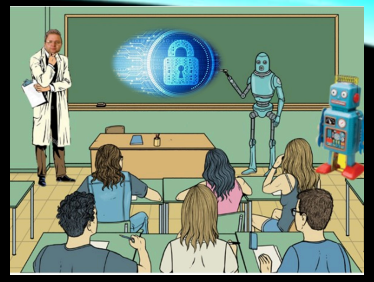
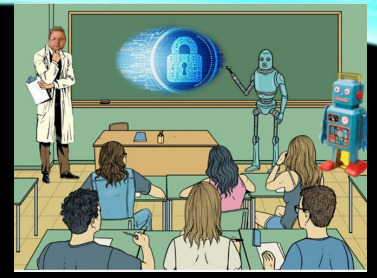


UD 8.2. SEGURIDAD EN LA RED.

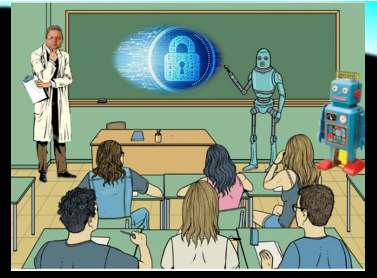
SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN.

1º TECNOLOGIAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.
TIC



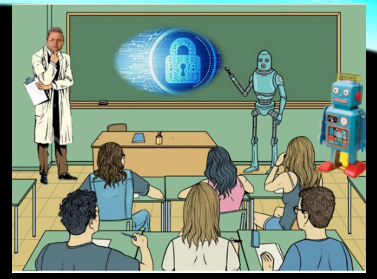
INTRODUCCIÓN

- **Estamos rodeados de virus, bacterias y hongos que producen enfermedades. Pero los seres humanos disponemos de mecanismos de defensa tanto internos, el sistema inmunológico, como externos, las medicinas y las vacunas.**
- Los ordenadores también sufren los ataques de programas, archivos y mensajes que atacan sus sistemas, pero también disponen de mecanismos que les permiten minimizar estos ataques.
- **La administración de la seguridad trata de conseguir la integridad y la protección de los procesos, de los recursos y los datos. Debemos distinguir por tanto entre** seguridad informática **y** seguridad de la información.

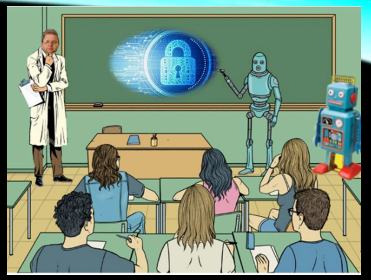


NECESIDADES DE SEGURIDAD

Un ordenador es una herramienta muy potente.
Debemos:
1. Saber utilizarlo.
2. Conocer las herramientas de seguridad disponibles.
3. Aplicar unas normas básicas de seguridad.



1. SEGURIDAD INFORMÁTICA



1. Seguridad Informática

- 1.1. Seguridad física y seguridad lógica
- 1.2 Delitos informáticos y legislación
- 1.3 Malware

LA SEGURIDAD INFORMÁTICA

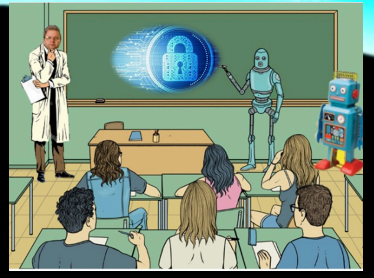
- **Se define como el conjunto de métodos y herramientas destinados a proteger los sistemas computacionales ante cualquier amenaza.**
- **El objetivo principal de la seguridad informática es garantizar que los recursos y la información estén protegidos y para protegerlos son necesarios conseguir los siguientes aspectos**:

1. Integridad.- sólo los usuarios autorizados podrán modificar la información.

2. Confidencialidad.- sólo los usuarios autorizados tendrán acceso a los recursos y a la información que utilicen.

3. Disponibilidad.- la información debe estar disponible cuando se necesite.

4. Irrefutabilidad.- el usuario no puede refutar o negar una operación realizada.

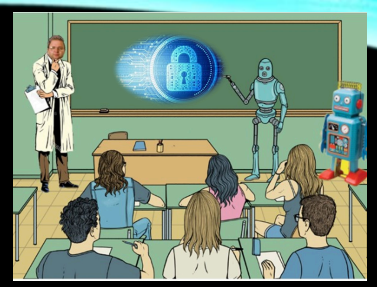


1. Seguridad Informática

1.1. Seguridad física y seguridad lógica

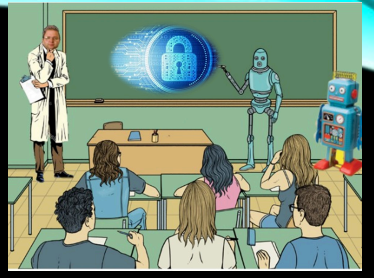
1.2 Delitos informáticos y legislación

1.3 Malware

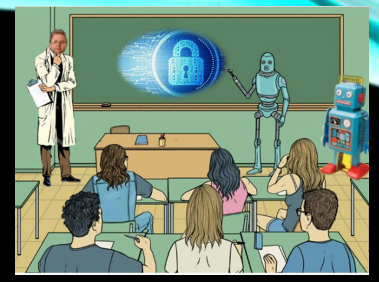


1.1. SEGURIDAD FÍSICA Y LÓGICA

La **seguridad física** de un sistema informático consiste en la aplicación de barreras físicas y procedimientos de control frente a amenazas físicas al hardware.



La **seguridad lógica** de un sistema informático consiste en la aplicación de barreras y procedimientos software que protejan el acceso a los datos y al información contenida en él.



1. Seguridad Informática

1.1. Seguridad física y seguridad lógica

1.2 Delitos informáticos y legislación

1.3 Malware

1.2. DELITOS INFORMÁTICOS Y LEGISLACIÓN

El **delito informático** es aquel que se refiere a actividades ilícitas realizadas por medio de ordenadores o de internet.

Legislación: En España está en vigor la Ley Orgánica de Delitos Informáticos

Vídeo

https://www.antena3.com/noticias/economia/aumentan-los-ciberataques-y-las-amenazas-de-daesh-en-espana_20170208589b81770cf207e09644d592.html

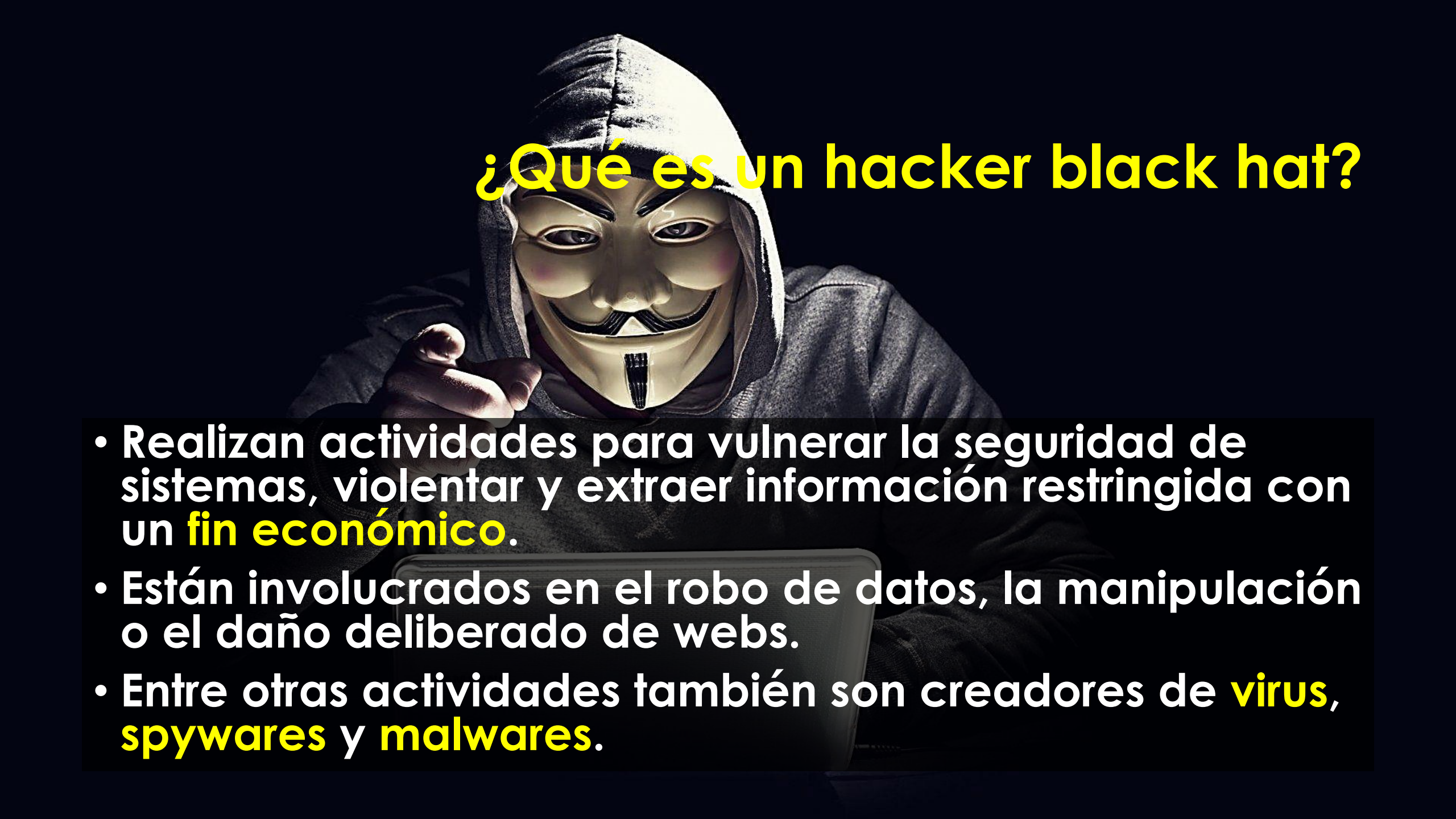
Hablemos en la siguiente diapositiva del HACKER informático.

Hacker

- ¿Qué es un hacker?
- ¿Qué es un hacker black hat?
- ¿Qué es un hacker white hat?
- ¿Qué es un hacker grey hat?

¿Qué es un hacker?

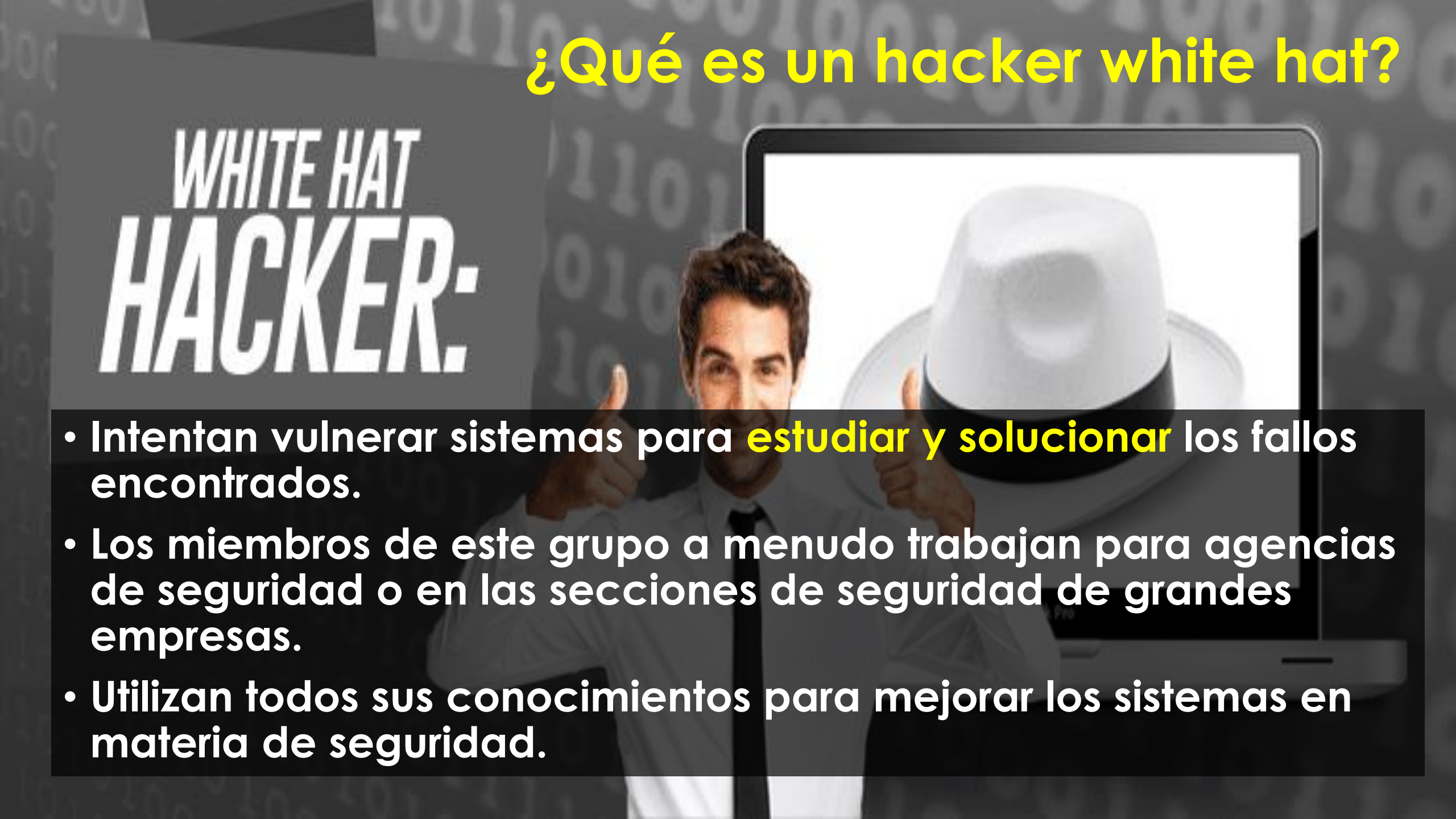
- El término hacker puede tener una **connotación positiva o negativa** dependiendo de la definición.
- En un **sentido negativo**, los hackers son personas o grupos que obtienen ***acceso no autorizado*** a sitios web explotando vulnerabilidades existentes.
- En un **sentido positivo**, los hackers son profesionales de la informática que ***descubren los puntos débiles*** de las aplicaciones informáticas y ayudan a resolverlos.



¿Qué es un hacker black hat?

- Realizan actividades para vulnerar la seguridad de sistemas, violentar y extraer información restringida con un **fin económico**.
- Están involucrados en el robo de datos, la manipulación o el daño deliberado de webs.
- Entre otras actividades también son creadores de **virus**, **spywares** y **malwares**.

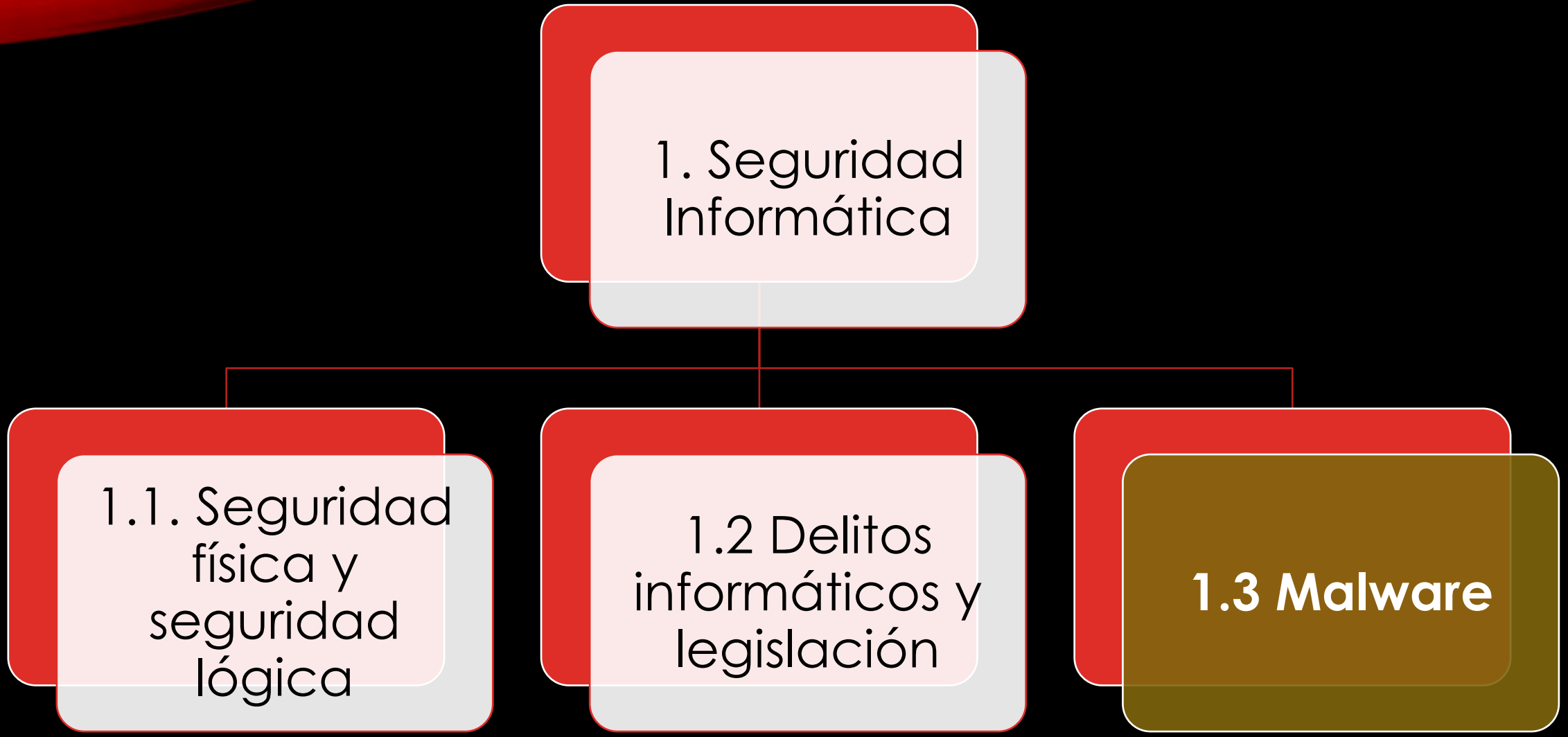
¿Qué es un hacker white hat?



- Intentan vulnerar sistemas para estudiar y solucionar los fallos encontrados.
- Los miembros de este grupo a menudo trabajan para agencias de seguridad o en las secciones de seguridad de grandes empresas.
- Utilizan todos sus conocimientos para mejorar los sistemas en materia de seguridad.

¿Qué es un hacker grey hat?

- En este grupo, no siempre se puede determinar claramente si las acciones son meramente con fines delictivos o si hay un propósito superior detrás de ellas.
- Un buen ejemplo de esto es el grupo Anonymous que atacó el servicio de pago PayPal en 2010, para protestar por el hecho de que PayPal no reenviara los pagos a WikiLeaks. El mismo grupo decidió en noviembre de 2015 luchar contra el Estado islámico de manera online. Anonymous en sí mismo no tiene una estructura fija. Los miembros de este grupo de hackers colaboran de forma descentralizada.
- Son un híbrido entre un hacker White y otro Black.


1. Seguridad Informática
1.1. Seguridad física y seguridad lógica
1.2 Delitos informáticos y legislación
1.3 Malware

1.3. MALWARE

MALWARE es cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

- **Tipos de MALWARE:**

a) Virus.
b) Gusano.
c) Troyano.
d) Bomba lógica.
e) Adware.
f) Spyware.
g) Malvertising.
h) Ransomware.
i) Keylogger.
j) Stealer.
k) Rogueware.
l) Decoy o señuelo.
m) Dialer.
n) Secuestrador de navegador.
o) Wiper.
p) Criptominado malicioso o Cryptojacking.
q) Web skimming.
r) Apropiador de formularios.

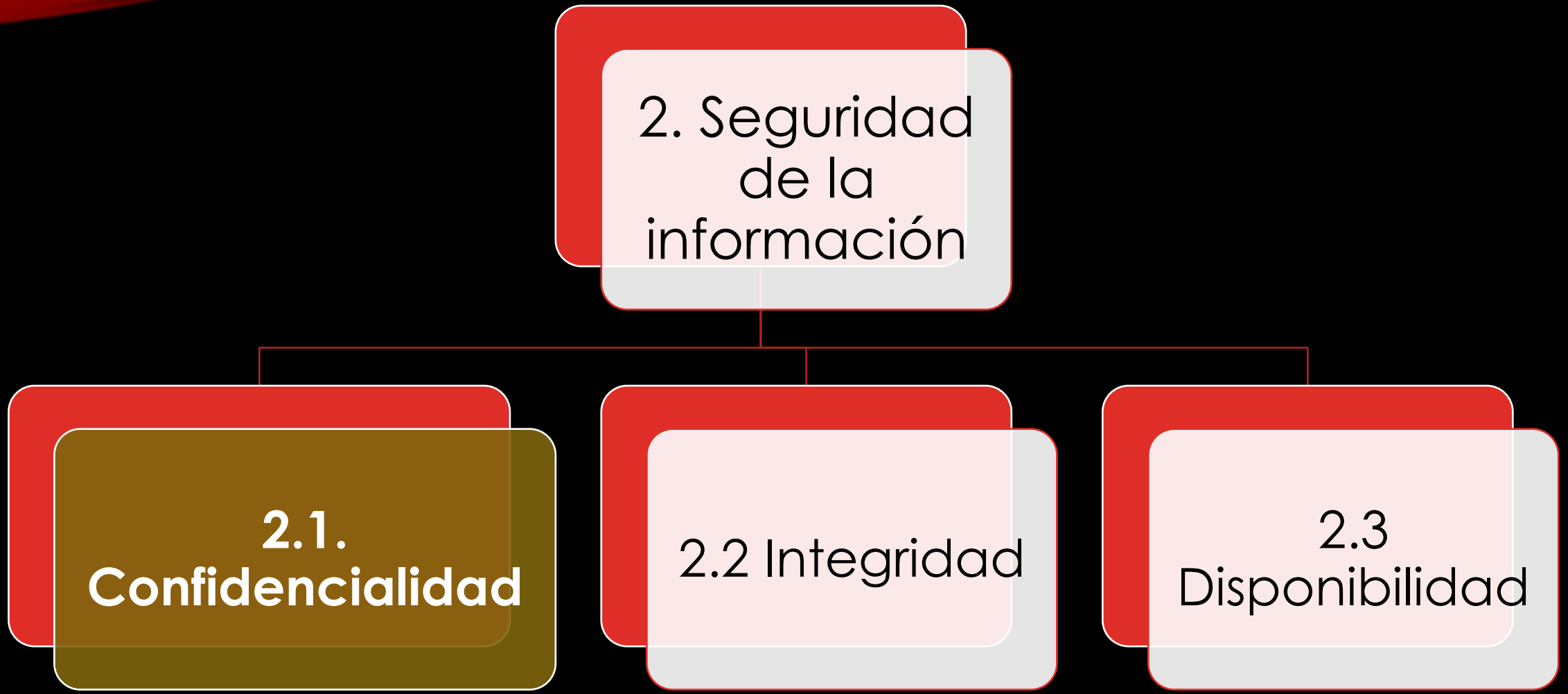
2. SEGURIDAD DE LA INFORMACIÓN

2. Seguridad de la información

- 2.1. Confidencialidad
- 2.2 Integridad
- 2.3 Disponibilidad

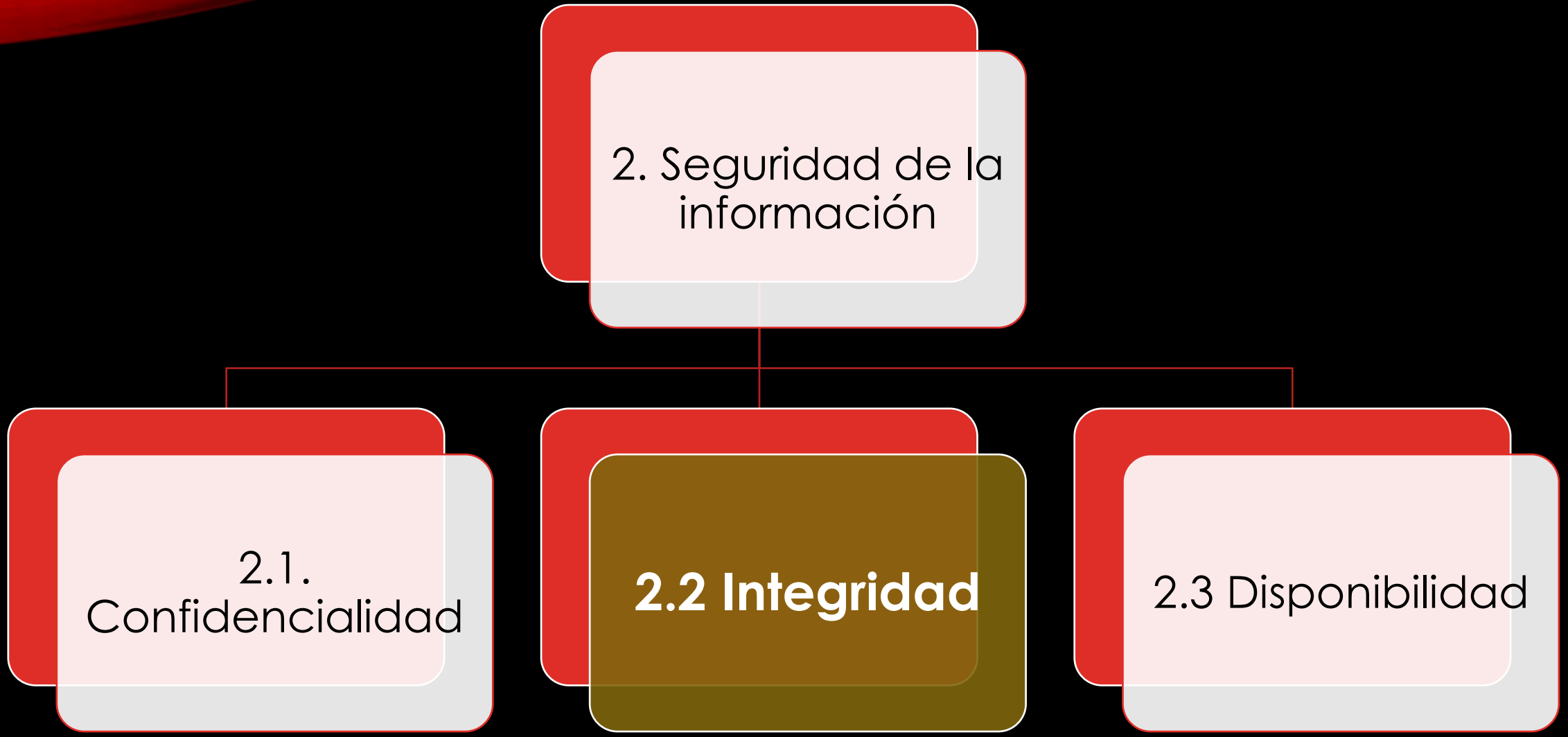
SEGURIDAD DE LA INFORMACIÓN

- Son las medidas tanto proactivas (aquellas que se toman para prevenir un problema) como reactivas (aquellas que se toman cuando el daño se produce, para minimizar sus efectos) que se toman por parte de las personas, organizaciones o sistemas tecnológicos.
- Su objetivo es resguardar y proteger la información buscando siempre mantener la confidencialidad, la disponibilidad e integridad de la misma.


2. Seguridad de la información
2.1. Confidencialidad
2.2 Integridad
2.3 Disponibilidad

2.1. CONFIDENCIALIDAD

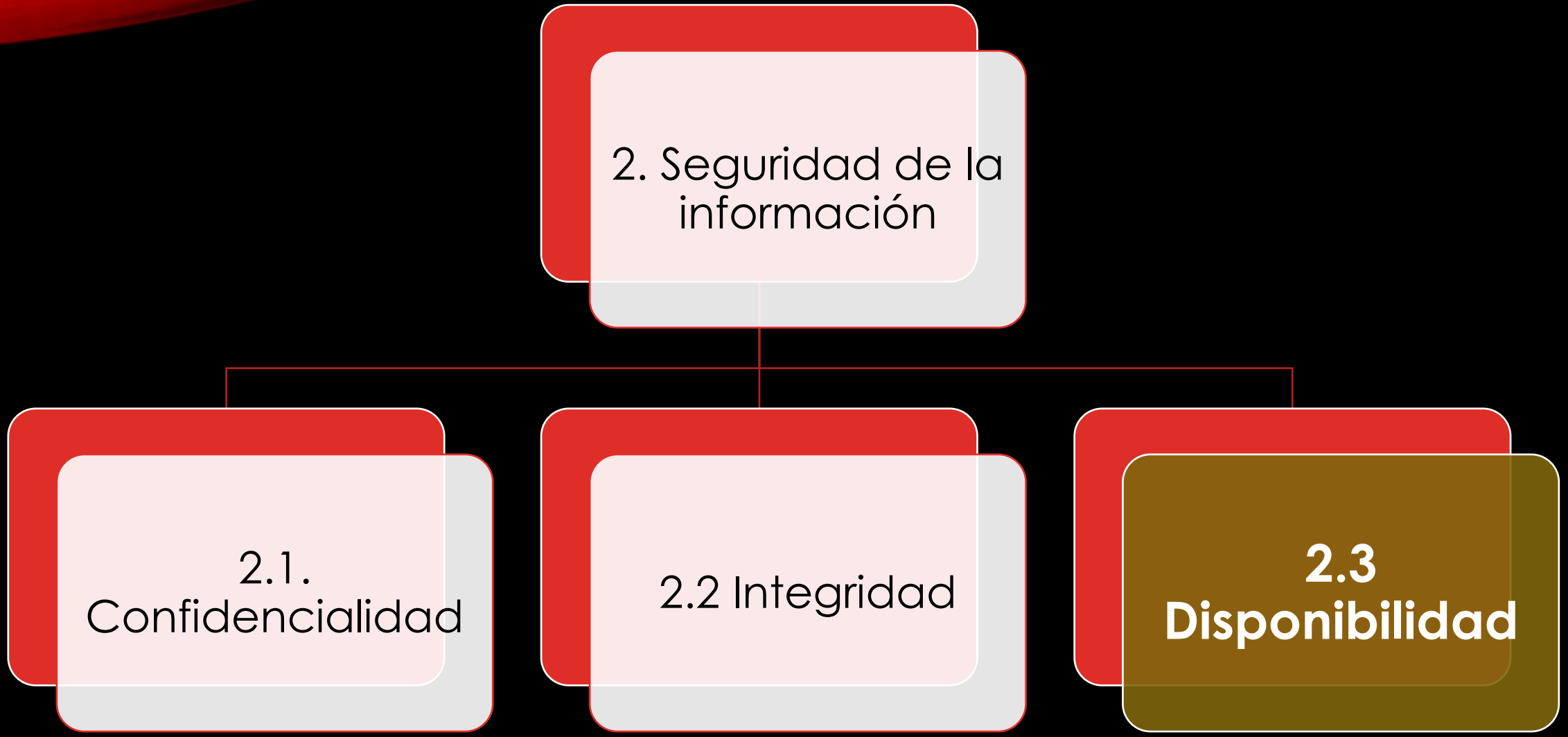
Es la propiedad de la información, por la que se garantiza que está **accesible únicamente a personal autorizado**. Implica por tanto la no divulgación de información a personas o sistemas no autorizados.


2. Seguridad de la información
2.1. Confidencialidad
2.2 Integridad
2.3 Disponibilidad

2.2. INTEGRIDAD

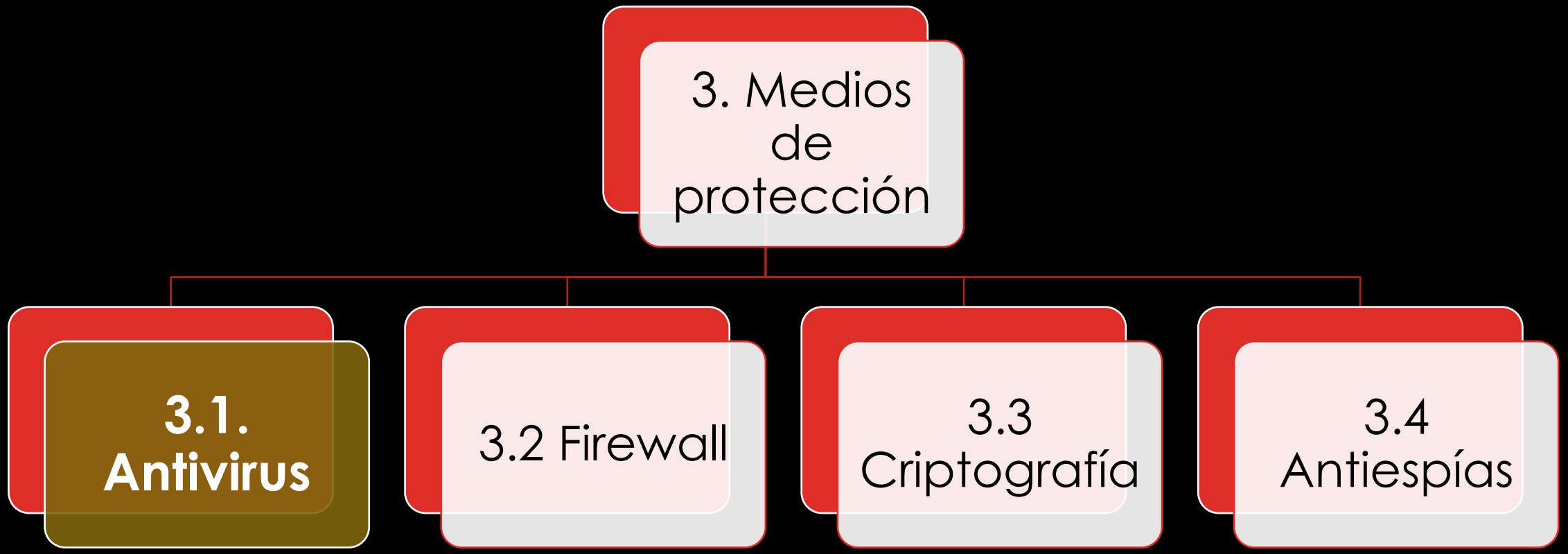
Es la propiedad que busca mantener los **datos libres de modificaciones no autorizadas**.

La tecnología actual facilita la integridad de un mensaje a través de la **firma digital**.


2. Seguridad de la información
2.1. Confidencialidad
2.2 Integridad
2.3 Disponibilidad

2.3. DISPONIBILIDAD

Es la característica de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

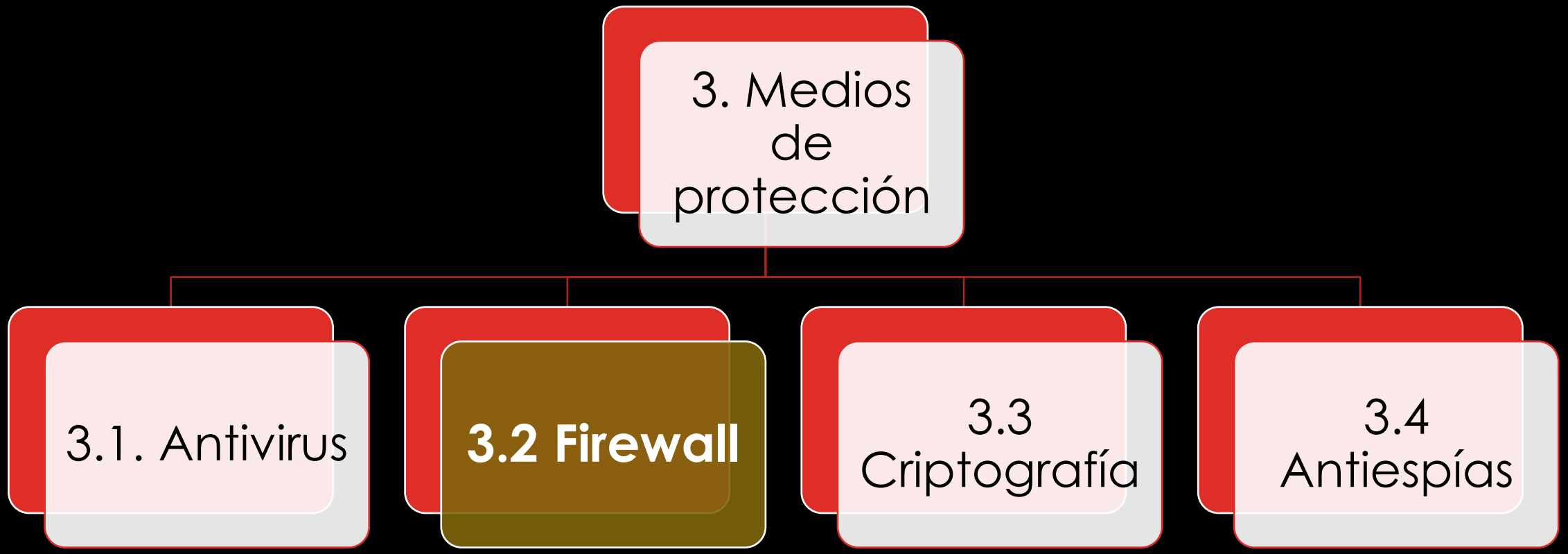

3. Medios de protección
3.1. Antivirus
3.2 Firewall
3.3 Criptografía
3.4 Antiespías

3.1. ANTIVIRUS

Son programas que detectan códigos maliciosos, evitan su activación y propagación y, si es posible, incluso eliminan el daño producido.

Se llaman antivirus porque surgieron para eliminar este tipo de **malware**, pero hoy en día han evolucionado y detectan otros tipos de malware como **troyanos, gusanos o espías**, y cuentan además con rutinas de recuperación y reconstrucción de archivos dañados.

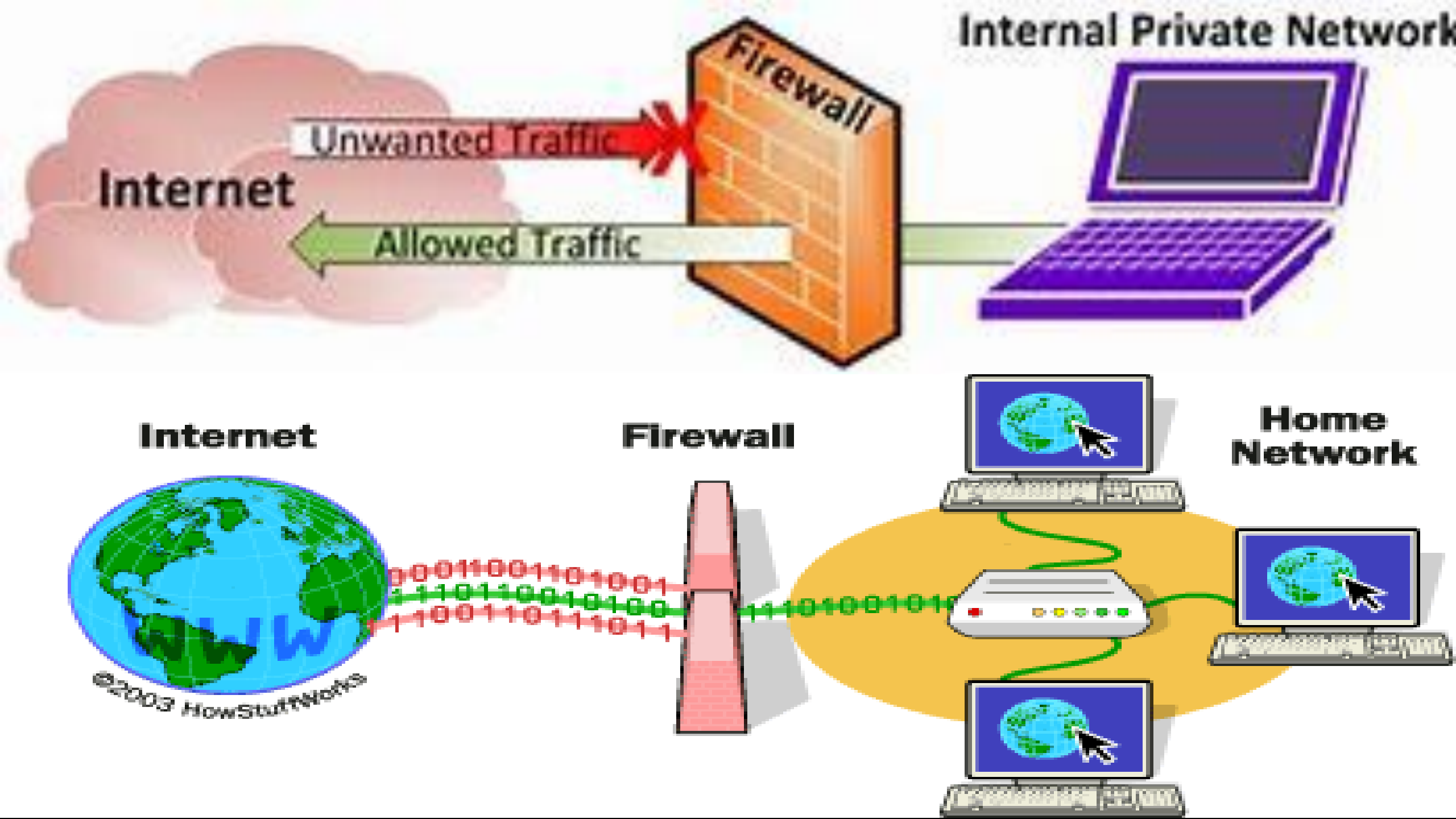

G DATA
PANDA SECURITY
webroot
ca
Norton from symantec
McAfee
pctools
BULLGUARD
Sunbelt Software
KASPERSKY
K7 Computing
ウイルスセキュリティ
RISING
LION STRONG SECURITY
F-SECURE
bitdefender
eset
Microsoft Security Essentials
AVG
TREND MICRO
AhnLab
avast!

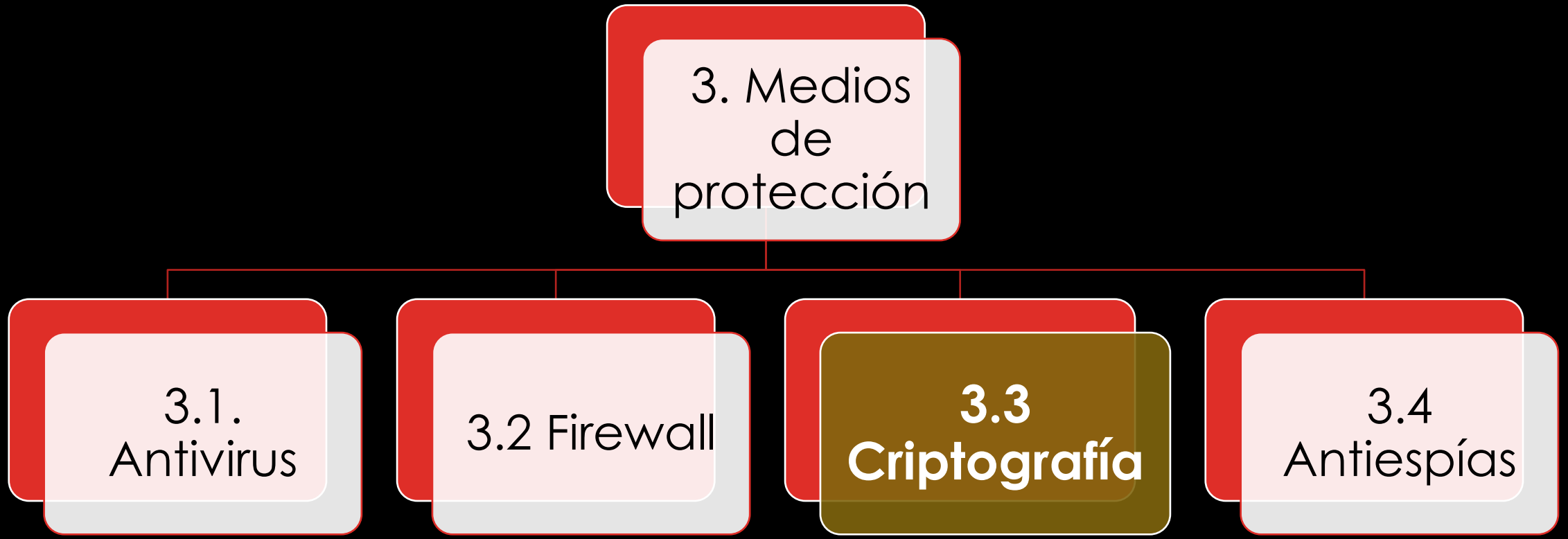

3. Medios de protección
3.1. Antivirus
3.2 Firewall
3.3 Criptografía
3.4 Antiespías

3.2. FIREWALL

Un firewall (pared cortafuegos) es un elemento de hardware o software ubicado entre dos redes y que ejerce la una política de seguridad establecida.

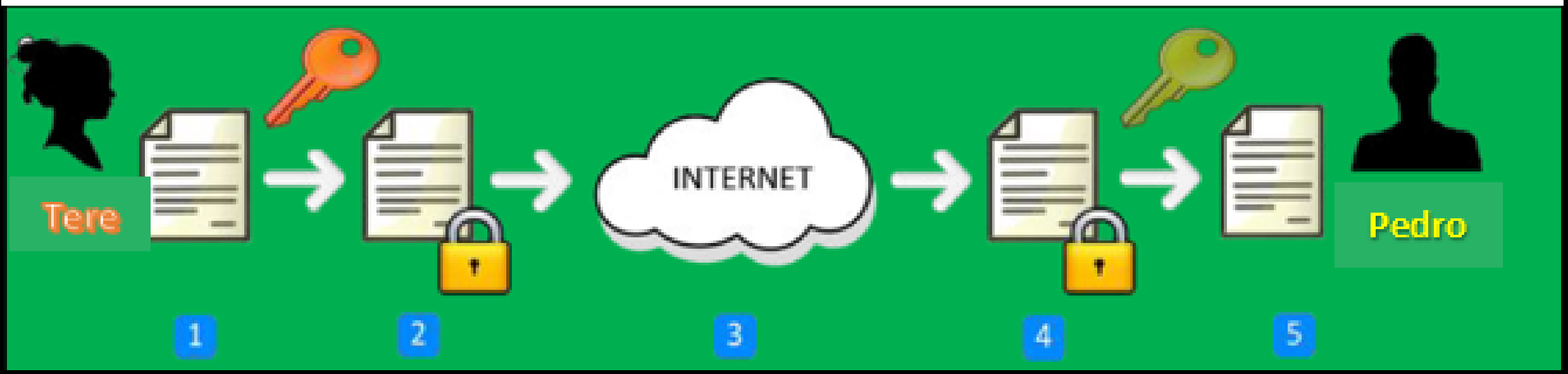
Protege una red confiable de una que no lo es (por ejemplo, internet) evitando que pueda aprovechar las vulnerabilidades de la red interna.

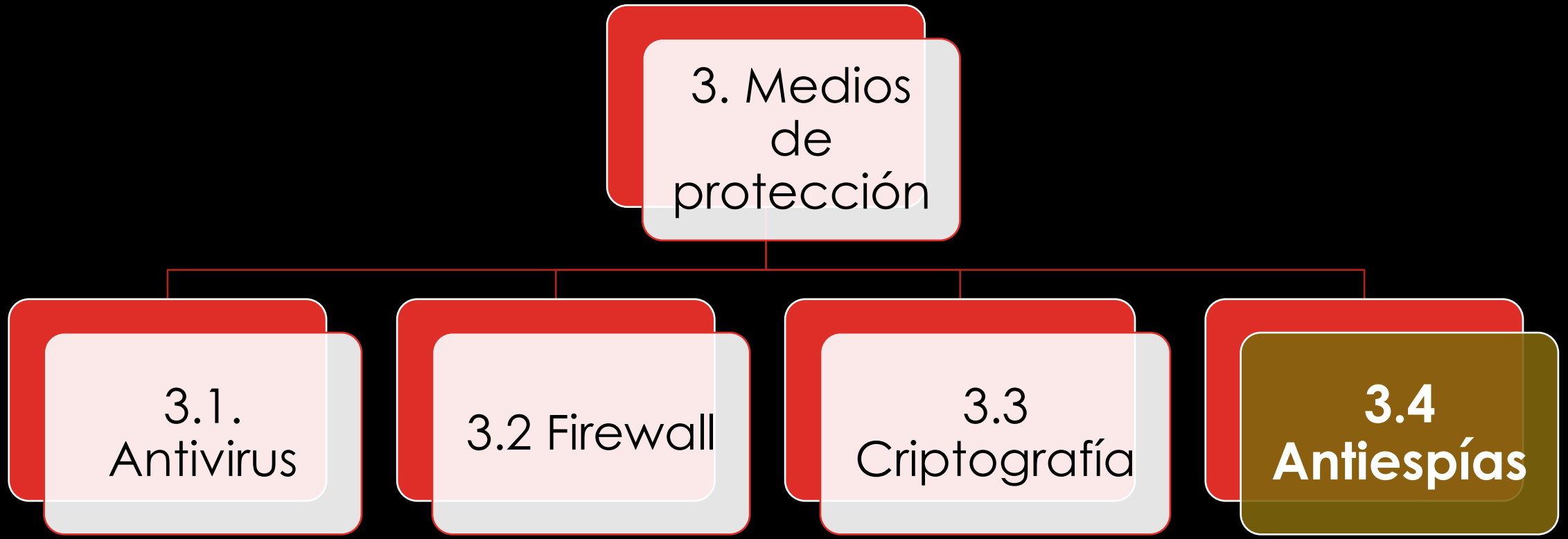

Internal Private Network
Firewall
Unwanted Traffic
Internet
Allowed Traffic
Internet
Firewall
Home Network
WWW
©2003 HowStuffWorks


3. Medios de protección
3.1. Antivirus
3.2 Firewall
3.3 Criptografía
3.4 Antiespías

3.3. CRIPTOGRAFÍA

Consiste en transformar un **mensaje inteligible en otro que no lo es** utilizando claves que sólo el **emisor** y el **destinatario** conocen, para después devolverlo a su forma original, sin que nadie que vea el mensaje cifrado sea capaz de entenderlo.


Tere
INTERNET
Pedro
1
2
3
4
5


3. Medios de protección
3.1. Antivirus
3.2 Firewall
3.3 Criptografía
3.4 Antiespías

3.4. ANTIESPÍAS

Son programas diseñados para detectar, detener y eliminar los códigos maliciosos de programas espías (spyware).

A veces, vienen incluidos en los antivirus, pero son más efectivos los diseñados específicamente para eliminar este tipo de malware.


McAfee AntiSpyware
McAfee
AntiSpyware
Auto-Protect is enabled.
Last update received 1/21/2004 10:32:39 AM.
Engine version: 1.00.1126.0
Signature version: 6.00.1089.0
What's New?
AntiSpyware recently removed Cydoor from your system.
> View properties of this program
> Restore this program
Scanning Statistics
Scanned
Processes 99
Files 91,388
Registry keys 8,390
I want to...
Scan now
Restore programs
View recent activity
Change settings
Learning Center
AntiSpyware Help
What is spyware?
How did it get on my system?


Antispywares


SUPERAntiSpyware Free Edition
SUPERAntiSpyware
Remove ALL the Spyware, NOT just the easy ones!
Scanning Progress
C:\USERS\NICK SKREPETOS\DESKTOP\VIRUSTOTALSCAN\C758A74C2EC3CD94F47BDB845F776F84.EXE
Trojan.Agent/Gen-FakeAV [1 Item Found]
Trojan.Agent/Gen-FakeFolder [1 Item Found]
Trojan.Agent/Gen-FakeAlert[SpyPro] [1 Item Found]
Trojan.Agent/Gen-Backdoor [2 Items Found]
Trojan.Agent/Gen-FakeAlert [2 Items Found]
Trojan.Agent/Gen-FraudAgent [2 Items Found]
Rogue.Agent/Gen [3 Items Found]
Trojan.Agent/Gen [5 Items Found]
Trojan.Agent/Gen-RunOnce [1 Item Found]
Trojan.Agent/Gen-FraudPack [4 Items Found]
Memory Items
Scanned : 831
Detected : 0
Registry Items
Scanned : 31015
Detected : 0
File Items
Scanned : 9590
Detected : 21
Threats Detected
21
Elapsed Time : 00:03:41
Pause Scan
Stop Scan
Cancel Scan

Fin del tema