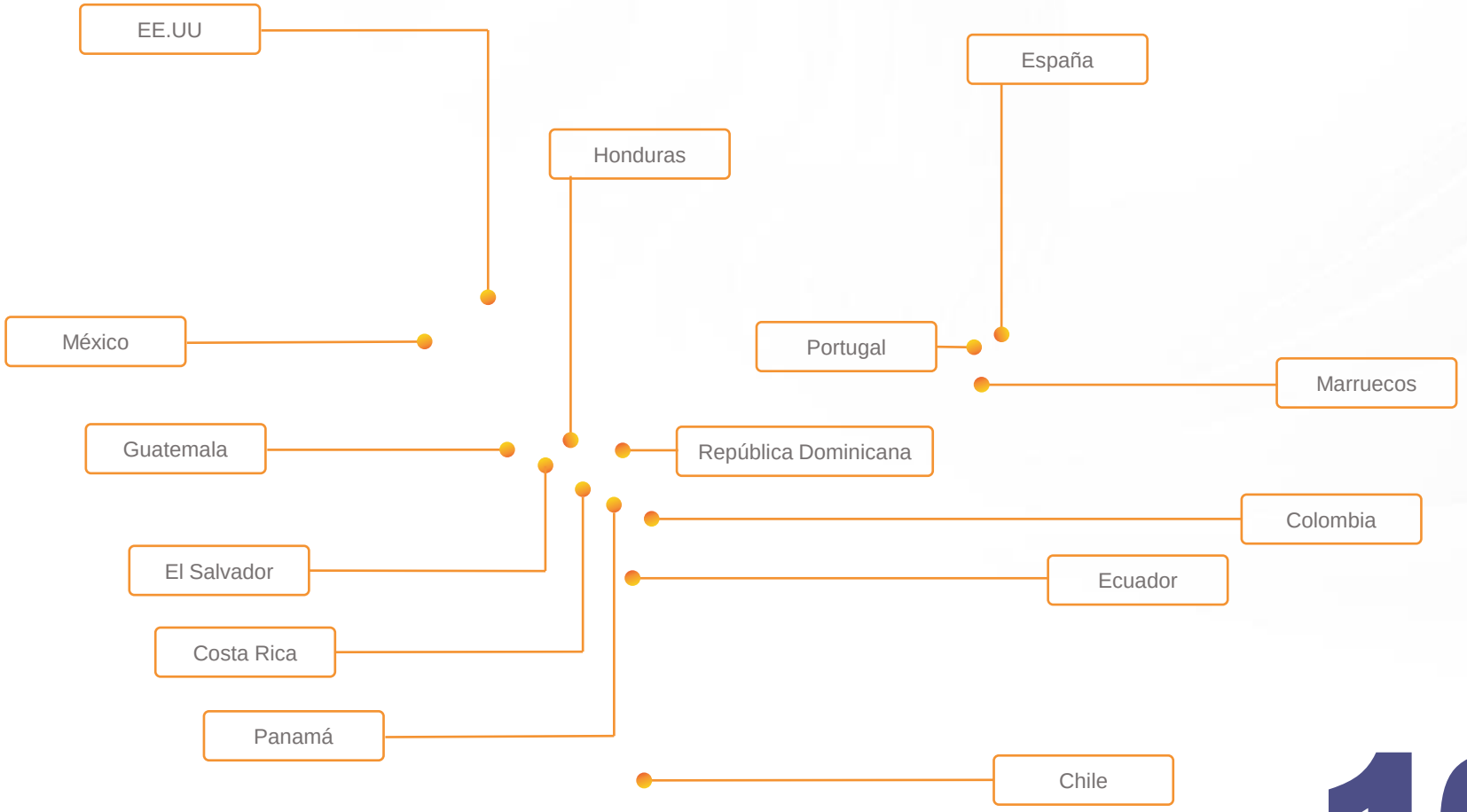
BABEL

We partner to wooow

La amenaza es real: consejos para enfrentarnos a un ataque ransomware

Quiénes somos

babelgroup.com



Cerca de
3.000
Profesionales

140MM€
Facturación
(Previsión a cierre de 2022)

14 Países en los que operamos

TOP 10 Consultoras tecnológicas de capital Español

* Fuente ranking Computing 20/22

Un punto de inflexión

12 de Mayo del 2017

WannaCry: el ransomware que tiene “secuestrados” los sistemas de Telefónica y de otras empresas

Un punto de inflexión

12 de Mayo del 2017

Impacto mundial del WannaCry

Un punto de inflexión

12 de Mayo del 2017

WannaCry lo consiguió:

Llegó el día en que todos hablamos de seguridad

Los titulares siguieron…

Titulares

- 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

Un año tras otro

Titulares

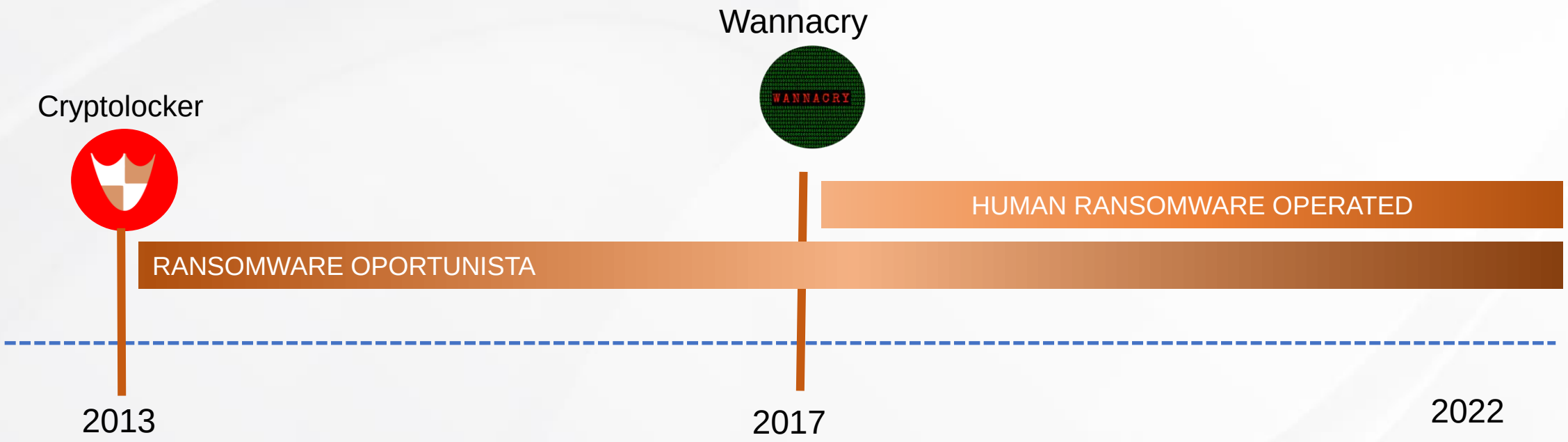
- Ataque por ransomware a Adif: un grupo de ciberdelincuentes anuncia el robo de 800 GB y amenaza con difundir información sensible
- Ciberataque a Phone House: piden un rescate por no difundir datos personales de más de 3 millones de clientes y empleados
- Una oleada de ciberataques tumba las webs del 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

Principales motivaciones

- **Económicas**
- **Prestigio personal**
- **Vandalismo**
  - Caos
  - Hacktivismo
- **Nuevos recursos para atacar**

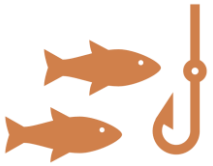
Ransomware

Evolución



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

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

Evolución del Ransomware: 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 el 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 [illegible] copia de la base de datos

RaaS

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

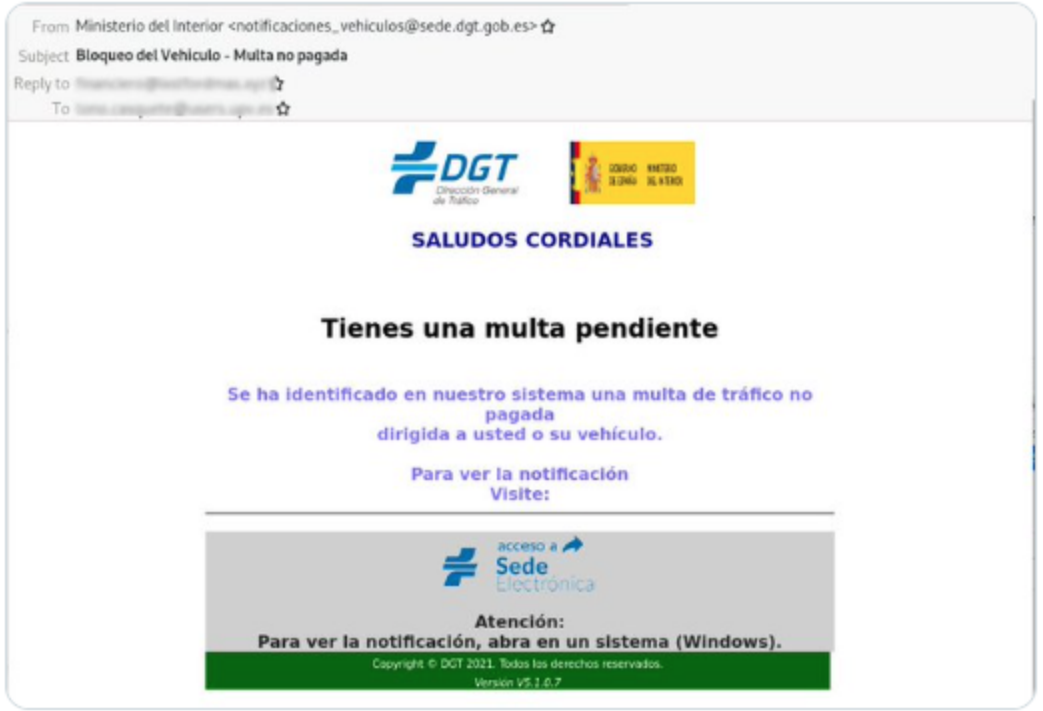
El ciberdelincuente : Posteriormente decide lanzar un ransomware, encriptar la información y pedir un rescate

Principales vías de infección

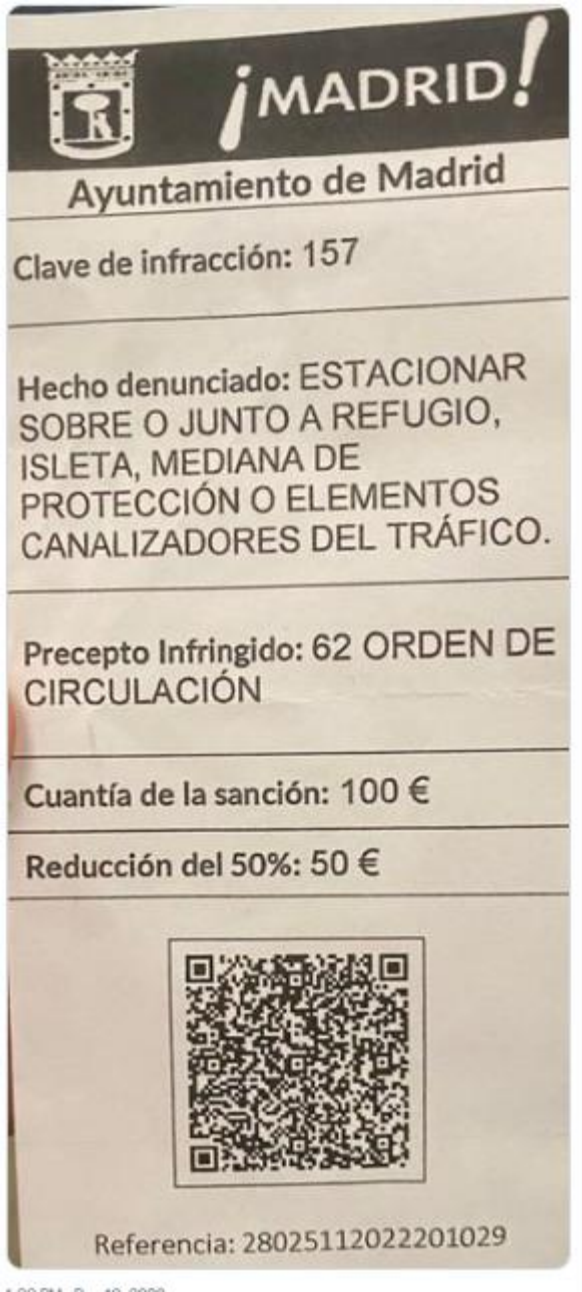
Guardia Civil
@guardiacivil · **Seguir**

⚠️ #ALERTA ❗ Detectada campaña fraudulenta a través del correo electrónico (#phishing) suplantando a la Dirección General de Tráfico (@DGTes). El mensaje contiene un enlace a una supuesta notificación que descarga #malware en el dispositivo. #NoPiques

osi.es/es/actualidad/...



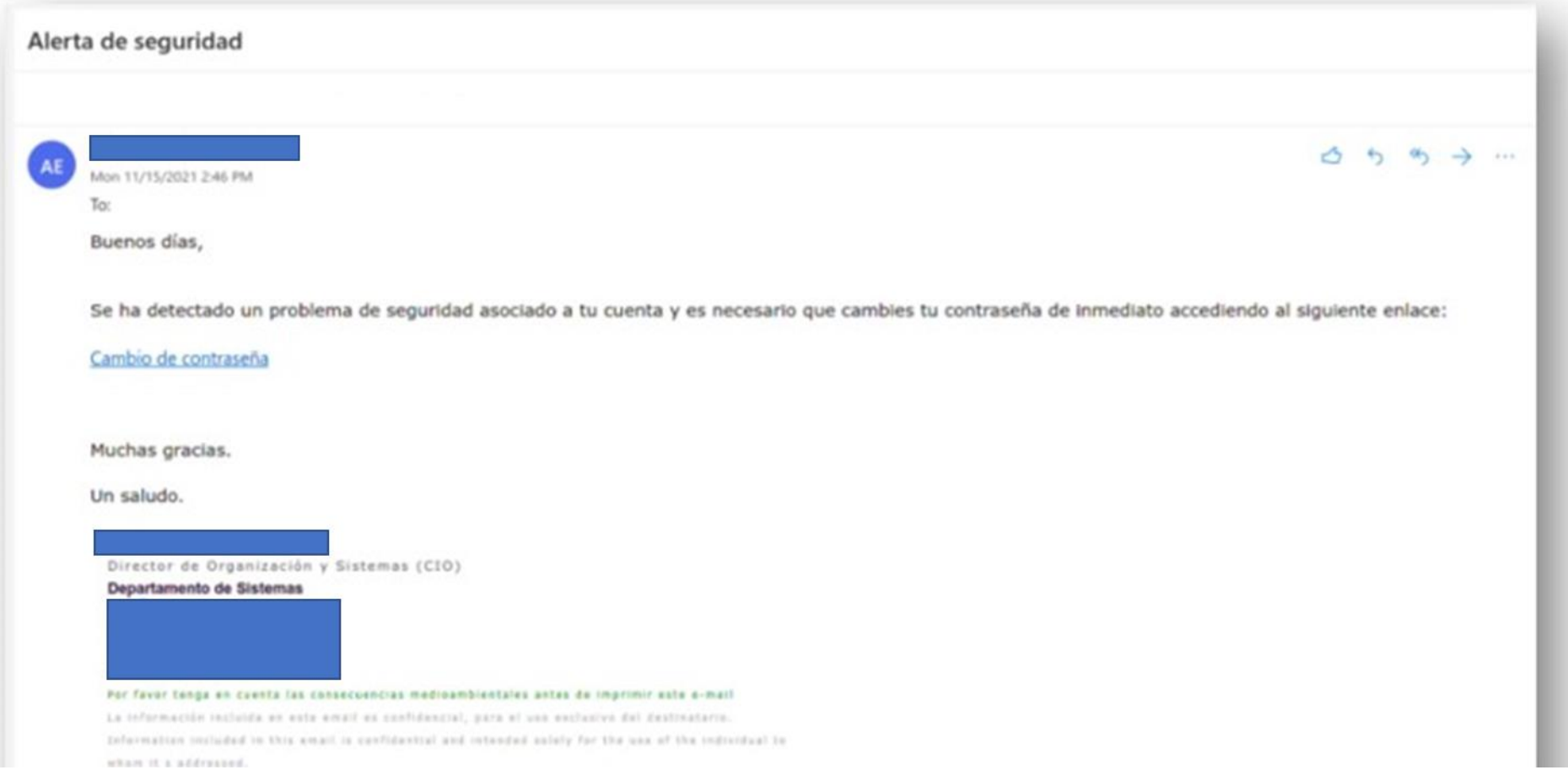
Principales vías de infección



Principales vías de infección

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

Asunto: Alerta de seguridad

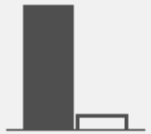


Datos 2022

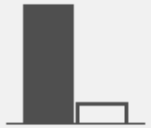
66 %
afectadas por el ransomware
en el último año

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

FUENTE: https://assets.sophos.com/X24WTUEQ/at/npk6g4rwkmqc4s5j7hcrvfpn/sophos-state-of-ransomware-2022-wpes.pdfm/X24WTUEQ/at/npk6g4rwkmqc4s5j7hcrvfpn/sophos-state-of-ransomware-2022-wpes.pdf

Medidas de protección

- ✓ Backup fuera de línea/protegidos
- ✓ Despliegue de tecnología de defensa: Antivirus, EDR, uso de sandboxes, etc.
- ✓ Segmentación de Red y control de acceso: Política de mínimos
- ✓ Control de versiones: parcheado y bastionado.
- ✓ Control de cuentas privilegiadas
- ✓ Concienciación
- ✓ Control de los puertos de salida a Internet
- ✓ Doble factor de autenticación
- ✓ Monitorización, capacidad de detección de anomalía
- ✓ Seguro de ciberriesgos que cubran el ransomware

Nivel de madurez

Muy bajo

Bajo

Medio

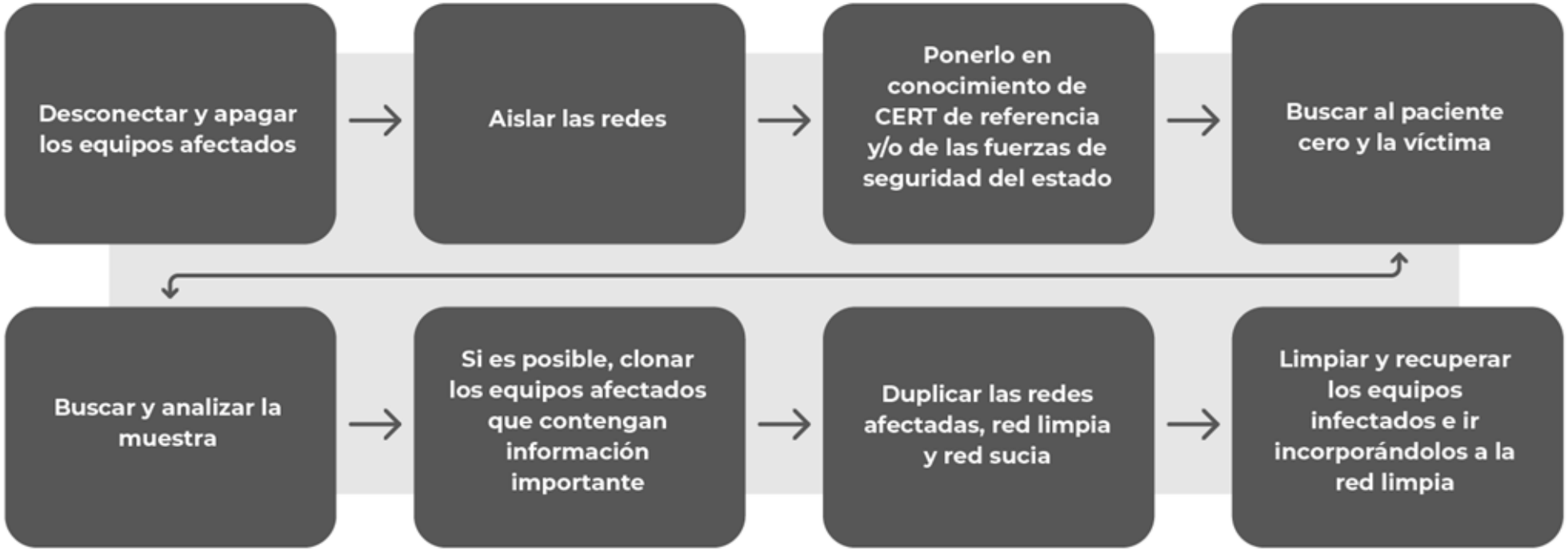
Aceptable

Alto

- ✓ Backup fuera de línea/protegidos
- ✓ Despliegue de tecnología de defensa: Antivirus, EDR, uso de sandboxes, etc.
- ✓ Segmentación de Red y control de acceso: Política de mínimos
- ✓ Control de versiones: parcheado y bastionado.
- ✓ Control de cuentas privilegiadas
- ✓ Concienciación
- ✓ Control de los puertos de salida a Internet
- ✓ Doble factor de autenticación
- ✓ Monitorización, capacidad de detección de anomalía
- ✓ Seguro de ciberriesgos que cubran el ransomware

Recuperación

Disponer de un procedimiento de gestión de incidentes



Lecciones aprendidas

Auxi Ureña
Consultora senior de ciberseguridad en Babel

auxi.urena@babelgroup.com