

# Lecturas RECOMENDADAS

Observatorio Nacional de Tecnología  
y Sociedad

28 enero 2022

# Ciberamenazas y tendencias

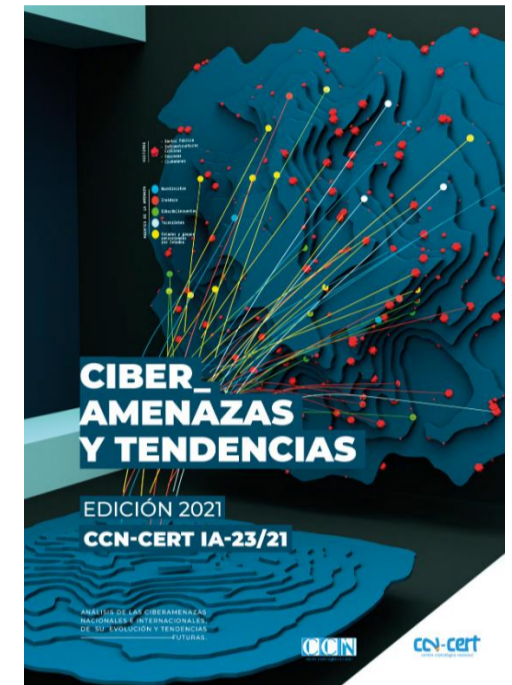
2021

Centro Criptológico Nacional

Fecha publicación octubre 2021 / 67 págs

## El estudio presenta las siguientes conclusiones:

- Con la pandemia, los ciberataques casi duplicaron los del año anterior. El Instituto Nacional de Ciberseguridad (INCIBE) ha gestionado 133.155 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).
- La *ciberpandemia* es la tendencia de ciberataques surgida de la crisis sanitaria, usando la COVID-19 como gancho.
- **En 2021 el 90% de los objetivos de ciberataques fueron organismos públicos, ONGs y entidades de políticas sociales o asuntos internacionales.**
- El *ransomware* (secuestro digital de datos) sigue siendo la vía principal de ciberataques. Sin embargo, se están consolidando nuevas ciberamenazas. Por ejemplo, **los ataques de BEC (Fraude por correo electrónico) se incrementaron en un 200% en 2021, aumentando en un 36% el número de organizaciones afectadas.**
- En la actualidad, la principal amenaza interna en las organizaciones son los empleados que cometen negligencias de forma involuntaria.
- Ante el rápido desarrollo tecnológico surgen también nuevas amenazas a la ciberseguridad. Por ejemplo, se estima que en 2025 habrá más de 30.000 millones de conexiones IoT y una media de cuatro dispositivos por persona. Por lo que asegurar su protección es urgente.



Informe

El informe detalla las principales amenazas y métodos de ataque registrados durante la pandemia. Repasa también las principales vulnerabilidades encontradas y los incidentes de mayor repercusión, tanto en términos de ciber espionaje o ingeniería social, como respecto a intrusiones en sectores que hasta el momento no habían sido un objetivo destacado.

A partir de ese análisis del pasado se ofrecen claves de futuro, apuntando las tendencias que se observan en 2021 en materia de ciberseguridad. También se proporcionarán recomendaciones y buenas prácticas para minimizar el riesgo y el impacto de las amenazas que vendrán.



# Global Cybersecurity Outlook 2022

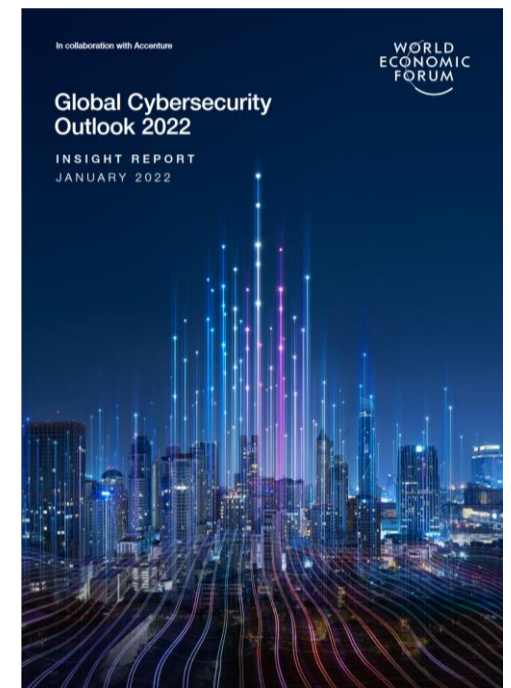
Insight Report January 2022

World Economic Forum

Fecha publicación enero 2022 / 35 págs

## El estudio presenta las siguientes conclusiones:

- La principal preocupación respecto a la ciberseguridad es que se caiga la infraestructura tecnológica de la empresa por un ciberataque (42%). Seguida por el robo de identidad (24%) y el secuestro de datos (20%).
- La amenaza del *ransomware* (secuestro de datos) sigue creciendo. Hasta el 80% de los/as ejecutivos/as subraya que es una amenaza peligrosa. **El 50% de los/as encuestados/as indican que el *ransomware* es una de sus mayores preocupaciones cuando se trata de ciberamenazas.**
- **Un 58% de los/as ejecutivos/as cree que el *machine learning* y la automatización son las herramientas que generarán una mayor respuesta en los próximos años**
- Aún existen diferencias entre la percepción de la ciberseguridad en los distintos ámbitos empresariales. En el entorno del negocio, un 41% considera que la ciberresiliencia es ya una prioridad establecida dentro de la empresa. Sin embargo, ese porcentaje desciende a un 13% entre los encargados de la seguridad



Informe

El informe analiza el estado de la seguridad y las percepciones sobre la ciberresiliencia a raíz de una encuesta realizada a ejecutivos/as, tanto del ámbito de negocio como del de la ciberseguridad, de distintas empresas.





# Open the door to open innovation

## Realizing the value of ecosystem collaboration

IBM

Fecha publicación octubre 2021 / 16 págs

### El estudio presenta las siguientes conclusiones:

- El concepto de innovación abierta -presentado por primera vez por Henry Chesbrough en 2003- afirma que compartir ideas, así como la colaboración tanto interna como externa, ofrece mejores resultados.
- La innovación abierta se ha convertido en una palanca de crecimiento. El 84% de los/as ejecutivos/as encuestados/as dicen que la innovación abierta es importante para su estrategia de crecimiento futuro. **El 61% afirmó que la innovación abierta tiene más éxito que la innovación clásica.**
- Las tecnologías abiertas como la nube híbrida, las API, el blockchain o la IA, facilitan la creación de valor desbloqueando el potencial oculto en las relaciones comerciales existentes.
- La innovación abierta necesita ecosistemas para crear oportunidades de valor. El 63% de los/as ejecutivos/as quiere fomentar nuevas ideas fuera de sus organizaciones.
- Un 56% de las personas entrevistada pretende aumentar su inversión en innovación en los próximos dos años.
- **Un 52% afirma que debido a la COVID-19, sus organizaciones se han visto envueltas con éxito en la transformación digital.** De esas, aquellas que combinaron la transformación digital con la innovación abierta tuvieron resultados muy superiores.



Informe

El estudio se basa en una encuesta a 2.379 ejecutivos/as, que representan 24 industrias y 26 países. Ha sido realizada por el *Institute for Business Value de IBM* en cooperación con *Oxford Economics*.

En este informe se analiza la innovación abierta, su aceptación en las empresas y sus primeros resultados. Se estudia además el vínculo entre este tipo de innovación y la transformación digital.



# Key enabling technologies for Europe's technological sovereignty

Parlamento europeo

Fecha publicación diciembre 2021 / 96 págs

## El estudio presenta las siguientes conclusiones:

- El informe agrupa las tecnologías habilitadoras en seis ámbitos clave: Manufactura, nanomateriales, biotecnología, micro y nano electrónica y fotónica, Inteligencia Artificial y Seguridad y conectividad. El desarrollo y dominio de estas tecnologías será clave para la soberanía europea.
- A pesar de los grandes esfuerzos para apoyar las Tecnologías Habilitadoras, **la Unión Europea se encuentra por detrás de China y los Estados Unidos, debido a la falta de: financiación del I+D (especialmente por parte del sector privado), competencias cualificadas en tecnología y líderes industriales en Tecnologías habilitadoras**
- El informe enuncia los siguientes retos en el camino a dicha soberanía:
  1. Falta de recursos y materiales
  2. Dependencia de proveedores extranjeros
  3. Falta de habilidades digitales
  4. Dificultad en conseguir que los resultados de la investigación científica se transformen en productos comerciales europeos.



Key enabling technologies for Europe's technological sovereignty

STUDY  
Panel for the Future of Science and Technology  
EPRS | European Parliamentary Research Service  
Scientific Foresight Unit (STOA)  
PE 697.184 - December 2021

EN

Informe

Según el Ministerio de Industria, Comercio y Turismo, las Tecnologías Habilitadoras Digitales (THD) son las “tecnologías de alto impacto y capacidad de disrupción, estratégicas para el desarrollo y la transformación digital de la economía y la sociedad”

Resultan fundamentales para una sociedad europea interconectada, digitalizada, resistente y más saludable. Además, son imprescindibles para la competitividad y la posición de la UE en la economía mundial.

Este estudio del Parlamento Europeo analiza la actuación de la UE en el desarrollo de estas tecnologías y la compara con China y Estados Unidos. Sobre la base de los retos identificados, en el informe se discuten las opciones políticas para reforzar la soberanía tecnológica de la UE en materia de Tecnologías Habilitadoras.



# Experiencias y percepciones juveniles sobre la adaptación digital de la escuela en pandemia

Centro Reina Sofía sobre Adolescencia y Juventud

Fecha publicación enero 2022 / 123 págs

## El estudio presenta las siguientes conclusiones:

- Los ordenadores portátiles son los dispositivos más utilizados en la formación online. Por eso las diferencias de clase son tan importantes. Una de cada cuatro personas con carencia material severa no tiene portátil mientras que, para las personas que no tienen carencias materiales, la proporción es de una de cada diez.
- Las diferencias socioeconómicas también influyen en las habilidades digitales. **El 10,5% de jóvenes con graves carencias materiales afirmó tener un nivel de destreza digital “bajo o muy bajo”, ocho puntos por encima del resto.**
- La mayoría de las dificultades durante la formación online no tienen tanto que ver con terceras personas (falta de apoyo, problemas de convivencia...) sino con cuestiones personales como la desconcentración, la desmotivación o el estrés.

Uno de los mayores desafíos que ha traído la pandemia ha sido el de la educación online. En este informe se analizan las vivencias y percepciones del alumnado a este respecto.

EXPERIENCIAS Y PERCEPCIONES JUVENILES  
SOBRE LA ADAPTACIÓN DIGITAL DE LA ESCUELA  
EN PANDEMIA



Educación  
Conectada

fad

BBVA

Informe



[@ONTSI](#)  
[www.ontsi.es](http://www.ontsi.es)

[Suscripción a las Novedades](#)