

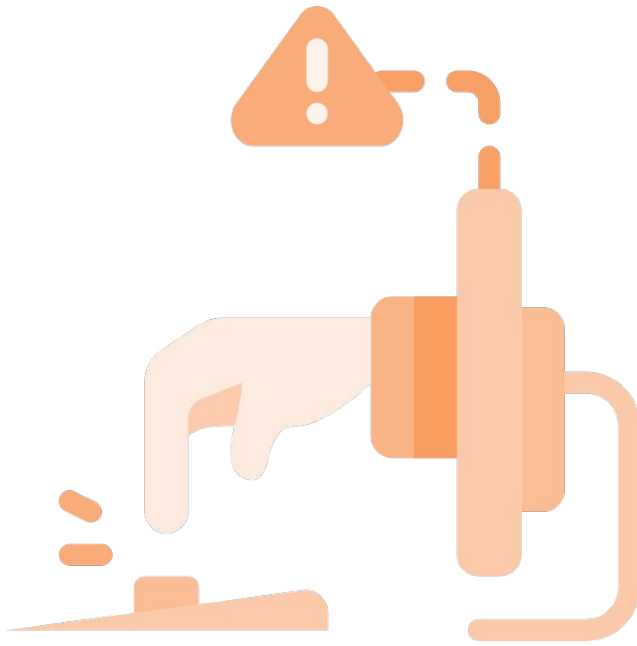


Guía para

Aprender Seguridad Informática

Quetzally Meza

¿Ciberseguridad?



"Todo lo que implica proteger el acceso o uso no autorizado de datos (electrónicos o digitales)".

Pre requisitos

Redes
computacionales

Protocolos de red, modelos
OSI, TCP/IP

Arquitectura de redes

Desarrollo de software /
lenguajes de programación

Sistemas
computacionales

Sistemas operativos

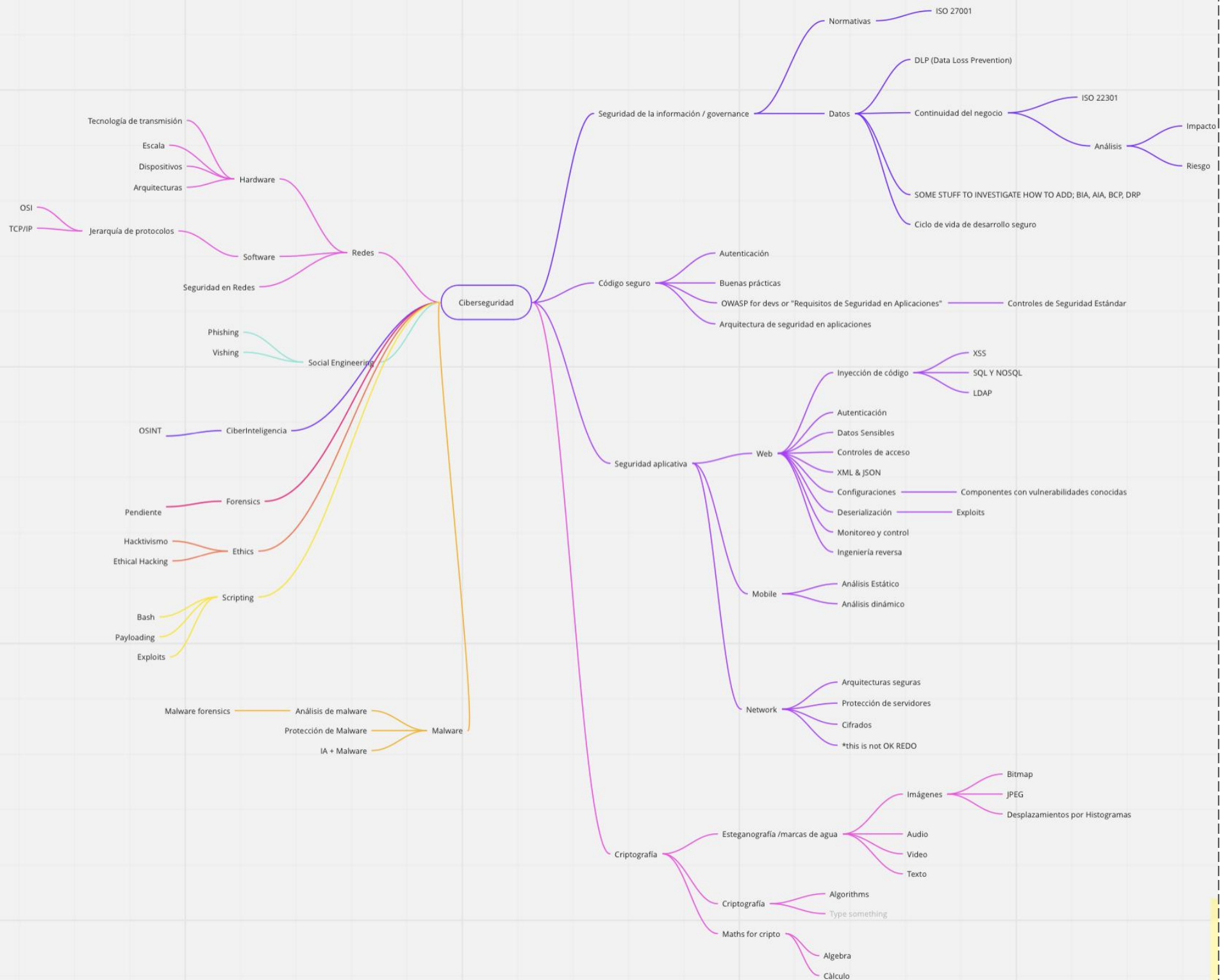
Arquitectura de
sistemas

Normativa y
legislación



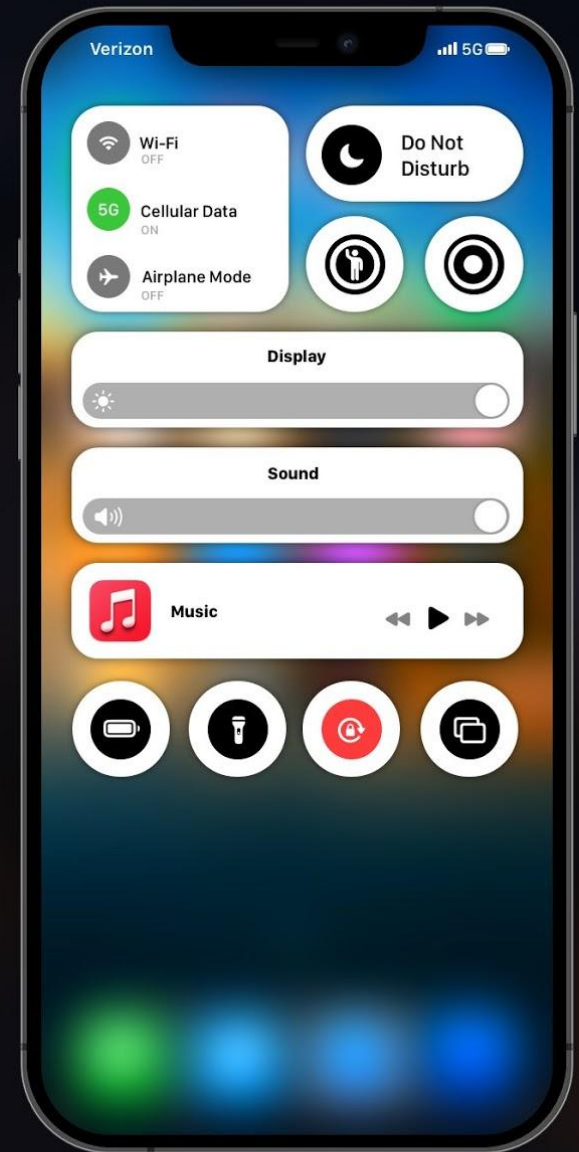
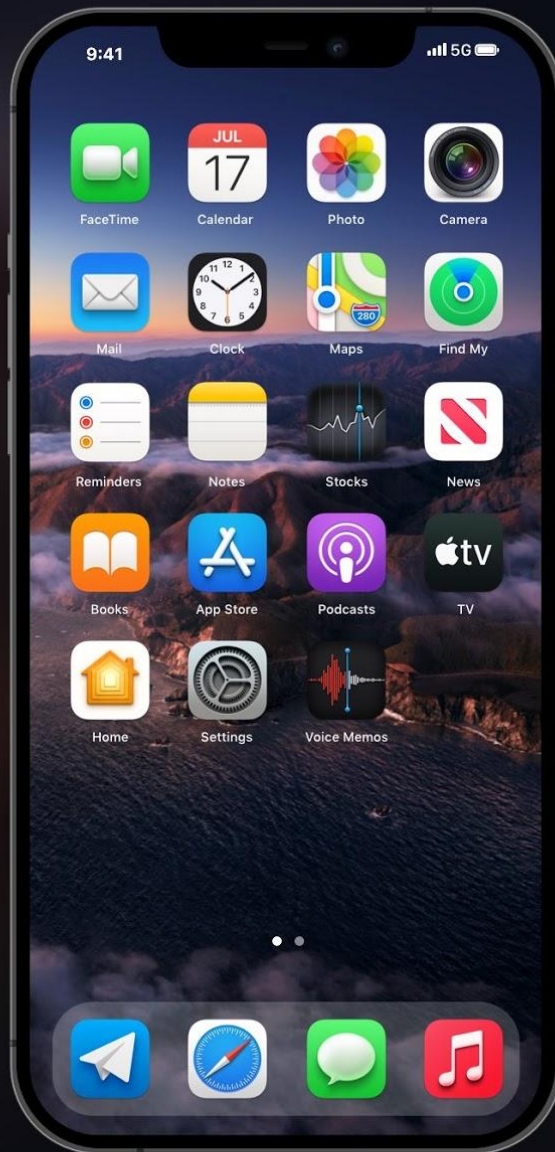
**Aprender inglés
es esencial**

**También experimentar
y no perder la curiosidad**



Hackeo antes del lanzamiento

iOS 14



iOS 15
made by @aapple_lab

Seguridad de la información



“

Medidas para resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

”

Ciber inteligencia



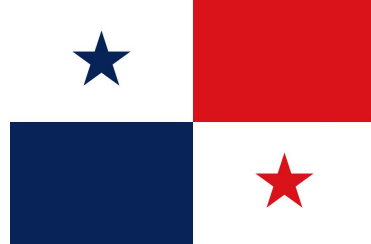
A dark silhouette map of Latin America, including Mexico, Central America, the Caribbean, and South America, is positioned in the background. The text is overlaid on this map.

Derechos digitales en Latinoamérica

Mantuvieron negociaciones



Compraron Remote Control System



Tienen antecedentes de espionaje



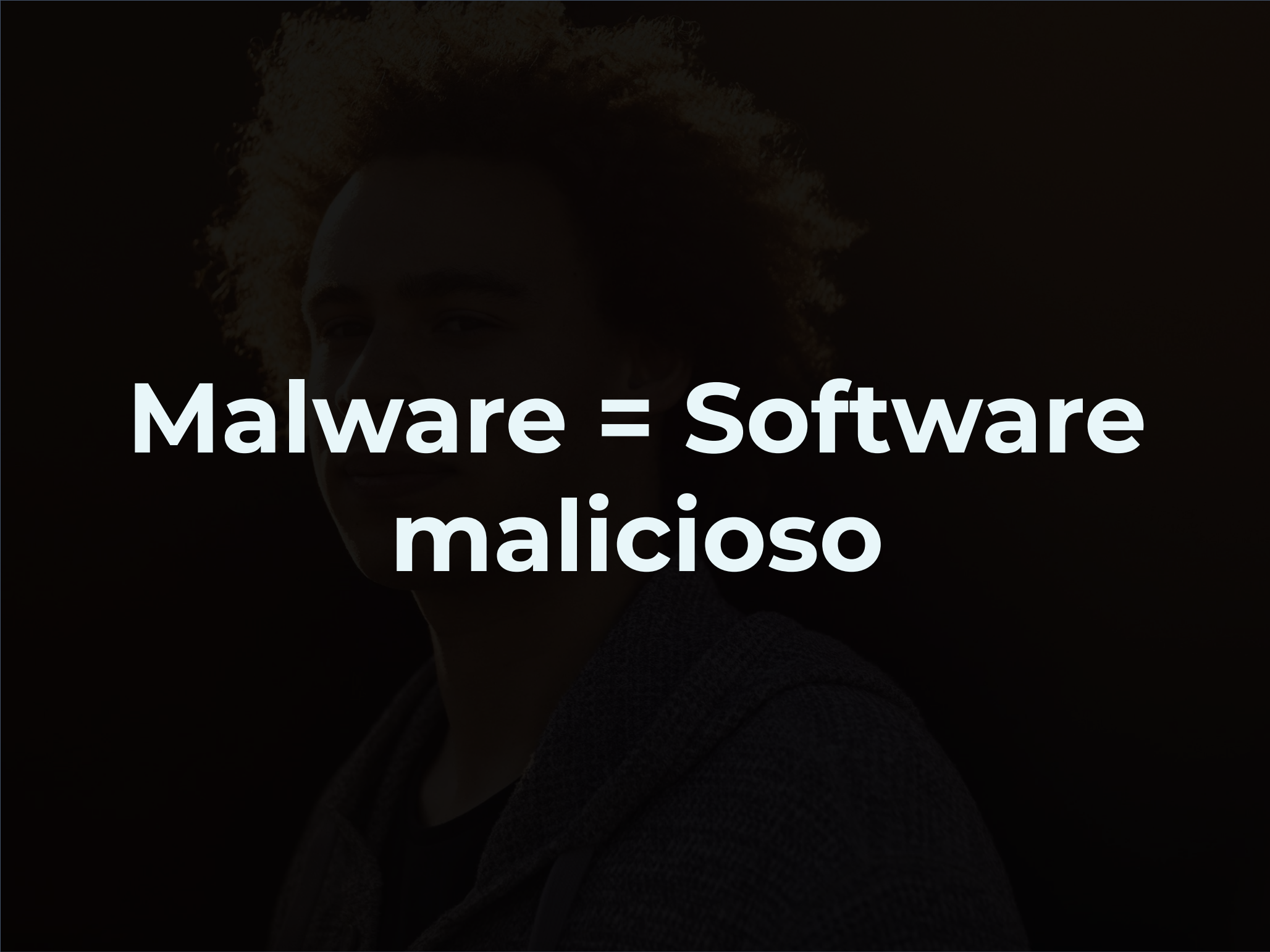
“

Adquisición y análisis de información
para identificar, rastrear y predecir
las capacidades, intenciones y
actividades cibernéticas que ayuden
a identificar amenazas

”

El Hacker que salvó internet





**Malware = Software
malicioso**

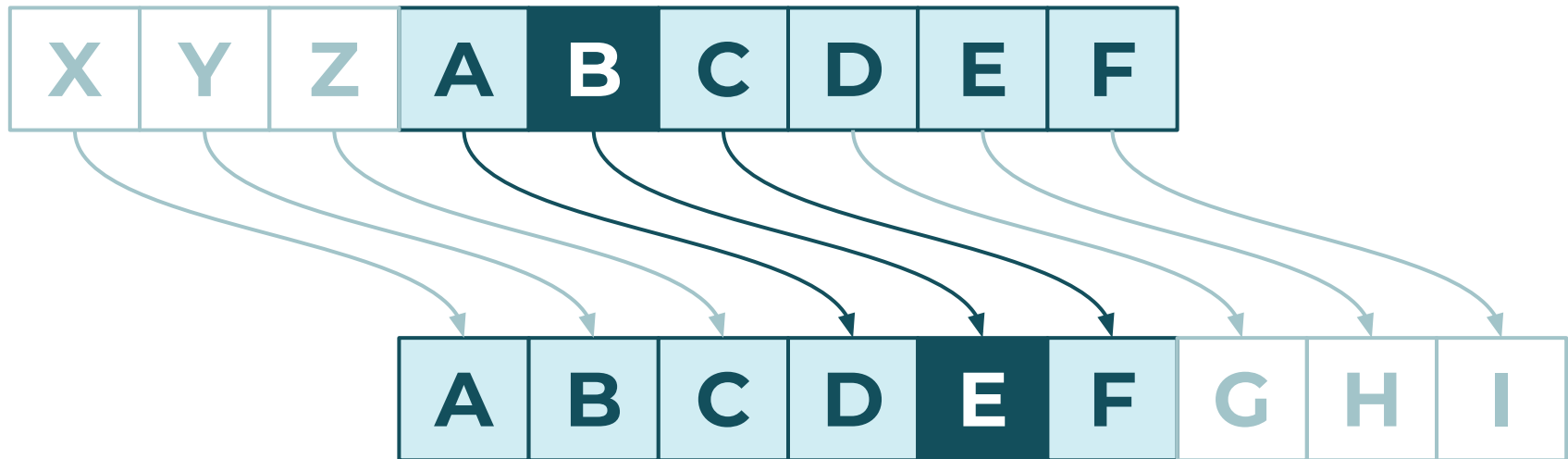
Criptografía

“

Criptografía = cifrar datos
Esteganografía = ocultar datos

”

La criptografía se usa desde siempre





Capacidad



Robustez



Transparencia o imperceptibilidad



Seguridad





Código seguro

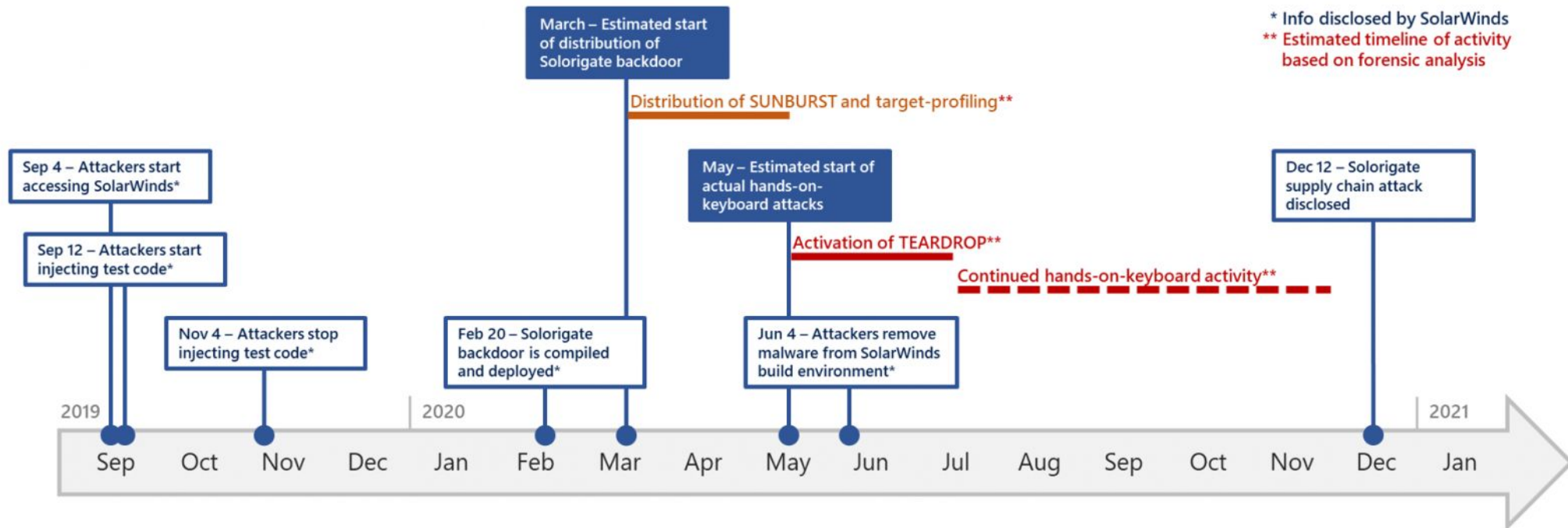
Ciclo de vida del desarrollo de software



Ciclo de vida del desarrollo de software



Pentesting y Solarwinds



<https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/>

SUPPLY CHAIN ATTACK

Attackers insert malicious code into a DLL component of legitimate software. The compromised DLL is distributed to organizations that use the related software.

EXECUTION, PERSISTENCE

When the software starts, the compromised DLL loads, and the inserted malicious code calls the function that contains the backdoor capabilities.

DEFENSE EVASION

The backdoor has a lengthy list of checks to make sure it's running in an actual compromised network.

RECON

The backdoor gathers system info

INITIAL C2

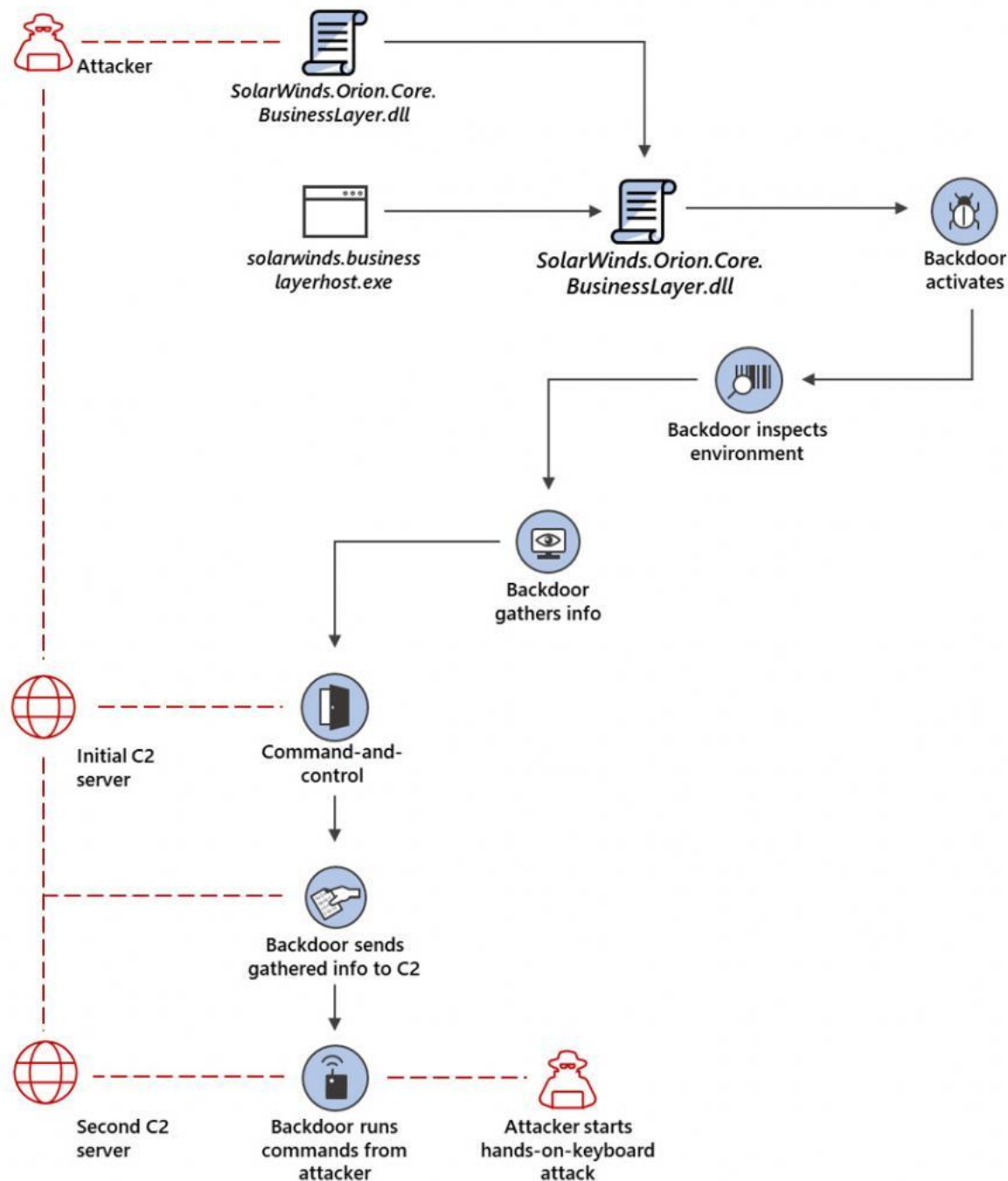
The backdoor connects to a command-and-control server. The domain it connects to is partly based on info gathered from system, making each subdomain unique. The backdoor may receive an additional C2 address to connect to.

EXFILTRATION

The backdoor sends gathered information to the attacker.

HANDS-ON-KEYBOARD ATTACK

The backdoor runs commands it receives from attackers. The wide range of backdoor capabilities allow attackers to perform additional activities, such as credential theft, progressive privilege escalation, and lateral movement.



Vectores de ataque

- Inyección de código.
- Pérdida de autenticación.
- Pérdida de controles de acceso.
- Uso de componentes con vulnerabilidades conocidas.
- Registros y monitoreos insuficientes.
- Deserialización insegura.

“

Las pruebas de seguridad o pentest consisten en realizar ataques informáticos a aplicaciones con el objetivo de encontrar vulnerabilidades existentes

”

El Chapo





Ingeniería Forense

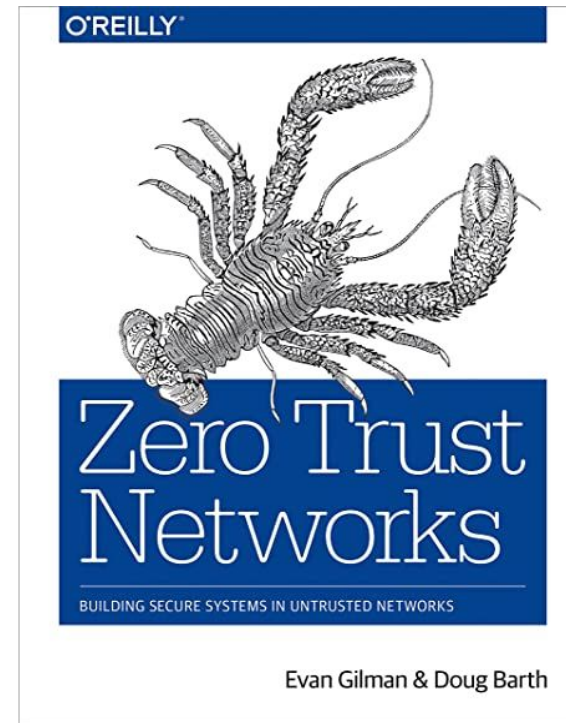
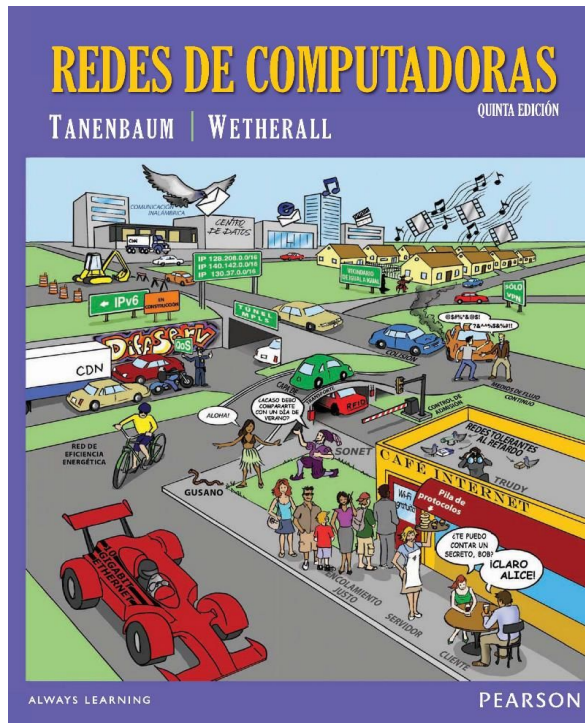
“

La ingeniería forense consiste en identificar la causa en el fallo de un sistema ya sea para mejorarlo o encontrar a los responsables

”

Seguridad en redes

1

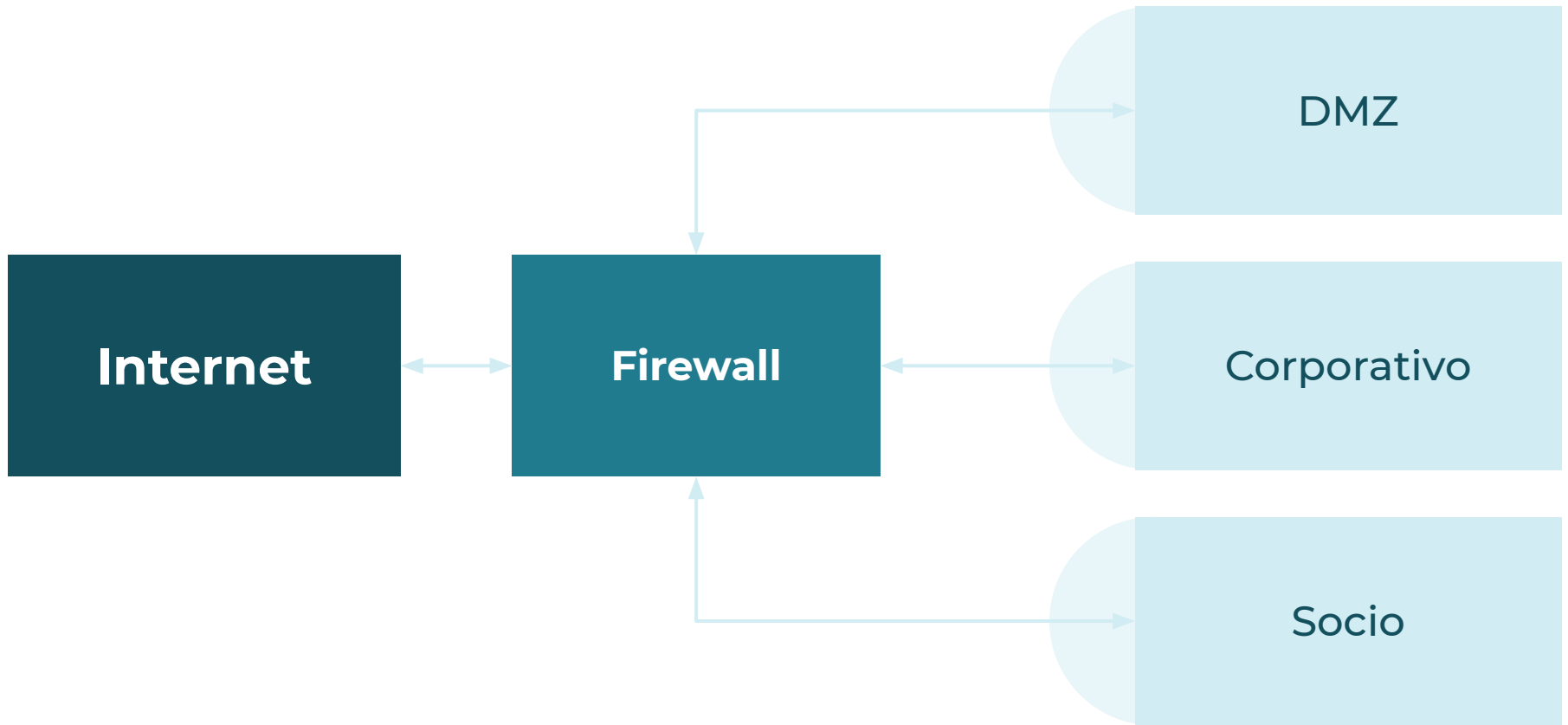




Curso de

Redes Informáticas de Internet

Quetzally Meza

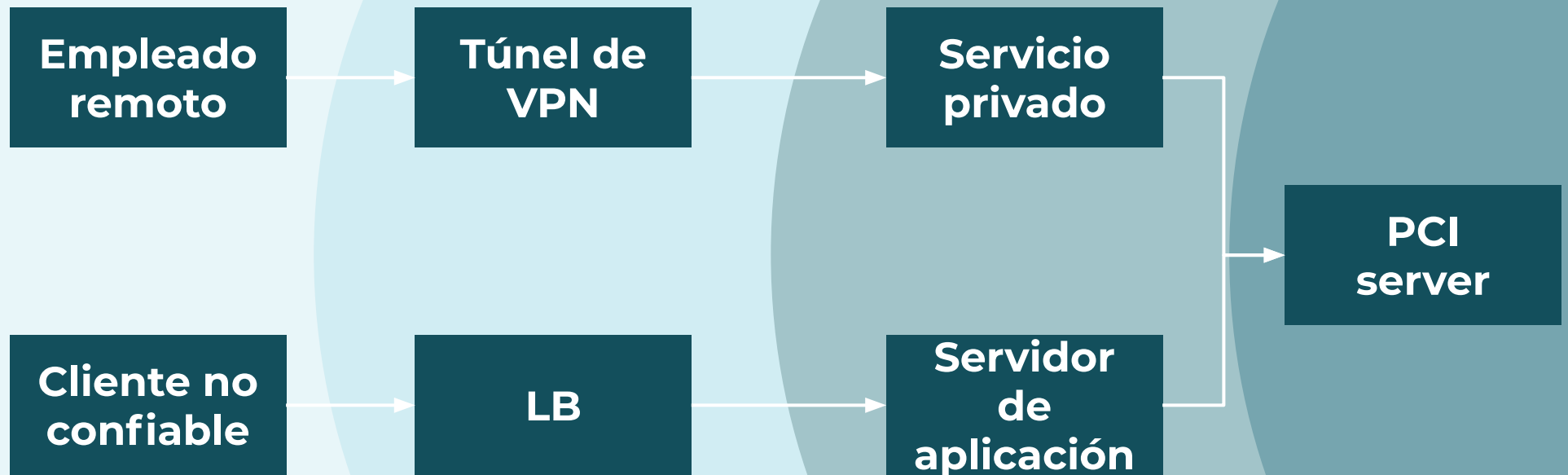


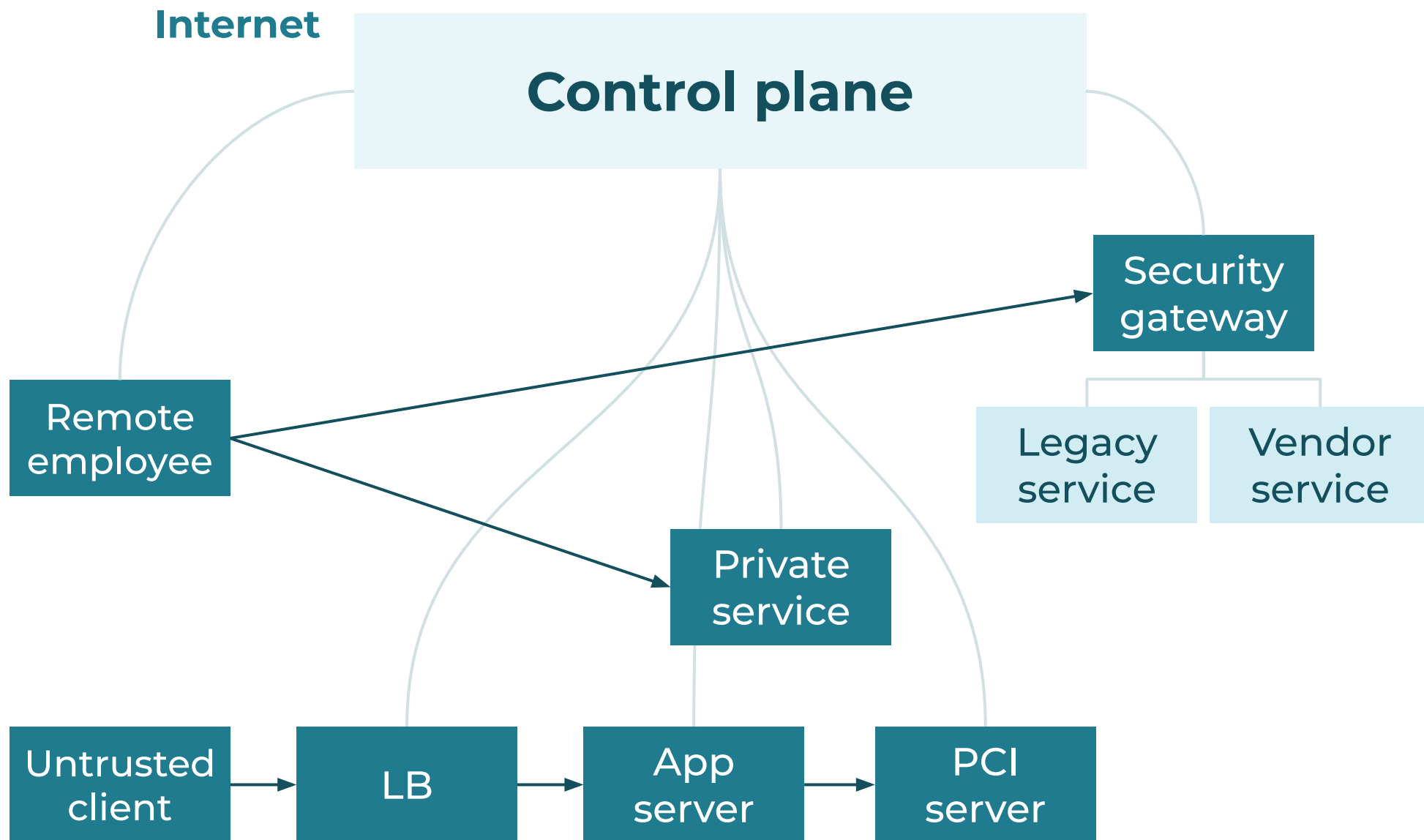
Internet

DMZ

Trusted

Privileged





**¿Y si no tengo acceso
a un empleo de
ciberseguridad?**

Empleos para acercarte a roles de ciberseguridad

Desarrollo web

Ingeniería de redes

Analista de sistemas

Bases de datos

Soporte técnico

Ingeniería de software

Administración
de sistemas, bases
de datos, redes,
seguridad

Testing / ingeniería de
pruebas

Campo normativo /
legal

Certificaciones

Comptia	Network+	Security+		
Offense Security	OSCP			
EC-Council	CND	CEH	ESCA	LPT
ISC2			ISSC2 CCSP	ISSC2 CISSP
Otras certificaciones/ entidades	ITIL	ISACA	SANS	



Dificultad

Roles en la industria

Los empleos más demandados en 2020

- Ingeniero en ciberseguridad.
- Analista de ciberseguridad.
- Arquitecto de redes/ciberseguridad.
- Consultor de ciberseguridad.
- Gerente de ciberseguridad.

Para principiantes

- Pentester Jr.
- Analista Jr.
- Técnico de redes.
- Respuesta a incidentes.
- Consultor Jr.

Intermedios

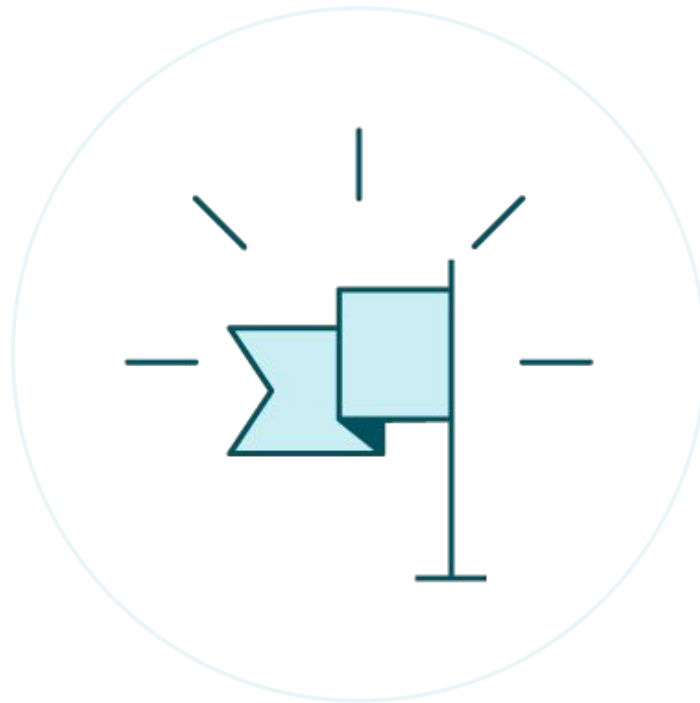
- Ingeniero de preventa.
- Ethical hacker.
- Ingeniero Forense / Análisis forense.
- Consultor en Seguridad de la información.

Avanzado

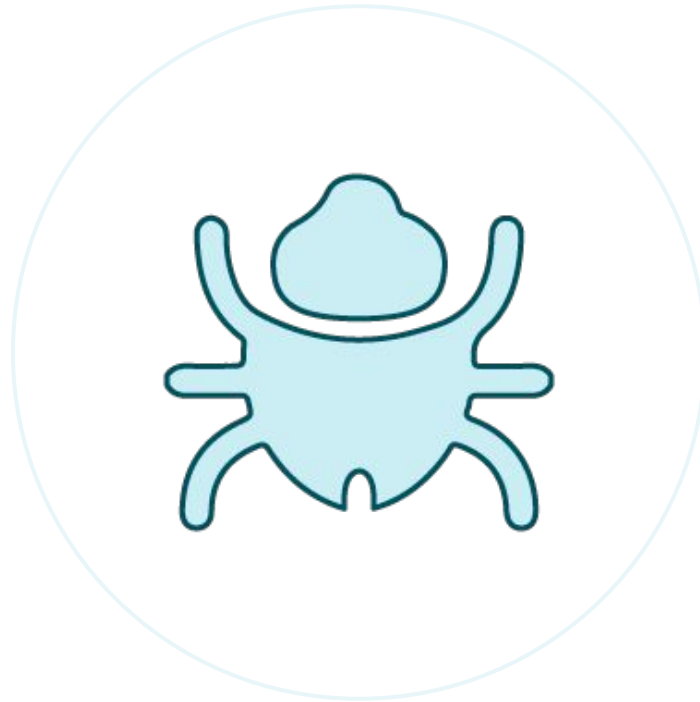
- Análisis de malware / Malware reversing.
- Ingeniería reversa.
- Líder de Red Team / Blue Team.
- Experto en nube.
- CISO, CSO, DPO.
- Especialista en incidencias.

¡Empieza a aprender!

Capture the Flag



Bug bounties



Cursos



Laboratorios



**¡Nunca pares de
aprender!**



Algunas opciones son

- Capture the Flag

- Bug Bountys

<https://docs.google.com/document/d/1OdLkz2LE-03jBDIKaT2mPG4q4Z8Vtj00ct11N1ivDr4/edit?usp=sharing>

- Cursos

- Laboratorios

- Herramientas interesantes

<https://docs.google.com/document/d/1zl3XBKIL-tXpSW6EbXjDRVk2BU3w31024BDOCKJTuzc/edit?usp=sharing>