

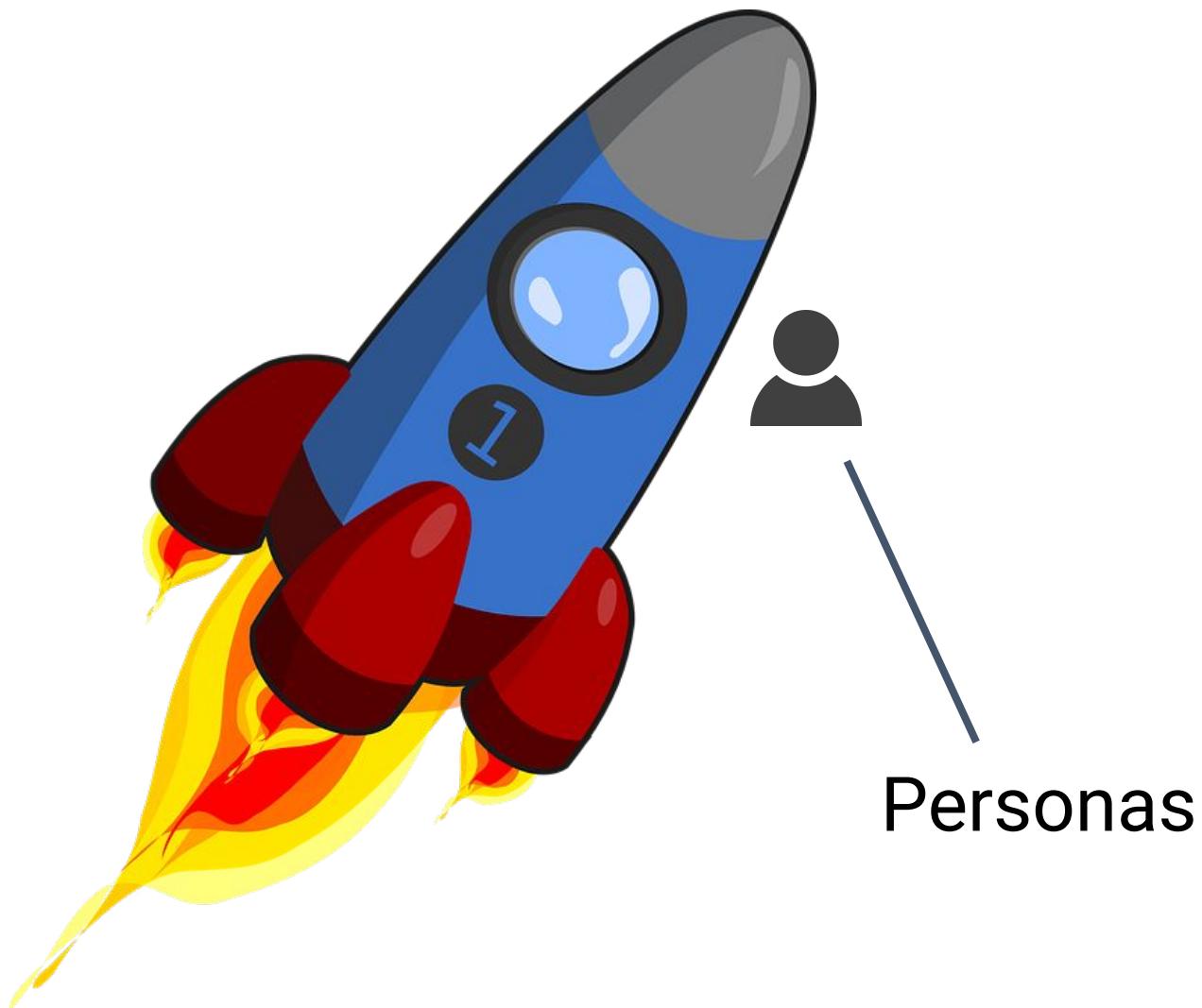
Curso de

Ciberseguridad para Empresas

Diego Ademir Duarte Santana
Juan José Torres

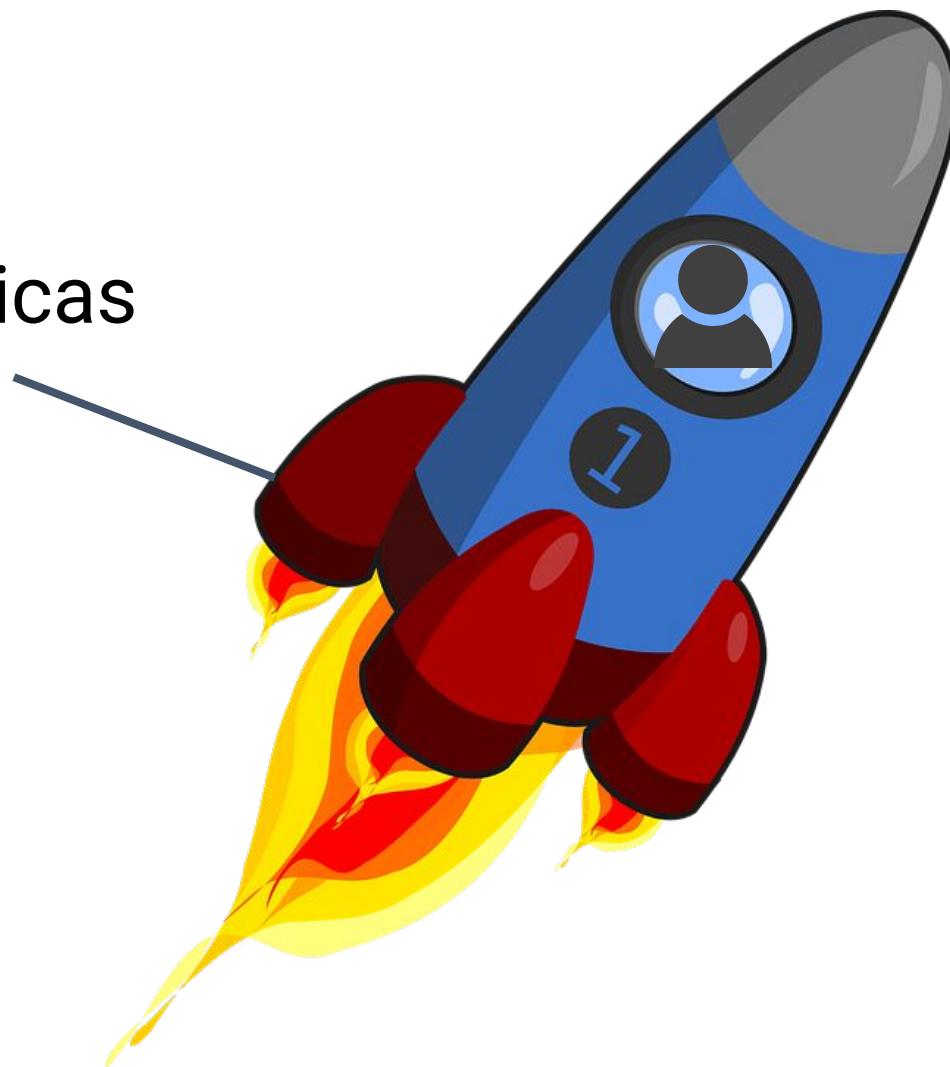
¿Qué es
la Ciberseguridad?

Conjunto de prácticas para desarrollar...

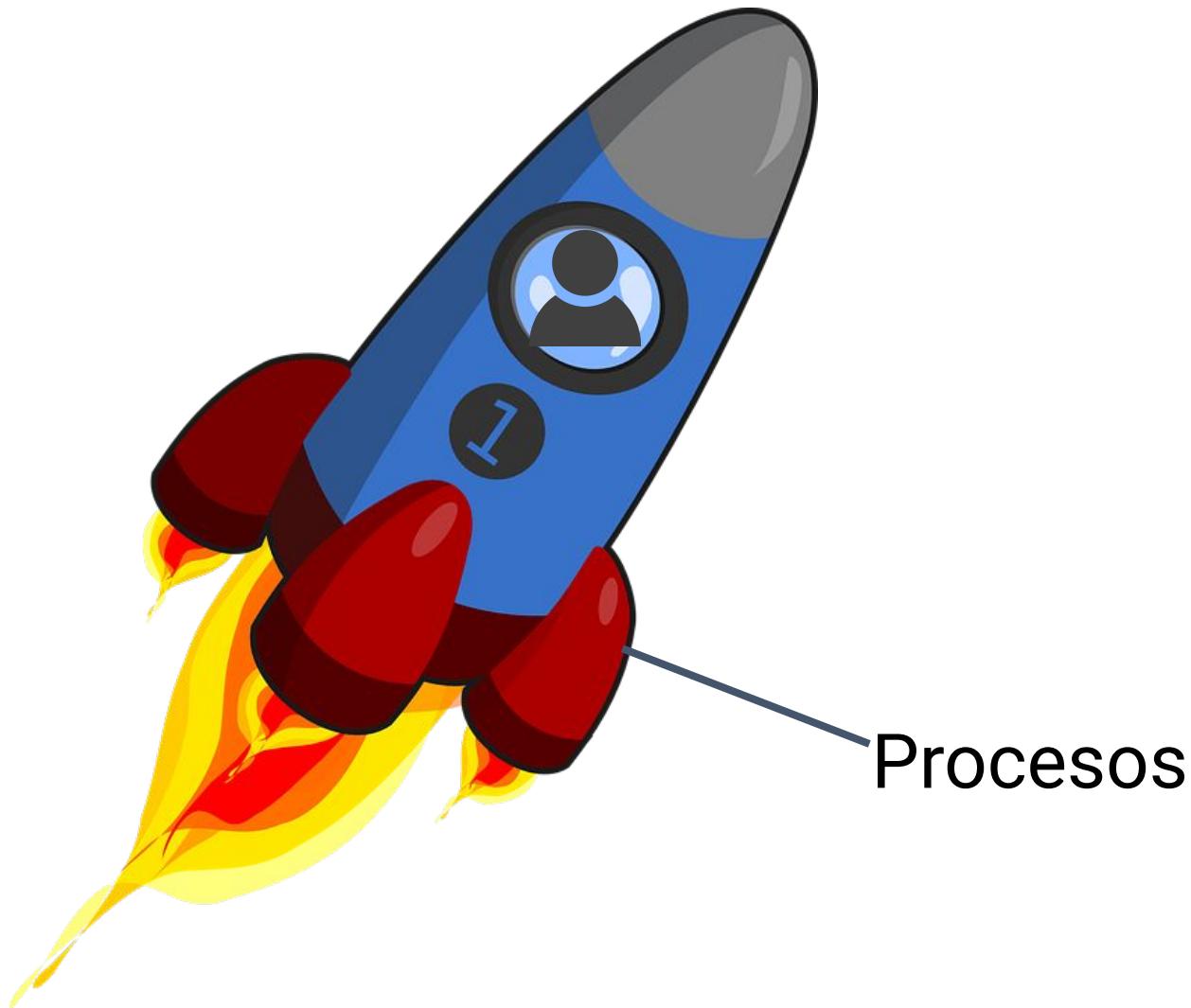


Conjunto de prácticas para desarrollar...

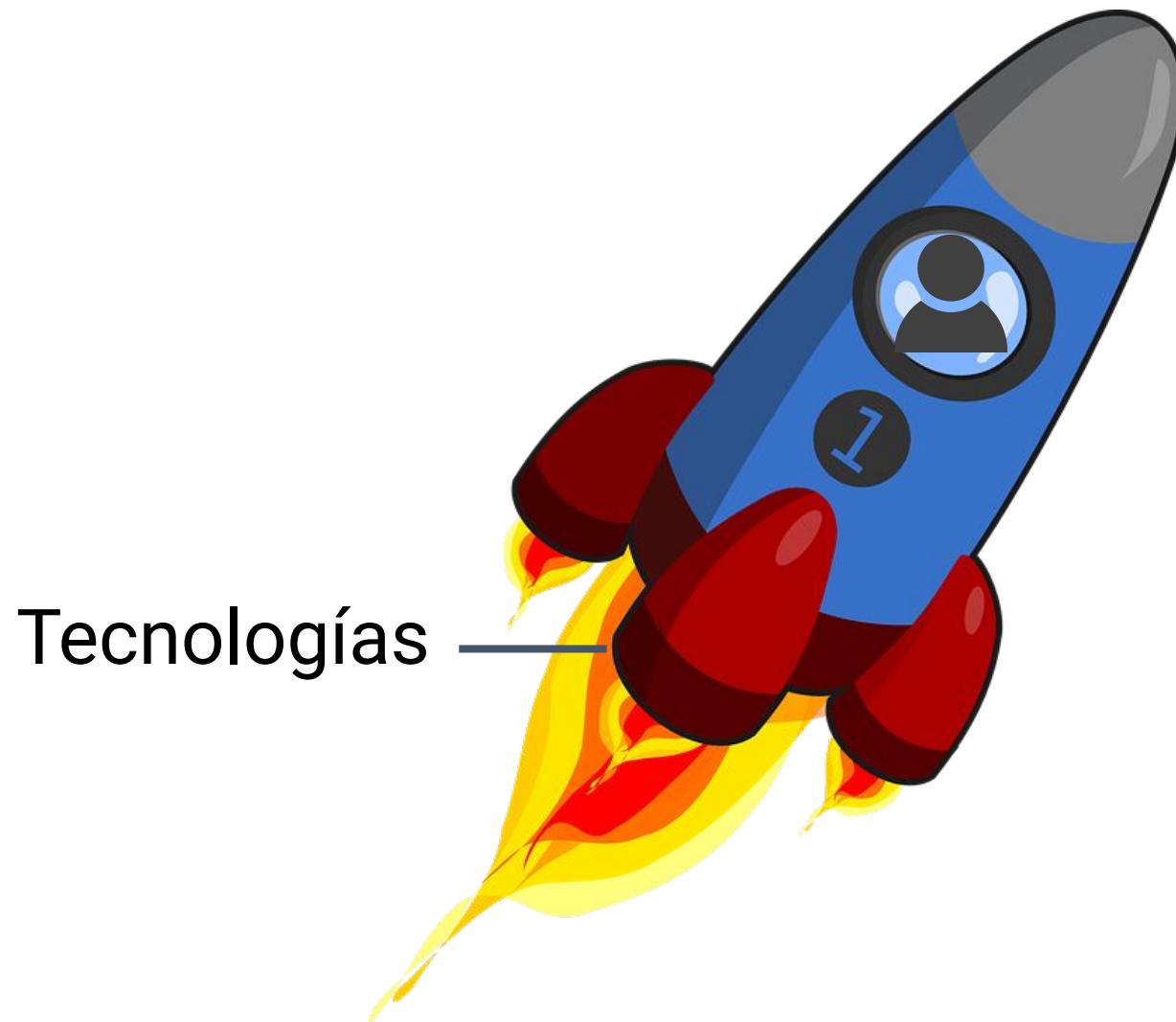
Políticas



Conjunto de prácticas para desarrollar...



Conjunto de prácticas para desarrollar...



¿Con qué motivo?

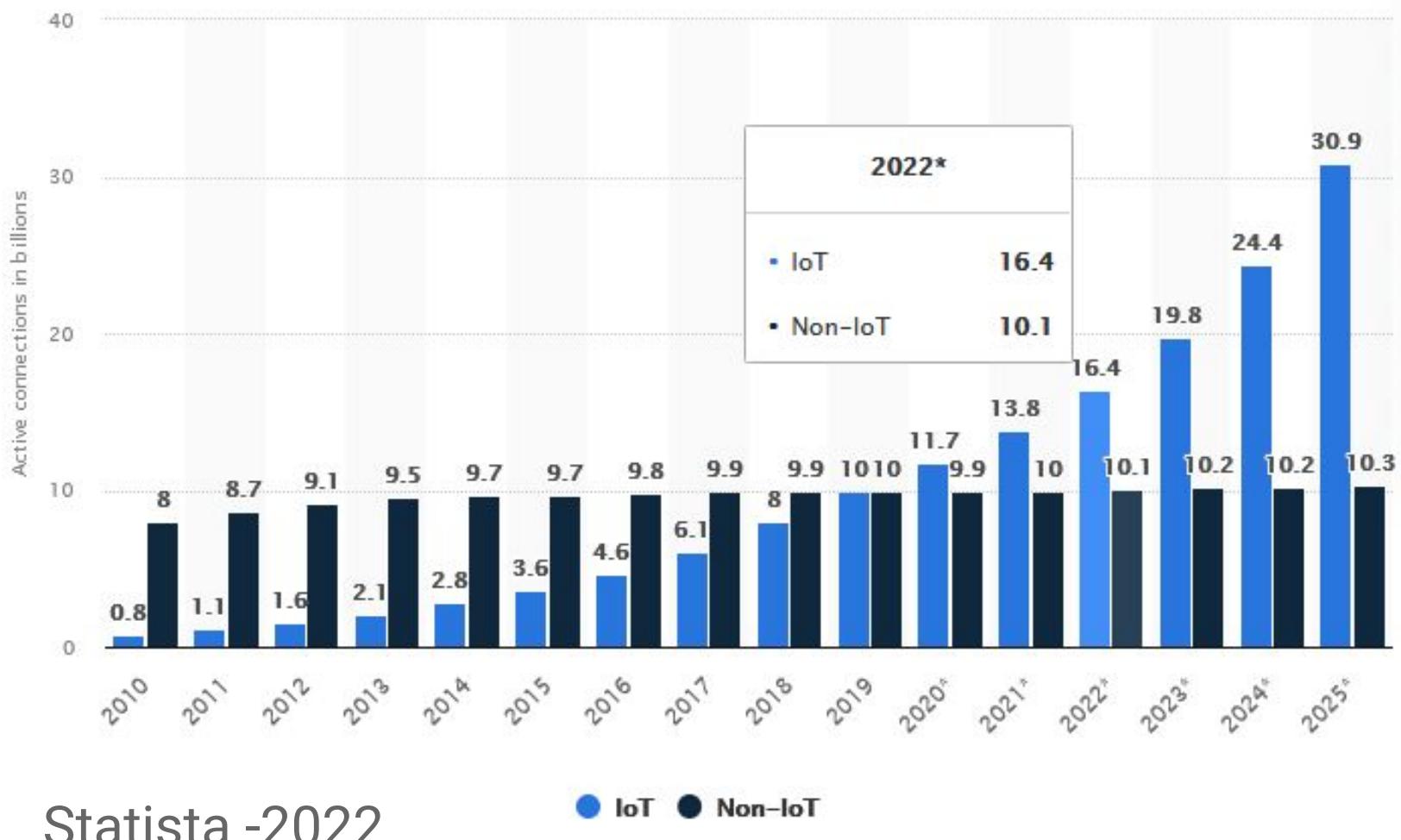
Para proteger tu empresa u organización,
sus sistemas críticos e información
sensible de ataques digitales.

| **¡Todo basado en RIESGOS!**



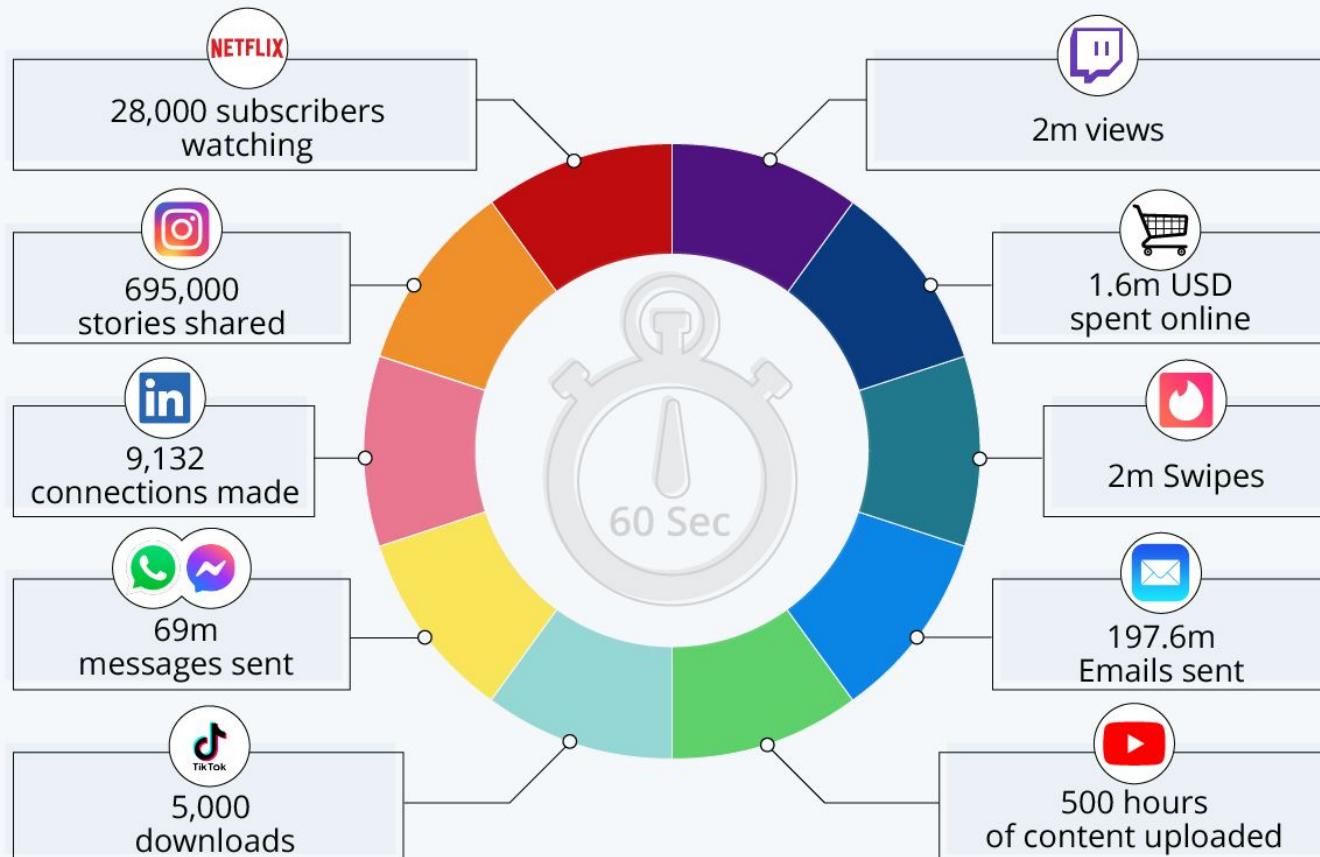
Importancia de la Ciberseguridad

Protección de Datos



A Minute on the Internet in 2021

Estimated amount of data created
on the internet in one minute



Source: Lori Lewis via AllAccess



“

**El costo promedio de una
brecha de seguridad en 2021
fue de USD \$4.24 millones.**

”

Cost of a Data Breach Report 2021 - IBM

“ “
**Se perdieron USD \$6.9 mil
millones en 2021 por
cibercrímenes.**

” ”

*Internet Crime Complaint Center 2021 Internet Crime
Report - FBI*

Mitigación de Riesgos



Financiero



Reputacional



Regulatorio

Exigencias



Gobiernos



Inversionistas



Usuarios

Beneficios de la Ciberseguridad

¿Qué logro con tener Ciberseguridad?

Aumento del nivel
de confianza hacia
mi empresa por
la gestión **SEGURA**
de la información.



...y otros logros más...

- **Compliance**

Incremento en nivel de cumplimiento en normativas de Ciberseguridad.

- **Data Privacy**

Correcto tratamiento de datos sensibles (GDPR).



...y aún más...

- **Availability**

Optimizar la disponibilidad de servicios tecnológicos.

- **Evolution**

Mejorar la imagen corporativa e ingreso a nuevos mercados.

Retos de la Ciberseguridad

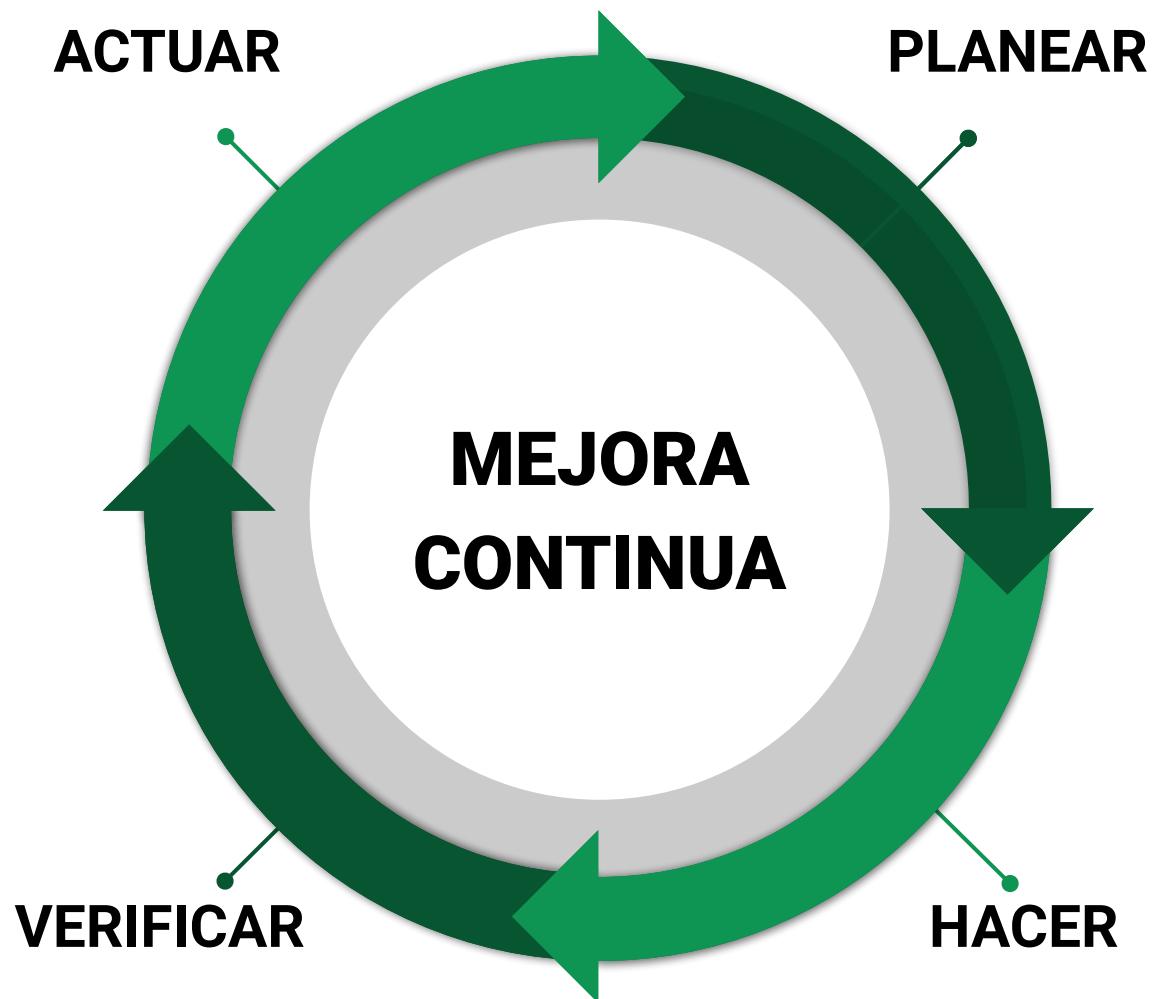
Innovación constante



Nuevas
Tecnologías



Zero-days

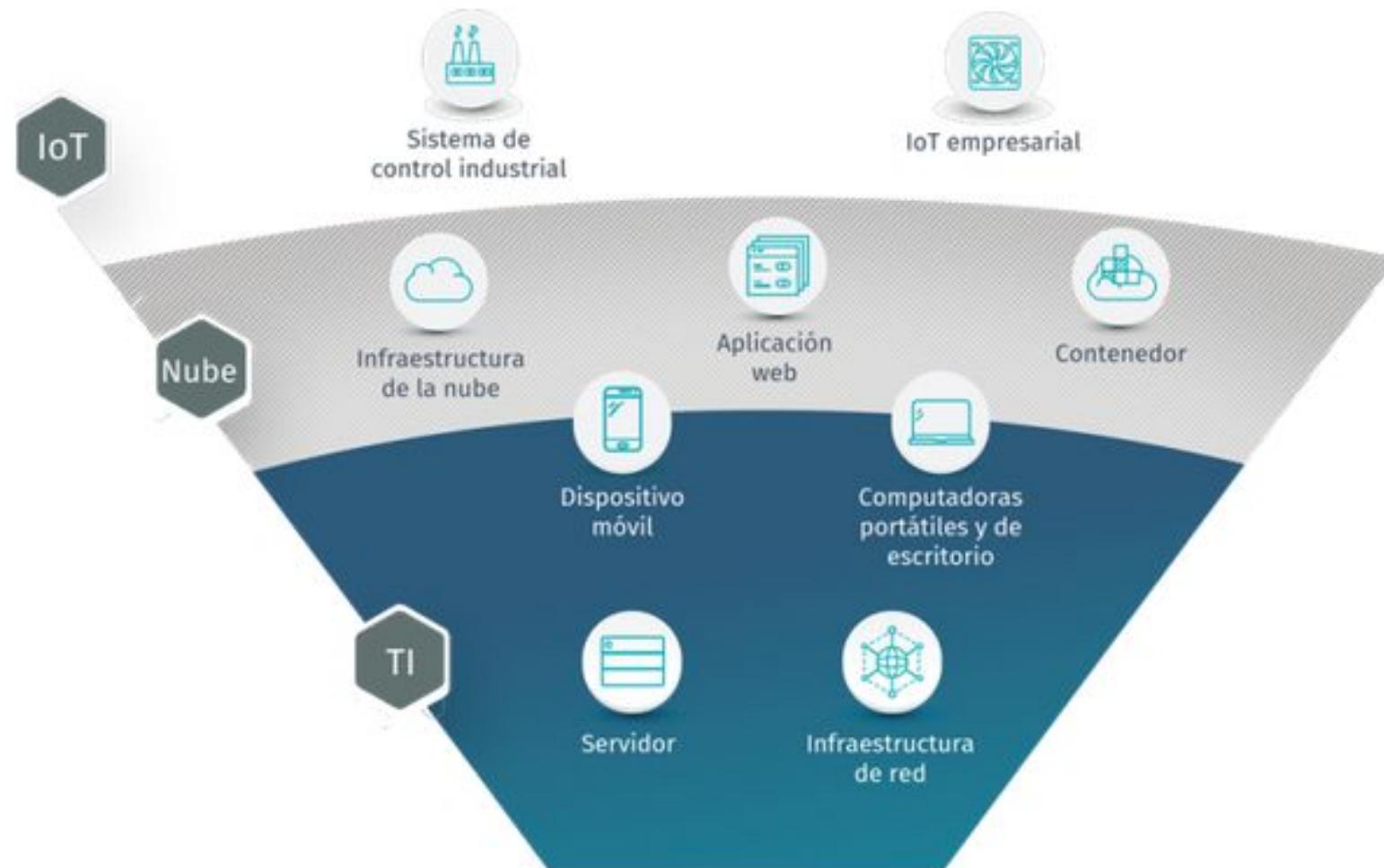


Mayor número de atacantes

- Script Kiddies
- Grupos criminales
- Naciones-estado
- Hacktivistas
- Competidores
- Internos



Mayor superficie de ataque



Cultura en seguridad



Entiende tus Riesgos

¿Conoces tus Ciber-Riesgos?

Toda organización
debe realizar un *GAP*
Análisis a sus procesos
en términos de
Ciberseguridad.



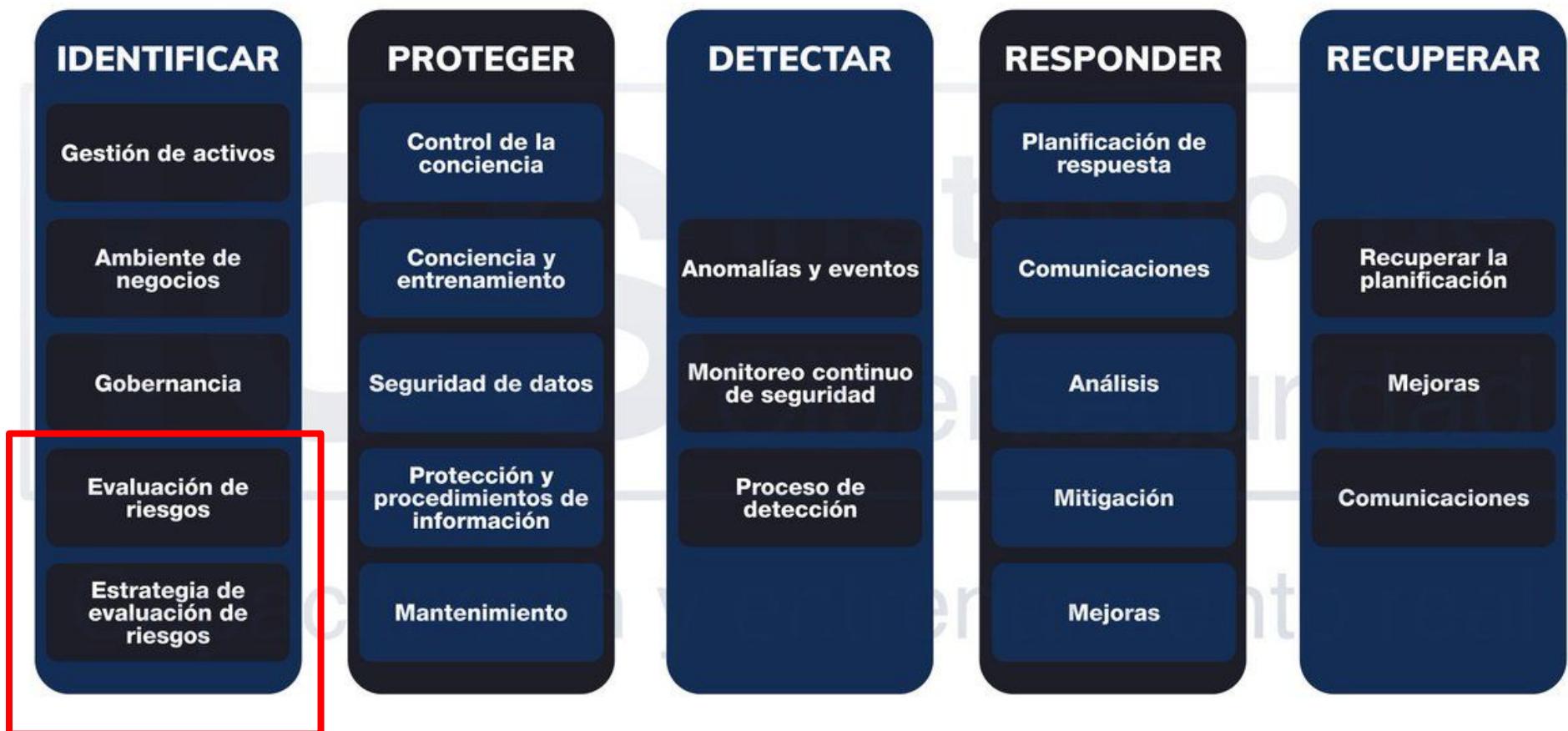
Autoevaluación

- **Amenazas**
¿Tengo claras las ciber-amenazas que podrían afectar la información de mi empresa?
- **Alcance**
¿Qué activos de información debo proteger de Ciberataques?

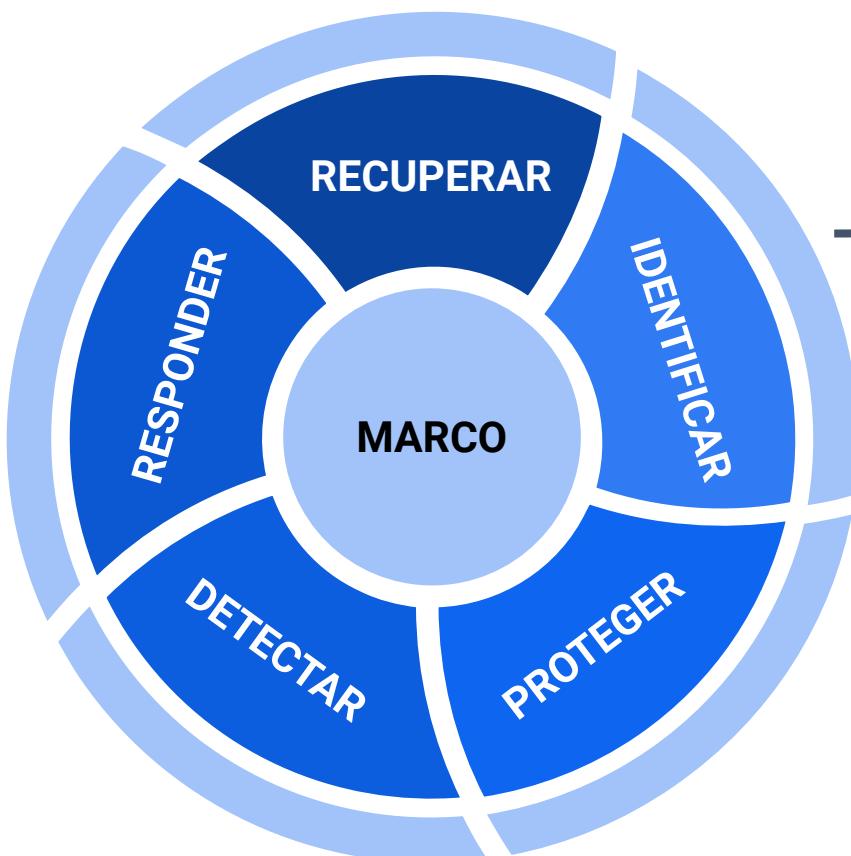
Autoevaluación

- **Transferencia del Riesgo**
¿Podría buscar apoyo en el tratamiento de riesgos identificados?
- **Apoyo**
¿Cuento con respaldo para implementar Ciber-Controles?

NIST Cybersecurity Framework



NIST Cybersecurity Framework



IDENTIFICAR

Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de: sistemas, activos, datos y capacidades.

Seguridad de la Información

¿Qué es?

Es la rama de la seguridad que se enfoca en la protección de la información y asegurar su **confidencialidad, disponibilidad e integridad** mediante medidas preventivas y reactivas basadas en el manejo de riesgos.

Conceptos Básicos

- **Confidencialidad**

La información es accesible solo para aquellos autorizados a tener acceso.

- **Disponibilidad**

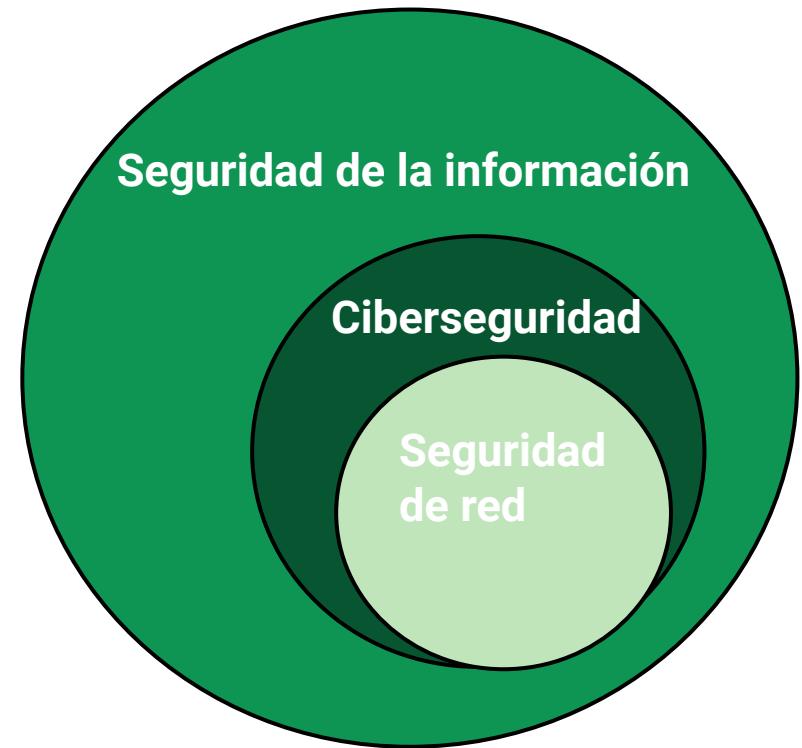
La información es accesible y utilizable por solicitud de una entidad autorizada, cuando está así lo requiera.

- **Integridad**

La información debe mantenerse inalterada. Libre de modificaciones no autorizadas.

Seguridad de la Información vs. Seguridad Informática

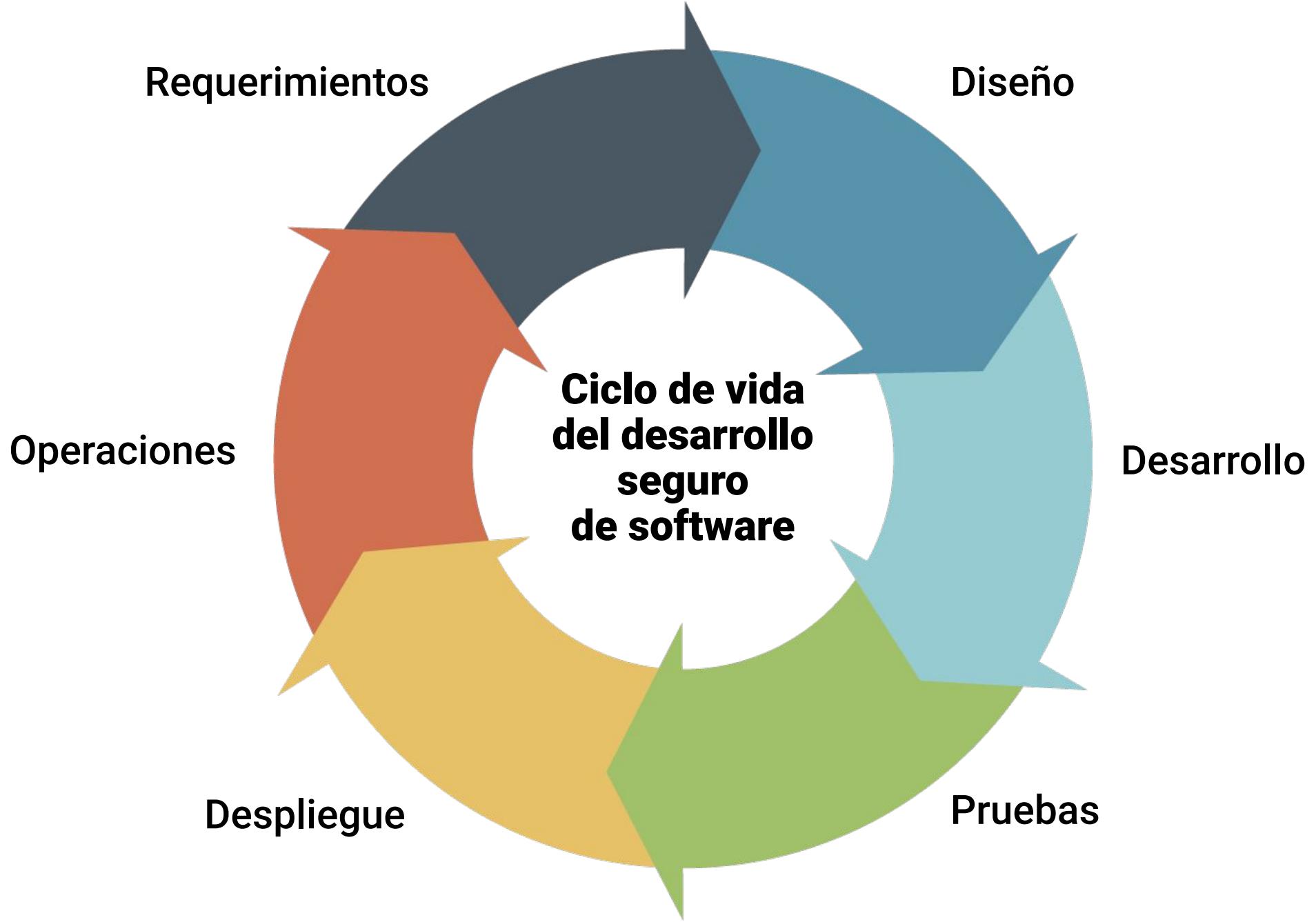
La seguridad de la información engloba más que solo sistemas digitales; incluye gestión de riesgos, normativas, estándares, planes, etc.



Seguridad de Aplicaciones

¿Qué es?

Es la rama de la seguridad que se preocupa por introducir prácticas seguras al ciclo de desarrollo de software. Busca mejorar las prácticas de seguridad y así prevenir incidentes de seguridad en las aplicaciones.



Controles de Seguridad

- Entrenamiento OWASP Top 10.
- Análisis estático de código.
- Análisis dinámico de código.
- Arquitecturas seguras.

Modelo de Madurez (OWASP SAMM)

El modelo de madurez de aseguramiento de Software (SAMM) es un framework abierto que ayuda a las organizaciones a formular e implementar una estrategia para la seguridad del software que se ajuste a los riesgos que enfrente la organización.

Business functions	Governance	Design	Implementation	Verification	Operations
Security practices	Strategy & Metrics Create & promote Measure & improve	Threat Assessment Application risk profile Threat modeling	Secure Build Build process Software dependencies	Architecture Assessment Architecture validation Architecture compliance	Incident Management Incident detection Incident response
	Policy & Compliance Policy & standards Compliance management	Security Requirements Software requirements Supplier security	Secure Deployment Deployment process Secret management	Requirements-driven Testing Control verification Misuse/abuse testing	Environment Management Configuration hardening Patch & update
	Education & Guidance Training & awareness Organization & culture	Secure Architecture Architecture design Technology management	Defect Management Defect tracking Metrics & feedback	Security Testing Scalable baseline Deep understanding	Operational Management Data protection Legacy management
	Stream A	Stream A	Stream A	Stream A	Stream A
	Stream B	Stream B	Stream B	Stream B	Stream B

Estándares

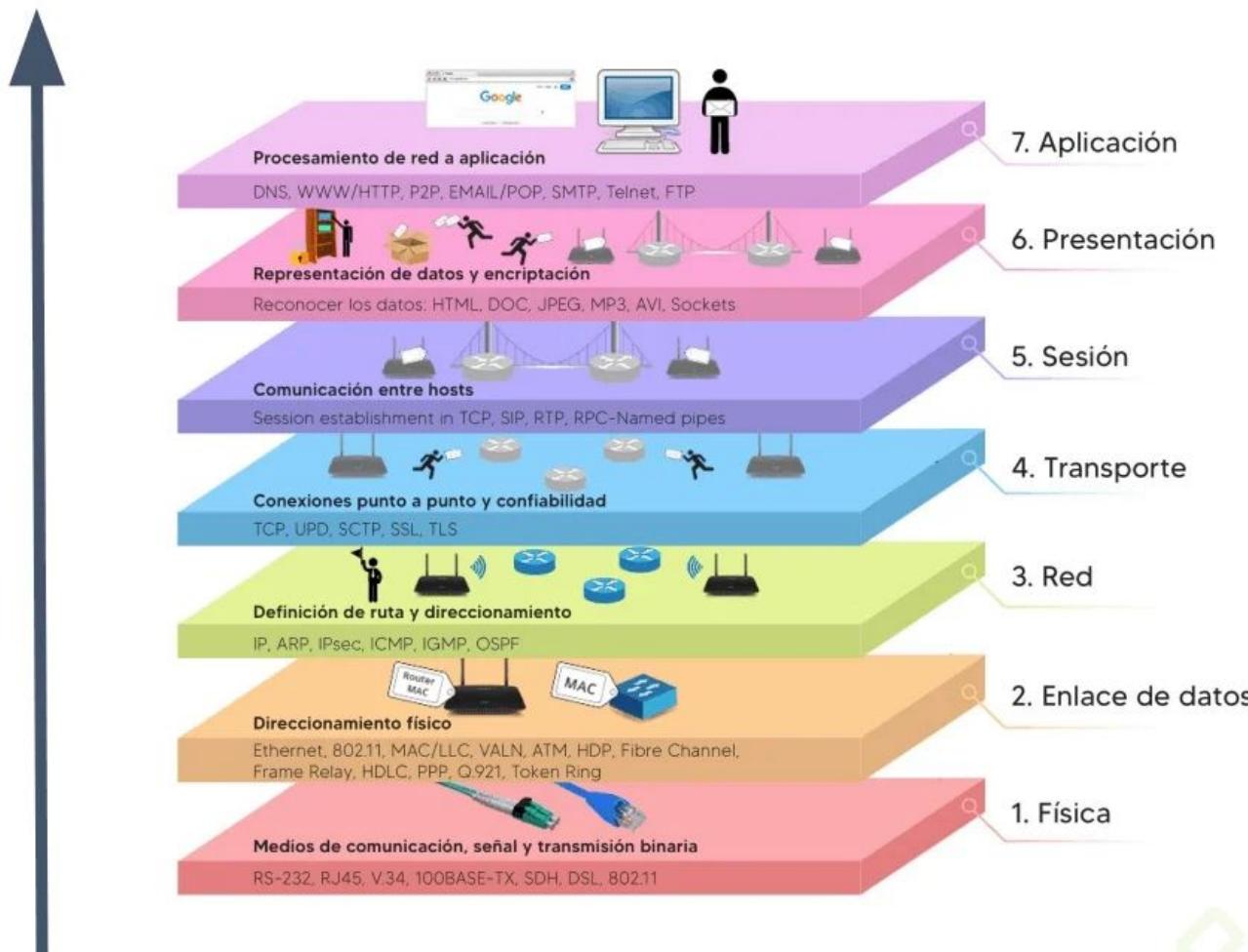
- CERT Secure Coding
- ISO/IEC 27034-1:2011
- ISO/IEC TR 24772:2013
- NIST Special Publication 800-53
- OWASP ASVS: Web Application Security Verification Standard

Seguridad en Redes

¿Qué es?

Es la rama que estudia la infraestructura de red, su conectividad y seguridad. Incluye políticas y soluciones para proteger el acceso, el uso y la integridad de la red y los datos corporativos.

Capas Modelo OSI



Principales Controles

- Firewalls
- Control de acceso
- Segmentación de redes
- DLP
- IPS
- VPN
- SIEM
- Seguridad Inalámbrica
- Protecciones correo

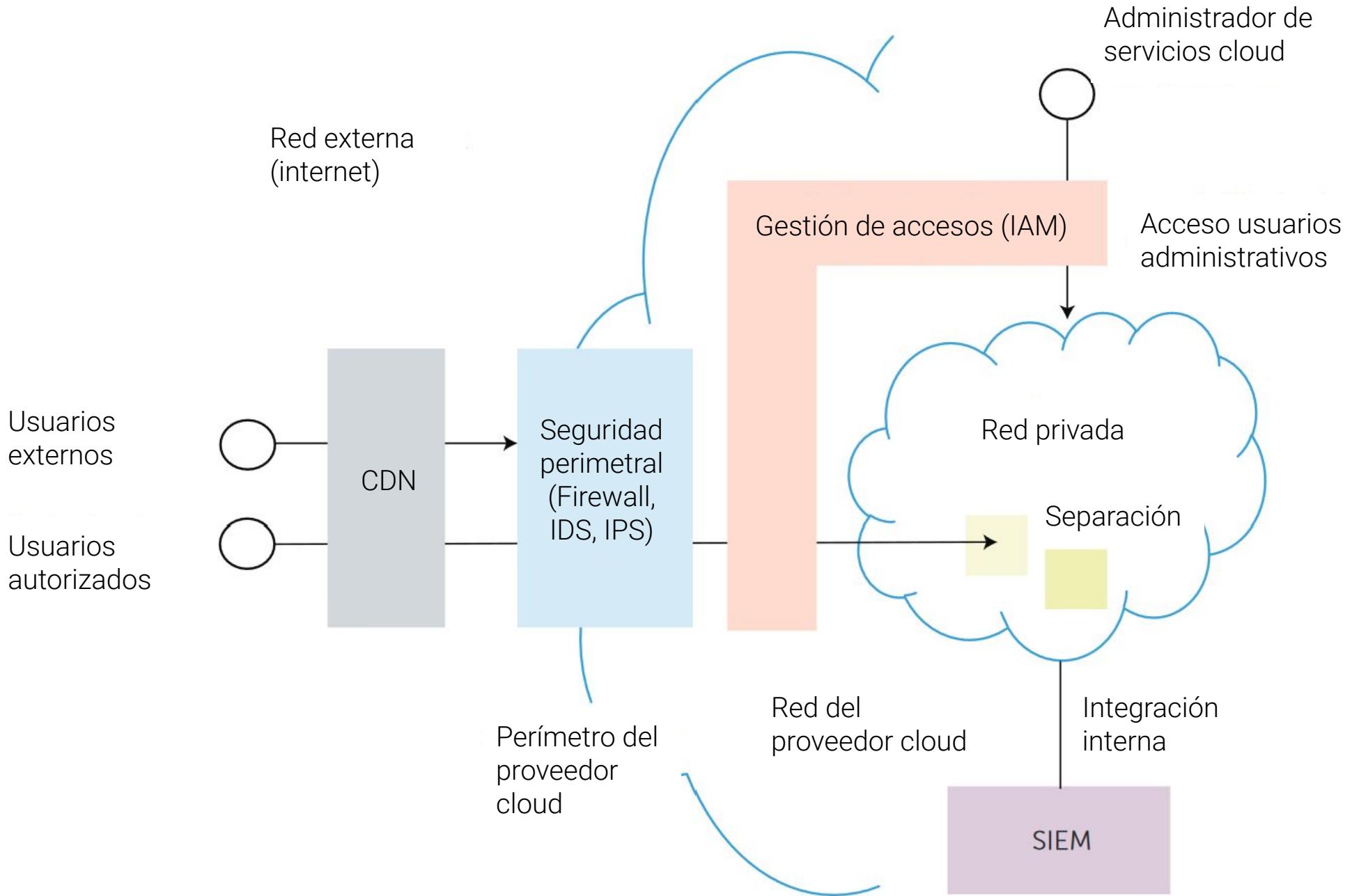
Seguridad en la Nube

¿Qué es?

Es la rama que se encarga específicamente de asegurar los sistemas de computación en la nube. Tiene varias intersecciones con las demás ramas de la seguridad; con algunas consideraciones especiales como el modelo de responsabilidad compartida.

Controles de Seguridad

- Perímetro de seguridad fuerte.
- IAM.
- Replicación.
- Observabilidad.
- Gobernanza.
- Compliance.
- Manejo de datos.



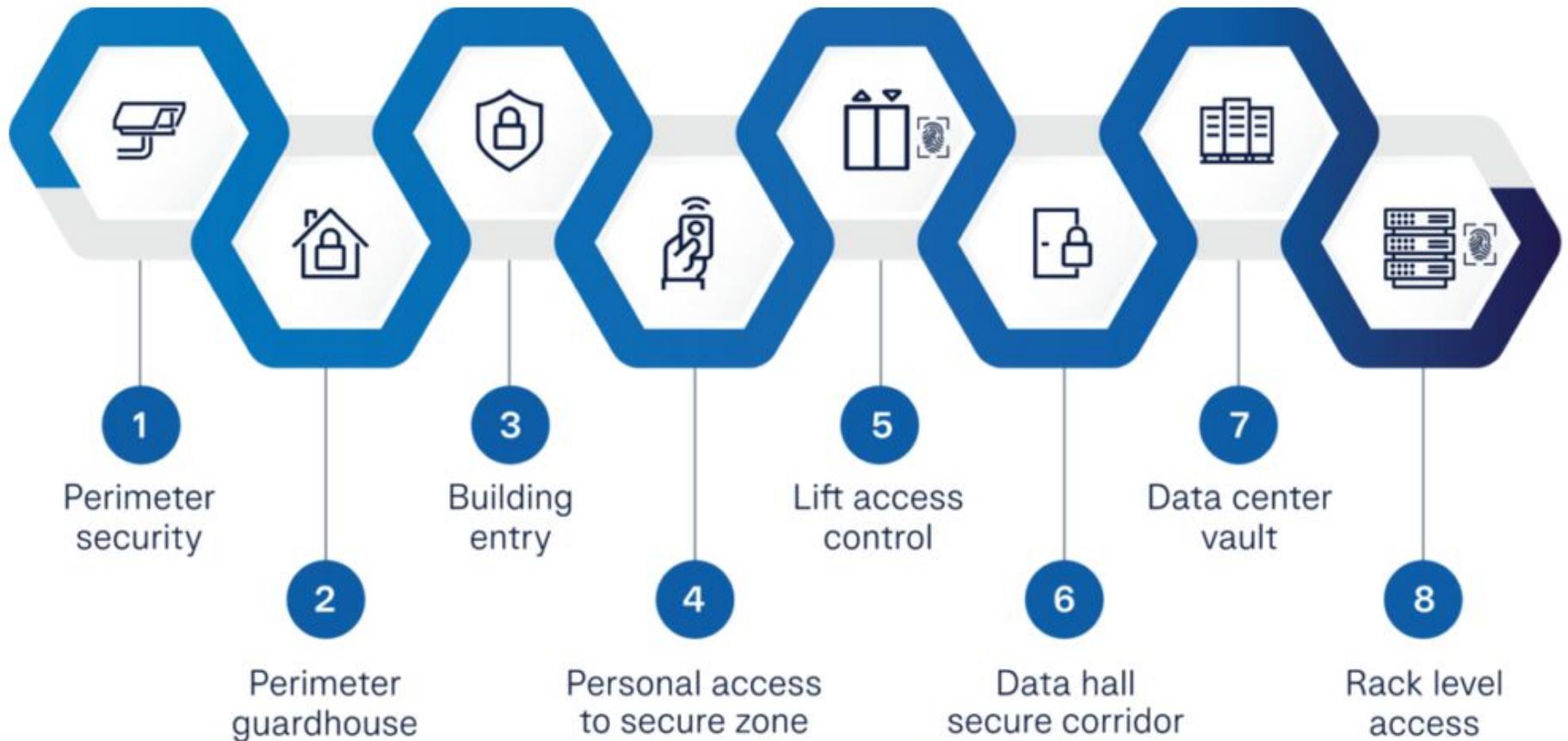
Seguridad Física

¿Qué es?

Es la rama que se atribuye la protección de los activos físicos de una organización mediante diferentes mecanismos y/o acciones de detección y prevención de riesgos.

Controles de Seguridad

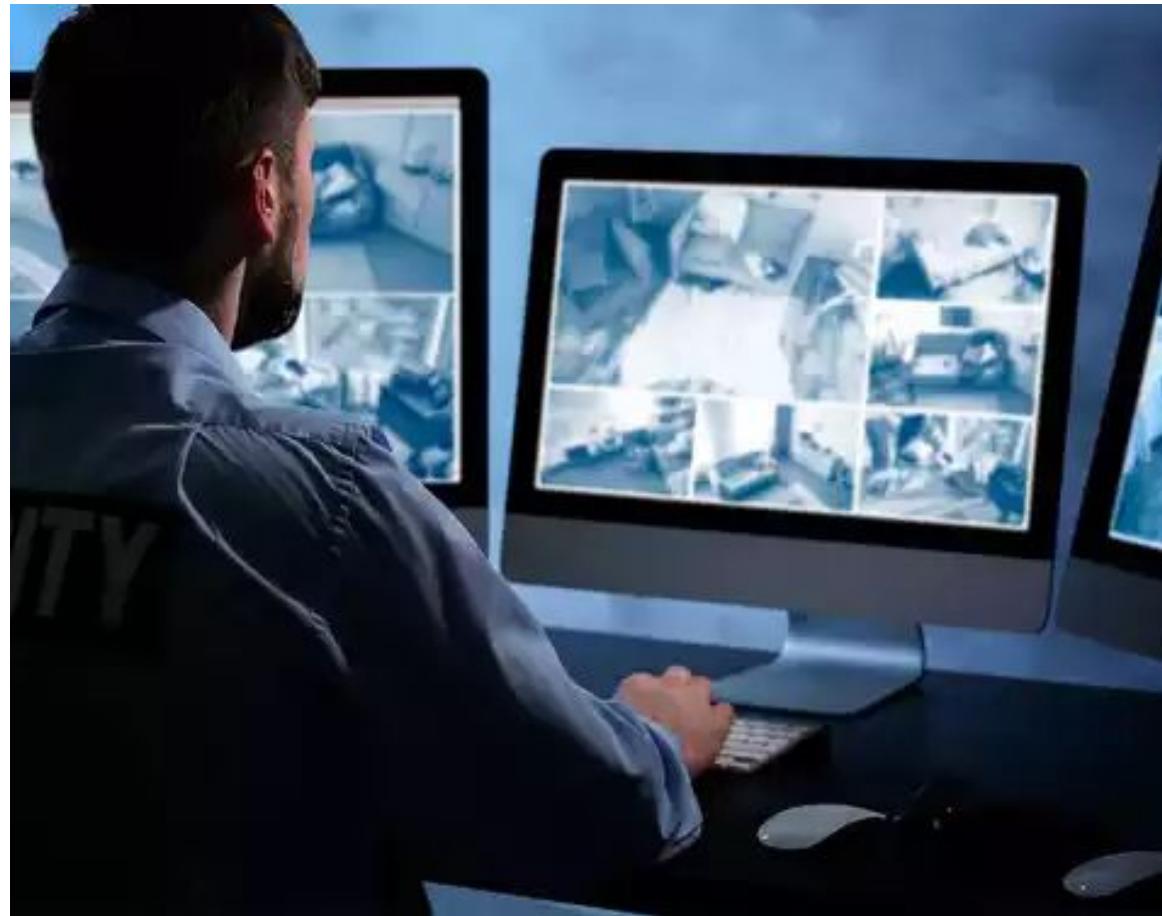
Capas de Seguridad



Control de Accesos



Sistemas de Vigilancia



Eliminación segura de información



Otras consideraciones



Cultura en Ciberseguridad

¿Qué es?

Son las ideas, costumbres y comportamientos sociales en una organización que impactan la seguridad de la información.

Principales elementos

- Actitudes
- Comportamientos
- Conocimiento
- Comunicación
- Cumplimiento
- Normas
- Responsabilidades

¿Por qué es
importante?

“

**El factor humano estuvo
involucrado en más del 85%
de brechas de seguridad.**

”

2021 Verizon Data Breach Investigations Report

Pasos para construir una cultura de seguridad fuerte

1. Crear objetivos estratégicos claros.
2. Medir el estado actual de la cultura.
3. Diseñar una estrategia de cambio cultural.
4. Ejecutar la estrategia de cambio cultural.
5. Revisión y mejora continua del proceso.

Recomendaciones

- Proceso constante y sin fin para crear resonancia dentro de los empleados.
- Tener un responsable directo de cuidar la cultura.
- Debe involucrar todos los niveles de la empresa.
- Hacerlo parte de la evaluación de los empleados.
- Realizar simulacros.

Malware

¿Qué es Malware?

Software malicioso
creado para causar
daño.

Afecta todo tipo de
dispositivos y
sistemas operativos.

```
1 PCHAR RC2Crypt_PackEncodedBuffer(PCHAR Buf, DWORD BufSize, PCHAR IV)
2 {
3     PCHAR Result = STR::Alloc(BufSize + 8);
4     if (Result == NULL)
5         return NULL;
6
7     PCHAR P = Result;
8
9     STR::Copy(IV, P, 0, 4);
10    P += 4;
11
12    PCHAR End = Buf + BufSize;
13    while (End > Buf && *(End - 1) == '=') End--;
14
15    STR::Copy(Buf, P, 0, End - Buf);
16    P += End - Buf;
17
18    STR::Copy(IV, P, 4, 4);
19    P += 4;
20
21    STR::Copy(End, P, 0, BufSize - (End - Buf));
22
23    return Result;
24 }
```

¿Qué puede hacer?

- **Crack passwords**

Descubrir contraseñas débiles almacenadas en el sistema operativo.

- **Intrusión**

Permitir acceso a sistemas críticos por línea de comando (*shell*) o similar.

¿Qué puede hacer?

- **Movimiento lateral**

Replicarse y actuar en un mismo segmento de red o VLAN.

- **Disponibilidad**

Afectar la operatividad de sistemas vitales para la empresa.

¿Qué puede hacer?

- **Cryptojacking**

Utiliza procesamiento para minería de cripto-divisas.

- **Secuestro de datos**

Alterar la integridad de información y/o datos personales.

¿Qué puede hacer?

- **Zombie**

Controlar equipos remotamente para generar ciberataques dirigidos (BotNet).

Tipos de Malware



Virus
Modifica otros
programas para
difundirse.

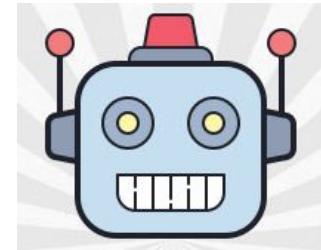


Ransomware
Cifra archivos y
cobra por rescate.

Tipos de Malware



Spyware
Accede passwords,
keystrokes o similar.



Bots
Ejecutan ciberataques
dirigidos.

Ejemplo

 Comparendo 2475569 SIMIT	8/18/2020 9:09 AM	Microsoft Word 97 - 2003 Document	239 K
 Rama Judicial proceso 2019	11/22/2019 10:46 AM	Rich Text Format	41 K



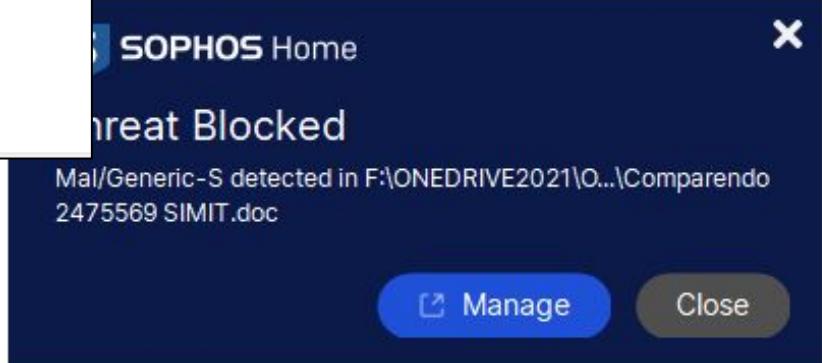
Amenaza detectada

Aplicación, archivo o contenido detectado como malicioso y debe limpiarse

Mal/Generic-S

F:\ONEDRIVE2021\OneDrive - UPB\SHARED\Virus\Comparendo 2475569 SIMIT.doc

miércoles, julio 13, 2022 9:33 a. m.

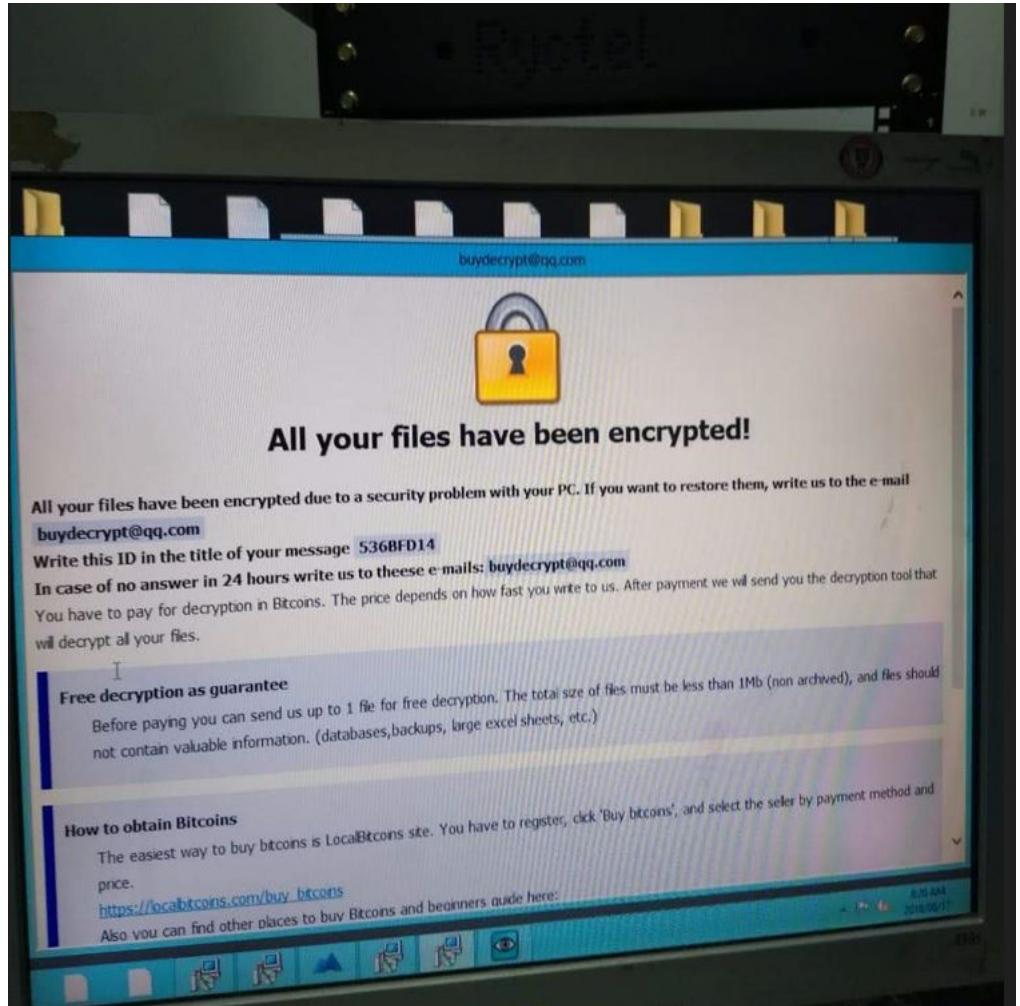


Ransomware

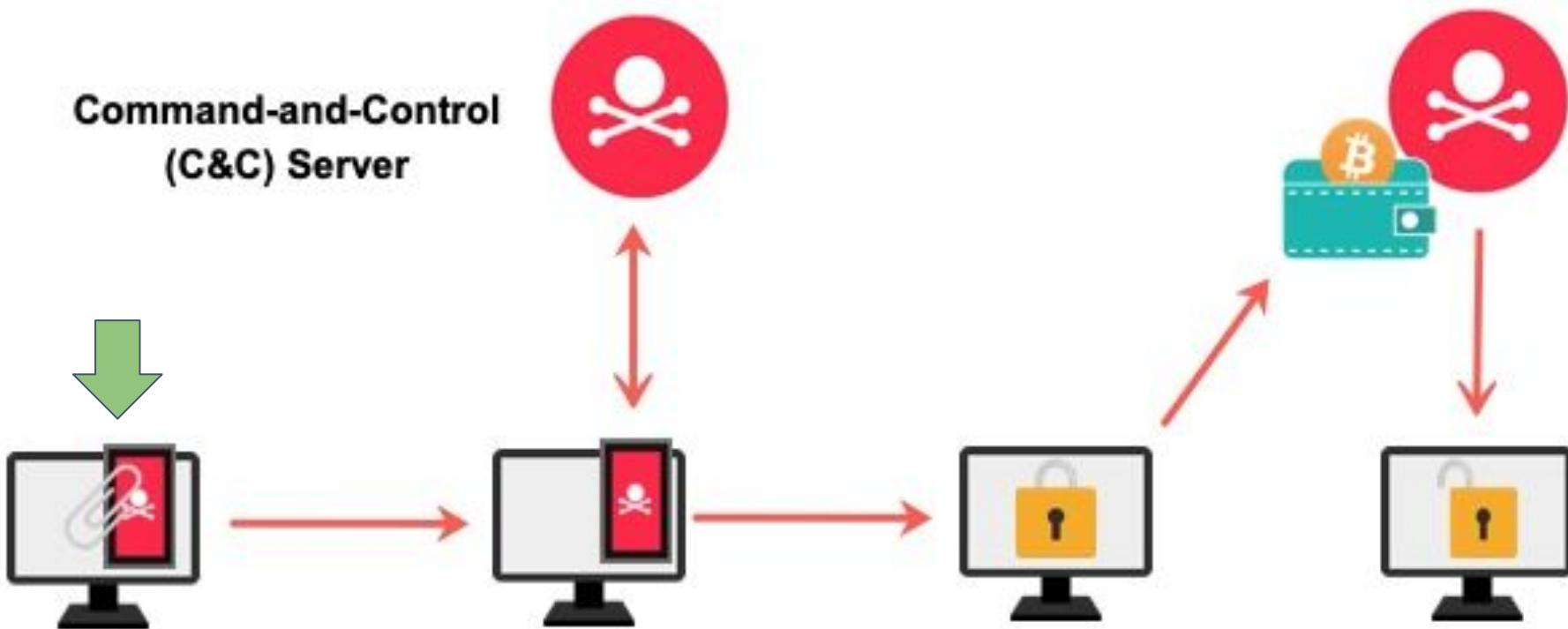
¿Qué es Ransomware?

Malware que utiliza técnicas de cifrado altamente robusto.

Muy lucrativo para ciberdelincuentes y casi siempre es dirigido a empresas.



¿Cómo opera?



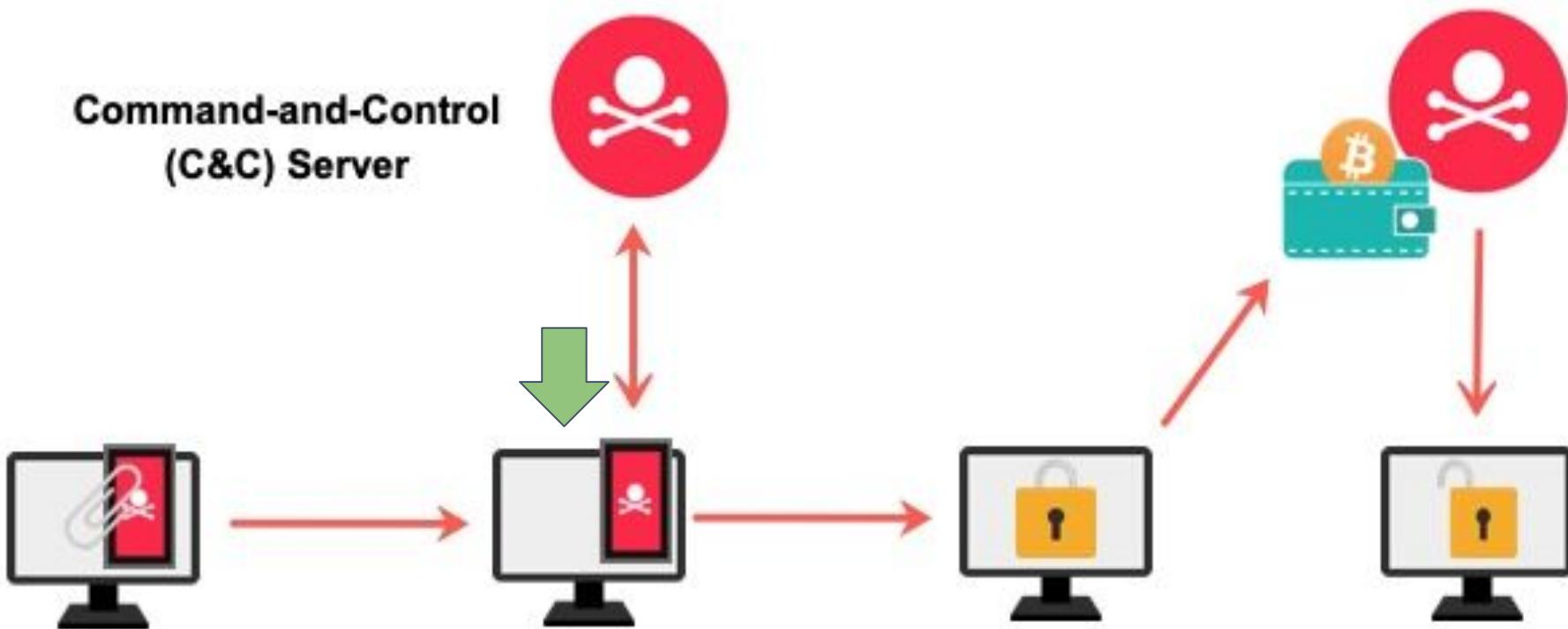
The victim acquires ransomware from email, exploit, or worm.

The ransomware malware contacts the attacker's C&C server and downloads a public key.

Data is encrypted and a ransom note provides ransom fee instructions.

After the ransom is paid, the attacker sends private key to decrypt data.

¿Cómo opera?



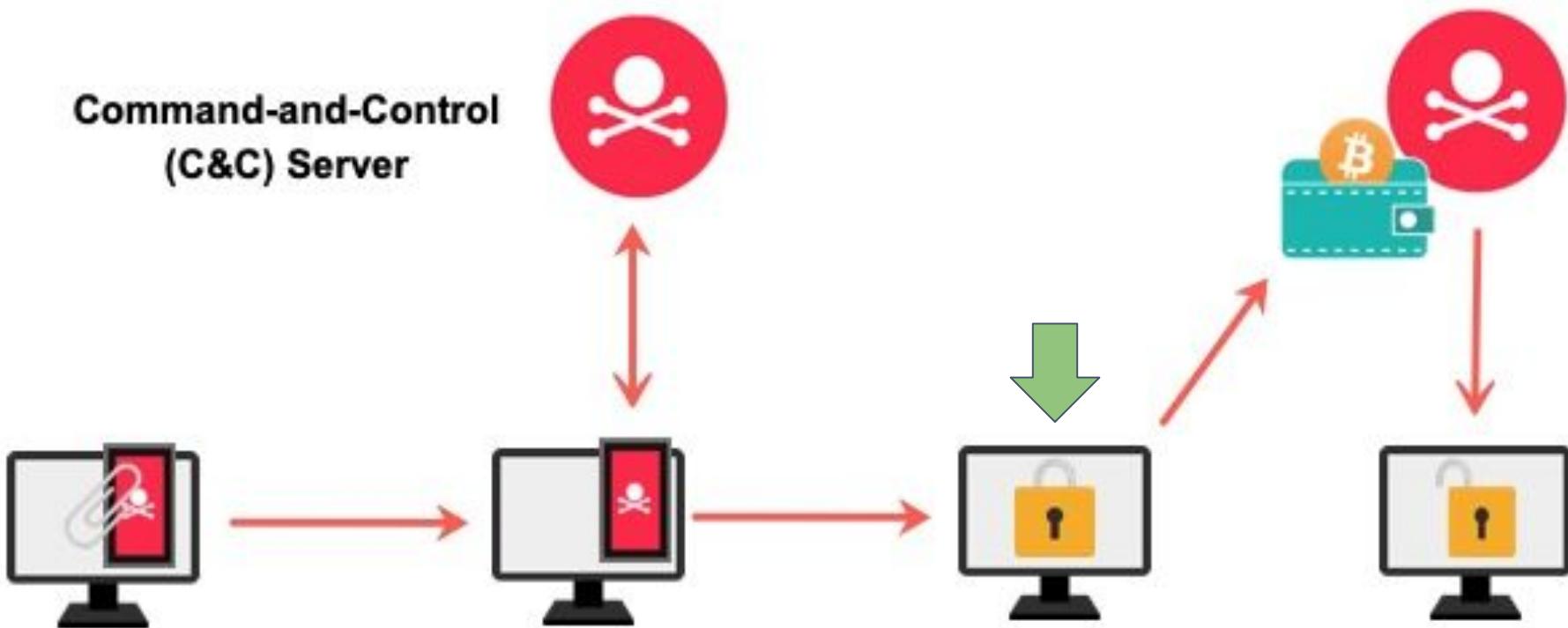
The victim acquires ransomware from email, exploit, or worm.

The ransomware malware contacts the attacker's C&C server and downloads a public key.

Data is encrypted and a ransom note provides ransom fee instructions.

After the ransom is paid, the attacker sends private key to decrypt data.

¿Cómo opera?



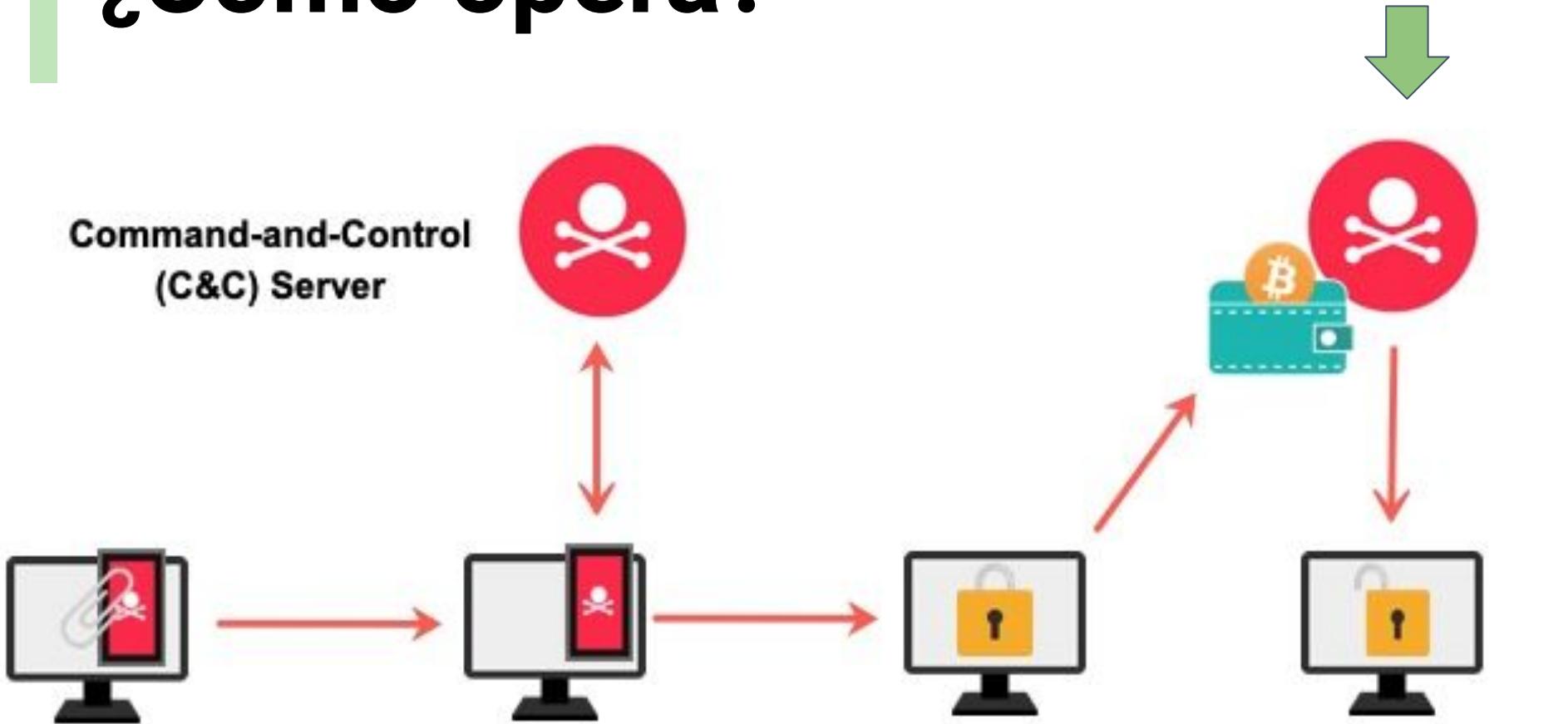
The victim acquires ransomware from email, exploit, or worm.

The ransomware malware contacts the attacker's C&C server and downloads a public key.

Data is encrypted and a ransom note provides ransom fee instructions.

After the ransom is paid, the attacker sends private key to decrypt data.

¿Cómo opera?



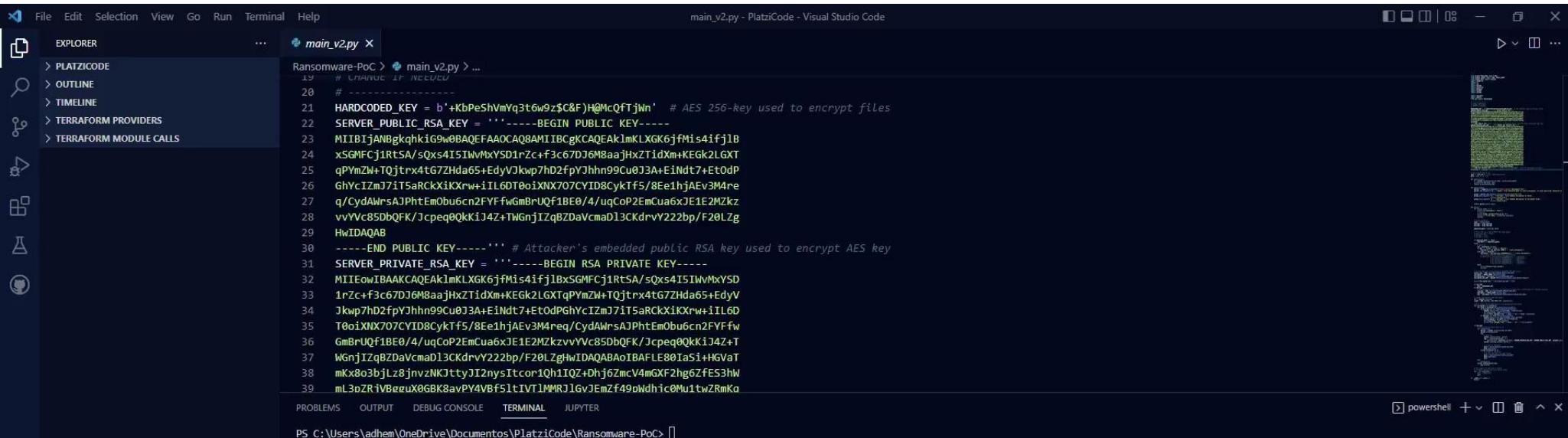
The victim acquires ransomware from email, exploit, or worm.

The ransomware malware contacts the attacker's C&C server and downloads a public key.

Data is encrypted and a ransom note provides ransom fee instructions.

After the ransom is paid, the attacker sends private key to decrypt data.

¡Ransomware en acción!



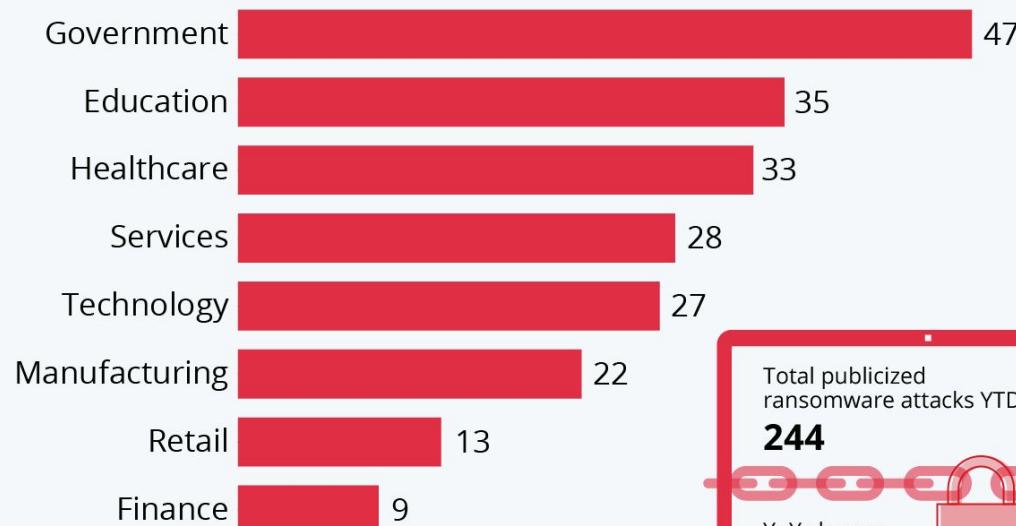
The screenshot shows a Visual Studio Code interface with a dark theme. The title bar reads "main_v2.py - PlatziCode - Visual Studio Code". The left sidebar has sections for "EXPLORER", "OUTLINE", "TIMELINE", "TERRAFORM PROVIDERS", and "TERRAFORM MODULE CALLS". The main editor area displays a Python script named "main_v2.py". The code is a ransomware PoC, containing hardcoded AES keys and RSA keys, file encryption logic, and communication with a server. The terminal tab at the bottom shows the command "PS C:\Users\adhem\OneDrive\Documentos\PlatziCode\Ransomware-PoC> []".

```
Ransomware-PoC > main_v2.py > ...
  # CHANGE IP IF NEEDED
20 #
21 HARDCODED_KEY = b'+KbPeShVmYq3t6w9z$c&F)H@McQfTjWn' # AES 256-key used to encrypt files
22 SERVER_PUBLIC_RSA_KEY = ''-----BEGIN PUBLIC KEY-----
23 MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAKlmKLXGK6jfMis4ifjlB
24 x5GMFCj1RtSA/sQxs4I5IwVlxYS01rZc+f3c67DjGm8aajhxZtidXm+KEgk2LGXT
25 qPMzW+TQjtrx4tG7ZHda65+EdyVkjup7hD2fpYJhhn99Cu0j3A+EiNdt7+Et0dP
26 GHycIZmJ7iTsaRckXkiXrw+iIL6D0i0iXNX707CYID8CykTf5/8Ee1hjAEv3M4re
27 q/CydAWrsAJPhEmObu6cn2FYFfwGmBrUQf1BE0/4/uqCoP2EmCua6xE1E2Mzkz
28 vVVc85DbQFK/Jcpeq0KKiJ4Z+TwGnjIZqBZDaVcmad13CKdrvY222bp/F20Lzg
29 HwIDAQAB
30 -----END PUBLIC KEY-----'' # Attacker's embedded public RSA key used to encrypt AES key
31 SERVER_PRIVATE_RSA_KEY = ''-----BEGIN RSA PRIVATE KEY-----
32 MIIEcwIBAAKCAQEAKlmKLXGK6jfMis4ifjlBx5GMFCj1RtSA/sQxs4I5IWVmXySD
33 1rZc+f3c67D16M8aajhxZtidXm+KEgk2LGXTqPMzW+TQjtrx4tG7ZHda65+EdyV
34 jkwp7hd2fpYJhhn99Cu0j3A+EiNdt7+Et0dP GhYcIZmJ7iTsaRckXkiXrw+iIL6D
35 T0oiXNX707CYID8CykTf5/8Ee1hjAEv3M4req/CydAWrsAJPhEmObu6cn2FYFfw
36 GmBrUQf1BE0/4/uqCoP2EmCua6xE1E2MzkzvvYVc85DbQFK/Jcpeq0KKiJ4Z+T
37 WGNjIZqBZDaVcmad13CKdrvY222bp/F20Lzg HwIDAQABoIBAFL80IaSi+HgVaT
38 mKx8o3bjLz8jnvzNKJttyJI2nysItcor1Qh1IQZ+Djh6ZmcV4mGXF2hg6ZfES3hW
39 mL3oRIVBeeuX0G8k8avPV4VBF51tIVT1MMRJ1gvEmZf49oWdhic0Mu1twZRmkA
```

¿Debemos preocuparnos?

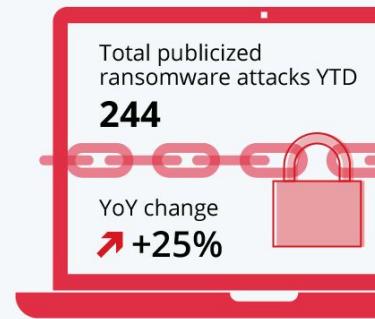
The Industries Most Affected by Ransomware

Number of publicized ransomware attacks worldwide by sector in 2021*



* As of Nov 1, 2021

Source: Blackfog



Factores de Riesgo

- **Direcciones IP públicas sin auditar**
Servicios Web, IoT, BBDD o similares con visibilidad en Internet.
- **Firewall ausente o sin tunning**
No existen dispositivos de control perimetral debidamente configurados.

Factores de Riesgo

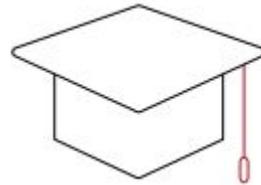
- **Carencia de Endpoint Protection**
Sistemas Operativos sin software antivirus o antimalware instalado y actualizado.
- **No existen prácticas de Hardening**
Servicios IT internos con instalaciones/configuraciones por defecto.

Factores de Riesgo

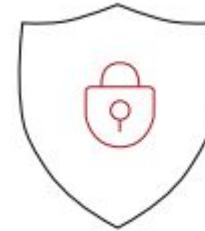
- **Falta de Cultura en Seguridad**

No existe *Cultura Organizacional en Seguridad de la Información* aplicada a procesos internos.

Ciber-Controles

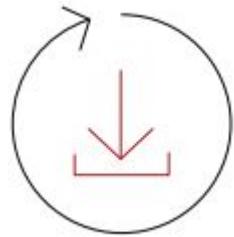


Educar a TODO el equipo y stakeholders.

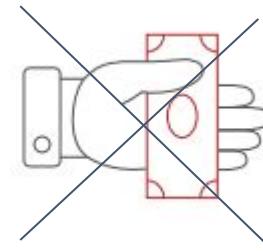


Asegurar TODOS los activos de información.

Ciber-Controles



Respaldar información
de alta importancia.



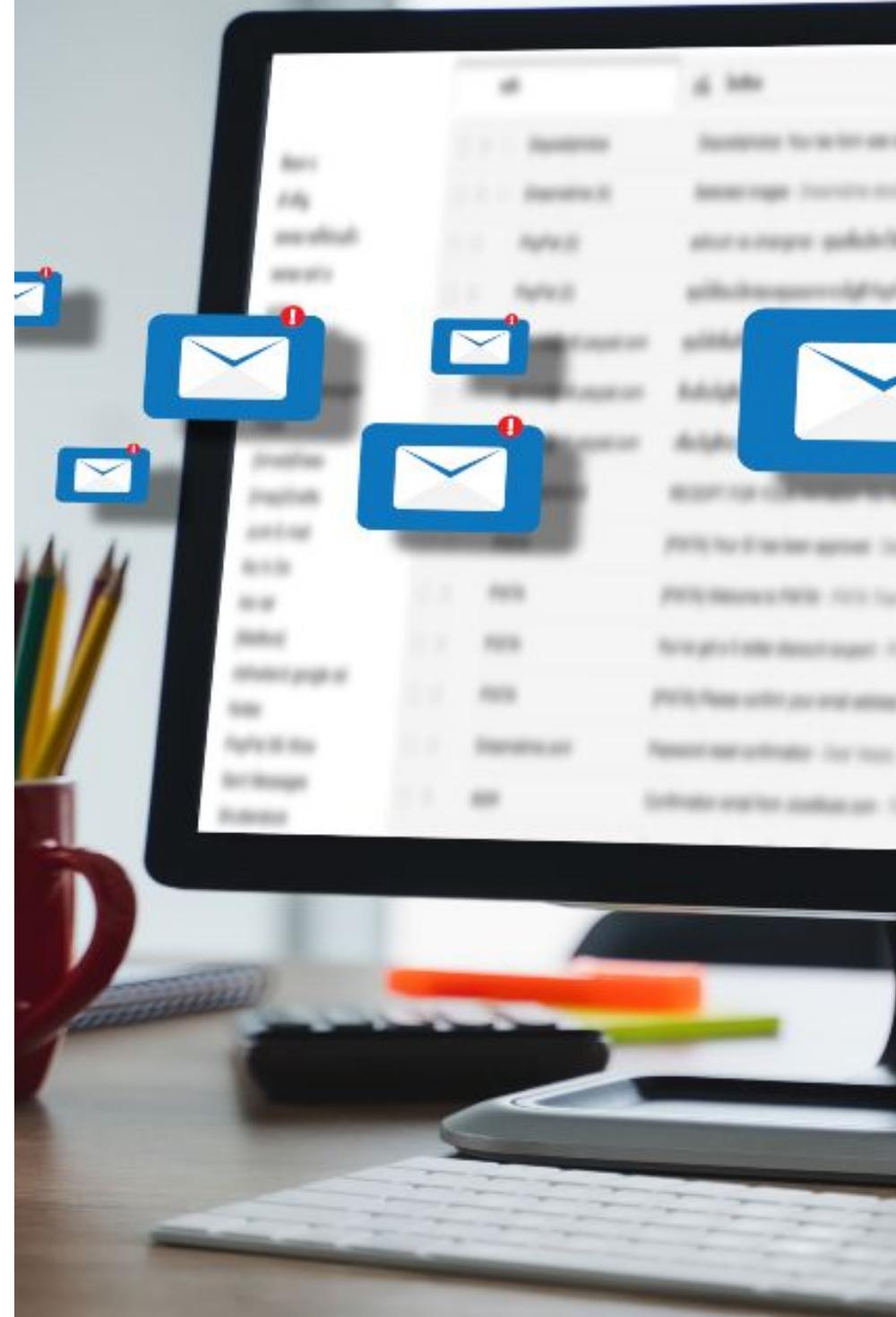
NUNCA pagar por
rescate.

Ingeniería Social

Definición

Interacciones y técnicas utilizadas por ciberdelincuentes para ejecutar delitos.

Utiliza manipulación psicológica motivada por gustos o tendencias.



Ciclo de vida

Investigation

- Identificación de víctima
- Captura de información
- Método de ataque



Ciclo de vida

Hook

- Enlace exitoso con víctima
- Control de la interacción



Ciclo de vida

Play

- Ejecución de ataque
- Obtención de información



Ciclo de vida

Exit

- Cierre de interacción
- Eliminación de evidencia



Modalidades

H Her [REDACTED]

To: [REDACTED]

Sat 2/12/2022 7:04 AM

500 dólares pueden darte 3000 dólares a través de una inversión en bitcoins. Siga el enlace para saber cómo <https://api.whatsapp.com/send?phone=12342814250>



Andre
Business Account
api.whatsapp.com

número de whatsapp estados unidos +1(234) 281-4250



+1 (234) 281-4250

last seen today at 8:11 AM



Get notified of new messages
Turn on desktop notifications >



Search or start new chat



Archived



+1 (405) 259-7816

11:03 AM

Según nuestro agente estás interesado en ...



+1 (234) 281-4250

1:17 AM

¿Cuál es tu nombre querida? Cuando escr...

YESTERDAY

🔒 Messages are end-to-end encrypted. No one outside of this chat, not even WhatsApp, can read or listen to them. Click to learn more.

hola 10:00 PM ✓✓

me interesa 10:00 PM ✓✓

500 dólares pueden darte 3000 dólares a través de una inversión en bitcoins

10:00 PM ✓✓

TODAY

Sí, queridos 500 dólares pueden darte una buena ganancia de 3000 dólares.

12:46 AM

Si estás interesado, escribe al administrador en este número de WhatsApp. Él te dirá todo lo que necesitas saber y te alegrarás de haberlo hecho.

12:51 AM

+1 405 259 7816 12:51 AM

¿Cuál es tu nombre querida? Cuando escribas al administrador me avisas ok

1:17 AM

 +1 (405) 259-7816  

 Get notified of new messages
Turn on desktop notifications >

 Search or start new chat

 Archived

 +1 (405) 259-7816 11:03 AM
Según nuestro agente estás interesado en ...

 +1 (234) 281-4250 1:17 AM
¿Cuál es tu nombre querida? Cuando escr...

TODAY

Hola 8:25 AM

Según nuestro agente estás interesado en invertir en bitcoin 11:03 AM

De: Hinze Pinelis [mailto:qgobearnardrh@outlook.com]

Enviado el: martes, 2 de octubre de 2018 7:30 p. m.

Para: [REDACTED]

Asunto: r [REDACTED] - mimi0120

I am well aware mimi0120 is your passwords. Lets get right to point. absolutely no one has compensated me to check
ering why you're getting this e mail?

Well, i setup a malware on the adult streaming (pornographic material) site and you know what, you visited this websi
tching videos, your browser started working as a Remote control Desktop with a key logger which gave me access to y
obtained your entire contacts from your Messenger, Facebook, and e-mailaccount. after that i created a video. First pa
lmao), and second part shows the view of your webcam, & it is u.

You do have just two choices. Shall we analyze the options in aspects:

First option is to dismiss this e mail. in this instance, i will send your very own recorded material to all of your contact
you be in a romance, precisely how it is going to affect?

in the second place choice will be to pay me \$9000. i will regard it as a donation. Then, i will right away erase your vi
ened and you will not hear back again from me.

You'll make the payment by Bitcoin (if you don't know this, search for 'how to buy bitcoin' in Google search engine).

BTC address to send to: 1JPD6bujHxXgtifkUZWnuTQ1kRc2Nz8BSN

[CaSe sensitive, copy & paste it]

Ciber-Controles

- **Validación de origen**

Descartar correos o contactos de dudosa procedencia.

- **2FA o MFA**

Fortalecer cuentas con doble o múltiple factor de autenticación.

Ciber-Controles

- **Cultura en Ciberseguridad**

Utilizar el sentido común y tener claro que “*no todo lo que brilla es oro*”.

Phishing

¿Qué es Phishing?

Técnica de ingeniería social utilizada para el robo de datos personales y financieros.

Normalmente, suplanta la identidad digital de empresas o bancos.



Técnicas de Phishing

- **Emails Scams**

El ciberdelincuente envía miles de falsos correos a usuarios/empresas que han comprometido sus datos.

- **Spear Phishing**

Ciberataque dirigido a empresas o sectores con previo conocimiento organizacional adquirido.

Ciber-Controles

- **Security-Education**

Campañas internas de concienciación en Ciberseguridad (*Gophish*) con métricas definidas.

- **2FA o MFA**

Fortalecer buzones de correo con doble o múltiple factor de autenticación.

Ciber-Controles

- **Denunciar enlaces**

Utilizar los servicios web diseñados para reportar casos de Phishing (Microsoft & Google).

Casos reales

10:19 📱 🌐 🌐 ⏱

📴 🔋 4G 🔋



col-13326.surge.sh

3



Sucursal Virtual Personas

Fecha y hora actual: Martes 21 de Junio de 2022

10:19:23 PM

Inicio de sesión

Usuario

Si no tienes un usuario asignado ingresa con tu documento de identidad

ⓘ Ingrresa tu usuario



Continuar

¿Olvidaste tu usuario?

¿Problemas para conectarte?

10:18 🌐 🌐 ⏱

📴 🔋 4G 🔋



col-13326.surge.sh

2



Sucursal Virtual Personas

Fecha y hora actual: Martes 21 de Junio de 2022

10:18:03 PM

Inicio de sesión

Por favor espera un momento estamos validando algunos datos.

Puede tardar entre 1 a 5 minutos. No cierres o recargues esta ventana.



Sucursal Telefónica Bancolombia: Bogotá 343 0000
- Medellín 510 9000 - Cali 554 0505 - Barranquilla
361 8888 - Cartagena 693 4400 - Bucaramanga 697

Casos reales

De: Upb Cloud-System <Oskar-Kuenkler@web.de>

Enviado: miércoles, 27 de mayo de 2020 8:04 a. m.

Para:

Asunto: Reporte- 38A309413

Office365



Servicio de cuenta.

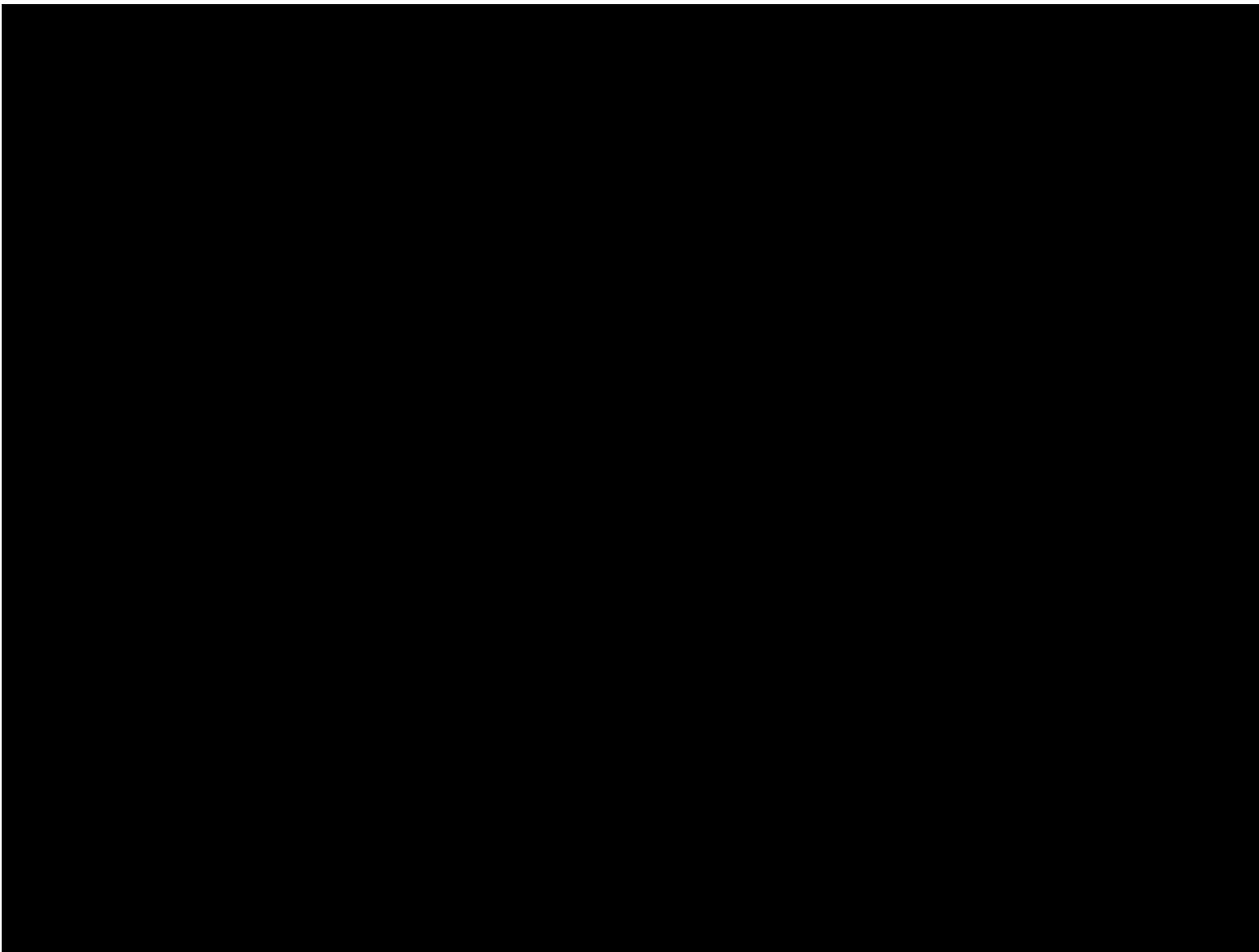
Tiene {5} correos electronicos no entregados agrupados en su nube debido a que la capacidad de almacenamiento de correo esta llena.

Esto hara que los correos electronicos entrantes se recuperen.:

Siga las instrucciones para resolver el problema y liberar correos electronicos pendientes. [Liberar mensajes](#) | [Limpiar correo](#)

Gracias

Phishing en acción!



Denegación de Servicios

¿Qué es Denegación de Servicio (DoS)?

- Ciberataque que afecta la disponibilidad de servicios tecnológicos por inundación de peticiones.
- Utiliza la generación excesiva de tráfico de red.

Tipos

- **Basados en volumen**

El objetivo es saturar el ancho de banda del sitio atacado (*UDP & ICMP*). Se mide en bits por segundo (Bps).

- **De protocolo**

consume los recursos del servidor o instancia (*SYN, Ping of Death*). Medible en paquetes por segundo (Pps).

Tipos

- **De capa de aplicación**

Generados por *request* masivos hacia servicios web hasta lograr *crashearlos*.

Se mide en *Request por segundo (Rps)*

Aplicación de DoS

- **Botnet y DDoS**

Redes de dispositivos *zombies* que generan ataques **Distribuidos** hacia objetivos específicos.

Caso real Botnet

Action	Botscore	Botscoresrcname	Clientasndescription	Clientasn	Clientcountrynam	Clientip
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited	45090	CN	42.193.253.152
managed_challenge	1	Heuristics	CLOUDDATA-NETWORKS-1	399955	HK	103.38.80.136
managed_challenge	1	Heuristics	CLOUDDATA-NETWORKS-1	399955	HK	103.38.80.136
managed_challenge	1	Heuristics	CLOUDDATA-NETWORKS-1	399955	HK	103.38.80.136
managed_challenge	1	Heuristics	CLOUDDATA-NETWORKS-1	399955	HK	103.38.80.136
managed_challenge	1	Heuristics	CLOUDDATA-NETWORKS-1	399955	HK	103.38.80.136
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	BPS-NETWORKS	36243	US	205.201.49.132
managed_challenge	1	Heuristics	CHINANET-SH-AP China Telecom Group	4812	CN	113.21.237.83
managed_challenge	1	Heuristics	CHINANET-SH-AP China Telecom Group	4812	CN	113.21.237.83

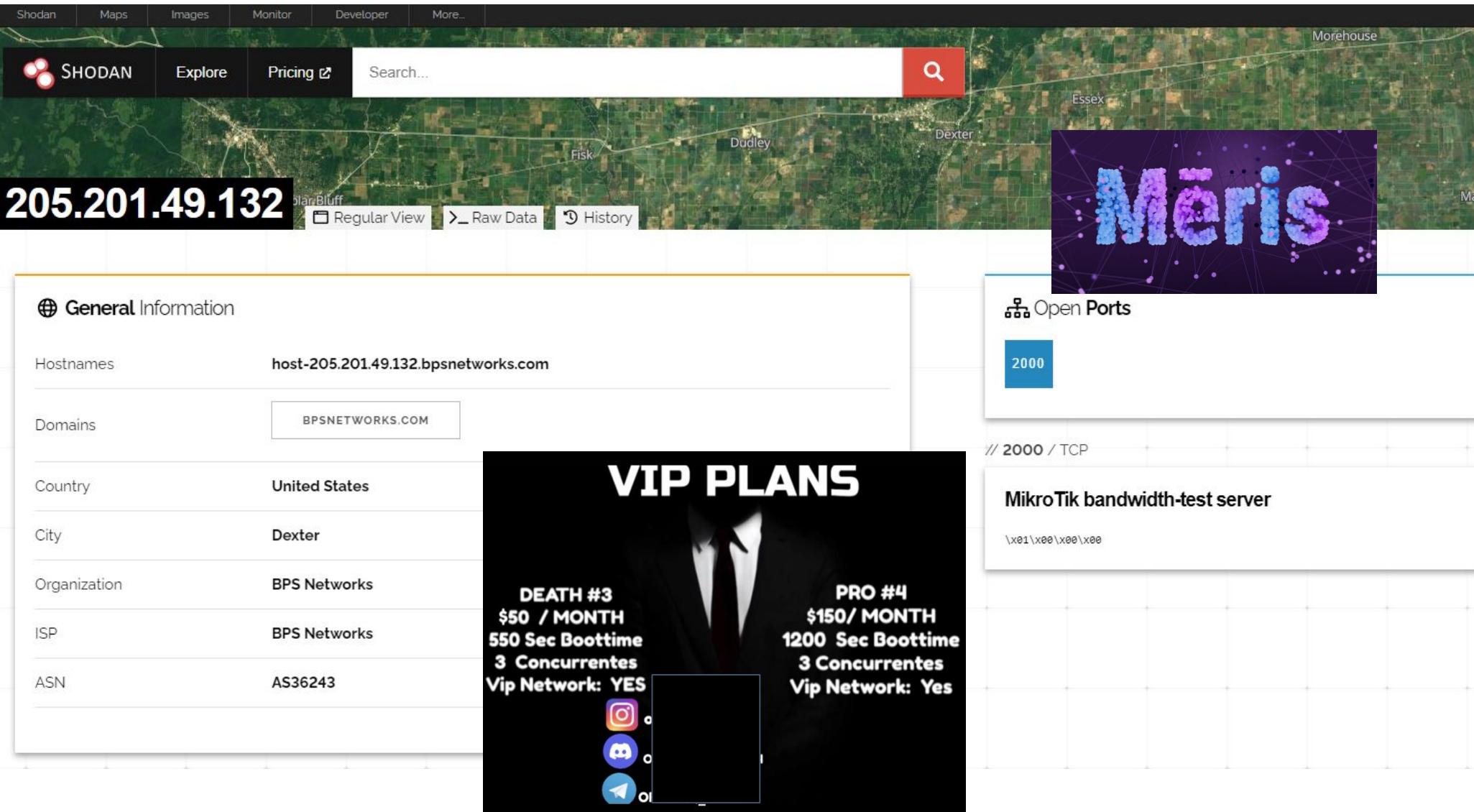
Shodan | Maps | Images | Monitor | Developer | More...

SHODAN Explore Pricing Search... 

205.201.49.132

Regular View Raw Data History

Fisk Dudley Essex Morehouse



General Information

Hostnames	host-205.201.49.132.bpsnetworks.com
Domains	BPSNETWORKS.COM
Country	United States
City	Dexter
Organization	BPS Networks
ISP	BPS Networks
ASN	AS36243



Open Ports

2000

// 2000 / TCP

MikroTik bandwidth-test server
\x01\x00\x00\x00

Ciber-Controles

- ***Security as a Service***

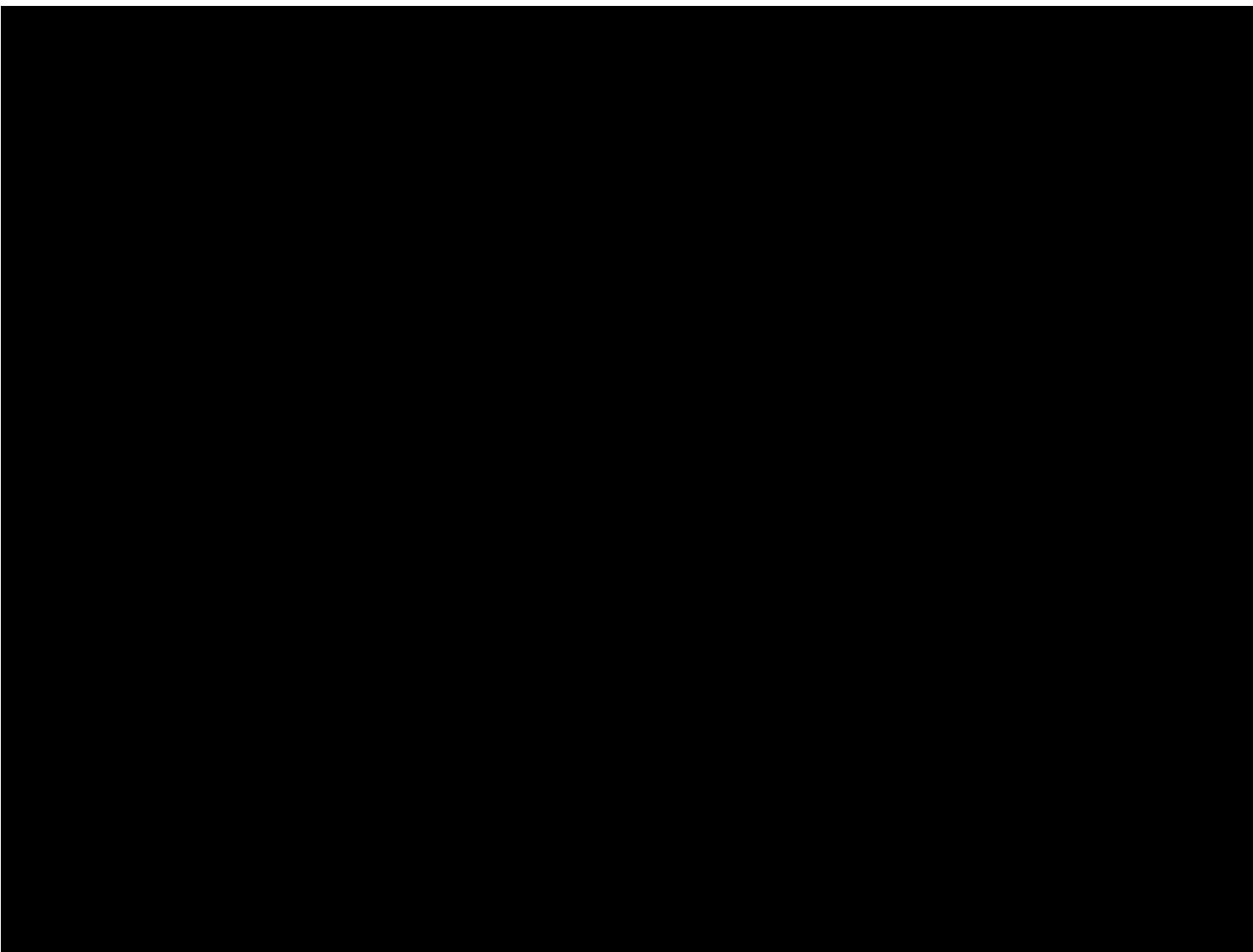
Adquirir soluciones integrales de seguridad que vinculen reglas y perfiles dedicados a controlar *DoS*.

- ***Hardening de servicios***

Aplicar robustecimiento de servicios + *Endpoint Protection* y evitar configuraciones por defecto.



¡DoS en acción!



Man-in-the-Middle

MitM

- Ciberataque que permite interceptar la comunicación *user-application*.
- Su objetivo es capturar información sensible y/o de alto riesgo.

Host List ✕

Targets ✕

Target 1

192.168.1.1

DeleteAdd

Target 2

192.168.1.103

192.168.1.102

192.168.1.101

192.168.1.100

Delete

Host 192.168.1.1 added to TARGET1

Host 192.168.1.103 added to TARGET2

Host 192.168.1.102 added to TARGET2

Host 192.168.1.101 added to TARGET2

Host 192.168.1.100 added to TARGET2

ARP poisoning victims:

GROUP 1 : 192.168.1.1 C4:6E:1F:50:75:60

GROUP 2 : 192.168.1.103 3C:77:E6:9E:B2:BB

GROUP 2 : 192.168.1.102 7C:F9:0E:E6:BF:B9

GROUP 2 : 192.168.1.101 00:24:D2:85:F1:D5

GROUP 2 : 192.168.1.100 E8:AB:FA:6B:17:02

Starting Unified sniffing...

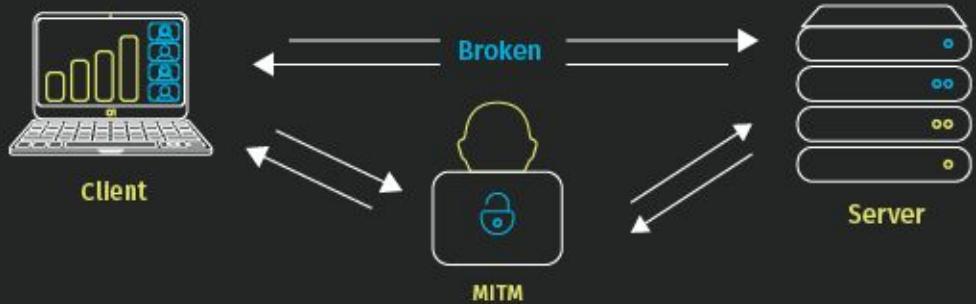
Work-Flow



Normal Flow



Man-in-the-Middle Flow



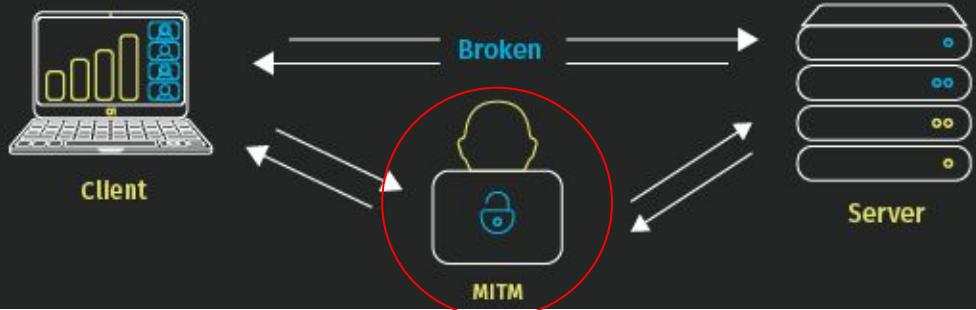
Work-Flow



Normal Flow



Man-in-the-Middle Flow

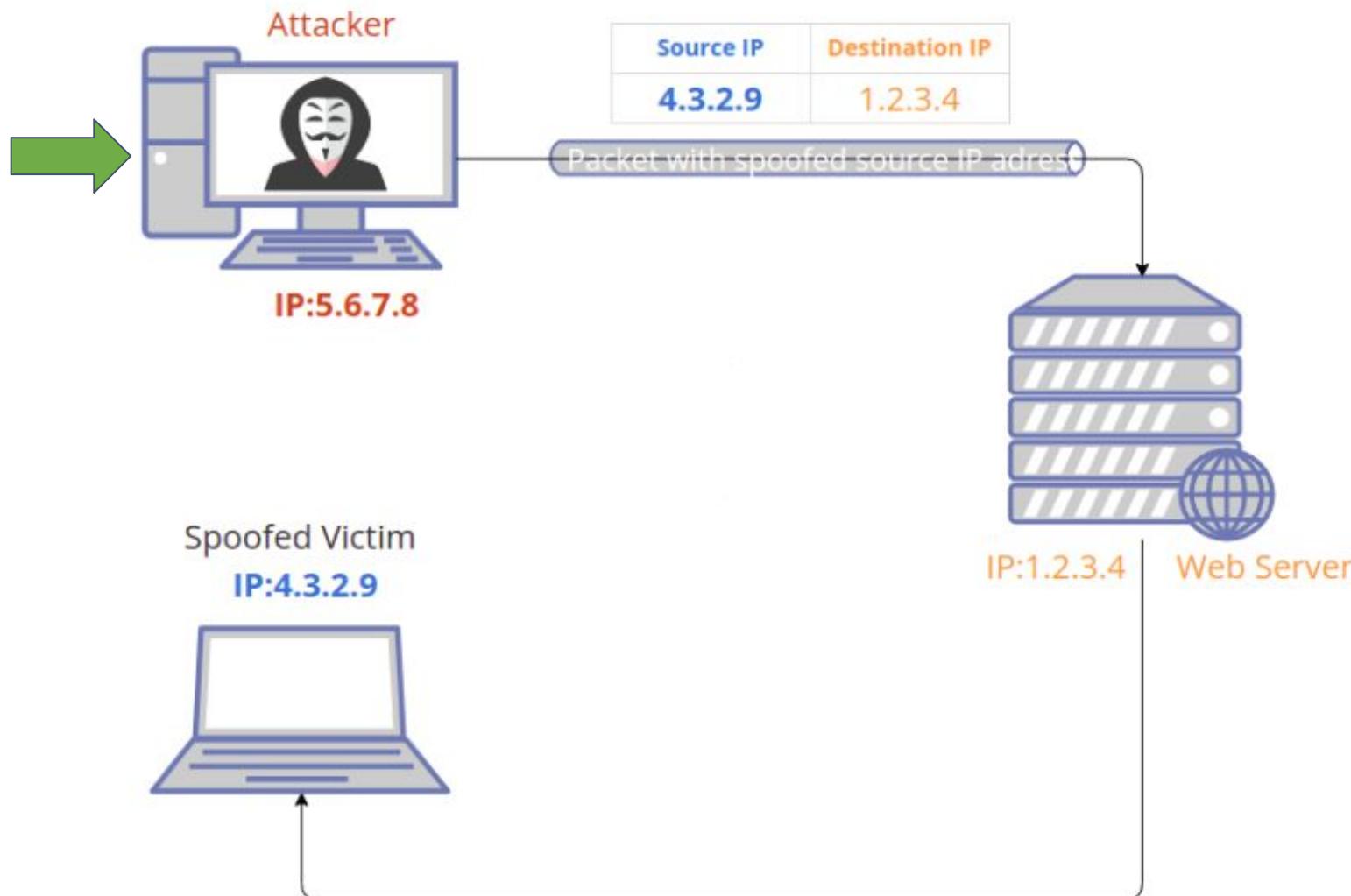


Tipos de MitM

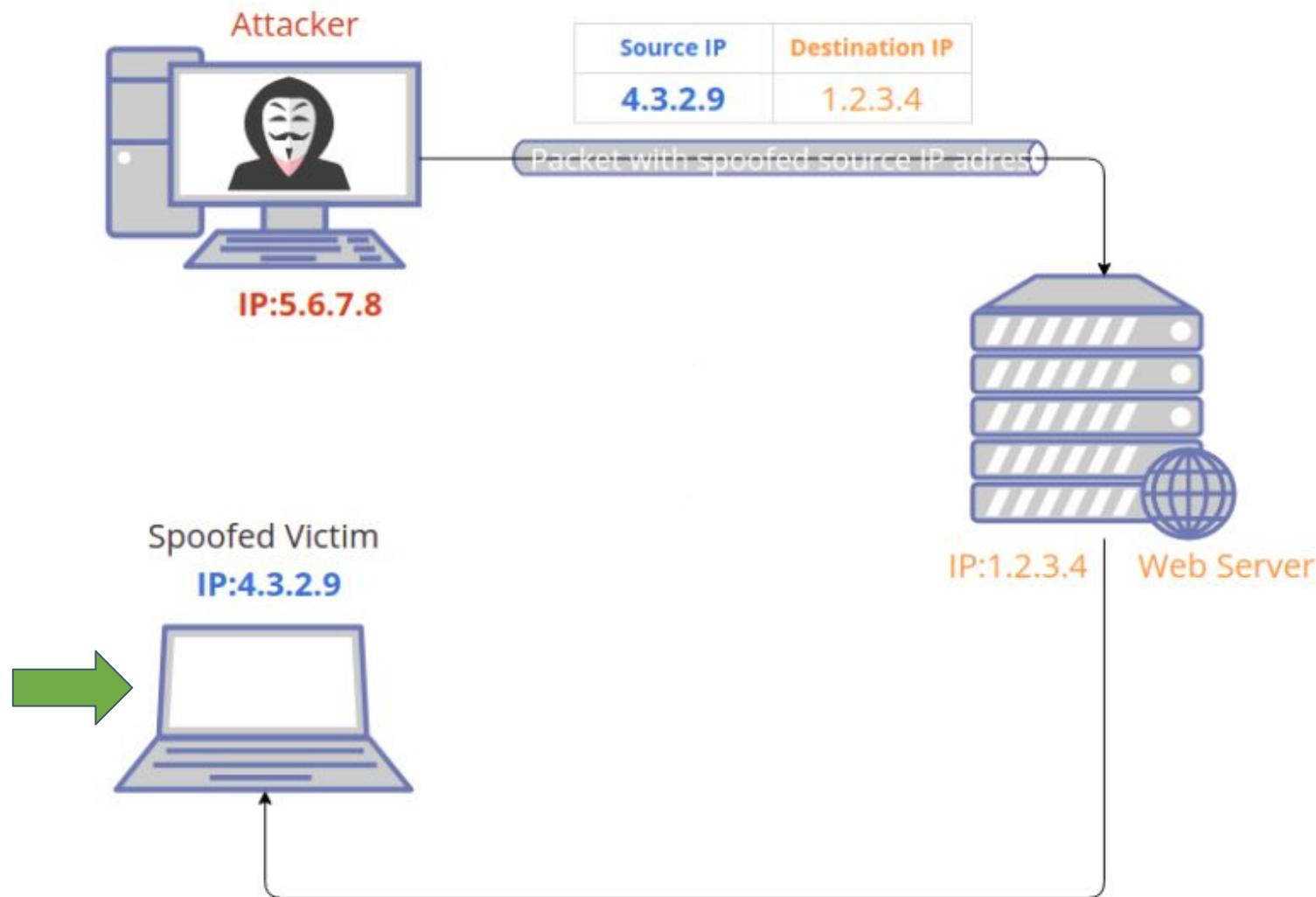
- **IP Spoofing**

Se alteran *packet headers* para suplantar una dirección IP.

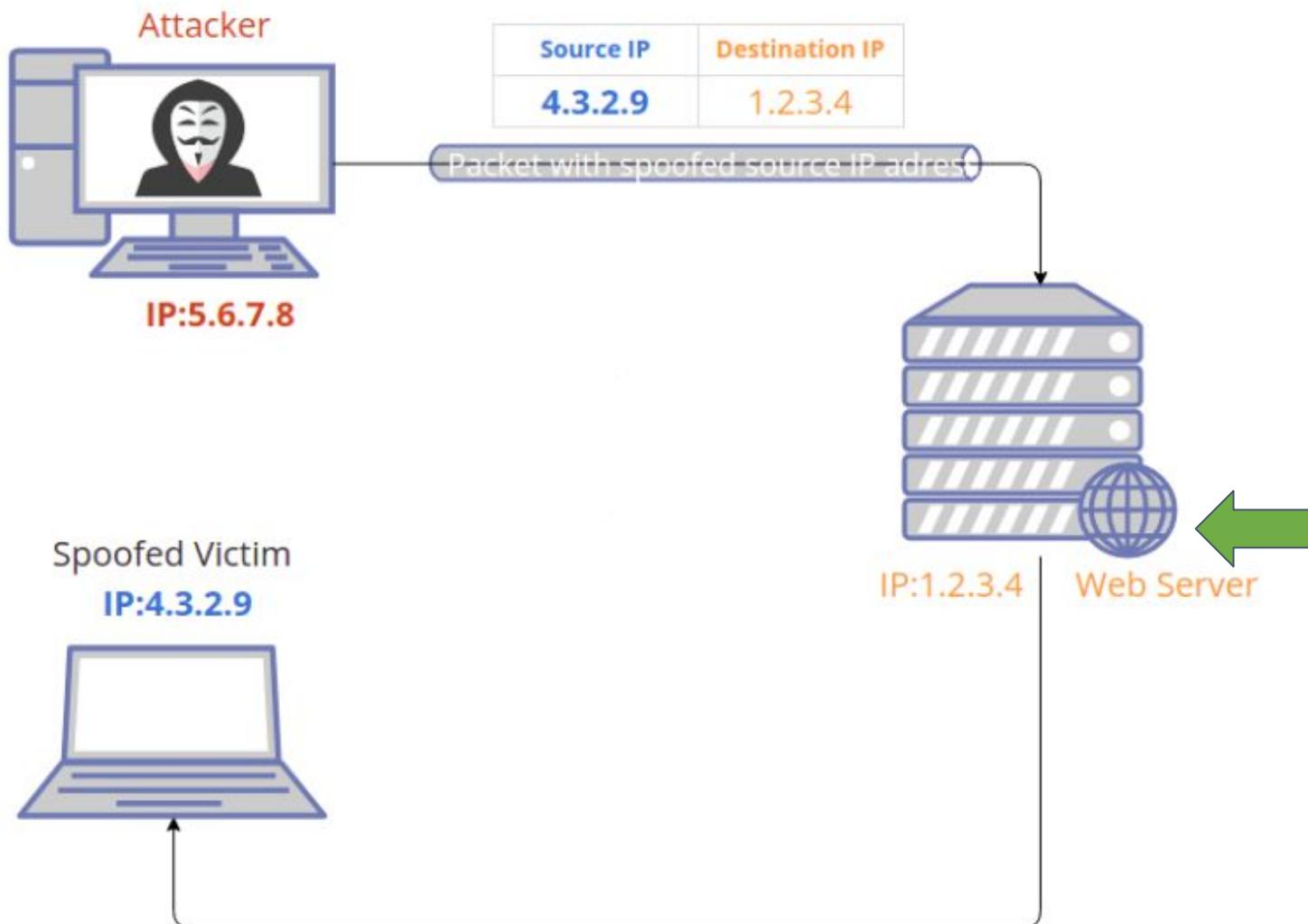
IP Spoofing



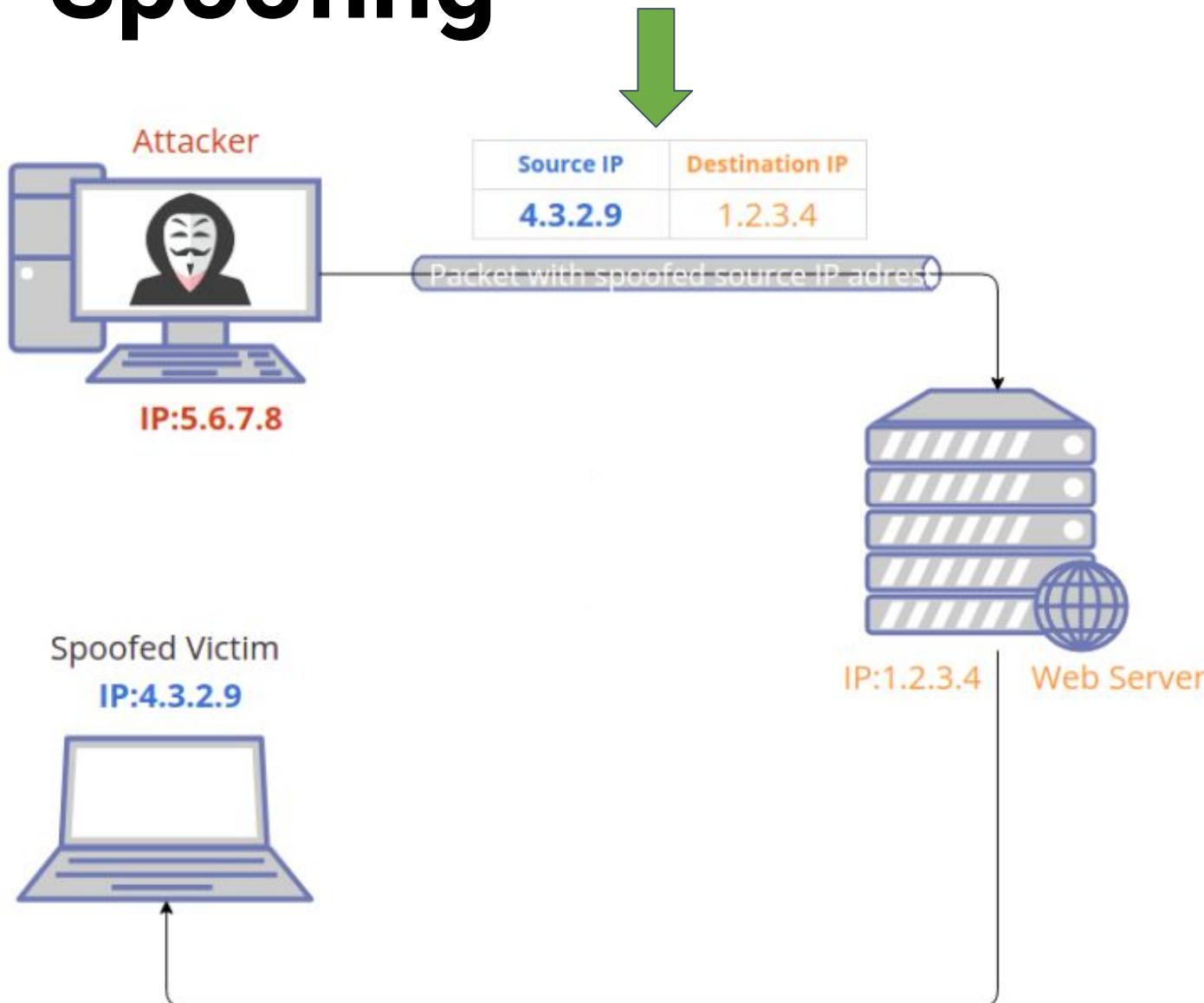
IP Spoofing



IP Spoofing



IP Spoofing

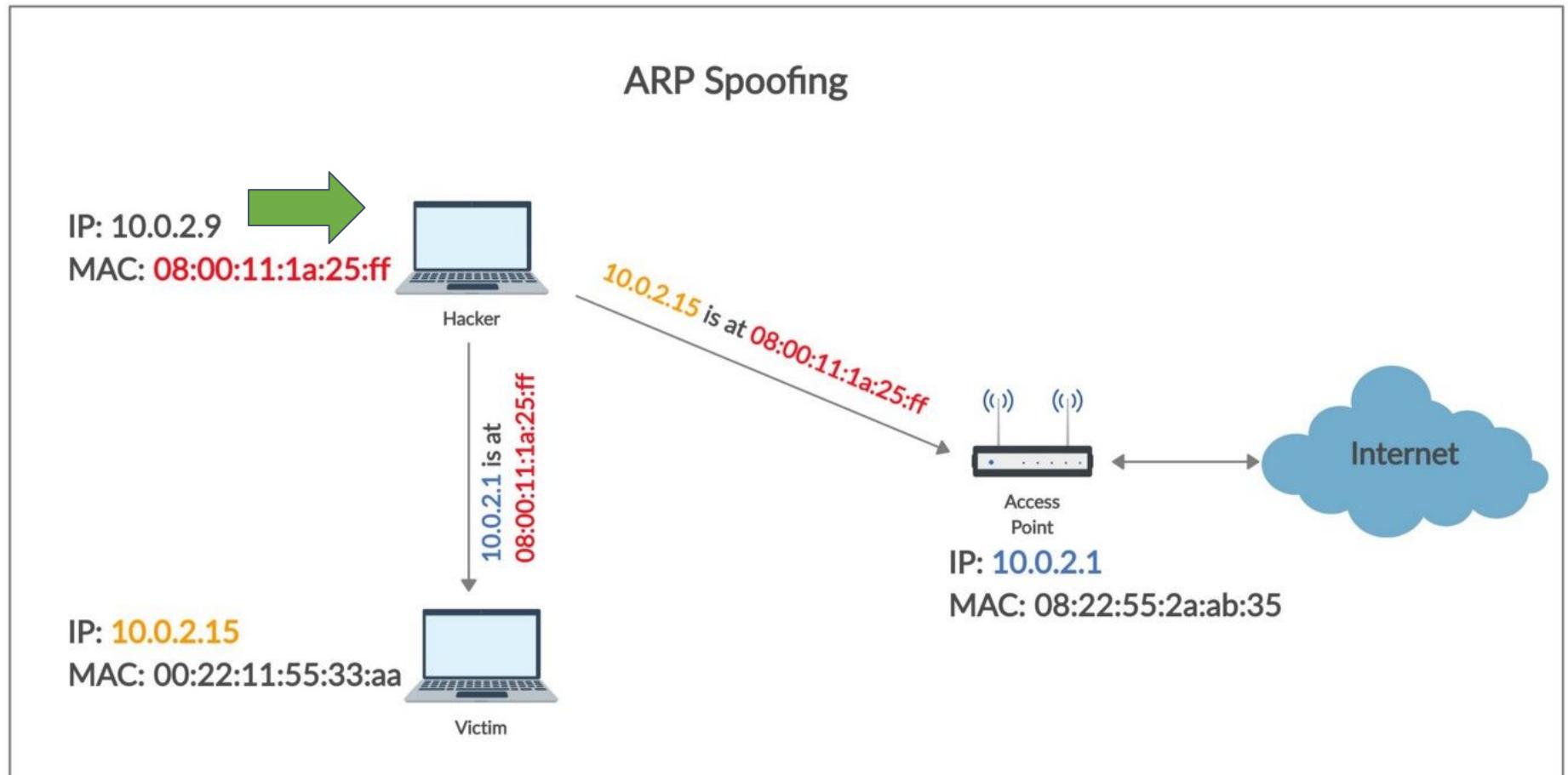


Tipos de MitM

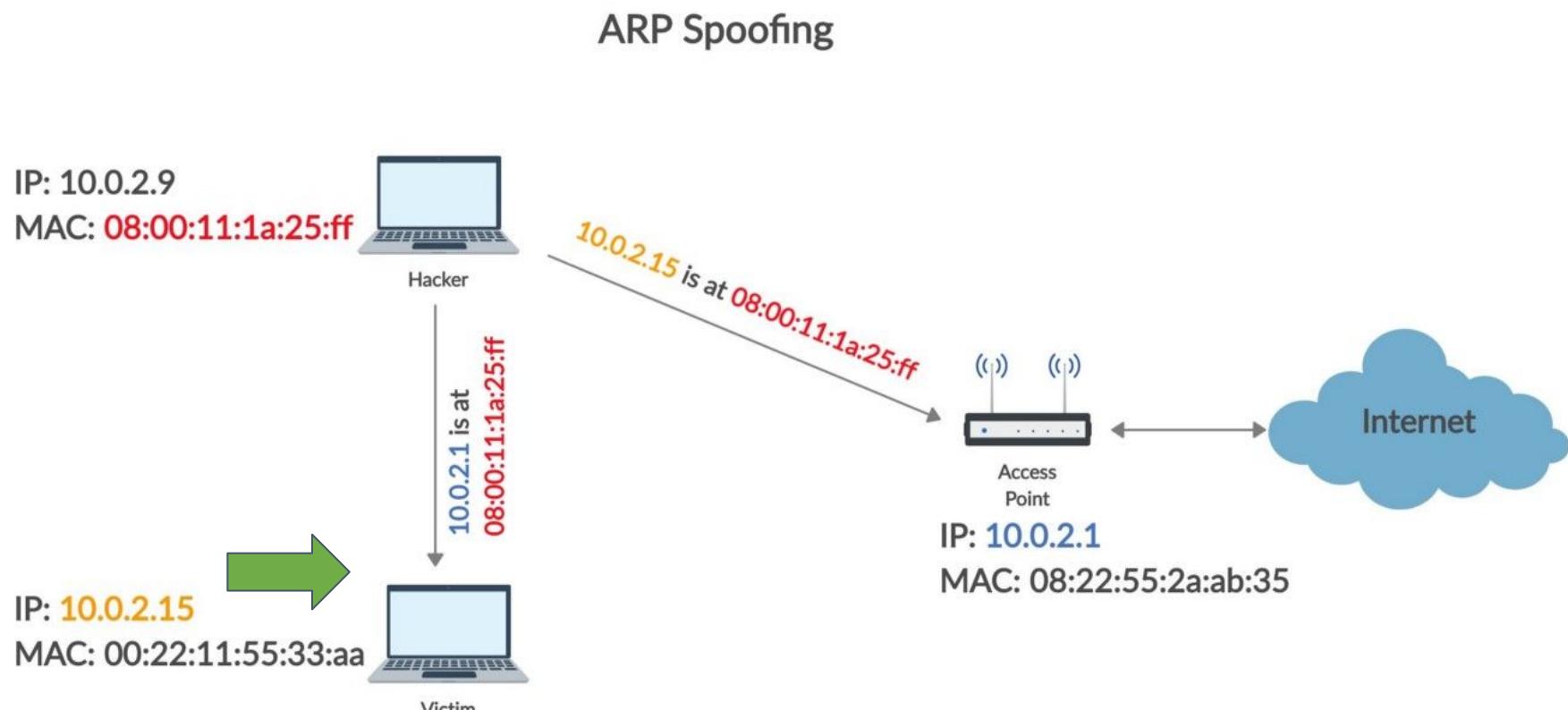
- **ARP Spoofing**

Enlaza una *MAC address* con la dirección IP de usuario legítimo.

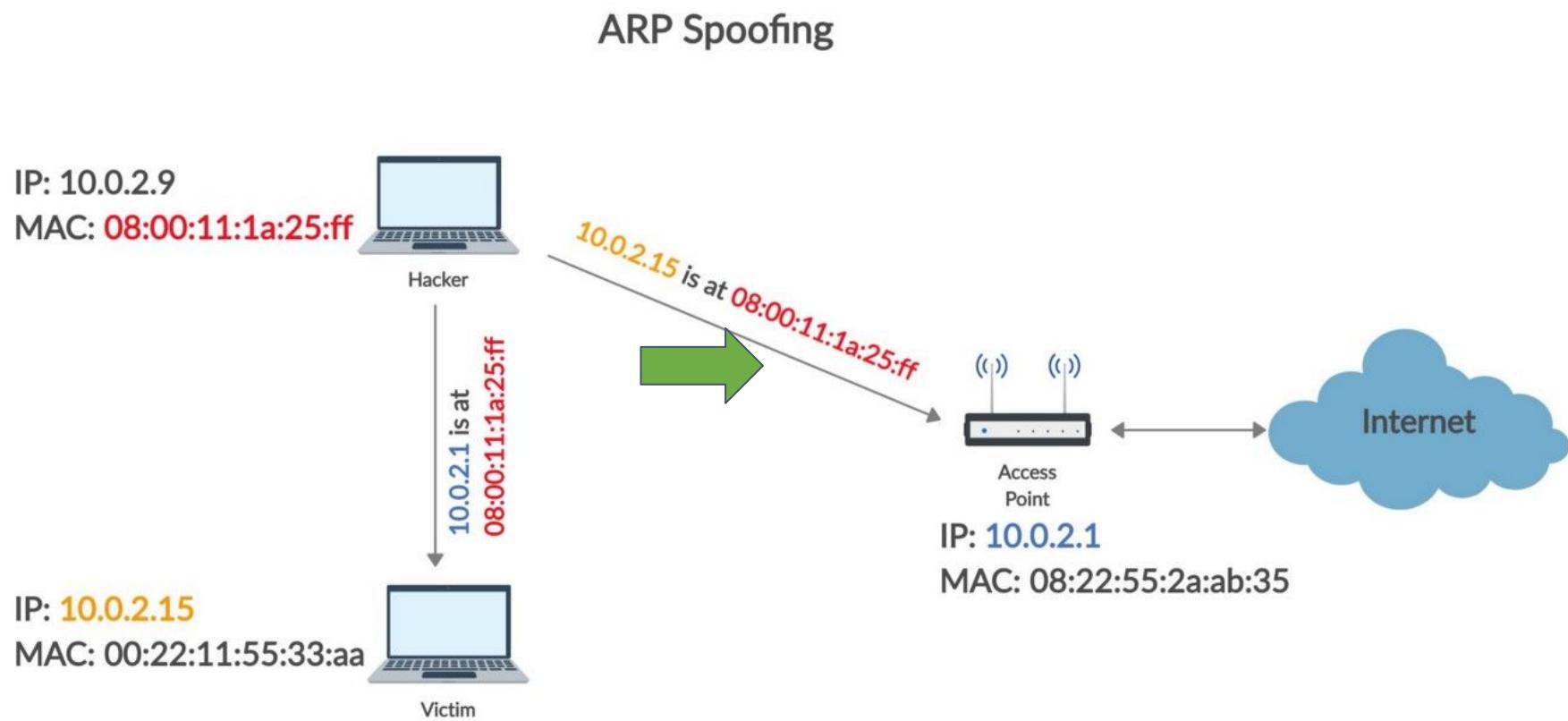
ARP Spoofing



ARP Spoofing



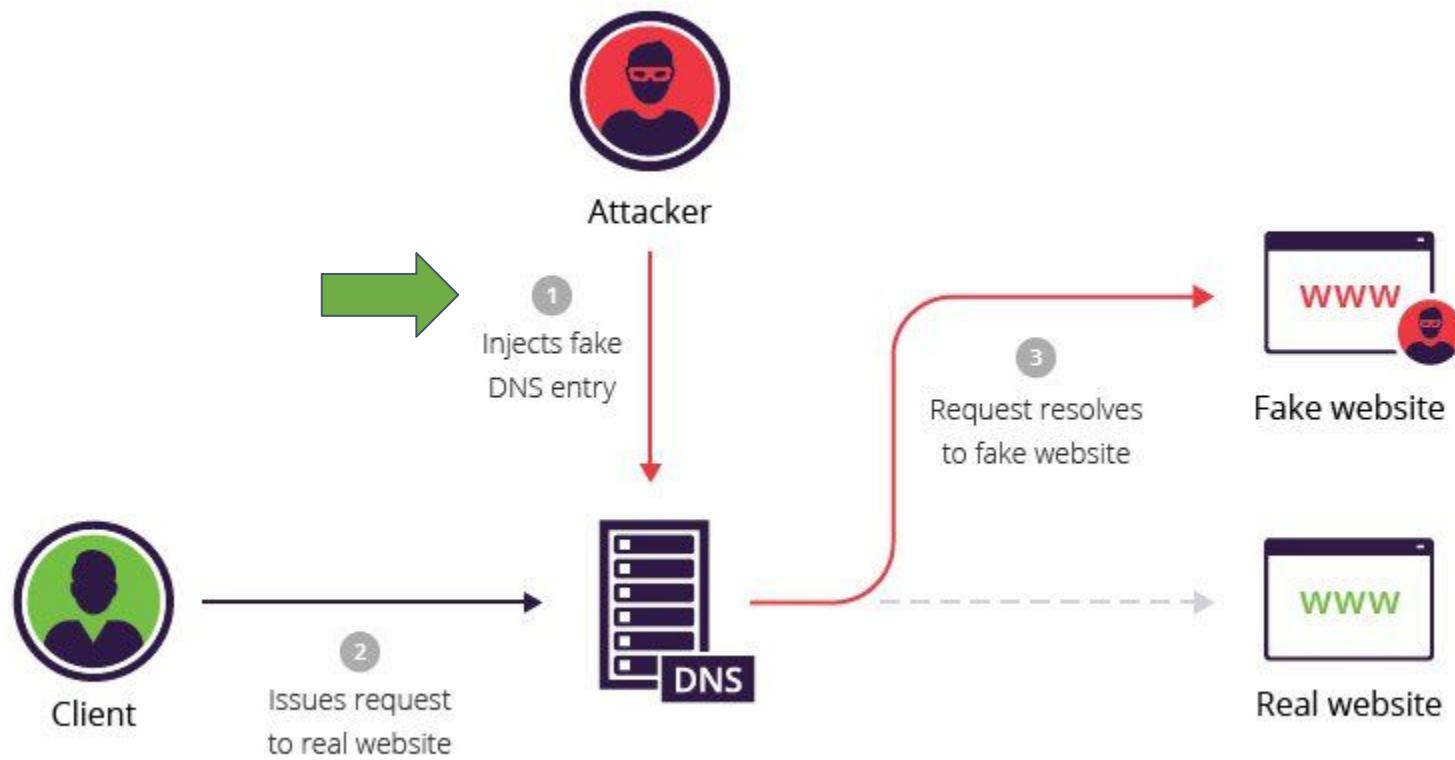
ARP Spoofing



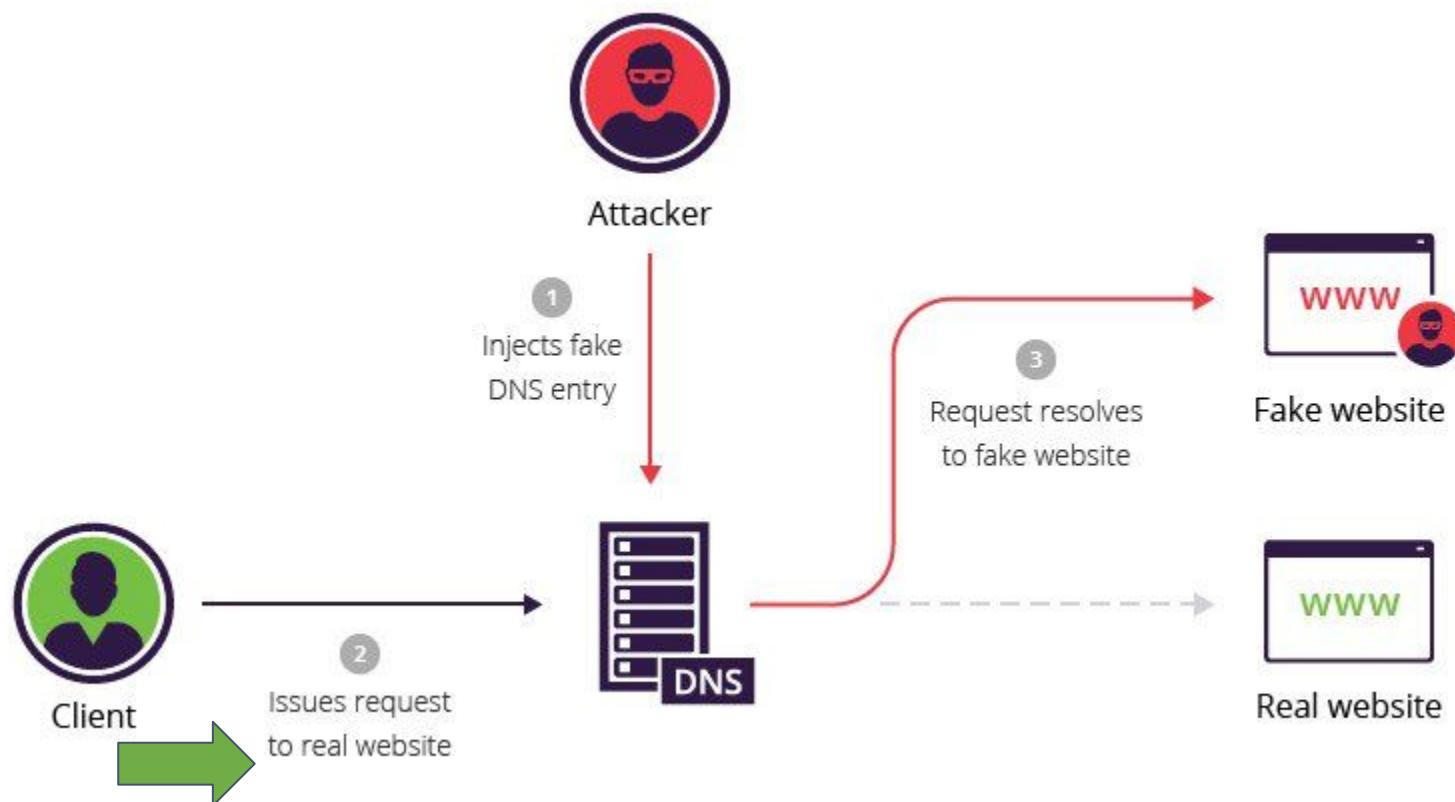
Tipos de MitM

- **DNS Spoofing**
Infiltra un *DNS Server*, alterando los registros de direcciones web.

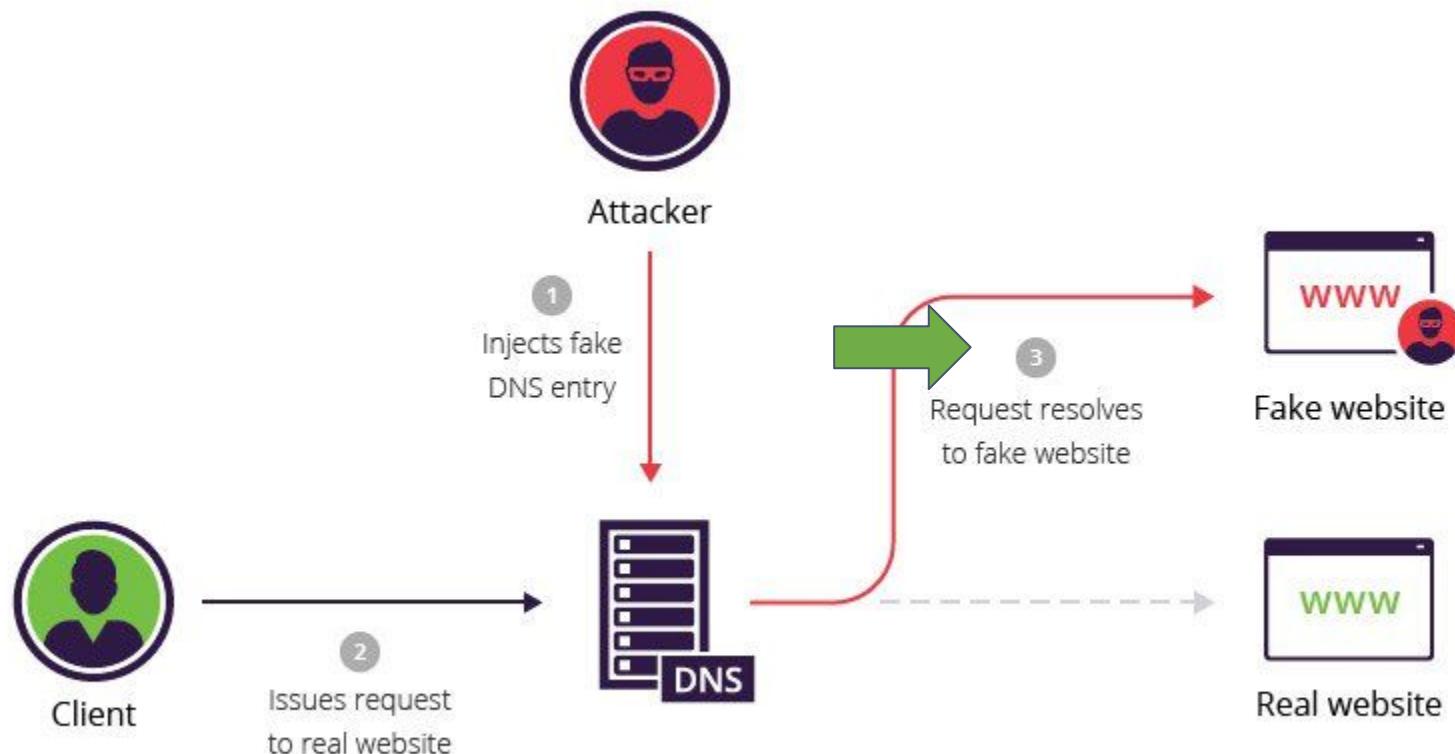
DNS Spoofing



DNS Spoofing



DNS Spoofing



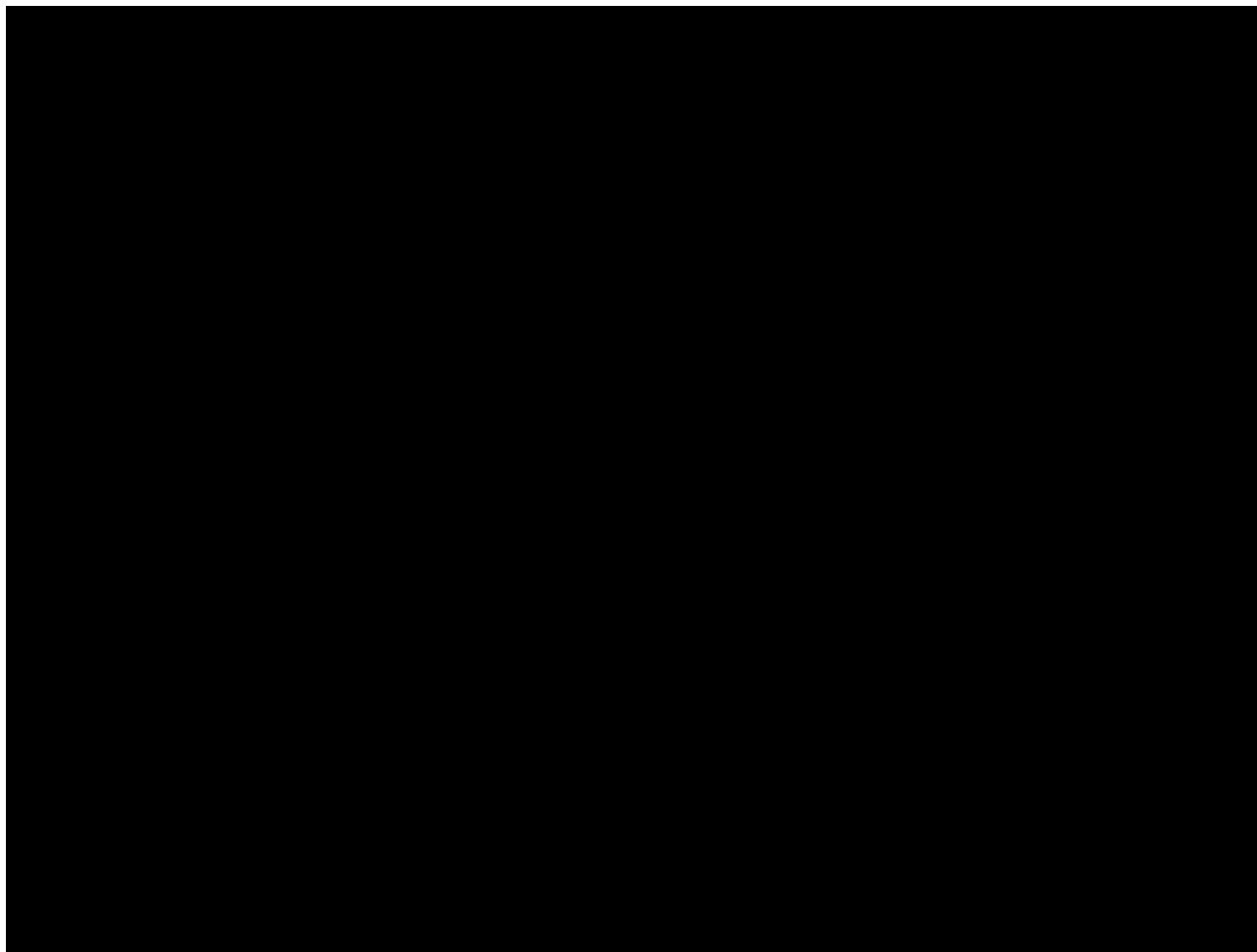
Ciber-Controles

- **Alertas en navegadores**
No omitir las alertas ofrecidas por los *web browsers*.
- ***Logging-out* obligatorio**
Si no utilizas una aplicación, cierra sesión.

Ciber-Controles

- **VPN**
Utilizar las bondades de las redes privadas virtuales.
- **Cifrar comunicaciones**
Utilizar *TLS 1.3+* con algoritmos de cifrado robusto.

Técnica MitM en acción!



Gestión de Accesos

Gestión de Accesos

Se refiere al tratamiento que se brinda a credenciales de acceso, tokens o cualquier otro recurso que permita Autenticación a un sistema.

¿Lo utilizas?

LastPass...| search my vault

dadhemir@g...
Free User

All Items

Sort By: Folder (a-z) ▾

(none) (7) ►

Alcaldía (4) ►

Apple (3) ►

Backup (1) ►

Business (30) ►

Docencia (1) ►

Education (35) ►

LastPass...| Try LastPass Families!

Organize and secure your entire family's digital life in LastPass.

LEARN MORE

The image shows the LastPass web interface. On the left is a dark sidebar with various menu items: 'Collapse', 'All Items' (selected), 'Passwords', 'Notes', 'Addresses', 'Payment Cards', 'Bank Accounts', 'Security Dashboard', 'Sharing Center', 'Emergency Access', 'Account Settings', and 'Advanced Options'. The main area is red and titled 'LastPass...|'. It features a search bar with 'search my vault' and a user profile icon for 'dadhemir@g...' (Free User). Below the title, it says 'All Items' and 'Sort By: Folder (a-z) ▾'. A list of items is shown with arrows: '(none) (7) ►', 'Alcaldía (4) ►', 'Apple (3) ►', 'Backup (1) ►', 'Business (30) ►', 'Docencia (1) ►', and 'Education (35) ►'. To the right, there's a sidebar with the text 'LastPass...| Try LastPass Families!', a circular graphic of a family using devices, and the text 'Organize and secure your entire family's digital life in LastPass.' with a 'LEARN MORE' button.

Clasificación

- **Locales (Offline)**

Permiten la administración de accesos en archivo local de tu equipo con *master key* (*KeePass*).

- **Servicio web (Online)**

Permite la sincronía de accesos en diferentes dispositivos a través de Internet (*1Password*).

Clasificación

- **Basados en token**

Permite autenticación con componente hardware, generalmente USB.

Beneficios (Online+Offline)

- Uso de contraseña maestra + token-file (MFA).
- Promueve el fortalecimiento de claves.

Beneficios (Online+Offline)

- Son repositorios de claves debidamente cifrados.
- Algunos implementan *passwordless option* (mobile).

Beneficios (Online+Offline)

- Cuentan con generadores de contraseñas.
- Permiten la gestión de accesos en equipos de trabajo.

Soluciones



NewDatabase	
General	
Windows	
Network	
Internet	
eMail	
Homebanking	

Title	User Name	Password	URL	Notes
029887e3-1c...	c7ab1bf3-548d...	*****	03e29e91-b3be...	3d8bb0e9-984a...
1465cbc8-a0...	96e1cac1-1790...	*****	2be2e42a-bdde...	9c0139f6-795c...
74ef5317-0b...	8142d5f0-21f7...	*****	7d139719-9aea...	69e4c15d-e896...
059d2469-40...	5b38e133-0548...	*****	9599ddee-c109...	bd653be9-9699...
fea0ba68-d3...	a2d84cb5-065c...	*****	c6eaa617-81be...	3925fa56-6f38...
c4454903-06...	ec17f8f8-4019...	*****	41f62055-c2a6...	d63f6ab0-3cc3...
2f8f5074-534...	485f9ff3-9655-4...	*****	278be296-2902...	ad490d63-fa18...
5a9fbdb31-34...	9e5d3818-cea3...	*****	3dcac7cc-5b62...	8816aba7-88ac...
14-215--L...	202--24- 7470	*****	107-4655-0642	222-5020-469f...

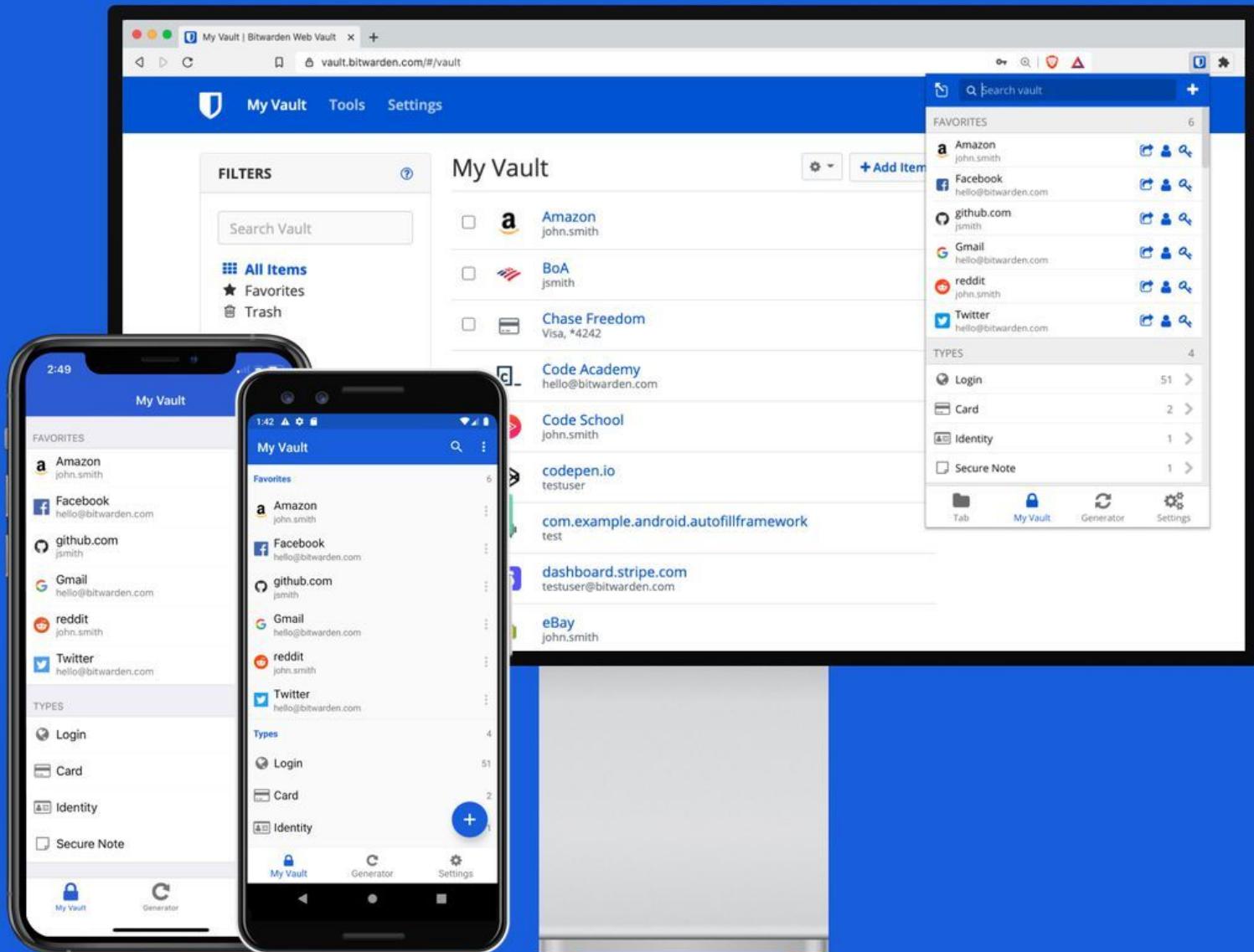
Open Password Database

Enter Composite Master Key
D:\Download_Go\NewDatabase.kdb

Master Password:

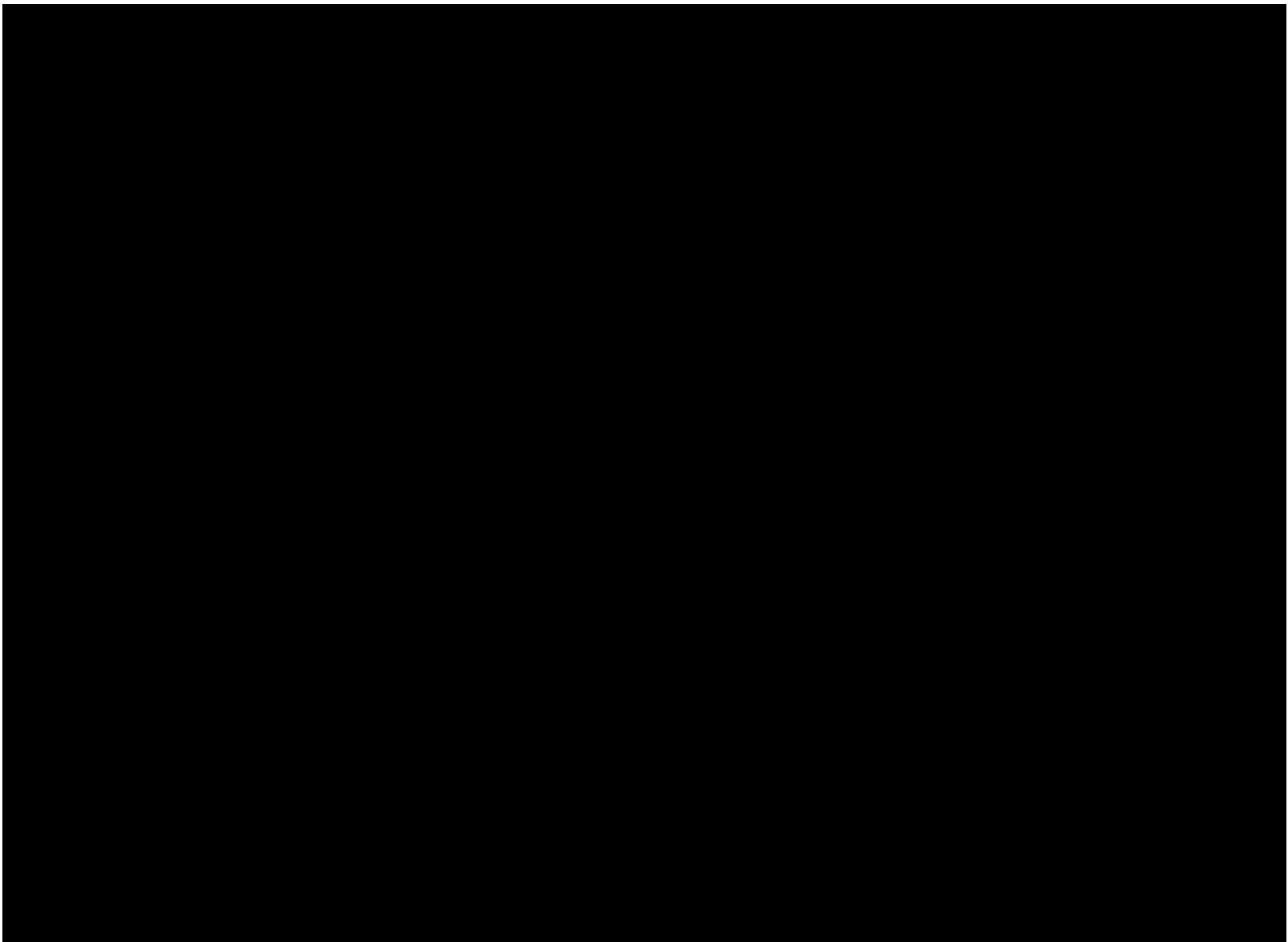
Key File:

Windows User Account





Ejemplo



Firewall

Firewall

Dispositivo o servicio de seguridad que monitorea y controla la entrada + salida de tráfico bajo reglas de seguridad definidas.

Aporta a Zero-Trust



Implementaciones

- **Appliance en sitio**

Hardware instalado y configurado de acuerdo a las necesidades de la empresa.

- **Cloud Security mode**

Servicios de seguridad adquiridos por demanda, modulares y escalables según necesidad.

Appliance en sitio

paloalto
NETWORKS®

Dashboard ACC Monitor Policies Objects Network Device

Export

Time
Last Hour 07/15 13:45:00-07/15 14:44:59

Global Filters Clear all

Application View
 Risk Sanctioned State
 Show system events

Network Activity Threat Activity Blocked Activity Tunnel Activity GlobalProtect Activity +

Application Categories

The treemap visualization shows the following structure:

- networking**:
 - ssl (orange)
 - encrypted-tunnel (orange)
- infrastructure**:
 - quic (green)
- saas**:
 - outlook-web-online (yellow)
 - general-business (light green)
 - windows-azure-base (light green)
 - facebook-base (light orange)
- business-systems**:
 - software-update (orange)
 - ms-update (orange)
 - internet-utils (light blue)
 - web-browsing (orange)
 - whatsapp-base (light green)
- media**:
 - general-intent (light blue)
 - facebook-base (light orange)
 - internet-utils (light blue)
 - web-browsing (orange)
- collaboration**:
 - general-intent (light blue)
 - internet-utils (light blue)
 - web-browsing (orange)

Application

Application	Risk	Bytes	Sessions	Threats	Content	URLs
ssl	4	43.8G	129.6k	3.7k	0	108.2k
quic	1	17.0G	40.4k	0	0	0
ms-update	4	14.6G	5.7k	16	16.2k	4.5k
outlook-web-online	3	8.1G	11.9k	1.2k	0	12.7k
windows-azure-base	1	6.2G	163	0	0	98
facebook-base	4	5.7G	10.2k	23	0	7.7k
ms-ds-smbv3	3	3.7G	3.8k	55	0	0
web-browsing	4	2.5G	18.0k	8.9k	919	12.6k
whatsapp-base	1	1.4G	4.1k	36	82	2.2k

Search: tor

731 Applications (Clear filters)

CATEGORY	SUBCATEGORY	TECHNOLOGY	RISK	CHARACTERISTIC
306 business-systems 59 collaboration 90 general-internet 40 media 62 networking 174 saas	11 audio-streaming 7 auth-service 3 database 7 email 9 encrypted-tunnel 6 erp-crm 136 file-sharing 7 gaming 44 general-business 136 ics-protocols 21 infrastructure	246 browser-based 374 client-server 91 network-protocol 20 peer-to-peer	329 1 169 2 134 3 81 4 18 5	125 Evasive 144 Excessive Bandwidth 73 Prone to Misuse 195 SaaS 320 Transfers Files 60 Tunnels Other Apps 41 Used by Malware 466 Vulnerabilities 278 Widely Used
NAME	CATEGORY	SUBCATEGORY	RISK	TECHNOLOGY
telex	networking	proxy	2	client-server
temptrak	business-systems	general-business	1	network-protocol
tenable-security-center	general-internet	internet-utility	1	client-server
tesla-car-app	business-systems	management	1	client-server
thinkfree	saas	office-programs	4	browser-based
tidal	media	audio-streaming	2	browser-based
tigertext	saas	social-business	3	client-server
tikiwiki-editing	collaboration	web-posting	2	browser-based
timbuktu	collaboration	internet-conferencing	4	client-server
tistory-blog-posting	collaboration	web-posting	2	browser-based
titanize	general-internet	file-sharing	3	browser-based
tivoli-network-monitoring	business-systems	management	1	client-server
tivoli-storage-manager	business-systems	storage-backup	3	client-server
tor	networking	encrypted-tunnel	4	client-server
tor2web	networking	proxy	4	browser-based
torch-browser				
└ torch-browser-base	general-internet	internet-utility	3	browser-based
└ torch-browser-music	media	audio-streaming	2	browser-based
└ torch-browser-games	media	gaming	2	browser-based
trendmicro-officescan	business-systems	management	2	client-server
tresorit				
└ tresorit-base	saas	storage-backup	2	client-server
└ tresorit-uploading	saas	storage-backup	2	client-server
└ tresorit-downloading	saas	storage-backup	2	client-server
trueshare	saas	file-sharing	3	client-server
turbouupload	general-internet	file-sharing	5	browser-based
turkcell-bip	collaboration	instant-messaging	2	client-server

Cloud Security

DDoS ①

URL Rewrites ①

Page Rules ①

IP Access Rules ①

Bots ①

WAF ①

Header Modification ①

Access ①

Workers ①



Beneficios

- **Panorama de seguridad**

Permite visualizar eventos en el tráfico de red para la toma de decisiones.

- **QoS**

Calidad en el servicio de la red empresarial.

Beneficios

- **Control permanente**

Bloquear ciberamenazas emergentes
y nuevos modelos de ataques.

- **Canales de red seguros**

Permite la implementación de VPN
o túneles para usos diversos.

¿Cuál es el mejor Firewall?

El que se encuentre alineado con tus activos de información y con el objetivo de negocio.



IDS/IPS

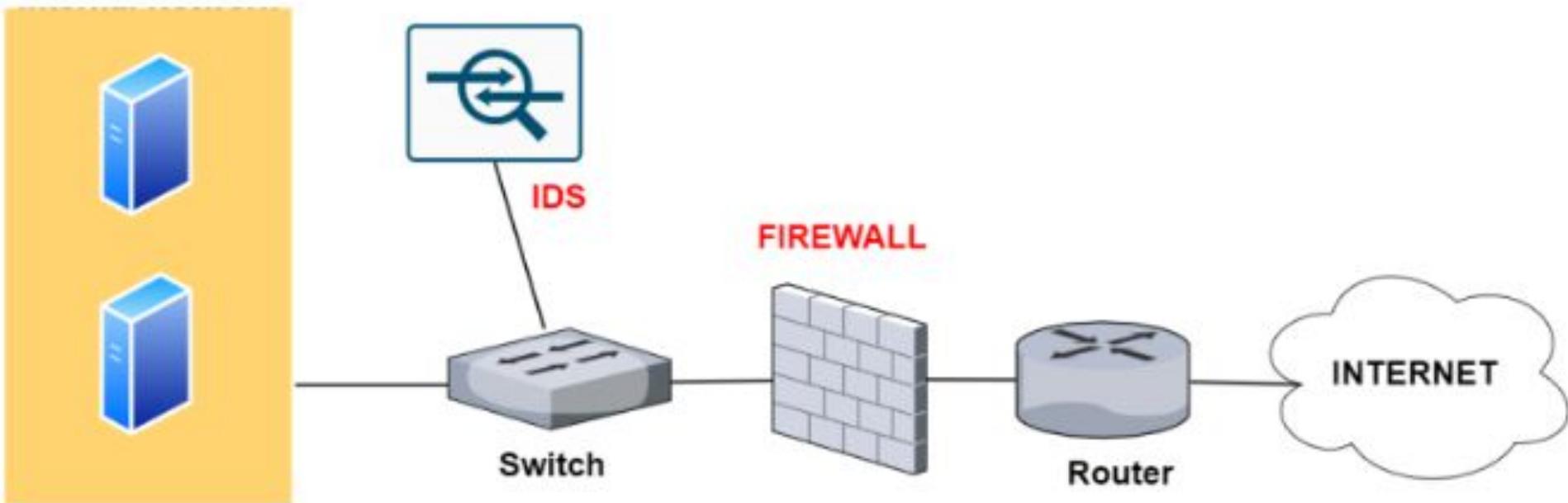
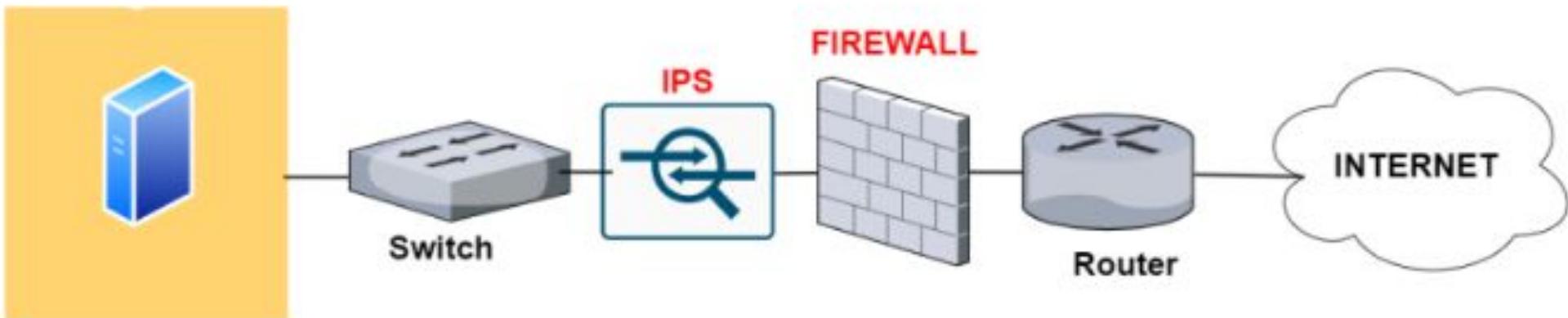
Sistema de Detección/Prevención
de Intrusos

IDS (Sistema de Detección de Intrusos)

Es una herramienta de seguridad en la red que analiza el tráfico interno para detectar actividad maliciosa y alertar al administrador del sistema.

IPS (Sistema de Prevención de Intrusos)

Es la evolución de los IDS. Este, además de alertar al administrador del sistema cuando detecta actividad maliciosa; puede bloquear, capturar o eliminar paquetes maliciosos.



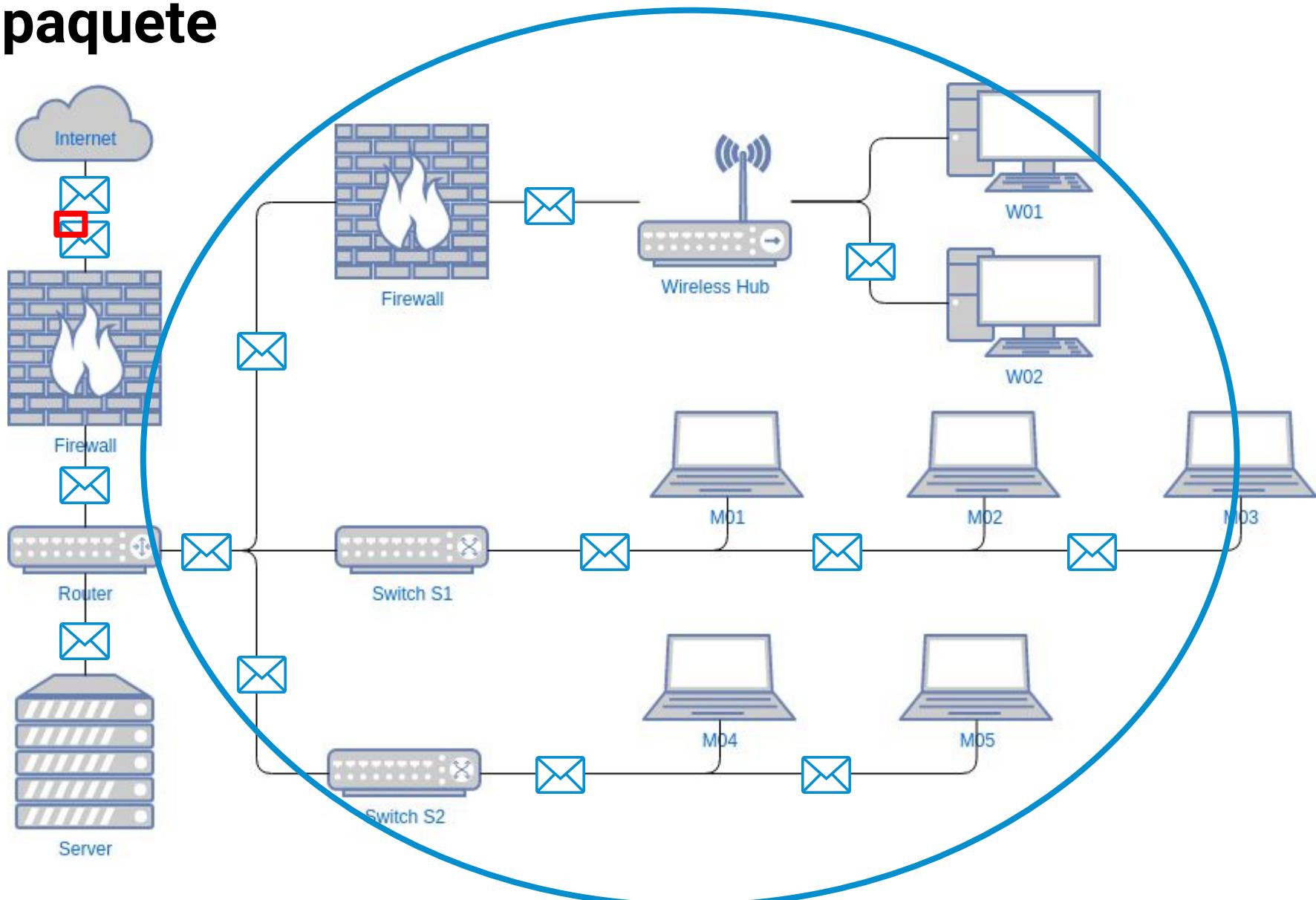
Funcionamiento

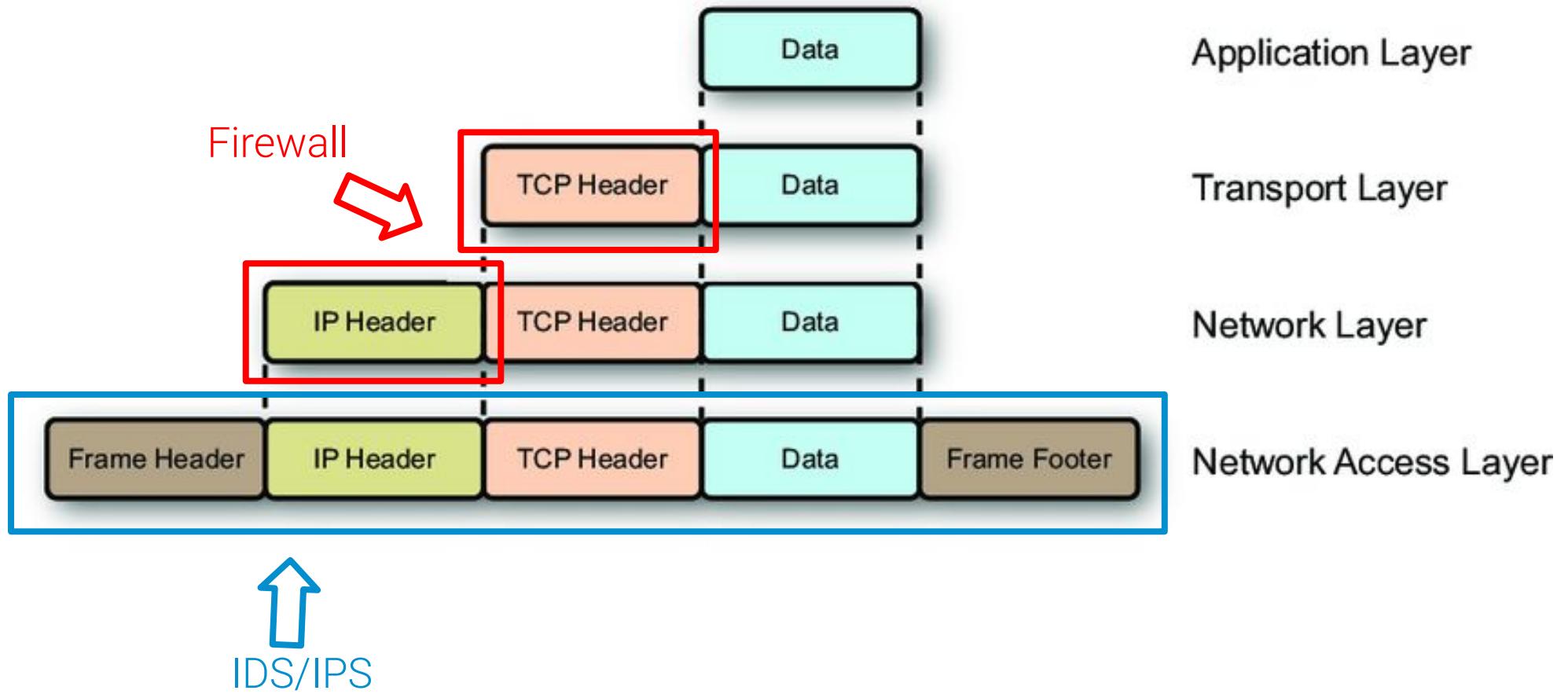
Estos se encuentran *inline* para analizar todo el tráfico en la red detrás del firewall. Identifican amenazas según los siguientes factores:

- **Firmas**
- **Anomalías**
- **Políticas**

Firewall IDS/IPS

✉ paquete

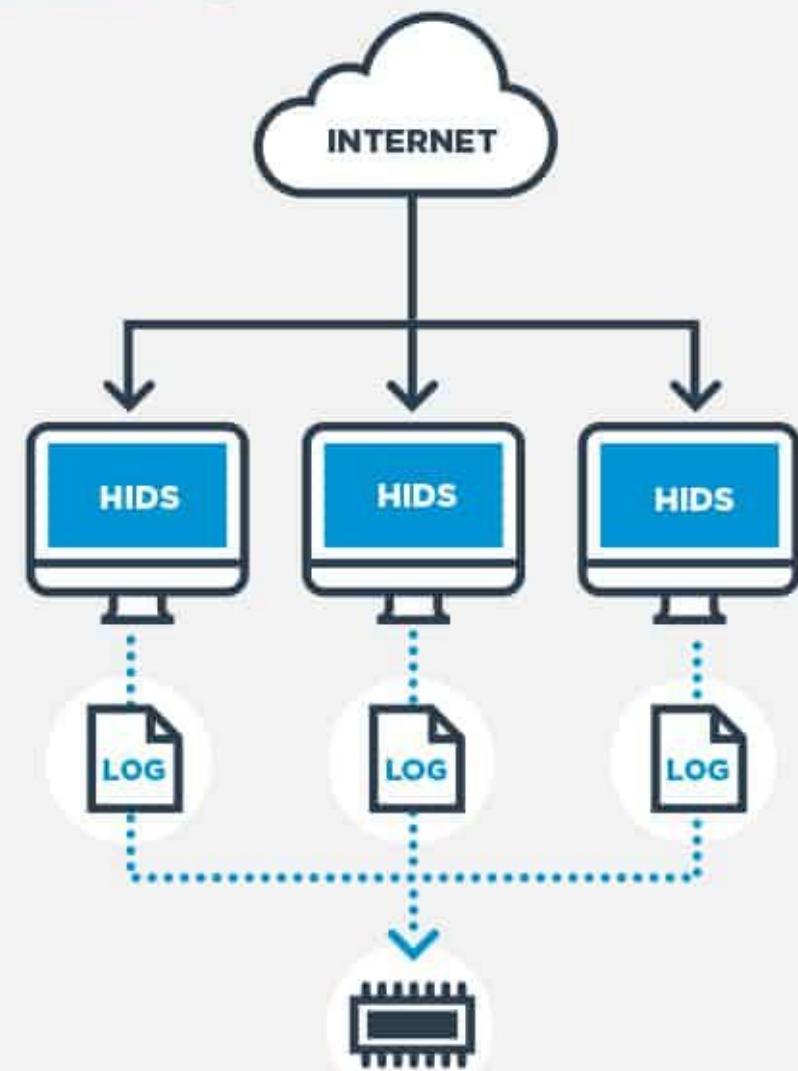
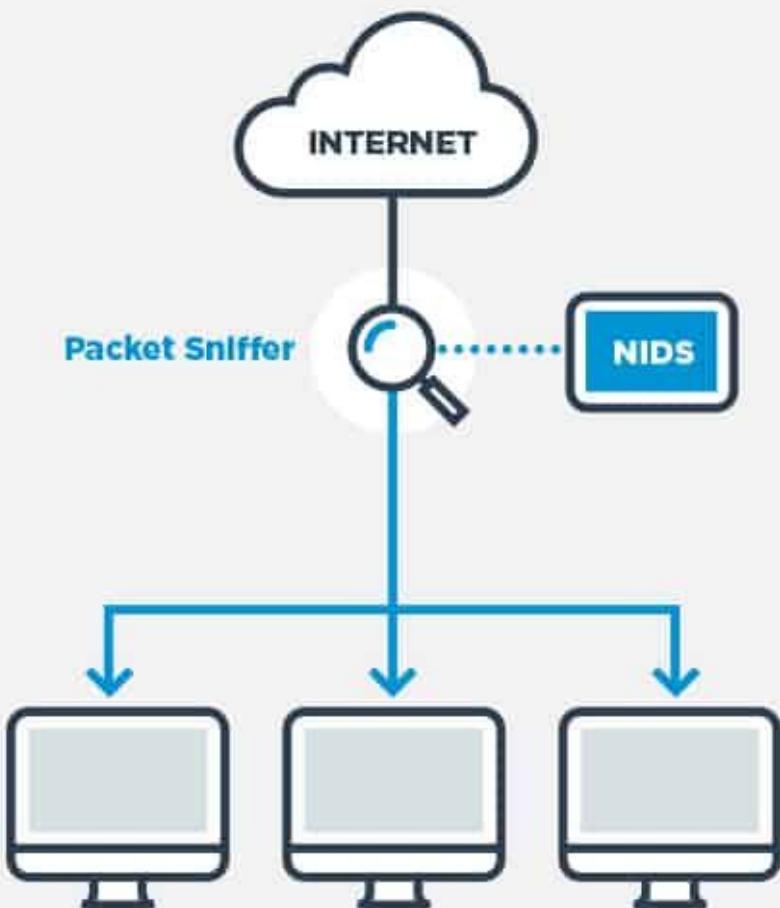




Clasificación

- **NIPS (Network Intrusion Prevention System)**
Sistema basado en la red
- **HIPS (Host Intrusion Prevention System)**
Sistema basado en el host (PC)

NIDS vs HIDS



Centralized Control Module

Clasificación

- **NBA (Network Behavior Analysis)**
Analiza tráfico inusual (DDoS)
- **WIPS (Wireless Intrusion Prevention System)**
Escanea redes WiFi

Beneficios

- Integración con otras soluciones
- Mayor eficiencia en otros controles de seguridad
- Ahorro de Tiempo
- Compliance
- Personalizable

Soluciones

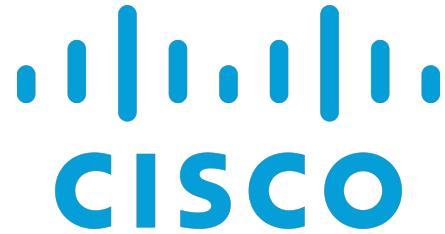
Soluciones

- Solución Independiente
- Firewall de Nueva Generación (NGFW)
- Gestor Unificado de Amenazas (UTM)

Proveedores Open Source



Proveedores Empresariales



TREND
MICRO™



Proveedores Cloud



Google Cloud



Correlación y Gestión de Eventos (SIEM)

¿Qué es SIEM?

Administración de eventos e información de seguridad. Es un campo de la seguridad informática del que surgen soluciones que centralizan todas las fuentes de información para así tener una visión más completa de posibles amenazas, cumplimiento y manejo de incidentes.

¿Cómo funciona?

1. Gestión de registros.
2. Correlación de eventos y análisis.
3. Monitoreo de incidentes y alertas de seguridad.
4. Gestión de compliance e informes.

Capacidades

- Agregación de Información
- Correlación
- Alerta
- Dashboard
- Compliance
- Retención
- Análisis Forense

¿Por qué es importante?

- Puede ayudar a detectar *zero-days*.
- Normalización y categorización de logs.
- Visualización de eventos.
- Detección de malas configuraciones.
- Puede detectar comunicaciones maliciosas y canales encriptados.

Ejemplos

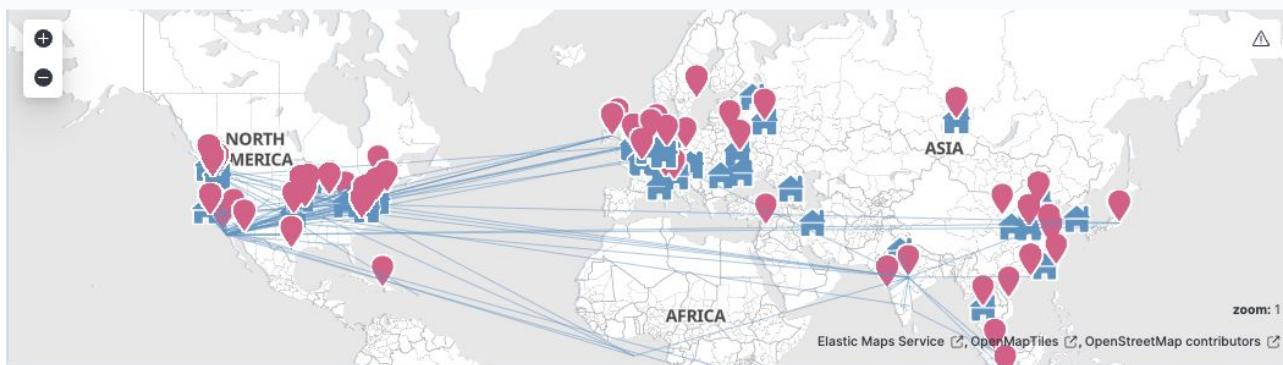
Regla	Objetivo	Trigger	Fuentes de Información
Fuente de inicio de sesión de ataque repetido	Alerta temprana para ataques de fuerza bruta, adivinación de contraseñas y aplicaciones mal configuradas.	Alerta sobre 3 o más inicios de sesión fallidos en 1 minuto desde un solo host.	Active Directory, Syslog (hosts Unix, conmutadores, enrutadores, VPN), RADIUS, TACACS, aplicaciones monitoreadas.
Repetir ataque-Firewall	Alerta temprana para escaneos, propagación de gusanos, etc.	Alerta sobre 15 o más eventos de caída/rechazo/denegación de firewall desde una sola dirección IP en un minuto.	Cortafuegos, enrutadores y conmutadores.

Ejemplos

Regla	Objetivo	Trigger	Fuentes de Información
Repita el sistema de prevención de intrusiones de ataque-host	Encuentre hosts que puedan estar infectados o comprometidos (exhibiendo comportamientos de infección)	Alerta sobre 3 o más eventos desde una sola dirección IP en 10 minutos	Alertas del sistema de prevención de intrusiones del host
Detección/eliminación de virus	Alerta cuando se detecta un virus, spyware u otro malware en un host	Alerta cuando un solo host ve una pieza identificable de malware	Antivirus, HIPS, detectores de anomalías de comportamiento de redes/sistemas

Search KQL Last 6 months Refresh

🕒 + Add filter



Network events
1,496,797

DNS queries
66,122

Unique private IPs
511 source 182 destinat...

Unique flow IDs
163,355

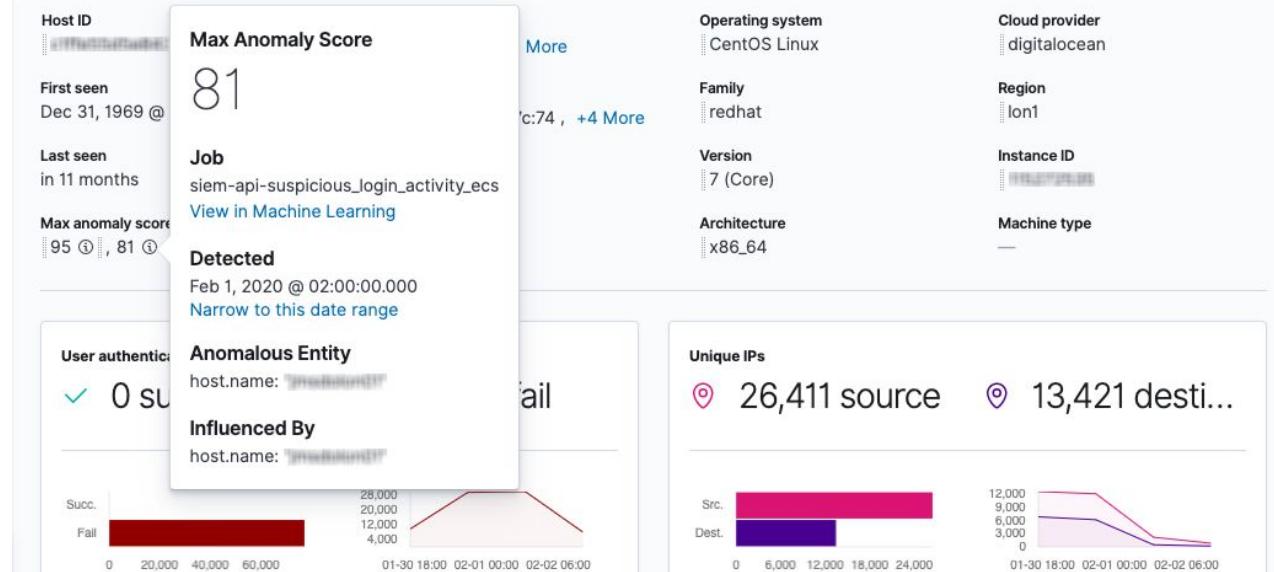
TLS handshakes
42

☰ D Security / Hosts / Machine Learning / Authentications

🕒 Search KQL Last 20 minutes Show dates Refresh

🕒 + Add filter

+ • Finance station compromise 37619390



Soluciones

Proveedores



AT&T Business



Copias de Seguridad

¿Qué es?

Son copias de la información original almacenadas en distintos medios y que pueden ser usadas para recuperar la información en caso de su pérdida.



¿Por qué se puede perder la información?

- Desastre natural
- Eliminación accidental
- Robo
- Corrupción de información
- Virus informático

Métodos

- Copia completa/espejo
- Copia incremental
- Copia en tiempo real (CDP)

Medios

- Cinta magnética
- Medios ópticos
- Disco duro tradicional (HDD)
- Disco duro en estado sólido (SDD)
- Servicio remoto (cloud)

Consideraciones

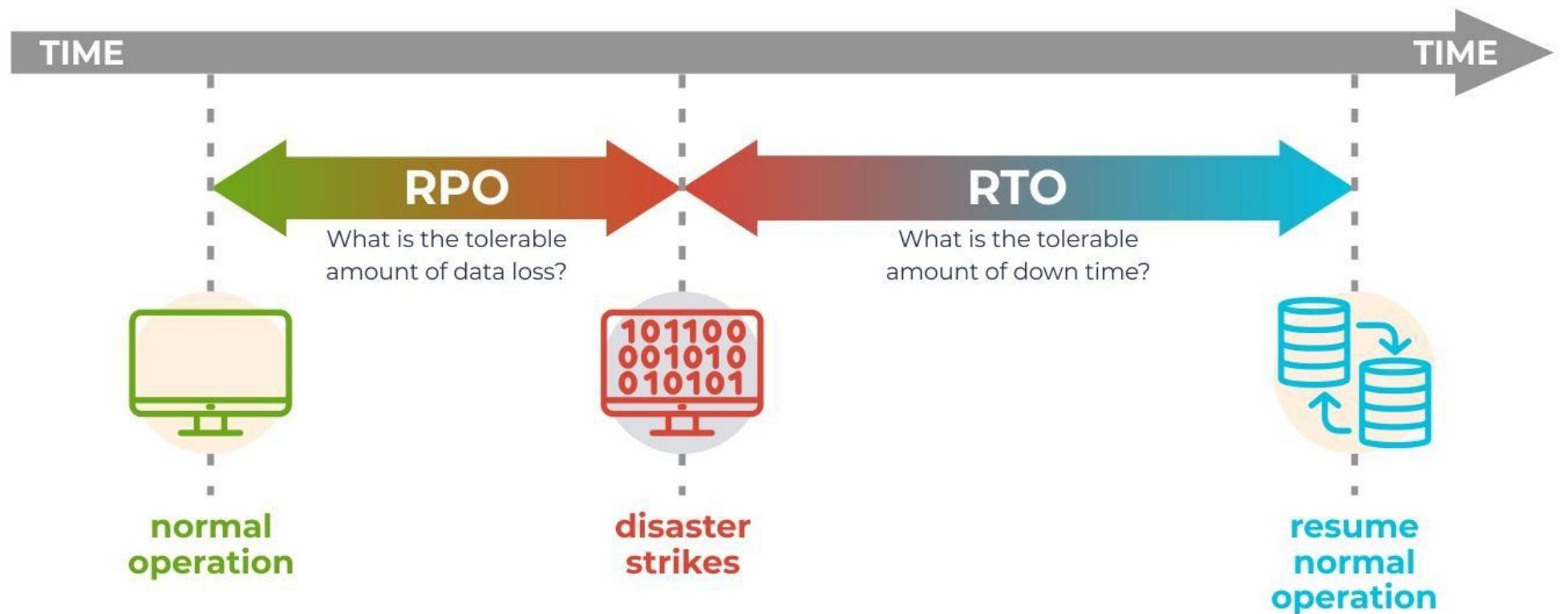
- Redundancia/replicación de las copias de seguridad
- Cifrado de los datos
- Refactorización
- Compresión
- Limpieza automática de datos

Consideraciones

- Seguridad de las copias de seguridad
- Periodo de retención de la información
- Validación de integridad
- Monitoreo

Conceptos Clave

- **Punto Objetivo de Recuperación (RPO)**
Periodo objetivo máximo del que se puede tolerar pérdida de información.
- **Tiempo Objetivo de Recuperación (RTO)**
Cantidad de tiempo entre un desastre y la recuperación de las funciones de negocio.



Soluciones

Proveedores Cloud



Open Software

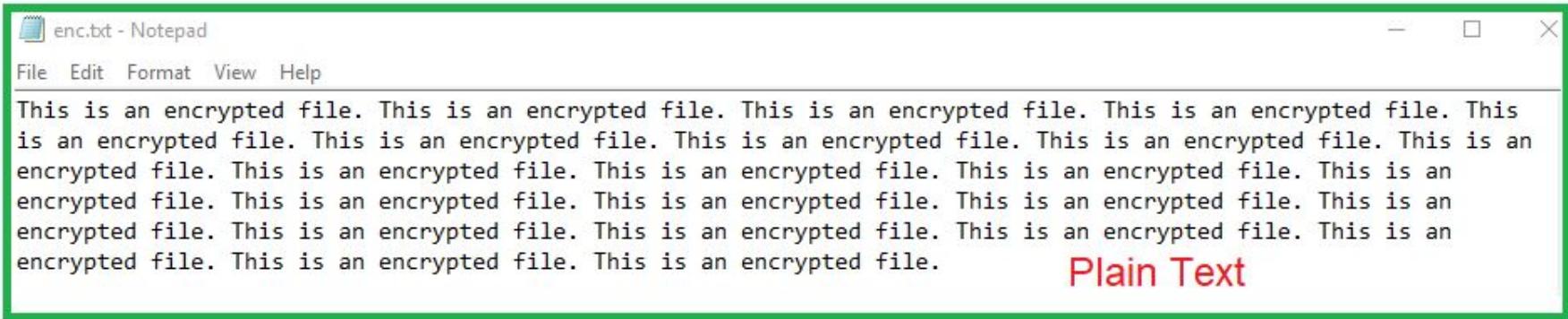
- Amanda
- AOMEI Backupper Standard
- Back In Time
- Bacula
- Duplicati
- EraseUS
- Fbackup
- Tar

Cifrado

¿Qué es cifrado?

Es el proceso de convertir información a un formato ilegible mediante el uso de una llave definida y procesos matemáticos con el fin de proteger la **confidencialidad** de la misma.

¿Qué es cifrado?

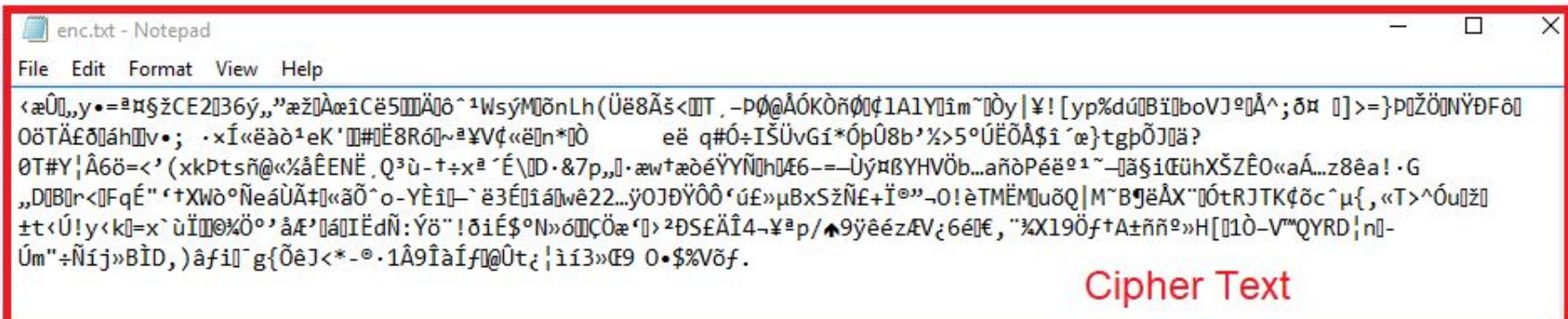


This is an encrypted file. This is an encrypted file.

Plain Text



**File Encryption Key
(AES-256)**



æÙ„y•=¤§žCE2]36ý, „æž]AœiCé5]A]ô^1WsýM]õnLh(Üe8Ãš<]T, -PØ@AÓKØñØ]ç1A1Y]im~]Øy|¥![yp%du]Bí]boV]ø]Å^;ð¤]>=}P]ZÖ]NÝDFô]OötA£ô]áh]v•; .xÍ«ëàò¹eK'¶#]E8Ró]~]¥V¢«ë]n*]Ø eë q#Ø÷IŠÜvGí*ØþÛ8b'%'>5°ÚËÖÅ\$í`æ}tgb]J]ä? 0T#Y]Å6ö=<'(xkDtšñ@«%åÊENÉ. Q³ù-+÷x¤`É\]D·&7p,,]·æw+æðéYYÑ]h]Æ6--=Ùý]BYHVÖb...añòPéé¤¹~=Ùä§i]EühXSZ]E0«aÁ...z8êa! ·G „]DIB]r<]FqÉ“‘+XWòºÑeáÜ]t]«æð^o-YÈi]–`é3É]iá]w22...ý]O]D]Y]Öö]‘ú]E»]µBxS]Ñ]E+]I]º”·0!èTM]EM]u]ØQ]M~]B]j]éAX”]ÓtR]TK]f]öc^]µ{, «T>^]Óu]z]±t<]Ú]y]k]=x^ù]I]Ø]K]º”·å]Æ’]á]I]Ed]Ñ:Y]ö”!δi]É\$]ºN]»]d]Ø]C]ö]º”·]²]D]S]f]Ä]I]4]–]¥]ºp/]¶]9]y]é]z]EV]ç]6]é]€, ”]X]1]9]Ö]f]t]A]±]ñ]º”]»]H[]1]ò]–]V]”]Q]Y]R]D]n]–]Ú]m]÷]Ñ]í]j]»]B]ì]D,) å]fi]º”g]{Ø]e]º”·1]A]9]I]à]f]@]Ù]ç;]l]i]3]»]E]9]0]·]\$]%]V]ö]f.

Cipher Text

¿Qué es descifrado?

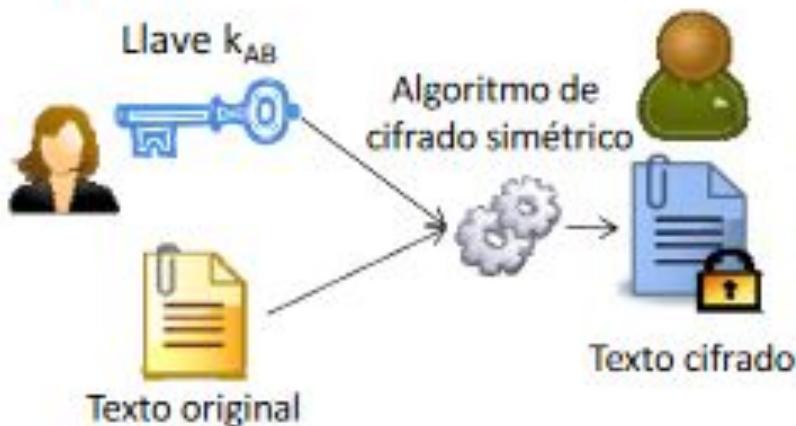
Es el proceso de revertir la información a su formato original mediante el uso de una llave para que pueda ser usada normalmente de nuevo.

Cifrado Simétrico

¿Cómo funciona?

Se usa la misma llave para cifrar
y para descifrar

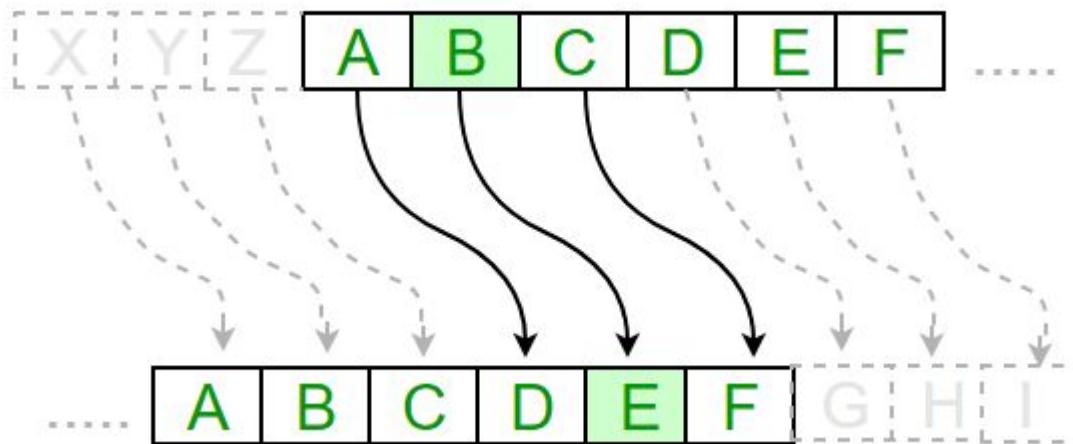
1. Cifrar



2. Descifrar



Cifrado de César



Texto Original: Hola

Llave: 3 espacios

Texto Cifrado: Krñd

Cifrado Asimétrico

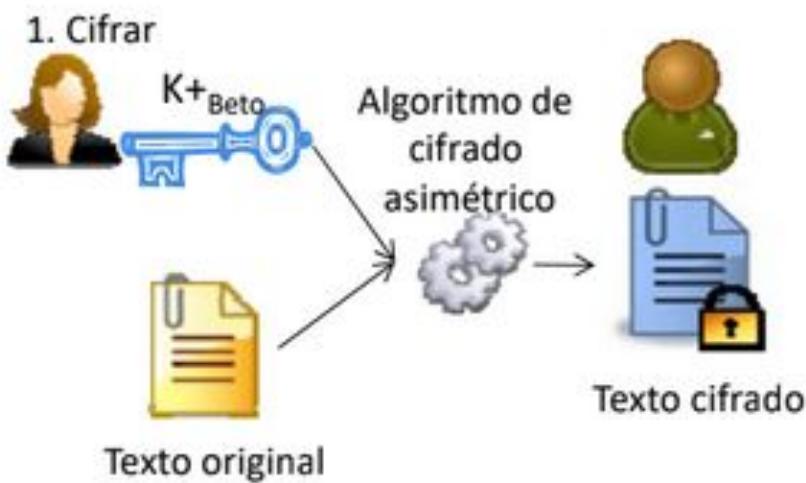
¿Cómo funciona?

Se tienen dos llaves:

- Llave pública ($k+$)
- Llave privada ($k-$)

Lo que se cifra con una llave pública solo puede ser descifrado con la llave privada correspondiente y viceversa.

¿Cómo funciona?



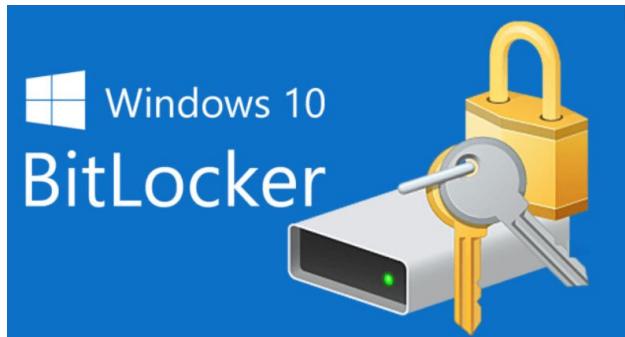
**Cifrado en
dispositivos
personales**

Caso de Uso

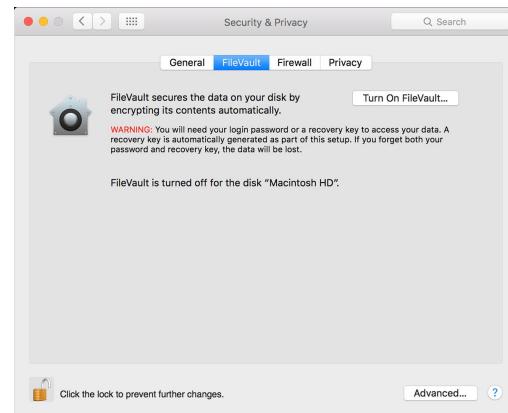
Si pierdes o te roban tu computador o celular, tus archivos estarán protegidos si el disco duro estaba cifrado.



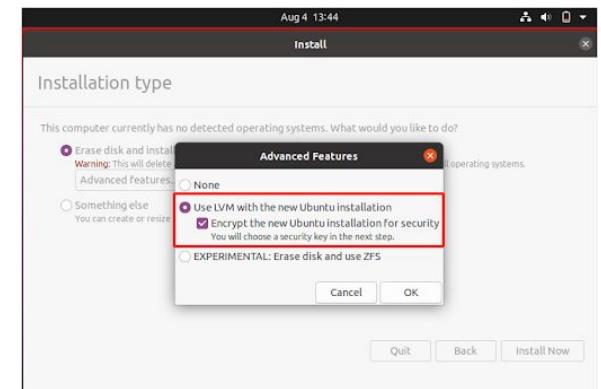
Herramientas OS



Windows



MacOS



Ubuntu

Cifrado en Dispositivos



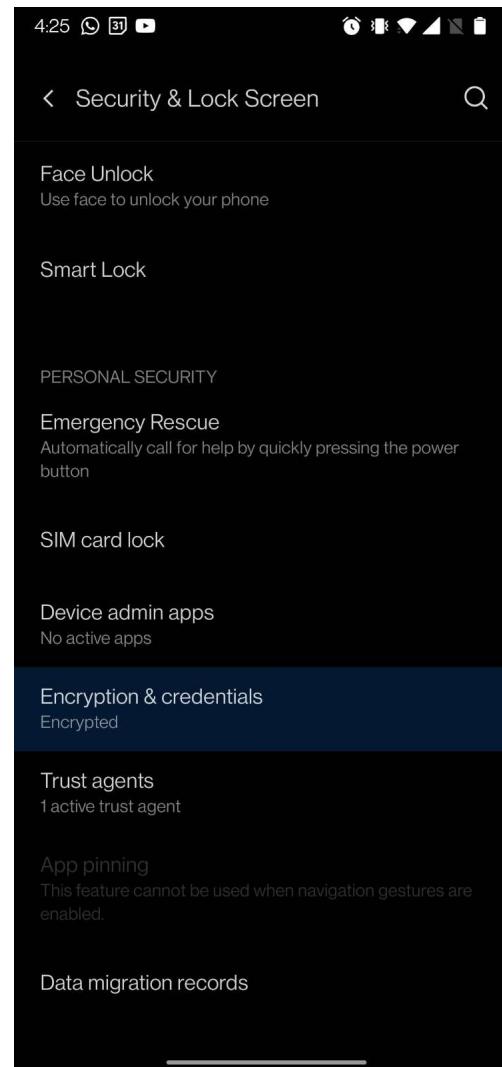
BitLocker (D:)

Enter password to unlock this drive.

A password input field with a clear button.

[More options](#)

[Unlock](#)

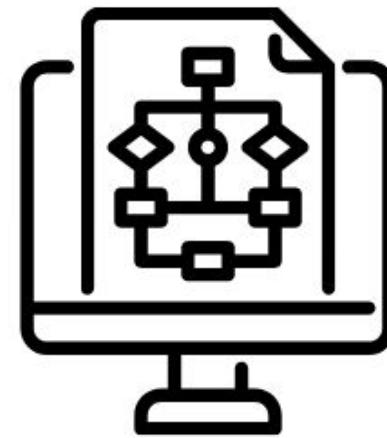


Principales Recomendaciones

Recomendaciones



Tamaño de Llave



Algoritmo de cifrado

Soluciones

Otras soluciones software



AxCrypt



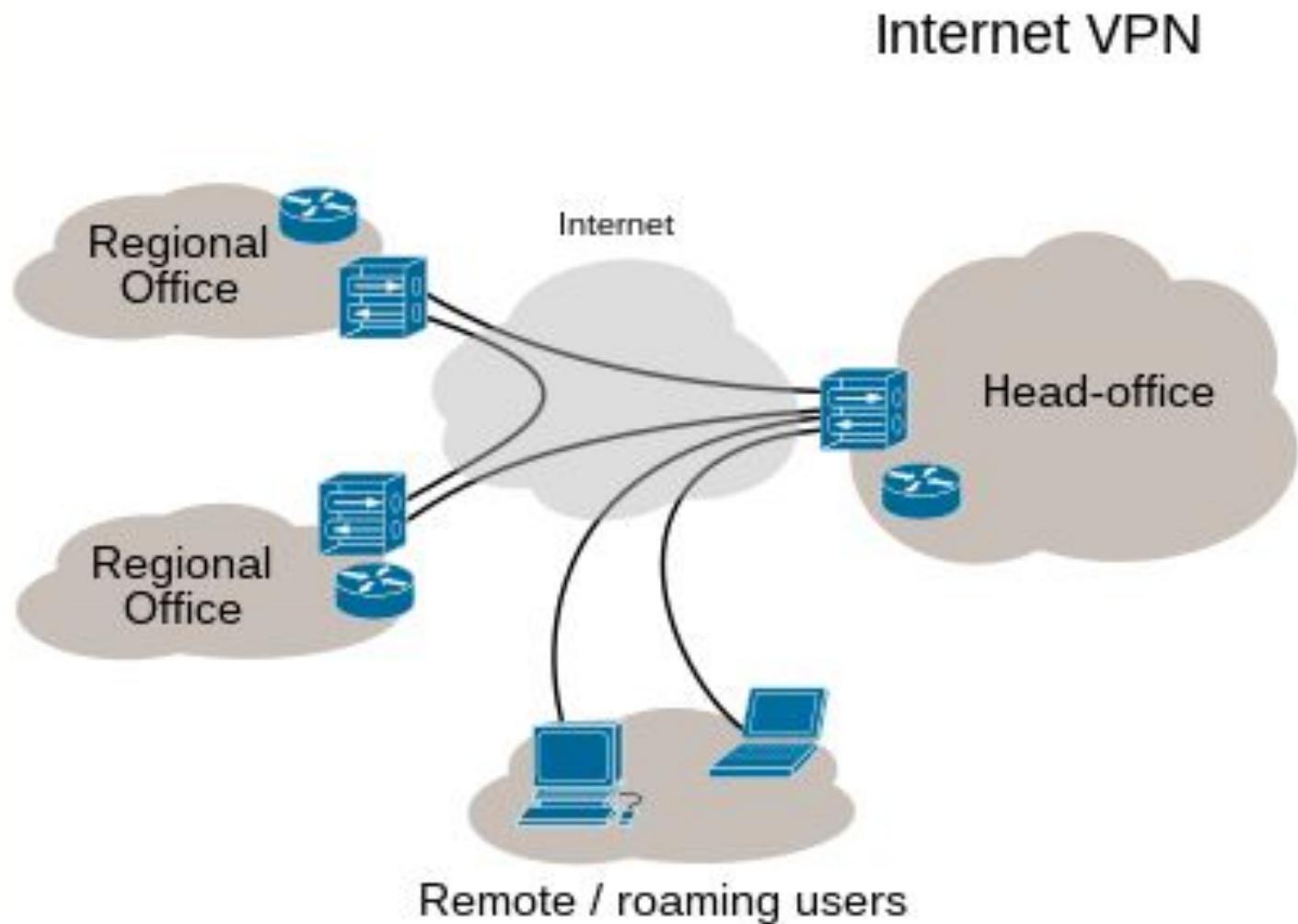
VPN

(Red Privada Virtual)

¿Qué es una VPN?

Es una tecnología que permite la conexión de un usuario a la red pública (internet) como si estuviera en una red privada (intranet empresarial) al tiempo que cifra toda la información enviada.

¿Qué es una VPN?



¿Cómo funciona?

Toda la actividad se cifra y pasa por un intermediario (servidor VPN) el cual reenvía y recibe las peticiones a otros sitios o servicios web.

¿Por qué debo usar una?

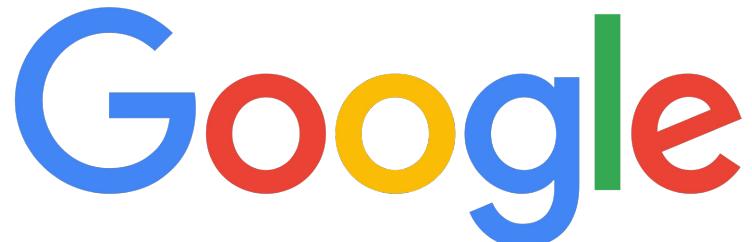
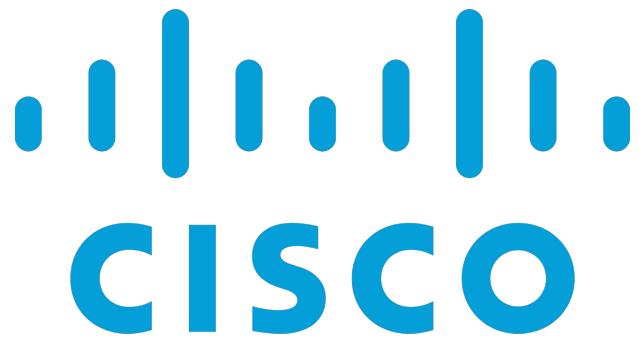
- Si la empresa tiene aplicaciones que solo pueden ser accedidas desde su red interna.
- Cifrar datos enviados en redes no confiables.
- Ocultar tu identidad a sitios que visites.

Soluciones

Implementaciones

- Servidor empresarial (on-premise)
- VPN as a Service (Cloud)
- VPN Comerciales

Proveedores



Endpoint Protection

¿Qué es?

Es la práctica de proteger todos los dispositivos finales de una red (computadores, celulares, IoT, etc.) mediante la integración de varias herramientas y soluciones. Es la siguiente iteración de las soluciones de antivirus tradicionales que se basaban en firmas digitales.

Características

- Clasificación con Machine Learning
- Protección avanzada de múltiples dispositivos
- Protección de navegación web
- DLP
- Firewall integrado

Características

- Bloqueo de phishing y ataques por correo
- Protección de amenazas internas
- Vista centralizada de todos los dispositivos
- Cifrado de datos

¿Cómo funciona?

La protección es brindada por una EPP. Estas soluciones funcionan bajo un paradigma cliente-servidor.

¿Cómo funciona?

Brindan una consola centralizada desde la que pueden monitorear y administrar todos los dispositivos de la red (servidor)

¿Cómo funciona?

Los clientes se pueden instalar remotamente o de forma manual en cada dispositivo y se actualizan bajo comando de la consola central.

Soluciones

Proveedores Cloud



SOPHOS



Malwarebytes™



SentinelOne®



Plan de Continuidad de Negocio (BCP)

¿Qué es “Continuidad de Negocio”?

Es la capacidad de una organización de continuar operando y entregando productos y/o servicios según unos niveles predefinidos *aceptables* luego de un incidente disruptivo.

¿Qué es un BCP?

Es un documento que contiene toda la información necesaria para lograr la “continuidad de negocio”. Recopila el resultado de un proceso completo que incluye, entre otras cosas, los siguientes pasos:

Análisis de Impacto de Negocio (BIA)

Identificar:

1. Principales funciones de negocio
2. RTO y RPO por función de negocio
3. Recursos requeridos por función de negocio
4. Impacto/costo financiero
5. Impacto/costo operacional
6. Impacto/costo legal

Elements of business impact analysis

	Fire in data center	Loss of specialized staff	Vehicle crash in front entrance of office building	Vandalism to primary product assembly line	Loss of staff due to COVID-19 illness
BUSINESS ACTIVITY AFFECTED	All activities in data center	Activities that require specialized staff	All activities at that location unless an alternate access option is available	Loss of primary production line	Loss of possibly key employees needed to run the business
POTENTIAL OPERATIONAL LOSS	Inability to function normally	Reduced ability to function normally	Nominal disruption based on how quickly the vehicle can be removed and the front entrance reopened	Inability to produce the company's primary product	May be nominal to significant depending on who is affected
POTENTIAL FINANCIAL LOSS	\$3,000 to \$4,000 revenue loss per hour	None, assuming backup staff is available	None, assuming alternate entrance is available and access to building facilities is available	\$25,000 to \$40,000 per hour in lost revenue	Could be minimal assuming employees can work remotely
MINIMUM TIME NEEDED TO RECOVER OPERATIONS	Three to four hours	One to two hours	Depending on the damage from the crash, up to one day	Days if a work-around can be built; weeks if an alternate production facility must be found and launched	24-48 hours depending on health status and if employees can work remotely
					

Análisis de Riesgos

- Se busca identificar amenazas, vulnerabilidades y riesgos de la información.
- Por cada amenaza identificada se considera su *probabilidad* y el *impacto*.
- Las amenazas se pueden clasificar en naturales, causadas por el hombre o fallas de infraestructura.
- Se pueden identificar controles y costos para cada riesgo.

ID	Category	Description	Consequence	Probability	Impact	Risk Level	Risk Modification Plan	Risk Owner	Residual Risk Level
1	Employee	It takes too long to contact a lead, and this time may not decrease with the new sales program	We will not increase sales revenue	High	High	High	Map out current processes to find inefficiencies so wasted steps are not included in new program	Brady	Medium
2	Customers	Customers are leaving, and we do not know why	We will not know how to reduce the number of customers who leave	Medium	High	High	Create a survey, and partner with firm to deliver survey to customers	Sami	Low
3	Employee	The new employee learning program may not be approved by the board	We will not be able to provide professional development to all employees	Low	Medium	Medium	Prepare and present ideas at board meeting next week	Jesse	Low
4	Employee	There is no documentation of different roles within the company	Cross-training employees will be inefficient	Medium	Medium	Medium	Begin creating tutorials specific to different roles	Jesse	Low

Plan de Recuperación

Desarrollar una guía que permita al negocio volver a un nivel de operación aceptable.

Esta guía debe contar con:

- Eventos que desencadenan el plan.
- Equipo responsable de atención de incidentes.
- Plan de recuperación de incidentes.
- Lista de contactos.

Plan de Recuperación de Desastres (DRP)

Este incluye:

- Inventario de infraestructura vital.
- Manual de procedimientos para restablecimiento.
- Operaciones manuales para reemplazar sistemas temporalmente.

Prueba y Mantenimiento

Se deben establecer estrategias para:

- Probar la efectividad del plan regularmente.
- Entrenar al personal para que conozcan el plan.
- Actualizar el plan continuamente.

DLP

Data Loss Prevention

¿Qué es?

Una solución que detecta y previene fugas de información. Detecta y bloquea la extracción de información *en uso* (dispositivos), *en movimiento* (red) y *almacenada* (discos).

¿Por qué es necesario?

- Previene fugas de información.
- Protege información sensitiva personal (PII)
- Protege propiedad intelectual (IP).
- Ayuda al cumplimiento de regulaciones como CCPA, GDPR, HIPAA, entre otros.

Implementaciones

Proveedores



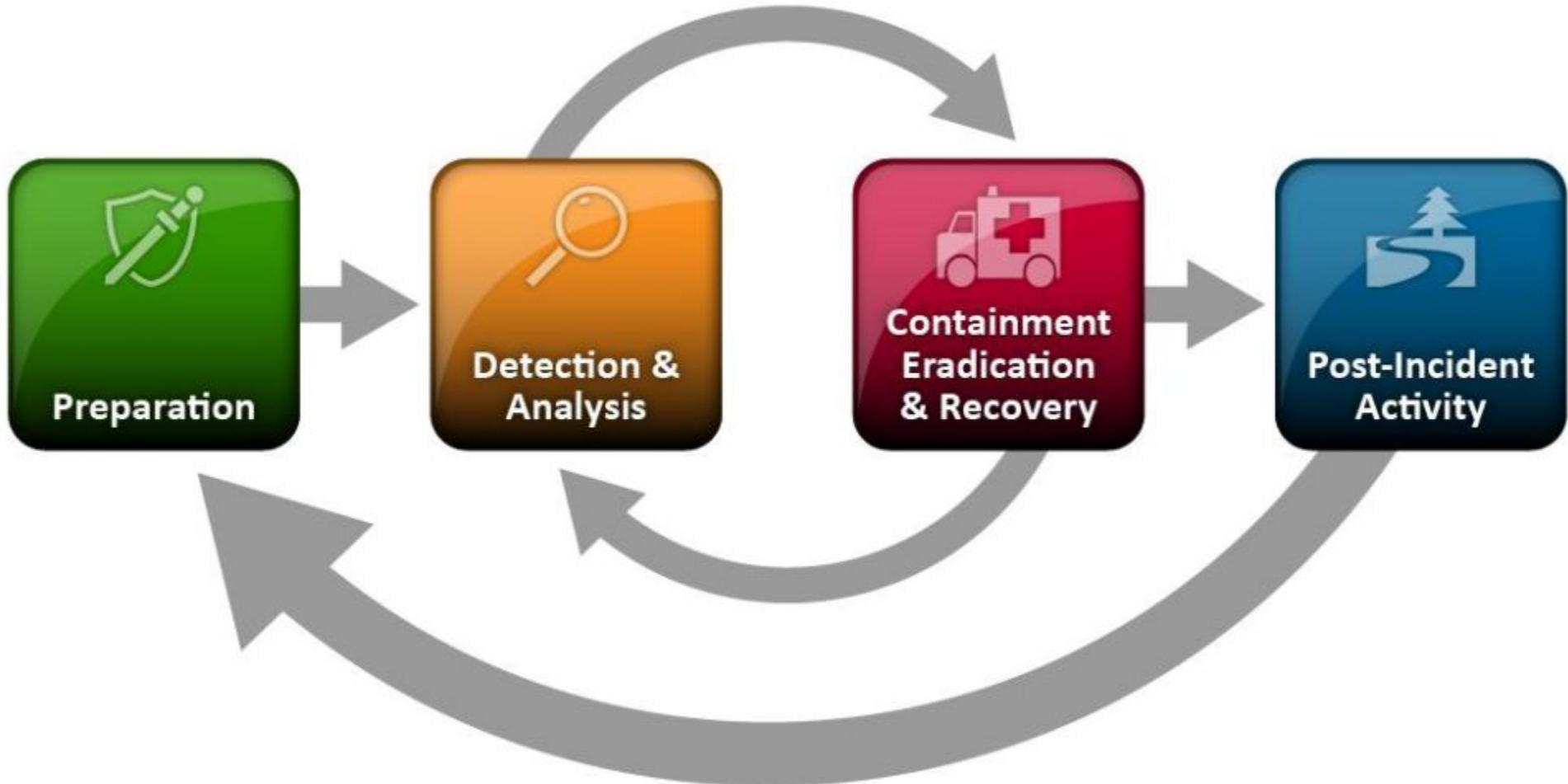
Gestión de Incidentes de Ciberseguridad

¿Qué es?

Es un proceso que permite una respuesta efectiva y rápida a ciberataques. Idealmente, existe un plan que documenta una serie de procesos y pasos que se deben realizar en cada fase de la respuesta a un incidente.

Estándar

Una buena práctica es basarse en estándares reconocidos por la industria, el más usado es la “Guía de manejo de incidentes de seguridad informática” NIST 800-61r2.



¿Cómo responder ante un incidente de seguridad?

1. **Preparación:** Estimamos las necesidades y establecemos procedimientos.
2. **Detección y Análisis:** Es identificar los signos inusuales que pueden generar dicho incidente.
3. **Identificación:** Identificamos qué tipo de incidente fue y ocurrió, qué tan grave puede ser.

¿Cómo responder ante un incidente de seguridad?

4. **Notificación:** Reportamos, notificamos y registramos el incidente.
5. **Clasificación y priorización:** Debemos determinar el tipo de incidente, clasificarlo y así saber qué tan grave es y qué tanto nos puede afectar.

¿Cómo responder ante un incidente de seguridad?

6. **Contención, resolución y recuperación:**
Detenemos el ataque y evitar que se propague. Resolvemos el incidente. Recuperamos los datos.
7. **Acciones posteriores al cierre:** Lecciones aprendidas. Identificamos las causas del incidente, por qué pasó y cómo podemos hacer, para qué no vuelva a pasar.

Controles para BYOD

Bring Your Own Device

Software Pirata

- Software pirata y activadores usualmente vienen con troyanos.
- Se debe restringir su instalación.
- Considerar opciones open source o pagas.

Actualización de Software

- Incluye parches de seguridad.
- Mejora rendimiento.
- Nuevas funcionalidades.

Redes Públicas

- Implementación de sniffers.
- Los ataques de Man-in-the-Middle son fáciles de llevar a cabo.
- Se recomienda evitar el uso de redes públicas en lo posible.
- Uso de VPNs si es necesario el uso de una red pública.

Cifrado Disco

- En caso de pérdida o robo, la información estará a salvo.
- Cada OS viene con herramientas por defecto para realizar este proceso.

DNS

- Libro telefónico de internet.
- Capa adicional de seguridad.
- Puede mejorar la latencia.

Cloudflare (1.1.1.1, 1.1.1.2, 1.1.1.3)

Google Public DNS (8.8.8.8)

OpenDNS (208.67.222.222)

Endpoint Protection

- Solución completa que incluye varios controles de seguridad.
- Preferiblemente de pago.
- Mantener actualizado.

Gestión de Contraseñas

Uso de frases en vez de contraseñas complejas.

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

3@pgcCfk

.....

It would take a computer about

8 hours

to crack your password

How Secure Is My Password?

The #1 Password Strength Tool. Trusted and used by millions.

me gusta la ciberseguridad

.....



It would take a computer about

1 nonillion years

to crack your password

Gestión de Contraseñas

Manejadores de contraseñas



CEO

Chief Executive Officer

¿Quién es?

Director Ejecutivo,
Gerente y líder general
de la empresa.

Patrocinador oficial de
la Seguridad de la
Información en la
empresa.



Responsabilidades

- **Recurso Humano para Ciberseguridad**
Aprueba las contrataciones de personal requerido.
- **Garantiza el cumplimiento**
Permite que sea obligatoria la aplicabilidad de ciber-controles.

Responsabilidades

- **Gestión de Riesgos**

Define como prioridad el tratamiento de riesgos de activos de información.

- **Cultura organizacional**

Promueve la concienciación en ciberseguridad para todo el equipo de trabajo (comunicación).

CISO

Chief Information
Security Officer

¿Quién es?

Es la persona responsable de la Seguridad de la Información en la empresa.

Alinea la seguridad con la misión del negocio.



Responsabilidades

- **Generar políticas de Seguridad**
Establece directrices y reglas al interior de la organización en función de la información.
- **Garantiza la privacidad de los datos**
Vela por el cumplimiento de normativas en la correcta Gestión de Datos Personales.

Responsabilidades

- **Auditor Interno en Ciberseguridad**
Revisa que los riesgos a los que se expone la información sean mitigados.
- **Acompaña los procesos de certificación**
Prepara a la empresa para cumplir estándares internacionales en Seguridad.

CSO

Chief Security Officer

¿Quién es?

Encargado de la Seguridad física y tecnológica.

Comparte la responsabilidad con el CISO.



Responsabilidades

- **Riesgos**

Detecta los ciber-riesgos a los que se enfrentan los activos de TI.

- **Gestionar proyectos**

Realiza labores de *project management* sobre proyectos de ciberseguridad aplicada.

Responsabilidades

- **Conocimiento Legal**

Investiga y tiene claridad sobre *Cibersecurity Compliance*.

- **BCP & DRP**

Ejecuta planes de Continuidad del negocio y Recuperación ante desastres o incidentes de Ciberseguridad.

Responsabilidades

- **Canal de comunicación con la Gerencia**
Su ubicación en la jerarquía organizacional permite enlace directo con el CEO.

CIO

Chief Information Officer

¿Quién es?

Encargado de las
Tecnologías de
la Información
en la empresa.

Aplica siempre la
Ciberseguridad en
su labor.



Responsabilidades

- **Ciber-receptivo**
Recibe conceptos sobre controles de ciberseguridad y los aplica.
- **Riesgo**
Gestiona los ciber-riesgos implícitos en la tecnología que administra.

Responsabilidades

- **Promotor de Ciberseguridad**
Es un *Security Champion* dentro del esquema organizacional de la empresa.
- **Ciber-inversionista**
Agrega el requerimiento de Ciberseguridad a toda inversión en tecnología (\$).

CIO en Acción!

Penetration Tester

Pentester

¿Quién es?

Auditor interno
o externo en
Ciberseguridad.

Simula ciberataques
hacia activos de TI
de la organización
(*penetration testing*).



Responsabilidades

- **Estado de Ciberseguridad**
Reporta fallas en la Ciberseguridad de la empresa y propone un nivel de Riesgo.
- **Ciber-Orientador**
En algunos casos, propone soluciones y posibles controles a fallas detectadas.

Metodología



Tipos de *Pentesting*

- **BlackBox**

No tiene mayor información de su objetivo, solo una URL o dirección IP.
- **WhiteBox**

Cuenta con accesos para realizar una auditoría más profunda.

Tipos de *Pentesting*

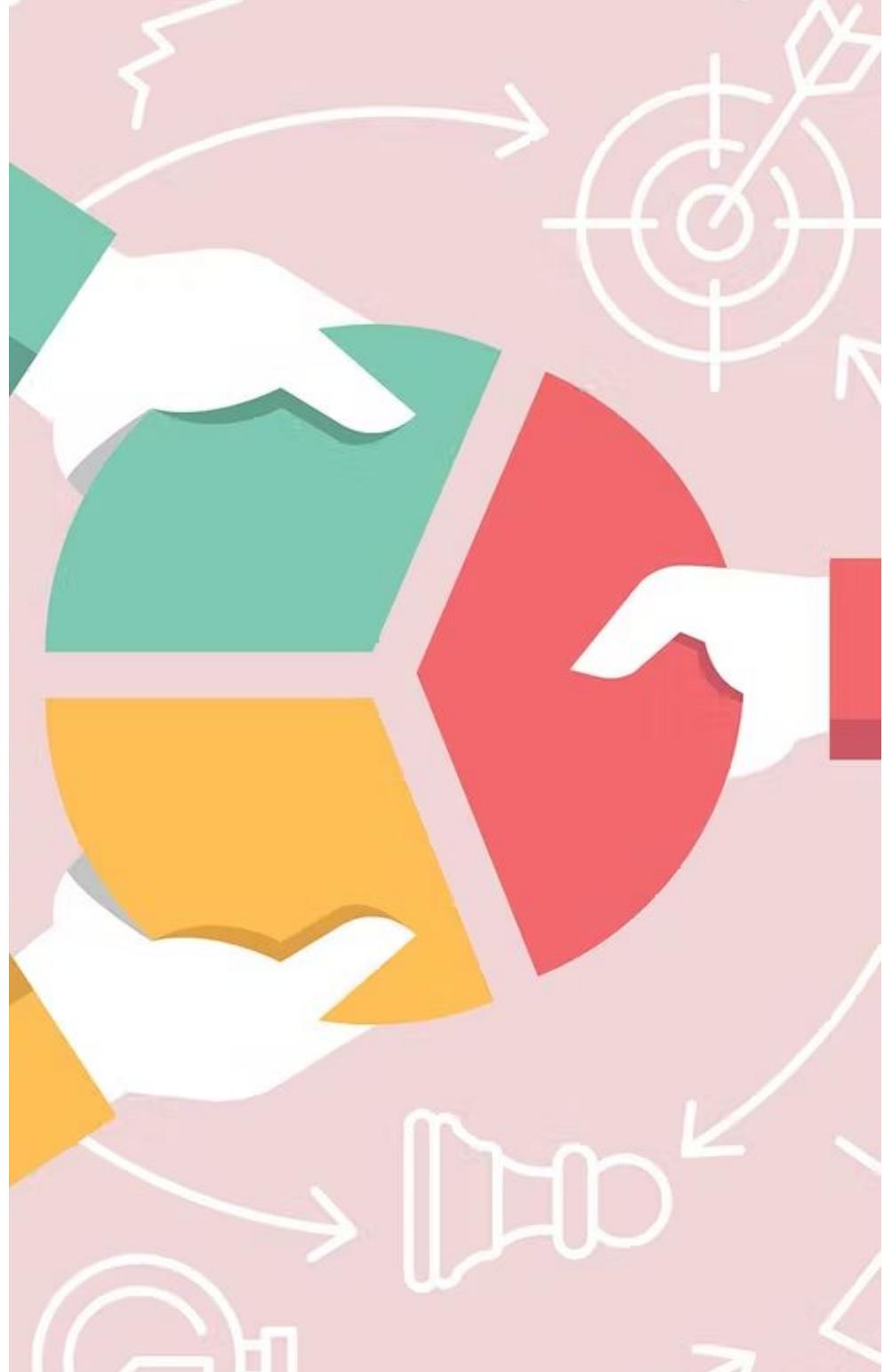
- **GrayBox**

Cuenta con ciertos accesos limitados para que realice su labor de auditoría (Ejemplo: acceso a *VLAN*).

Stakeholders

¿Quiénes son?

Todas aquellas personas, empresas o aliados que aportan al cumplimiento de controles de Ciberseguridad.



Tipos

- **Sector Privado**

Todos aquellos proveedores de tecnología y ciberseguridad como AWS, Google y Microsoft.

- **Sector Público (Gobiernos)**

Entidades que generan directrices y normativas en ciberseguridad (NSA, Ministerios TIC).

Responsabilidades

- **Aplican controles**

Se comprometen con la ejecución de controles de Ciberseguridad definidos por la empresa.

- **Promueven *Compliance***

Adquieren certificaciones internacionales en Ciberseguridad y transmiten ciber-tranquilidad.

Responsabilidades

- **Ciber-Auditores**

Vigilan que las buenas prácticas en Ciberseguridad se cumplan.

- Bienvenida
- Presentación de Diego
- Presentación de JJ
- Overview de los módulos
 - Qué es la ciberseguridad
 - Campos de acción
 - ciberamenazas
 - controles
 - roles

- 
- Felicitar por haber finalizado el curso
 - Qué aprendieron?
 - Estarán atentos a las preguntas
 - Tomar examen y dejar reseña
 - Continuar con los siguientes cursos de la ruta.
 -