Ciberseguridad: Estrategia Nacional

Javier Candau
Centro Criptológico Nacional
ccn@cni.es

centro criptológico nacional

TLP:CLEAR

ENERGÍA

Iberdrola sufre un ciberataque que deja expuestos los datos de 850.000 clientes

05/24

Endesa alerta sobre posible filtración de datos de clientes tras sufrir una brecha de seguridad

El robo masivo de datos del Banco Santander que afecta a millones de clientes en Chile, Uruguay y España, y a todos sus empleados

SECTORES ESTRATÉGICOS

06/24

Filtración de datos en la empresa Energía XXI, la comercializadora de referencia de Endesa

Filtran datos personales de pacientes, sanitarios y colaboradores del Clínic tras el pirateo informático

OBSERVATORIO DE LA ENERGÍA

TotalEnergies sufre un ciberataque que afecta a 210.715 clientes en España

07/24

La compañía se suma a Iberdrola, Telefónica y Santander, que también han sido víctimas de ciberdelincuentes en los últimos meses.

Ciberseguridad

Un total de 2,3 GB de datos de Telefónica han quedado expuestos debido a una filtración masiva

• Telefónica le ha confirmado al medio Bleeping Computer que ha sufrido un ciberataque masivo que ha filtrado más de 2 GB de datos, pero que estos no son datos de

01/25

ATAQUES INFORMÁTICOS >

Repsol sufre un ciberataque a su base de datos de clientes de electricidad y gas en España

09/24

Filtrados los datos de 2 millones de clientes de Asisa

Unos ciberdelincuentes están vendiendo al menos 2 millones de datos de clientes de Asisa que habrían podido obtener a partir de una base de datos de esta compañía.

CCN centro criptológico nacional

TLP:CLEAR

INCIDENTES EN EL SECTOR MARÍTIMO - RANSOMWARE

JUNIO 2017

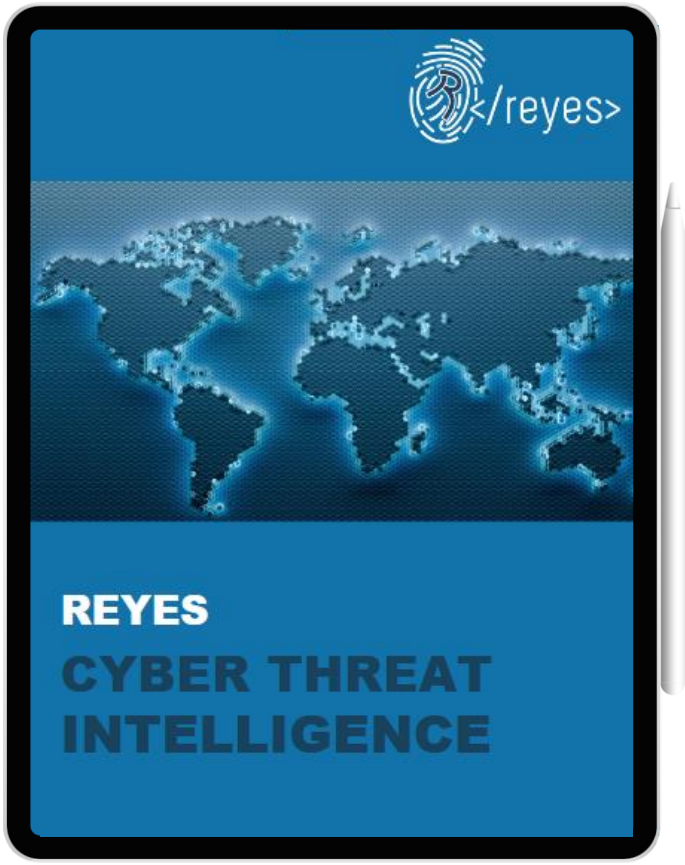
NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million

NOVIEMBRE 2023

Australia Cyberattack Leaves 30,000 Containers Stuck at Ports

- Operations resuming at Melbourne, S
- Normal service won't return for a wee

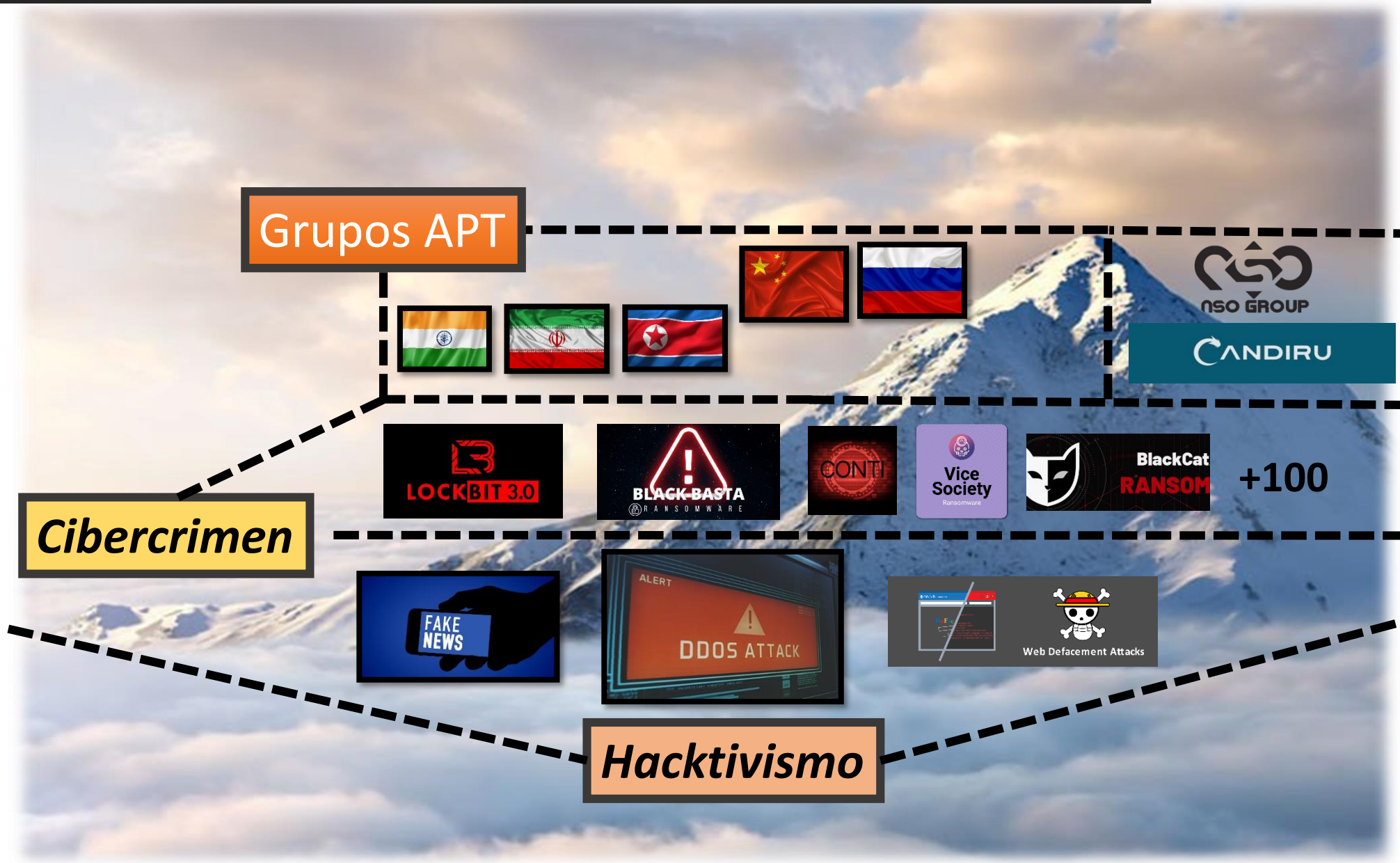
¿CONTRA QUÉ LUCHAMOS?



CCN-CERT
centro criptológico nacional

CCN
centro criptológico nacional

¿CONTRA QUÉ LUCHAMOS?



Incidentes'24

175k Incidentes gestionados

297 incidentes **críticos**

Enero

APT Turla
Accesos M365

Cibercrimen
Datos DGT

Lockbit 3.0
Ayto. Calviá

Febrero

APT
Explotación CVE Ivanti

APT28
Phishing

APT Turla
Evasión 2FA

Marzo

Cibercrimen
Filtración datos AAPP

Lockbit 3.0
Ayto. Torre Pacheco

APT Turla
Empresa privada ingeniería

Abril

APT Turla
Accesos fallidos + Kazuar

Cibercrimen
Ataque app CCAA

APT desconocido
Accesos correo electrónico

Cibercrimen
Ataque empresa pública

Ransomware SEXi
Casa Árabe

Mayo

APT28 y Turla
Accesos M365

Cibercrimen
Venta de datos
Universidad Complutense

APT redes ORB
Escaneos universidades

Junio

APT15
Nodo en España

Cibercrimen
Acceso Diputación

APT Earth Stries
Empresa privada ingeniería

APT Turla
Infección servidor Exchange

APT15?
Compromiso entorno virtualización

APT
Explotación CVE Check Point

Julio

Cibercrimen
Robo datos app Organismo

APT redes ORB
Escaneos empresas

APT
Ataque *password spraying*

APT
Volcado credenciales

Cibercrimen
¿Leak portal CCN-CERT?

Agosto

APT redes ORB
Escaneos empresas

Cibercrimen
Venta credenciales AGE

Cibercrimen
Filtración RFEA

APT28 y STORM-1957
Accesos M365

APT desconocido
Acceso VPN corporativa + volcado credenciales

Septiembre

APT redes ORB
Compromiso AGE

Cibercrimen
Explotación app Comunidad Autónoma

Cibercrimen
Primera etapa *ransomware*

Octubre

APT
Empresa privada

Cibercrimen
Venta credenciales AGE

Cibercrimen
Filtración RFEA

Noviembre

APT redes ORB
Compromiso AGE

Cibercrimen
Explotación app Comunidad Autónoma

Cibercrimen
Accesos datos Diputación

ccn-cert
centro criptológico nacional

COVID – 2020 UN ANTES Y DESPUÉS

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

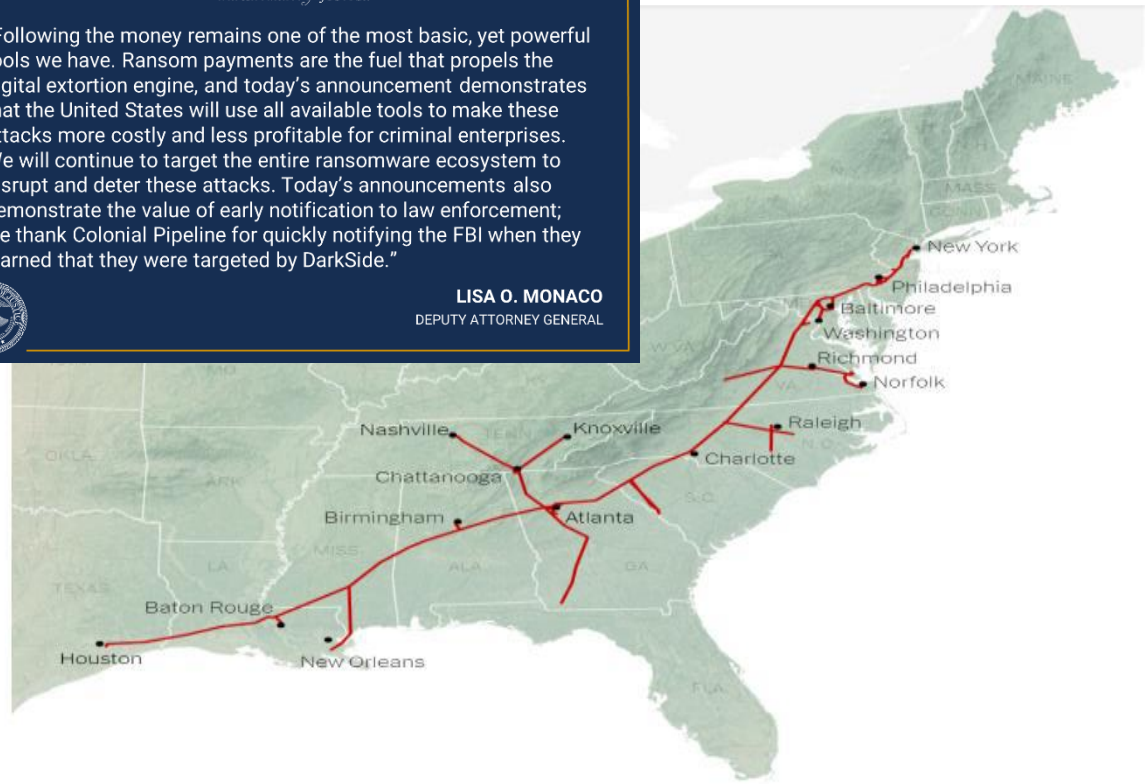
4. ATAQUES DE PHISHING → ESQUEMA TRADICIONAL DE ATAQUE

Colonial. Distribución Hidrocarburos

THE UNITED STATES DEPARTMENT of JUSTICE

"Following the money remains one of the most basic, yet powerful tools we have. Ransom payments are the fuel that propels the digital extortion engine, and today's announcement demonstrates that the United States will use all available tools to make these attacks more costly and less profitable for criminal enterprises. We will continue to target the entire ransomware ecosystem to disrupt and deter these attacks. Today's announcements also demonstrate the value of early notification to law enforcement; we thank Colonial Pipeline for quickly notifying the FBI when they learned that they were targeted by DarkSide."

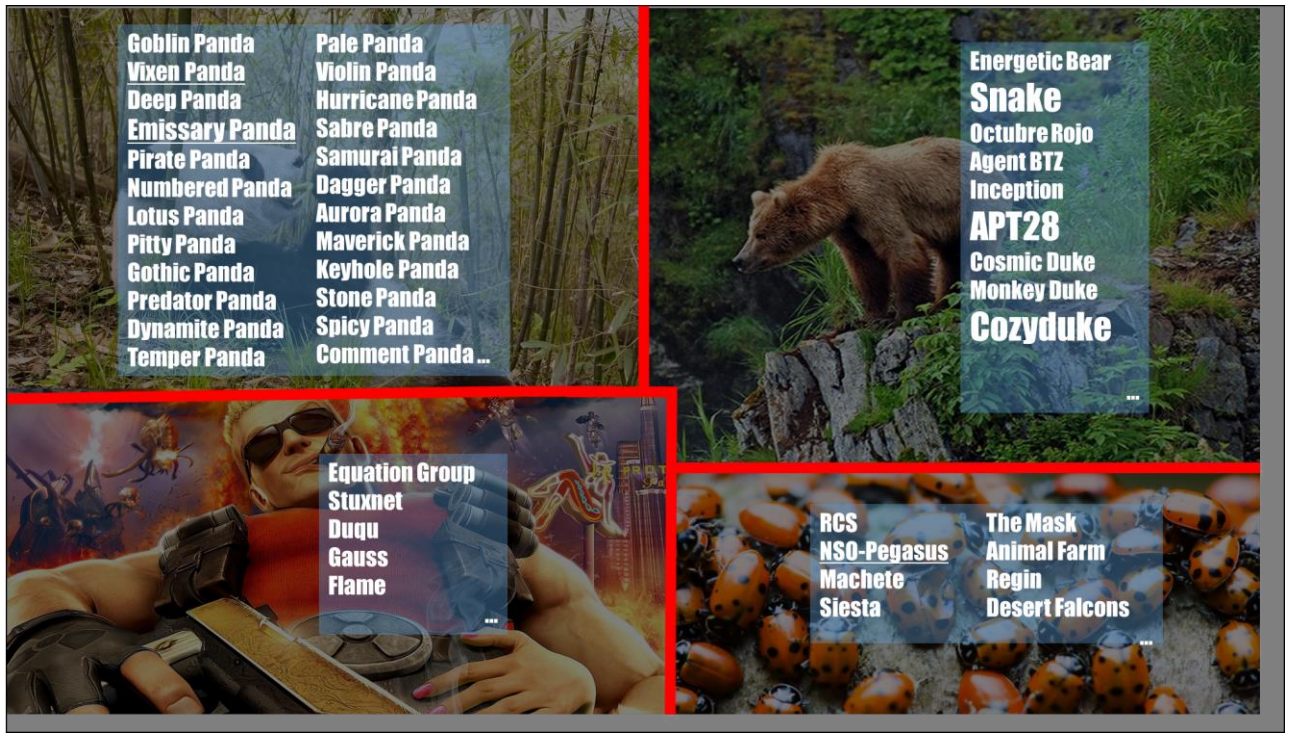
LISA O. MONACO
DEPUTY ATTORNEY GENERAL

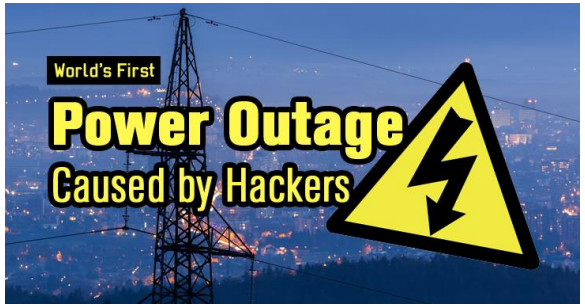


- Inicio del incidente: **07.05.2021**
- Fin del incidente: **14.05.2021**
- **Impacto:**
  - Interrupción de operación en oleoducto de 8.000 km. 45% combustible de la Costa Este
  - Temor a desabastecimiento en 50M personas
  - Pago rescate: 5.000.000 $
- **Grupo de Ataque:**
  - DARKSIDE

- USA vincula a cibercriminales ubicados en Rusia e insta a acciones por parte del gobierno Ruso
- **12.05.2021** Presidente BIDEN firma la orden ejecutiva **PARA MEJORA DE LA CIBERSEGURIDAD DE LA NACIÓN**
  - Plan de mejora en 100 días

ACTORES ESTADOS





Ciberespionaje ---------- Cibersabotaje

CCN centro criptológico nacional

https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-

90%

Maersk CEO now sees the good side of the incident

"It was an important wake-up call," he said. "We were basically average when it comes to cyber-security, like many companies. And this was a wake-up call to become not just good —we actually have a plan to come in a situation where our ability to manage cyber-security becomes a competitive advantage."

In the subsequent discussions, Snabe also urged fellow Davos World Economic Forum participants to focus on securing cyberspace.

A video of Snabe's comments regarding Maersk's NotPetya recovery efforts, and more, is embedded below. The discussion is right at the beginning, following the 02:20 mark.

onPetya

ución de un

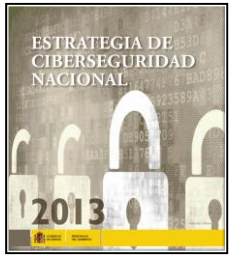
pueden ser

scate sólo se

posible).

CCN
centro criptológico nacional

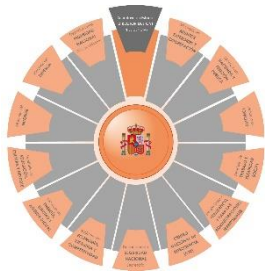
Estrategia Seguridad Nacional



CCN
centro criptológico nacional

HISTORIA ENCS

02.2014



10.2014

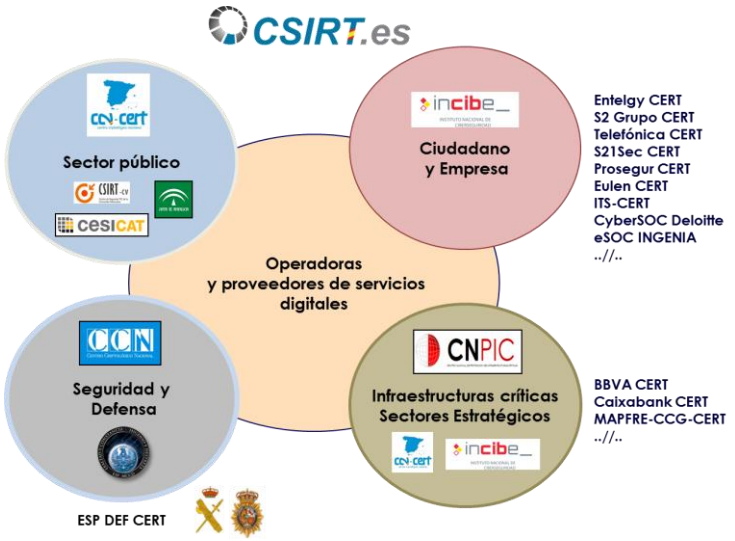
Plan Nacional de Ciberseguridad

07.2015

9 Planes derivados

03.2020

02.2022

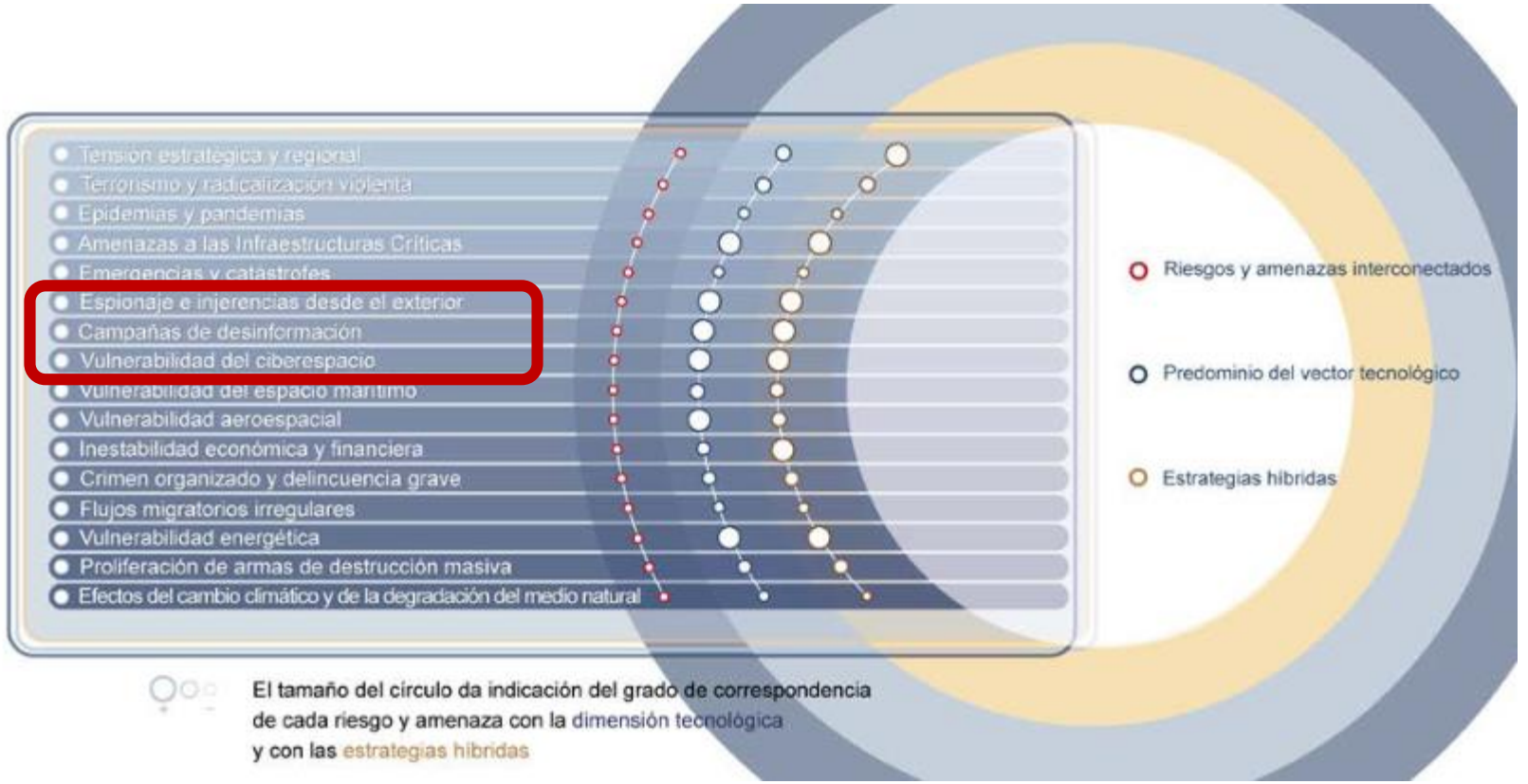


COMISIÓN PERMANENTE

Plan NACIONAL

ESTRATEGIA DE SEGURIDAD NACIONAL 2021

UN PROYECTO COMPARTIDO



En el ciberespacio:

L.A. 17. Avanzar en la integración del modelo de gobernanza de la ciberseguridad en el marco del Sistema de Seguridad Nacional.

CCN centro criptológico nacional

Estrategia Nacional de Ciberseguridad

- Gobernanza de ciberseguridad
- Impacto NIS 1.0 / NIS 2.0
- Transversal a otras estrategias
- Objetivos y líneas de acción

ENCS 2019. LÍNEAS DE ACCIÓN

- LA 1 ***Reforzar las capacidades ante las amenazas provenientes del ciberespacio.***
- LA 2 ***Garantizar la seguridad y resiliencia de los activos estratégicos para España.***

- LA 3 ***Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.***
- LA 4 ***Impulsar la ciberseguridad de ciudadanos y empresas***
- LA 5 ***Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital.***
- LA 6 ***Contribuir a la seguridad del ciberespacio en el ámbito internacional, promoviendo un ciberespacio abierto, plural, seguro y confiable, en apoyo de los intereses nacionales.***
- LA 7 ***Desarrollar una cultura de ciberseguridad.***

CCN
centro criptológico nacional

NIS 2.0. Gobernanza ciberseguridad

+ 3 CSIRT de referencia

Centro Nacional de Ciberseguridad

Autoridad de Control

Punto Contacto Sectorial

MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

CCN Centro Criptológico Nacional

OCC Oficina de Coordinación de Ciberseguridad

GOBIERNO DE ESPAÑA MINISTERIO DE TRANSPORTES, MOVILIDAD Y AGENDA URBANA

SECRETARÍA DE ESTADO DE TRANSPORTES, MOVILIDAD Y AGENDA URBANA

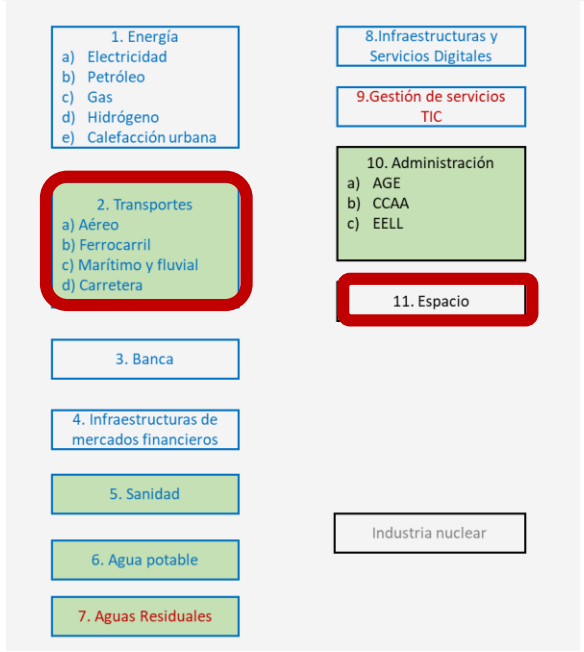
AEE Agencia Espacial Española

CCN centro criptológico nacional

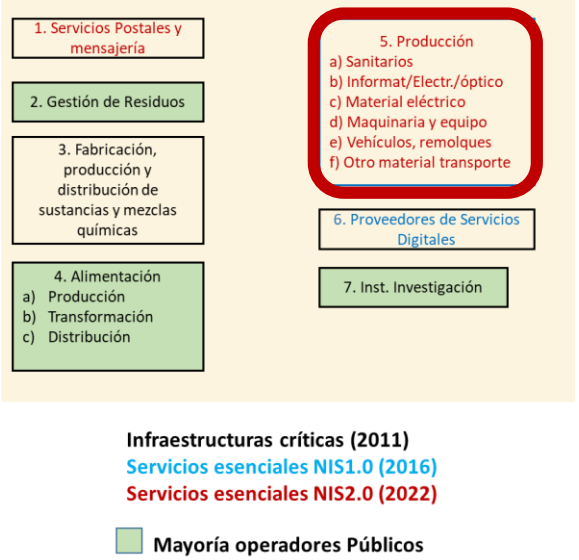
SUJETO A CAMBIOS

RETOS NIS 2.0

SECTORES ALTA CRITICIDAD



SECTORES CRITICOS



Infraestructuras críticas (2011)
Servicios esenciales NIS1.0 (2016)
Servicios esenciales NIS2.0 (2022)

Mayoría operadores Públicos

+ 50 EI
+250 EE

empleados

+8k EI
+3k EE

empresas

1
2
3
4
5

LISTADO EE/EI

Auto registro / validación

MEDIDAS DE CIBERSEGURIDAD

Homogéneas que permitan conocer el nivel de ciberseguridad. **Actos de ejecución**

DEMOSTRACIÓN CUMPLIMIENTO

Certificación / Declaración de conformidad

NOTIFICACIÓN INCIDENTES. PNNSC

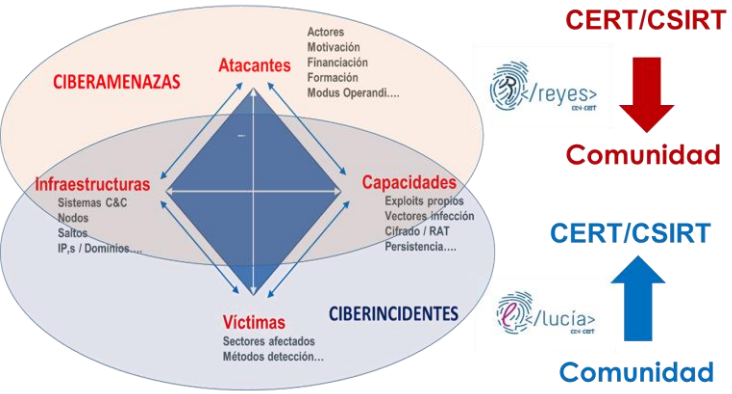
Conocer todos los incidentes
Notificar vulnerabilidades

GESTIÓN DE CRISIS

Reaccionar ante los incidentes críticos
Centro Nacional de Ciberseguridad + CCN-CERT
Red Nacional de SOC,s

CCN
centro criptológico nacional

1. OBLIGACIONES. AUTOREGISTRO Y VALIDACIÓN



CERT/CSIRT

</reyes>

Comunidad

CERT/CSIRT

</lucía>

Comunidad

PNNSC

INTERCAMBIAR
+
RESPONDER

SSO
Single Sign On

https://rns.ccn-cert.cni.es/

Red Nacional de SOC

Modulo de Auto registro

</amparo>

</inés>

</pilar>

CNPIC Autoridad Nacional
Autoridades Control
Puntos Control Sectoriales
aepd agencia española protección datos

https://plataformanacionalciber.gob.es

CCN centro criptológico nacional

RNS – INTERCAMBIO ACTIVO

753 FIRST

111 Nations

CSIRT.es **(70)**

2023

Red Nacional de SOC **(249)**

ENSOC EUROPEAN NETWORK OF SOC

EVOLUCIÓN EVENTOS COMPARTIDOS

+300 eventos/día

CCN centro criptológico nacional

AGENCIA DE CIBERSEGURIDAD, ¿BALA DE PLATA?

8131
Ayuntamientos

52
Diputaciones y cabildos

1101
Mancomunidades y comarcas

+ 5500
Empresas públicas, fundaciones…

MEJOR MÁS AGENCIAS

- Comunidades con Agencia
- Comunidades con proyecto de Agencia
- Comunidades con capacidad de SOC / CERT / CSIRT

CCN centro criptológico nacional

2. OBLIGACIONES. MEDIDAS CIBERSEGURIDAD

Medidas generales de la Directiva NIS2	Medidas de seguridad del ENS relacionadas
Art. 21 a) las políticas de seguridad de los sistemas de información y análisis de riesgos.	**Art. 12.** Política de seguridad y requisitos mínimos de seguridad **[org.1]** Política de Seguridad **[org.2]** Normativa de Seguridad **[op.pl.1]** Análisis de riesgos
Art. 21 b) La gestión de incidentes.	**Art. 25.** Incidentes de seguridad. **[op.exp.7]** Gestión de incidentes
Art 21 c) La continuidad de las actividades, como la gestión de copias de seguridad y la recuperación en caso de catástrofe, y la gestión de crisis.	**Art. 26.** Continuidad de la actividad. **[op.cont.4]** Medios alternativos **[mp.info.6]** Copias de seguridad **[op.cont.1]** Análisis de impacto (BIA) **[op.con.2]** Plan de Continuidad **[op.cont.3]** Pruebas periódicas
Art. 21 d) La Seguridad de la cadena de suministro, incluidos los aspectos de seguridad relativos a las relaciones entre cada entidad y sus proveedores o prestadores de servicios directos.	**[op.ext.3]** Protección de la cadena de suministro **[op.ext.1]** Contratación y acuerdos de nivel de servicio **[op.ext.2]** Gestión diaria **[op.ext.4]** Interconexión de sistemas
Art. 21 e) La seguridad en la adquisición, y el desarrollo y mantenimiento de sistemas de redes y de información, incluida la gestión y divulgación de las vulnerabilidades.	**Art. 19.** Adquisición de productos de seguridad y contratación de servicios de seguridad. **[op.pl.3]** Adquisición de nuevos componentes **[op.pl.5]** Componentes certificados **[mp.sw.1]** Desarrollo de aplicaciones **[mp.sw.2]** Aceptación y puesta en servicio **[op.exp.4]** Mantenimiento y actualizaciones de seguridad **[op.mon.3]** Vigilancia

- Las **entidades esenciales**, con independencia de la categoría del sistema, deberán ser **certificadas** conforme cumplen los requisitos del ENS **por una entidad de certificación(EC) acreditada por ENAC** o por un **Órgano de Auditoría Técnica (OAT)** del sector público reconocido por el CCN.

- Las **entidades importantes**, podrán optar por una **Declaración de Conformidad obtenida mediante la solución INES del Portal de Gobernanza del ENS**, aunque se recomienda una auditoría externa.

- Hoja de ruta a partir del PCE-RFS, solución **automatizada en INES del Portal de Gobernanza del ENS**, con obtención del correspondiente Certificado de Conformidad en base al PCE-RFS. **Durante dos (2) años** aplicar mejora continua para poder alcanzar la categoría adecuada, requiriéndose **acta o documento formal de asunción del compromiso de mejora y del riesgo asumido.**

3. OBLIGACIONES. DEMOSTRACIÓN CUMPLIMIENTO

PCE-RFS: PERFIL DE CUMPLIMIENTO ESPECÍFICO DE REQUISITOS FUNDAMENTALES DE SEGURIDAD.

Marco Organizativo (4):
[org.1] Política de seguridad
[org.2] Normativa de seguridad
[org.3] Procedimientos de seguridad
[org.4] Proceso de autorización

Marco Operacional (14):
[op.pl] Planificación
[op.pl.1] Análisis de riesgos
[op.pl.3] Adquisición de nuevos componentes
[op.acc] Control de acceso
[op.acc.1] Identificación
[op.acc.2] Requisitos de acceso
[op.acc.4] Proceso de gestión de derechos de acceso
[op.acc.5] Mecanismos de autenticación (usuarios externos)
[op.acc.6] Mecanismo de autenticación (usuarios de la organización)
[op.exp] Explotación
[op.exp.1] Inventario de activos
[op.exp.2] Configuración de seguridad
[op.exp.4] Mantenimiento y actualizaciones de seguridad
[op.exp.6] Protección frente a código dañino
[op.exp.7] Gestión de incidentes
[op.exp.8] Registro de la actividad
[op.exp.10] Protección de claves criptográficas
[op.mon] Monitorización del sistema
[op.mon.2] Sistema de métricas

PCE-RFS
38

Medidas de Protección (19):
[mp.if] Protección de las instalaciones e infraestructuras
[mp.if.1] Áreas separadas y control de acceso
[mp.per] Gestión del personal
[mp.per.2] Deberes y obligaciones
[mp.per.3] Concienciación
[mp.per.4] Formación
[mp.eq] Protección de los equipos
[mp.eq.1] Puesto de trabajo despejado
[mp.eq.2] Bloqueo de puesto de trabajo
[mp.eq.3] Protección de dispositivos portátiles
[mp.eq.4] Otros dispositivos conectados a la red.
[mp.com] Protección de las comunicaciones
[mp.com.1] Perímetro seguro
[mp.com.2] Protección de la confidencialidad
[mp.si] Protección de los soportes de información
[mp.si.3] Custodia
[mp.si.4] Transporte
[mp.si.5] Borrado y destrucción
[mp.info] Protección de la información
[mp.info.1] Datos de carácter personal
[mp.info.3] Firma electrónica
[mp.info.5] Limpieza de documentos
[mp.info.6] Copias de seguridad (backup)
[mp.s] Protección de los servicios
[mp.si.1] Protección del correo electrónico
[mp.s.3] Protección de la navegación web

* En rojo: Medidas nuevas respecto al antiguo PCE-RES

¿DISPONE DE CERTIFICADO ENS?

ens Esquema Nacional de Seguridad

SÍ
- ALTA
- MEDIA | BÁSICA

✓ CUMPLE MEDIDAS DE LA NIS2

NO

Entidades **incluidas** en el ámbito del **Reglamento de Ejecución** (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024

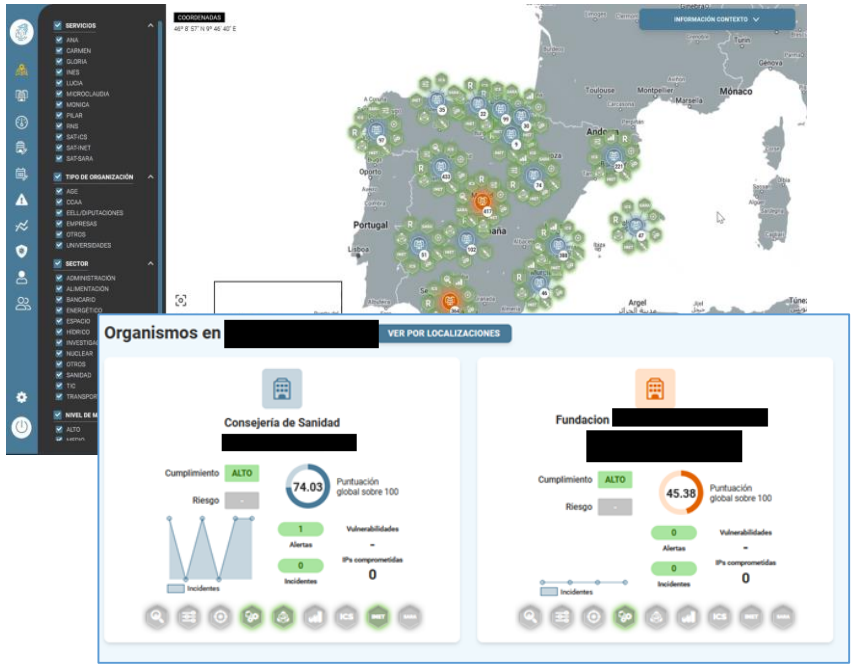
CCN-STIC 892 PCE-Aplicación NIS2

Entidades **no incluidas** en el ámbito del **Reglamento de Ejecución** (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024

ADECUACIÓN ENS / PCE

CCN centro criptológico nacional

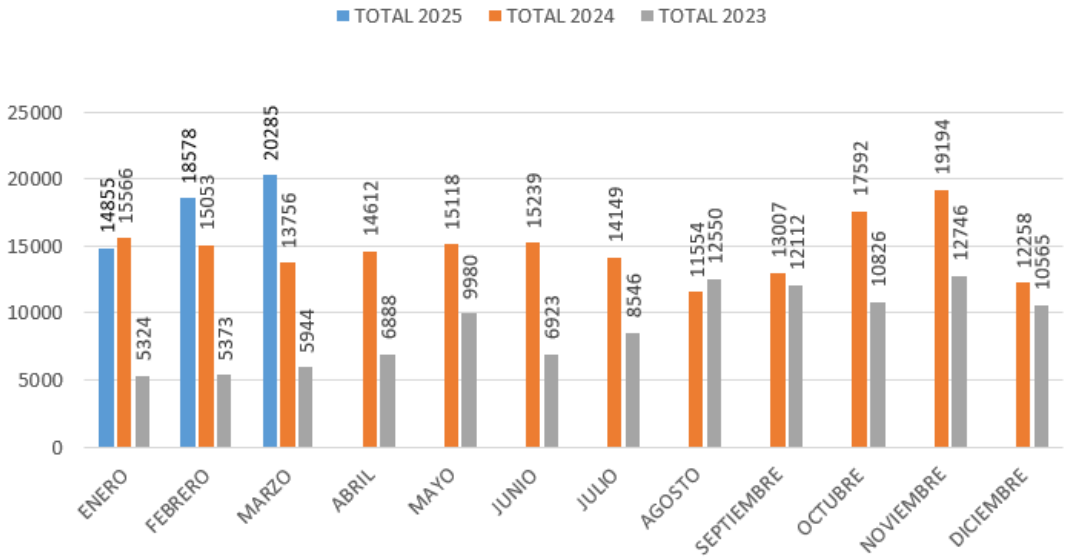
4. OBLIGACIONES. NOTIFICACIÓN CIBERINCIDENTES.



4691

ENTIDADES EN EL SISTEMA

+177.000 incidentes



Acumulado Anual

2025: 53.718

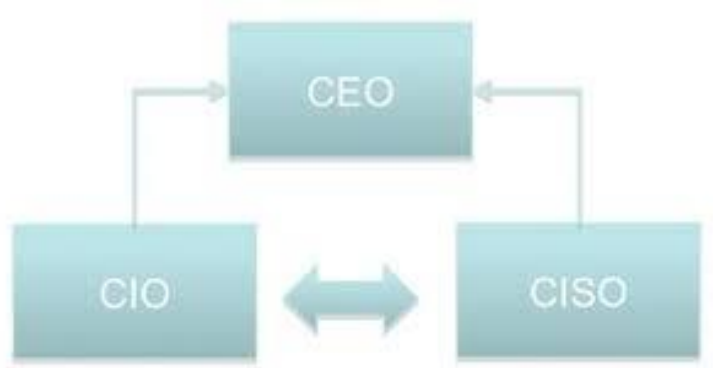
2024: 177.098

2023: 107.777

CCN centro criptológico nacional

Obligaciones de la dirección

Art.	Obligación
30	**Notificación voluntaria de información pertinente**
	▪ Las entidades esenciales e importantes en el caso de incidentes, ciberamenazas y cuasi-incidentes; u otras entidades, independientemente de si están o no comprendidas en el ámbito de aplicación de la presente Directiva, en el caso de incidentes, ciberamenazas o cuasiincidentes significativos, **podrán presentar notificaciones de forma voluntaria** a los CSIRT o a las autoridades competentes.
32 33	**Medidas de supervisión y ejecución relativas a entidades esenciales / importantes** (responsabilidad de los órganos de dirección)
	▪ **Cualquier persona física** responsable de una entidad esencial o importante, o que actúe como representante de ella con facultades para representarla, autoridad para tomar decisiones en su nombre o autoridad para ejercer control sobre ella, que **será quien tendrá las competencias para velar por que se cumpla** la presente Directiva, y será considerada **responsable por el incumplimiento** de su deber de garantizar el cumplimiento de la Directiva.
20	**Gobernanza (Órganos de Dirección)**
	▪ Aprobar las medidas para la gestión de riesgos de ciberseguridad. ▪ Supervisar su puesta en práctica. ▪ Responder por el incumplimiento. ▪ Asistencia a formaciones de los miembros de los órganos de dirección y fomentar formaciones periódicas similares a los empleados para adquirir conocimientos y destrezas suficientes que les permitan detectar riesgos y evaluar las prácticas de gestión de riesgos de ciberseguridad y su repercusión en los servicios proporcionados por la entidad.



Acciones Urgentes:

- **Empoderar al CISO**
- **Certificación ENS. Aceptación de la hoja de ruta y asunción del riesgo**

OBLIGACIONES ENTIDADES ESENCIALES E IMPORTANTES

Entidades Esenciales

- Supervisión Ex Ante & Ex post
- Inspecciones in situ y supervisión externa
- Auditorías de seguridad periódicas y específicas
- Análisis de seguridad
- Solicitudes de información
- Solicitudes de información necesarias para evaluar, es post, las medidas de gestión de riesgos de ciberseguridad adoptadas por la entidad en cuestión
- Auditorías ad hoc, por ejemplo, después de un incidente significativo

Entidades importantes

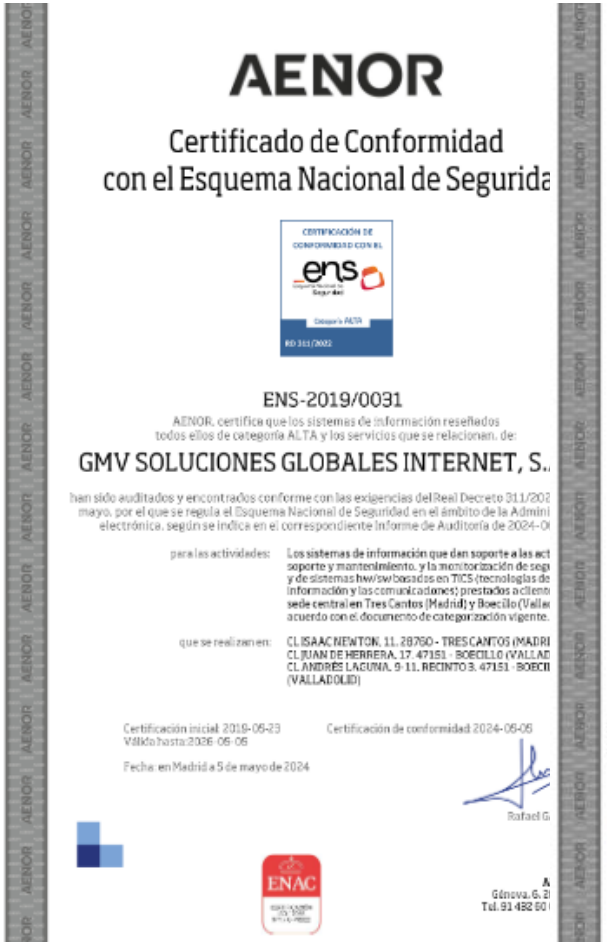
- Supervisión Ex post
- Inspección in situ y supervisión expost fuera de instalaciones
- Auditorías de seguridad específicas
- Análisis de seguridad
- Solicitudes de información
- Solicitudes de información necesarias para evaluar, es post, las medidas de gestión de riesgos de ciberseguridad adoptadas por la entidad de que se trate
- **Auditorías ad hoc, por ejemplo, después de un incidente significativo**

CCN centro criptológico nacional

Proyecto piloto con AEE

AGENCIA ESPACIAL ESPAÑOLA

1. Piloto de auto registro
2. Acompañamiento en análisis de riesgo, categorización y auditorias
3. Apoyo a la demostración de cumplimiento mediante la certificación
4. Impulso a la notificación de ciberincidentes


AENOR

Certificado de Conformidad con el Esquema Nacional de Seguridad

ENS-2019/0031

GMV SOLUCIONES GLOBALES INTERNET, S.


AENOR

Certificado de Conformidad con el Esquema Nacional de Seguridad

ENS-2018/0006

E.P.E. ENAIRE

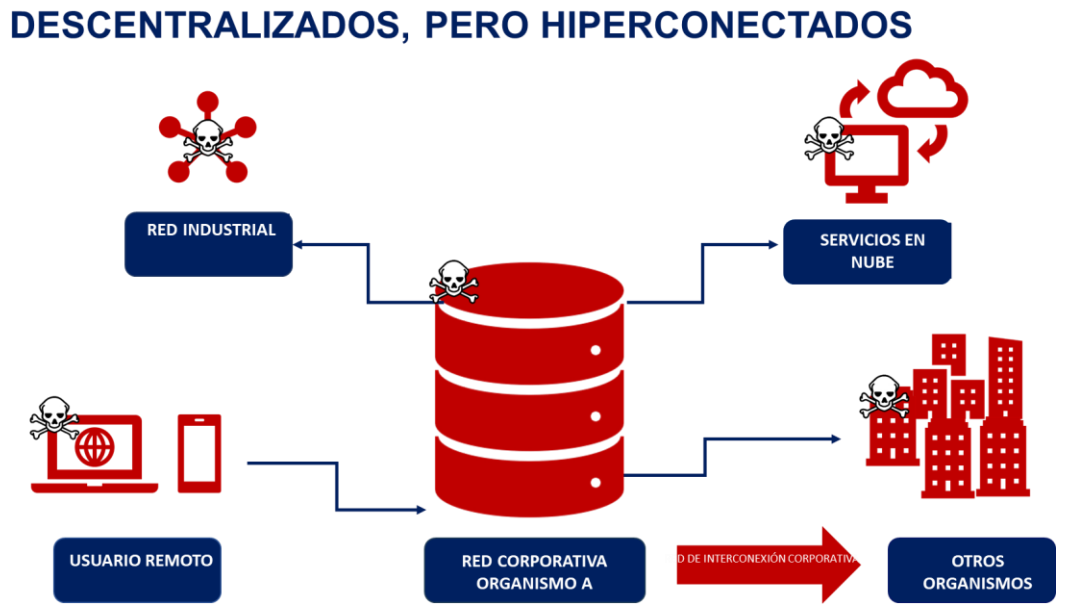
espacio-poc-sectorial@aee.gob.es

CCN centro criptológico nacional

CONCLUSIONES

- **Directiva NIS 2.0. MEJORAR EL NIVEL DE CIBERSEGURIDAD**

- **España tiene mucha capacidad en los campos de gestión de riesgos, medidas de seguridad y notificación de incidentes.**



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 + Red Nacional de SOC.

CIBERDEFENSA ACTIVA

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

centro criptológico nacional

Muchas Gracias

E-mails

info@ccn-cert.cni.es

ccn@cni.es

Páginas web:

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

LÍNEA DE ACCIÓN 1

Reforzar las capacidades técnicas ante las amenazas provenientes del ciberespacio.

12. Implantar medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta.

[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