sedian

Seguridad Digital
de Andalucía

El Esquema Nacional de Seguridad como antídoto contra Ransomware,casos prácticos

Junta de Andalucía

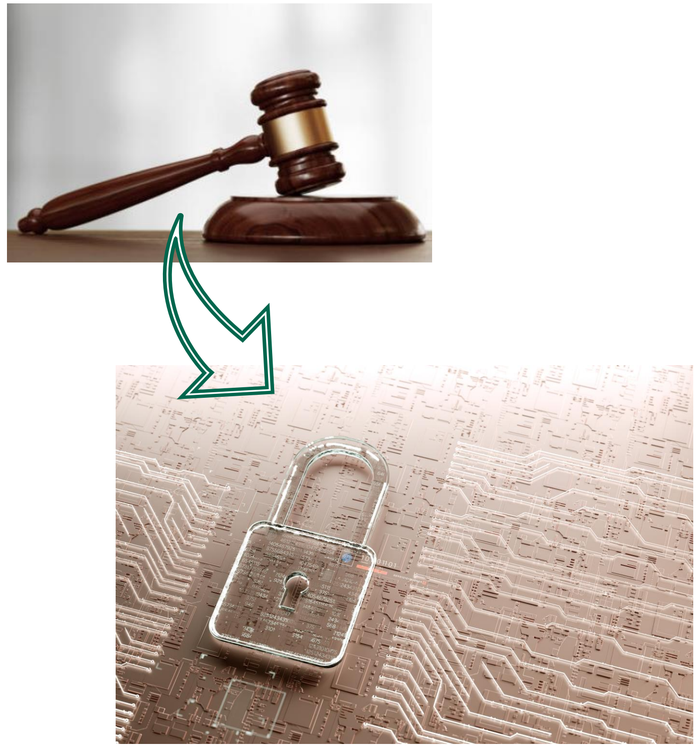
ÍNDICE

1. Introducción: la necesidad de requisitos regulatorios

Seguro que más vale cumplir que curar

1.1 Objetivos

- Alcanzar los niveles de confianza a través del cumplimiento legal.
- Patrones para proteger los activos digitales .
- Transformación digital protegida.



- **Disponibilidad**
- **Integridad**
- **Confidencialidad**

2. El ambiente regulatorio nacional y europeo

Una panoplia normativa con aspectos comunes y relaciones de interdependencia

2.1 Un Tetris de leyes (normativas) españolas y estándares

Normativa

Legislación de protección de datos personales (LOPDGDD)

Ley de Protección de Infraestructuras Críticas (LPIC)

Ley y Reglamento NIS

Esquema Nacional de Seguridad (ENS)

Estándares y buenas prácticas

ISO 27701 Gestión de la privacidad

IEC 62443-3-3 Seguridad de la red y del sistema

ISO 27001 Gestión Seguridad

NIST SP 800-53, CSF NIST

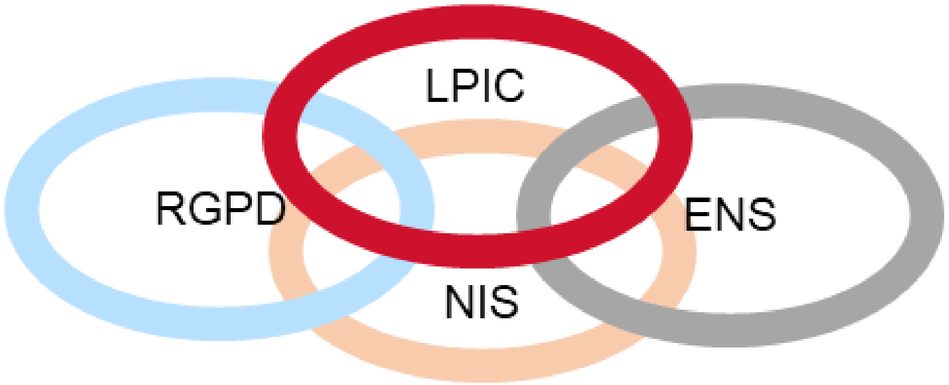
2.2 ¿Qué requisitos exigen estas normas en general?

2.3 ¿Qué medidas técnicas y organizativas se exigen en general?

- Medidas para proteger las diferentes piezas que componen los sistemas de información y operación.
- Medidas de la operación y explotación.
- Otras medidas para mitigar riesgos.

2.4 Requisitos normativos cruzados: una simbiosis constructiva

Normativa que exige	Normativa exigida			
	ENS	RGPD/ LOPDGDD	LPIC	NIS
ENS		Mp.info.1		
RGPD/ LOPDGDD	Para administración pública (disposición adicional primera LOPDGDD)			
LPIC	Guías de Buenas Prácticas de contenidos Mínimos PSO y PPEs			
NIS	Artículo 6	Artículo 6.7. Disposición adicional quinta.	Si es IC	



3. Ecosistema de amenazas ante las que protegernos: Caso Ransomware

Cuando la materialización de una amenaza por no cumplir con la legislación tiene un impacto más allá del de la brecha legal

3.1 Amenazas contra las que protegerse

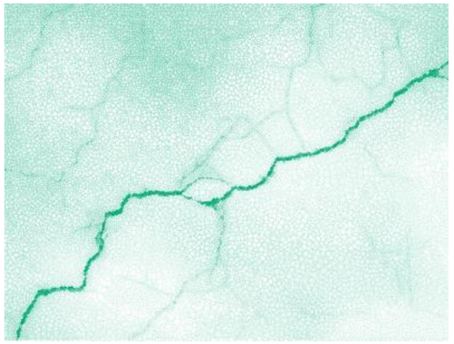
- Ingeniería social
- Robo de equipamiento
- Robo de información
- Denegación de servicio
- Ataque a través del acceso remoto
- Utilización de recursos (dark mining)
- Manipulación de datos
- Ransomware y extorsión (pago por el rescate)

3.2 Impactos si no nos protegemos

Pérdidas económicas

Infracciones

Daños de imagen



Incluso peligro para las vidas humanas

3.3 Impactos de una amenaza en una organización

Pérdidas económicas

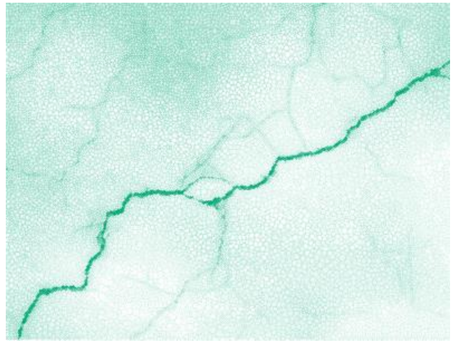
- Por perdida de actividad en caso de indisponibilidad
- Por robo de información (por ejemplo, de tarjetas bancarias)
- Por cese de negocio si se corrompen datos (por ejemplo, si se encriptan)

Infracciones

- No toda la normativa es sancionable directamente (RGPD si lo es, por ejemplo), pero el incumplimiento de una que no lo sea, sí que puede devenir en otro que lo sea.

Daños de imagen

- Perdida reputacional y de confianza ante la sociedad al conocerse que la información está expuesta, sobre todo si es sensible.



Incluso peligro para las vidas humanas

- Algunos ciberincidentes puede causar pérdidas de vidas humanas: accidente en una planta tele controlada, acceso a fórmulas en la industria que puedan causar incluso envenenamiento, indisponibilidad en un hospital.

3.4 El temido ransomware. Seguro que todos lo conocemos

Cuando el ataque por malware consiste en encriptar, pedir un recate y amenazar con difundir información

Desde **el primer ransomware de la historia en diciembre de 1989**, cuando aún no había nacido la primera página web, se escondió **en disquetes** de 5,25 pulgadas (los populares 'cinco y cuarto') se enviaron desde Londres como regalo de una revista a numerosas empresas tanto británicas como de otros países.

A partir de ahí han aparecido otros muchos:

- **Criptolocker** (2013) fue el inicio de **ransom *oportunista***, que se enviaba de forma masiva y pedía pequeñas cantidades de dinero a mucha gente haciendo que fuera un negocio muy lucrativo.
- A partir del **Wanacry (2017)** el ransoware oportunista cede territorio al **ransomware *operado*,** que busca hacer el mayor daño posible y va dejando atrás el usuario final como objetivo y centrándose en organizaciones, empresas y organismos públicos.
- Y llegaron **muchos más...**

3.5 Impacto mundial del WannaCry

3.6 Los titulares siguieron…

- El Gobierno alerta de un ciberataque que afecta a "empresas estratégicas”
- Un ciberataque con ransomware deja KO los sistemas de la cadena SER y de Everis
- Un ataque informático a Prosegur confirma la amenaza del Ransomware
- Paralizan el Ayuntamiento de Jerez encriptando su base de datos con un virus informático y piden un rescate para liberarlo
- Así ha afectado un ataque de 'ransomware' a una de las mayores aseguradoras de España
- El 90% de los ordenadores de Mapfre quedó fuera de servicio

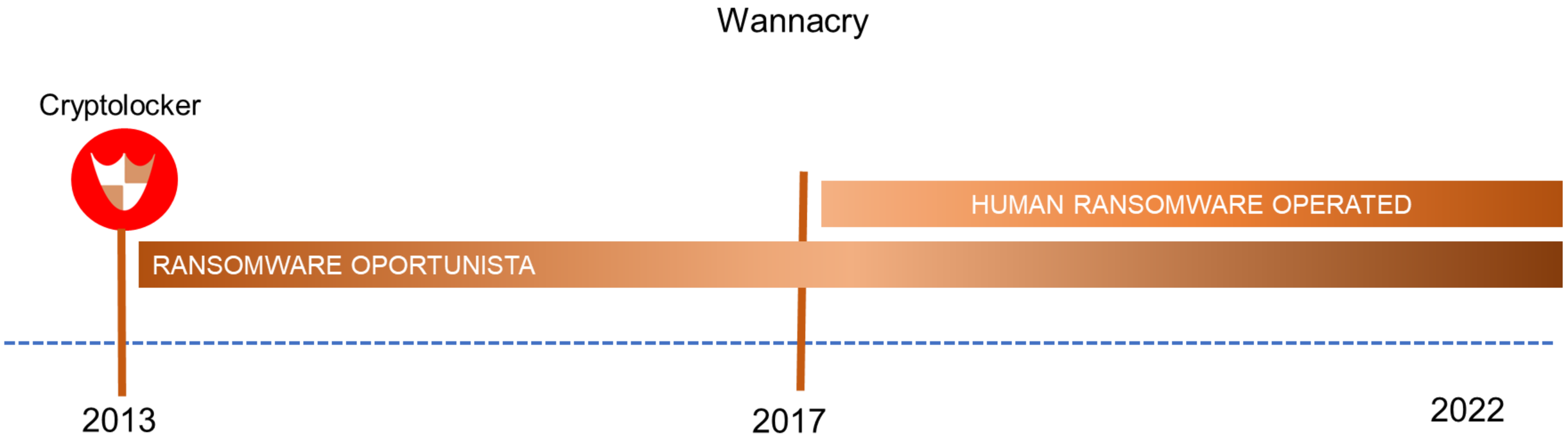
3.7 Un año tras otro

- Ataque por ransomware a Adif: un grupo de ciberdelincuentes anuncia el robo de 800 GB y amenaza con difundir información sensible
- Ciberataque a Phone House: piden un rescate por no difundir datos personales de más de 3 millones de clientes y empleados
- Una oleada de ciberataques tumba las webs del INE, Justicia, Economía y más ministerios
- Un ciberataque prácticamente paraliza el servicio de al menos tres hospitales catalanes.
- El Banco de España sufre un ciberataque que impide el acceso a su web desde servidores externos
- Ciberataque al 'corazón' del sistema judicial: millones de datos personales, en riesgo

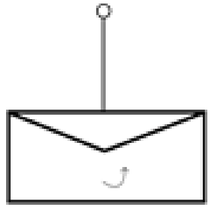
3.8 Principales motivaciones

- **Geopolíticas y geoestratégicas**
- **Arma de guerra**
- **Económicas**
- **Prestigio personal**
- **Vandalismo**
  - Caos
  - Hacktivismo

3.9 Evolución



3.10 Vías de infección principales



Ataques masivos normalmente no dirigidos
CORREO – PHISING es la principal vía de infección

Ataques dirigidos HOR (HUMAN OPERATED RANSOMWARE)

Búsqueda de debilidades: vulnerabilidades, contraseñas expuestas

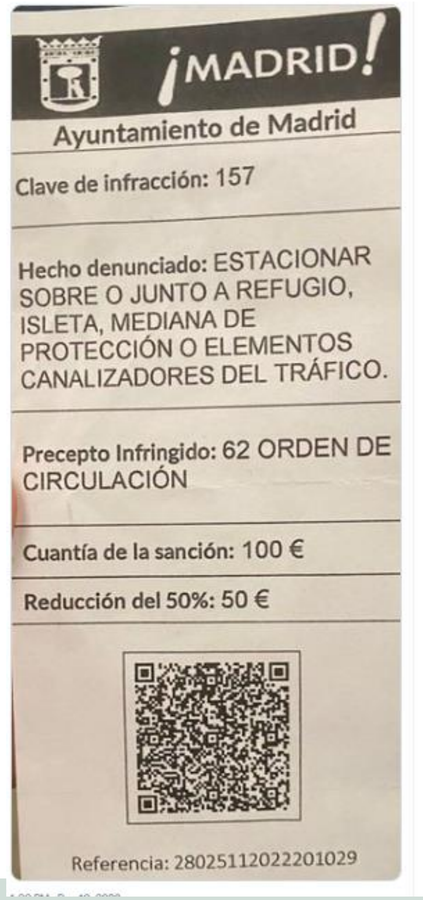
Entrada en la red de la víctima y despliegue de MALWARE espía

Recolección de **información, movimiento laterales y despliegue** del Ransomware

Explotación de Ransomware

Extorsión

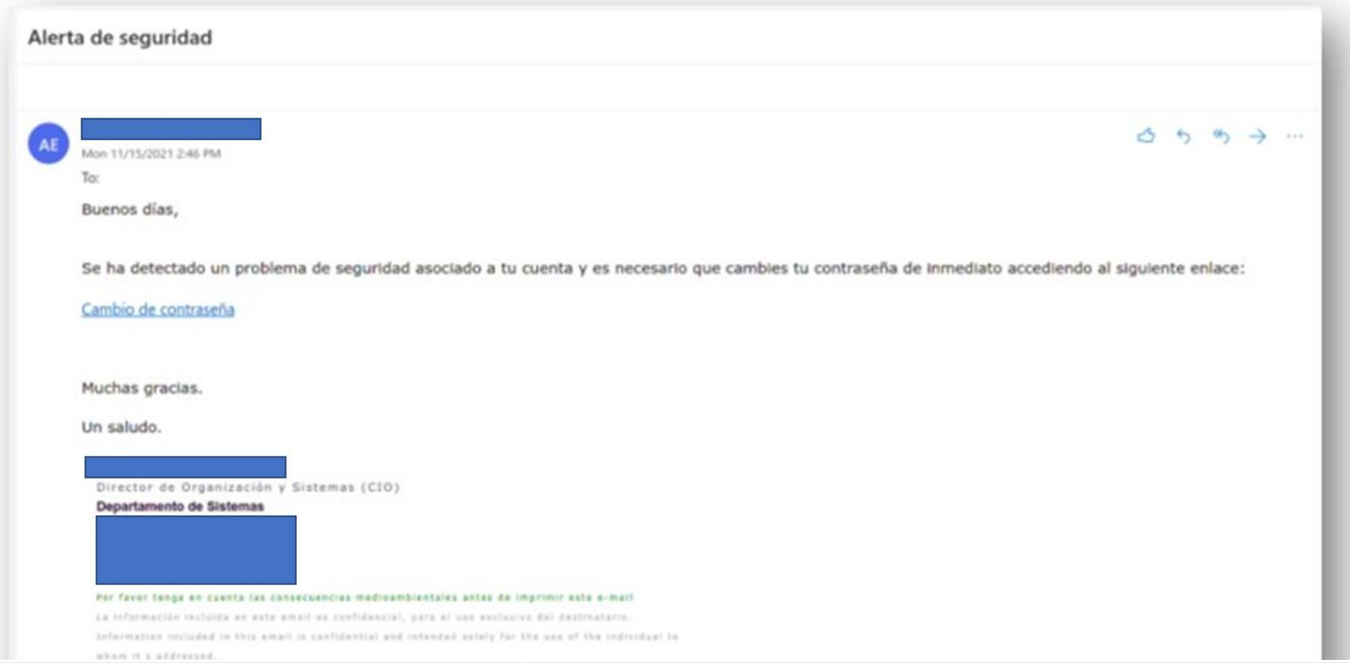
3.10 Vías de infección principales - 2



3.10 Vías de infección principales - 3

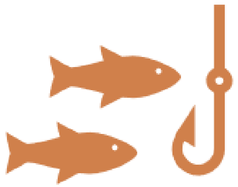
Dirección de envío: soporte@XXX-YYY.com (dominio original XXXYYY.com)

Asunto: Alerta de seguridad



3.11 Ejemplo de un ataque

A un **usuario** mediante Phishing le capturan las credenciales de VPN



El ciberdelincuente: Investiga la red y encuentra un base de datos de pagos

El ciberdelincuente: Aprovecha que al la servidor le faltan parches importantes de seguridad y consigue las credenciales de la máquina mediante un exploit

El ciberdelincuente : Utiliza las credenciales de administrador para hacer una copia de la base de datos

El ciberdelincuente : Copia el backup de la base de datos y exfiltra la base de datos

El ciberdelincuente : Posteriormente decide lanzar un ransomware, encriptar la información y pedir un rescate

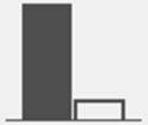
3.12 Datos

66 %
afectadas por el ransomware
en el último año

65 %
ataques conllevaron el cifrado de datos

72 %
experimentaron un aumento
en el volumen/complejidad/
impacto de los ciberataques

90 %
vieron afectada su capacidad operativa
por un ataque de ransomware



86 %
sufrieron pérdidas de negocio/ingresos
por un ataque de ransomware

1,4 millones USD
coste medio de
remediación de un ataque

UN MES
tiempo medio de recuperación
tras un ataque

46 %
pagaron
el rescate

4 %
que pagaron
el rescate
recuperaron
TODOS sus
datos

4. Las medidas del ENS contra el ransomware

4.1 Medidas de protección y su nivel de madurez

Muy bajo

- ✓ Backup fuera de línea/protegidos
- ✓ Despliegue de tecnología de defensa: Antivirus, EDR, uso de sandboxes, etc.

Bajo

- ✓ Segmentación de Red y control de acceso: Política de mínimos
- ✓ Control de versiones: parcheado y bastionado.
- ✓ Control de cuentas privilegiadas

Medio

- ✓ Concienciación
- ✓ Control de los puertos de salida a Internet

Aceptable

- ✓ Doble factor de autenticación
- ✓ Monitorización, capacidad de detección de anomalía
- ✓ Seguro de ciberriesgos que cubran el ransomware

Alto

4.2 Como protegernos con medidas técnicas y organizativas

Previniendo que entre en la organización →
- Formación y concienciación.
- Seguridad Perimetral
- Sistemas bastionados
- Aplicaciones seguras
- Accesos seguros

Previniendo que una vez abierto sea capaz de encriptar los datos del propio equipo →
- Antivirus y parches actualizados

Previniendo que se difunda por la red y pueda llegar a otros equipos →
- Monitorización
- Segmentación de red

Previniendo que infecte a otros equipos a los que alcance →
- Parcheado y bastionado de todo el parque de equipos incluyendo servidores

Recuperando la información si ya se ha encriptado →
- Copias de seguridad adecuadas (no accesibles por el ransom)

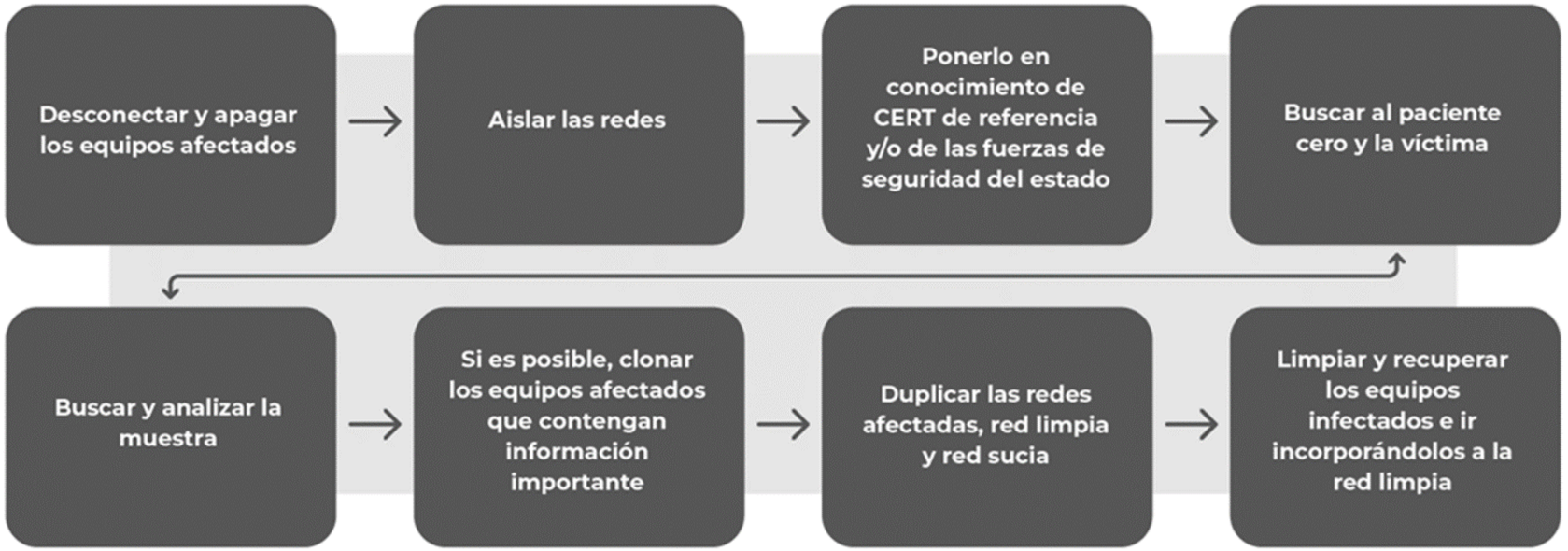
Tomando medidas para que no vuelva a pasar →
- Generación y protección de logs para realización de análisis forenses, que indiquen las causas y nos ayude a evitarlas.

¡Todos son requisitos del ENS!

Además, las medidas **organizativas** de gestión de incidentes, con los procedimientos desde la detección hasta el análisis forense y seguro de ciberriesgos.

4.3 Recuperación

Disponer de un procedimiento de gestión de incidencias



Lecciones aprendidas

5. CONCLUSIONES

5.1 Cumplir para protegerse

Se han visto algunos ejemplos clásicos de ciberataques ransomware y justificado como se podrían haber evitado o aminorado su impacto cumpliendo requisitos regulatorios (ENS).

La legislación, por lo tanto, persigue una **protección** y, por tanto, la observación por entidades y ciudadanos nos evitará todos los impactos negativos asociados a los ciberataques.

La legislación en ciberseguridad protege, en particular el ENS

ens
Esquema Nacional de Seguridad

6. Ruegos y Preguntas

sedian Seguridad Digital de Andalucía