. Todo esto conlleva a dejar espacios para que los hackers puedan entrometerse en los ordenadores y en los datos.



Dichos problemas llevan a una privacidad difícil de controlar. Se pueden llegar a corromper las transmisiones y la integridad de los datos peligra. Normalmente las causas de dichas inseguridades son os hackers y los virus informáticos.



Maneras de resguardar y proteger los sistemas distribuidos

Criptografía

Cifra y descifra información mediante la utilización de distintas técnicas que hacen posible el intercambio de los mensajes de forma segura.

Sistema de detección de intrusos (SDI)

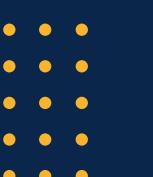
Basan su funcionamiento en recolectar y analizar información de varias fuentes para determinar la existencia de un peligro.

Firewall

Combina varios componentes, los programas, los dispositivos físicos y las actividades de administración.

Conclusión

La seguridad es una parte fundamental de un sistema, ya que esta es la encargada de la protección de los datos de un usuario que como vimos en la presentación esta puede ser de diferentes escalas, desde un ordenador personal hasta los servidores de una empresa, por lo que se han creado todo tipo de mediciones y protocolos de seguridad para preservar los datos de un usuario ante las amenazas que intentan irrumpir dentro del sistema y que de esta manera pueda robar o manipular los datos privados almacenados en un sistema, por lo que identificamos el tipo de amenaza con la que nos enfrentamos así como la magnitud de esta, y poder lidiar con ella de manera adecuada y precisa utilizando el protocolo correcto y que no afecte al usuario



Referencias

- Stallings, W. (2006). Sistemas operativos. <https://dl.acm.org/citation.cfm?id=1211881>
- Tanenbaum, A. S. (2004).
- Sistemas operativos modernos. En Prentice-Hall, Inc eBooks.
<http://dl.acm.org/citation.cfm?id=1205752>
- Deucalion. (2022, 11 julio). 10 principales tipos de virus informáticos. Skynet Systems SL.
<https://skynet-sys.es/10-principales-tipos-de-virus-informaticos/>
- J.L. Hennessy, D.A Patterson. Computer Architecture A Quantitative Approach. Cuarta edición. s.l. : Morgan Kauffman, 2007.