Informe de tendencias en ciberseguridad

Enero de 2025

Financiado por la Unión Europea NextGenerationEU

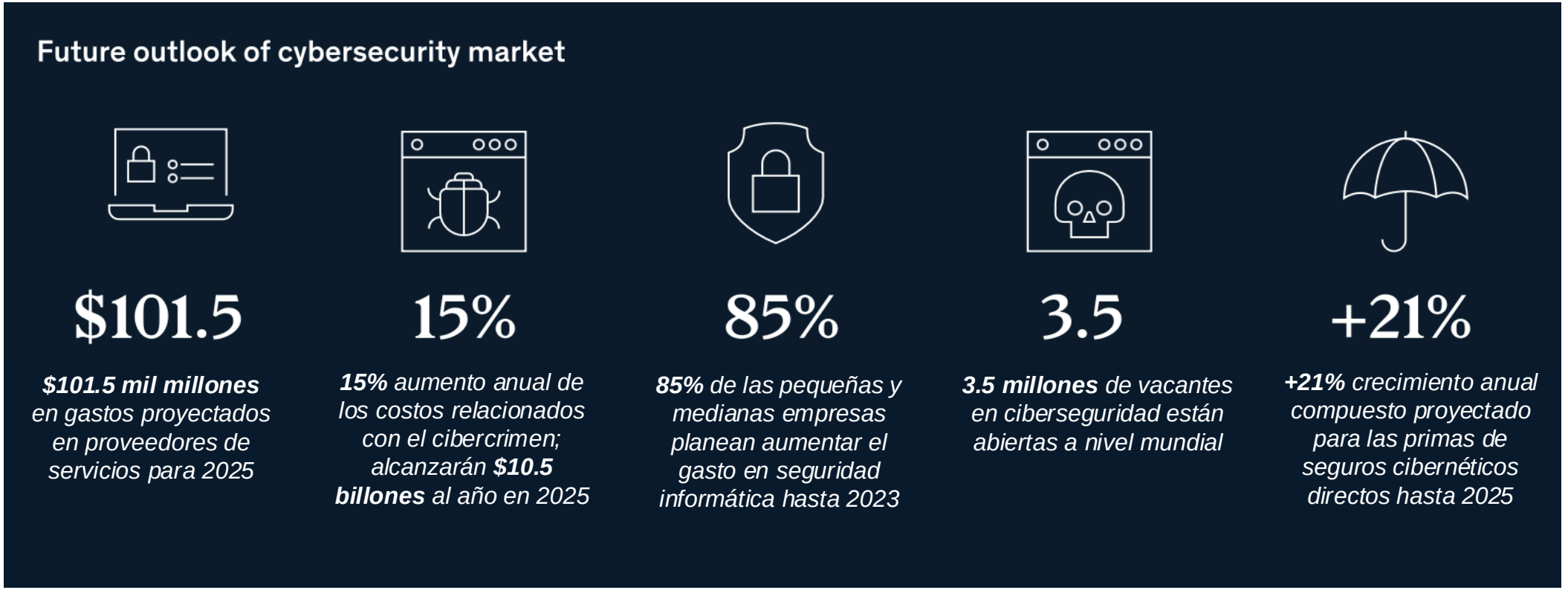
Plan de Recuperación, Transformación y Resiliencia

La Rioja · Gobierno de Aragón · Gobierno de Navarra · Nafarroako Gobernua · Gobierno de Cantabria · Generalitat Valenciana · Generalitat de Catalunya

Informe elaborado por WORSLEY ACCELERATION SERVICES

1. **Introducción a la Ciberseguridad**
   - Conceptos básicos
   - Necesidad de mercado
2. **Oportunidad de mercado**
   - Mercado en cifras
   - Sectores y segmentación
   - Tendencias
3. **La ciberseguridad en España**
   - Panorama en España
   - Empresas del ecosistema Tech FabLab

Los ciberataques están al alza, y los indicadores de mercado reflejan un miedo a que estos se incrementen



https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

¿Qué es un ciberataque?

Un **ciberataque** es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

La **ciberseguridad** es la práctica de proteger sistemas informáticos, redes, dispositivos y datos frente a ataques maliciosos, garantizando la confidencialidad, integridad y disponibilidad de la información.

¿Por qué debería preocuparnos por la ciberseguridad?

Nuestro mundo funciona a base de datos, y **la integridad de nuestros sistemas depende de medidas de ciberseguridad sólidas para protegerlos**. Las medidas de ciberseguridad débiles pueden tener un impacto enorme, pero las tácticas de ciberseguridad sólidas pueden mantener los datos seguros.

https://www.ibm.com/es-es/topics/cyber-attack / https://www.varonis.com/blog/cybersecurity-statistics#cybersecurity-statistics-faqs

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Las amenazas cibernéticas evolucionan constantemente, adaptándose para explotar nuevas vulnerabilidades

Business Email Compromise (BEC)

Se comprometen correos electrónicos empresariales para engañar a organizaciones y empleados con el objetivo de robar dinero, bienes o información confidencial.

Phishing

Comunicaciones fraudulentas que parecen provenir de fuentes confiables con el objetivo de robar información o acceder a sistemas. A menudo simulan ser correos de bancos o empresas legítimas.

Malware

Software malicioso diseñado para dañar o acceder a un sistema o red de forma no autorizada. Tipos: Troyanos, virus, gusanos, keyloggers, ransomware.

Ransomware

Software que encripta datos y exige un pago para desbloquearlos. Las demandas no cumplidas pueden llevar a la destrucción de datos.

Imposter Scams

Intentos de estafa donde alguien se hace pasar por una entidad legítima para obtener dinero o información.

Identity Theft

Robo de información personal para realizar actividades fraudulentas, como obtener préstamos o beneficios bajo una identidad falsa. Impacto**:** Difícil recuperación de la identidad y consecuencias a largo plazo.

Data Breaches

Acceso no autorizado a información sensible o personal. Puede ser usada para estafas dirigidas o robo de identidad.

Hacking

Ataque a sistemas o redes para explotar vulnerabilidades. Métodos**:** Robar datos, obtener contraseñas, instalar malware.

https://www.tpb.gov.au/sites/default/files/2024-02/Cyber%20Security%20-%20back%20to%20basics%20-%20webinar%20slides.pdf

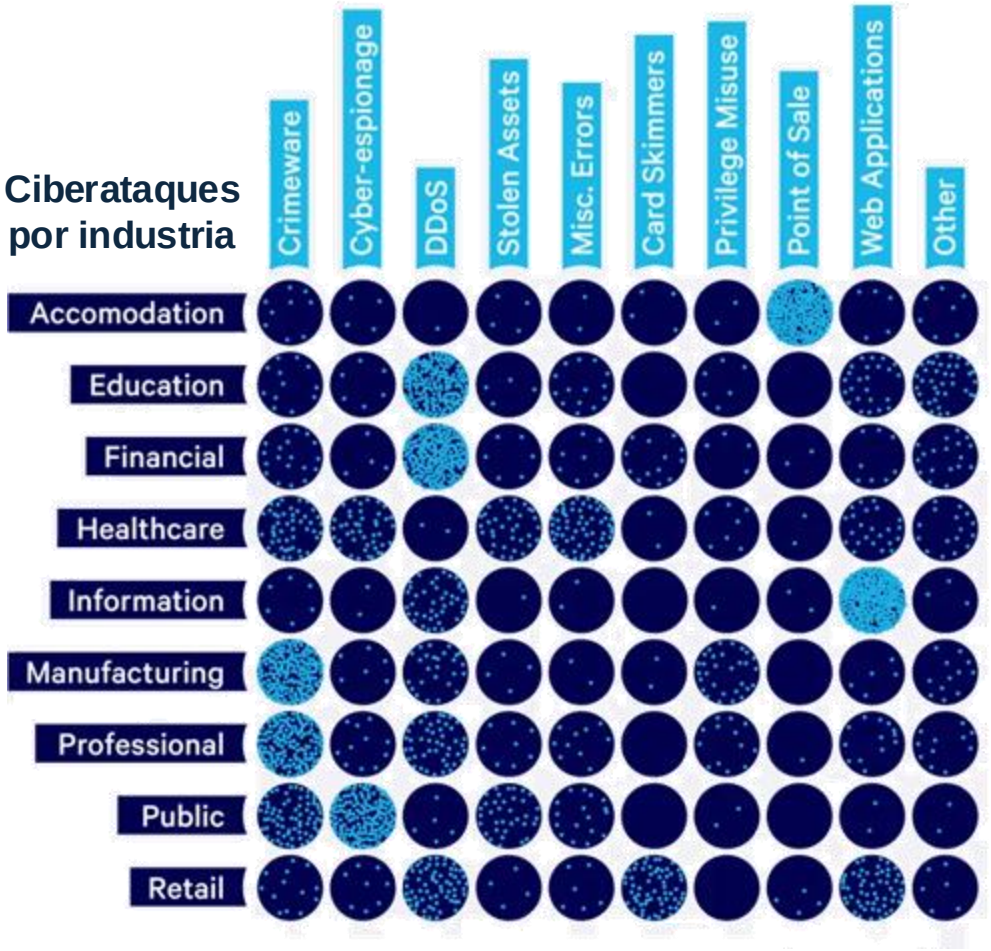
Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Algunas industrias son más vulnerables a los ciberataques debido a la naturaleza de su negocio y la sensibilidad de los datos que manejan

A continuación, se destacan los sectores más afectados en 2023:

- **Fabricación**: Lideró los ciberataques en 2023, representando el 25% del total, especialmente en la región Asia-Pacífico.
- **Banca y finanzas**: Segundo sector más afectado, con el 18.2% de los ataques, debido a la cantidad de datos sensibles que maneja.
- **Servicios profesionales**: Incluye contabilidad, derecho y marketing, representando el 15% de los ciberataques por su acceso a datos sensibles de clientes.
- **Energía**: Registró el 11% de los incidentes en 2023, con un aumento constante desde 2019, impactando petróleo, gas, electricidad y renovables.

Las empresas que poseen **datos confidenciales** o **información de identificación personal** son **objetivos comunes** de los piratas informáticos.



(Fuente: Embroker)

https://www.embroker.com/blog/cyber-attack-statistics/

Financiado por la Unión Europea NextGenerationEU
Gobierno de España Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Los actores de amenazas suelen irrumpir en las redes informáticas de las empresas porque buscan algo específico

Objetivos de los ciberataques

Los objetivos comunes incluyen:

- Dinero
- Datos financieros de las empresas
- Listas de clientes
- Datos de clientes
- Direcciones de email y credenciales de inicio de sesión
- Propiedad intelectual, como secretos comerciales o diseños de productos

En algunos casos, los ciberatacantes no quieren robar nada, simplemente **desean interrumpir los sistemas de información o la infraestructura de TI para dañar** un negocio, una agencia gubernamental u otro objetivo.

Efectos de los ciberataques en las empresas

Los ataques cibernéticos pueden **causar tiempo de inactividad**, **pérdida de datos** y **pérdida de dinero** de diversas formas:

- **Programas maliciosos**: interrupción de sistemas, causando pérdidas promedio de $1,42 millones, según el informe *Cost of a Data Breach*.
- **Inyección SQL**: alteración, eliminación o robo de datos.
- **Suplantación de identidad**: engaño a las víctimas para obtener dinero o información confidencial.
- **Cibersecuestro**: desactivación de sistemas hasta que se pague un rescate, con un promedio de 812.360 dólares.

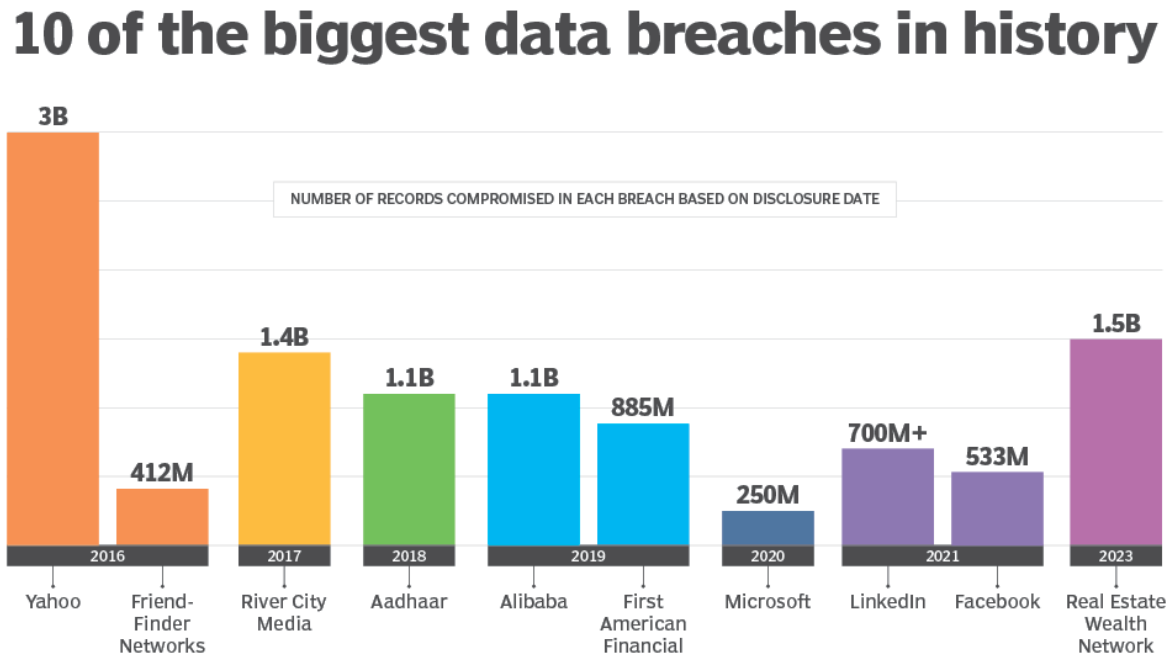
Además, **estos ataques generan costes secundarios**; las empresas gastan $2,62 millones en promedio en remediar infracciones, según *Cost of a Data Breach*.

https://www.ibm.com/es-es/topics/cyber-attack

Financiado por la Unión Europea NextGenerationEU
Gobierno de España – Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Para 2025, el volumen de datos de la humanidad alcanzará los 175 zettabytes (un número con 21 ceros), destacando la importancia de proteger datos sensibles en sistemas globales

- El coste promedio de una brecha de datos en 2024 fue de **$4,88 millones**, el más alto registrado hasta ahora. (Fuente: IBM)
- El **88% de las brechas de ciberseguridad** son causadas por **errores humanos**. (Fuente: Stanford)
- El **ciclo promedio** de una brecha de datos es de **292 días**, desde su identificación hasta su contención. (Fuente: IBM)
- Desde el inicio de la guerra entre Rusia y Ucrania, el 97% de las organizaciones ha experimentado un aumento en las amenazas cibernéticas. (Fuente: Accenture)
- En 2023, los incidentes de ciberseguridad aumentaron un 72% respecto a 2021. (Fuente: Forbes)
- La ciberdelincuencia costará a la economía mundial **10,5 billones de dólares** al año de aquí a 2025. (Fuente: IBM)

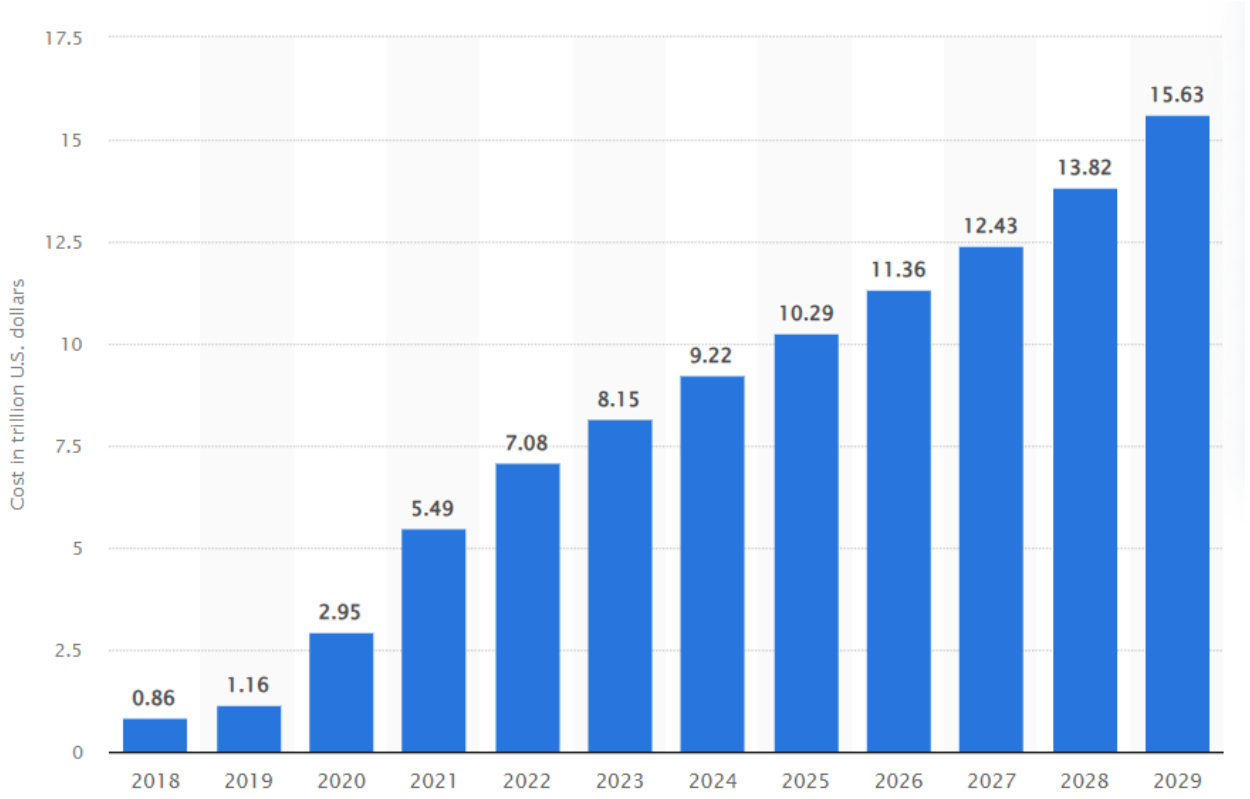


Las 10 mayores brechas de datos a empresas en la historia, clasificadas por el número de registros comprometidos.

https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 / https://www.varonis.com/blog/cybersecurity-statistics#23-security-spending-and-cost-stats

El costo global estimado del cibercrimen aumentará en 6,4 billones de dólares (+69,41%) entre 2024 y 2029, alcanzando un pico de 15,63 billones de dólares en 2029

Previsión de coste global de ciberataques 2018-2029 (en billones de dólares) (Fuente: Statista)

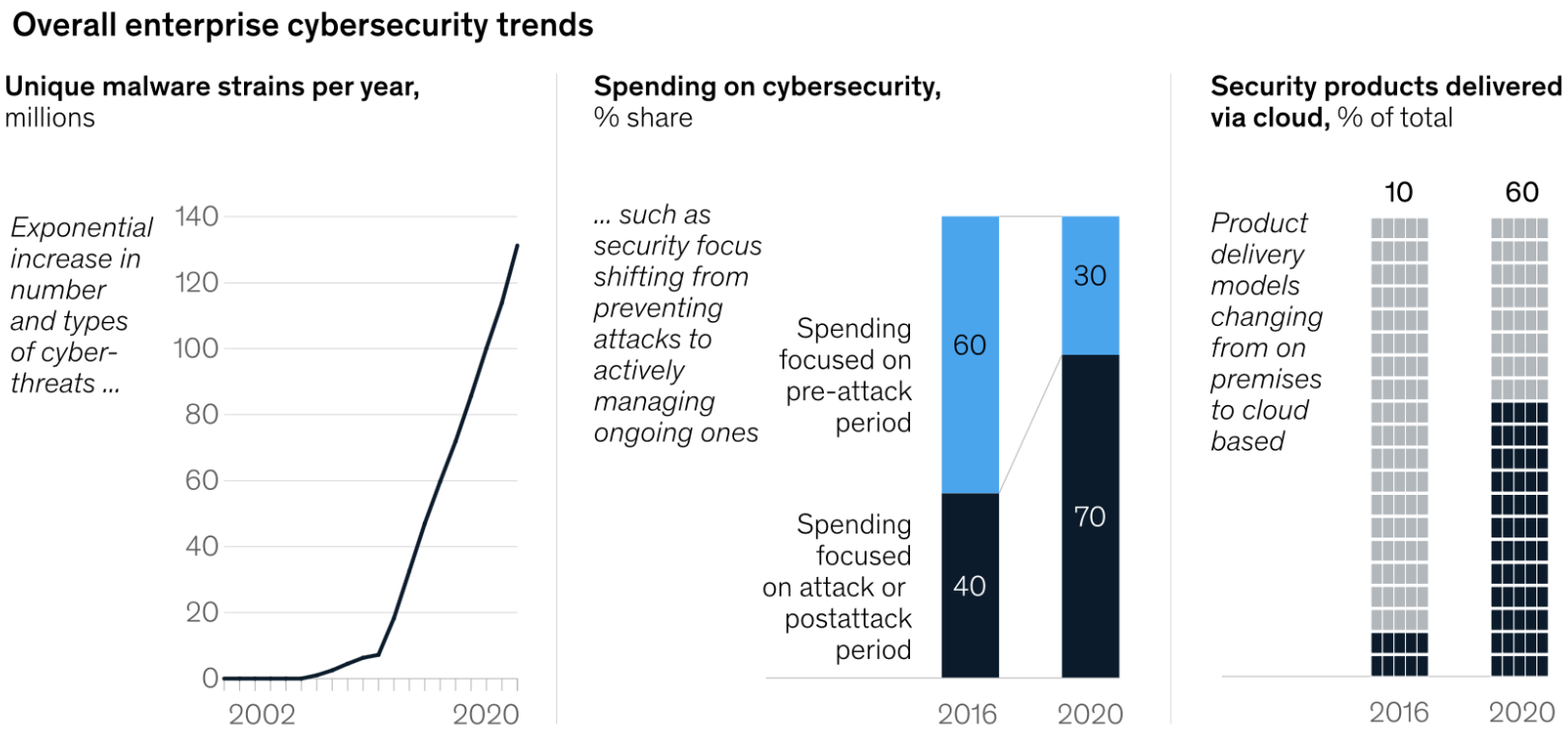


- El ransomware representó alrededor del **70% de los incidentes** cibernéticos detectados.
- La industria manufacturera fue el sector más afectado a nivel global, convirtiéndose en el principal objetivo de los ataques de ransomware.
- El **40% de los usuarios de internet** ya reconoce términos como "ransomware".
- En 2024, los presupuestos de seguridad de TI crecieron un **5,7% anual** en promedio.
- En 2023, la prioridad de gasto de las empresas fue mejorar la **resiliencia cibernética** de sus equipos de seguridad.

https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

A medida que las ciberamenazas incrementan en frecuencia y tipos, el gasto en ciberseguridad también aumentará



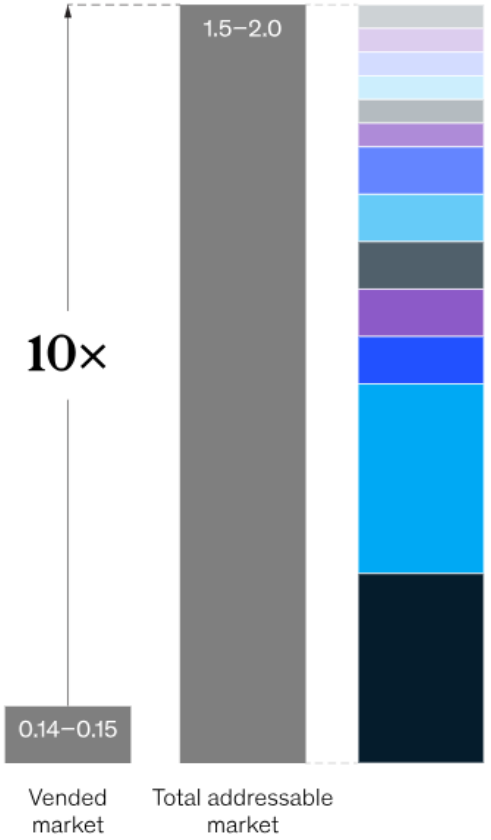
- Según McKinsey, las organizaciones deben desarrollar **capacidades defensivas para mitigar riesgos e impactos de futuras ciberamenazas**.
- Estas capacidades no están vinculadas exclusivamente a cambios específicos, sino que pueden aplicarse a múltiples escenarios.
- Los equipos de gestión deben evaluar todas las capacidades y centrarse en las más relevantes según el contexto y la situación única de su empresa

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

En 2021, el mercado *Total Adressable Market* de ciberseguridad podría alcanzar entre $1,5 billones y $2,0 billones, aproximadamente 10 veces el tamaño del *Vended Market*

Global cybersecurity market size, 2021, $ trillion



Segment	Total addressable market, $ billion	Current penetration, %
Data protection	50–100	30–35
Governance, risk, and compliance	50–100	30–35
Email security and awareness	50–100	10–15
Cloud security	50–100	1–5
Network security	50–100	15–20
Identity and access management	50–100	20–25
Security consulting	100–200	15–20
Web security	100–200	5–10
IoT/OT[1]	100–200	1–5
End point security	100–200	5–10
Application security	100–200	1–5
Security and operations management	400–500	1–5
MSSP[2]/outsourcing	400–500	5–10

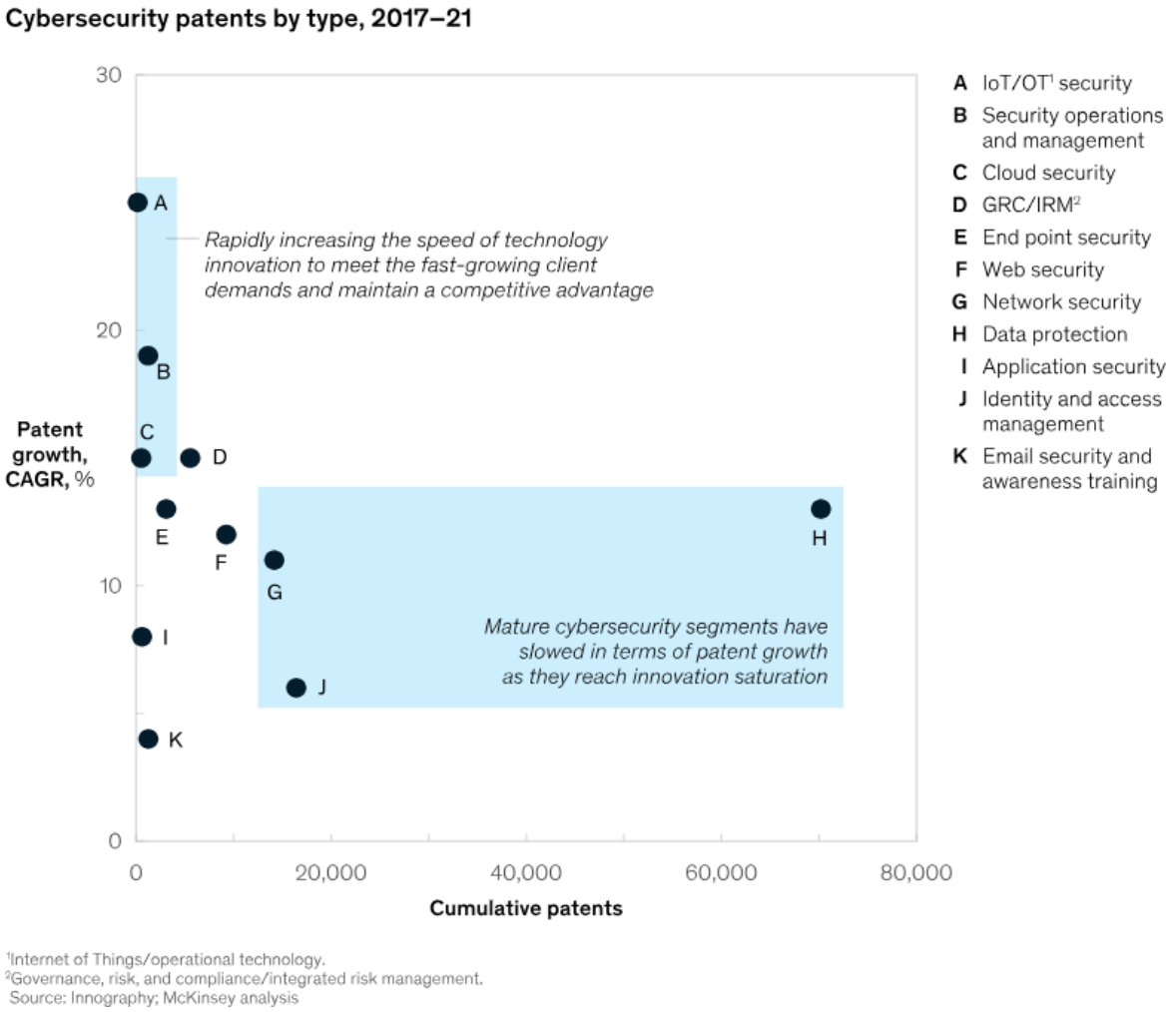
[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

- El *gap* entre el *Vended Market* (tamaño del mercado actual) y el *Total Addressable Market* (TAM) refleja el enorme potencial no explotado en el mercado de ciberseguridad.
- Este desfase se debe a varias razones: la **adopción insuficiente de soluciones avanzadas**, la **falta de proveedores que cubran necesidades complejas** en sectores como el multicloud o industrias altamente reguladas y la **limitada oferta de servicios en mercados emergentes** y PYMEs.
- Este gap representa una **oportunidad clave** para que los proveedores innoven y amplíen su alcance en áreas como seguridad en la nube, protección de datos y gestión de identidades.

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Mientras los segmentos más tradicionales como la seguridad de red han alcanzado madurez, áreas emergentes como IoT/OT y seguridad en la nube están en crecimiento

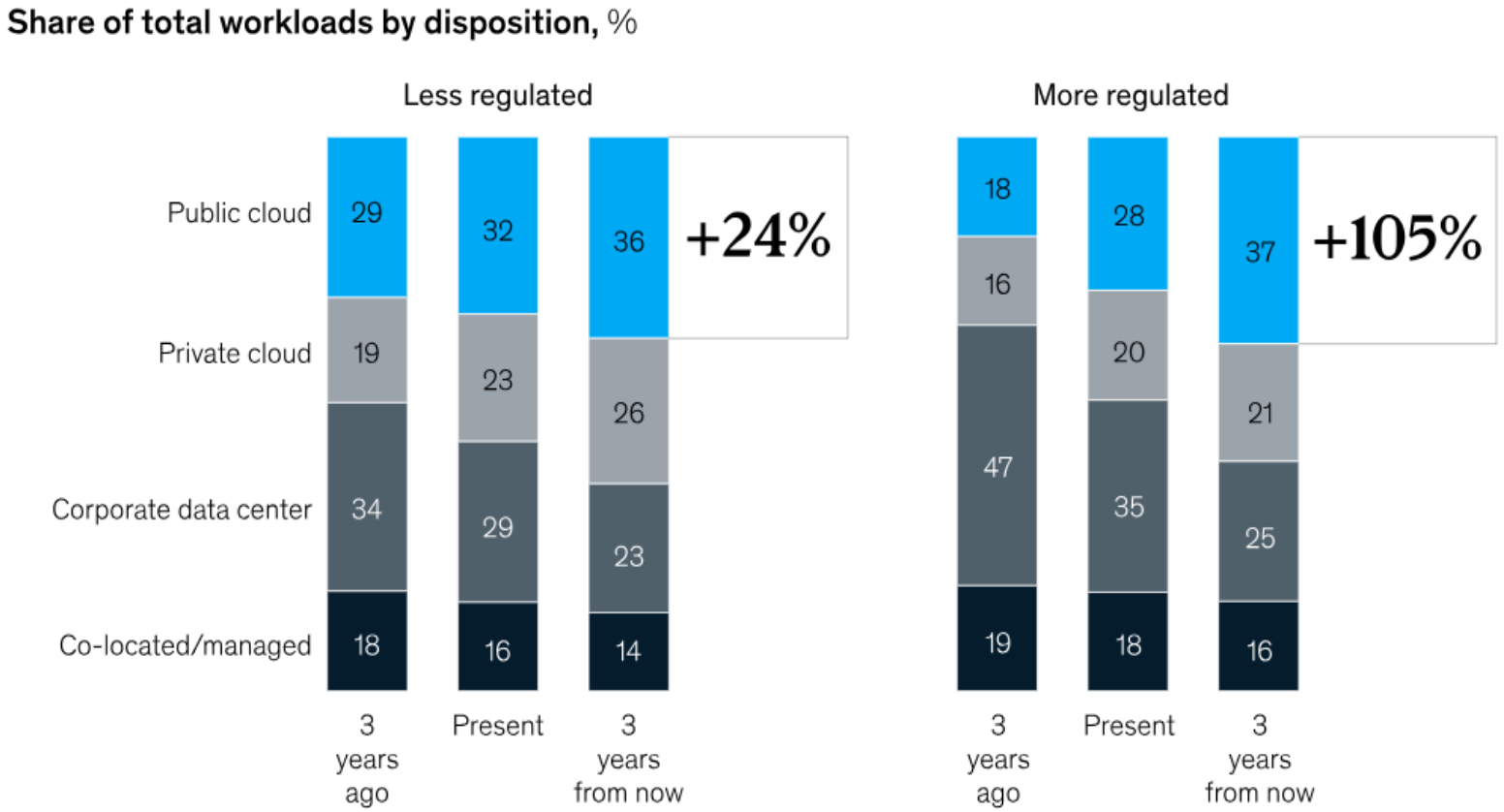


- Los segmentos de **seguridad IoT/OT (*Internet of Things/Operational Technology*)** y **operaciones y gestión de seguridad** (A y B en la gráfica) muestran un crecimiento acelerado en patentes. Esto refleja un enfoque creciente en estas áreas debido a la **expansión de dispositivos conectados y la necesidad de mejorar las capacidades de gestión y respuesta a amenazas**.
- Áreas como la **seguridad en la nube (*Cloud Security*)** y la **gestión de gobernanza, riesgo y cumplimiento (GRC/IRM)** (C y D) también están experimentando un crecimiento significativo. Esto indica una **demanda creciente de soluciones avanzadas en entornos híbridos y multicloud**, junto con necesidades regulatorias más estrictas.
- Tecnologías más maduras como **seguridad de red**, **gestión de identidades y accesos**, y **seguridad web** (G, J y F) tienen un **alto número acumulativo de patentes**, pero su tasa de crecimiento es más baja. Esto sugiere que estos segmentos han alcanzado una **saturación de innovación**, con menos espacio para avances disruptivos.
- La **protección de datos (*Data Protection*)** (H) tiene la mayor cantidad acumulativa de patentes, lo que la posiciona como una prioridad clave en el mercado de ciberseguridad. Sin embargo, su tasa de crecimiento también es moderada, reflejando su madurez como segmento.

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Las industrias altamente reguladas están migrando a la nube pública 4 veces más rápido que las industrias menos reguladas



Note: More-regulated industries include banking, insurance, government; less-regulated industries include manufacturing, software, media, and education.
Figures may not sum to 100%, because of rounding.
Source: McKinsey Cyber Market Map 2022

- La **migración a la nube pública** está redefiniendo las infraestructuras de TI, ya que cada vez más empresas adoptan estas estrategias tecnológicas.
- Para los proveedores de ciberseguridad, es clave no solo adaptarse, sino también **especializarse en arquitecturas híbridas y multicloud** para satisfacer las necesidades emergentes.
- Este cambio representa una **oportunidad de mercado significativa**, con una creciente demanda de **soluciones de seguridad especializadas** diseñadas para este entorno.

https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

La IA ya no es solo una herramienta para las empresas; también es un arma poderosa para los ciberdelincuentes

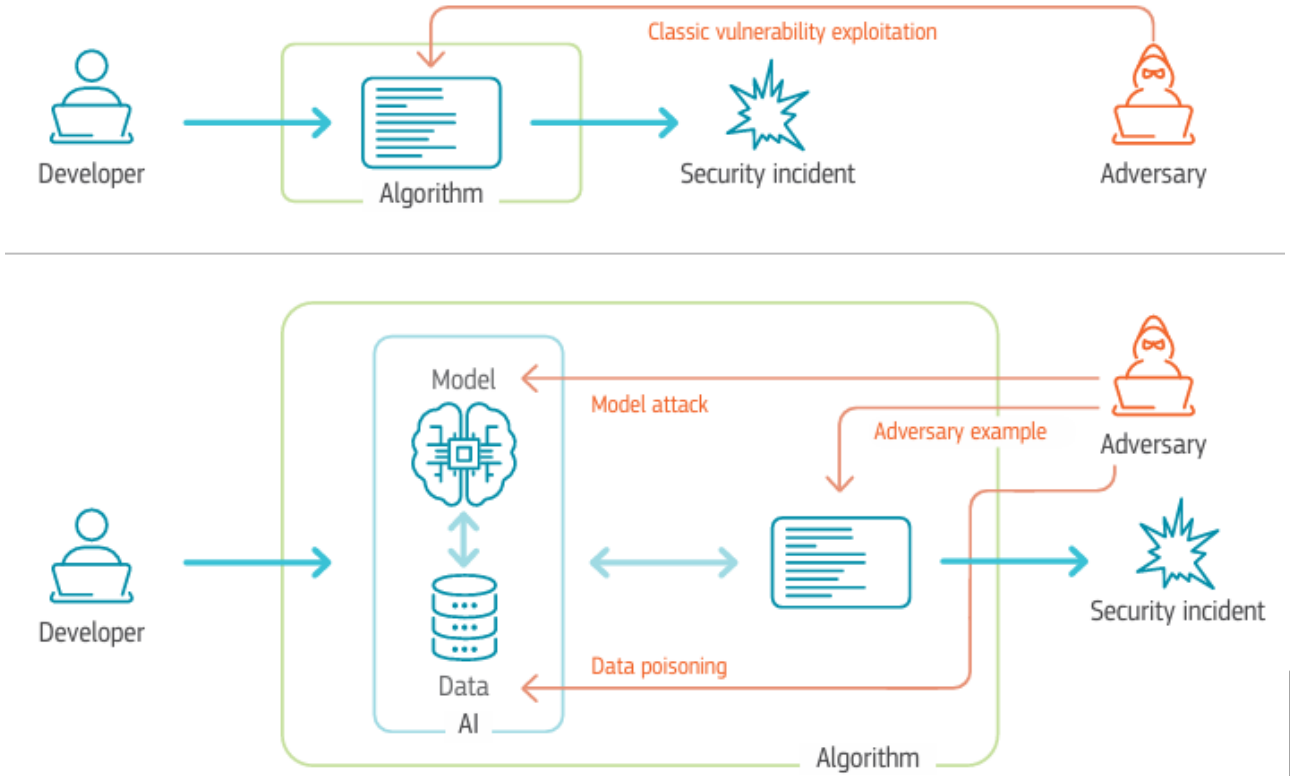
En los ciberataques impulsados por IA, los atacantes utilizan **IA** y **aprendizaje automático (ML)** para automatizar y mejorar cada fase de sus ataques, desde identificar vulnerabilidades hasta implementar campañas sofisticadas.

- **Aumento de ciberataques impulsados por IA:** Se prevé que para 2025 se registren aproximadamente 1,31 millones de quejas relacionadas con ciberataques potenciados por IA, con pérdidas estimadas en $18.600 millones. (Fuente: VPNRanks)
- **Phishing generado por IA:** Se estima que entre el 45% y el 50% de los correos electrónicos de phishing dirigidos a empresas podrían ser creados mediante IA para 2025, con una tasa de respuesta potencial del 62% al 65%. (Fuente: VPNRanks)
- **Incremento de incidentes de seguridad relacionados con IA:** Se proyecta que el 54% de las organizaciones experimentarán incidentes de seguridad vinculados con IA para 2025, debido al aumento de amenazas adversarias basadas en aprendizaje automático. (Fuente: VPNRanks)

https://www.vpnranks.com/es-es/recursos/estadisticas-de-ciberataques-con-ia/

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

La IA ya no es solo una herramienta para las empresas; también es un arma poderosa para los ciberdelincuentes (cont.)



- Al **corromper los datos proporcionados al algoritmo** de IA, el atacante intenta modificar el modelo generado por el algoritmo o la decisión tomada utilizando este modelo.
- Estas vulnerabilidades en **aplicaciones reales**, como los automóviles autónomos, crean **peligros tangibles para la vida de los usuarios finales**.
- Como es probable que aumente la cantidad de sistemas del mundo real que contienen IA, proteger dichos sistemas es de suma importancia.

La inclusión de componentes de IA puede afectar la seguridad del sistema subyacente. (Fuente: *Cybersecurity – Our Digital Anchor*, European Comission)

El desafío de **proporcionar sistemas de IA capaces de resistir ataques maliciosos** desempeñará un papel cada vez más crítico en el ámbito de la ciberseguridad

https://publications.jrc.ec.europa.eu/repository/handle/JRC121051

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

La creciente sofisticación de los ataques ha obligado a las organizaciones a adoptar herramientas más avanzadas, como defensas basadas también en inteligencia artificial

La inteligencia artificial **mejora significativamente los sistemas de seguridad.** Tiene la capacidad de analizar grandes cantidades de datos en tiempo real y detectar patrones y comportamientos anormales que pueden indicar un ataque en curso.

"La IA puede ayudar a fortalecer las defensas de una organización al detectar tempranamente las amenazas, analizar las vulnerabilidades, mejorar la eficacia de los sistemas de seguridad existentes y automatizar tareas de seguridad*. Por lo tanto, es importante que las organizaciones consideren la utilización de soluciones de seguridad cibernética avanzadas que incorporen la IA en sus estrategias de seguridad"*

Víctor González, Consultor TIC de Deusto Formación

https://computerhoy.20minutos.es/tecnologia/impacto-ia-ciberseguridad-ataques-avanzados-defensas-mejoradas-1241912

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia

Ciberdefensa estratégica: aprovechar la inteligencia artificial para anticipar y neutralizar las amenazas modernas

https://smartdev.com/strategic-cyber-defense-leveraging-ai-to-anticipate-and-neutralize-modern-threats/

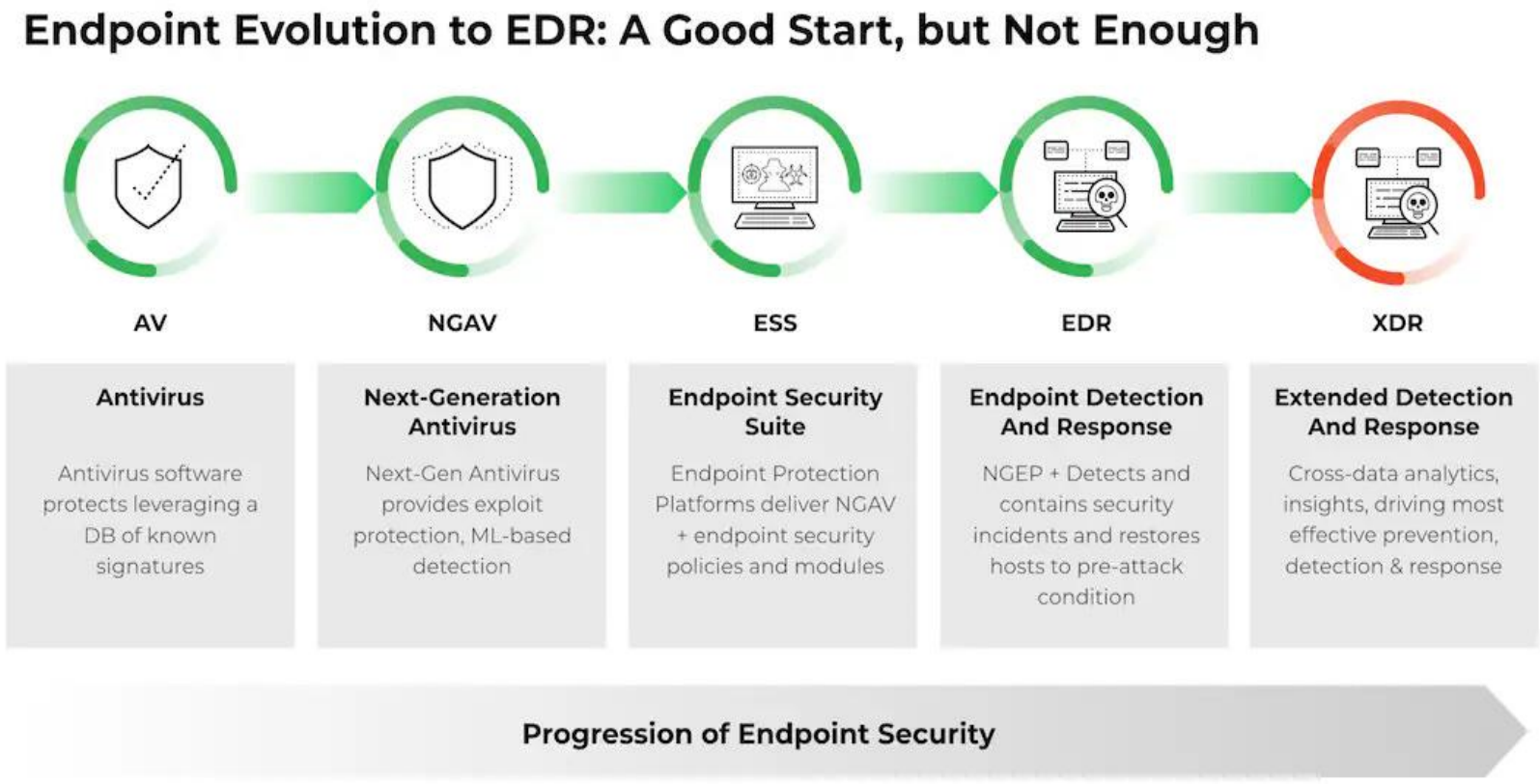
Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Las prácticas de la seguridad de la información son amplias y contemplan varios tipos, cada uno centrado en diferentes aspectos

Seguridad de la red	La protección de la red **garantiza la integridad y uso adecuado de los datos, evitando accesos no autorizados y ataques maliciosos**. Incluye tecnologías y procesos como el monitoreo del tráfico, que analiza los datos en circulación para detectar amenazas.
Seguridad de la información	Centrada en **proteger los datos sensibles del acceso no autorizado, la divulgación, la alteración y la destrucción.** La seguridad de la información es crucial para mantener la confidencialidad, integridad y disponibilidad de dichos datos.
Seguridad de las aplicaciones	Este tipo de ciberseguridad consiste en **proteger las aplicaciones de software con la detección, corrección y prevención de las vulnerabilidades**. Es esencial para garantizar que estén a salvo de ataques que podrían explotar sus vulnerabilidades.
Seguridad de la nube	A medida que más empresas trasladan sus operaciones a la nube, la necesidad de medidas sólidas de seguridad en ese entorno se hace cada vez más importante. Por lo tanto, esta práctica engloba **políticas, tecnologías y controles desplegados para proteger los datos, las aplicaciones y la infraestructura asociada a la computación en la nube**.
Seguridad de los endpoints	**Protege dispositivos como computadoras, smartphones y tablets contra ciberamenazas**, previniendo brechas que podrían comprometer toda la red. Es fundamental para mantener la integridad de los sistemas organizativos.

https://blog.invgate.com/es/ciberseguridad#tipos-de-ciberseguridad

Endpoint Security: La primera línea de defensa contra las ciberamenazas corporativas



La seguridad en los *endpoints* se encarga de proteger los dispositivos que usamos diariamente, como teléfonos, laptops y equipos de escritorio, ya que **cada dispositivo conectado a la red incrementa la superficie de ataque de una organización.**

La imagen muestra la evolución de la *endpoint security* desde las soluciones básicas como los antivirus tradicionales (AV) hasta los sistemas más avanzados como el *Extended Detection and Response* (XDR). Cada etapa refleja una mejora en las capacidades para proteger, detectar y responder a amenazas.

https://blog.publiccomps.com/cybersecurity-industry-primer/

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Top 10 empresas que marcan la diferencia en ciberseguridad a nivel mundial

paloalto NETWORKS	Palo Alto Networks se dedica a proteger activos digitales en nubes, dispositivos móviles y redes. Ofrece soluciones como cortafuegos de próxima generación, seguridad en la nube y detección de amenazas. Además, cuenta con Cortex, una plataforma de seguridad continua basada en inteligencia artificial
CROWDSTRIKE	CrowdStrike ofrece protección de endpoints basada en la nube a través de su plataforma Falcon, que utiliza inteligencia artificial para detectar y detener ataques en tiempo real, incluyendo ransomware y malware.
McAfee	McAfee proporciona soluciones de seguridad para consumidores y empresas, incluyendo software antivirus, protección de datos y seguridad de red. Sus productos están diseñados para proteger contra malware, ransomware y otras amenazas cibernéticas.
deepwatch	Deepwatch se especializa en servicios gestionados de detección y respuesta (MDR), proporcionando monitoreo continuo de amenazas y análisis de seguridad para ayudar a las organizaciones a proteger sus activos digitales.
RAPID7	Rapid7 ofrece soluciones de seguridad de TI y IoT, incluyendo herramientas de gestión de vulnerabilidades, pruebas de seguridad de aplicaciones y detección y respuesta ante incidentes. Sus servicios ayudan a las empresas a identificar y mitigar riesgos de seguridad.

https://builtin.com/articles/cyber-security-companies

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

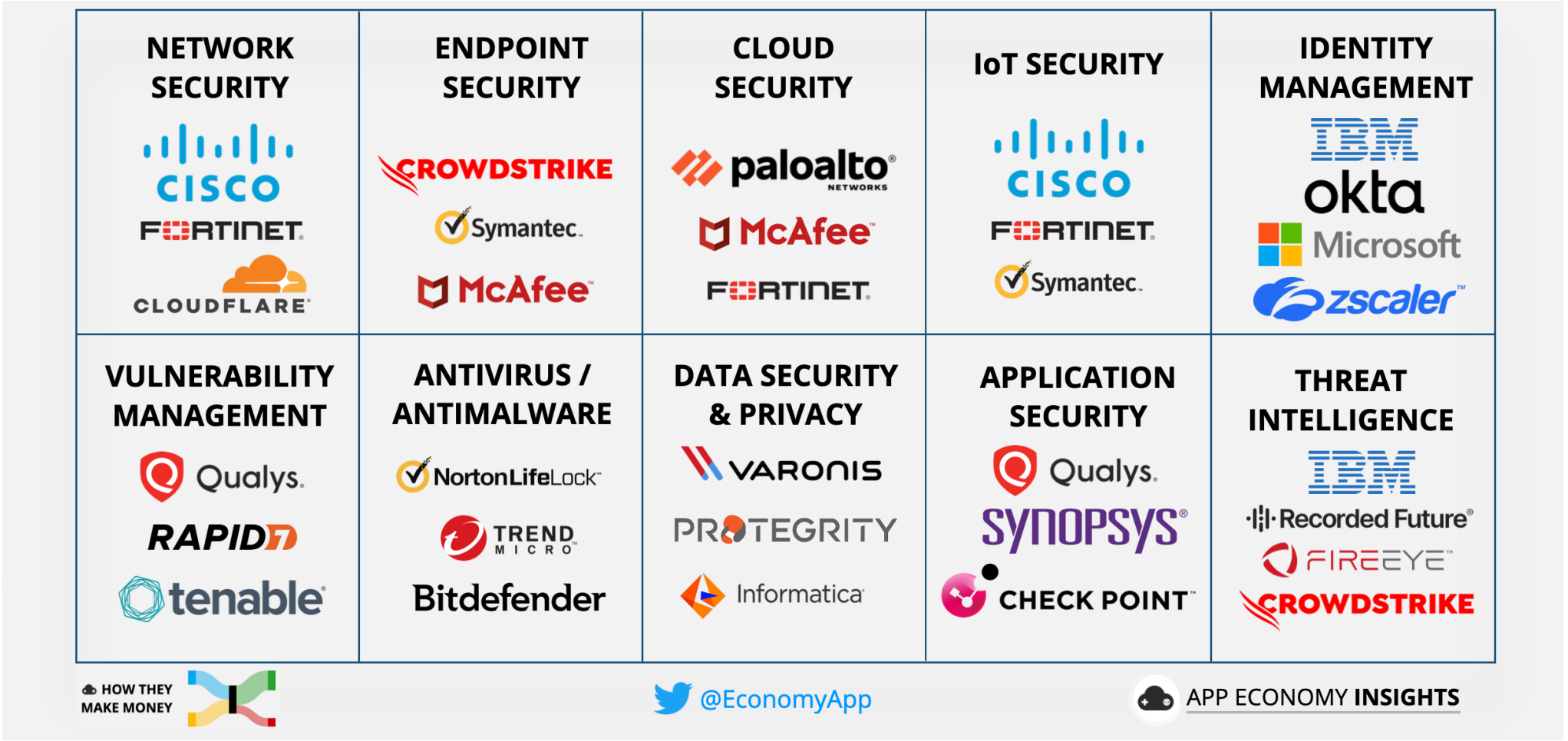
Top 10 empresas que marcan la diferencia en ciberseguridad a nivel mundial

KnowBe4	KnowBe4 proporciona formación en concienciación sobre seguridad y simulaciones de phishing para ayudar a las organizaciones a educar a sus empleados y prevenir ataques basados en ingeniería social.
Ping Identity	Ping Identity se especializa en la gestión de identidades y accesos, ofreciendo soluciones como autenticación única (SSO), gestión de identidades en la nube y autenticación multifactor (MFA) para asegurar el acceso a aplicaciones y datos.
DUO	Duo Security, parte de Cisco, proporciona soluciones de autenticación multifactor (MFA) y control de acceso para ayudar a las organizaciones a protegerse contra accesos no autorizados y garantizar la seguridad de sus aplicaciones y datos.
BAE SYSTEMS	BAE Systems es una empresa multinacional de defensa y seguridad que ofrece soluciones de ciberseguridad, incluyendo protección contra amenazas avanzadas, inteligencia de amenazas y servicios de seguridad para gobiernos y empresas críticas.
FORTINET	Fortinet es líder en ciberseguridad, ofreciendo soluciones como FortiGate (cortafuegos avanzado) y el Fortinet Security Fabric, una arquitectura de seguridad integrada. Proporciona protección para redes, aplicaciones y datos, destacando en industrias como salud, educación y finanzas.

https://builtin.com/articles/cyber-security-companies

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Panorama del mercado de ciberseguridad: líderes por categoría de soluciones



https://www.appeconomyinsights.com/p/cybersecurity-industry-showdown

Para protegerse contra las diversas amenazas que existen hoy en día, es fundamental aplicar las mejores prácticas de ciberseguridad como parte de una sólida estrategia amplia

Algunas buenas prácticas para impulsar la ciberseguridad:

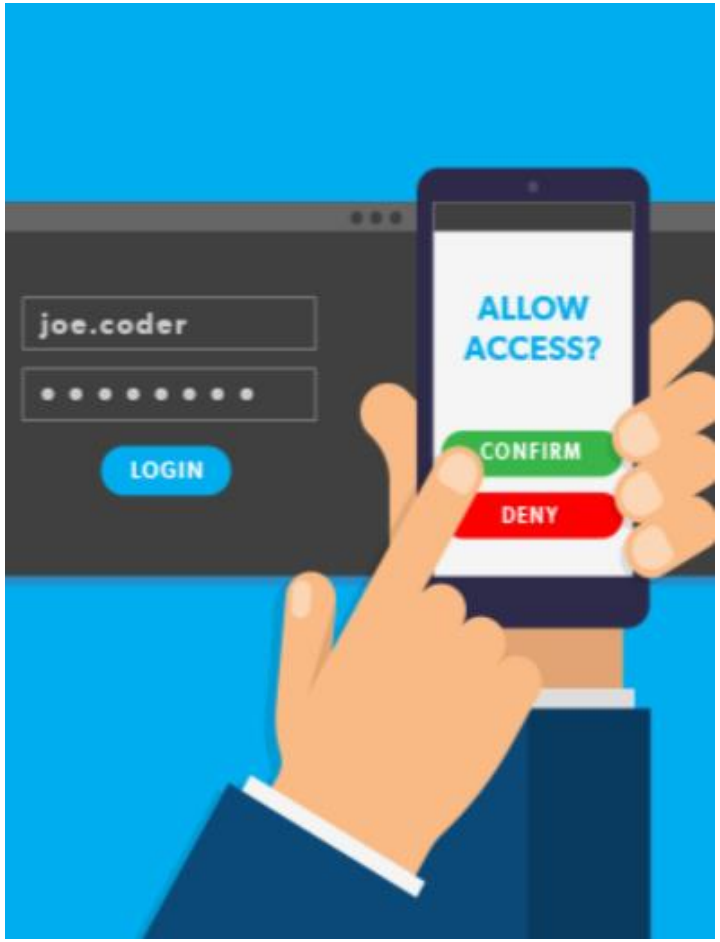
1) **Actualizaciones periódicas del software**: El mantenimiento del software actualizado garantiza que cualquier vulnerabilidad sea parcheada, reduciendo el riesgo de explotación por parte de los atacantes.

2) **Políticas de contraseñas seguras**: La aplicación de políticas de contraseñas sólidas, incluido el uso de passwords complejos y únicos, es crucial para evitar accesos no autorizados. Las herramientas de gestión de contraseñas también pueden ayudar a mantener credenciales seguras.

3) **Formación de los empleados**: Para crear una cultura consciente de la seguridad, resulta fundamental educar y formar a los empleados sobre las mejores prácticas de ciberseguridad y los riesgos de las ciberamenazas.

4) **Autenticación multifactor**: La autenticación multifactor (MFA - multi factor authentication) añade una capa adicional de seguridad al exigir algo más que una contraseña para ingresar a las cuentas, reduciendo significativamente la probabilidad de acceso no autorizado.

5) **Cifrado de datos**: Gracias al cifrado de datos, si éstos caen en las manos equivocadas, serán ilegibles sin la clave. Esta práctica es esencial para proteger la información sensible.



https://blog.invgate.com/es/ciberseguridad#tipos-de-ciberseguridad

En 2024, las organizaciones experimentaron un incremento del 30% en el número de ataques informáticos semanales en comparación con el año anterior

Ataques y violaciones de datos recientes

Month/Year	Company	Sector	Incident Type	No. of People
December 2024	Volkswagen Group	Automobile	Data Breach/Theft/Leak	800,000
December 2024	River Region Cardiology Associates	Healthcare	Data Breach/Theft/Leak	500,000
December 2024	Texas Tech University Health Sciences Center	Education	Data Breach/Theft/Leak	1,460,000
December 2024	AT&T	Telecommunication	Data Breach/Theft/Leak	110,000,000
December 2024	Texas Tech University Health Sciences Center	Education	Data Breach/Theft/Leak	1,400,000
December 2024	Ascension Health	Healthcare	Data Breach/Theft/Leak	6000,000
December 2024	Byte Federal Inc.	Technology	Data Breach/Theft/Leak	58,000
December 2024	PIH Health hospitals	Healthcare	Data Breach/Theft/Leak	17,000,000
December 2024	SRP Federal Credit Union	Financial Services	Data Breach/Theft/Leak	240,000
November 2024	OnePoint Patient Care (OPPC)	Healthcare	Data Breach/Theft/Leak	1,741,152
November 2024	Set Forth	Financial Services	Data Breach/Theft/Leak	1,500,000
November 2024	City of Columbus	Government	Data Breach/Theft/Leak	500,000
November 2024	Free	Technology	Data Breach/Theft/Leak	22,000,000
November 2024	Thompson Coburn	Legal	Data Breach/Theft/Leak	305,088
November 2024	Forth	Transportation	Data Breach/Theft/Leak	133,154
November 2024	Great Plains Regional Medical Center	Healthcare	Data Breach/Theft/Leak	133,149
November 2024	SelectBlinds	Retail	Data Breach/Theft/Leak	200,000
October 2024	Patelco Credit Union	Financial Services	Data Breach/Theft/Leak	1,009,472
October 2024	Harvard Pilgrim Health Care	Healthcare	Data Breach/Theft/Leak	210,354
October 2024	Change Healthcare	Healthcare	Data Breach/Theft/Leak	100,000,000
October 2024	Landmark Admin	Insurance	Data Breach/Theft/Leak	800,000
October 2024	Transak	Financial Services	Data Breach/Theft/Leak	92,000
October 2024	The Centers for Medicare & Medicaid Services	Insurance	Data Breach/Theft/Leak	940,000
October 2024	Omni Family Health	Healthcare	Data Breach/Theft/Leak	468,000
October 2024	Infosys McCamish Systems	Technology	Data Breach/Theft/Leak	6,000,000

https://intellizence.com/insights/business-signals-trends/major-cyber-attacks-data-breaches-leading-companies / https://insights.integrity360.com/es/2024-in-24-cyber-security-statistics

Financiado por la Unión Europea NextGenerationEU
Gobierno de España Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Treasury Department Systems Hacked by China, Reports Say

The U.S. Treasury Department informed Congress in a letter Monday that a state-sponsored Chinese actor hacked its systems through a third-party software provider, according to reports. [1] [2]

Diciembre 2024

Krispy Kreme is latest to report a cyberattack that's hampering its business

Doughnut company is still working to determine extent of hack but says it's having a material impact on business

Diciembre 2024

Cyprus on high alert after cyberattack threat by hackers

Hackers claim politically motivated attack targeting critical infrastructure, linked to Cyprus' ties with Israel.

Octubre 2024

Poland says a fake news report on mobilizing 200,000 men was likely the work of Russia

WARSAW, Poland (AP) — A fake news report that appeared on Poland's national news agency saying that Prime Minister Donald Tusk was mobilizing 200,000 men starting on July 1 was probably the work of Russia-sponsored hackers and was designed to interfere with the upcoming European Parliament election, authorities said.

Mayo 2024

UK Armed Forces Data Exposed: MoD Cyber Attack Timeline

The British Armed Forces experienced a significant cyber attack believed to be orchestrated by Chinese hackers. This attack compromised the personal data of approximately 270,000 serving personnel, reservists, and veterans.

Mayo 2024

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

La estafa de Gmail creada con Inteligencia Artificial que es casi imposible de detectar

Los cibercriminales ya hacen uso de esta herramienta para sus fraudes

Diciembre 2024

Boeing confirms attempted $200 million ransomware extortion attempt

That attempt was one of multiple “extremely large” ransom demands made by LockBit over the years, authorities said.

Octubre 2023

More than 3.8 billion records exposed in DarkBeam data leak

Billions of login credentials were available online after a database was left unprotected

Septiembre 2023

Pro-Russian hackers claim attacks on Italian banks

A pro-Russian hacking group has claimed responsibility for cyberattacks on Italian banks, businesses, and government agencies which flooded networks and disrupted services.

Agosto 2023

Israeli firm 'boasted' of meddling in more than 30 elections worldwide

Febrero 2023

TECHNOLOGY

An Israeli firm sought to influence more than 30 elections around the world for clients by hacking, sabotage and spreading disinformation, according to an undercover media investigation published Wednesday.

Petr Pavel's website is under attack by Russian hackers. The presidential candidate's website faced a similar attack on Wednesday

Enero 2023

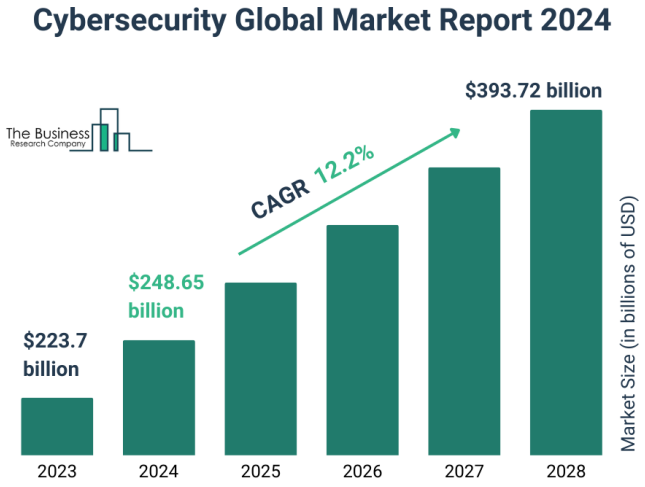
The website of presidential candidate General Petr Pavel has been under a strong hacker attack since Friday morning. As a result, some users are unable to access it, his election team said. The website reportedly faced a similarly strong attack all Wednesday. According to the operator, the attack is being conducted from various IP addresses across Europe.

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
Plan de Recuperación, Transformación y Resiliencia

1. **Introducción a la Ciberseguridad**
   - Conceptos básicos
   - Necesidad de mercado
2. **Oportunidad de mercado**
   - Mercado en cifras
   - Sectores y segmentación
   - Tendencias
3. **La ciberseguridad en España**
   - Panorama en España
   - Empresas del ecosistema Tech FabLab

La demanda de innovación impulsa inversiones récord en ciberseguridad en 2024

El **tamaño del mercado de la ciberseguridad ha crecido rápidamente** en los últimos años. Pasará de $223.700 millones en 2023 a $393.720 millones en 2028, a una tasa de crecimiento anual compuesta (CAGR) del 12,2%.



El crecimiento del mercado se puede atribuir al **creciente número de ataques** cibernéticos, el fuerte **crecimiento económico en los mercados emergentes**, el surgimiento de **nuevas empresas** y la **pandemia de covid-19,** según este informe.

- Los **$9.500 millones recaudados en el año fiscal 2024** representan un **aumento del 9% en la financiación obtenida** en comparación con 2023 ($8700 millones). (Fuente: Pinpoint)
- El volumen de financiación disminuyó un 12%, con **304 rondas de financiación registradas en 2024** en comparación con las 346 de 2023. (Fuente: Pinpoint)

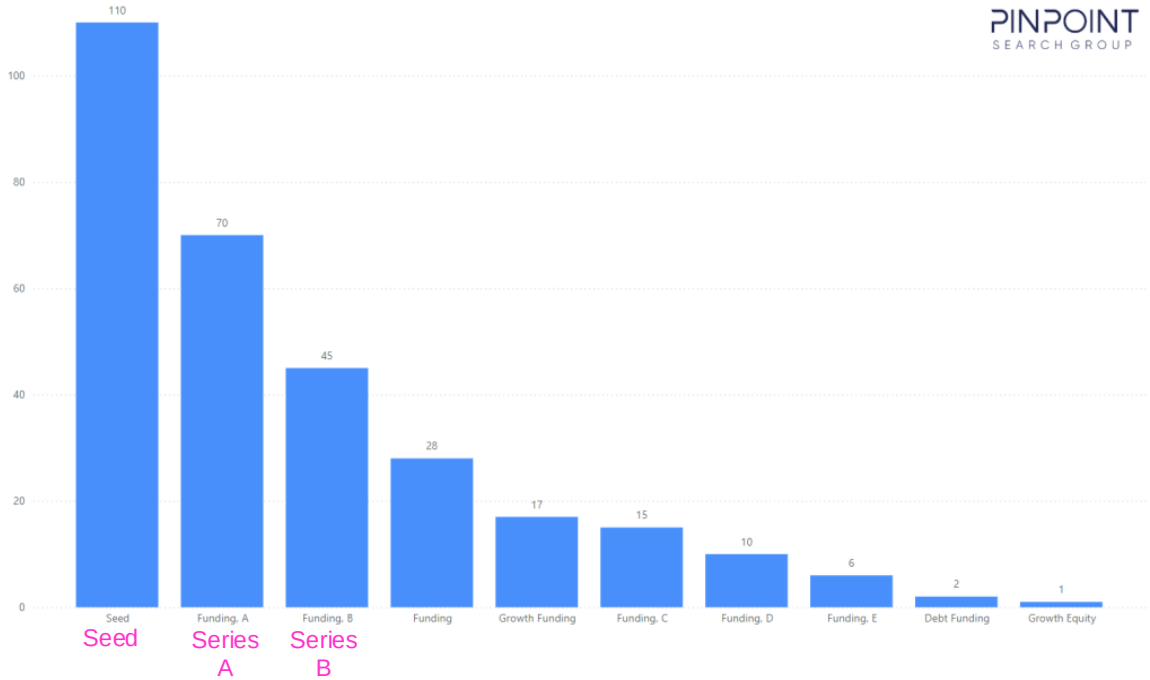
#	Companies (7.670)	Segment	Subsegment	Revenue	Total Raised ↓ $M	HQ Location
1	Broadcom (General Purpose Semiconductor...	Endpoint Security	Endpoint Protection, Detection and Response	47.430,03	63.099,98	Palo Alto, CA
2	Oracle (NYS: ORCL)	Identity & Access Management	Identity Governance & Administration	50.586,70	44.694,75	Austin, TX
3	Microsoft (NAS: MSFT)	Endpoint Security	Endpoint Protection, Detection and Response	234.396,22	29.666,94	Redmond, WA
4	Visa (NYS: V)	Identity & Access Management	Fraud Prevention	33.128,44	13.819,83	San Francisco, CA
5	PayPal Holdings (NAS: PYPL)	Identity & Access Management	Fraud Prevention	29.007,44	12.153,14	San Jose, CA
6	Cisco Systems (NAS: CSCO)	Network Security	Secure Networking	48.719,38	11.430,79	San Jose, CA
7	McAfee	Endpoint Security	Endpoint Protection, Detection and Response	1.623,96	11.209,76	San Jose, CA
8	Cloud Software Group	Endpoint Security	Endpoint Protection, Detection and Response	2.942,93	10.699,82	Fort Lauderdale, FL
9	Deutsche Telekom (ETR: DTE)	Security Operations	Managed Security Services	111.317,00	10.463,54	Bonn, Germany
10	Lumen Technologies (NYS: LUMN)	Security Operations	Managed Security Services	12.260,64	10.450,14	Monroe, LA
11	VMware	Network Security	Secure Networking	12.920,51	6.476,92	Palo Alto, CA
12	Accenture (NYS: ACN)	Security Operations	Managed Security Services	61.111,17	6.452,01	Dublin, Ireland
13	MasterCard (NYS: MA)	Identity & Access Management	Fraud Prevention	25.105,91	4.991,06	Purchase, NY
14	OpenText (TSE: OTEX)	Endpoint Security	Anti-Phishing Platforms	5.176,06	4.924,27	Waterloo, Canada
15	SolarWinds (NYS: SWI)	Security Operations	Log Ingestion & SIEM	723,62	4.911,12	Austin, TX
16	Epicor Software	Security Operations	Managed Security Services		3.955,97	Austin, TX
17	Flexera Software	Security Operations	Managed Security Services	244,43	3.915,20	Itasca, IL
18	BT Group (LON: BT.A)	Security Operations	Managed Security Services	23.966,29	3.735,03	London, United Kingdom
19	Infoblox	Network Security	Secure Networking	144,59	3.051,78	Santa Clara, CA
20	Flexential	Security Operations	Managed Security Services	336,43	2.893,28	Aurora, CO

https://www.thebusinessresearchcompany.com/report/cybersecurity-global-market-report / https://pinpointsearchgroup.com/2024-cyber-security-vendor-funding-report/ / Pitchbook

Financiado por la Unión Europea NextGenerationEU
Gobierno de España Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

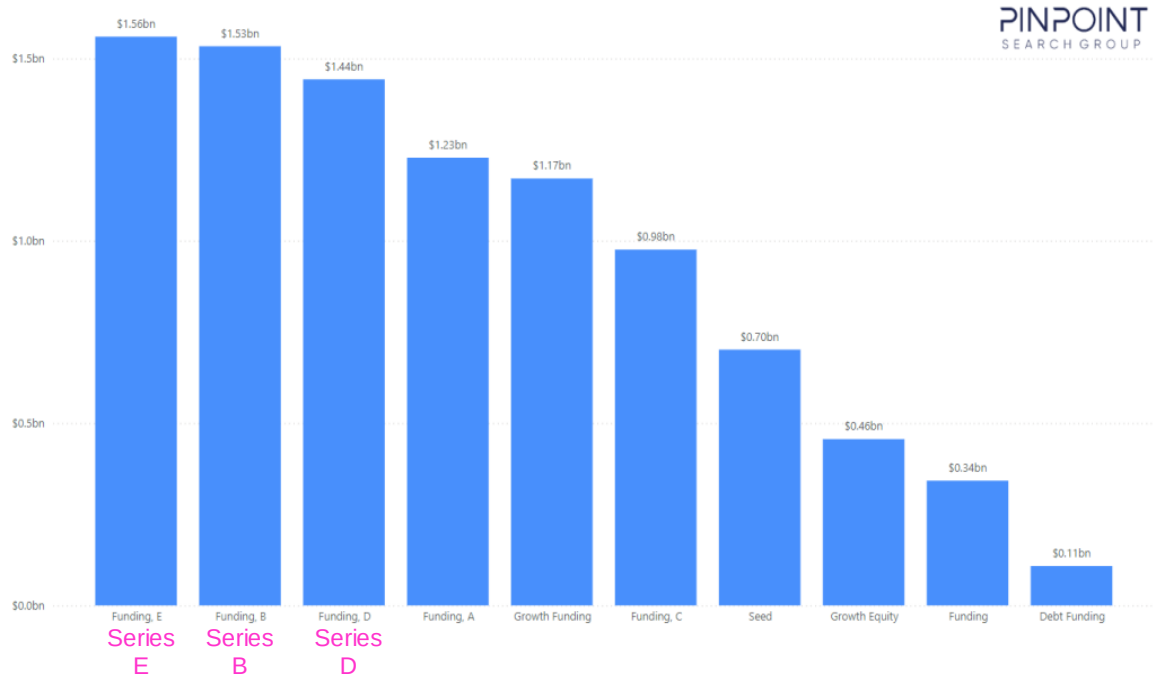
Las operaciones en etapa inicial lideran las transacciones, mientras que las empresas maduras captan la mayoría del capital de financiación

Annual number of investments by category



La **financiación en fase inicial (seed, series A) dominó en 2024** y representó el 59% del volumen total de financiación. Este hecho nos hace pensar que hay muchas startups emergentes aún no consolidadas.

Annual funding by category



Las **rondas en fase avanzada (crecimiento y series C, D, E) representaron el 54%** de todos los dólares recaudados, aunque solo representaron el 16% del volumen de financiación.

https://pinpointsearchgroup.com/2024-cyber-security-vendor-funding-report/

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Las organizaciones toman conciencia de los riesgos de ciberseguridad y aumentan su inversión

El informe *Shielding the Future: Europe's Cyber Threat Landscape* de Cloudflare, en el que se entrevistan 4.261 CISOs (Chief Information Security Officers), destaca lo siguiente:

- El **72% de las organizaciones informaron al menos de un incidente cibernético en los últimos 24 meses**, y la frecuencia de los ataques aumentó (el 84% registró más incidentes año tras año).
- Los sectores más afectados son la **informática, la energía y el transporte**, mientras que **España, Suecia y el Reino Unido** lideran la cantidad de incidentes.
- Los impactos financieros son sustanciales: el 63% de los incidentes resultaron en pérdidas superiores a los 940 000 €. En total, se estima que **los ciberataques cuestan a las empresas europeas unos 8.000 millones de euros al año**.
- A pesar de esto, **solo el 29% se siente preparado para futuros incidentes**. Las organizaciones planean invertir más en ciberseguridad, priorizando la seguridad de la fuerza laboral híbrida y las estrategias de confianza cero.

La inversión en ciberseguridad está aumentando significativamente, impulsada por el cambio hacia el trabajo remoto e híbrido tras la pandemia de COVID-19. Este cambio puso en evidencia la **necesidad de fortalecer la protección de las organizaciones**, llevando a una priorización de los presupuestos en ciberseguridad.

https://assets.ctfassets.net/slt3lc6tev37/75ElqwrRueH9MItWszjLYn/ea0b28d37bf19319605bb31c2cf0b3f0/Shielding-the-future-europes-cyber-threat-landscape.pdf

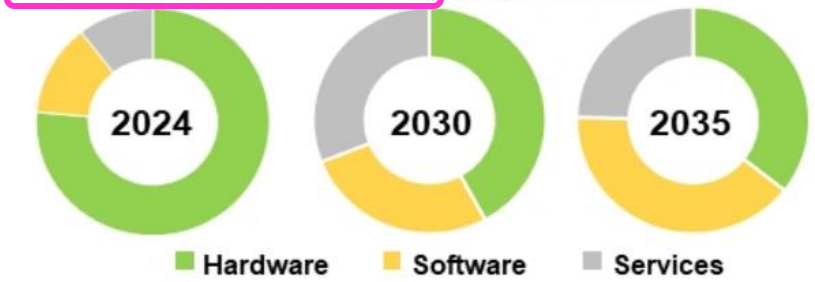
El mercado global de la ciberseguridad se puede segmentar de muchas formas

USD 215 Billion
Value in 2024

11.3% CAGR
2024 - 2035

USD 697 Billion
Value in 2035

Segment 1: Type of Component, 2024, 2030, 2035



Segment 2: Geographical Regions

Segment 3: Deployment Mode

This segment presents the market across:

- On-premises
- Cloud
- Hybrid

Segment 4: Solution Type

This segment presents the market across:

- Identity and Access Management
- Antivirus / Antimalware
- Intrusion Detection Systems / Intrusion Prevention Systems
- Security Information, Log Management and Event Management
- Firewall
- Encryption and Tokenization
- Compliance and Policy Management
- Patch Management
- Other Solutions

Segment 5: End-user

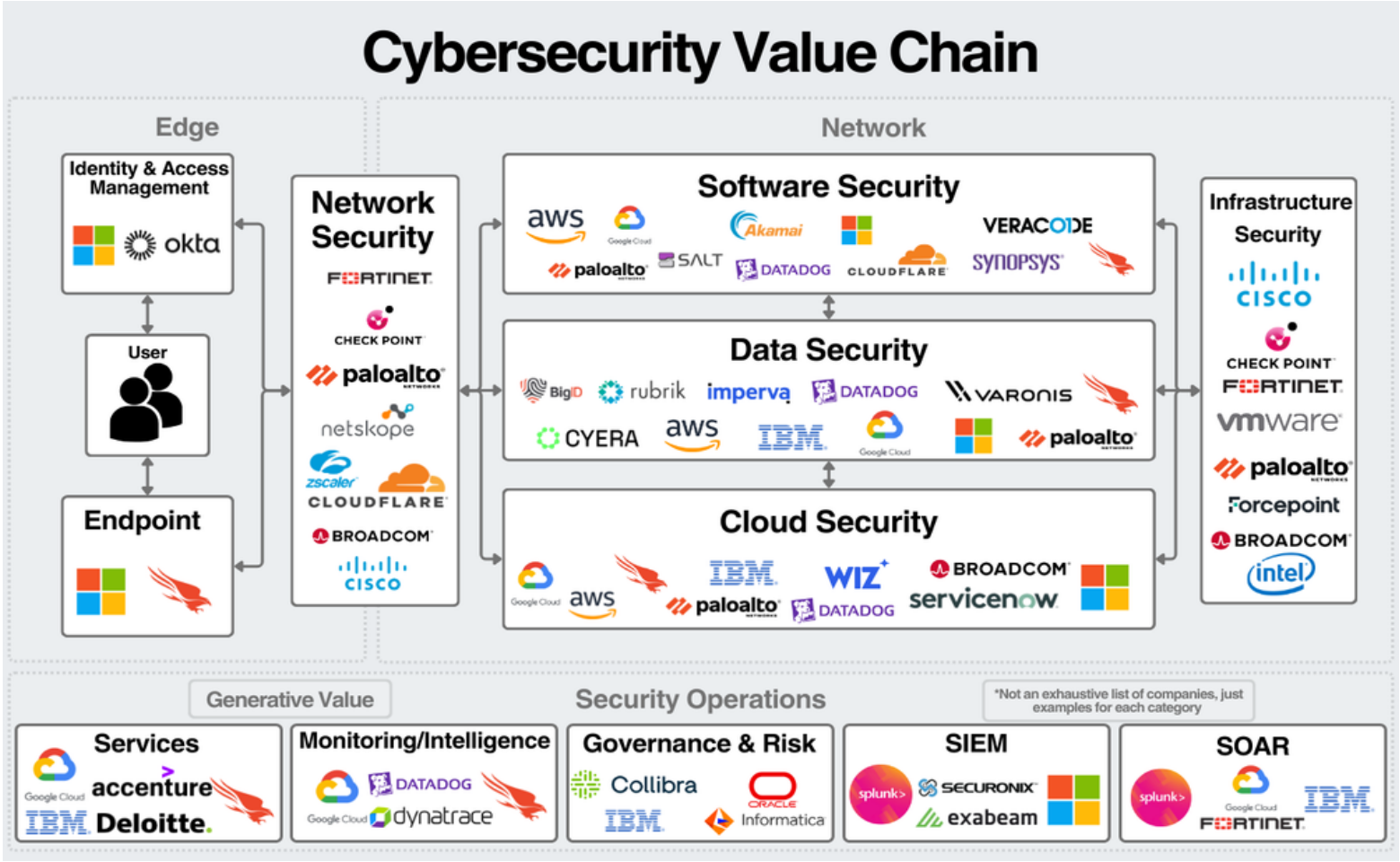
This segment presents the market across:

- Government / Defense
- BFSI
- Healthcare
- Aerospace
- Retail and eCommerce
- Energy and Utilities
- Telecommunication
- Transportation and Logistics
- Media and Entertainment
- Other End-users

https://www.rootsanalysis.com/cyber-security-market

La metodología “Zero-Trust” asume que ningún dispositivo o red es seguro

- Las empresas utilizan métodos de **defensa en profundidad** para tener **muchas capas de defensa**.
- Si una capa de defensa se ve comprometida (un firewall, por ejemplo), una amenaza tendrá que enfrentarse a otras medidas de seguridad (otros firewalls, cifrado, seguridad de acceso, seguridad en la nube, seguridad de software, seguridad física) para obtener acceso a los recursos protegidos.
- Dado que los datos se intercambian constantemente entre estos segmentos, estos **deben estar estrechamente integrados para crear un entorno seguro**.



Modelo de la segmentación de la ciberseguridad 2024 (Fuente: Eric Flaningam)

https://blog.publiccomps.com/cybersecurity-industry-primer/

Tendencia 1
Arquitectura de *Zero Trust* (confianza cero)

Las organizaciones están adoptando modelos de seguridad que no confían automáticamente en ninguna entidad, verificando continuamente la identidad y el contexto de los usuarios y dispositivos.

Más del 80% de todos los ataques implican el uso o mal uso de credenciales en la red. (Fuente: CrowdStrike)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Tendencia 2
Seguridad en redes 5G e IoT

La expansión de la tecnología 5G y el Internet de las Cosas incrementa la superficie de ataque, requiriendo medidas de seguridad más robustas.

Se estima que para 2025 habrá más de 75 mil millones de dispositivos IoT conectados en todo el mundo. (Fuente: IHS)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://electronics360.globalspec.com/article/6551/75-4-billion-devices-connected-to-the-internet-of-things-by-2025

Tendencia 3
Aumento de la necesidad de seguridad en la nube

A medida que las organizaciones migran a la nube, es crucial abordar desafíos como configuraciones erróneas y accesos no autorizados mediante cifrado, controles de acceso y monitoreo continuo para proteger datos y cumplir normativas.

El 61% de las organizaciones informaron haber sufrido al menos un incidente de seguridad en la nube en el 2024, comparado con el 24% del año anterior. (Fuente: Check Point)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.checkpoint.com/resources/items/cloud-security-report-2024

Tendencia 4
Técnicas avanzadas de phishing

Los ciberdelincuentes utilizan técnicas cada vez más sofisticadas para infiltrarse en las organizaciones y robar información sensible, lo que exige priorizar la formación de los empleados y la implementación de soluciones avanzadas de seguridad en correos electrónicos.

En 2023, los ataques de phishing representaron el 36% de todas las violaciones de datos en EE.UU. (Fuente: Verizon)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.techopedia.com/es/estadisticas-sobre-phishing

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Tendencia 5

Programas de gestión continua de exposición a amenazas (CTEM)

Estos programas ofrecen una alternativa proactiva a las evaluaciones tradicionales, proporcionando visibilidad en tiempo real de riesgos y vulnerabilidades en todo el ecosistema digital y físico de las organizaciones.

Se espera que para 2026, las organizaciones que prioricen sus inversiones en seguridad basándose en un programa CTEM logren una reducción de dos tercios en las violaciones de seguridad. (Fuente: Gartner)

https://www.aztechit.co.uk/blog/cyber-security-trends

Tendencia 6

Escasez de habilidades en ciberseguridad

La escasez de habilidades en ciberseguridad sigue siendo un desafío importante para las organizaciones de todo el mundo, con una brecha creciente entre la demanda y la oferta de profesionales calificados en ciberseguridad.

Se calcula que se necesitan 3,40 millones de profesionales para cubrir el déficit mundial de empleados en ciberseguridad. (Fuente: Fortinet)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.computing.es/informes/aumentan-las-brechas-de-seguridad-por-falta-de-habilidades-en-ciberseguridad/

Tendencia 7

Riesgos de ciberseguridad en el trabajo remoto

El aumento del trabajo remoto ha introducido nuevos desafíos en ciberseguridad, ya que las organizaciones deben asegurar redes y dispositivos distribuidos.

El 90% de los profesionales de TI considera que el trabajo remoto incrementa los riesgos de ciberseguridad. (Fuente: Sortlist)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.sortlist.es/datahub/reports/estadisticas-sobre-el-trabajo-remoto/

Tendencia 8

Gestión eficiente de la ciberseguridad por parte de terceros

Dado que las empresas dependen cada vez más de servicios externos, es esencial implementar controles y auditorías que aseguren la protección de datos sensibles frente a posibles vulnerabilidades en la cadena de suministro digital.

El 61% de las empresas experimentaron una brecha de datos de terceros o un incidente de ciberseguridad en 2023. (Fuente: Prevalent)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.prevalent.net/blog/2024-third-party-risk-management-study/

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública
Plan de Recuperación, Transformación y Resiliencia

Tendencia 9

Brecha de comunicación en las juntas directivas

Existe una desconexión entre los equipos de TI y las juntas directivas, lo que dificulta la toma de decisiones informadas sobre ciberseguridad.

Solo el 25% de las empresas presentan actualizaciones de seguridad informática a la junta más de una vez al año, lo que indica una falta de comunicación frecuente y efectiva en este ámbito. (Fuente: McKinsey)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/a-framework-for-improving-cybersecurity-discussions-within-organizations

Tendencia 10

Ciberataques patrocinados por estados

La ciberguerra entre naciones está en aumento, con ataques dirigidos a infraestructuras críticas, agencias gubernamentales y corporaciones multinacionales.

Entre 2022 y 2023, casi el 50% de los ciberataques lanzados por actores estatales afiliados a Rusia estuvieron dirigidos contra Ucrania. Los estados miembros de la OTAN ocuparon el segundo lugar, con el 36% de los ataques. (Fuente: Statista)

https://www.aztechit.co.uk/blog/cyber-security-trends / https://www.statista.com/topics/11808/cyber-warfare/#editorsPicks

1. **Introducción a la Ciberseguridad**
   - Conceptos básicos
   - Necesidad de mercado
2. **Oportunidad de mercado**
   - Mercado en cifras
   - Sectores y segmentación
   - Tendencias
3. **La ciberseguridad en España**
   - Panorama en España
   - Empresas del ecosistema Tech FabLab

España, el quinto país más amenazado por ciberataques en 2024

- España es el **quinto país más afectado por ataques de ransomware** en 2024, con un **aumento del 23% respecto a 2023**, según S21sec**.** Estados Unidos lidera a nivel de ataques de ransomware, seguido por Reino Unido, Alemania e Italia.
- El ransomware es un ciberataque que **bloquea el acceso a los sistemas de una empresa** al encriptar sus datos. Para liberar la información, los atacantes exigen un pago económico. Este tipo de ataque ha aumentado considerablemente en España, convirtiéndose en una amenaza creciente para las organizaciones.
- Sectores más afectados: **manufactura, consultoría y servicios**, reflejando un alcance amplio de los ataques.
- **LockBit es el grupo de ransomware más peligroso en España**, responsable de 18 ataques en un periodo reciente. Le siguen **Ransomhub** con 8 ataques y **Cactus** con 5. Estos grupos operan desde la Dark Web, usando herramientas como Telegram para coordinarse y vender software malicioso.
- **Conflictos geopolíticos**, especialmente entre Rusia y Ucrania, han intensificado los patrones de ataque en Europa. Los **grupos *hacktivistas*** vinculados a estas guerras **han dirigido sus ataques hacia gobiernos, empresas y organizaciones que apoyan a sus enemigos**.

https://cibersafety.com/espana-quinto-pais-mas-amenazado-ciberataques-2024/

Los grupos de ransomware, como LockBit, BlackCat y Hive, representan una gran amenaza, especialmente para grandes empresas e instituciones críticas.

Las 10 últimas grandes organizaciones que han sufrido ciberataques en España

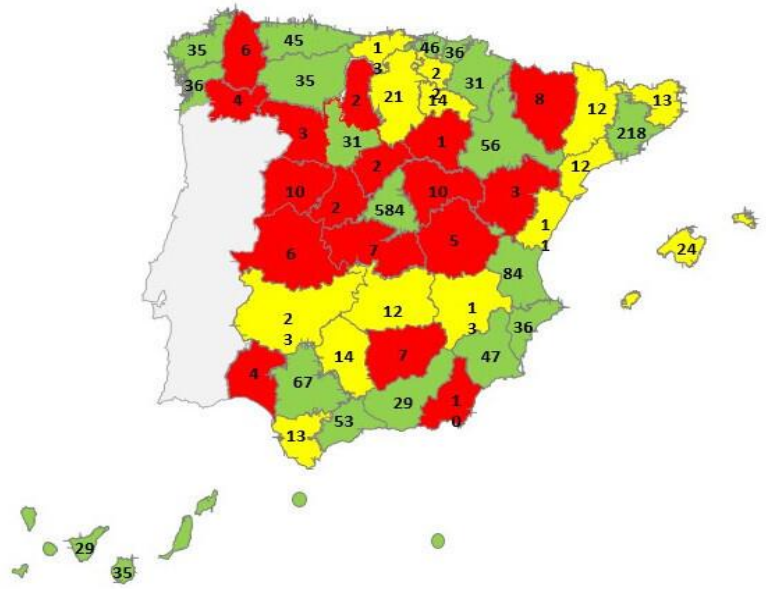
1) **Ministerio de Defensa (junio 2024):** Ransomware que comprometió datos sensibles.
2) **Indra (mayo 2024):** Los hackers robaron información confidencial.
3) **Hospital Puerta de Hierro (mayo 2024):** El ataque afectó servicios y atención a pacientes.
4) **Renfe (abril 2024):** El ciberataque causó cancelaciones y retrasos en trenes.
5) **Eulen (abril 2024):** El ransomware impactó operaciones en varios países.
6) **Amadeus (marzo 2024):** Los hackers accedieron a datos sin daños reportados.
7) **Banco Sabadell (febrero 2024):** Phishing que comprometió datos de clientes.
8) **Telefónica (febrero 2024):** El ataque interrumpió servicios de internet y telefonía.
9) **Correos (enero 2024):** Ataque DDoS que afectó servicios y web.
10) **Iberdrola (enero 2024):** Los hackers robaron datos sensibles sin afectar operaciones.

https://www.revistaciberseguridad.com/2024/07/estado-actual-de-la-ciberseguridad-en-espana/

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

En 2023 en España aumentaron los presupuestos de ciberseguridad de forma global un 5%

En un informe de Deloitte del 2023 el 58% de los CISOs indicaron que sus presupuestos habían aumentado en ese año, un 40% los mantuvieron y solo un 2% los redujeron.



Mapa de empresas que ofrecen productos y servicios en ciberseguridad por provincias en España. (Fuente: INCIBE)

Top 25 empresas españolas del sector de la ciberseguridad que han recibido financiación (Fuente: Pitchbook)

#	Companies (130)	Segment	Subsegment	Revenue	Total Raised	HQ Location	Company Financing Status
1	Gigas Hosting (MAD: GIGA)	Data Security	Data Protection & Encryption	70,77	52,00	Madrid, Spain	Formerly VC-backed
2	IriusRisk	Application Security	DevOps Security Platforms	5,95	41,10	Huesca, Spain	Venture Capital-Backed
3	Smart Protection	Identity & Access Management	Fraud Prevention	4,39	22,72	Madrid, Spain	Venture Capital-Backed
4	S2 Grupo	Endpoint Security	Endpoint Protection, Detection and Response	37,06	20,00	Valencia, Spain	Private Debt Financed
5	Qusido	Data Security	Data Protection & Encryption		17,78	Barcelona, Spain	Venture Capital-Backed
6	Lynx Tech	Identity & Access Management	Fraud Prevention		16,90	Madrid, Spain	Venture Capital-Backed
7	Revelock	Identity & Access Management	Fraud Prevention	7,10	13,81	Madrid, Spain	Formerly VC-backed
8	Nextel Engineering Systems	Security Operations	Managed Security Services	13,41	12,60	Zamudio, Spain	Formerly PE-Backed
9	Babel Sistemas De Informacion	Security Operations	Managed Security Services	220,08	8,63	Madrid, Spain	Private Equity-Backed
10	Izertis (MAD: IZER)	Security Operations	Managed Security Services	122,65	8,40	Gijon, Spain	Corporation
11	CounterCraft	Endpoint Security	Endpoint Protection, Detection and Response	1,25	8,09	Donostia-San Sebastian,...	Venture Capital-Backed
12	Cuatroochenta (MAD: 480S)	Security Operations	Managed Security Services	24,95	7,35	Castellon, Spain	Formerly Accelerator/Incubat...
13	Nymiz	Data Security	Data Protection & Encryption	0,60	7,17	Bilbao, Spain	Venture Capital-Backed
14	Blueliv	Security Operations	Log Ingestion & SIEM	6,67	6,50	Barcelona, Spain	Private Equity-Backed
15	Pridatect	Data Security	Data Privacy & Compliance	3,23	5,79	Barcelona, Spain	Corporate Backed or Acquired
16	Mobile Security Software	Data Security	Data Protection & Encryption		5,00	Huesca, Spain	Formerly VC-backed
17	Sothis	Security Operations	Managed Security Services	64,80	5,00	Paterna, Spain	Formerly PE-Backed
18	Xygeni	Application Security	DevOps Security Platforms		4,99	Valladolid, Spain	Venture Capital-Backed
19	Disruptive Consulting	Security Operations	Managed Security Services	82,41	4,00	Madrid, Spain	Private Debt Financed
20	Barbara (Network Management Software)	Endpoint Security	IoT/OT Security	1,04	3,66	Bilbao, Spain	Venture Capital-Backed
21	Entelgy	Security Operations	Managed Security Services	47,40	3,00	Madrid, Spain	Private Debt Financed
22	Ironchip	Identity & Access Management	Identity Governance & Administration	1,00	2,84	Barakaldo, Spain	Venture Capital-Backed
23	Datos 101	Data Security	Data Protection & Encryption	2,24	2,68	Madrid, Spain	Venture Capital-Backed
24	Validated ID	Identity & Access Management	Identity Governance & Administration	3,32	2,33	Barcelona, Spain	Venture Capital-Backed
25	Tranxfer	Endpoint Security	Anti-Phishing Platforms		2,00	Barcelona, Spain	Venture Capital-Backed

$M

https://www.deloitte.com/es/es/services/risk-advisory/blogs/cyber-pills/analisis-presupuesto-ciberseguridad-entidades-financieras-espana.html / Pitchbook

Empresas del ecosistema Tech FabLab

DOC EXPLOIT

- Fundación: 2021
- Localización: Logroño
- Empleados: No disp.
- https://docexploit.com/
- Descripción: Docexploit es una empresa que ayuda a proteger el software y los sistemas de las empresas. Su enfoque principal está en herramientas que analizan y detectan vulnerabilidades en el código fuente y en los contenedores de aplicaciones (entornos donde se ejecutan programas). Estas soluciones están diseñadas para prevenir posibles ataques cibernéticos y garantizar que el desarrollo de software sea seguro.

S S H {}

- Fundación: 2018
- Localización: Logroño
- Empleados: 11-50 (Crunchbase)
- https://sshteam.com/
- Descripción: Empresa dedicada a proporcionar soluciones integrales de ciberseguridad para empresas, incluyendo auditorías de seguridad, consultoría tecnológica, cumplimiento normativo (compliance), formación y concienciación en seguridad, y desarrollo de software seguro.

ABF CIBERSEGURIDAD y SISTEMAS

- Fundación: 2016
- Localización: Navarrete
- Empleados: 11-50 (Crunchbase)
- https://abfsistemas.es/
- Descripción: Ofrece servicios de ciberseguridad y sistemas TIC, como auditorías técnicas de seguridad, análisis de riesgos, monitorización de amenazas informáticas, protección del perímetro, copias de seguridad en la nube, y formación en ciberseguridad para usuarios.

mass SECURITY & TELECOM

- Fundación: 2007
- Localización: Logroño
- Empleados: 11-50 (LinkedIn)
- https://mass-security.es/
- Descripción: Empresa de seguridad integral que proporciona soluciones en videovigilancia, sistemas de alarma, ciberseguridad (análisis y auditorías, protección de datos), control de accesos, protección contra incendios, y auditoría y compliance, adaptándose a diversos sectores como industria, comercio, hoteles y hospitales.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Empresas del ecosistema Tech FabLab

inforges

- Fundación: 1978
- Localización: Valencia
- Empleados: 250-500 (Crunchbase)
- https://inforges.es/
- Descripción: INFORGES se especializa en soluciones de ciberseguridad y networking diseñadas para proteger los sistemas de las empresas. Sus servicios incluyen auditorías de seguridad, protección frente a malware y ransomware, gestión de redes seguras, y soluciones de continuidad del negocio.

480

- Fundación: 2011
- Localización: Valencia
- Empleados: +270
- https://cuatroochenta.com/
- Descripción: Cuatroochenta combina servicios de desarrollo de software en la nube y ciberseguridad. Ofrece soluciones para proteger la infraestructura tecnológica de las empresas, como análisis de vulnerabilidades, sistemas de autenticación segura y software a medida.

DATAORIGIN

- Fundación: 2024
- Localización: Valencia
- Empleados: No disp.
- https://dataorigin.es/
- Descripción: DataOrigin ofrece un buscador avanzado que organiza y personaliza la extracción de información en tiempo real desde la web. Su producto garantiza la privacidad y seguridad de los datos de sus clientes, enfocado en mantener la integridad y confidencialidad de la información. Lo que distingue a la empresa es su enfoque en la gestión eficiente de grandes volúmenes de datos con un alto nivel de seguridad.

COSMIKAL ENDURANCE

- Fundación: 2013
- Localización: Polanco
- Empleados: <10 (Expansión)
- https://www.cosmikal.es/
- Descripción: COSMIKAL ofrece una solución de seguridad integral llamada COSMIKAL ENDURANCE, diseñada para crear un espacio de trabajo remoto blindado. Este servicio se enfoca en proteger los entornos laborales frente a amenazas cibernéticas, garantizando la seguridad de la información en sistemas distribuidos.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Empresas del ecosistema Tech FabLab

- Fundación: 2012
- Localización: Santander
- Empleados: 13 (elEconomista)
- https://viacoreit.com/
- Descripción: Viacore IT se especializa en consultorías e implementación de medidas de ciberseguridad, ayudando a empresas a proteger sus activos digitales mediante soluciones personalizadas y alineadas con las normativas de seguridad.

- Fundación: 2022
- Localización: Tudela
- Empleados: 2 (2023) (eInforma)
- https://meta-data.es/
- Descripción: META DATA ofrece servicios de ciberseguridad como servicio (SECaaS), incluyendo auditorías de TI, pruebas de intrusión avanzadas, gestión de vulnerabilidades, auditorías de seguridad e investigación forense. También proporcionan servicios de cumplimiento legal y normativo, como GDPR y planes directores de ciberseguridad.

- Fundación: 2023
- Localización: Pamplona
- Empleados: 1-10 (Crunchbase)
- https://www.zaindari.com/
- Descripción: ZAINDARI ofrece una solución de control parental que actúa directamente sobre la red, proporcionando supervisión integral de todos los dispositivos conectados, tanto dentro como fuera del hogar. Permite establecer límites de tiempo, filtrar contenido inapropiado y proteger contra amenazas cibernéticas, garantizando un entorno digital seguro para las familias.

- Fundación: 2012
- Localización: Pamplona
- Empleados: 180
- https://veridas.com/en/
- Descripción: VERIDAS es una empresa especializada en soluciones de verificación de identidad digital y autenticación biométrica, incluyendo reconocimiento facial y de voz. Sus productos permiten a las organizaciones verificar identidades de manera segura y eficiente, mejorando la experiencia del usuario y garantizando altos estándares de seguridad.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia

Empresas del ecosistema Tech FabLab

AraSafe Ciberseguridad

- Fundación: 2022
- Localización: Zaragoza
- Empleados: 10
- https://arasafe.es
- Descripción: Arasafe ofrece servicios especializados como auditorías de ciberseguridad, pruebas de hacking ético, monitorización de amenazas, gestión de vulnerabilidades, protección contra pérdida de datos (DLP) y cumplimiento normativo. Su enfoque está en personalizar soluciones para proteger la información y garantizar la seguridad digital de sus clientes.

SIQURË

- Fundación: 2017
- Localización: Zaragoza
- Empleados: 1-10 (Crunchbase)
- https://www.siqure.es/
- Descripción: SIQURË ofrece servicios integrales en protección de datos personales, seguridad de la información, compliance y canales de denuncias, igualdad para empresas, seguridad global, asesoría legal y legaltech, y gestión de la formación. Su enfoque abarca desde la elaboración de planes de seguridad hasta la implementación de sistemas de gestión y formación especializada.

cibergob

- Fundación: 2016
- Localización: Zaragoza
- Empleados: No disp.
- https://www.cibergob.es/
- Descripción: Cibergob se especializa en la gestión ágil de la ciberseguridad, ayudando a organizaciones públicas y privadas a integrar y gobernar su ciberseguridad para garantizar la protección de datos. Ofrecen servicios para empresas y sector público, incluyendo cumplimiento del Esquema Nacional de Seguridad (ENS) y el Reglamento General de Protección de Datos (RGPD).

BALUSIAN

- Fundación: 2015
- Localización: Zaragoza
- Empleados: 1-10 (Crunchbase)
- https://www.balusian.com/es/
- Descripción: Balusian ofrece servicios de consultoría en ciberseguridad, ética en inteligencia artificial y gestión de riesgos y cumplimiento, atendiendo a organizaciones públicas y privadas a nivel nacional e internacional.

Fuente: TBBC Medium

Empresas del ecosistema Tech FabLab

- Fundación: 2022
- Localización: Barcelona
- Empleados: No disp.
- https://axeliacybersecurity.com/
- Descripción: Axelia se especializa en ofrecer soluciones avanzadas de ciberseguridad diseñadas para startups y pymes. Sus servicios incluyen auditorías de seguridad, simulaciones de ciberataques y seguridad gestionada, con el objetivo de proteger a las empresas de amenazas digitales. Además, proporcionan servicios de seguridad ofensiva (ethical hacking), gestión de vulnerabilidades, gestión de riesgos de seguridad de la información, cumplimiento normativo (ISO 27001, GDPR), desarrollo seguro (DevSecOps) y gestión de incidentes.

- Fundación: 2014
- Localización: Barcelona
- Empleados: 62 (Pitchbook)
- https://ackcent.com/
- Descripción: Ackcent es una empresa especializada exclusivamente en ofrecer servicios y soluciones de ciberseguridad. Su misión es ayudar a los clientes a proteger sus activos digitales críticos mediante una cartera de servicios profesionales especializados. Con sede en Barcelona, Ackcent adapta sus soluciones a las necesidades particulares de ciberseguridad de cada cliente, garantizando la calidad y el éxito de cada proyecto.

- Fundación: 2023
- Localización: Barcelona
- Empleados: 4 (Pitchbook)
- https://www.allpriv.com/
- Descripción: AllPriv es una empresa innovadora en ciberseguridad que utiliza tecnologías avanzadas como IA descentralizada y blockchain para proteger dispositivos y redes. Su producto principal, Cyber-Brick, protege equipos médicos y empresariales mediante una red privada encriptada que detecta y responde a amenazas en tiempo real. Además, ofrecen soluciones para asegurar el teletrabajo, protegiendo dispositivos remotos frente a ataques y brechas de datos.

- Fundación: 2022
- Localización: Barcelona
- Empleados: 2 (Picthbook)
- https://www.asperis.es/
- Descripción: Asperis Security es una empresa especializada en ciberseguridad que ofrece soluciones para proteger los activos digitales de las organizaciones. Sus servicios incluyen pruebas de intrusión (pentesting), auditorías de código fuente y aplicaciones web, gestión de eventos de seguridad (SIEM), y servicios como CISO y SOC externos. Además, destacan en peritaje informático y consultoría estratégica en ciberseguridad. Con un enfoque directo y efectivo, ayudan a las empresas a prevenir amenazas y garantizar la seguridad de sus sistemas e información.

Fuente: TBBC Medium

TECH FAB LAB

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

La Rioja

GOBIERNO DE ARAGON

Gobierno de Navarra

Nafarroako Gobernua

GOBIERNO de CANTABRIA

GENERALITAT VALENCIANA

Generalitat de Catalunya

Informe elaborado por WORSLEY ACCELERATION SERVICES