CCN-CERT. Ciberamenazas 2024

Desafios y Soluciones

Javier Candau
Adjunto al Subdirector
Centro Criptológico Nacional
ccn@cni.es / adjccn@ccn.cni.es

- # PREGUNTA 1

¿Cómo ve la situación de la ciberseguridad?

Diario de Sevilla

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

Clínic tema

EL PAÍS

España

ANDALUCÍA · CATALUÑA · COMUNIDAD VALENCIANA · GALICIA · MADRID · PAÍS VASCO · ÚLTIMAS NOTICIAS

Actualidad

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

08/11/2022

21/03/2023

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»

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

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

22/03

NO HAY TRANSFORMACIÓN DIGITAL SIN CIBERSEGURIDAD

RED CORPORATIVA | NEGOCIO

USO DE LA NUBE

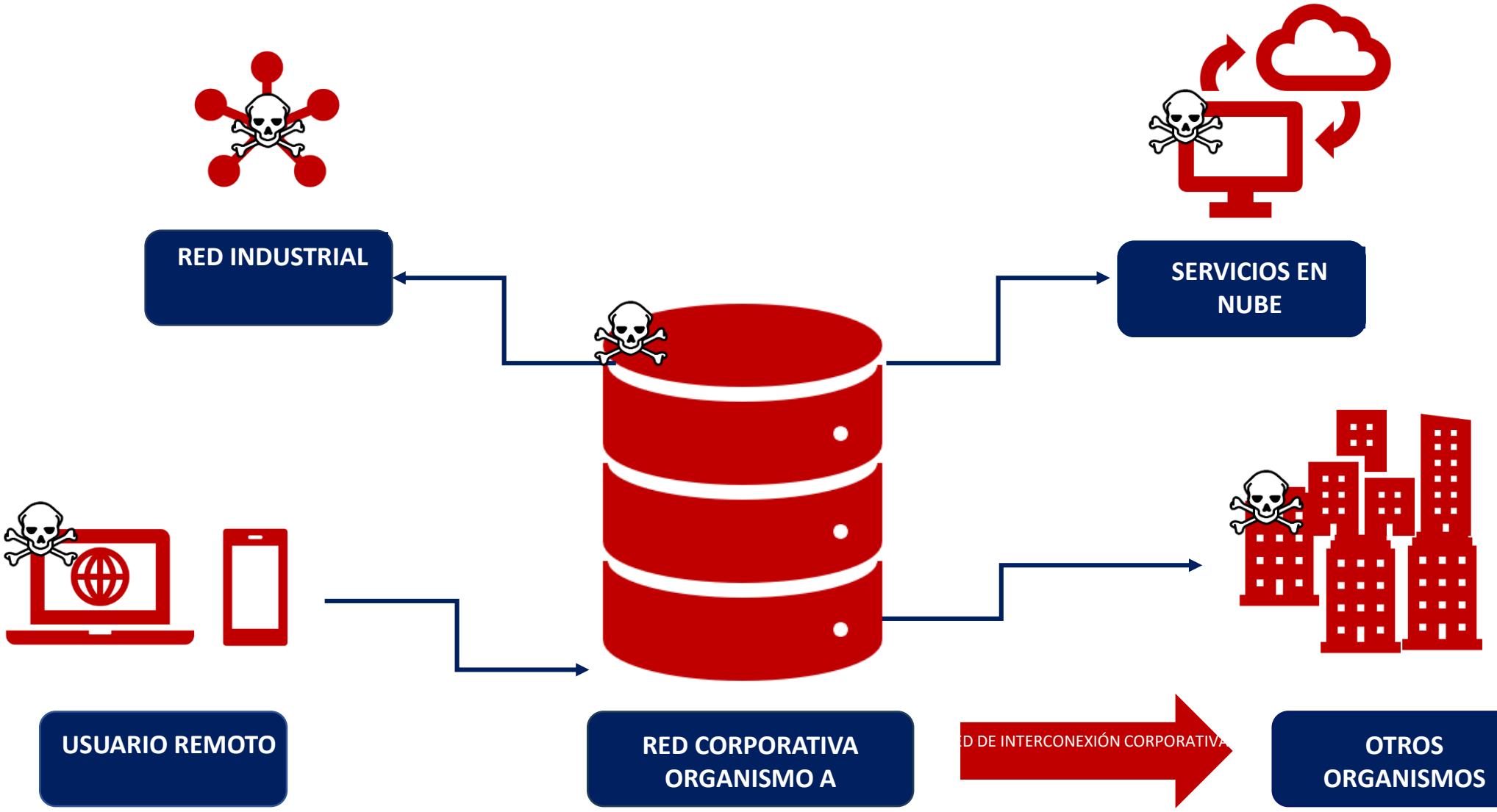
TELEFONÍA MÓVIL

RED INDUSTRIAL

ACCESOS REMOTOS

CCN
centro criptológico nacional

DESCENTRALIZADOS, PERO HIPERCONECTADOS



Incidentes

2022

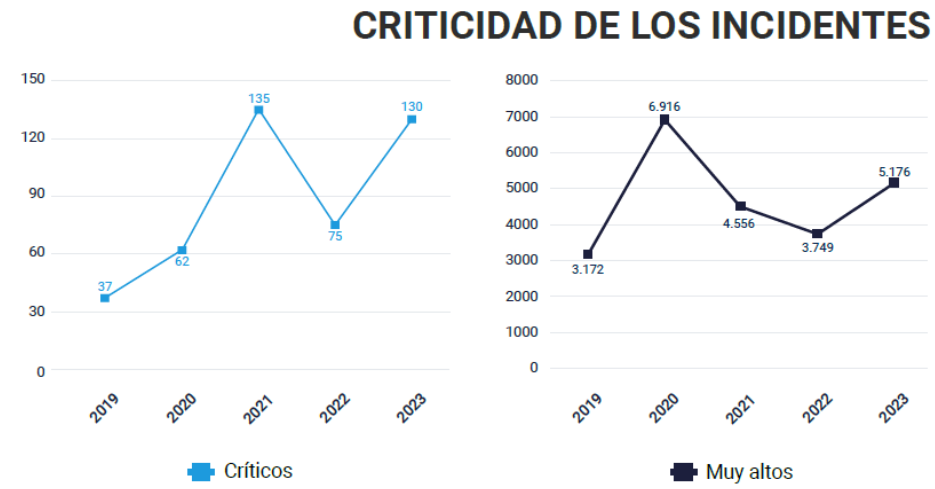
+55k	29%	75
Incidentes gestionados	notificados por organismos	incidentes **críticos**

2023

+105k	52%	+120
Incidentes gestionados	notificados por organismos	incidentes **críticos**

*Datos estimados a diciembre de 2023

¿Estamos viendo todos los incidentes?



+30.000 | INCIDENTES CRÍTICOS Y MUY ALTOS GESTIONADOS DESDE 2007

CCN centro criptológico nacional

¿Contra qué luchamos?

¿Quién nos ataca?

RANSOMWARE

AMENAZAS MÓVILES

ACTORES ESTADOS

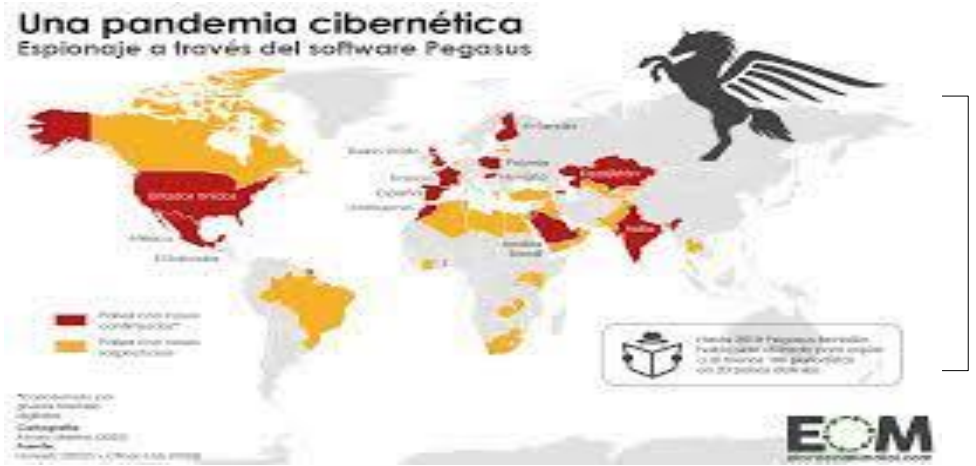
HACKTIVISMO

ACTORES INVITADOS

centro criptológico nacional

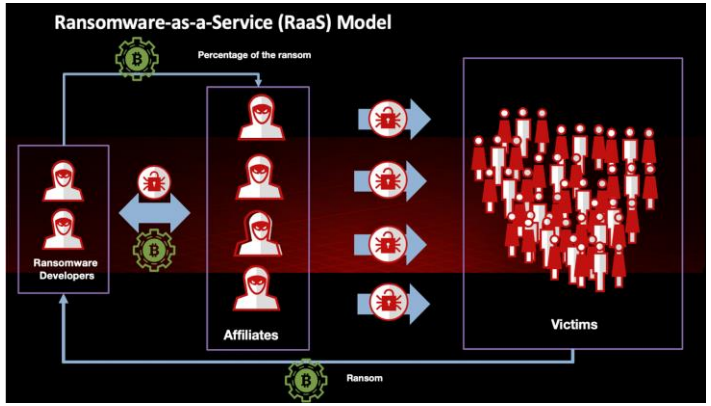
AMENAZAS MÓVILES 2022 / 23

- “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.



CCN
centro criptológico nacional

• CIBERCRIMEN



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

2. COMPRA DE CREDENCIALES LEGÍTIMAS EN MERCADO NEGRO

3. EXPLOTACIÓN DE VULNERABILIDADES EN PERÍMETRO

TELETRABAJO

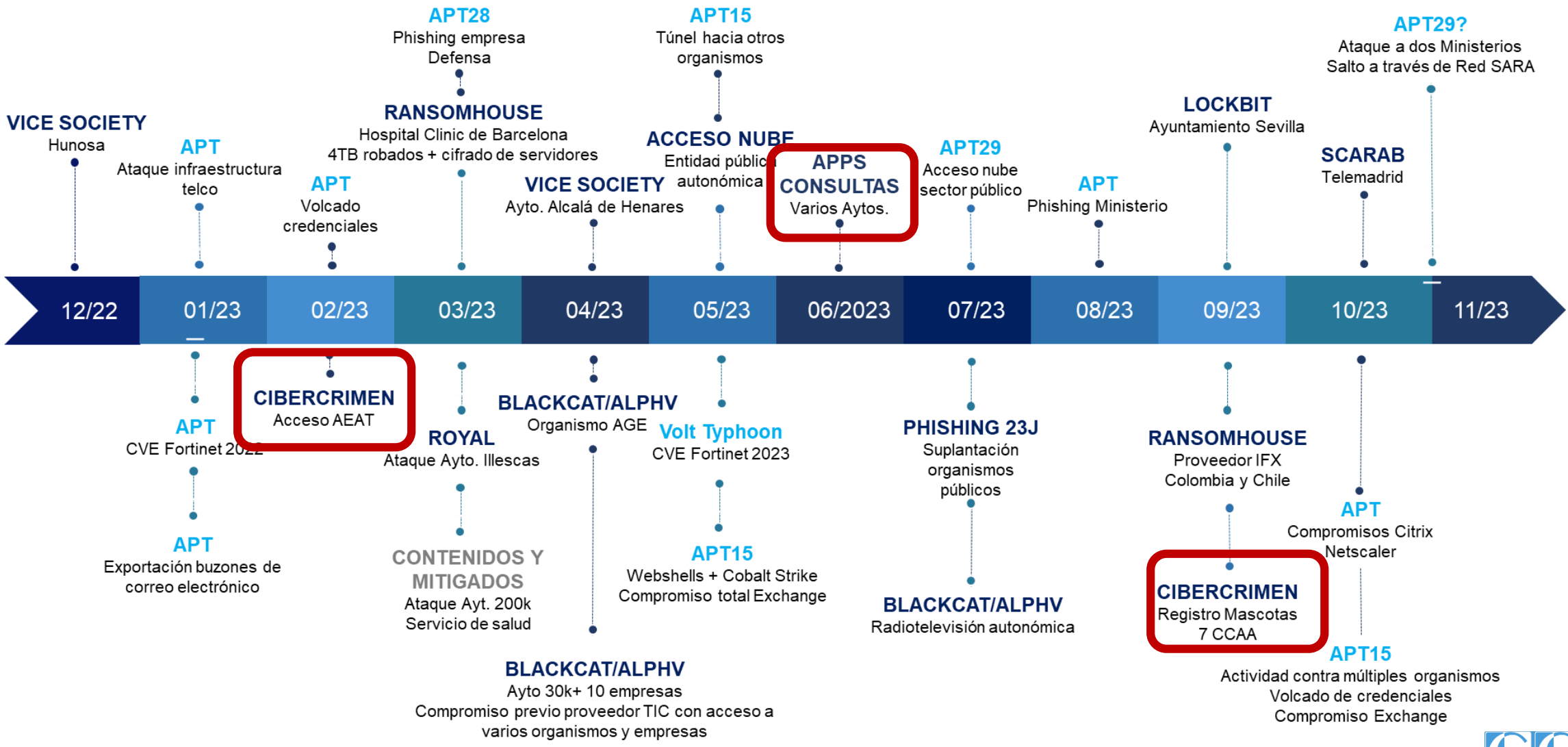
4. ATAQUES DE PHISHING → ESQUEMA TRADICIONAL DE ATAQUE

• CIBERCRIMEN. Lecciones no aprendidas

- **Backups** en línea (o incluso sin backup).
- Accesos remotos (VDI, VPN, RDP) **sin 2FA**
- Redes ‘planas’ –> Necesidad de segmentación.
- Usuarios como administradores locales
- Logs muy limitados. Sin correlación.
- Falta de monitorización en / fuera de horas trabajo (horario habitual del despliegue del código dañino)
- Redes de confianzas (unidades compartidas)
- Ausencia de EDR / microCLAUDIA

CCN centro criptológico nacional

Ciberamenazas 2023

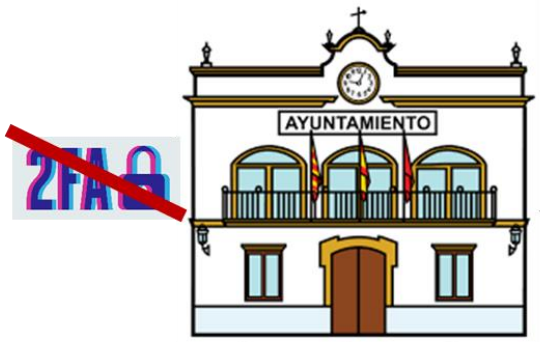


centro criptológico nacional

- **ACTORES INVITADOS**

PROBLEMA RECURRENTE

CCAA



redNEREA
LA RED INTERADMINISTRATIVA DE ANDALUCÍA

Red SARA

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS

Agencia Tributaria

Consejo General del Poder Judicial

EuroCop
Security Systems

DGT

CCN
centro criptológico nacional

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**

- **PREGUNTA 2**

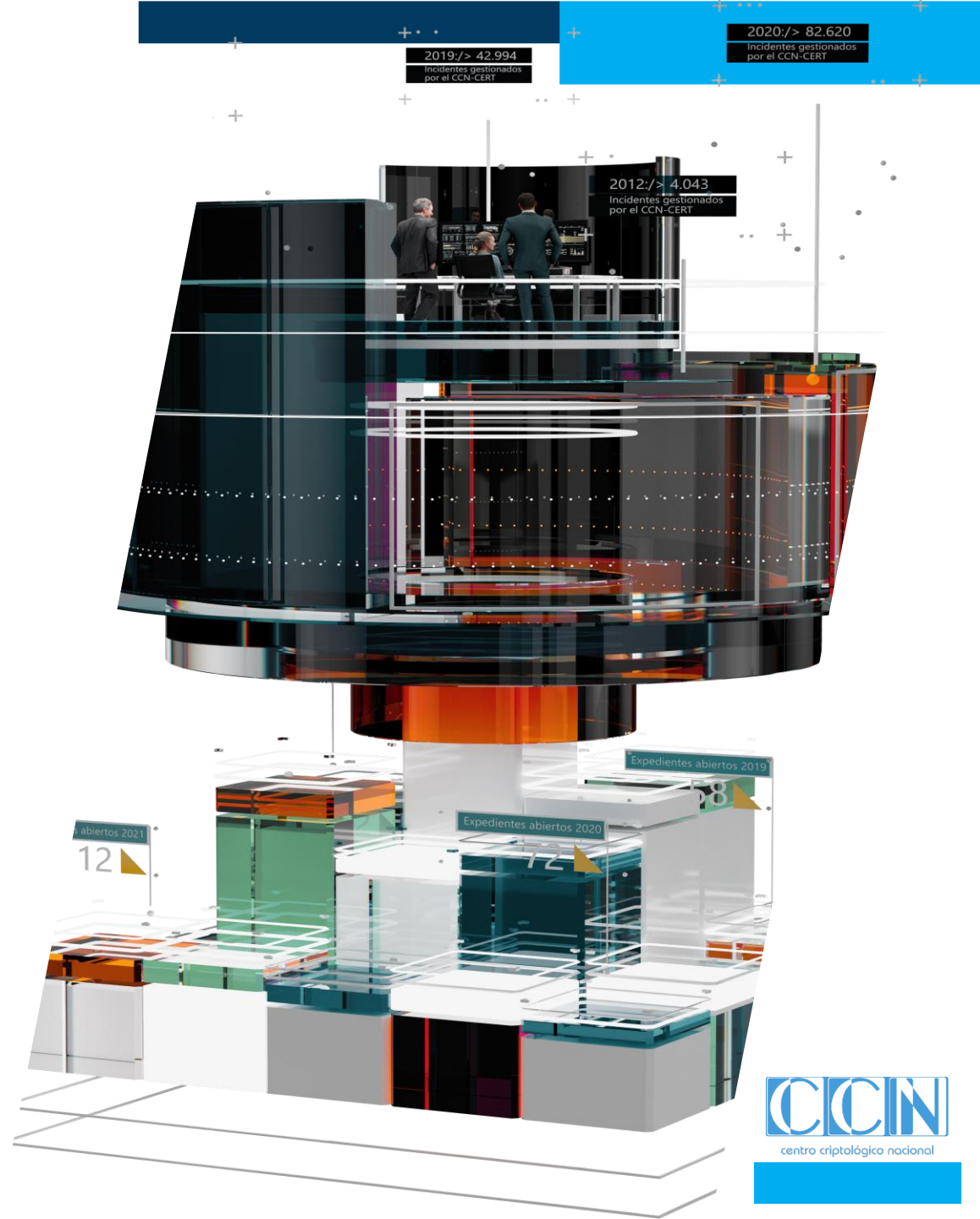
En un contexto de un ciberespacio hostil como el actual y con la imparable transformación digital

¿cómo considera que se ha de enfocar la ciberseguridad a medio y largo plazo?

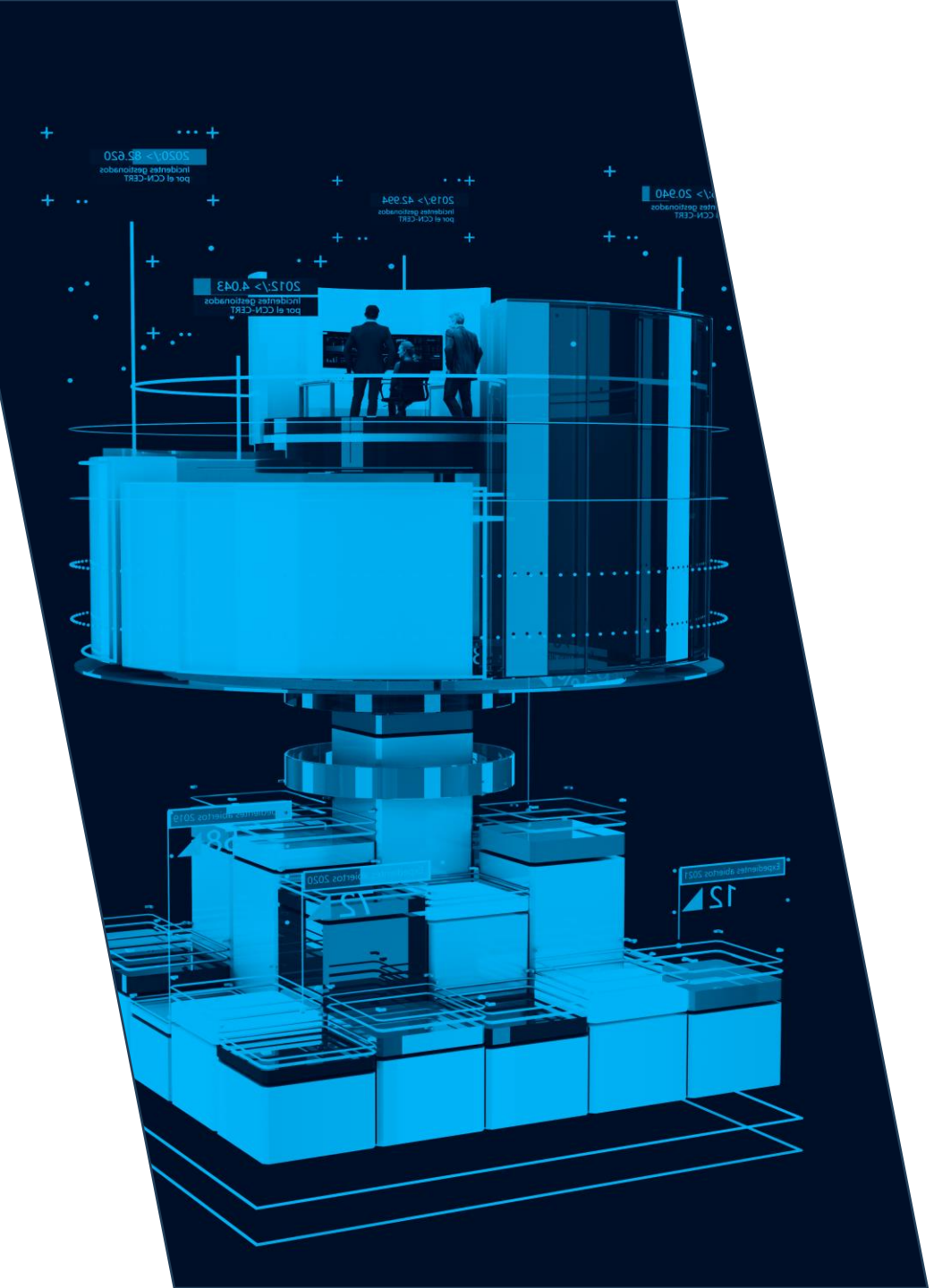
CCN
centro criptológico nacional

- **CAMBIO DE MODELO**

FULL TRUST



CCN
centro criptológico nacional



CAMBIO DE MODELO

ZERO TRUST

+ Vigilancia + Intercambio

CCN
centro criptológico nacional

- # A MEDIO / LARGOPLAZO. *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

AXENCIA PARA A MODERNIZACIÓN TECNOLÓXICA DE GALICIA · fegamp · incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD · CCN-CERT

Deputación DA CORUÑA · DEPUTACIÓN DE LUGO · DEPUTACIÓN OURENSE · DEPUTACIÓN PONTEVEDRA

ciber.gal

CSIRT.gal

- Servicios de Detección 24*7
- Servicios de Auditoria
- Superficie de exposición
- Servicios de cumplimiento ENS
- Servicios AntiDOS

µclaudia

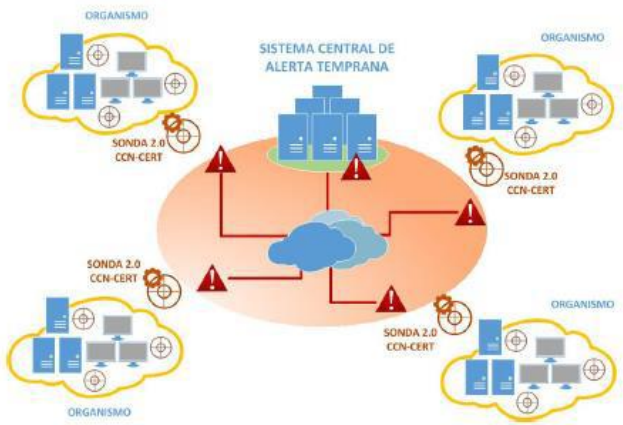
+130	+1.2 M	+900 K equipos	+2.2K organismos
vacunas desarrolladas	alertas generadas	protegidos con microCLAUDIA	dados de alta

VACUNAS ESPECÍFICAS

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

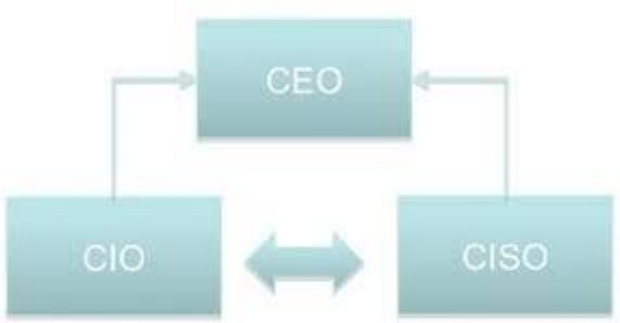
sat-inet

+400 sondas



CCN centro criptológico nacional

2. Empoderar al CISO. Certificación ENS



RESPONSABLE DE SEGURIDAD

+290
Organismos certificados

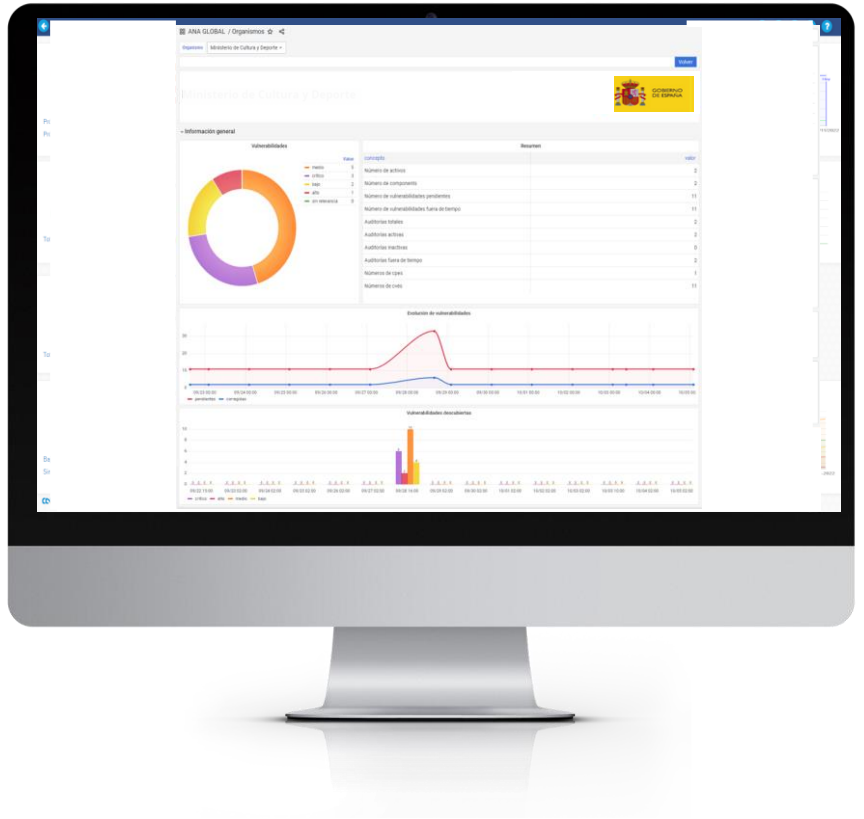
+730
Empresas certificadas

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

CCN
centro criptológico nacional

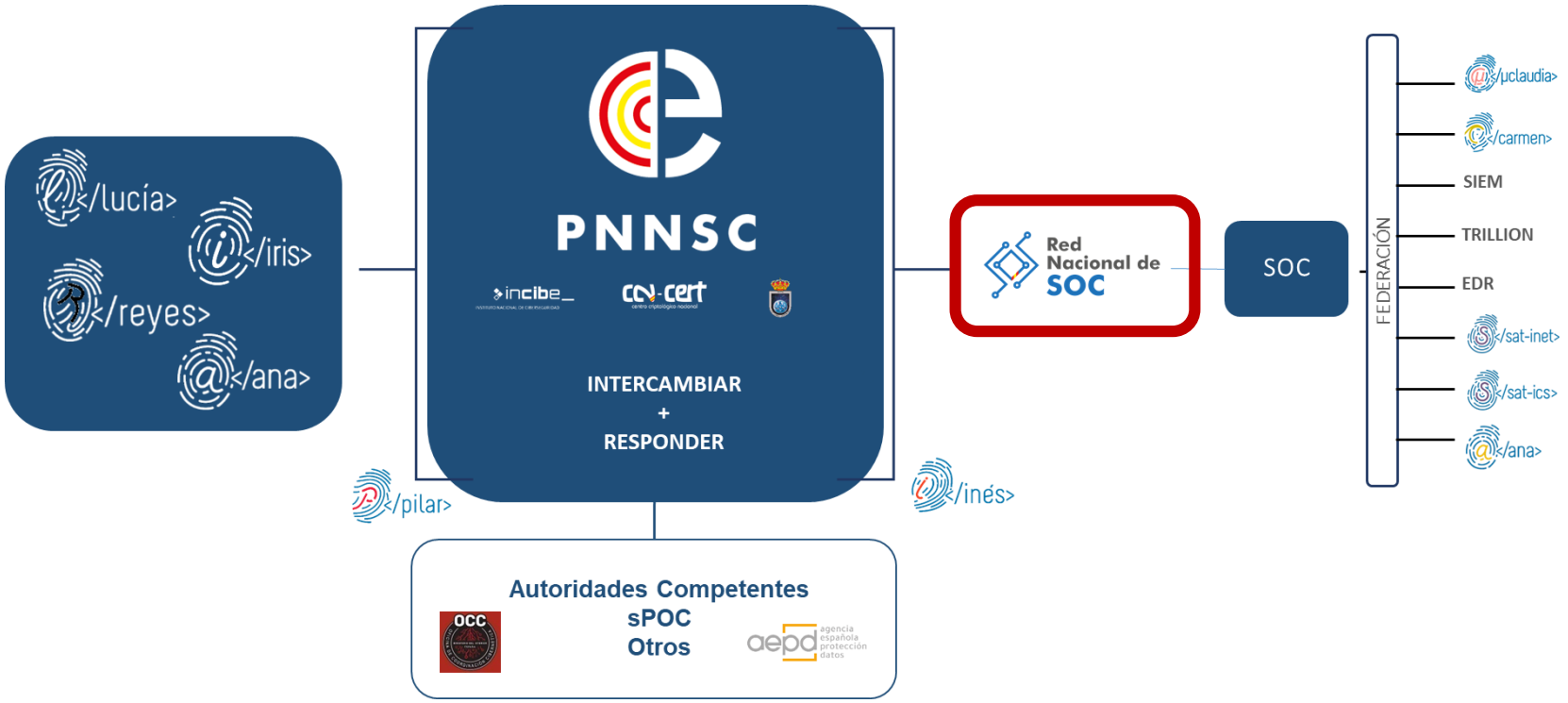
3. Reducir superficie de exposición

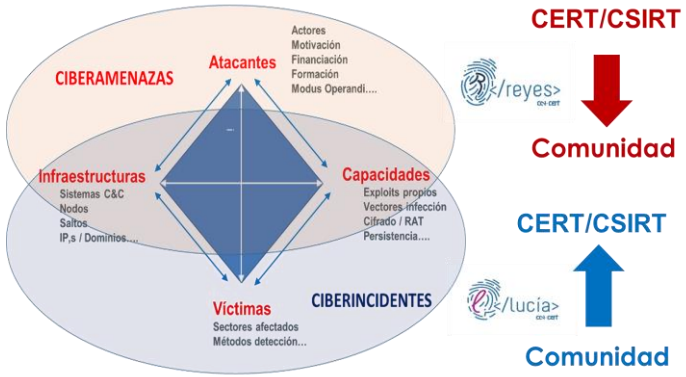
¿Auditoria para cumplimiento normativo o como mejora continua?



Conocer la superficie de exposición y reducirla

4. Compartir antes que responder





Intercambiar TODO y por máquinas, no humanos.

IoC, IoA y buenas prácticas ¡¡¡¡¡

5. Salir a Ganar. Medidas Ciberdefensa Activa

[MCDA_1]

DNS ADMINISTRACIÓN

[MCDA_2]

CAPACIDAD CAZA AMENAZA

2.1IDENTIFICACIÓN Y ELIMINACIÓN DE C2

2.2 DETECCIÓN DE ATAQUES BASADO ANOMALÍAS

[MCDA_3]

SUPERFICIE DE EXPOSICIÓN AUTOMÁTICA (ANA-ELSA)

[MCDA_4]

PREVENCION y CUMPLIMIENTO

INES / ANGELES / µCENS

[MCDA_5]

DETECCIÓN AVANZADA EN MÓVILES

[MCDA_6]

COORDINACION 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

E-mails

ccn@cni.es

info@ccn-cert.cni.es

sat@ccn-cert.cni.es

microclaudia@ccn-cert.cni.es

ens@ccn-cert.cni.es

organismo.certificacion@cni.es

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

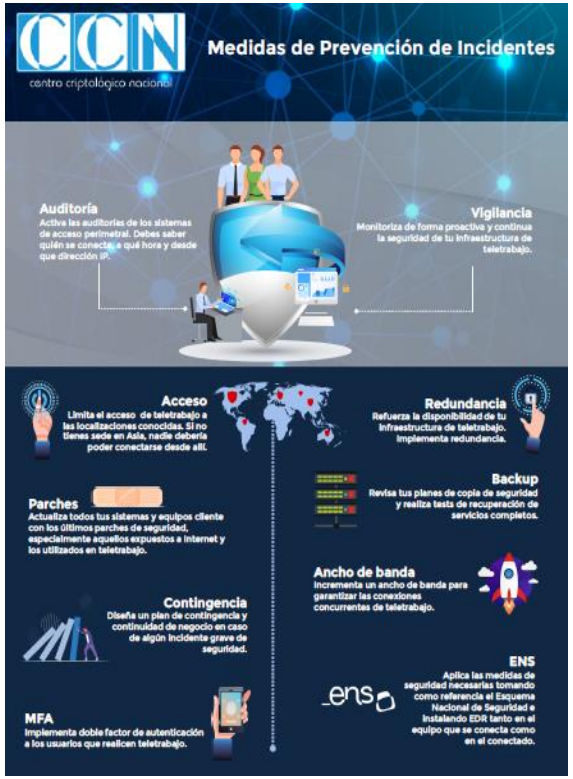
Contribuir a la mejora de la **ciberseguridad española**, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente al **Sector Público** a afrontar de forma activa las nuevas ciberamenazas.

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.

Medidas Prevenir ciberincidentes



CSIRT.es

Red Nacional de SOC

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**.

CCN
centro criptológico nacional