

IV ENCUENTRO REGIONAL DE MUNICIPIOS INTELIGENTES



Ciberseguridad Reto del presente

Javier Candau
Jefe Departamento Ciberseguridad
Centro Criptológico Nacional
ccn@cni.es / jdciber@ccn.cni.es



01

CONCEPTOS Y CONTEXTO.

Repaso a la situación actual.
¿Qué ha cambiado?

02

CNI / CCN.

CCN-CERT Funciones y
mandato

03

LEGISLACIÓN.

Evolución durante los
últimos años

04

CIBERAMENAZAS

Agentes más relevantes.
Incidentes 2023

05

INCIDENTES.

Casos últimos años

06

DESAFIOS.

Defensa vs ataque

07

CONCLUSIONES

Compartir para ganar. Escudo
único para España



<https://youtu.be/ZdCvYXhKqi0?si=ZyOtlxzAsL2k55VC>



<https://youtu.be/FqdaFsHcJns?si=1vrtHe2JrldPG5IA>



<https://youtu.be/iue2WgmHRIE?si=DpT5gHipzeejwUAa>



Un ataque informativo afecta a datos personales del Registro de animales de compañía de Cantabria

El Gobierno de Cantabria alerta: un ataque informático ha afectado a datos personales del Registro de animales de compañía de la comunidad.

Santander | 25.09.2023 12:38

Hackers roban DNIs y contraseñas a la Xunta procedentes de la base registro de animales de compañía

Es muy recomendable que las personas afectadas cambien sus contraseñas cuanto antes para evitar que los piratas informáticos puedan utilizarlas para acceder a otras bases de datos donde puedan haber utilizado la misma contraseña o variaciones de ésta.



Redacción | Martes, 3 de octubre de 2023, 20:06

Un ciberataque ha dejado a Telemadrid sin emisión en directo: ha tenido que recurrir a programas enlatados

Durante tres horas, la cadena autonómica ha tenido que emitir programas enlatados como el documental 'Madrid, desde el Aire'

6 comentarios

06.10.2023



Clínica

bilidad de

21/03/2023



grandes pañ

La web del Ayuntamiento de Los Llanos de Aridane recupera la normalidad tras un ciberataque

Los servicios jurídicos del Consistorio han denunciado ante la Agencia Española de Protección de Datos el ataque

22/03



El equipo de la Real Sociedad sufre un ciberataque que afecta a sus socios



08/11/2022

Un intento de hackeo obliga a parar el teletrabajo a la Agencia Tributaria

El ciberataque obligó al organismo a revocar los certificados de acceso en remoto por seguridad

[Alerta por un SMS que suplanta a la Agencia Tributaria: «No pinches, es un fraude»](#)

NO HAY TRANSFORMACIÓN DIGITAL SIN CIBERSEGURIDAD



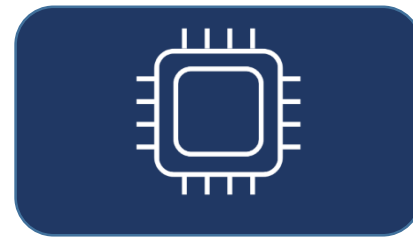
RED CORPORATIVA | NEGOCIO



USO DE LA NUBE



TELEFONÍA MÓVIL



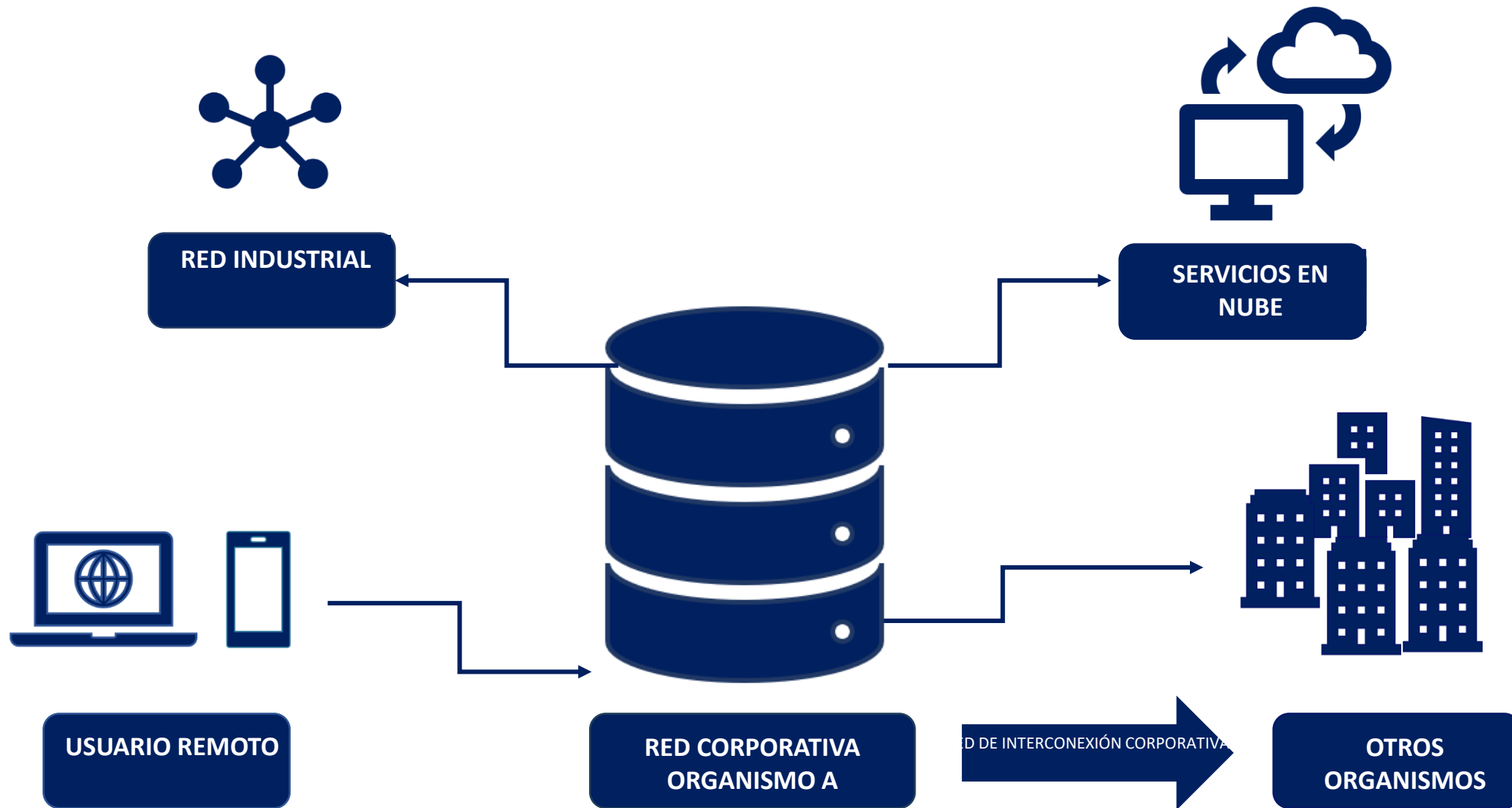
RED INDUSTRIAL



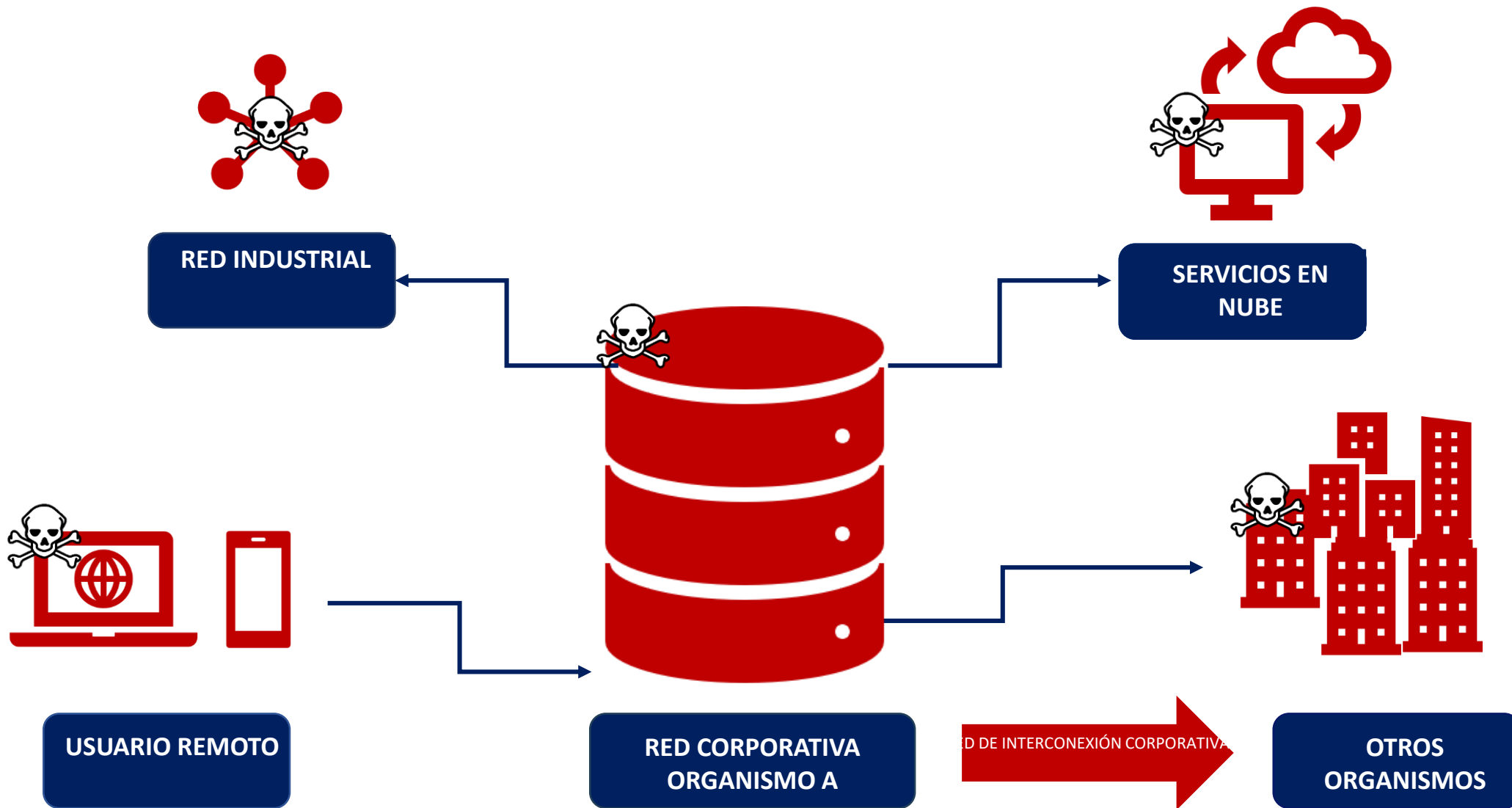
ACCESOS REMOTOS



- DESCENTRALIZADOS, PERO HIPERCONECTADOS

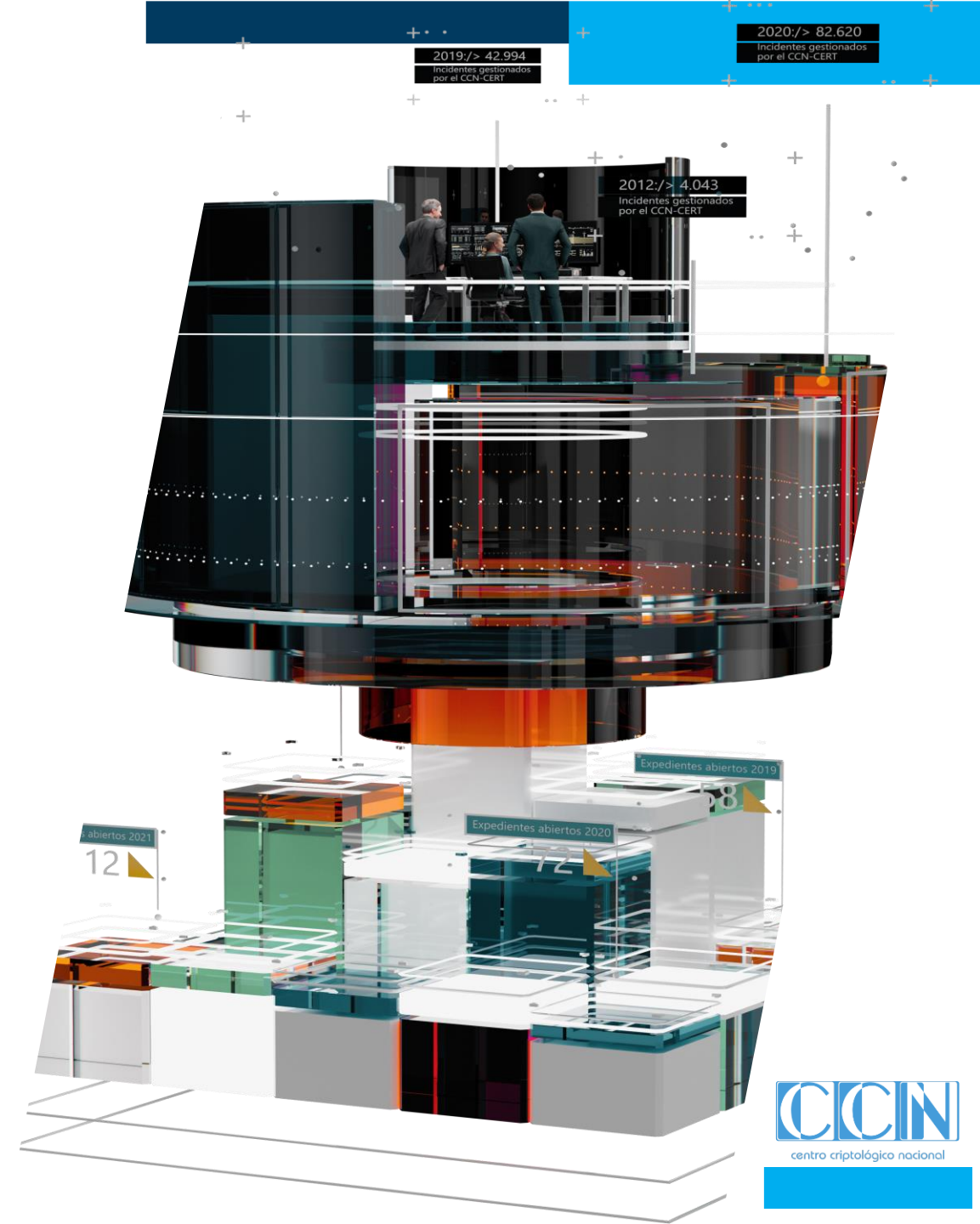


- DESCENTRALIZADOS, PERO HIPERCONECTADOS



- CAMBIO DE MODELO

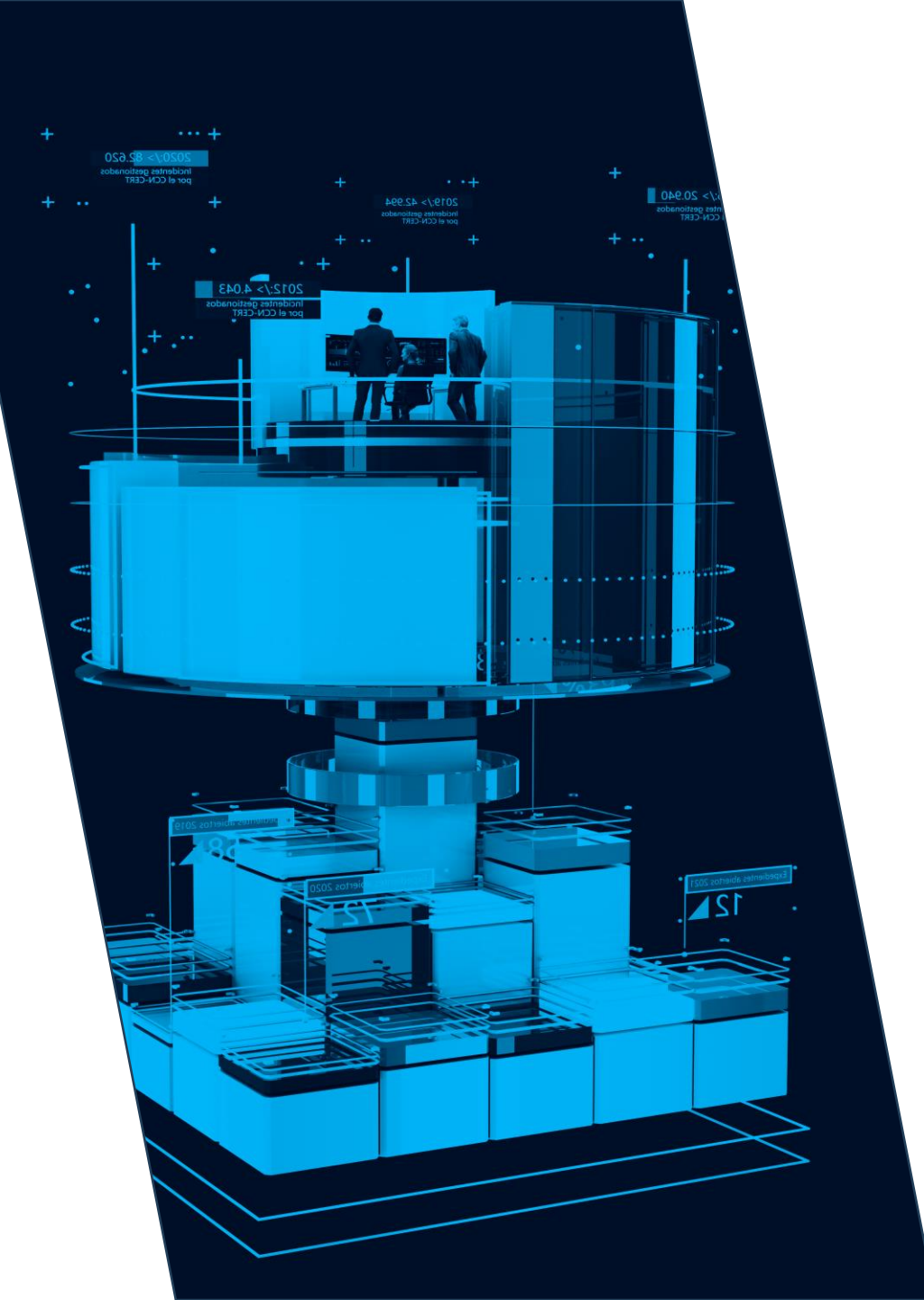
FULL TRUST



CAMBIO DE MODELO

ZERO TRUST

+ Vigilancia + Intercambio



01

CONCEPTOS Y CONTEXTO.

Repaso a la situación actual.
¿Qué ha cambiado?

02

CNI / CCN. CCN-CERT Funciones y mandato

03

LEGISLACIÓN.

Evolución durante los
últimos años

04

CIBERAMENAZAS

Incidentes 2023
Agentes más relevantes

05

INCIDENTES.

Casos últimos años

06

DESAFIOS.

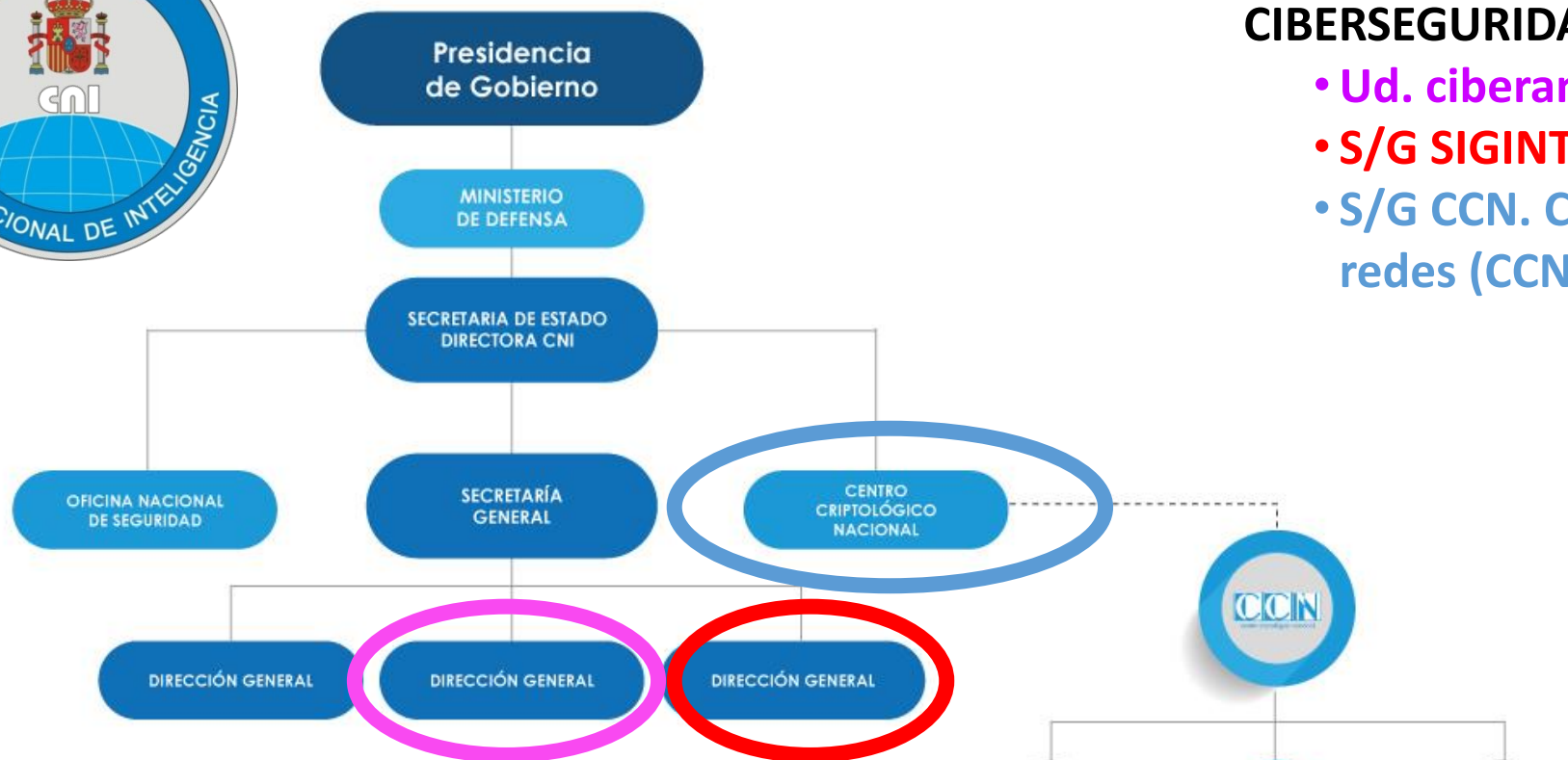
Defensa vs ataque

07

CONCLUSIONES

Compartir para ganar. Escudo
único para España

CNI /CCN



CIBERSEGURIDAD. Objetivo prioritario:

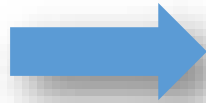
- Ud. ciberamenaza
- S/G SIGINT y capacidades de respuesta
- S/G CCN. Capacidades defensa de redes (CCN-CERT)



CCN / CCN-CERT



- Ley 11/2002 reguladora del **Centro Nacional de Inteligencia**.
- RD 421/2004, 12 de Marzo, que regula y define el ámbito y funciones del **CCN**.



- RD 311/2022 de 4 de mayo, que regula el **Esquema Nacional de Seguridad** para todo el **Sector Público** + sistemas manejan **información clasificada** + **Sector privado** (preste servicios S. Público). (Antecedentes: RD 3/2010 y RD 951/2015) (Desarrollo: Art 156.2 de la Ley 40/2015)
- RDL 12/2018, de 7 de septiembre, de Seguridad de las Redes y Sistemas de Información. **Coordinación incidentes**.
- RDL 14/2019, de 31 de octubre, Medidas urgentes. **Coordinación CSIRT públicos y enlace con exterior**
- RD 43/2021, de 28 de enero, Desarrollo RDL 12/2018. **Plataforma Nacional**

MISIÓN

Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al **Sector Público** a afrontar de forma activa las nuevas ciberamenazas.

COMUNIDAD

Responsabilidad en ciberataques sobre:

- **sistemas clasificados**,
- sistemas del **Sector Público**,
- empresas y organizaciones de **sectores estratégicos** para el país en coordinación con el CNPIC.

SERVICIOS CCN-CERT

PREVENCIÓN

Reducir la superficie de exposición



DETECCIÓN

Vigilancia Continua



RESPUESTA

Eficiente e integrada



- ✓ Guías y estándares de seguridad
- ✓ Avisos y vulnerabilidades
 - Amenazas | Malware | Mejores prácticas
- ✓ Auditorías | Inspecciones
- ✓ **Formación- ANGELES**
- ✓ Implantación del ENS



- ✓ **Sistemas de Alerta Temprana**
- ✓ Análisis de Anomalías
- ✓ **Intercambio de información**
 - Ciberincidentes y ciberamenazas
 - Plataforma Nacional
- ✓ Despliegue de equipos RRT. **Ataques complejos**
- ✓ Centro de Operaciones de Ciberseguridad
 - **Red Nacional de COCS**
- ✓ Coordinación técnica de CERTs / SOC,s
 - Ataques NO complejos



• ÁNGELES. NUEVA APROXIMACIÓN A LA FORMACIÓN

En colaboración con



+15,8k

alumnos formados en
2023

+2,8k

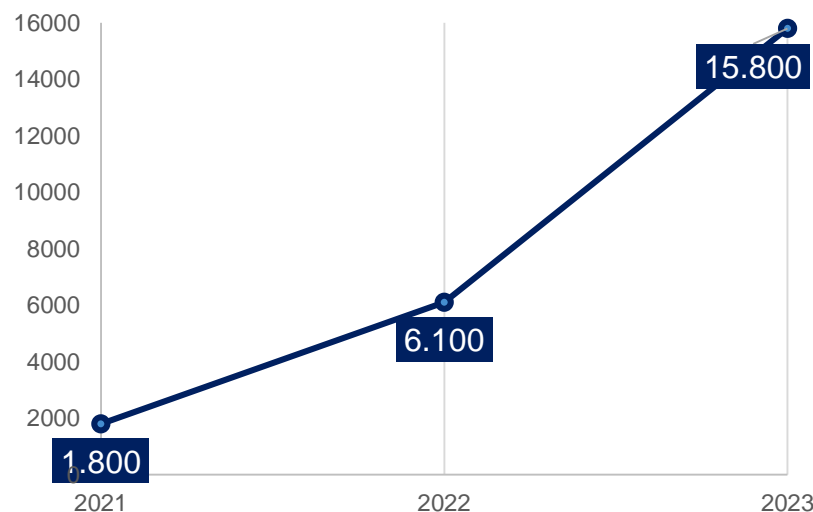
horas de formación
impartidas en 2023

113

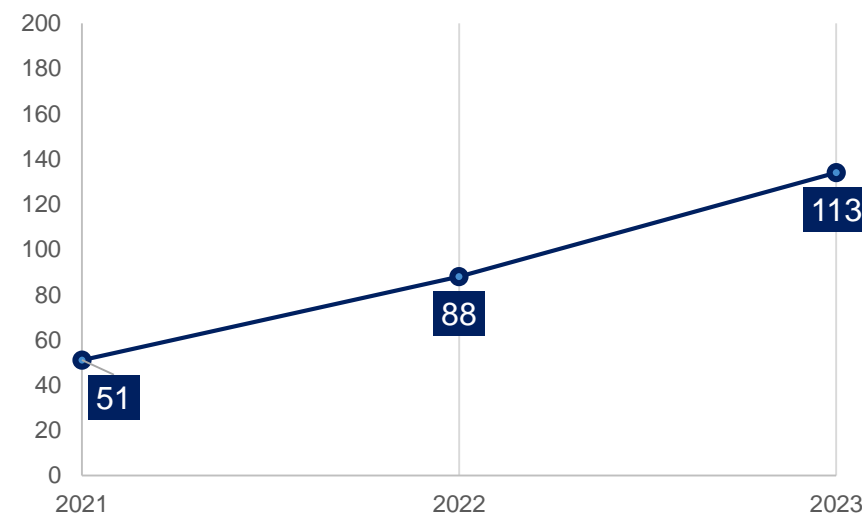
cursos impartidos en
2023

+31k

usuarios registrados en
ÁNGELES



Evolución alumnos formados



Evolución cursos impartidos

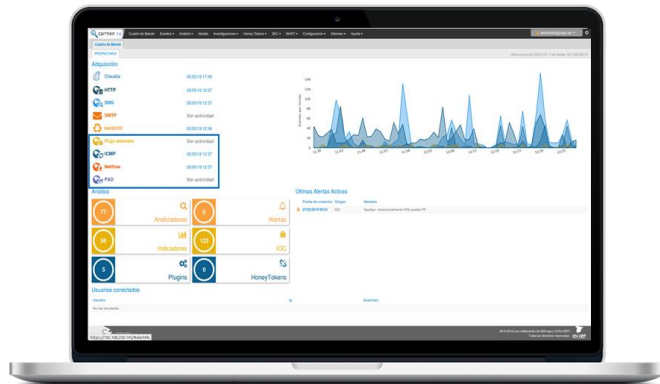
- Vigilancia Continua. Servicios de detección

 **403 / 406**
organismos y empresas
adscritos

+70
nuevos organismos
adscritos en 2023

 **50**
Áreas de conexión

 **47/38**
entidades **+10** en 2023



 **74**
Implantaciones en
organismos y empresas

 **carmen**
central **47**
Integraciones con
CARMEN Central

 **24**
Despliegues en
servidores y puestos
usuarios

01

CONCEPTOS Y CONTEXTO.

Repaso a la situación actual.
¿Qué ha cambiado?

02

CNI / CCN.
CCN-CERT Funciones y
mandato

03

LEGISLACIÓN.
Evolución durante los
últimos años

04

CIBERAMENAZAS
Incidentes 2023
Agentes más relevantes

05

INCIDENTES.

Actualización de datos anuales
Casos últimos años

06

DESAFIOS.

Defensa vs ataque

07

CONCLUSIONES

Compartir para ganar. Escudo
único para España

• Incidentes

2022

+55k

Incidentes gestionados

29%

notificados por organismos

75

incidentes críticos

2023

+105k

Incidentes gestionados

52%

notificados por organismos

+120

incidentes críticos

*Datos estimados a diciembre de 2023

Evolución de incidentes
aportados por organismos



27%
2019



14%
2020



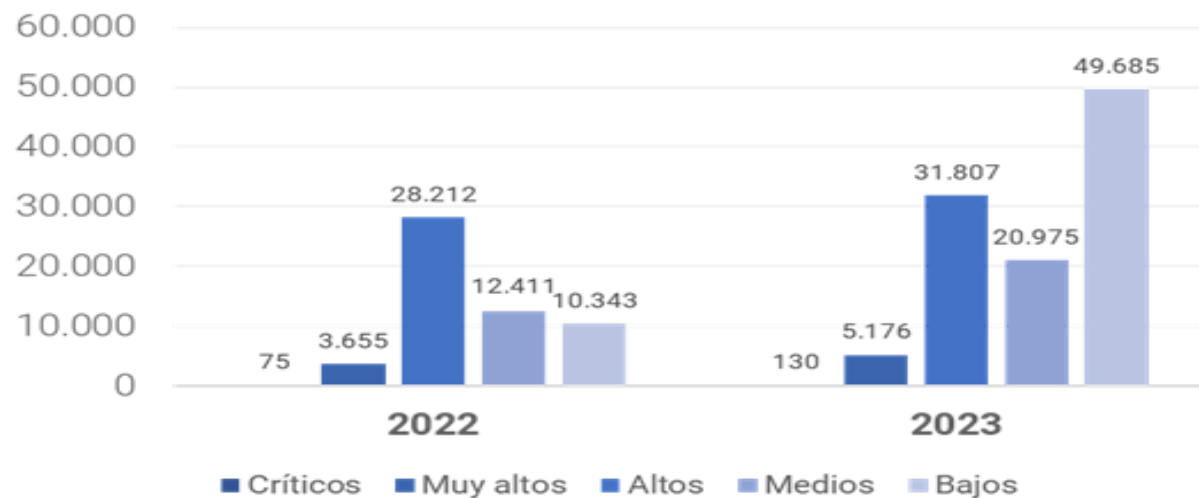
19%
2021



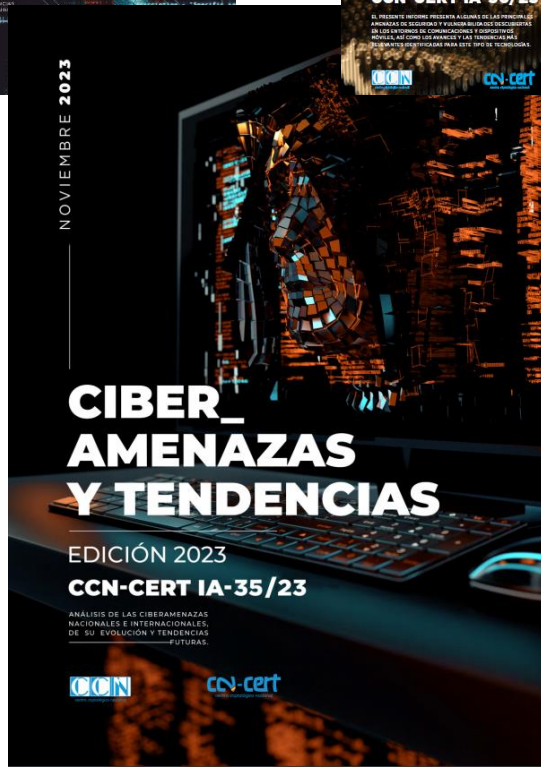
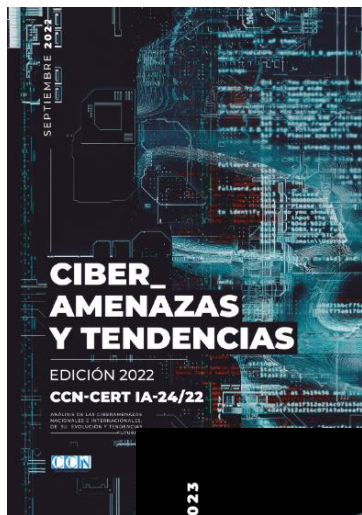
29%
2022

¿Estamos viendo todos los incidentes?

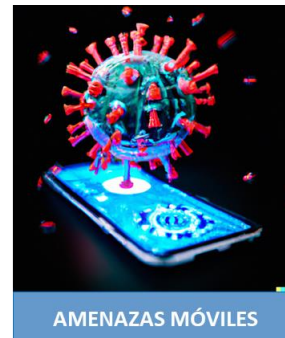
CRITICIDAD DE LOS INCIDENTES



¿Quién nos ataca?



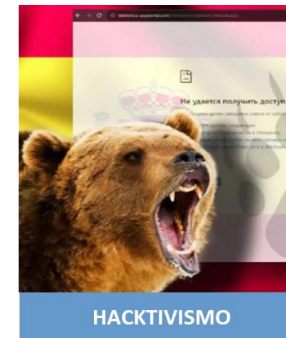
RANSOMWARE



AMENAZAS MÓVILES



ACTORES ESTADOS

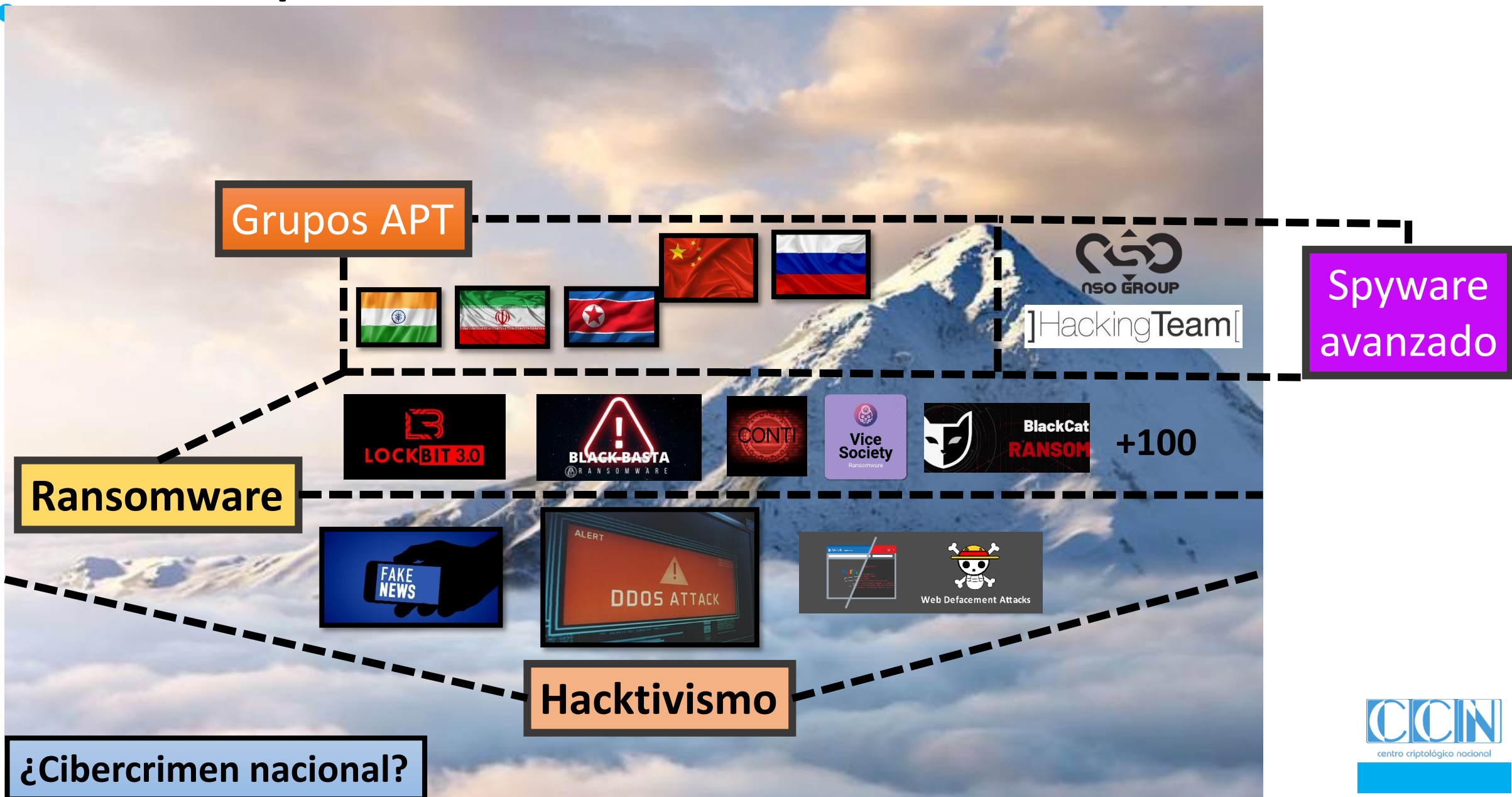


HACKTIVISMO



ACTORES INVITADOS

¿Contra qué luchamos?

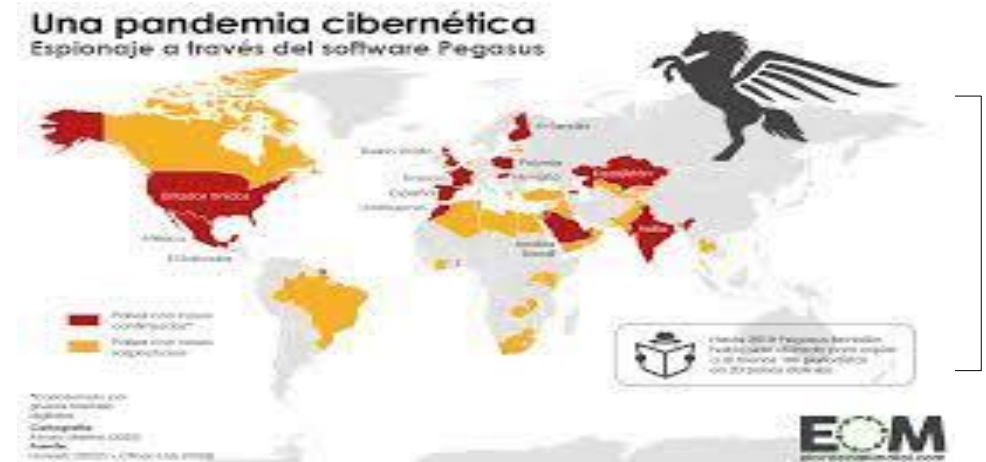


AMENAZAS MÓVILES 2022 / 23



AMENAZAS MÓVILES

- “Nuevo” escenario.
- Difícil detección y defensa frente a ellas.
- Responsabilidad repartida entre AAPP.
- Frontera entre datos personales y oficiales.
- No asociadas a un único actor.
- Sistemas “cerrados”.
- Malware autoprotegido.



01

CONCEPTOS Y CONTEXTO.

Repaso a la situación actual.
¿Qué ha cambiado?

02

CNI / CCN.

CCN-CERT Funciones y
mandato

03

LEGISLACIÓN.

Evolución durante los
últimos años

04

CIBERAMENAZAS

Agentes más relevantes

05

INCIDENTES.

Casos últimos años

06

DESAFIOS.

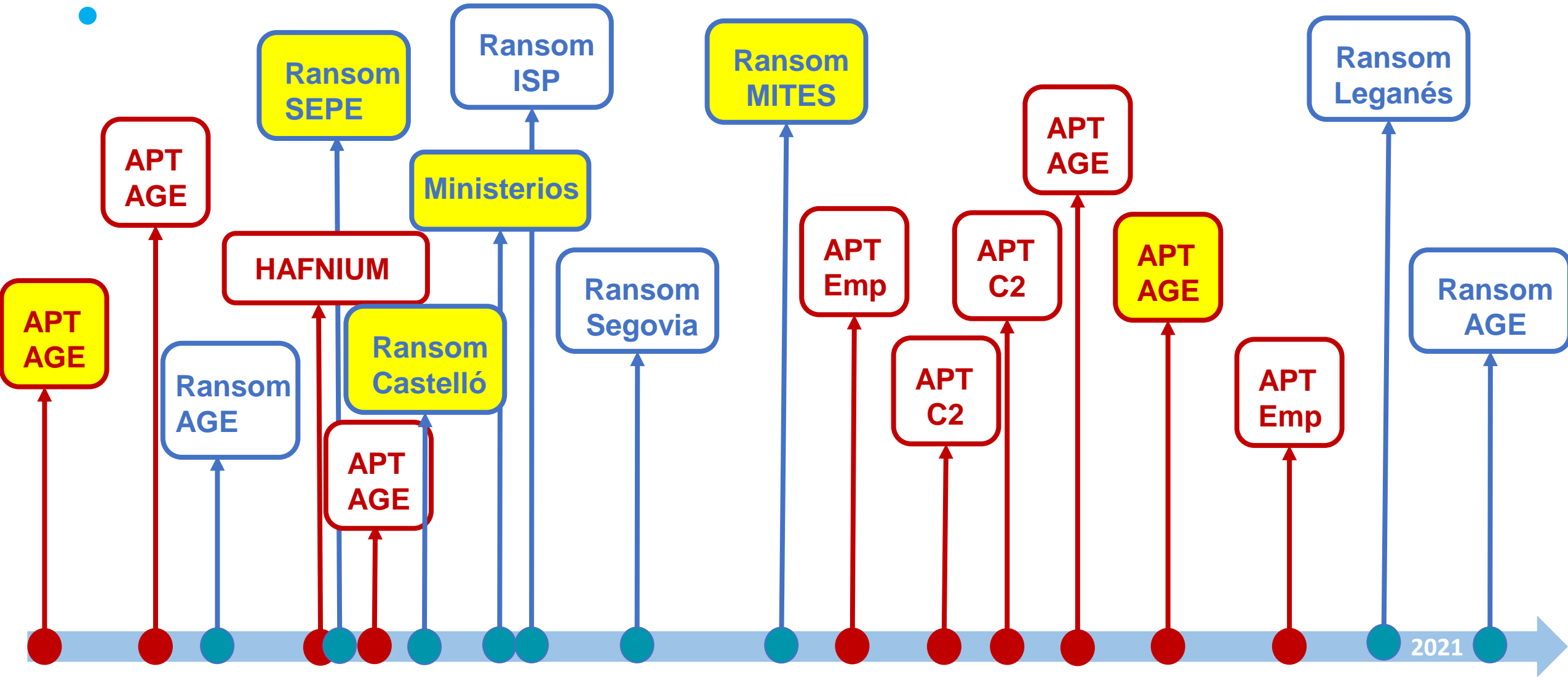
Defensa vs ataque

07

CONCLUSIONES

Compartir para ganar. Escudo
único para España

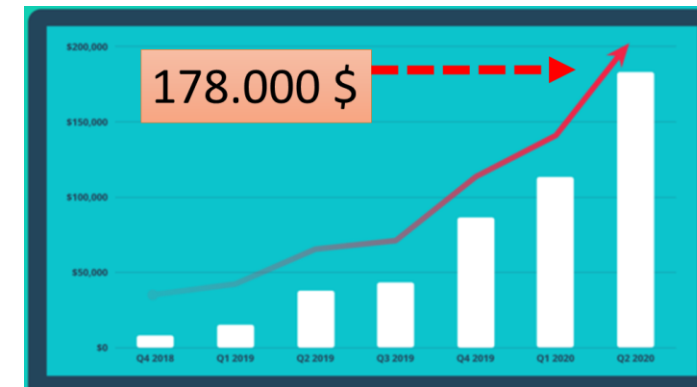
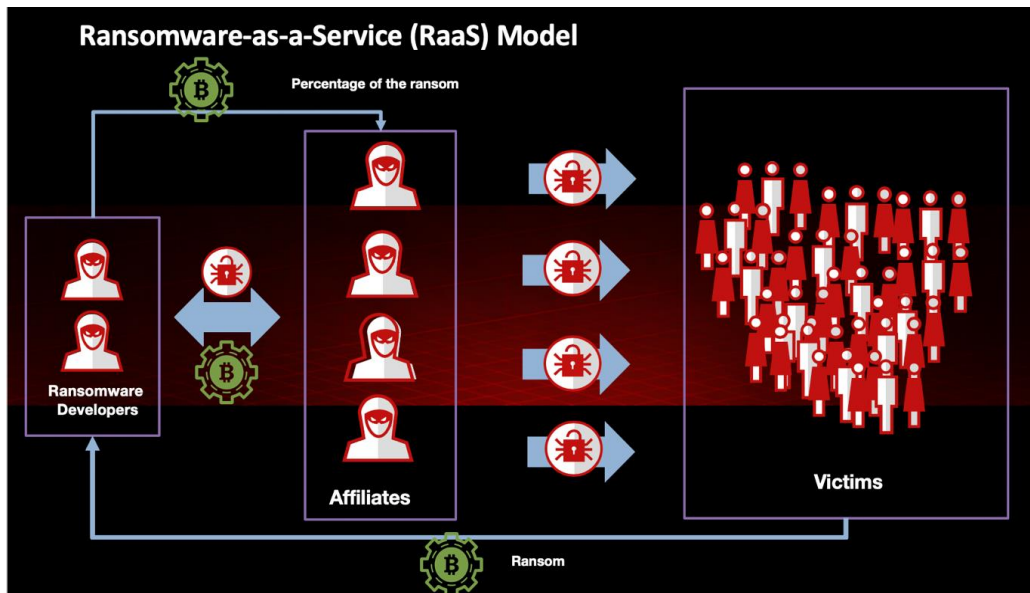
CIBERAMENAZAS 2021. LA PANDEMIA DE RANSOMWARE



• CIBERCRIMEN



- **Inicio:** 1998
- **Inicio en España:** 1998. **Actor:** Varios. Grupos de ataque de ransomware
- **Estado actual:** RIESGO MUY ALTO
- **Acción más relevante:** +50 acciones al año (media)



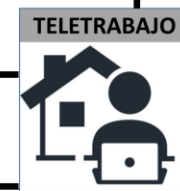
1. CREDENCIALES DÉBILES EN SISTEMAS DE ACCESO REMOTO (VPN/CITRIX/..)

2. COMPRA DE CREDENCIALES LEGÍTIMAS EN MERCADO NEGRO

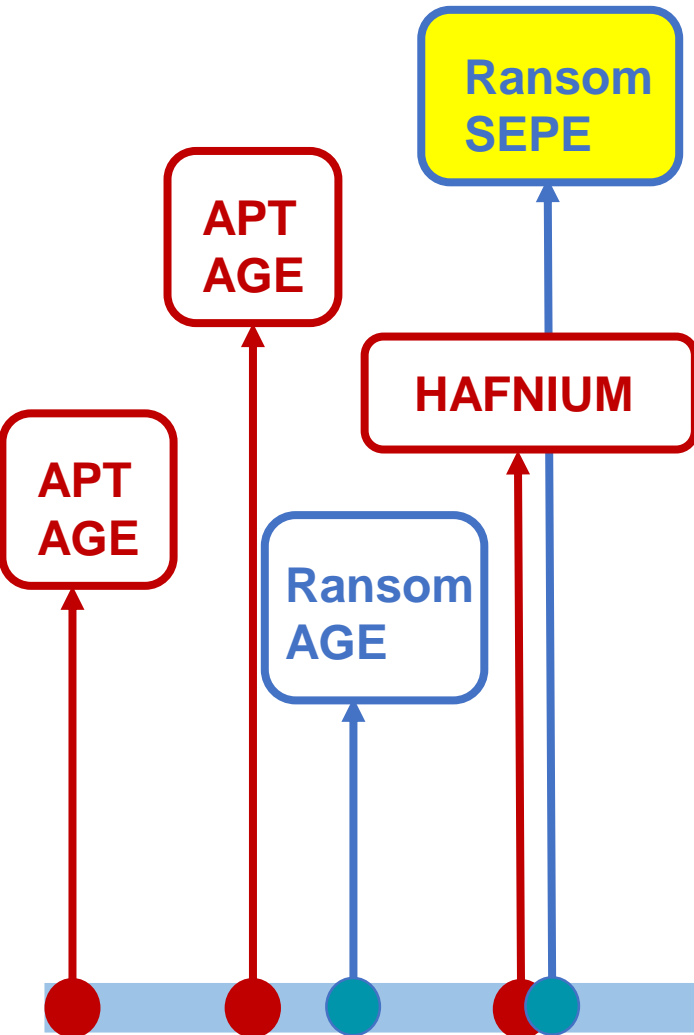
3. EXPLOTACIÓN DE VULNERABILIDADES EN PERÍMETRO

4. ATAQUES DE PHISHING

ESQUEMA TRADICIONAL DE ATAQUE



INCIDENTES 2021

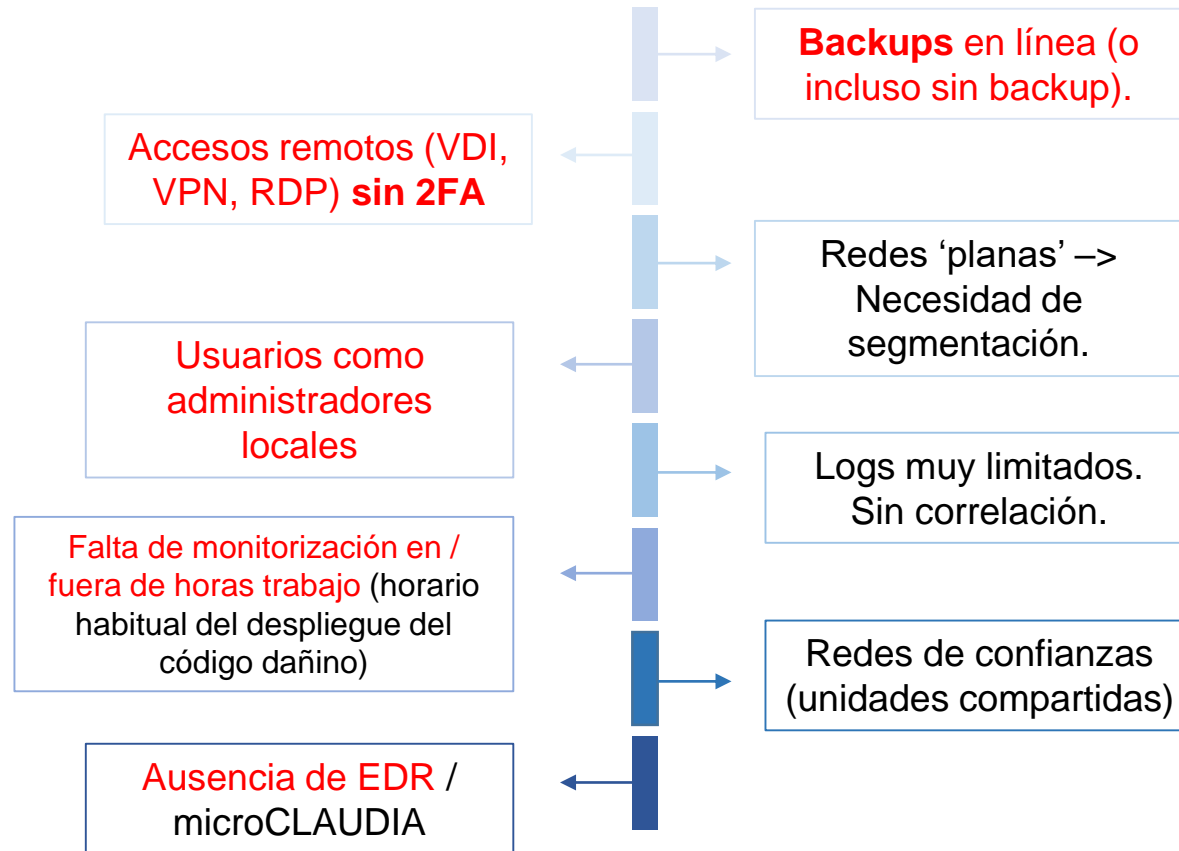


Marzo 2021 – Ryuk

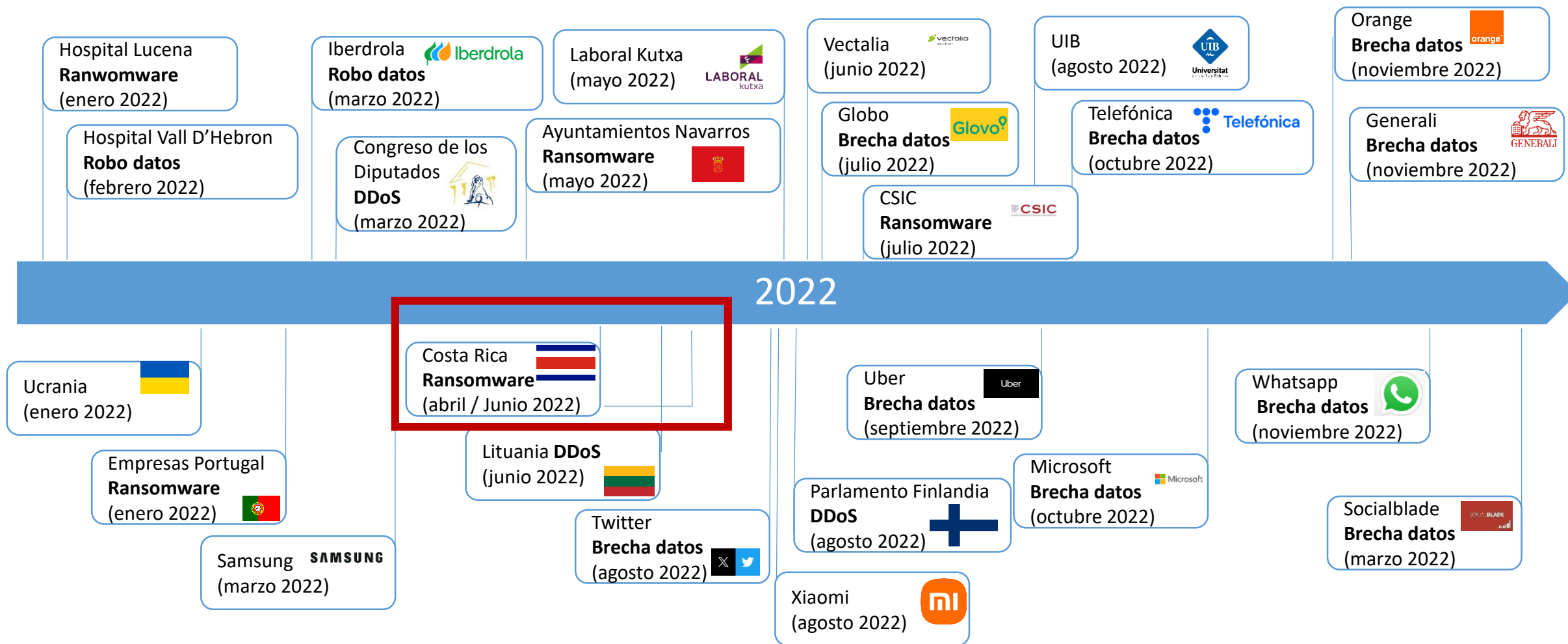
- Afectación servicios críticos
- Sedes remotas
- Acceso vía Citrix (~10USD)
- Cobalt Strike Beacon + BazaarLoader + SystemBC
- Despliegue RRT

El SEPE sufre un ataque informático que paraliza sus servicios y retrasa la gestión de "centenares de miles de citas"

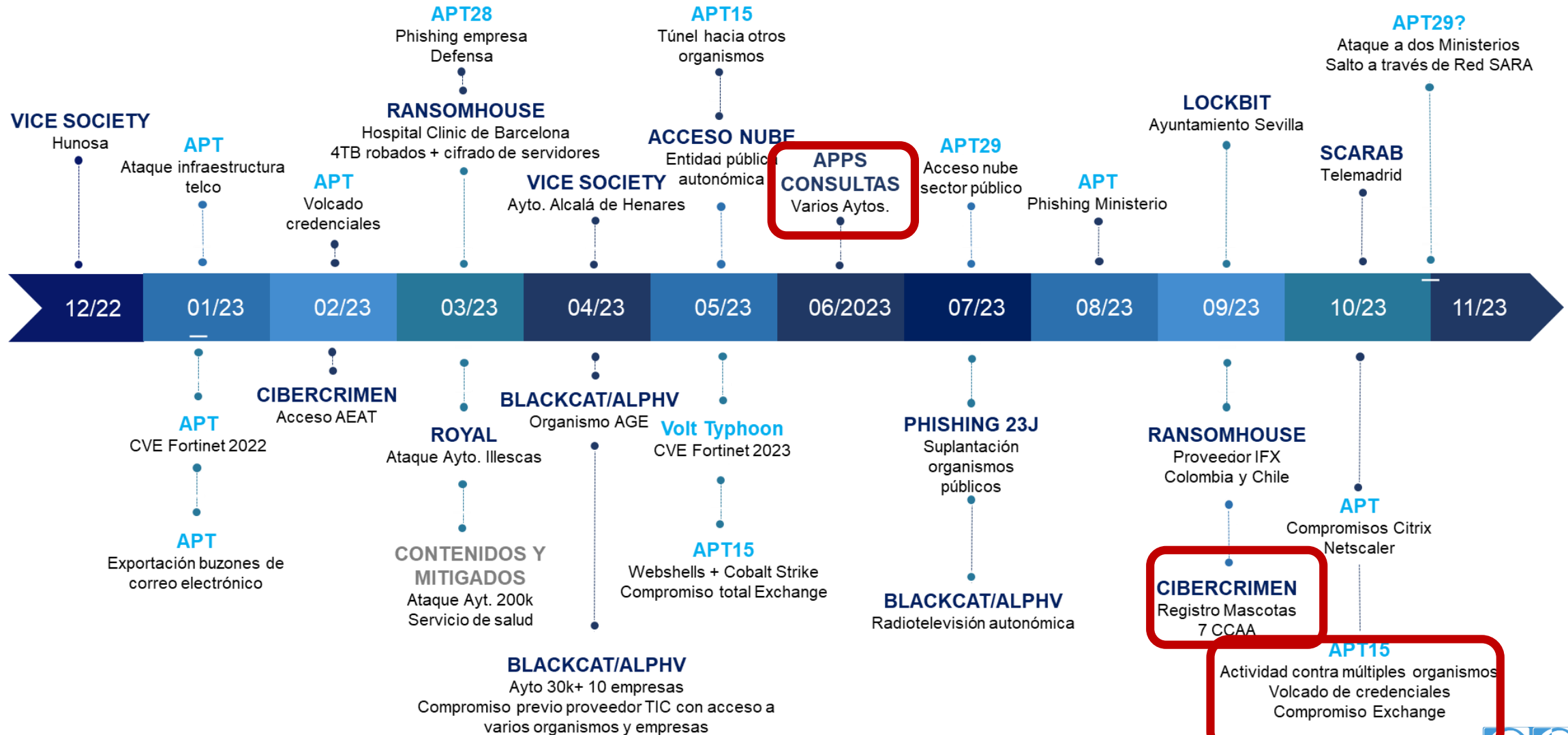
• Lecciones **no** aprendidas



• Ciberamenazas 2022



Ciberamenazas 2023



Modus operandi

1. INVESTIGACIÓN SOBRE VÍCTIMA

- ✓ Recopilación de información en fuentes abiertas, manuales, etc.
- ✓ Identificación de punto de entrada a INTRANET, CITRIX, RDP, VPN → **SUPERFICIE DE EXPOSICIÓN**

2. COMPRA DE ACCESOS EN MERCADO NEGRO, FOROS, BILATERAL A OTROS ACTORES // **PHISHING**

3. ENTRADA Y RECONOCIMIENTO

- ✓ Empleo de VPN y PROXY desde VPS contratado con BTC → **BUEN OPSEC**
- ✓ Identificación de web-services consumibles
- ✓ Identificación de escritorios remotos accesibles
- ✓ Pivotaje y movimiento lateral

4. PERSISTENCIA EN RED

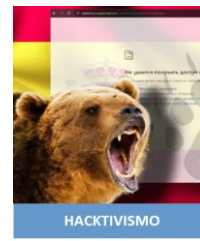
- ✓ Creación de nuevos usuarios con privilegios
- ✓ Despliegue de webshells, RATs, etc.

5. PRUEBAS DE CONSUMO AUTOMATIZADO DE LA INFORMACIÓN

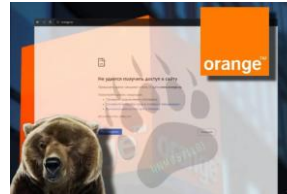
- ✓ Desarrollo de scripts de ingesta en base de datos → **EXFILTRACIÓN**

6. MONETIZACIÓN DE LA INFORMACIÓN → **VENTA EN MERCADO NEGRO // ENCARGOS PARTICULARES**

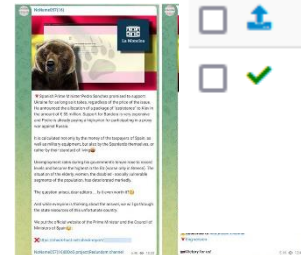
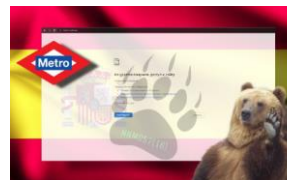
• HACKTIVISMO. DDOS



NoName057(16)



We shut down the official website of the royal family of Spain:
<https://check-host.net/check-report/10ab55b6k77a>
 Subscribe to NoName057(16)
 Join our DDoS-project
 Subscribe to reserve channel
 Victory will be ours!
 t.me/noname05716eng/2013 1.2K edited Jul 19 at 11:34



<input type="checkbox"/>	<input type="checkbox"/>	Creator org	ID	Tags	#Attr.
<input type="checkbox"/> <td><input checked="" type="checkbox"/></td> <td>RNS (Red Nacional de SOC)</td> <td>? 7584</td> <td> red-nacional-soc:source="element" red-nacional-soc:file="DDOSNONAME19072023tetxt" source:red-nacional-soc red-nacional-soc:org="CCN-CERT" </td> <td>2528</td>	<input checked="" type="checkbox"/>	RNS (Red Nacional de SOC)	? 7584	red-nacional-soc:source="element" red-nacional-soc:file="DDOSNONAME19072023tetxt" source:red-nacional-soc red-nacional-soc:org="CCN-CERT"	2528



- 17-03-2023 10 Organismos AGE
- 30-03-2023 4 Organismos AGE
- 31-03-2023 3 Organismos AGE
- 13-04-2023 3 Organismos AGE
- 06-06-2023 2 Organismos AGE
- 30-07-2023 17 Organismos + empresas
- 07-09-2023 CERT Europeos
- 21-09-2023 12 Organismos AGE
- 03-10-2023 18 Organismos
- 27-10-2023 14 Organismos gallegos**



01

CONCEPTOS Y CONTEXTO.

Repaso a la situación actual.
¿Qué ha cambiado?

02

CNI / CCN.
CCN-CERT Funciones y
mandato

03

LEGISLACIÓN.
Evolución durante los
últimos años

04

CIBERAMENAZAS
Agentes más relevantes

05

INCIDENTES.

Actualización de datos anuales
Casos últimos años

06

DESAFIOS.

Defensa vs ataque

07

CONCLUSIONES

Compartir para ganar. Escudo
único para España

• **CONCLUSIONES. Salir a Ganar**

- 1. Necesidad de servicios horizontales de ciberseguridad**
- 2. Tenemos que empoderar al CISO. Cumplir el ENS**
- 3. Tenemos que reducir superficie de exposición**
- 4. Compartir antes que responder. RNS + PNNSC**
- 5. Salir a Ganar. Medidas de Ciberdefensa Activa**

• 1. Servicios Horizontales Ciberseguridad



Servicios de Detección 24*7
 Servicios de Auditoría
 Superficie de exposición
 Servicios de cumplimiento ENS
 Servicios AntiDOS



 +130 vacunas desarrolladas	 +1.2 M alertas generadas	 +900 K equipos protegidos con microCLAUDIA	 +2.2K organismos datos de alta
---	---	--	--

VACUNAS ESPECÍFICAS

- | | |
|-----------------|-----------------|
| ▪ PYSa | ▪ Phobos |
| ▪ Avaddon | ▪ Robbin Hood |
| ▪ BitPaymer | ▪ Sadogo |
| ▪ Cobalt Strike | ▪ Snake |
| ▪ Conti | ▪ Sodinokibi |
| ▪ Egregor | ▪ Wannacry |
| ▪ Lockbit | ▪ Zeppelin, etc |



+400
sondas



● AGENCIA DE CIBERSEGURIDAD, ¿BALA DE PLATA?



8131
Ayuntamientos

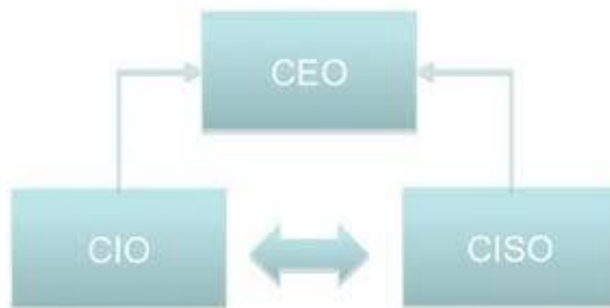
52
Diputaciones y cabildos

1101
Mancomunidades y comarcas

+ 5500
Empresas públicas, fundaciones...

MEJOR MÁS AGENCIAS

• 2. Empoderar al CISO. Certificación ENS



ESQUEMA NACIONAL
DE SEGURIDAD

RESPONSABLE DE SEGURIDAD



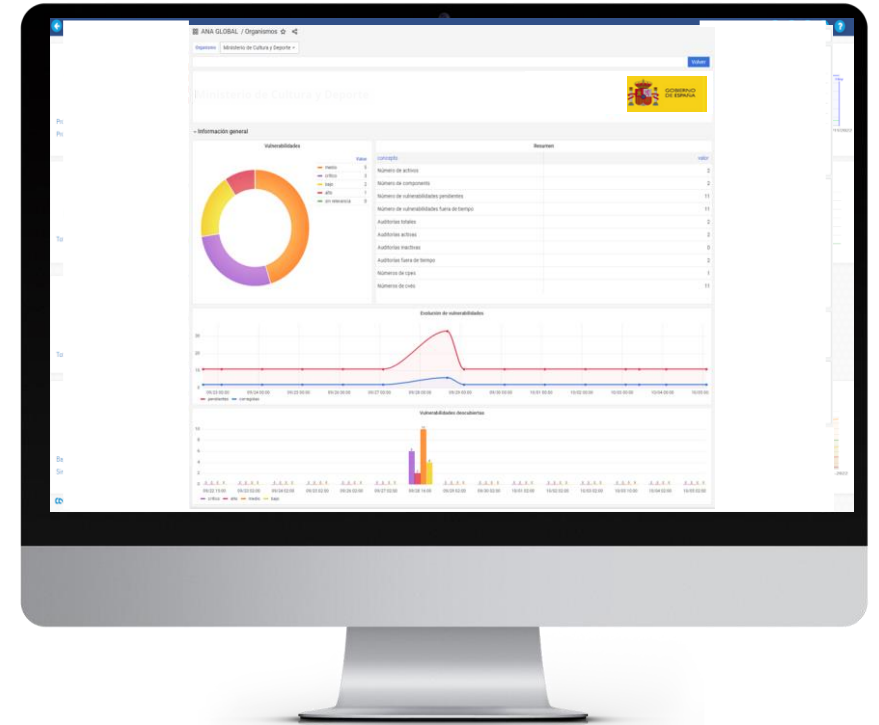
+290
Organismos certificados

+730
Empresas certificadas

Ante esta Transformación Digital.
La visión de la ciberseguridad es CRÍTICA

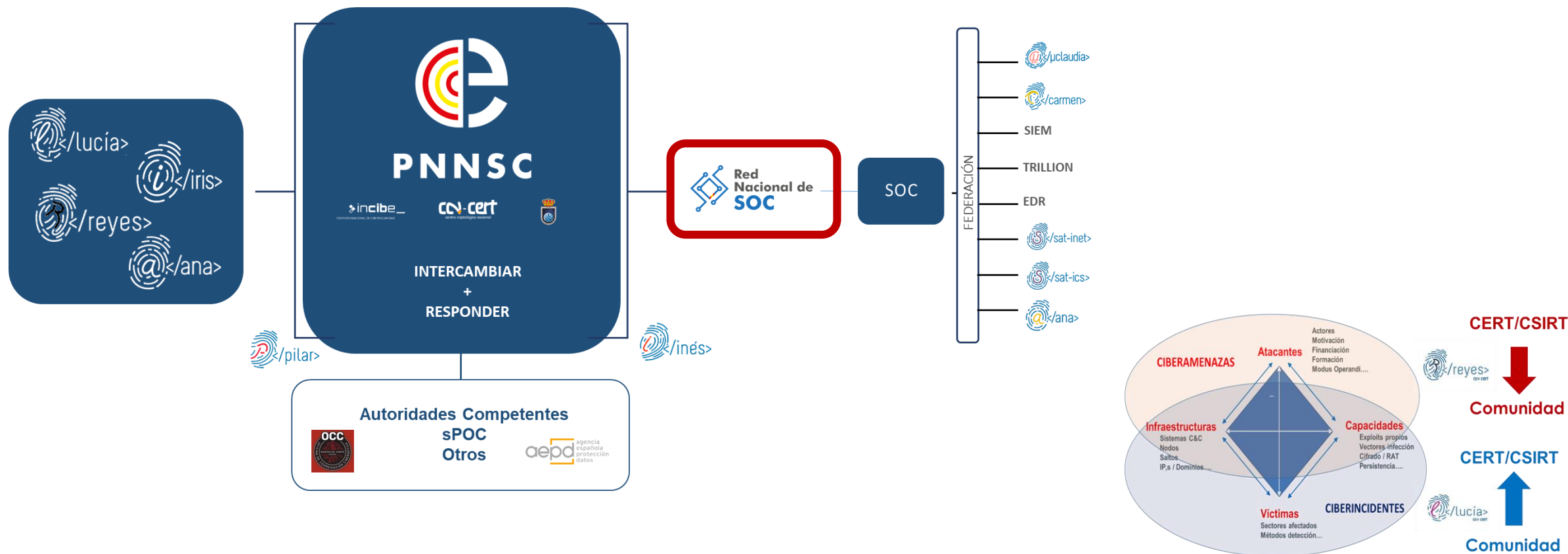
- **3. Reducir superficie de exposición**

¿Auditoria para cumplimiento normativo o como mejora continua?



Conocer la superficie de exposición y reducirla

4. Compartir antes que responder



Intercambiar TODO y por máquinas, no humanos.
IoC, IoA y buenas prácticas iiii

• 5. Salir a Ganar. Medidas Ciberdefensa Activa



[MCDA_1]

DNS ADMINISTRACIÓN



[MCDA_2]

CAPACIDAD CAZA AMENAZA

2.1 IDENTIFICACIÓN Y ELIMINACIÓN DE C2
2.2 DETECCIÓN DE ATAQUES BASADO ANOMALÍAS



[MCDA_3]

SUPERFICIE DE EXPOSICIÓN
AUTOMÁTICA (ANA-ELSA)



[MCDA_4]



PREVENCIÓN y CUMPLIMIENTO
INES / ANGELES / μCENS



[MCDA_5]

DETECCIÓN AVANZADA EN
MÓVILES



[MCDA_6]

COORDINACIÓN RESPUESTA
COCS-AGE / ENSOC / RNS



[MCDA_7]

PNNSC
CIBERINTELIGENCIA / CIBERINCIDENTES



[MCDA_8]

SERVICIOS DETECCIÓN COMUNES
SAT INET / SAT ICS / μCLAUDIA

• CONCLUSIONES

DESAFÍOS DEL SECTOR PÚBLICO



No hay transformación digital sin ciberseguridad



TECNOLOGÍA CERTIFICADA

Tecnologías certificadas y sistemas de conformidad con el ENS. CPSTIC|CCN-STIC 105. Certificación LINCE a las aplicaciones que utilizamos.



AUDITORÍA CONTINUA

Auditorías periódicas de todo lo que entre en producción. Reducir superficie de exposición. PNNSC (REYES + ELSA).



MÍNIMO PRIVILEGIO

Aplicación de políticas de seguridad por defecto. Cambio de modelo del FULL TRUST al ZERO TRUST. .



VIGILANCIA CONTINUA

Vigilancia 24/7 a través de los Centros de Operaciones de Ciberseguridad (SOC). Compartir y responder a través de la Red Nacional de SOC.



RESPUESTA INTEGRADA

Intercambio continuo de incidentes e información sobre ciberamenazas. Compartir para ganar. Plataforma Nacional + RRT.



CIBERDEFENSA ACTIVA

Medidas de basadas en capacidades de ciberinteligencia para una mejor protección y defensa. Llevar el combate al campo del atacante.

Muchas

Gracias



**IV CONGRESO
JORNADAS & ROOTED_
STIC CON**

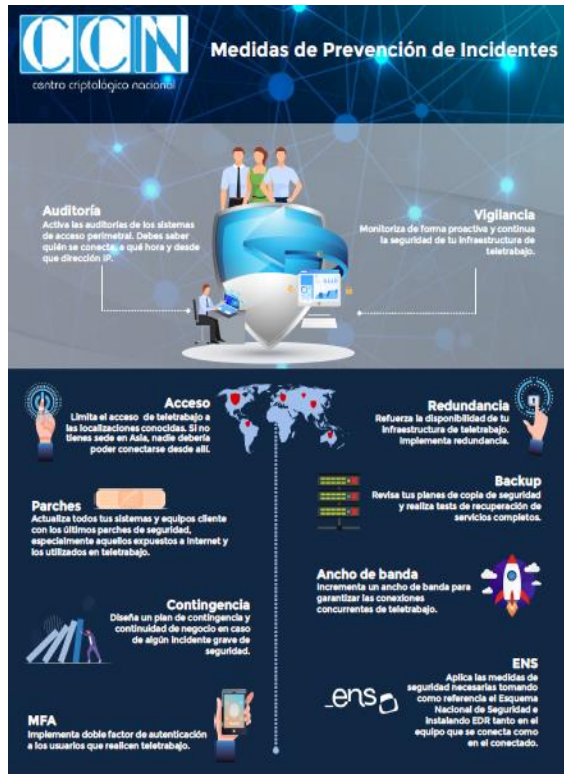
CAPÍTULO PANAMÁ

CCN-cert **espedef-cert** **/RootedCON®** **incibe_** **REPÚBLICA DE PANAMÁ** **AIG**

**PANAMÁ,
DEL 10 AL 12 DE ABRIL DE 2024** | **#STICPANAMÁ**



Medidas Prevenir ciberincidentes



1. Comprobar los posibles **compromisos de contraseñas cada vez que se hacen públicas**. Además, sería útil **monitorizar la clandestinidad criminal / underground** y buscar regularmente indicios de brechas de seguridad en la red.
2. Si se sospecha de que algunas de sus credenciales están expuestas, **activar un restablecimiento de contraseña para todos los usuarios**. Considerar también restablecer las credenciales de sistema y cuentas de servicio.
3. Implementar un **sistema de autenticación de dos factores (2FA)** para los usuarios remotos, si aún no lo ha hecho.
4. Después de un ataque, valorar **escenario de múltiples fases / atacantes**. Los ataques hoy en día ocurren en dos o más etapas.
5. Supervisar el **comportamiento de los usuarios** buscando anomalías. Chequear los registros SIEM/MDR y establecer alertas.
6. Estar atento a lo que ocurre en la DMZ. Dar por sentado que los servicios orientados a internet (VPN, correo web, servidores web, entre otros) están **bajo constante ataque en un entorno hostil**.
7. Implementar la **segmentación y la microsegmentación de la red** para dificultar el movimiento lateral y permitir la supervisión de la seguridad.
8. Seguir las **mejores prácticas y estándares de referencia**.
9. **Suponer que los usuarios han perdido sus contraseñas y, por lo tanto, se está siempre expuesto**.
10. **Monitorizar continuamente la postura de seguridad**.