Detección de ransomware mediante análisis de tráfico

Santiago Garcia-Jimenez

upna Universidad Pública de Navarra Nafarroako Unibertsitate Publikoa
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
IRIS POLO DE INNOVACIÓN DIGITAL DE NAVARRA
GOBIERNO DE ESPAÑA MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU
NAVARRA CYBER SECURITY CENTER
AGENDA 2030
Nafarroako Gobernua Gobierno de Navarra

El ransomware no gusta

En la UPNA te adoptamos

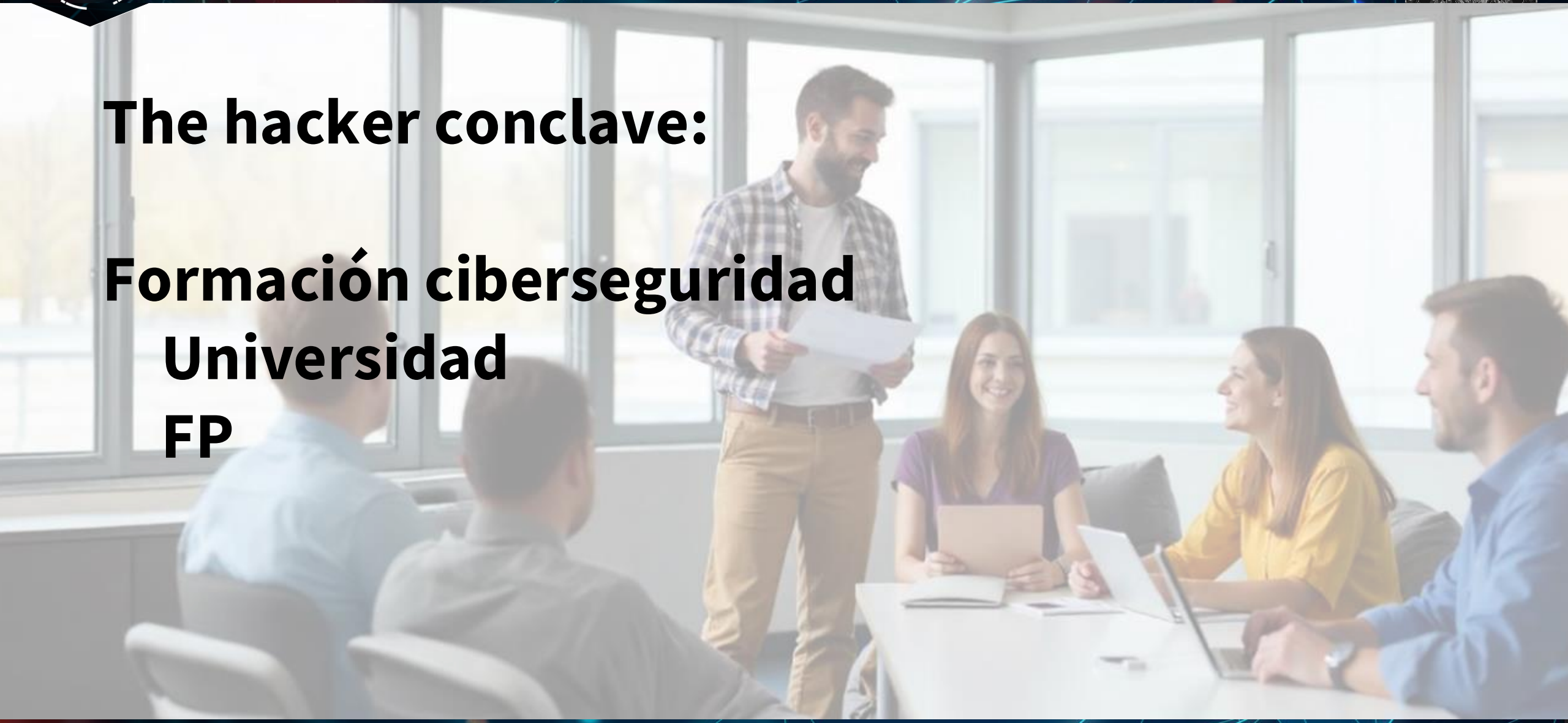
¿UPNA?

UPNA

Universidad Pública de Navarra
Area de telemática

Somos muy majos
Hacemos cosas grandiosas


Bueno igual no muy grandiosas
Pero hacemos cosas



The hacker conclave:

Formación ciberseguridad

- Universidad
- FP

Sistema de control parental

Integrado
Dispositivos WiFi
Comunicación movil

Pribait

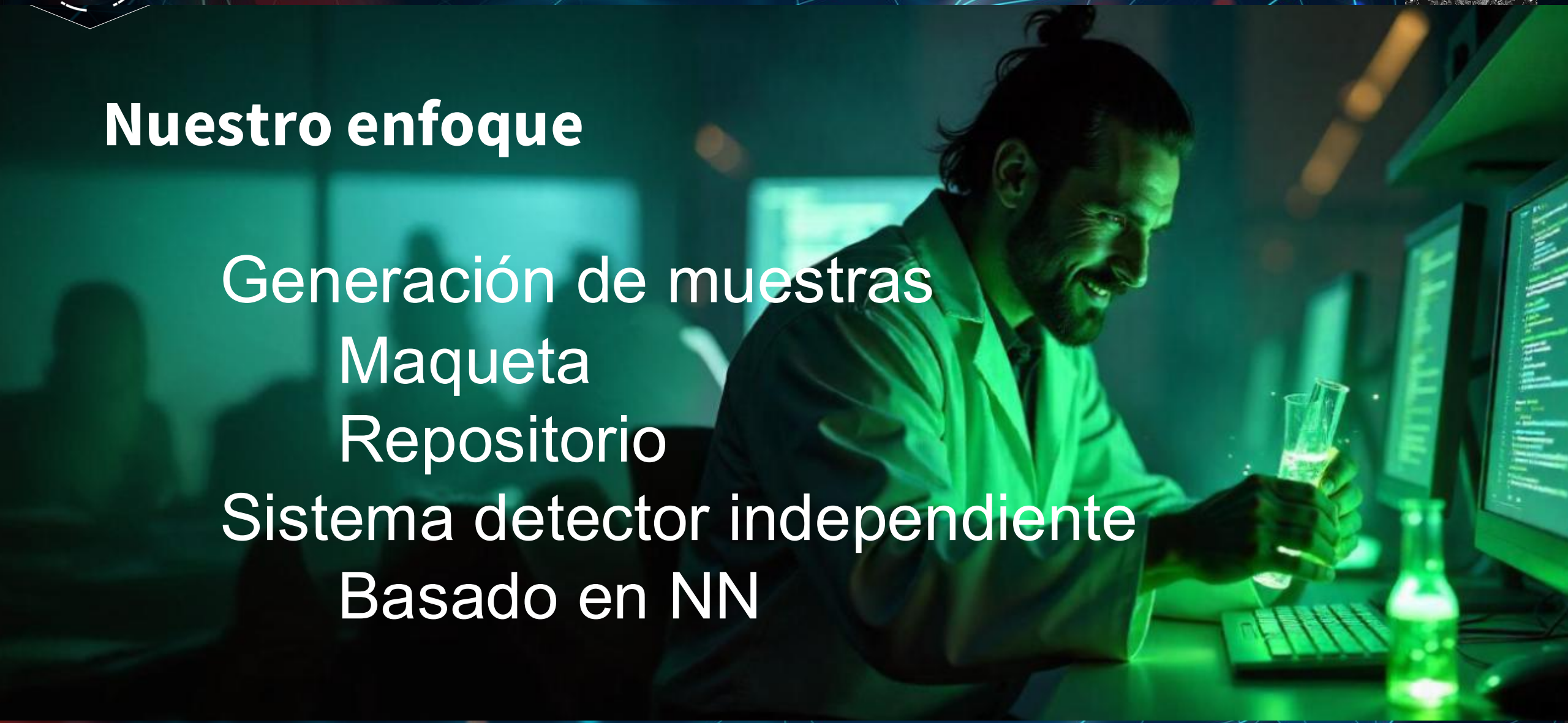
Protección de exfiltración
- Evita error humano.
- Agnóstica a la aplicación.
- Tiempo real.

http://pribait.com

Detectores de ransomware

Nuestro enfoque

Tráfico de red
Discos compartidos
Sistema detector independiente



Nuestro enfoque

Generación de muestras
- Maqueta
- Repositorio

Sistema detector independiente
- Basado en NN

Maqueta actual

Servidor SAMBA

Set de archivos

Impressions

Cliente Windows

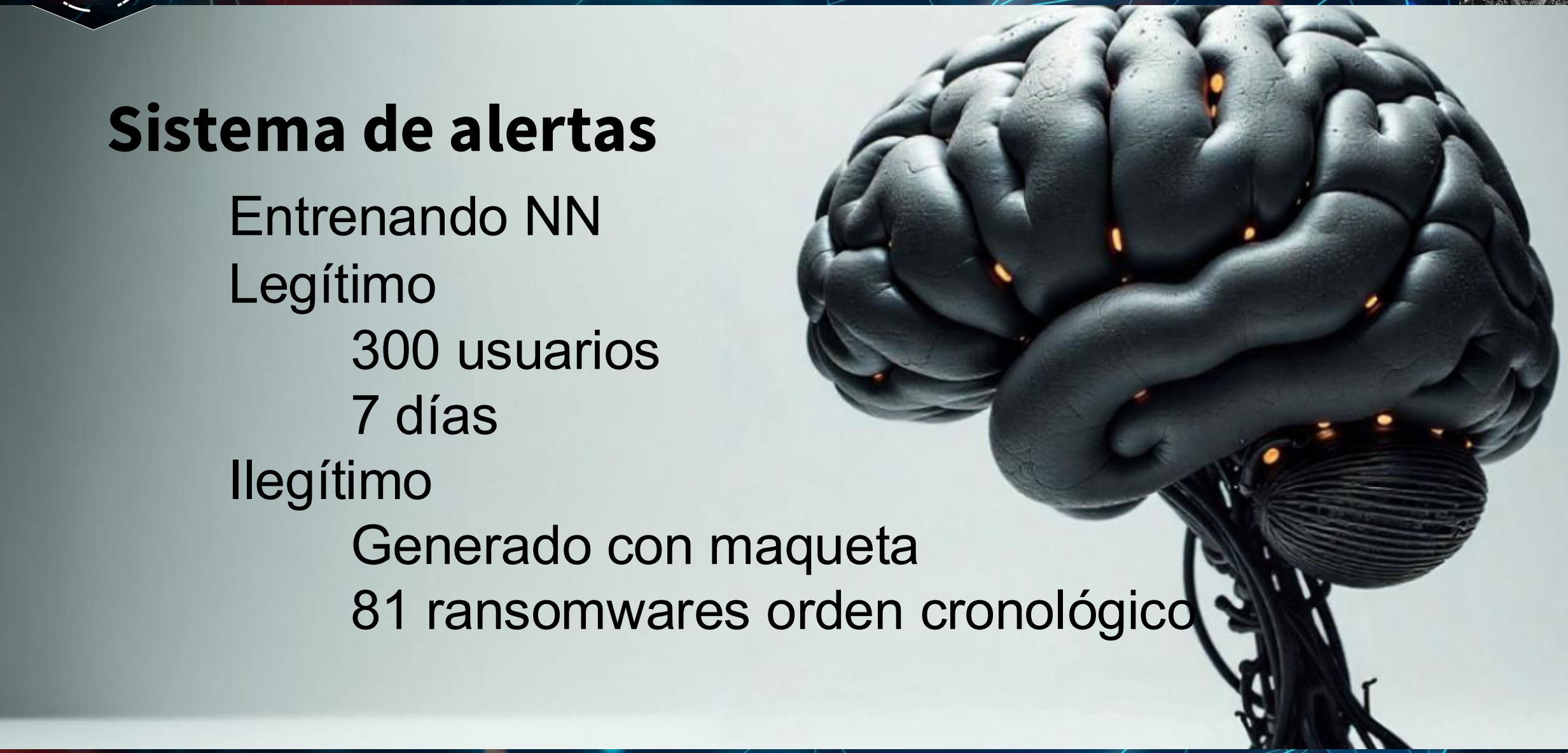
Tiene compartido el directorio

Maqueta actual

Ejecución
Recuperación de estado inicial
Obtención de las trazas de red PCAP

Repositorio

- PCAP file
- DNS & HTTP
- I/O Ops del servidor
- ~100 muestras



Sistema de alertas

Entrenando NN

Legítimo

- 300 usuarios
- 7 días

Ilegítimo

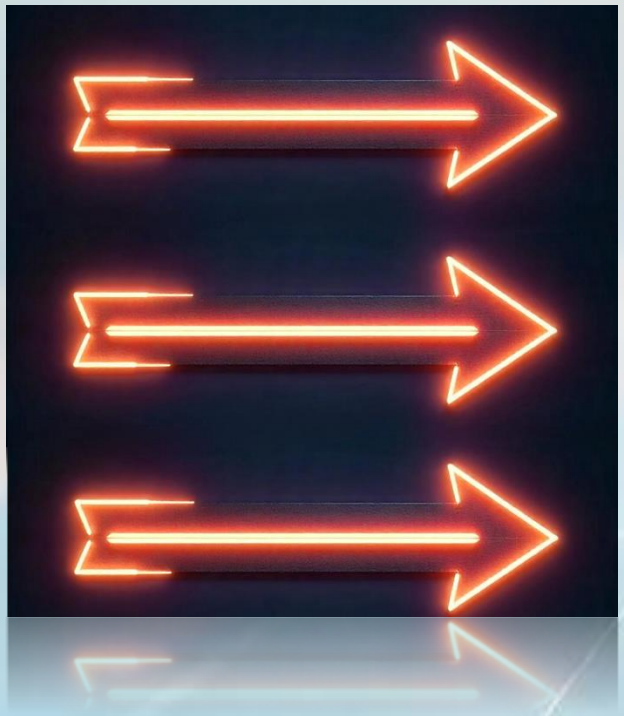
- Generado con maqueta
- 81 ransomwares orden cronológico

Sistema de alertas

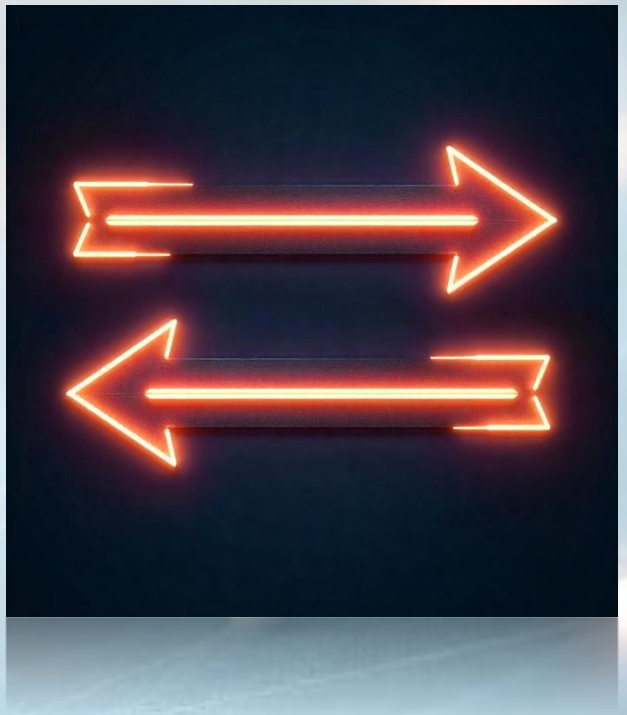
Series temporales
- 1 segundo
- Bytes escritura
- Bytes lectura
- Comandos cortos

Sistema de alertas

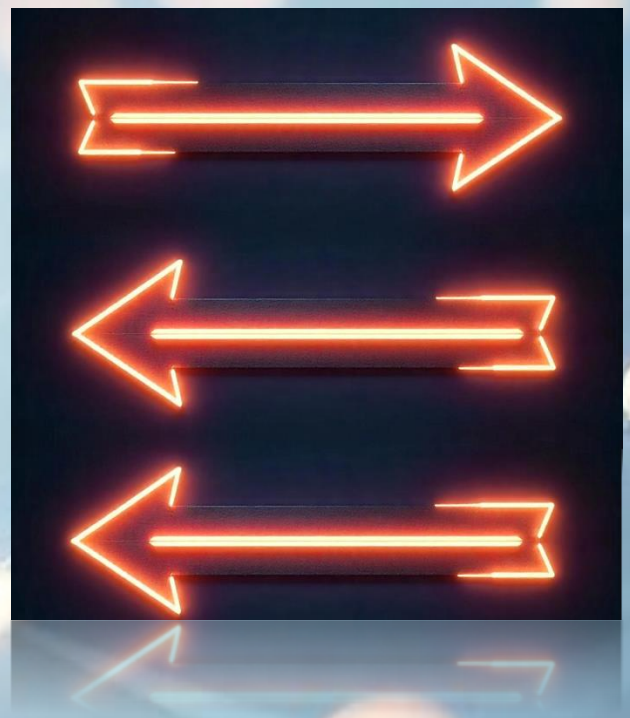
Bytes escritura



Comandos cortos



Bytes lectura



Sistema de alertas

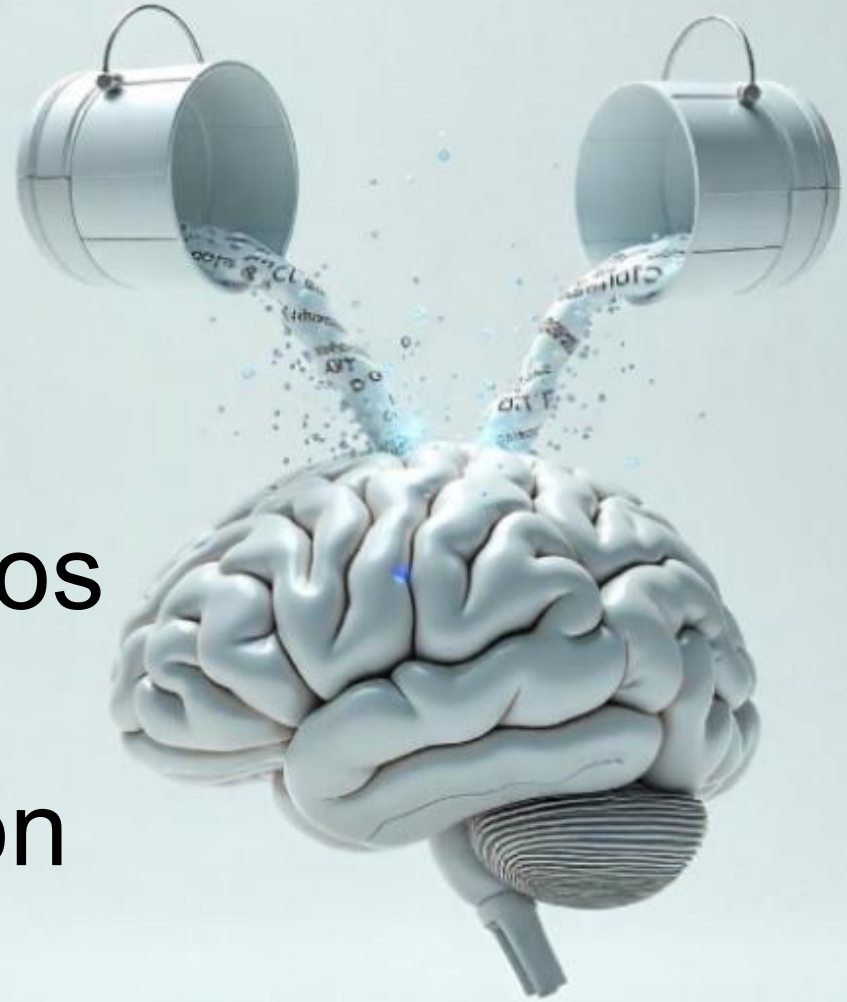
Alimentamos la NN

vector de 10 segundos

Tráfico

En orden de aparición

Total 81 NN



Sistema de alertas

Cada NN

- Entrenada
  - Hasta una fecha
  - Un día de usuario

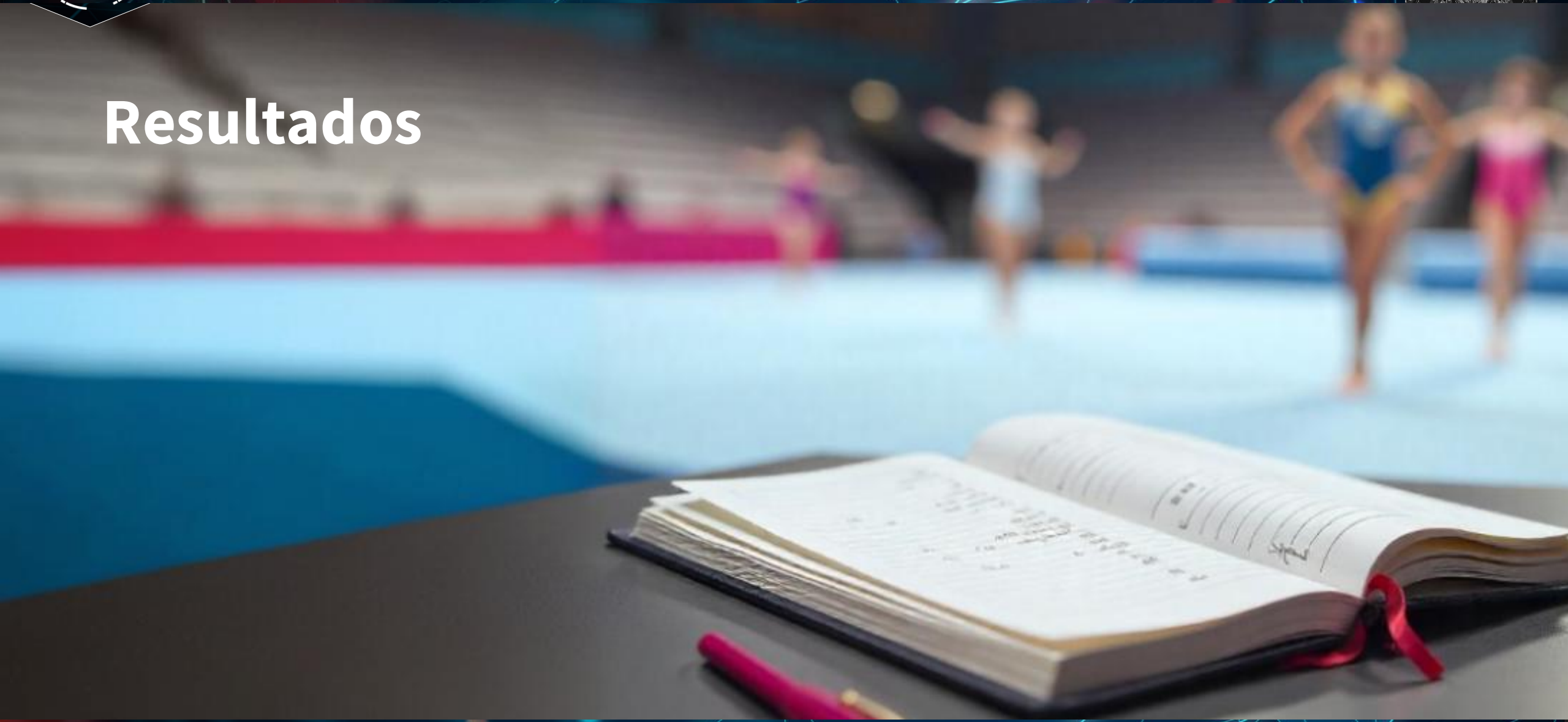
- Testeada
  - Todo el ransomware
  - 7 días de usuarios

Sistema de alertas

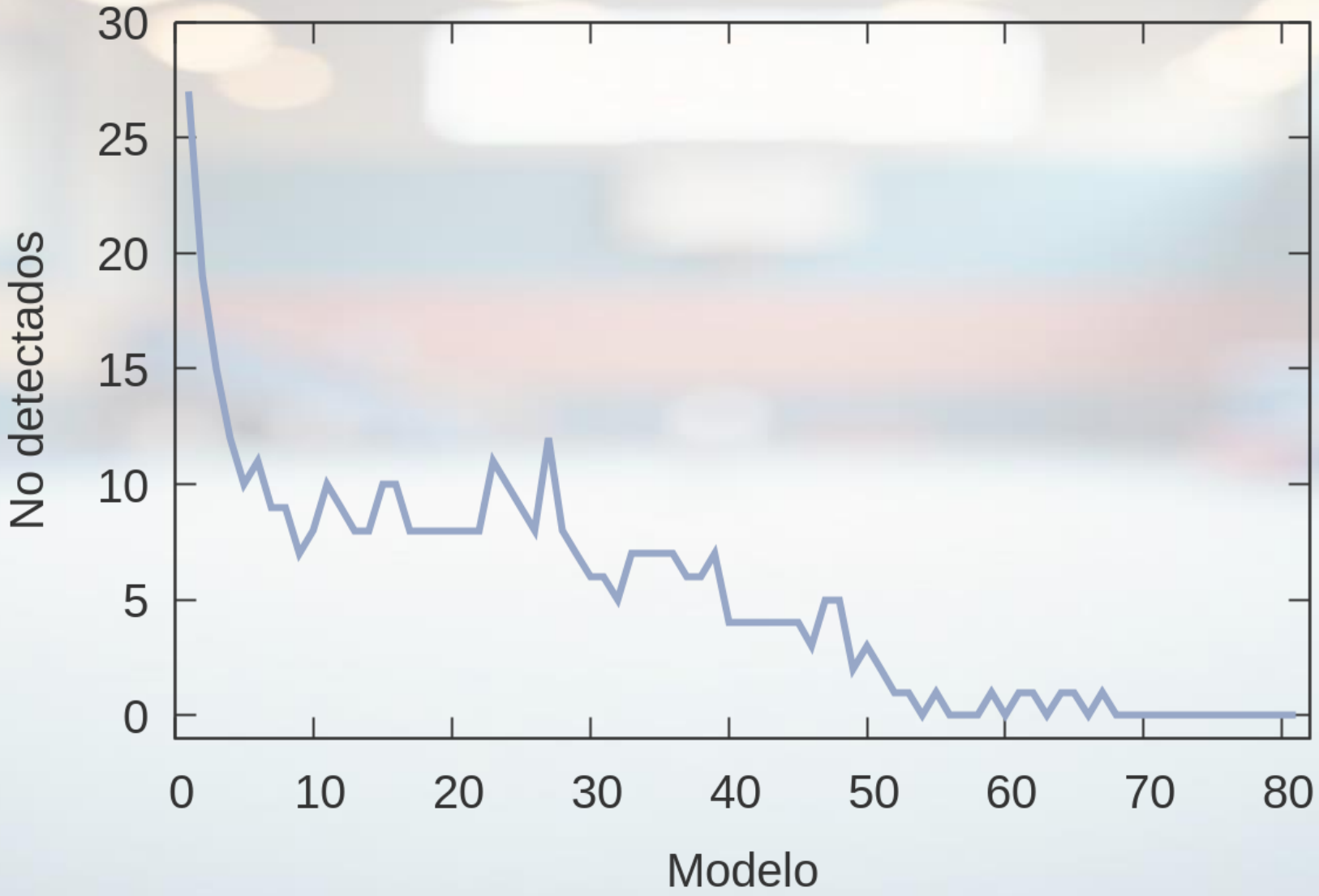
7 positivos seguidos
Alerta

5 minutos sin alertas
Considera nueva alerta

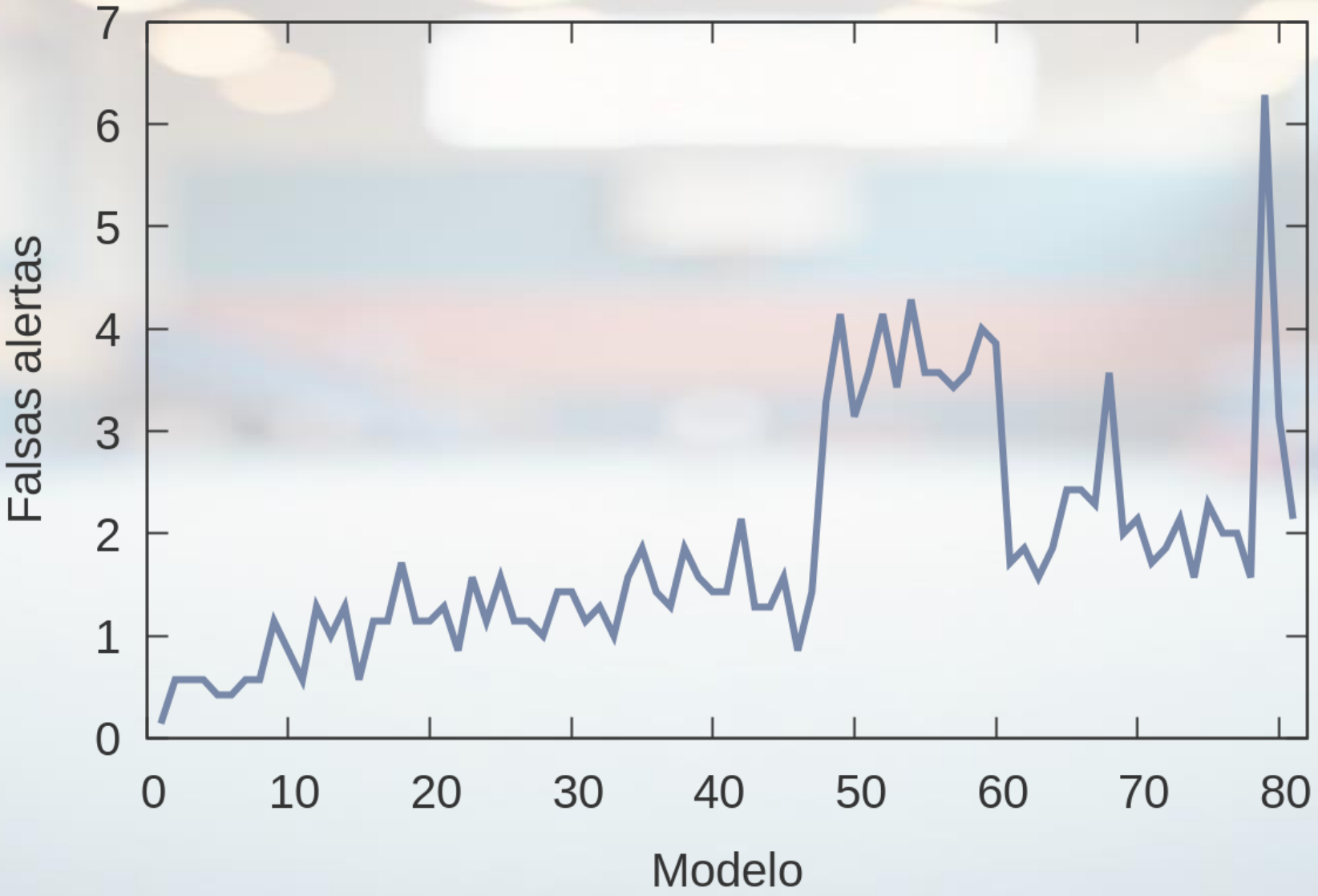
Resultados



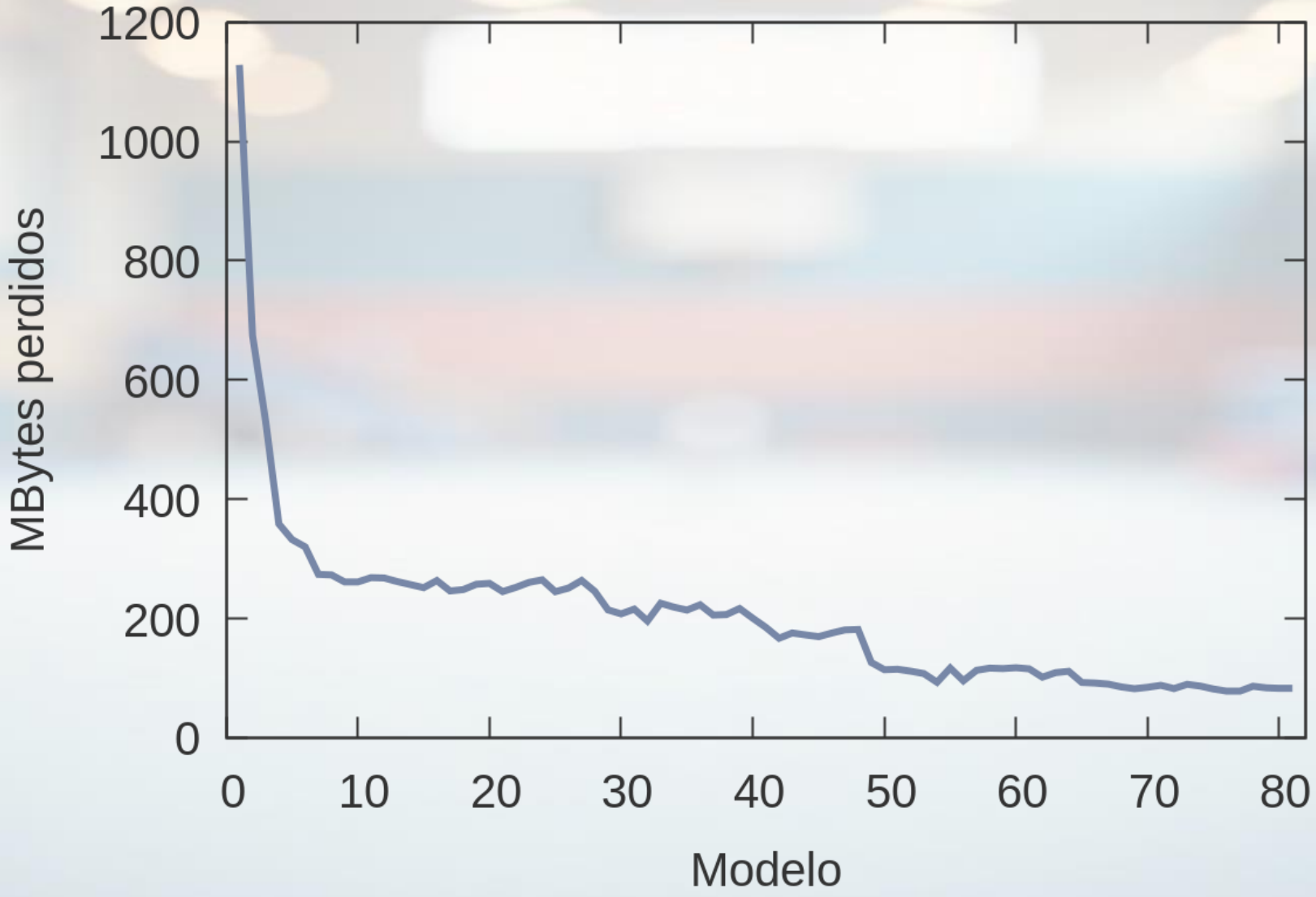
Detección de ransomware mediante análisis de tráfico



Detección de ransomware mediante análisis de tráfico



Detección de ransomware mediante análisis de tráfico



Conclusiones

- Basado en comportamiento
- Nuevas amenazas
- Aislado del entorno de usuario

Detección de ransomware mediante análisis de tráfico

¡MUCHAS GRACIAS!

ESKERRIK ASKO!

NAVARRA CYBER SECURITY CENTER
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
GOBIERNO DE ESPAÑA MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE
Plan de Recuperación, Transformación y Resiliencia
Financiado por la Unión Europea NextGenerationEU
IRIS POLO DE INNOVACIÓN DIGITAL DE NAVARRA
upna Universidad Pública de Navarra Nafarroako Unibertsitate Publikoa
AGENDA 2030
Nafarroako Gobernua Gobierno de Navarra