APROXIMACIÓN A LA CIBERDEFENSA

Miguel Ángel Ballesteros

Madrid, 17 de septiembre de 2020

DSN

Escenario estratégico actual

GLOBALIZACIÓN → se caracteriza por la gran velocidad de cambio

riesgos y amenazas poliédricas, cambiantes, difíciles de evaluar y de predecir

Nuestra región, en su extensión más amplia, es cada vez más inestable e insegura
(Federica Mogherini)

Conflictos híbridos

Desinformación

Necesidad de estrategias de comunicación y análisis de la información y redes sociales permanente

Necesidad de adelantarse a los acontecimientos mediante la realización de análisis geopolíticos con actualización permanente

Para hacer frente a los riesgos y amenazas actuales es necesario aplicar un ENFOQUE INTEGRAL

DSN

Amenazas y desafíos: la necesidad de la ciberseguridad y ciberdefensa

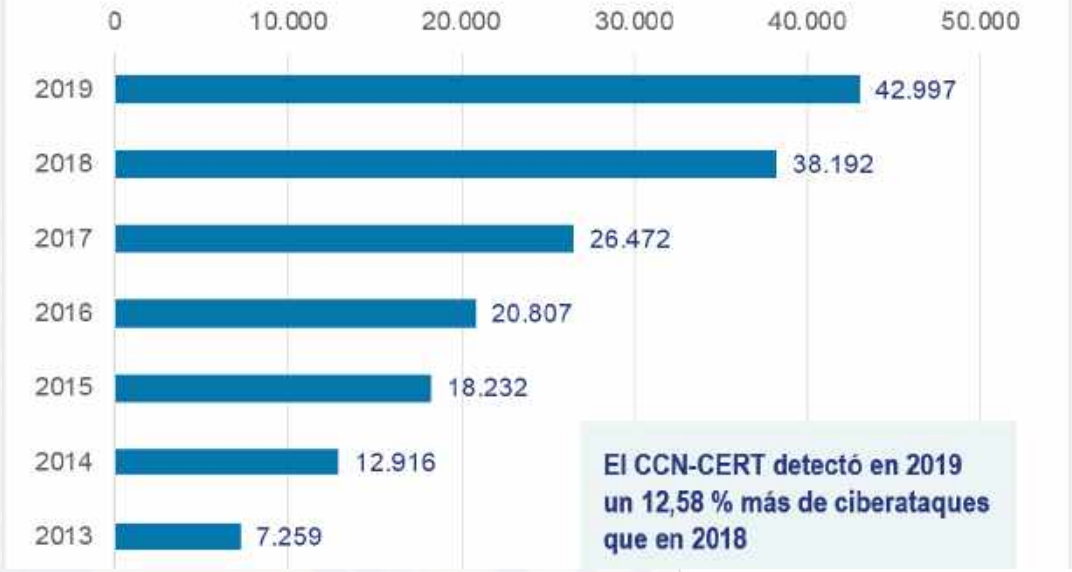
Amenazas híbridas

DSN

ESN-2017

Ciberataques registrados por CCN-CERT y su peligrosidad

Número de ciberataques registrados por el CCN-CERT 2013-2019



El CCN-CERT detectó en 2019 un 12,58 % más de ciberataques que en 2018

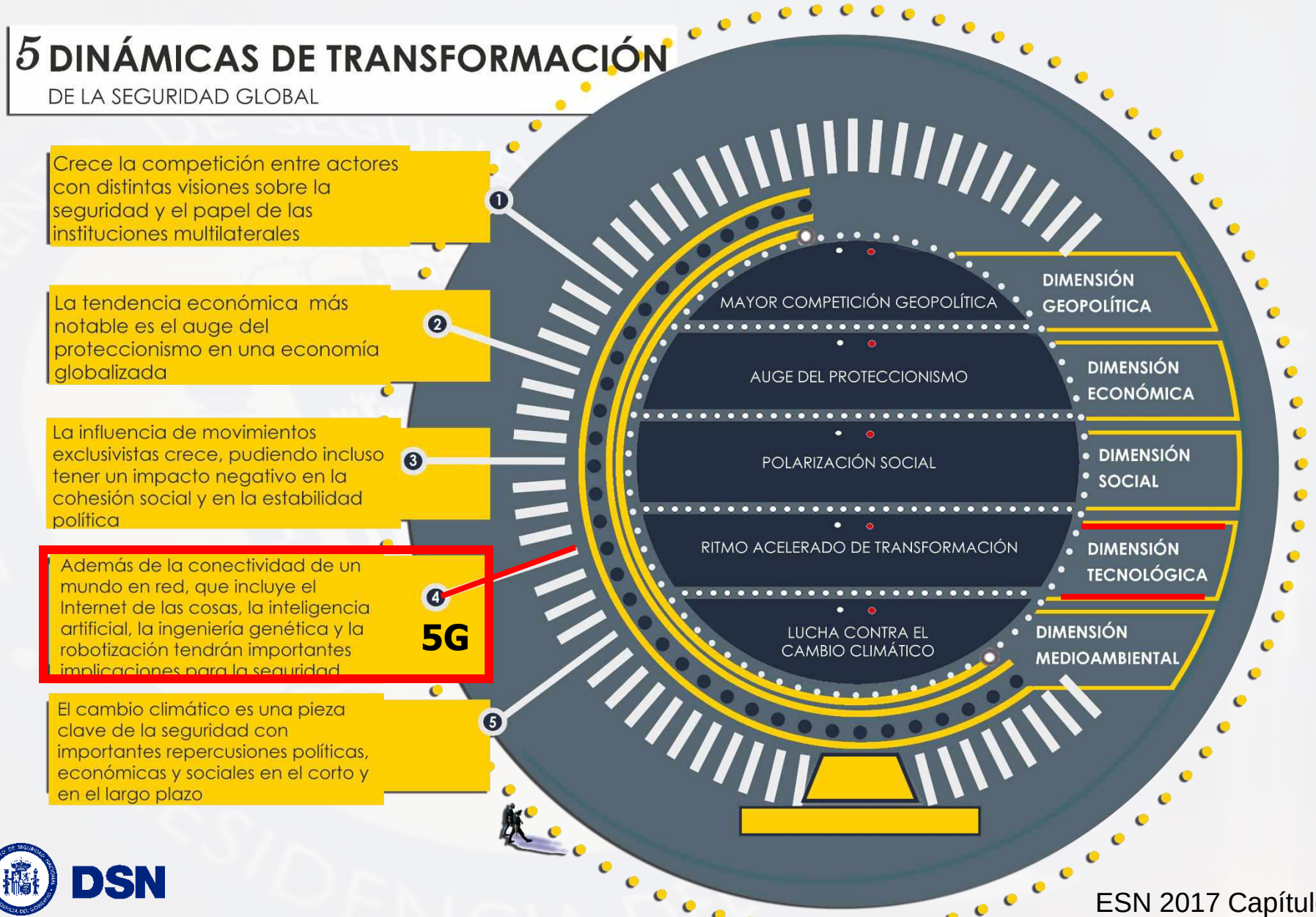
Peligrosidad de los ciberataques en 2019

Los ciberataques más recurrentes en 2019 han sido las intrusiones, que representan el 38% del total de los ciberincidentes registrados en el año

Fuente: Centro Nacional de Inteligencia

DSN

Dinámicas de transformación de Seguridad Global



DSN

¿Qué es la guerra hibrida?

Amenaza híbrida como
"cualquier adversario que de manera simultánea y adaptativa emplea una mezcla de armas convencionales, tácticas irregulares, terrorismo y comportamiento criminal en el espacio de batalla para alcanzar sus objetivos políticos (Hoffman)

Guerra Compuesta (Compound Warfare)
para dar respuesta a la situación generada por el hecho de combatir fuerzas regulares e irregulares de manera concertada, pues sus capacidades complementarias influyen en el adversario obligando a un despliegue de recursos que el permita hacer frente a la panoplia de diferentes amenazas a las que hacer frente, dificultándole la concentración, planteando el viejo dilema militar de concentración frente a dispersión. Huber

GUERRA HÍBRIDA
es aquella en la que se emplea una combinación de instrumentos convencionales y no convencionales (ciberataques, desinformación, presión económica, etc.)

- **Guerra Israel vs Hizbulá 2006 "nacimiento" de la guerra híbrida**
- **Conflicto de Ucrania: El triunfo de la estrategia hibrida rusa**

LOS PLANES DE CIBERDEFENSA EN EL SISTEMA DE SEGURIDAD NACIONAL

POLÍTICA NACIONAL

Para alcanzar los objetivos fijados por la política

1º nivel

ESTRATEGIA DE SEGURIDAD NACIONAL
Consejo de Seguridad Nacional

Comité de Situación
Gestión de crisis

Conferencia Sectorial para Asuntos de Seguridad Nacional

2º nivel

Estrategias particulares (ministeriales o trasversales)

ESTRATEGIA NACIONAL CIBERSEGURIDAD

- E. CONTRA TERRORISTA
- E. CONTRA CRIMEN ORGANIZADO
- E. PROTECCIÓN CIVIL
- E. DEFENSA
- E.ECONOMICA
- SEG. ENERGETICA
- SEG. MARÍTIMA
- SEG. AEROSPACIAL

3er nivel

Planes estratégicos

- Plan contra la radicalización
- Plan contra la financiación del terrorismo

E. Militar

Planes de Ciberdefensa Protección/ Disusión

Plan Nacional de Ciberseguridad

DSN

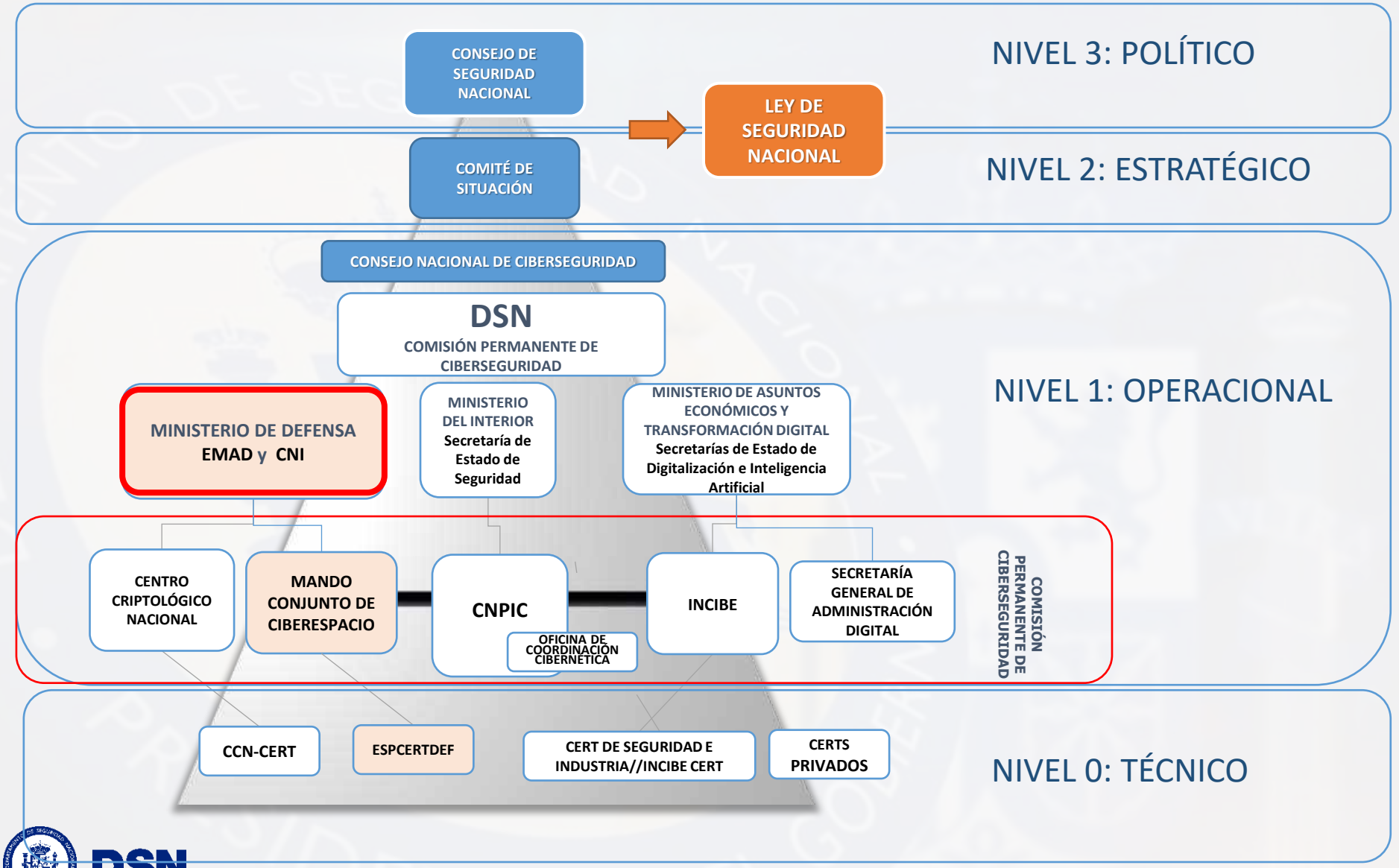
Operaciones

Claves de la Estrategia Nacional Ciberseguridad 2019

- ✓ La ciberseguridad es un ámbito de especial interés establecido en la Ley de Seguridad Nacional 36/2015.
- ✓ La ENCS 2019 respecto a la de 2013 es un documento más global, integrado y social; que promueve la colaboración público - privada.
- ✓ **Modelo de gobernanza de la ciberseguridad**
  - ✓ Liderado por el **Presidente del Gobierno con el apoyo del Consejo de Seguridad Nacional,** asesorado por el Consejo Nacional de Ciberseguridad.
  - ✓ A nivel operacional y para gestión de crisis cuenta con el apoyo de la **Comisión Permanente de ciberseguridad.**
  - ✓ A nivel **técnico**, se cuenta con 3 Equipos de Respuesta ante incidentes de seguridad de la información (ciudadanos, empresas e infraestructuras críticas; Administración y defensa)
- ✓ Integrado en el modelo se cuenta con el Centro Nacional de Protección de Infraestructuras y Ciberseguridad.

DSN

Procedimiento de gestión de crisis-ciberseguridad



DSN

LA GESTIÓN DE CRISIS EN LA ENCS 2019

- ✓ Un hito importante ha significado la transposición de la **Directiva NIS**.
- ✓ La **Comisión** recomienda que los mecanismos de gestión de crisis deben adecuarse a la respuesta de incidentes de ciberseguridad, contando con procedimientos adecuados para cooperar.
- ✓ La **Ley 36/2015** de Seguridad Nacional desarrolla la Gestión de crisis en el marco del Sistema de Seguridad Nacional
- ✓ Contamos con un **procedimiento de coordinación** en materia de gestión de crisis para la ciberseguridad.
- ✓ Hay que continuar avanzando a nivel europeo para enlazar los niveles técnicos y el estratégico/político (IPCR) de gestión de crisis.

Francia (ANSSI) y España (DSN) organizaron en 2019 el ejercicio Blueprint para preparar la gestión de crisis en el ciberespacio

DSN

Las amenazas y desafíos en el ciberespacio

La ESN 2017 distingue entre ciberamenazas y actividades maliciosas

Ciberamenazas

- Las ciberamenazas son todas aquellas disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos
- Su carácter transversal, exige que la ciberseguridad perspectiva público y privado
- la seguridad de las redes y sistemas de información requiere potenciar las medidas de prevención, detección y **respuesta**

Acciones que usan el ciberespacio para fines maliciosos:

- Estados, grupos organizados y hasta individuos aislados pueden alcanzar gran poder.
- La conectividad permite que movimientos globales tengan importancia estratégica
- **El ciberespionaje**: económico, rápido y de difícil atribución de la autoría.
  tendencia creciente de las **amenazas híbridas (Estados democráticos)**
- **La cibercriminalidad** actividades ilícitas cometidas en el ciberespacio
  - **Ciberterrorismo**: financiación, ciberataques, radicalización, etc.
  - **grupos hacktivistas**, contratación de servicios de cibercriminales
  - empleo malintencionado de **datos personales**
  - **campañas de desinformación**

OBJETIVOS DE LA ESTRATEGIA

OBJETIVO GENERAL

En línea con la Estrategia de Seguridad Nacional, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.

Objetivos que afectan a la Ciberdefensa

Objetivo **01** Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.

Objetivo **02** Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.

Objetivo **03** Protección del ecosistema empresarial y social de los ciudadanos.

Objetivo **04** Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.

Objetivo **05** Seguridad del ciberespacio en el ámbito internacional.

DSN

Estrategia Nacional de Ciberseguridad: Líneas de acción

OBJETIVOS

Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales

Seguridad y resiliencia del ecosistema empresarial y social y de los ciudadanos

Uso seguro y fiable del ciberespacio frente a su uso ilícito o malicioso

Cultura y compromiso con la ciberseguridad y potenciación de las capacidades humanas y tecnológicas

Seguridad del ciberespacio en el ámbito internacional

DSN

ENCS 2019: Líneas de acción y medidas

Línea de Acción 1.

Reforzar las capacidades ante las amenazas del ciberespacio:

1. Ampliar y mejorar las capacidades de detección y análisis de las ciberamenazas
2. Potenciar la colaboración de los centros de excelencia e investigación
3. Potenciar la creación, difusión y aplicación de mejores prácticas y estándares
4. Asegurar la coordinación técnica y operacional de los organismos
5. Desarrollar y mantener actualizadas las normas, procedimientos, etc.
6. **Potenciar las capacidades de ciberdefensa y de ciberinteligencia**
7. Promover la participación de empresas en plataformas sectoriales de información
8. Potenciar y apoyar los desarrollos realizados en la red de CSIRT española
9. Impulsar el desarrollo de plataformas de notificación, intercambio de información
10. **Desarrollar instrumentos de prevención, detección, respuesta**
11. Garantizar la coordinación, la cooperación y el intercambio de información
12. Implantar medidas de ciberdefensa activa en el sector público

CAPÍTULO 4: Líneas de acción y medidas

Línea de Acción 5.

Potenciar la industria española de ciberseguridad, y la generación y retención de talento, para el fortalecimiento de la autonomía digital:

1. Impulsar programas de apoyo a la I+D+i en seguridad digital y Ciberseguridad
2. Dinamizar el sector industrial y de servicios de Ciberseguridad
3. Incrementar el desarrollo de productos, servicios y sistemas de Ciberseguridad
4. Promover la normalización y la exigencia de requisitos en los productos y servicios de TIC
5. Desarrollar marcos de competencias en Ciberseguridad
6. Identificar las necesidades de capacidades profesionales de Ciberseguridad y cibereducación
7. Impulsar la inclusión de perfiles profesionales de Ciberseguridad
8. Detectar, fomentar y retener el talento en Ciberseguridad (investigación)
9. **Impulsar programas específicos de I+D+i en ciberseguridad y ciberdefensa.**

MUCHAS GRACIAS