

Curso de

Hacking de Servicios de Red

Daniel Carvajal



Componentes de una red

Introducción al Hacking
de Servicios de Red



¿Qué es una red?

Es el enlace de comunicación entre dos o más dispositivos para compartir recursos.





Componentes de una Red

- Modem
- Router
- Gateway
- Switch
- Bridge
- Repeater
- Access Point
- Firewalls





Dispositivos de una Red

- Computadora de escritorio
- Laptops
- Tablets
- Smartphones
- IoT
- Sistemas embebidos
- Servidores
- Impresoras





Dispositivos de una Red

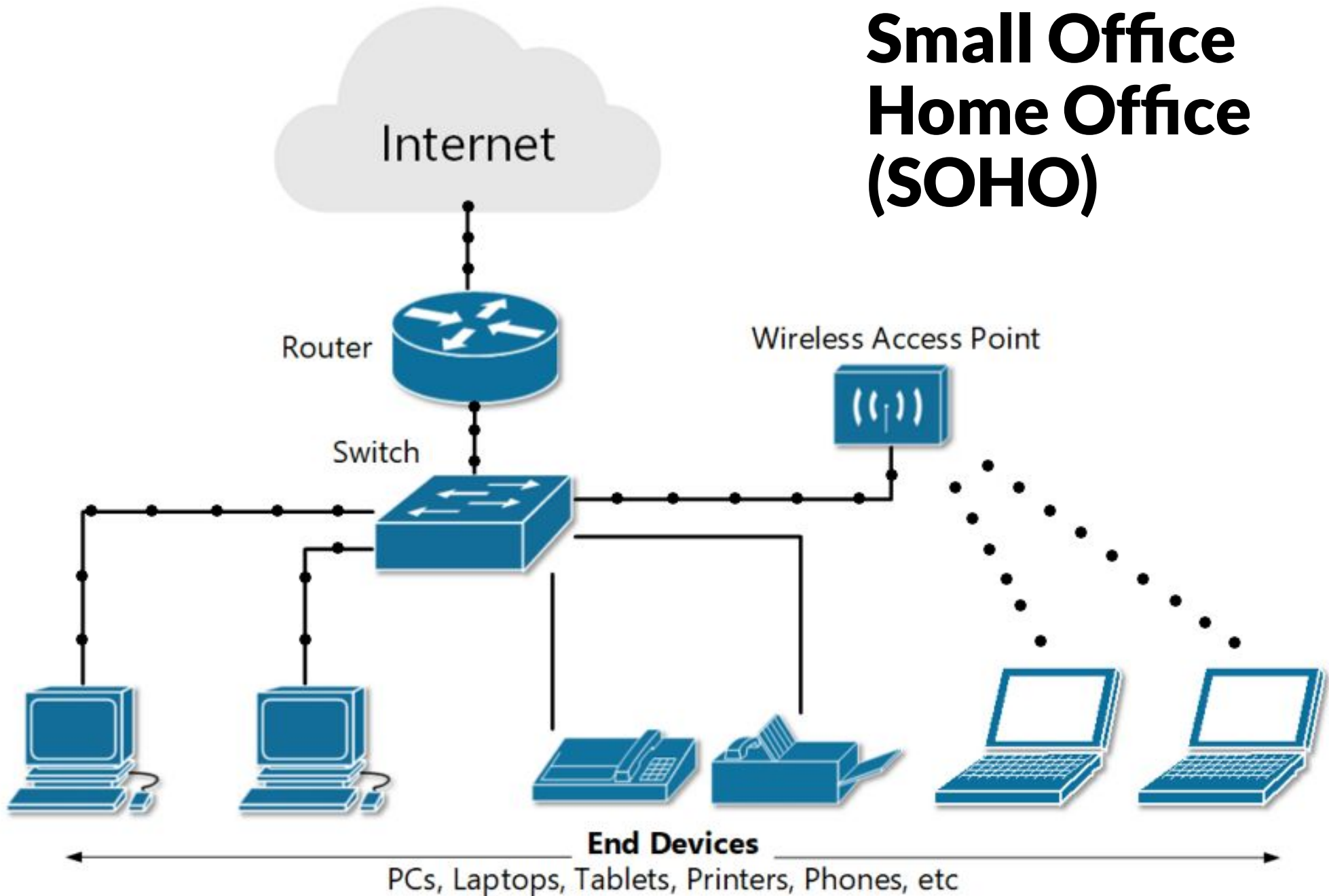
- VoIP
- Cámaras de vigilancia
- Sensores
- Actuadores
- PLCs

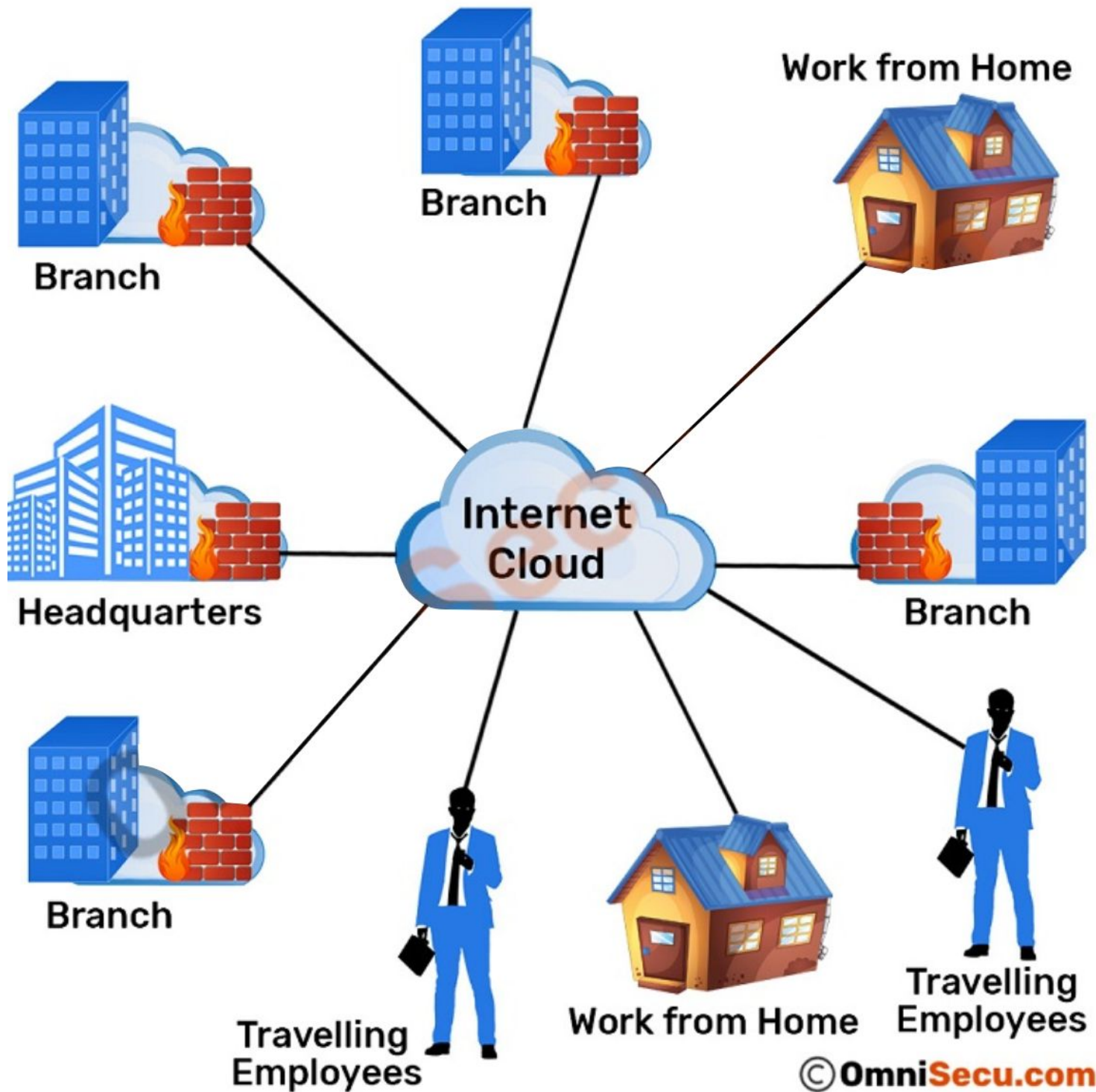


Tipos de redes LAN

Introducción al Hacking
de Servicios de Red

Small Office Home Office (SOHO)







Infraestructura como servicio (IaaS)



Plataforma como servicio (PaaS)



Software como servicio (SaaS)



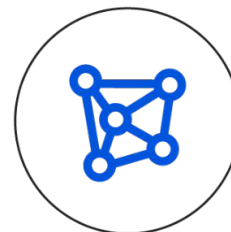
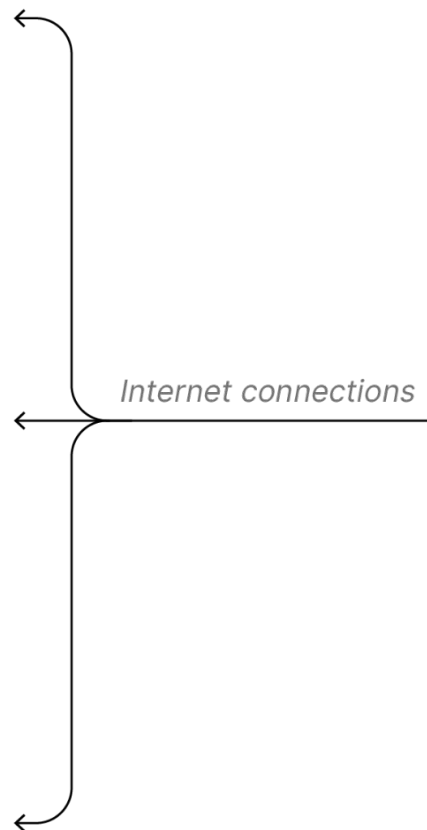
Remote users



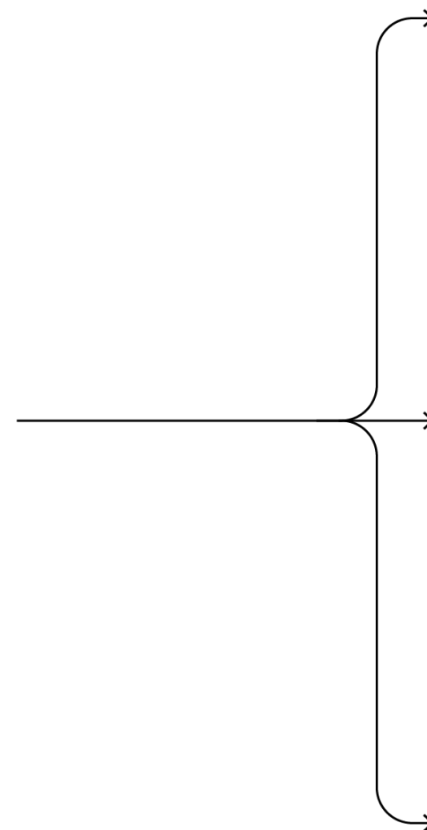
Branch offices



Data centers



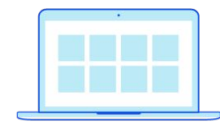
NaaS



Public internet



SaaS



Internet apps

INTRANET



ACCESS



COLLABORATION



DATA



COMMUNICATION



PRIVATE NETWORK



INFORMATION



Tipos de firewall

Introducción al Hacking
de Servicios de Red



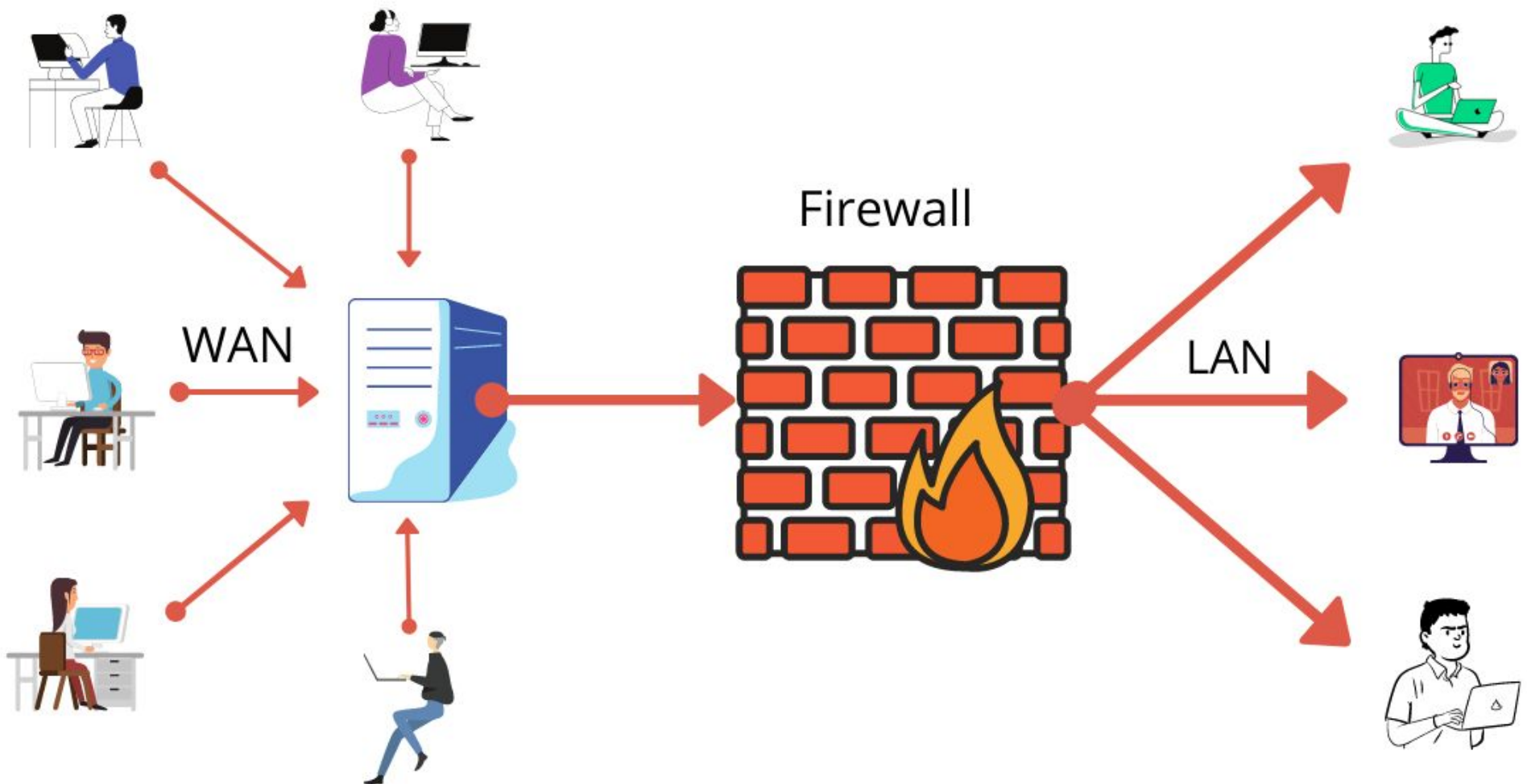
Tipos de FireWall

- Firewall
- IDS
- IPS
- NGFW
- FWaaS
- WAF





Firewall





IDS Vs IPS





FWaaS

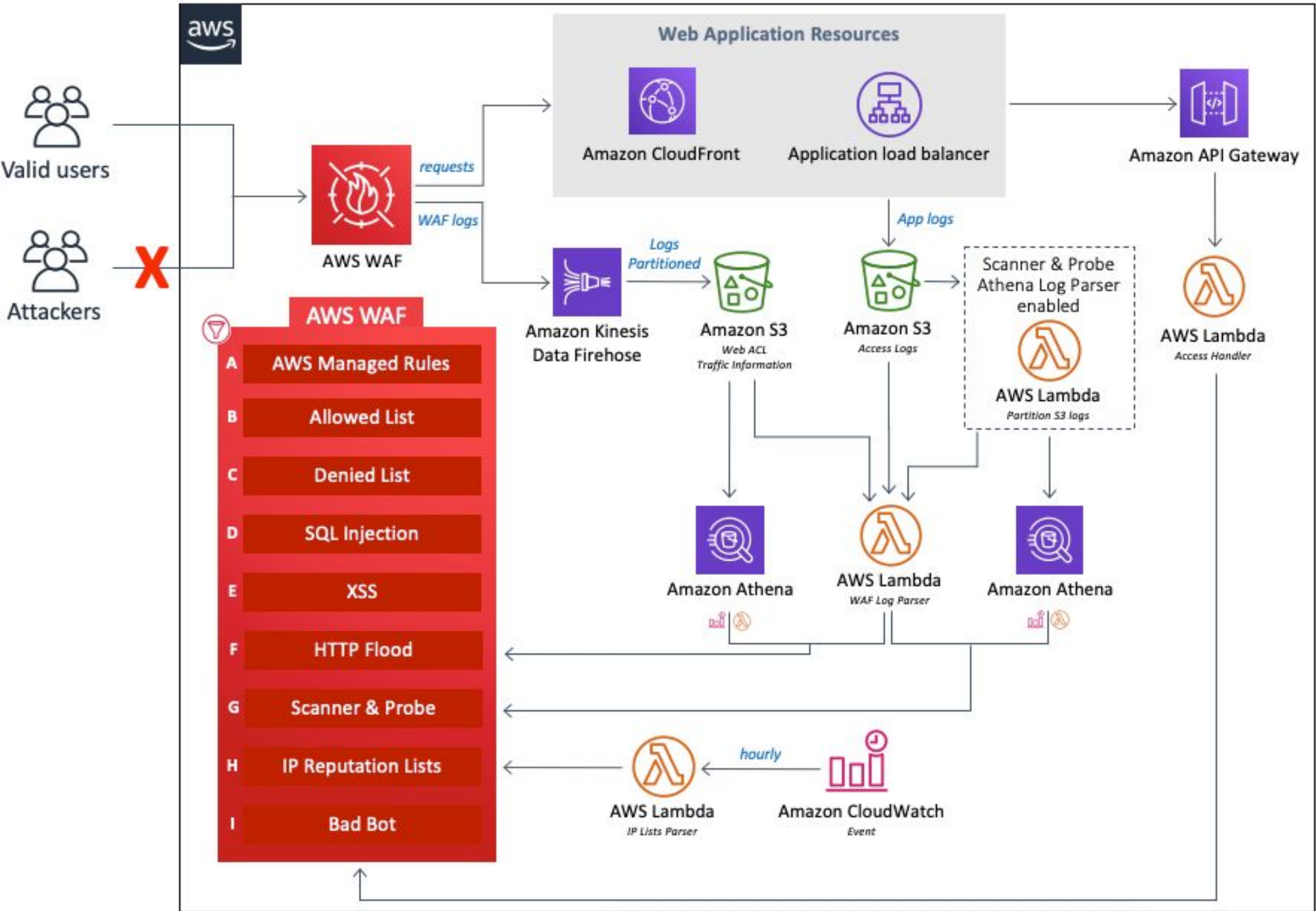
- Firewall hosted in the cloud.
- Managed by the cloud vendor.
- Scalability.
- Near real-time service provisioning.
- Improved performance with cloud applications.
- DNS Security

Next- Generation Cloud Firewall



NGFW

- Intrusion Prevention System.
- Deep Packet Inspection.
- Application Control.
- Threat Intelligence feeds.
- URL filtering.
- Traffic shaping.



Tipos de servicios de red

Introducción al Hacking
de Servicios de Red



Tipos de servicios

Servicios públicos

- SSH
- FTP/s
- HTTP/s
- SMTP/s
- POP3/s
- IMAP/s
- MySQL

Servicios privados

- SMB
- DNS *
- NTP *
- RDP
- DHCP
- IPP
- Active Directory
- NetBIOS
- RPC service

*Puede ser público o privado



Servicios públicos

- SSH.

Secure SHell.

El puerto TCP asignado
es el 22.





Servicios públicos

- FTP/s.

*File Transfer
Protocol.*

Utilizando
normalmente el puerto
de red 20 y el 21.





Servicios públicos

- HTTP/s.

*Hypertext
Transfer
Protocol.*





Servicios públicos

- SMTP/s.

*Simple Mail
Transfer
Protocol.*





Servicios públicos

- POP3/s.

*Post Office
Protocol.*

- IMAP/s.

*Internet Message
Access Protocol.*





Servicios públicos

- MySQL.

Puerto 3306.



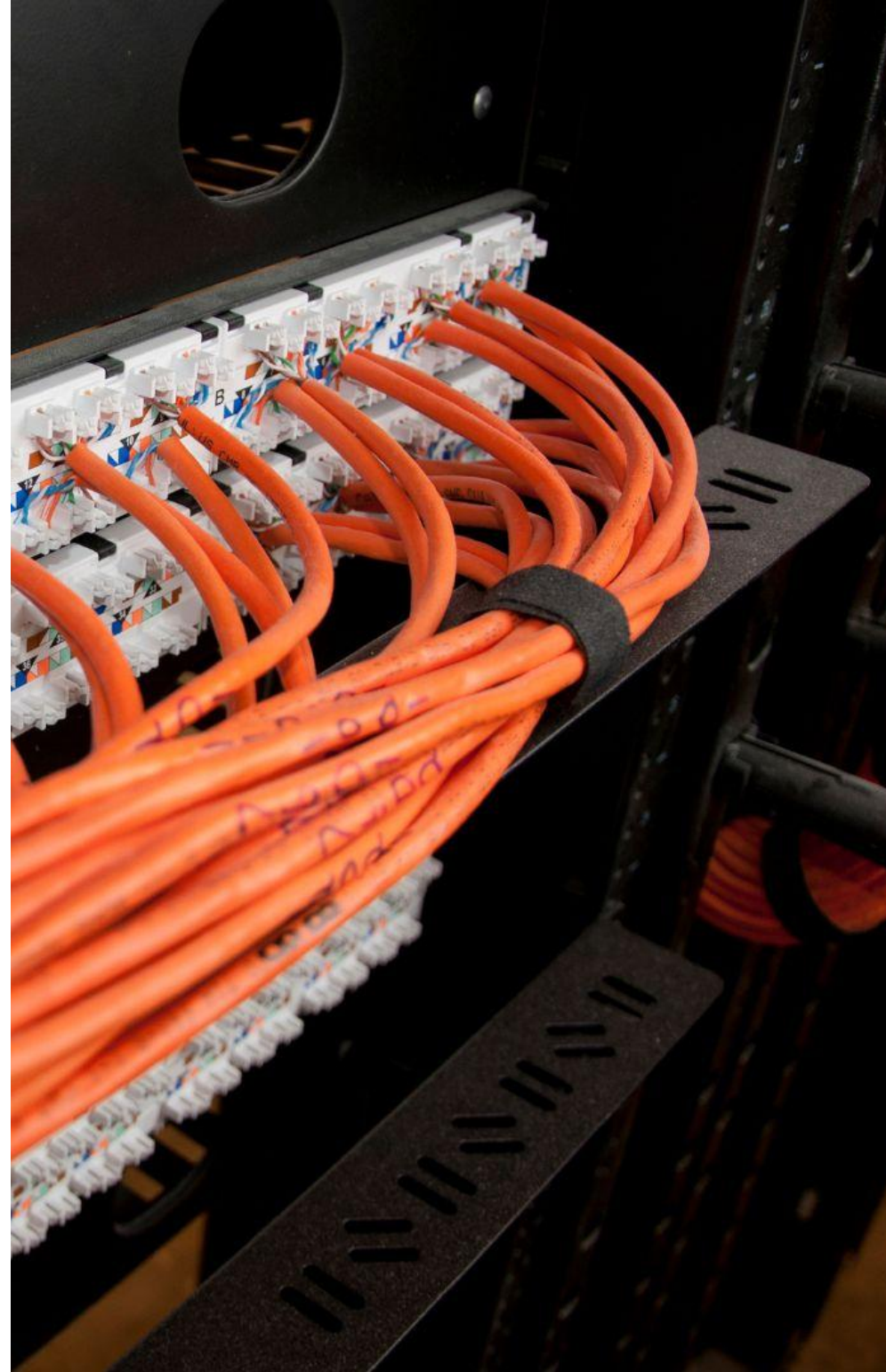


Servicios privados

- SMB.

*Server Message
Block .*

Usa el puerto 445.

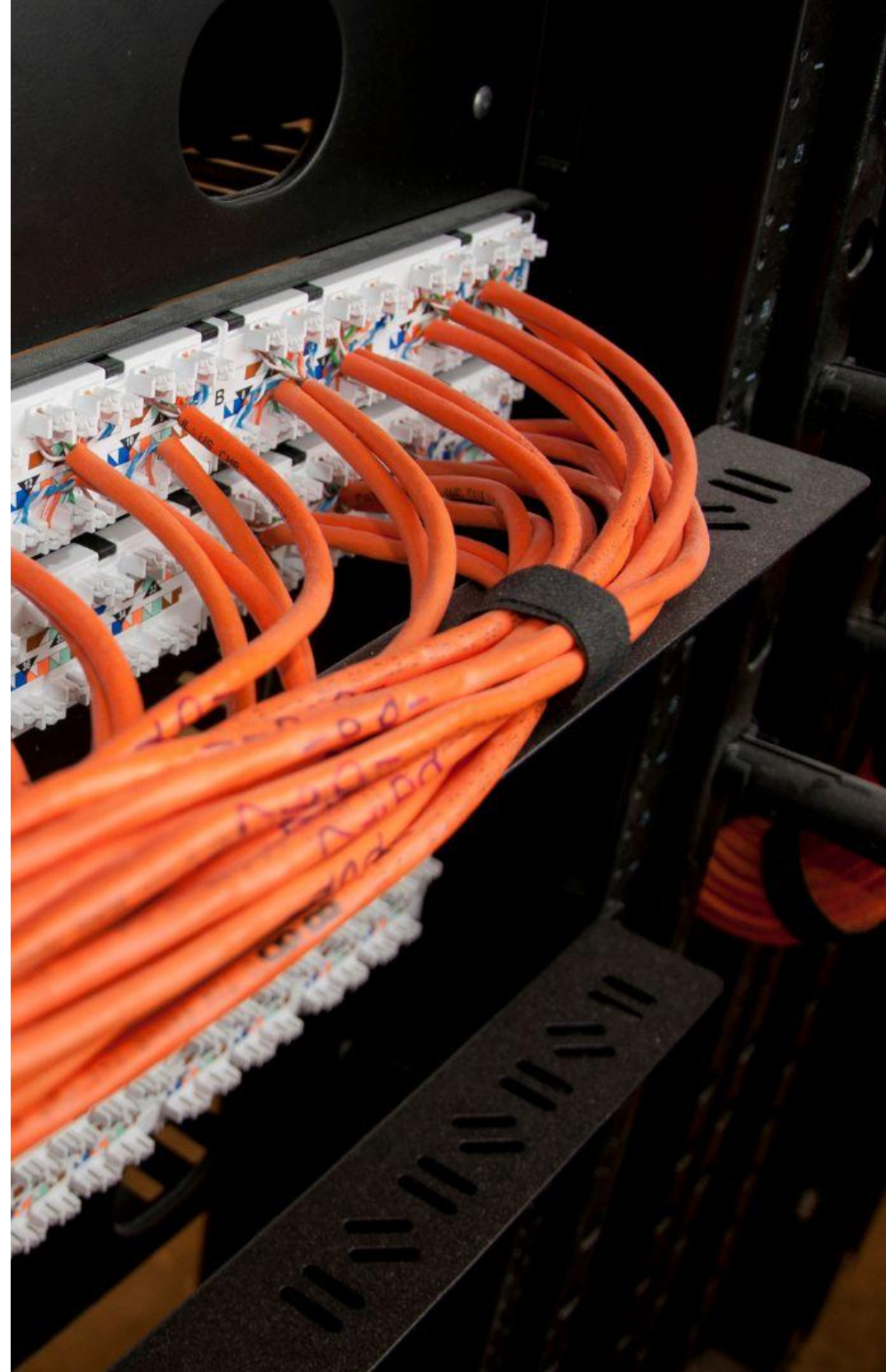




Servicios privados

- DNS.

*Domain Name
System.*

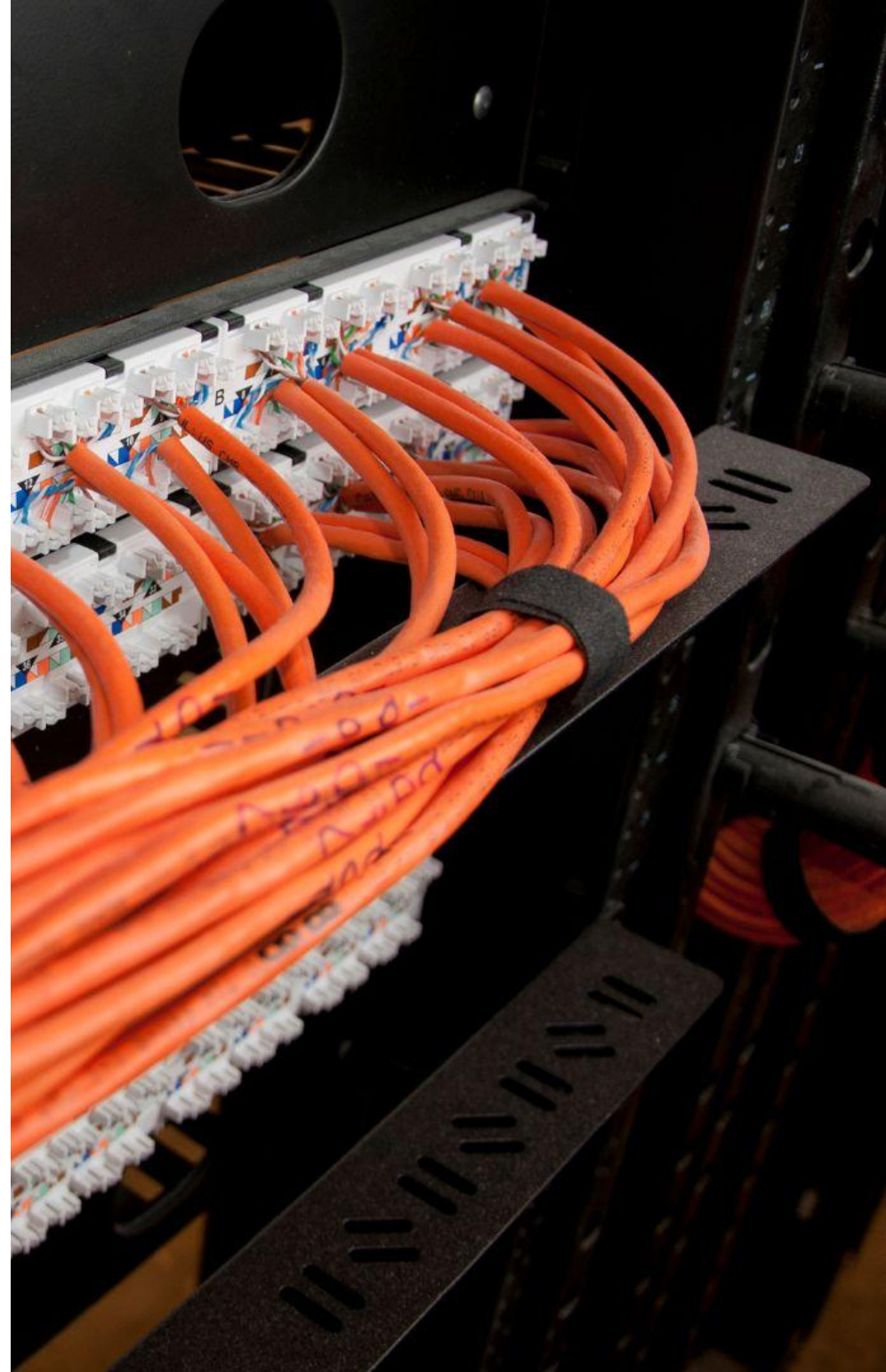




Servicios privados

- NTP.

*Network Time
Protocol.*

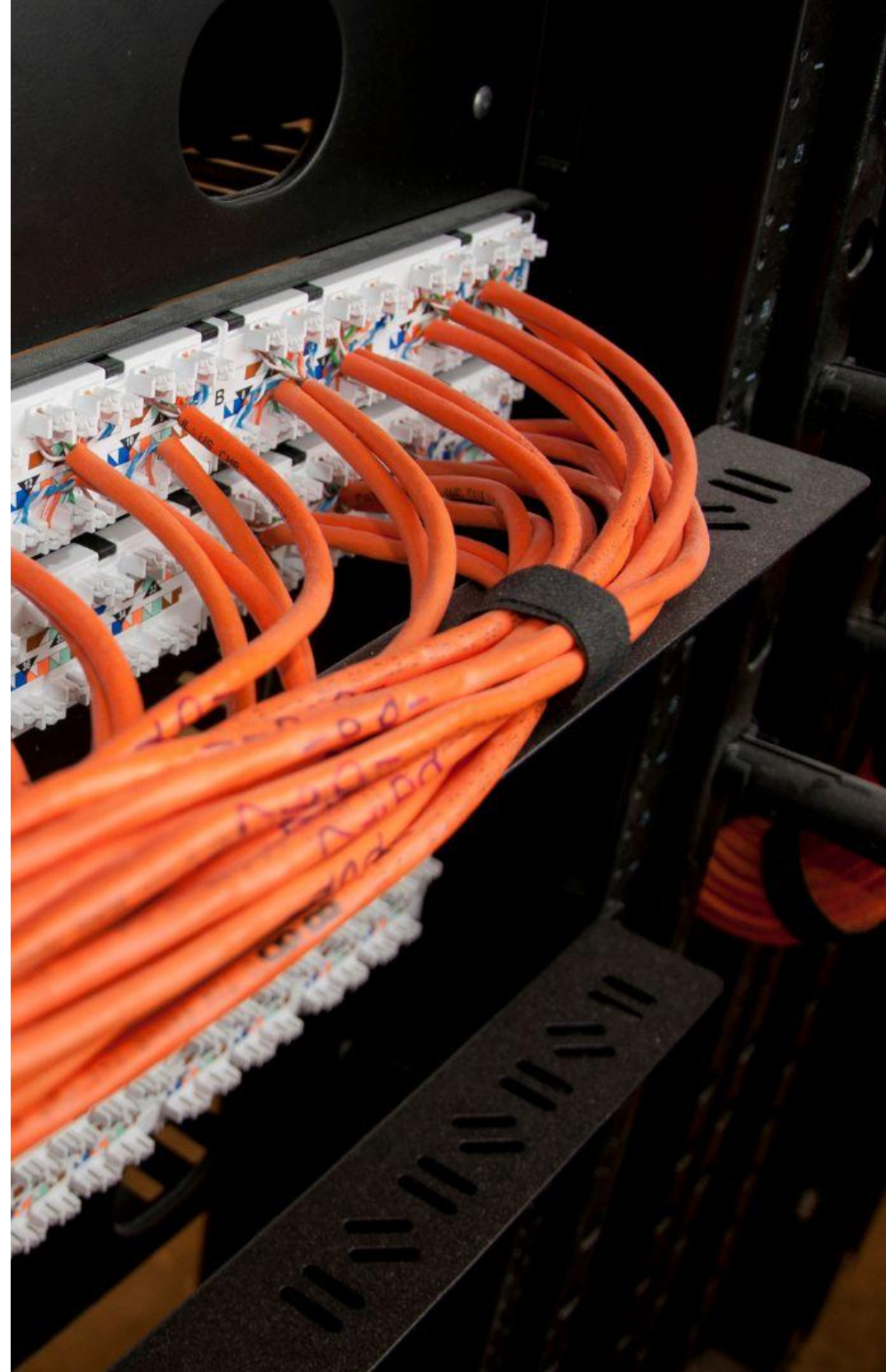




Servicios privados

- RDP.

*Remote Desktop
Protocol.*

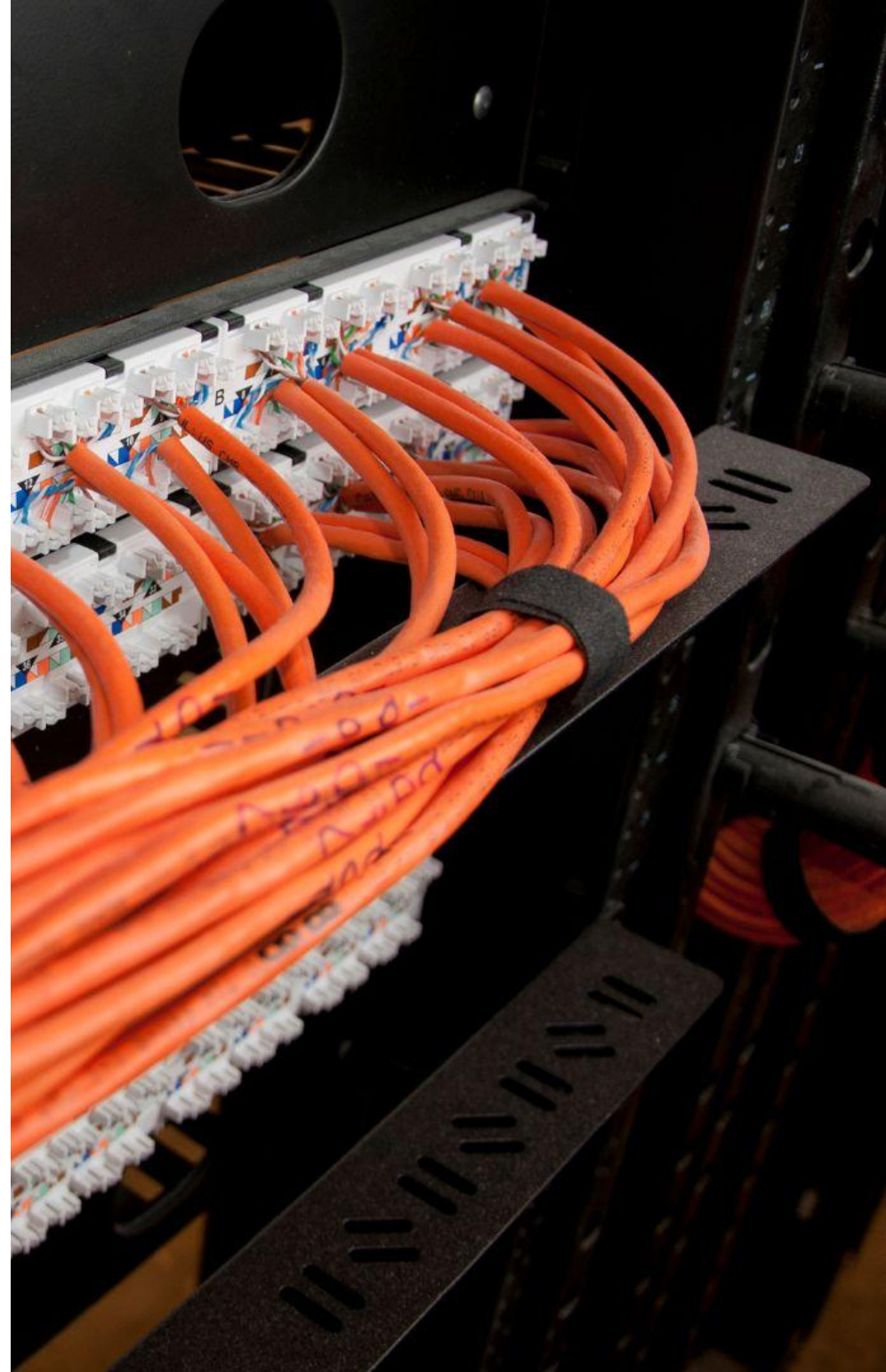




Servicios privados

- DHCP.

*Dynamic Host
Configuration
Protocol.*



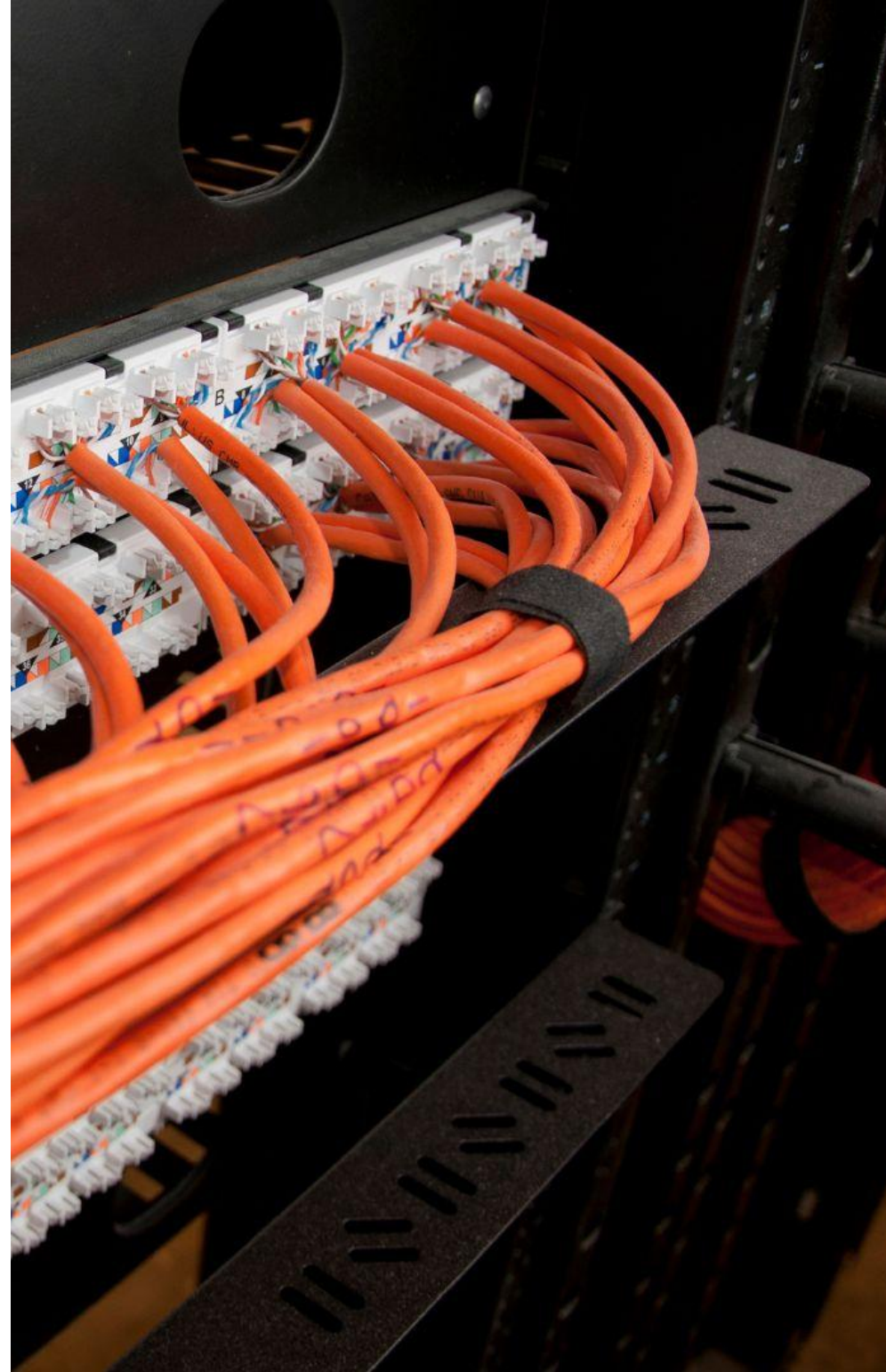


Servicios privados

- IPP.

Internet Printing Protocol.

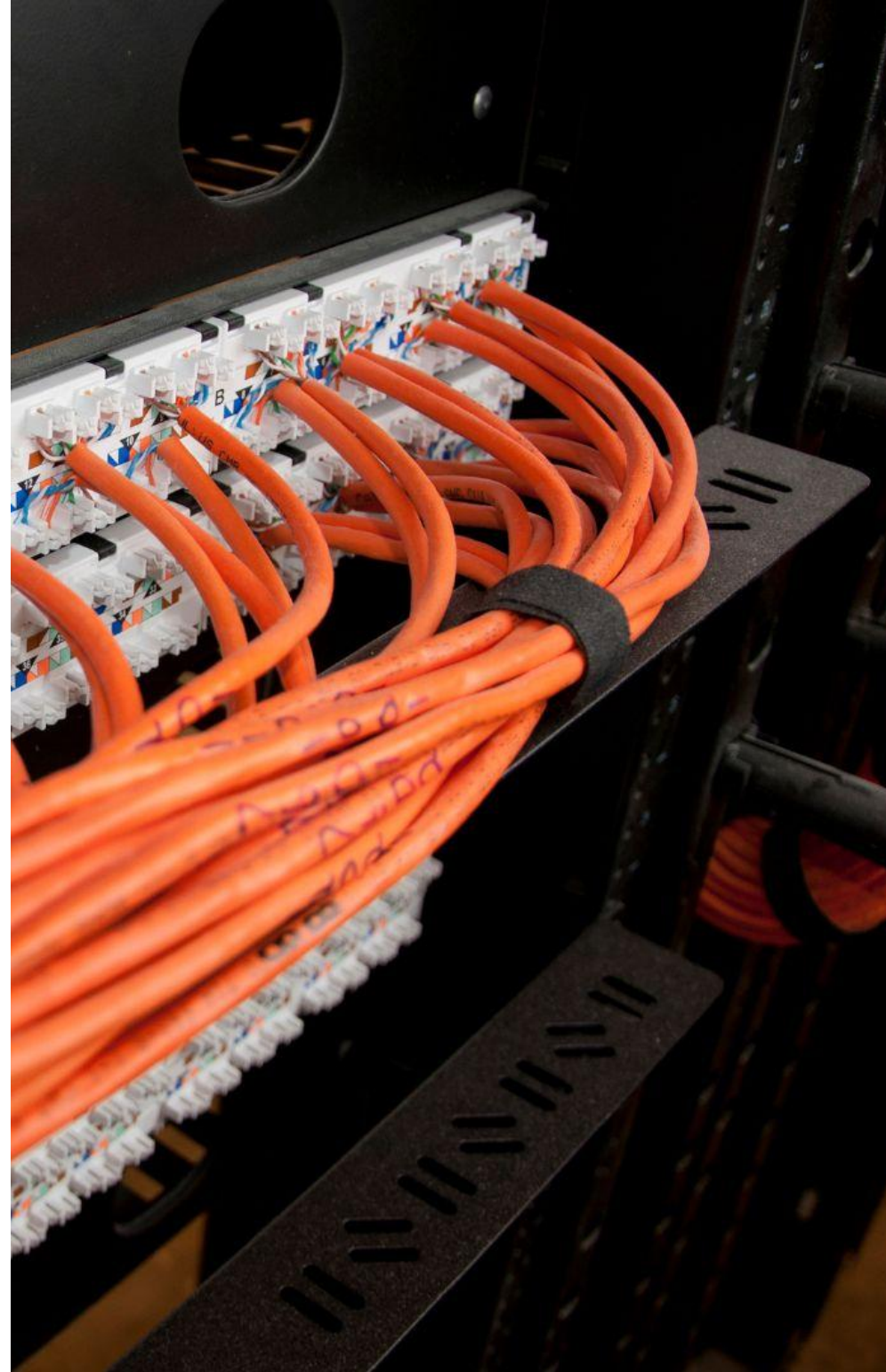
Usa el puerto 631.





Servicios privados

- Active directory.
- RPC services.





Recolección de inteligencia activa

Hacking de Servicios de Red



Análisis de vulnerabilidades

Hacking de Servicios de Red

Credenciales por defecto

Hacking de Servicios de Red

Seguridad por obscuridad

Hacking de Servicios de Red

Búsqueda de exploits

Hacking de Servicios de Red

Configuración de TryHackMe

Hacking de Servicios de Red

Explotación de servicios en Windows

Hacking de Servicios de Red

Hardcoded backdoor

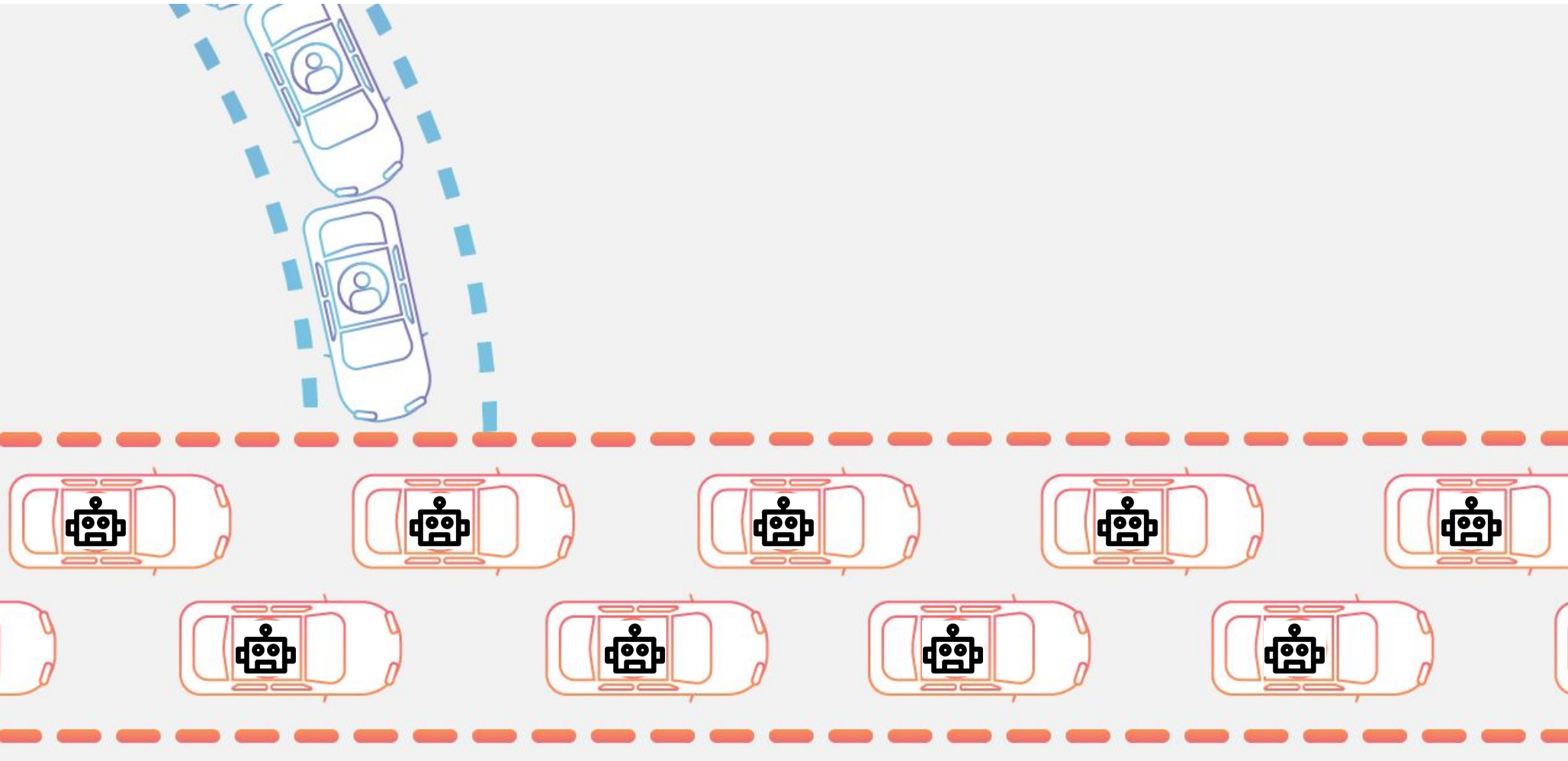
Hacking de Servicios de Red

Tipos de ataques DoS

Hacking de Servicios de Red

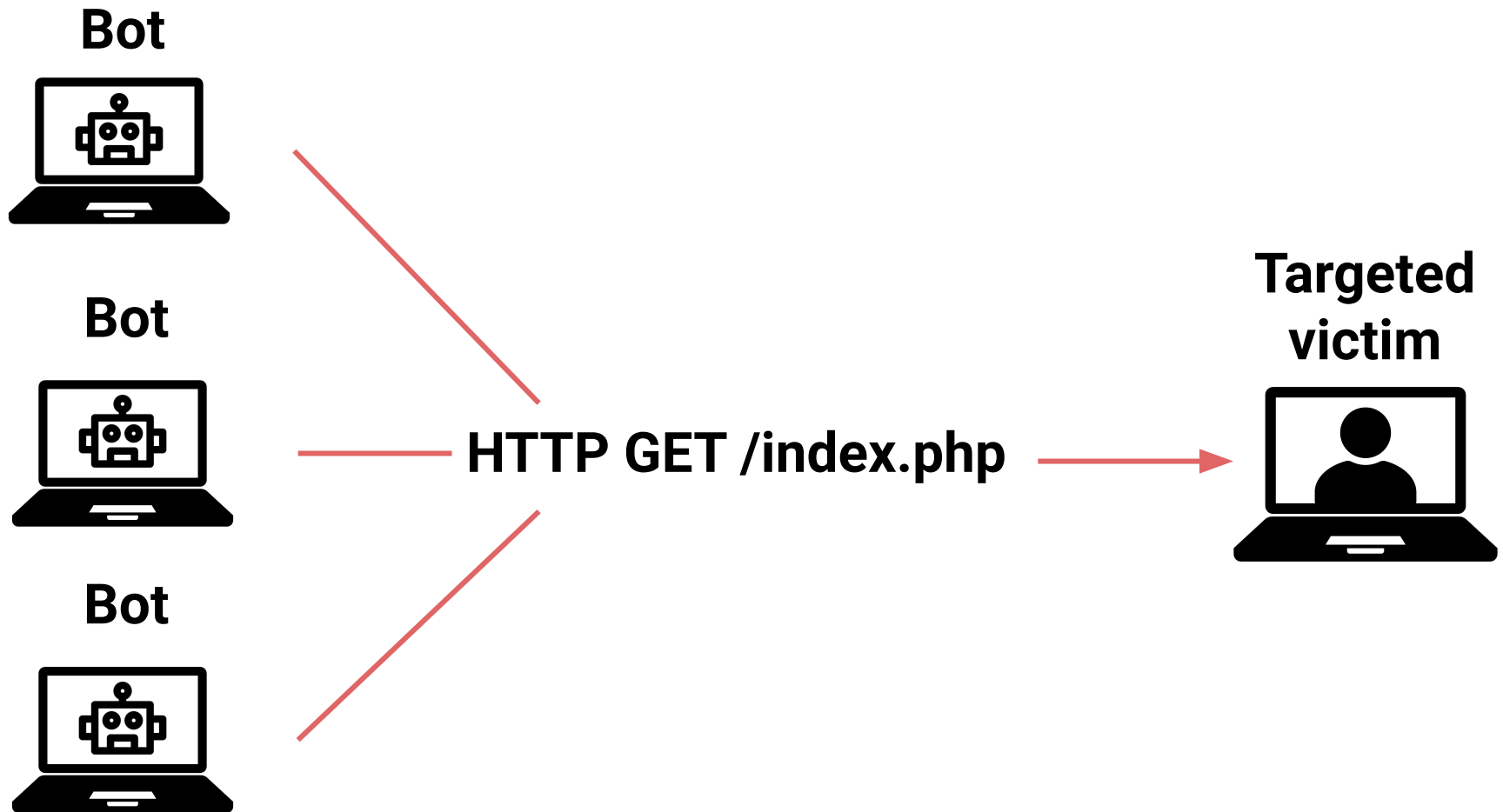


¿Qué es un ataque DoS?





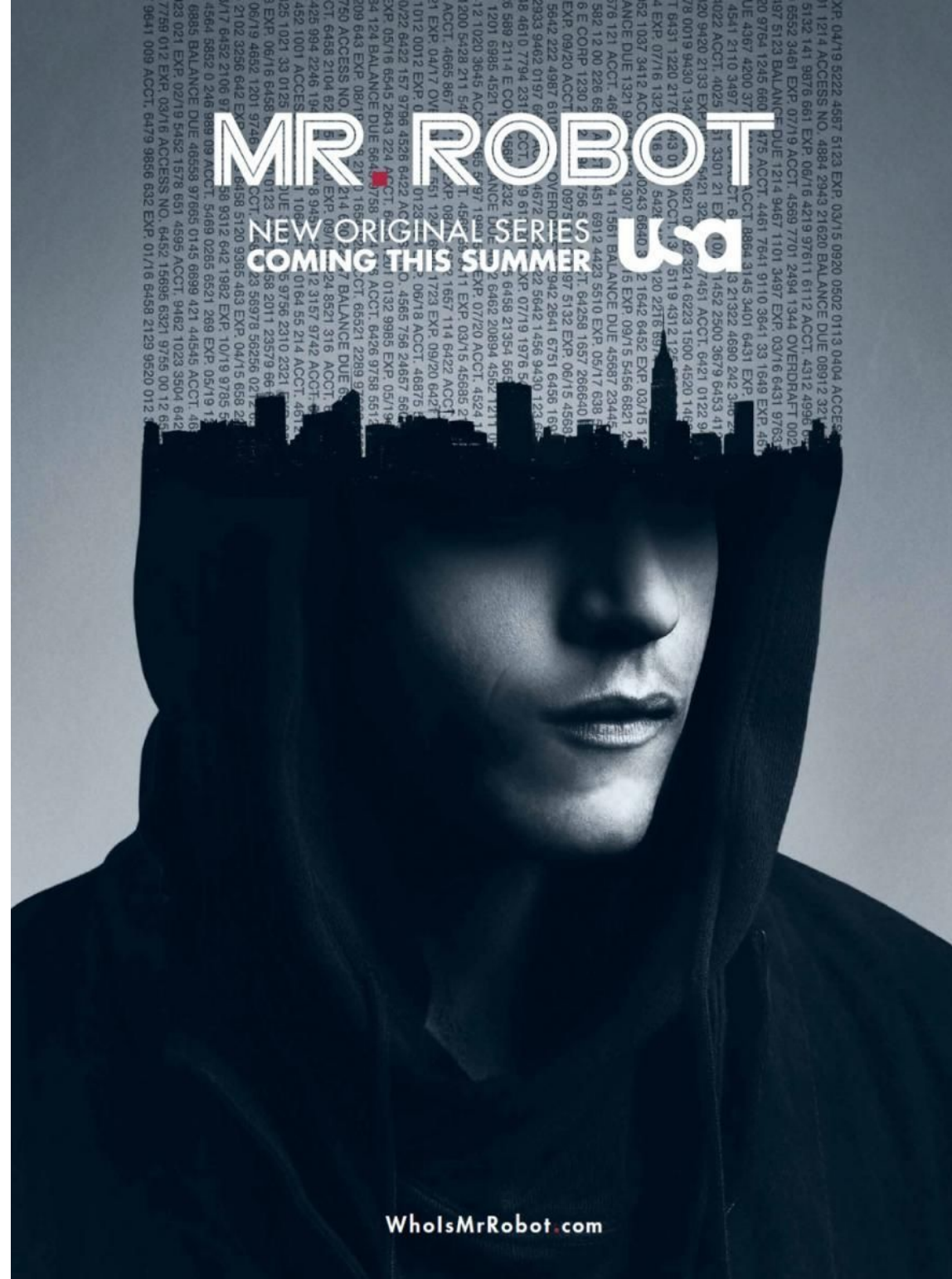
Ataques de aplicación





R.U.D.Y

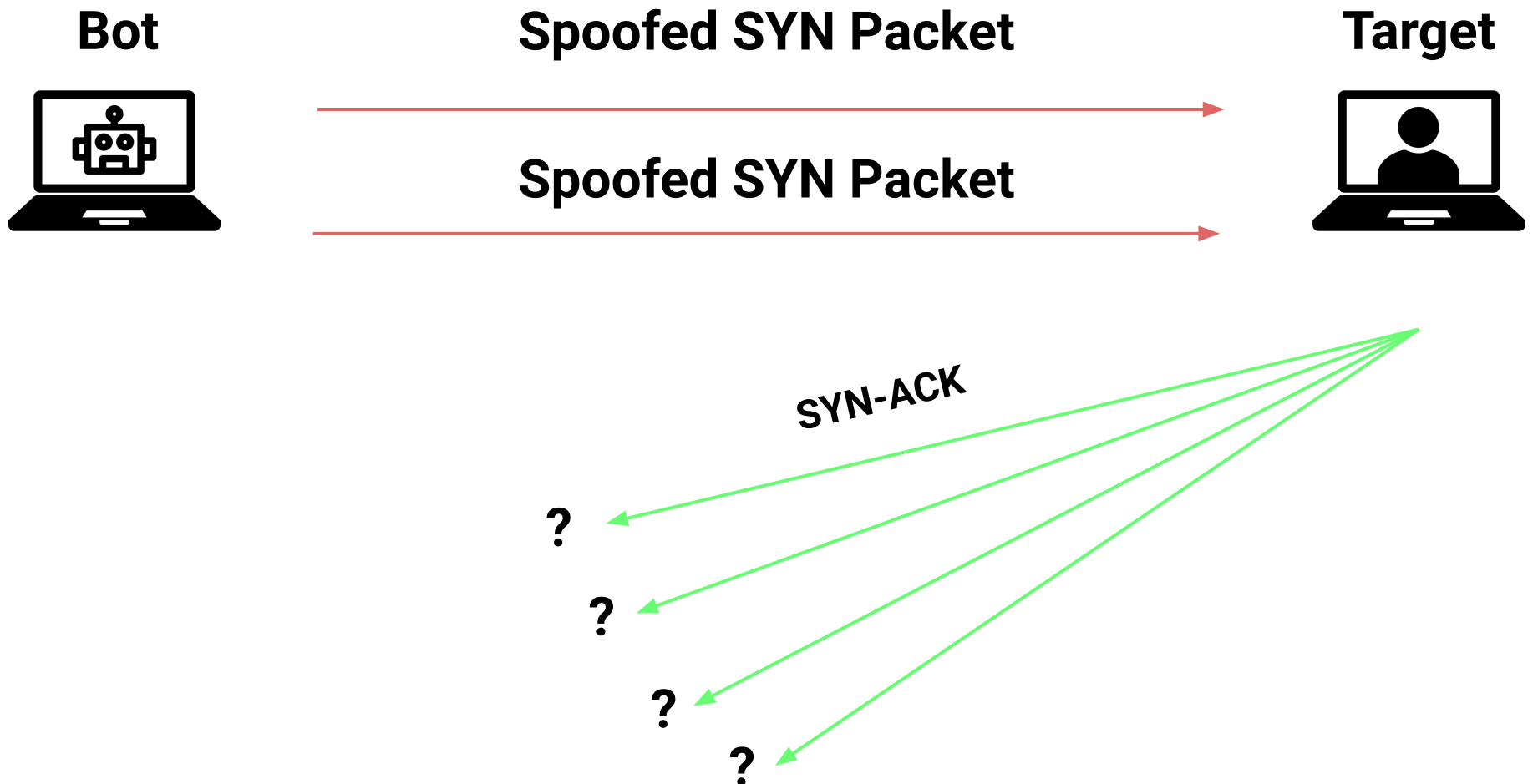
R. U. Dead. Yet.



WholsMrRobot.com

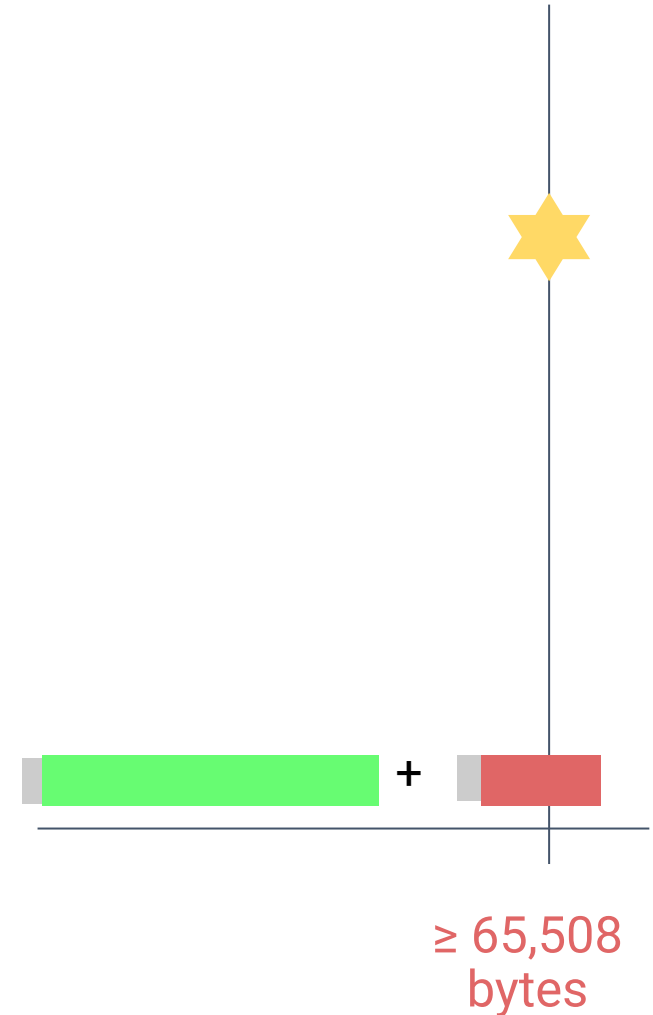


Ataques de protocolo



Ataque PoD

¿Cómo funciona?

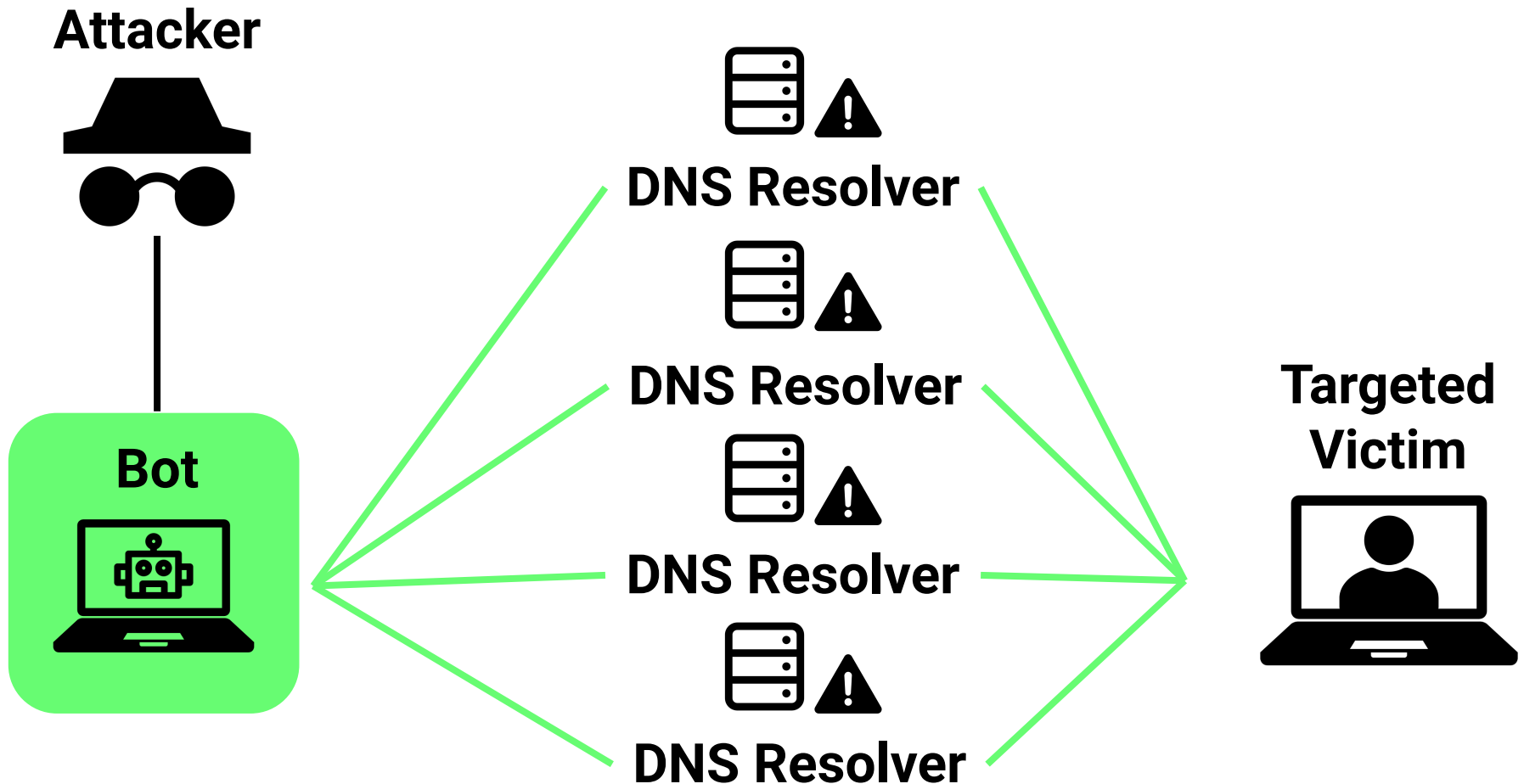


Paquetes del ping de la muerte

IP header	ICMP header	ICMP data
20 bytes	8 bytes	$\geq 65,508$ bytes



Ataques por amplificación








```
POST /xmlrpc.php HTTP/1.1
Host: withinsecurity.com
Connection: keep-alive
Content-Length: 293
```

```
<methodCall>
<methodName>pingback.ping</methodName>
<params>
<param>
<value><string>http://173.244.58.36/</string></value>
</param>
<param>
<value><string>https://example.com/blog/how-to-make-a-salad</
string></value>
</param>
</params>
</methodCall>
```



Ataques de vulnerabilidad





Type

dos

Clear

Platform

Any

Author


Begin typing...

Port

Any

Tag

Any


Advanced



































☐ Verified ☐ Has App

Filters

Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2022-01-05				Siemens S7 Layer 2 - Denial of Service (DoS)	DoS	Hardware	RoseSecurity
2021-11-22				Modbus Slave 7.3.1 - Buffer Overflow (DoS)	DoS	Windows	Yehia Elghaly
2021-11-22				Pinkie 2.15 - TFTP Remote Buffer Overflow (PoC)	DoS	Windows	Yehia Elghaly
2021-11-12				Xlight FTP 3.9.3.1 - Buffer Overflow (PoC)	DoS	Windows	Yehia Elghaly
2021-11-11				AbsoluteTelnet 11.24 - 'Phone' Denial of Service (PoC)	DoS	Windows	Yehia Elghaly
2021-11-11				AbsoluteTelnet 11.24 - 'Username' Denial of Service (PoC)	DoS	Windows	Yehia Elghaly
2021-10-21				NIMax 5.3.1f0 - 'VISA Alias' Denial of Service (PoC)	DoS	Windows	LinxzSec
2021-10-21				NIMax 5.3.1 - 'Remote VISA System' Denial of Service (PoC)	DoS	Windows	LinxzSec
2021-09-23				Redragon Gaming Mouse - 'REDRAGON_MOUSE.sys' Denial of Service (PoC)	DoS	Windows	Quadron Research Lab
2021-09-21				Yenkee Hornet Gaming Mouse - 'GM312Fitr.sys' Denial of Service (PoC)	DoS	Windows	Quadron Research Lab
2021-09-06				SmartFTP Client 10.0.2909.0 - 'Multiple' Denial of Service (PoC)	DoS	Windows	Eric Salario
2021-09-01				Telegram Desktop 2.9.2 - Denial of Service (PoC)	DoS	Windows	Aryan Chehreghani
2021-07-26				Leawo Prof. Media 11.0.0.1 - Denial of Service (DoS) (PoC)	DoS	Windows	stresser
2021-06-14				Notex the best notes 6.4 - Denial of Service (PoC)	DoS	iOS	Geovanni Ruiz

Ataques DoS

Hacking de Servicios de Red

Fuerza bruta

Hacking de Servicios de Red



Sistemas industriales e infraestructura crítica

Hacking de Servicios de Red



Sistemas de Control Industrial (ICS)





Infraestructuras críticas

Sector químico

Instalaciones
comerciales

Comunicaciones

Manufactura crítico

Base industrial de
defensa

Servicios de
emergencia

Tecnologías de la
información

Salud y salud pública

Servicios financieros

Agroalimentario

Sistemas de
transporte

Agua y saneamiento

Instalaciones
gubernamentales

Sector de control de
presas

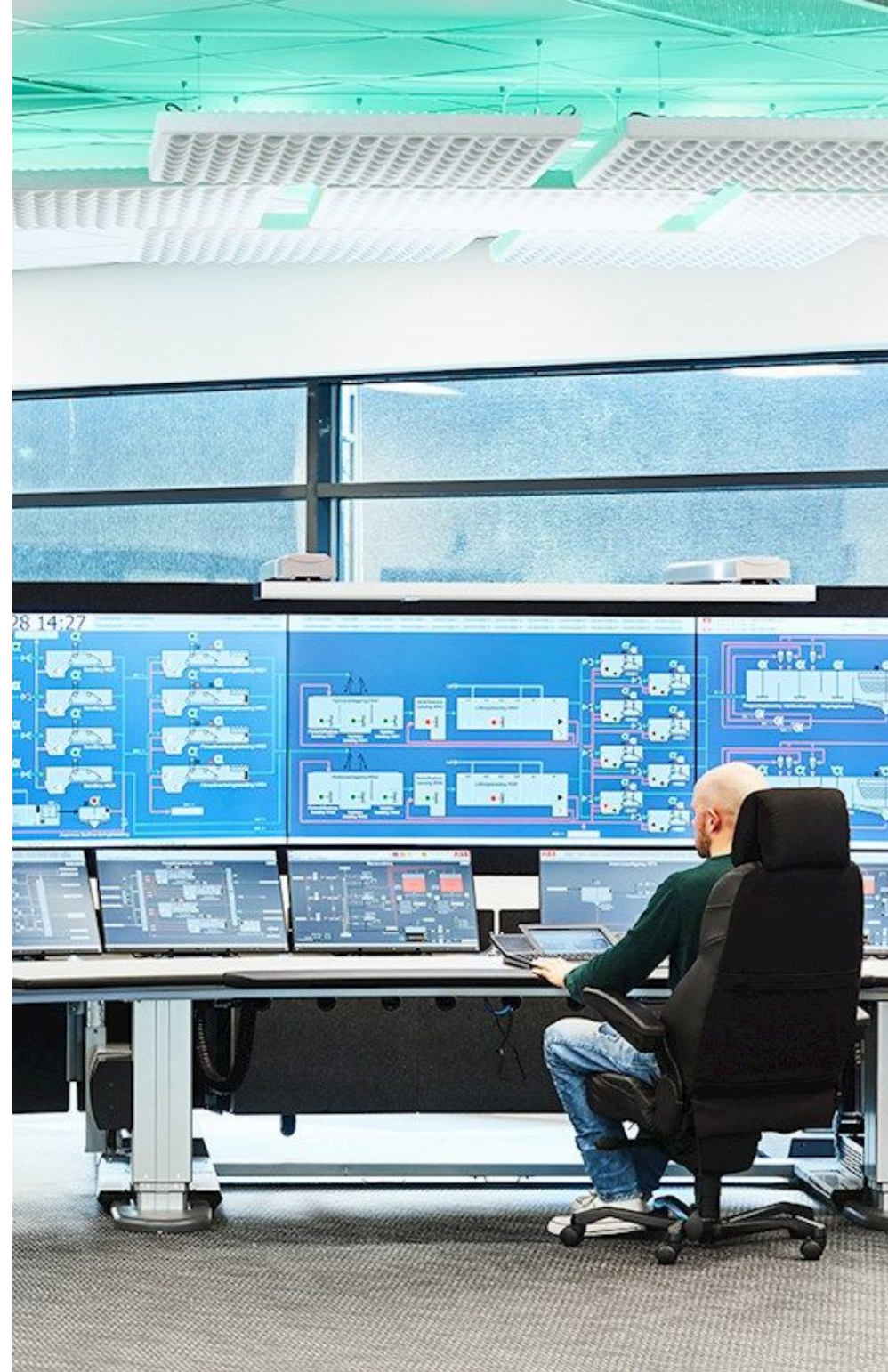
Reactores Nucleares,
Materiales y Residuos

Sector energético



Tecnologías ICS

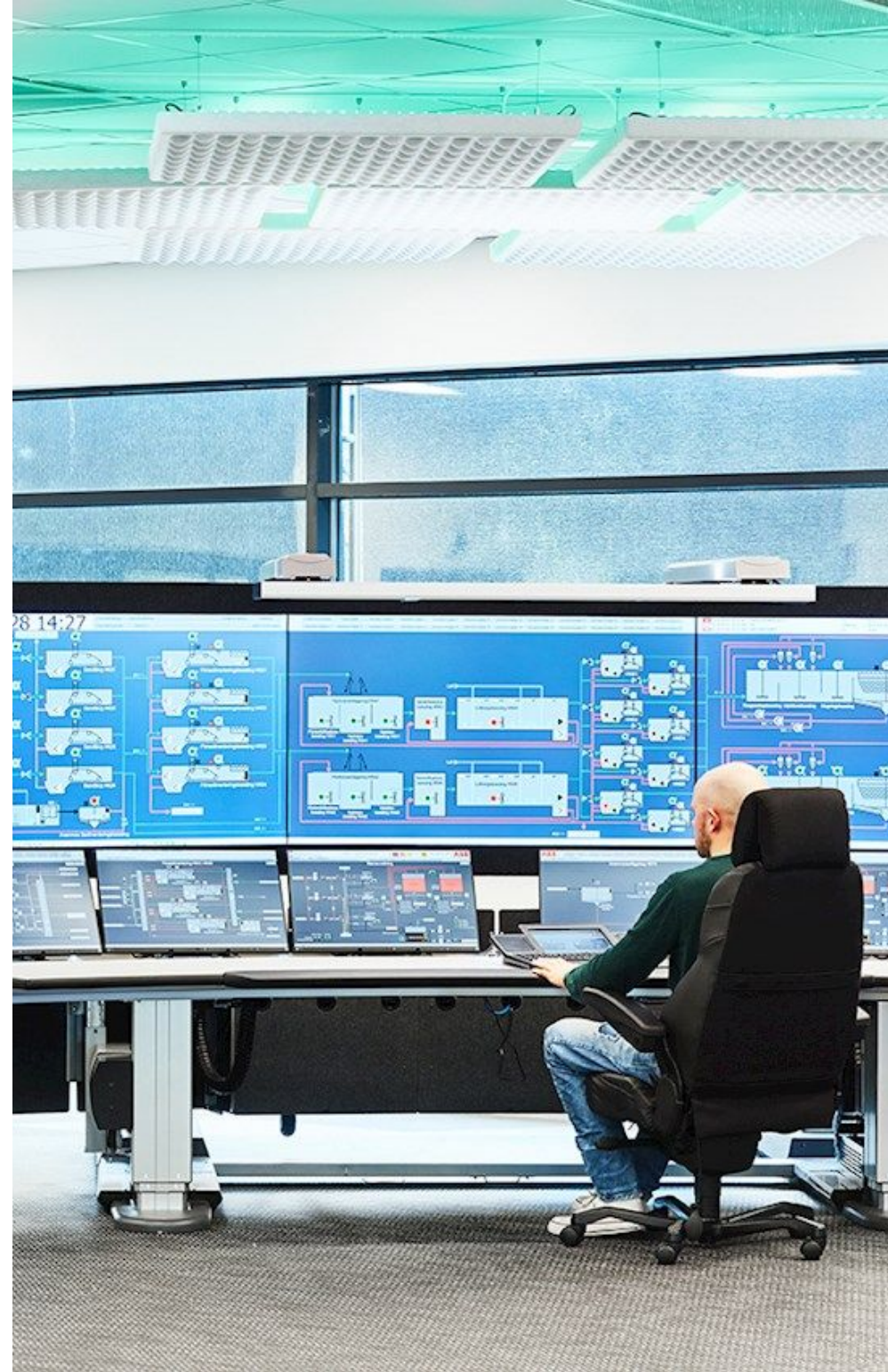
- Sistema de Control Distribuido (DCS)





Tecnologías ICS

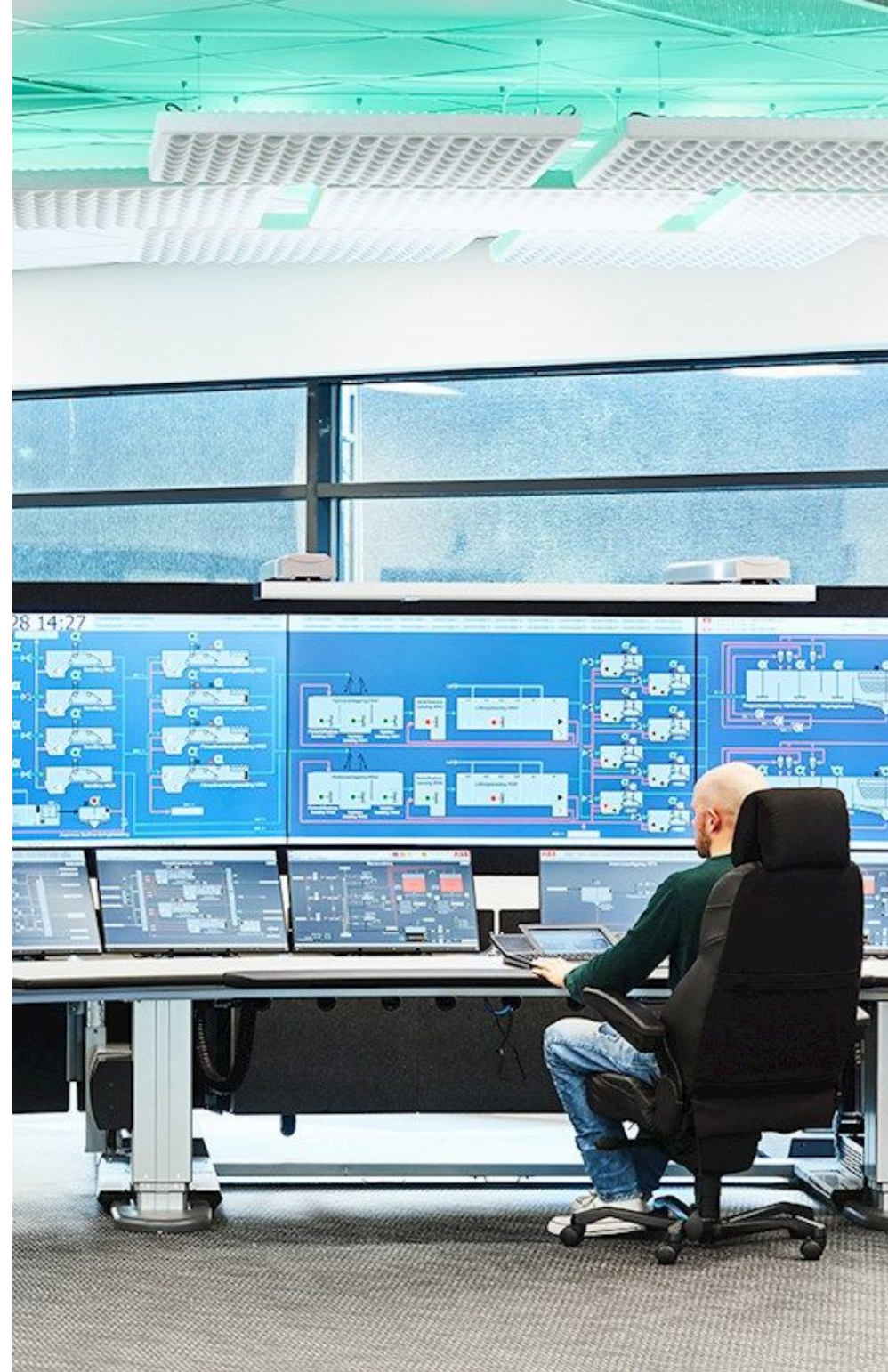
- Sistemas de Control y Automatización Industrial (IACS)





Tecnologías ICS

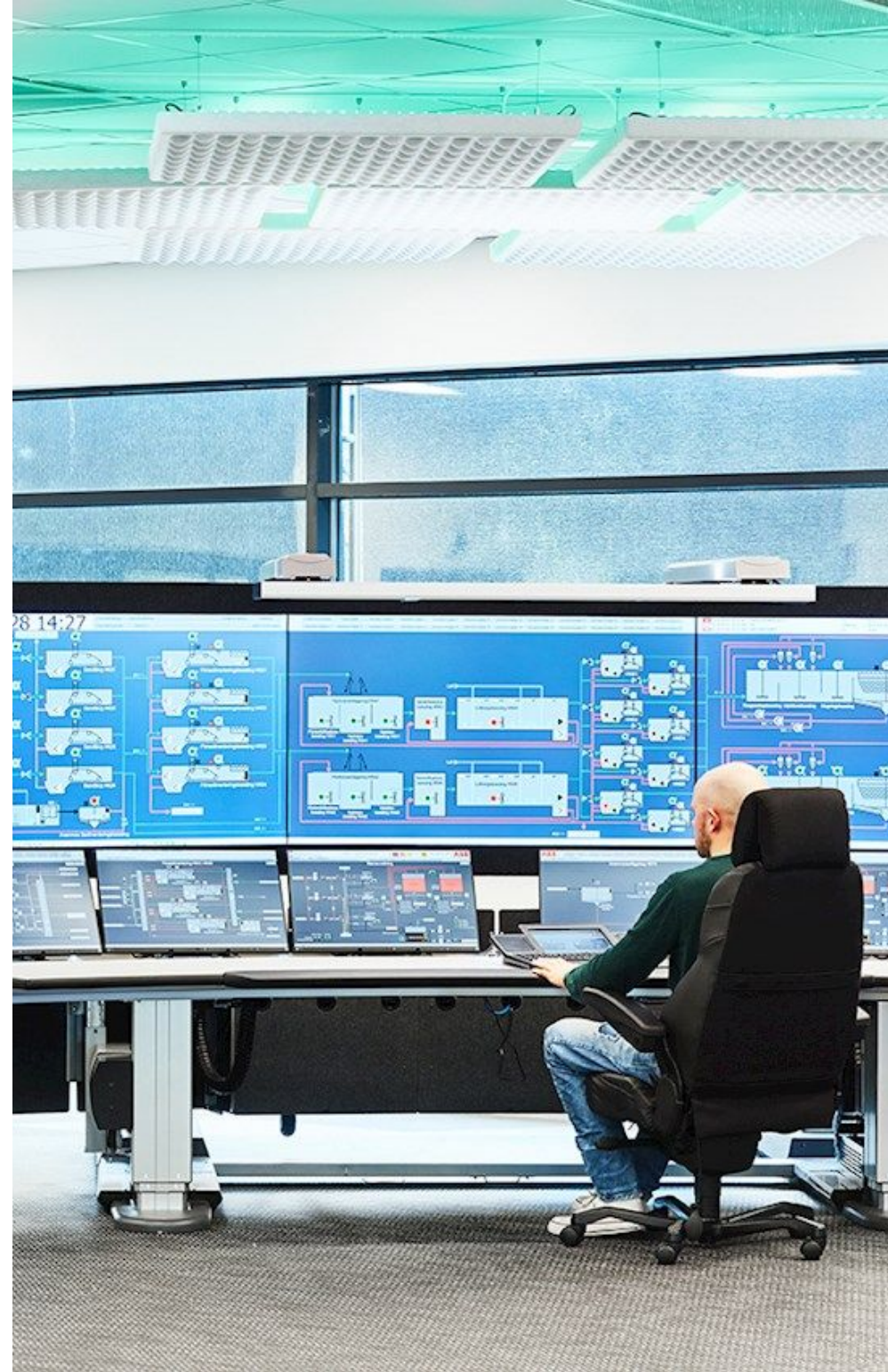
- Control de Supervisión y adquisición de datos (SCADA)





Tecnologías ICS

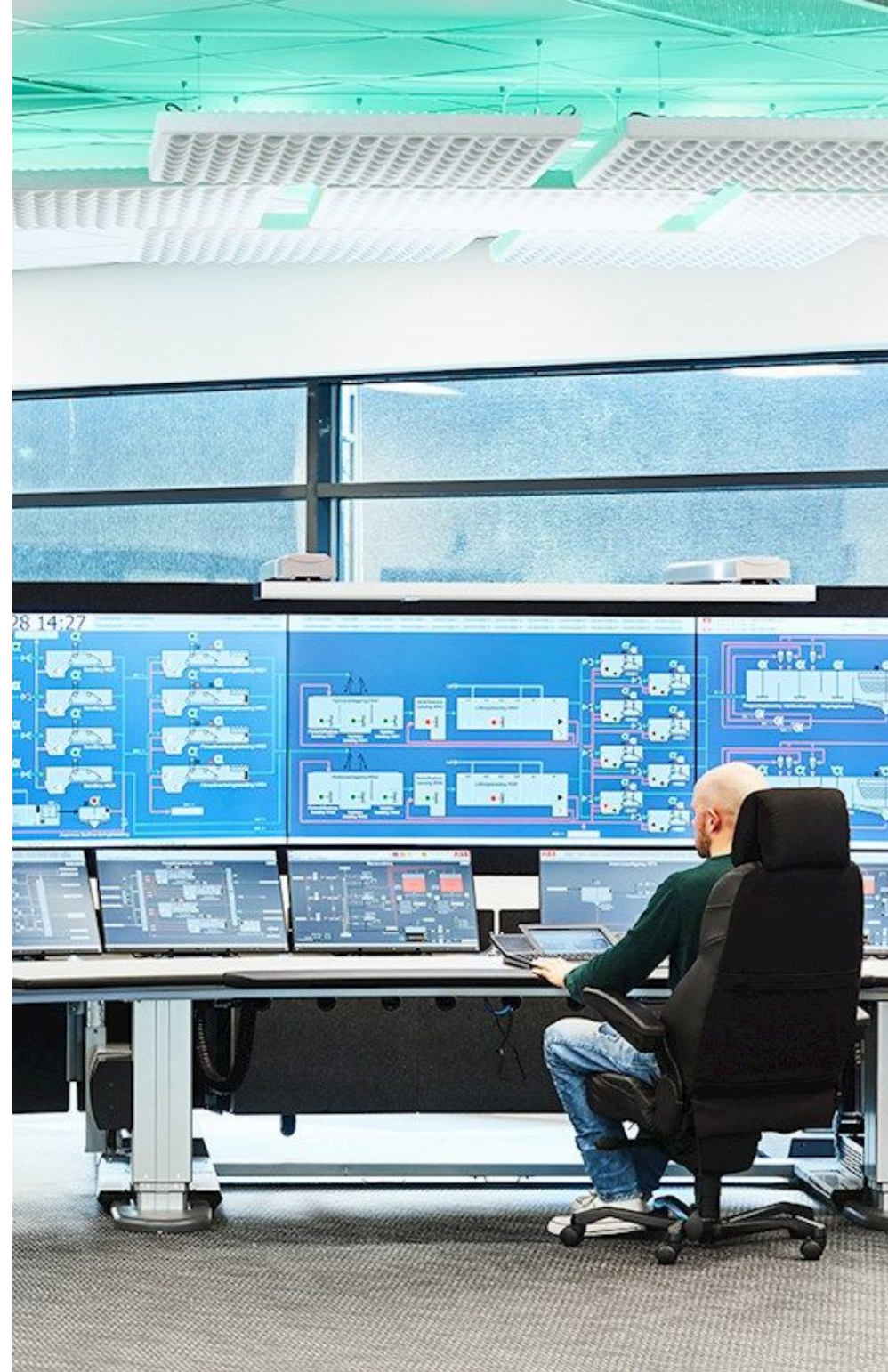
- Controladores Lógicos Programables (PLC)





Tecnologías ICS

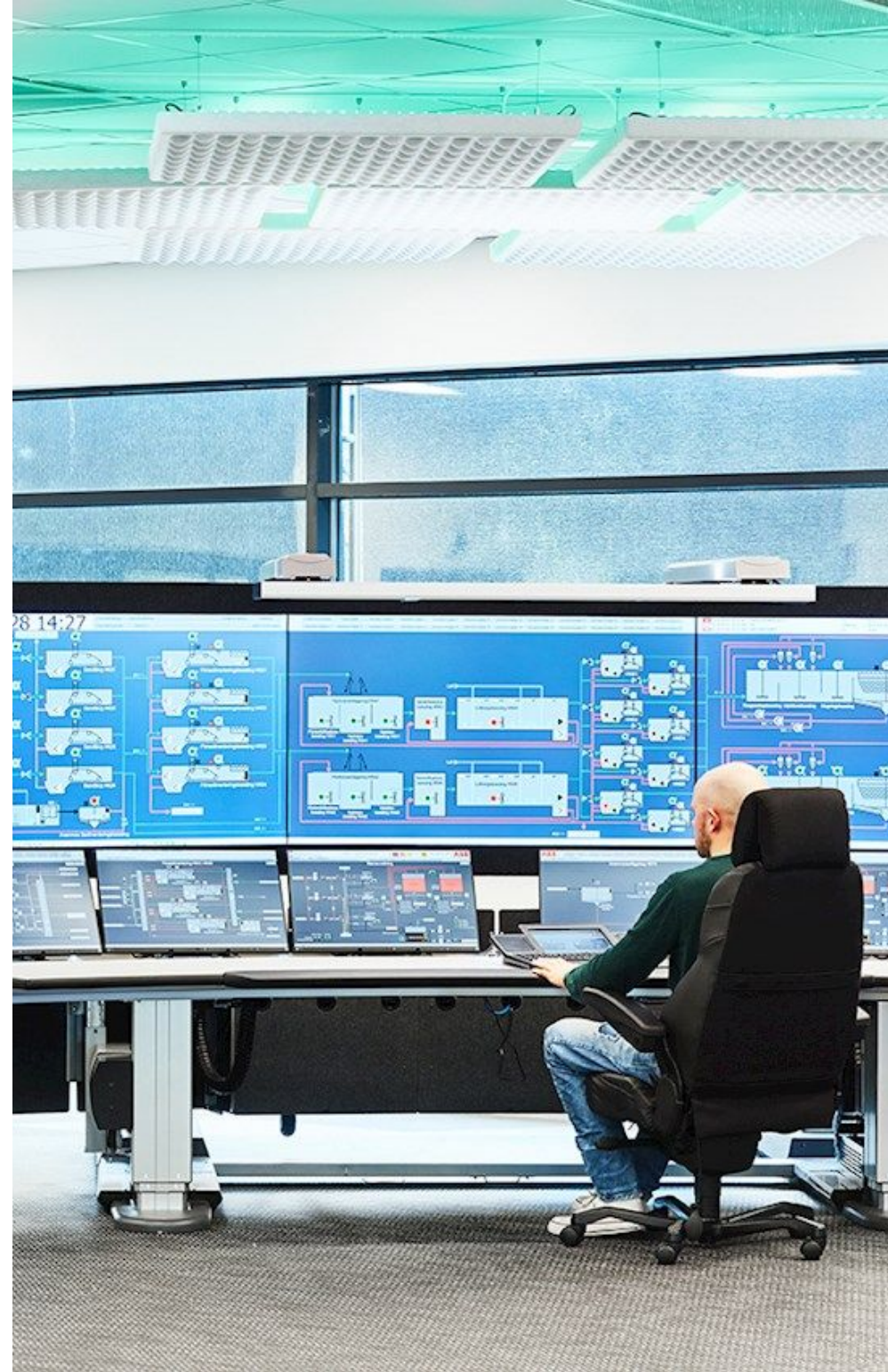
- Controladores de Automatización Programables (PAC)





Tecnologías ICS

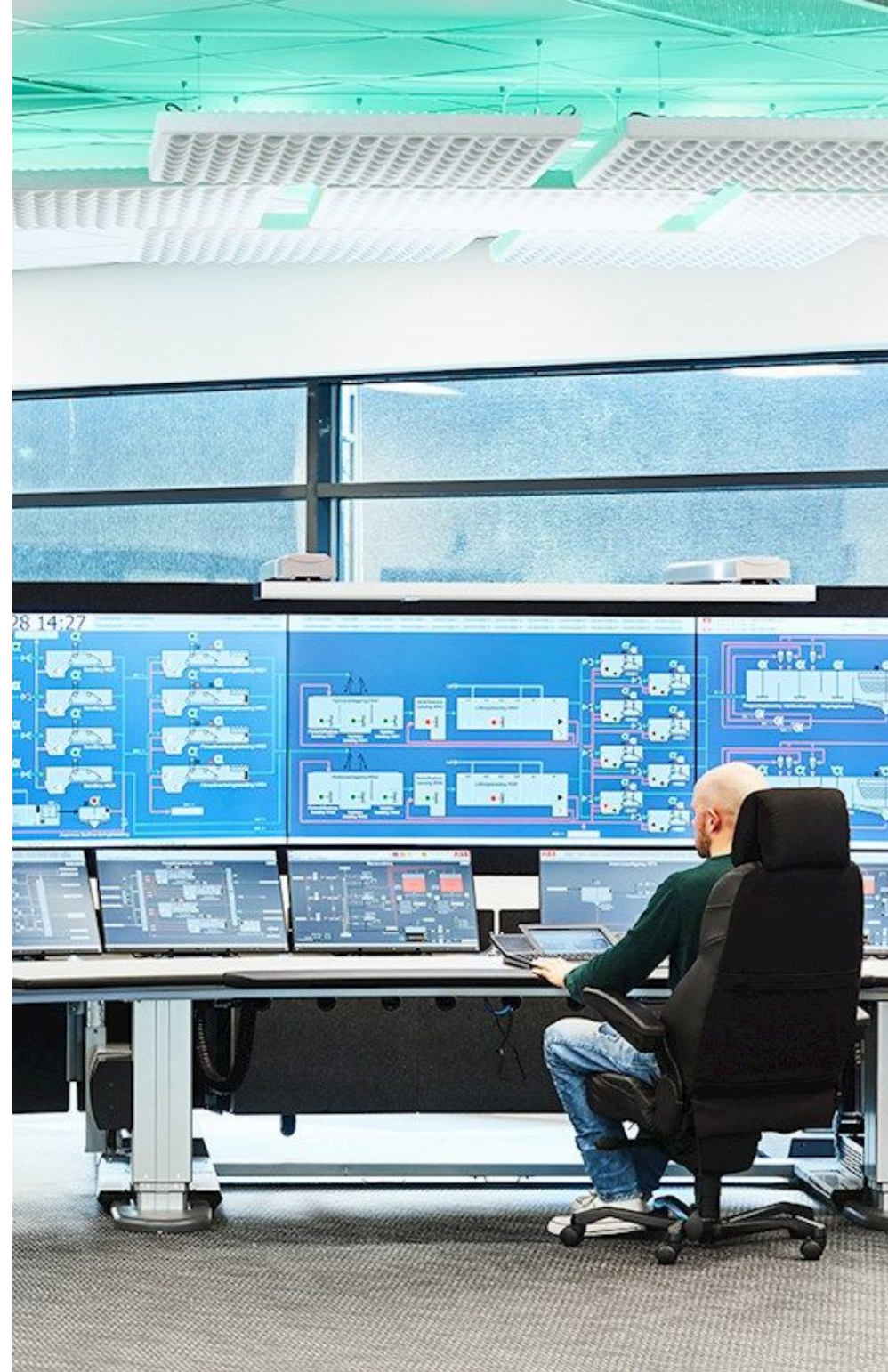
- Unidad Terminal Remota (RTU)





Tecnologías ICS

- Interfaz Humano Máquina(HMI)



CONTROL ROOM BUILDING



HUMAN MACHINE INTERFACE
(HMI)



SCADA SERVER
(SUPERVISORY CONTROL &
DATA ACQUISITION)



The SCADA systems
reads the measured flow
and level, and send the
setpoints to the PLCs



PROGRAMMABLE
LOGIC
CONTROLLERS 1
(PLC)



INDUSTRIAL
EQUIPMENT 1



PLANT



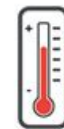
PROGRAMMABLE
LOGIC
CONTROLLERS 2
(PLC)



INDUSTRIAL
EQUIPMENT 2



REMOTE
TRANSMISSION
UNIT
(RTU)



TEMPERATURE
SENSOR

PLC1 could e.g. Compare
the measured flow to the
setpoint, controls the pump
speed as required to match
flow to setpoint.

PLC2 could e.g. Compare
the measured level to the
setpoint, controls the
flow through the valve to
match level to setpoint.

Análisis de firmware

Hacking de Servicios de Red

Hacking de impresoras

Hacking de Servicios de Red



Basic pentesting

Hacking de Servicios de Red



Basic pentesting

Hacking de Servicios de Red