# CIBERSEGURIDAD

## Informe de situación 2021

DISRUPTIV

Plataforma Tecnológica Española
de Tecnologías Disruptivas

Con financiación de:

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA E INNOVACIÓN

Secretaria técnica a cargo de:

APTE
Asociación de Parques Científicos y Tecnológicos de España

# INDICE

# INTRODUCCIÓN

Con el aumento de las actividades en la esfera digital también han aumentado los riesgos en materia de ciberseguridad.

Según un estudio de Google de 2019, el 99,8% del tejido empresarial español —compuesto por pymes— no se consideraba un objeto atractivo a los ciberataques y c**asi 3 millones de empresas en España estaban poco o nada protegidas contra hackers.**

El Instituto Nacional de Ciberseguridad (INCIBE), a través de INCIBE-CERT (su Centro de Respuesta a Incidentes de Seguridad), ha gestionado 13**3.155 incidentes de ciberseguridad durante el año 2020,** de los cuales 106.466 hacen referencia a ciudadanos y empresas, 1.190 a operadores estratégicos y 25.499 a la Red Académica y de Investigación española (RedIRIS).

Durante 2019 el Centro Nacional de Inteligencia (CNI) detectó 3.172 ciberincidentes de peligrosidad muy alta, mientras que en el presente año 2020 se **han duplicado hasta alcanzar los 6.690.** Por su parte, el Centro Criptológico Nacional (CCN) ha detectado durante 2020 un total de 73.184 ciber amenazas totales, un **aumento del 70% respecto al año anterior.**

Además, una investigación realizada por Ironhack sitúa España como **el tercer país más atractivo del mundo para los ciberdelincuentes**. El análisis otorga al país 30,2 puntos en cuanto a riesgo de sufrir ataques virtuales, solo por detrás de Alemania, con 31,6 puntos, y de Estados Unidos, con 100 puntos.

Este informe pretende ser una foto del momento actual en el que se encuentra dicha tecnología en España y que sirva para poder comparar la situación en un futuro próximo.

# CONCEPTOS BÁSICOS

**Ciberataque:** Es cualquier maniobra ofensiva de explotación deliberada que tiene como objetivo de tomar el control, desestabilizar o dañar un sistema informático.

**Darkweb:** Son aquellas webs intencionalmente ocultas a los motores de búsqueda, con direcciones IP enmascaradas y accesibles sólo con un navegador web especial.

**Esquema Nacional de Seguridad:** Tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito público y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada".

**Plan director de ciberseguridad:** consiste en la definición y priorización de un conjunto de proyectos en materia de seguridad de la información con el objetivo de reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables, a partir de un análisis de la situación inicial.

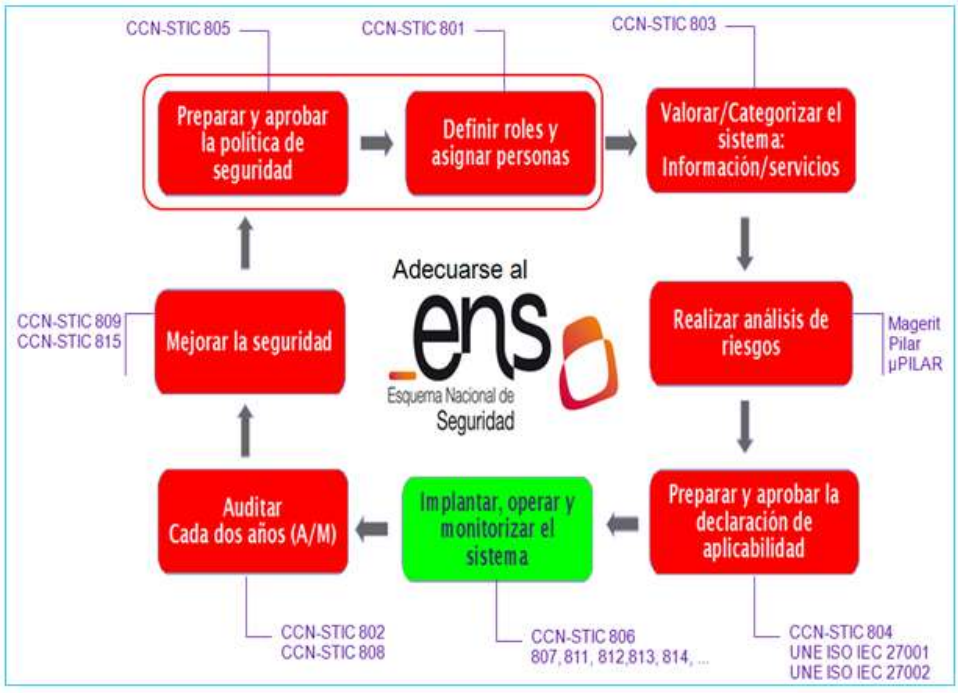



*Figura: Adecuación al Esquema Nacional de Seguridad.*

Fuente: PAE (Portal de la Administración Electrónica)

Estos son algunos de los ejemplos de conceptos básicos, aunque hay muchos más que puedes conocer, por ejemplo, consultando el blog de la **oficina de Seguridad del Internauta**.

# RETOS Y OPORTUNIDADES

Los **principales retos** con los que se encuentra esta tecnología son los siguientes:

- **Cumplimiento normativo** de estándares y regulaciones relevantes en el campo de la seguridad de la información.
- Potenciar y gestionar la **resiliencia cibernética**.
- **Formación y concienciación** de los profesionales.
- Potenciar la **ciberinteligencia**, diseñando, desarrollando y aplicando otras tecnologías digitales disruptivas para ofrecer medidas o acciones a realizar ante las amenazas y riesgos.


Con respecto a la potenciación de la resiliencia cibernética, **Ingenia** recomienda adoptar un sistema de gestión de la seguridad de la información (SGSI) basado en la norma **ISO 27001**, cumplir con el **Esquema Nacional de Seguridad (ENS)** o el **Reglamento General de Protección de Datos (RGPD)**, para poder identificar y valorar nuestros activos, conocer mejor los riesgos a los que está expuesta nuestra información y aplicar controles adecuados a todos los niveles para preservar su confidencialidad, integridad y disponibilidad.

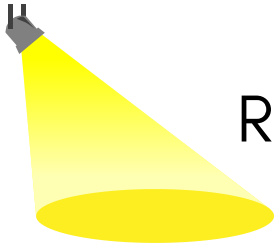
# RETOS Y OPORTUNIDADES

En mayo de este año el gobierno anuncia el **"Plan de Choque de ciberseguridad"**


Fuente: Ministerio de Asuntos Económicos y Transformación Digital

Las medidas incluidas en el 'Plan de choque de ciberseguridad' están vinculadas al **Plan de Recuperación, Transformación y Resiliencia** en su Componente 11 (Inversión 1. Modernización de la Administración General del Estado: **960 M€**) y en su Componente 15 (Inversión 7. Ciberseguridad: **524 M€**).

**El Plan de digitalización de pymes 2021-2025** incluye también programas relacionados con la ciberseguridad como el programa **Protege tu empresa** que gestiona INCIBE o **Activa Ciberseguridad** gestonada por el Ministerio de Industria, Turismo y Comercio a través de la iniciativa Industria Conectada 4.0.



# RETOS Y OPORTUNIDADES

Asimismo, durante este año se han publicado varias **manifestaciones de interés** por parte de los distintos ministerios para garantizar la eficacia del Plan de Recuperación y asegurar la eficiencia en el desarrollo de los proyectos:

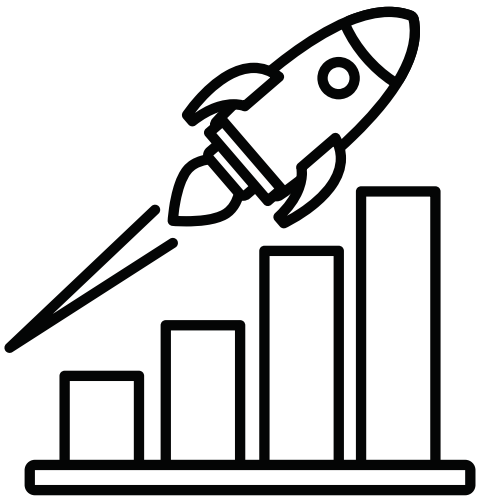
**Fortalecimiento de las capacidades de ciberseguridad de las pymes y el impulso a la industria del sector por parte del Ministerio de Asuntos Económicos y Transformación Digital**

Esta manifestación cerrada el pasado 21 de abril consiguió atraer un total de 325 proyectos, de los que un 76% se corresponden con acciones sobre las PYMEs y el restante 24% de fortalecimiento industrial. 216 propuestas tienen un componente de I+D y 163 contribuyen de manera directa o indirecta al objetivo de transición verde. Los proyectos se concentran mayormente en Madrid, tanto en número de proyectos (55%) como en presupuesto (35%), seguido en número de proyectos por Cataluña, País Vasco y Comunitat Valenciana.

**Consulta Pública al Mercado para la definición de actuaciones de impulso de la ciberseguridad a través de la Compra Pública Innovadora y la elaboración del Mapa de Demanda Temprana** que ha estado abierta hasta el 6 de septiembre.

Asimismo, INCIBE, a través de la Compra Pública de Innovación (CPI) del Instituto de Competitividad Empresarial de Castilla y León (ICE), ha colaborado en la proposición de diversos **retos relacionados con Ciberseguridad.**

# ESTRATEGIA EN ESPAÑA



España cuenta con la **Estrategia Nacional de Ciberseguridad** elaborada en 2019 y que desarrolla las previsiones de la Estrategia Nacional de 2017 en materia de ciberseguridad.

La estrategia establece la posición de España ante una nueva concepción de la ciberseguridad en el marco en el marco de la Política de Seguridad Nacional.

Esta **nueva concepción de la ciberseguridad pasa por entenderla más allá del campo meramente de la protección del patrimonio tecnológico para adentrarse en las esferas política, económica y social.**

Algunas de las novedades que incluye esta estraegia que sustituye a la anterior de 2013 es la creación del Foro Nacional de Ciberseguridad como elemento de colaboración público - privada y el **Centro de Operación de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS).** Este nuevo instrumento previsto en el Plan de Choque de ciberseguridad reforzará las capacidades de vigilancia, prevención, protección, detección, respuesta ante incidentes de ciberseguridad, asesoramiento y apoyo a la gestión de la ciberseguridad de un modo centralizado.

# ECOSISTEMA

Según INCIBE, España cuenta con una industria de la ciberseguridad formada por más de **1.600 empresas**, cuya facturación ronda los **1.300 millones de euros anuales**

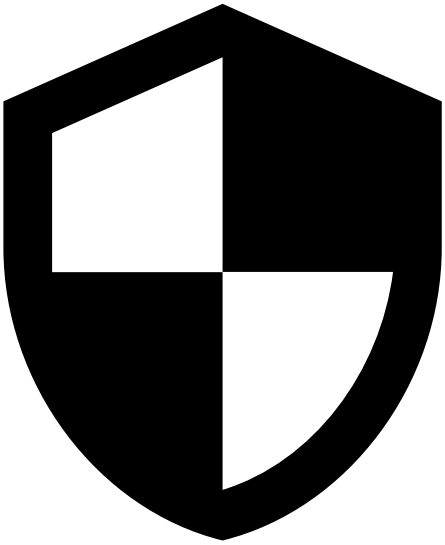
La revista **Red Seguridad** ha reunido en un **número especial a** las empresas más importantes en este ámbito.

Sin embargo, a continuación, se enumeran también a las instituciones relacionados con esta tecnología:

**Consejo de Seguridad Nacional**
**Consejo Nacional de Ciberseguridad**
**Comité de Situación**
**Comisión Permanente de Ciberseguridad**
**Foro Nacional de Ciberseguridad**
**Centro Nacional de Inteligencia (CNI)**
**Centro Criptológico Nacional (CCN)**
**Ministerio de Asuntos Económicos y Transformación Digital**
**Secretaría de Estado de Digitalización e Inteligencia Artificial**
**Instituto Nacional de Ciberseguridad**
**Plataforma Tecnológica Española de Seguridad industrial - PESI**
**Jornadas Nacionales de Investigación en Ciberseguridad**

# CASOS DE USO

A continuación os mostramos algunos de los ejemplos de casos de uso que DISRUPTIVE ha ido recopilando durante junio y julio de2021 y que puedes consultar con más detalle pinchando aquí



**BÁRBARA IOT- Global Omnium**

Gestión de infraestructuras críticas y IoT con un sistema operativo ciberseguro y basado en Edge Computing.
Se trata de un proyecto de monitorización de la ciberseguridad en los sistemas SCADA y de control industrial de sus instalaciones. El sistema cuenta con un diseño mínimamente invasivo y no tiene capacidad de bloquear acciones de los operadores de la planta o interferir en el tráfico en las redes. Además, su concepción es la de un sistema de alerta y, por lo que se refiere a su ejecución, garantiza que en ningún caso se va a introducir tráfico proveniente del exterior en la red de telecontrol.

**APLICACIÓN AL ESPECTRO RF- SpectrumSens**

Sistema de detección, monitorización y actuación (preventiva o proactiva) sobre el espectro RF para la ciberprotección del mismo en todas las bandas requeridas (de uso para WiFi, LPWAN, telefonía, etc.).

# ENLACES DE INTERÉS

Aquí os remitimos a enlaces de noticias, webs, documentos normativos o informes de interés, así como a bibliografía sobre esta tecnología.

**Estrategia Nacional de Ciberseguridad**

**Balance de ciberseguridad de 2020**

**Panorama actual de la ciberseguridad en España**

**La ciberseguridad, la tarea pendiente de las empresas en la era del teletrabajo**

**Ciberpreparación de las empresas españolas**

**Los países más amenzados por los ciberdelincuentes y piratos informáticos en 2020**

**Balance 2020 de los ciberincidentes en España y proyección para 2021**

**Informe 2020 del estado de cultura de ciberseguridad en el entorno empresarial**

**Análisis del Crimen Organizado en Internet - Informe IOCTA 2020**

**Qué es la Dark Web, en qué se diferencia de la Deep Web y cómo puedes navegar por ella**

**Plan director de ciberseguridad**

**Real Decreto 43/2021 por el que se desarrolla nuestro Reglamento de Seguridad de las Redes y Sistemas de Información (Reglamento NIS)**

**Ciberseguridad, principales retos y tendencias**

**Plan de choque de ciberseguridad**

**Reglamento para la actuación y funcionamiento del sector público por medios electrónicos**

**Revista Red Seguridad**

Informe realizado por la **Asociación de Parques Científicos y Tecnológicos de España (APTE),** entidad que gestiona la secretaría técnica de la **Plataforma Tecnológica Española de Tecnologías Disruptivas (DISRUPTIVE)** con la colaboración de su **grupo de trabajo de ciberseguridad** durante los meses de julio y agosto de 2021

DISRUPTIVE Plataforma Tecnológica Española de Tecnologías Disruptivas

Con financiación de: GOBIERNO DE ESPAÑA MINISTERIO DE CIENCIA E INNOVACIÓN

Secretaria técnica a cargo de: APTE