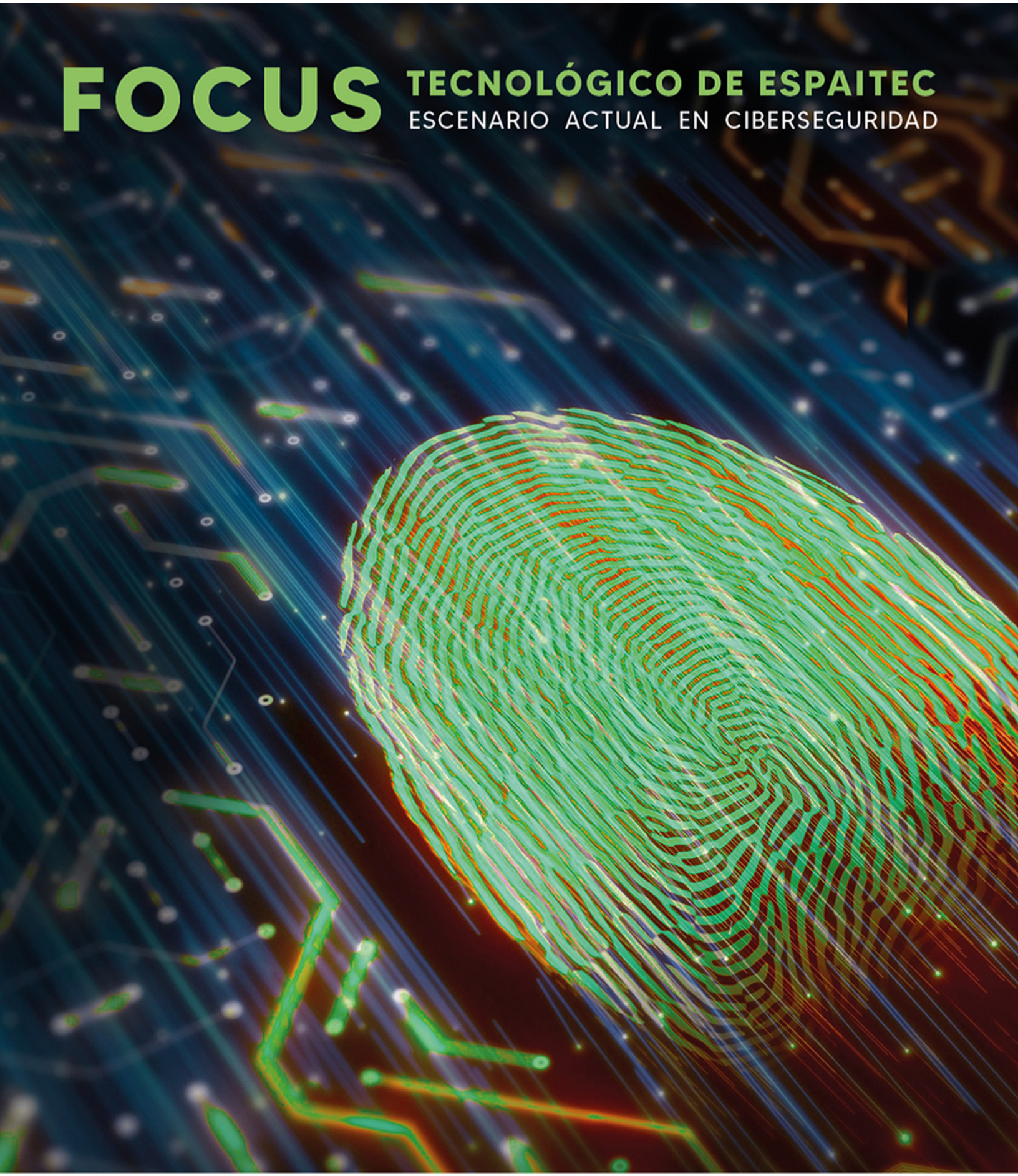
FOCUS TECNOLÓGICO DE ESPAITEC

ESCENARIO ACTUAL EN CIBERSEGURIDAD



UNIVERSITAT JAUME I
Fundació General · FUGEN

espaitec
Parc Científic i Tecnològic

GENERALITAT VALENCIANA
Conselleria d'Innovació, Indústria, Comerç i Turisme

Development /
iale TECNOLOGÍA

CONTENIDOS

Introducción

Objetivo del Informe

El presente estudio de *Vigilancia Tecnológica e Inteligencia Competitiva* tiene por objetivo mostrar un panorama de los últimos avances tecnológicos y la situación a nivel competitiva y de mercado en relación al ámbito de la **Ciberseguridad**.

Metodología de Investigación

Para la realización de este estudio **IALE Tecnología** ha usado herramientas propias de búsqueda y monitoreo de la información y herramientas open source de análisis estadístico y ciencia de datos, que incluyen librerías y algoritmos de Aprendizaje Automático (ML), Procesamiento del Lenguaje Natural (NLP), así como herramientas para la visualización.

Inicialmente se ha realizado un estudio de los principales desarrollos tecnológicos a partir de **información de Patentes**, obtenida mediante la consulta a bases globales de patentes de las principales oficinas de PI en el mundo: Patentscope, de la OMPI, la Oficina Mundial de la Propiedad Industrial; Espacenet, de la EPO, la Oficina Europea de Patentes y la bases de datos a texto completo de la USPTO, la Oficina de Patentes de los Estados Unidos.

La información de patentes revela aspectos estratégicos relacionados con la identificación de actores que están actualmente destinado recursos de I+D a proteger nuevas tecnologías e invenciones en este ámbito y, por tanto, pueden desarrollar potencialmente productos que incorporen esas tecnologías al mercado en unos años; asimismo el análisis de los contenidos tratados en las patentes permite detectar temas de interés y su evolución, si éstos son sostenidos en el tiempo o emergentes.

Estrategia general de busqueda

El ámbito de búsqueda se focalizó en los desarrollos e invenciones en Ciberseguridad publicadas en los últimos 6 años (desde el año 2019 hasta 2024[1]).

[1] datos de 2024 incompletos

Las búsqueda se configuró a partir de conceptos clave asociados genéricamente con la ciberseguridad y con las principales tipologías de ciberataques, junto con clasificaciones de patentes asociadas -se usó en particular la versión más actualizada de la Clasificación Internacional, la *Clasificación Cooperativa de Patentes* o *CPC*[2], que integra las clasificaciones de las Oficinas de la Propiedad Industrial Europea (EPO) y de Estados Unidos (USPTO)- que ayudaron a acotar los ámbitos tecnológicos abarcados:

> *cybersecurity OR "cyber security" OR "cyber attack" OR cyberattack? OR "denial-of-service attack" OR "DoS attack" OR "distributed denial-of-service" OR "DDoS attack" OR "Replay attack" OR "Man-in-the-Middle" OR MitM OR "Cross-site scripting" OR phishing OR malware OR ransomware OR "SQL injection attack" OR "Insider threads" OR "advanced persistent threads" OR "IP spoofing" OR "eavesdropping attack" OR "password attack" OR "password spraying" OR "cyber vulnerability" OR "cyber fraud" OR "session hijacking" OR "DNS attack" OR "data breach" OR "data theft" OR cyberincident? OR "cyber incident" OR cyberthreat? OR "cyber threat" OR cyberdefense OR "cyber defense" OR "Trusted execution environment" OR "Privacy-preserving technologies" OR "Deception Technologies"*

Se tuvieron en cuenta específicamente los siguientes códigos de clasificación de patentes (CPCs):

- H04L63 - *Network architectures or network communication protocols for network security (cryptographic mechanisms or cryptographic arrangements for secret or secure communication H04L9/00; network architectures or network communication protocols for wireless network security H04W12/00; security arrangements for protecting computers or computer systems against unauthorised activity G06F21/00)*
- G06F 21 - *Security arrangements for protecting computers, components, programs or data against unauthorised activity*
- G06F 2221 - *Indexing scheme relating to security arrangements for protecting computers, components, programs or data against unauthorised activity*
- H04L 9 - *Cryptographic mechanisms or cryptographic arrangements for secret or secure communications; Network security protocols*
- G06F 16 - *Information retrieval; Database structures therefor; File system structures*
- G06N20 - *Machine learning*
- G06F 9 - *Arrangements for program control, e.g. control units (program control for peripheral devices G06F13/10)*
- G06N 3 - *Computing arrangements based on biological models*
- H04L41 - *Arrangements for maintenance, administration or management of data switching networks, e.g. of packet switching networks*
- G06N 5 - *Computing arrangements using knowledge-based models*

Periodo estudiado: 2019-2024 (datos del último año incompletos)

[2] https://www.epo.org/en/searching-for-patents/helpful-resources/first-time-here/classification/cpc

Alcance y Limitaciones

El presente trabajo ha usado la metodología de la Vigilancia Tecnológica para obtener una visión general y sistemática de los desarrollos tecnológicos en el ámbito de la ciberseguridad.

En una primera aproximación, se ha partido de información de patentes. La búsqueda realizada ha permitido encontrar todas las invenciones registradas por este medio en los últimos seis años (2019-2024) asociadas a aspectos relacionados con la Cibersecuridad y a partir de ellas se han podido identificar a los principales actores y áreas de aplicación. Este enfoque permite identificar de forma sistemática a las empresas que destinan recursos de I+D y que por tanto, contemplan como prioritario en su estrategia la protección de su Propiedad Industrial.

Sin embargo este enfoque no es, por sí solo, exhaustivo a la hora de identificar todos y cada uno de los actores involucrados en este sector, puesto que no todas las empresas que operan en el ámbito de la ciberseguridad patentan sus desarrollos. Muchas de ellas, por el contrario, son pymes centradas en desarrollos especificos de software que en muchos casos no son patentados.

Es por ello, que en la segunda parte del informe se complementan los primeros hallazgos obtenidos, incorporando otras fuentes de información secundarias, tales como prensa especializada, informes de mercado, estudios de consultoras especializadas y otras fuentes disponibles de forma distribuida en internet, para completar de este modo la visión general del mercado y de los principales actores en el ámbito de la ciberseguridad.

Panorama tecnológico

Primeros resultados

Los resultados de la búsqueda han permitido identificar a los principales actores y áreas de aplicación.

A partir de la búsqueda se obtuvieron un total de **12409 solicitudes de patente** y **3966 patentes concedidas** publicadas durante los últimos 6 años.

Tendencias

El recuento del número de patentes -agrupadas por familias (todos los documentos asociados a una misma invención)- publicadas en los últimos 5 años completos muestra una clara evolución creciente, que deja constancia del interés suscitado y de los esfuerzos crecientes en R+D y protección de nuevas tecnologías al respecto.

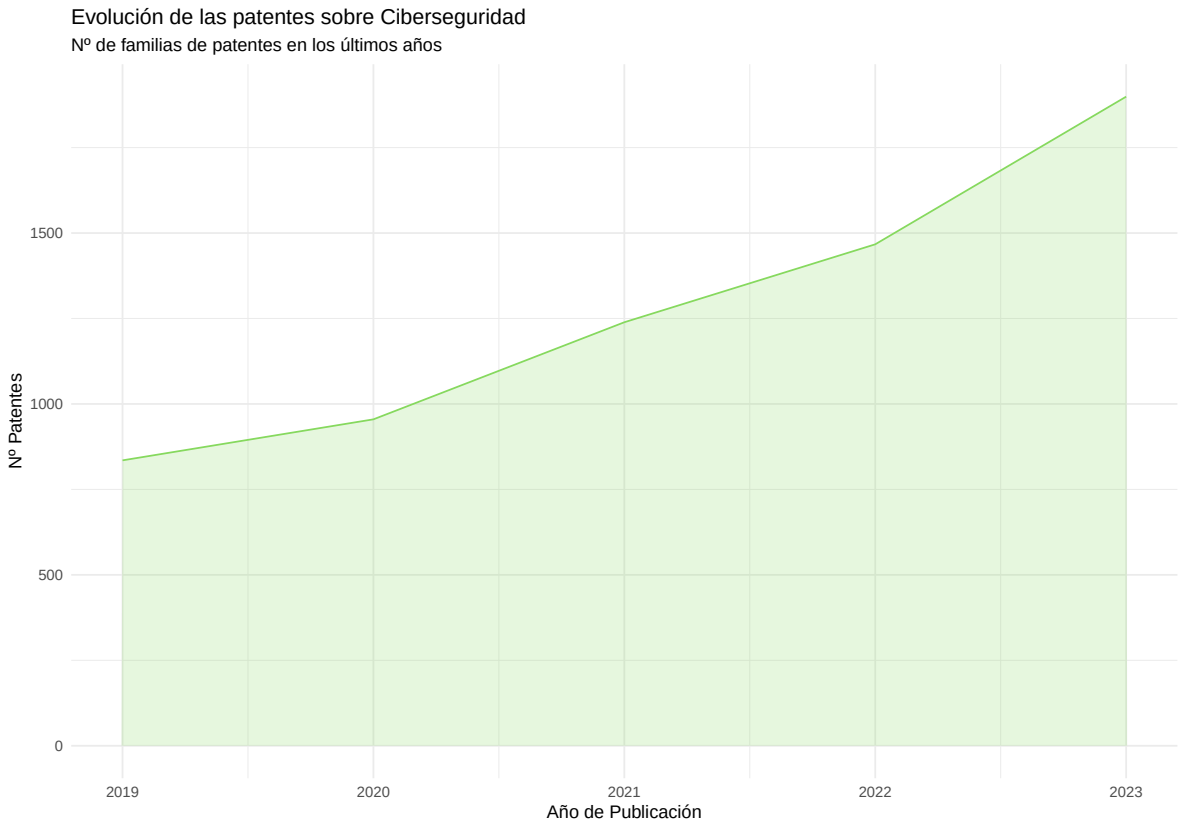


Figura 1: Evolución de las patentes sobre Ciberseguridad

Principales players

Las principales instituciones (empresas y centros de investigación) con desarrollos e invenciones protegidas por medio de patentes en Ciberseguridad son:

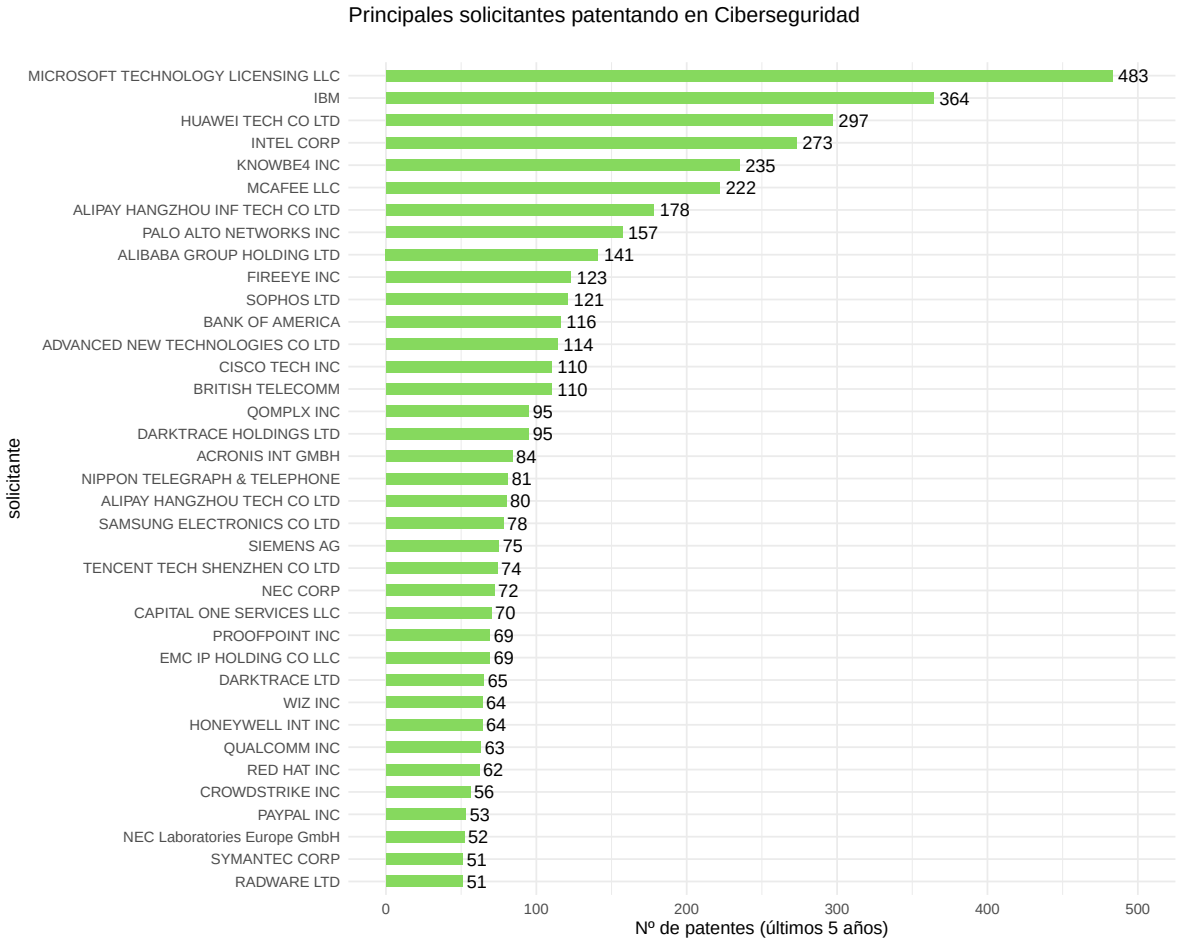


Figura 2: Principales solicitantes

Microsoft, una de las mayores empresas de sofware del mundo con 211 mil millones de USD en ingresos anuales e **IBM**, la otra compañía tecnológica norteamericana para la que la ciberseguridad es también una de sus prioridades estratégicas de innovación, lideran el rankin de actores.

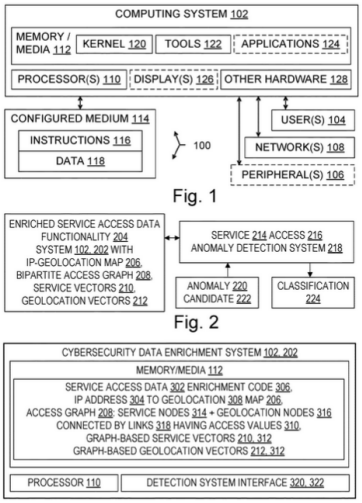


Figura 3: Patente de Microsoft: US11647034B2, Service access data enrichment for cybersecurity

Encontramos asimismo grandes empresas especializadas en cibersecuridad, tales como **Palo Alto Networks**, **McAfee**, **Sophos**, **FireEye** y **CrowdStrike** así como la plataforma de análisis y gestión de riesgos de **Qomplx** o la empresa de seguridad en la nube con sedes en New Jersey y Tel Aviv **Radware**; empresas de telecomunicaciones tales como **Huawei**, **British Telecom** o **Nippon Telegraph** y empresas de servicios financieros tales como **Bank of America** o **Capital One**, entre otras.

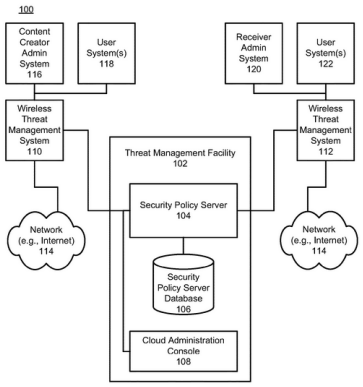


Figura 4: Patente de Sophos Ltd: US11683350B2, System and method for providing and managing security rules and policies

Entre los actores asiáticos, aparte de **Huawei**, que es el primer titular chino, destaca el grupo corporativo chino **Alibaba** que patenta bajo los nombres de titular: *Alibaba group*, *Alipay Hanghzou* y *Alipay Inf Hangzhou*.

Nowbe4 https://www.knowbe4.com, una empresa de Florida especializada en soluciones de formación en ciberseguridad y ciber-resiliencia para empresas y organizaciones, aparece también ocupando una posición destacada con un considerable número de invenciones patentadas en el periodo estudiado.

En Europa, destacan la suiza **Acronis** y la alemana **Siemens**.

Principales centros de investigación con desarrollos patentados

La **Universidad de Xidian** es el centro de investigación con más invenciones patentadas (37) en ciberseguridad; la Universidad de Zhejiang le sigue (29 patentes); la tercera institución de investigación en cuanto a registro de patentes es el KAIST Coreano (22); siguen otras universidades chinas como la de Shanghai Jiaotong y la Universidad del Sudoeste de China (con 21 respectivamente); el primer centro de investigación del continente norteamericano es el Battelle Memorial Institute (20).

Evolución de la actividad de los principales actores en los últimos años

El análisis de la evolución en el patentamiento de los principales titulares muestra como **Qualcomm** y la británica especializada en ciberseguridad apoyada con IA, **Darktrace Holdings** han incrementado significativamente su actividad en años recientes.

Alibaba, **Advanced New Technologies** o **Fireeye**, en cambio, cesan su actividad de patentamiento en años más recientes.

Figura 5: Evolución de los principales solicitantes

Wiz Inc https://www.wiz.io, startup de seguridad en la nube con sede en Nueva York, que ha alcanzado una valoración 10 mil millones de USD [1] y a quien Google tiene intención de adquirir [2], destaca como player emergente en los últimos dos años.

[1] https://pitchbook.com/news/articles/wiz-series-d-cybersecurity
[2] https://techcrunch.com/2024/07/14/google-reportedly-in-talks-to-acquire-cloud-security-company-wiz-for-23b

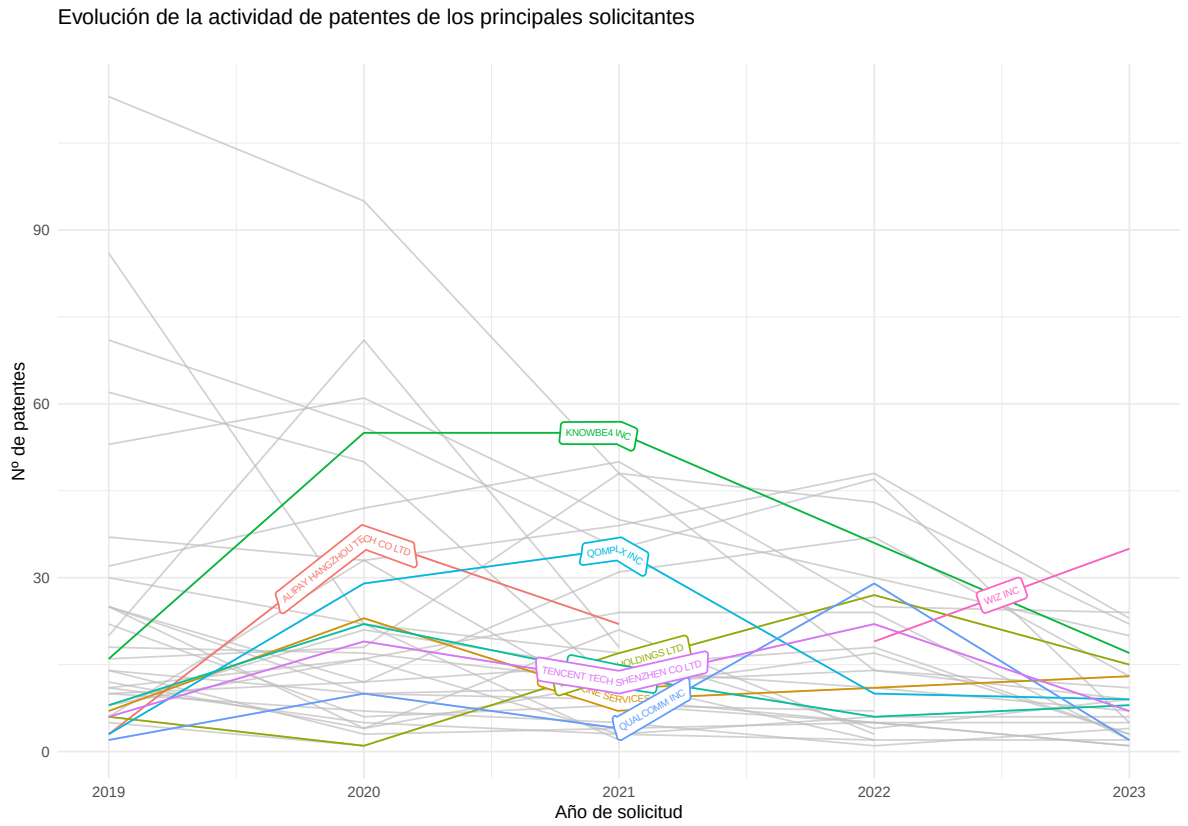


Figura 6: Evolución de los principales solicitantes

Principales países

En cuanto a los países donde se protege la tecnología, Estados Unidos -con más de 6000 patentes sobre ciberseguridad publicadas en el periodo estudiado, según nuestra búsqueda- es el país líder en número de invenciones protegidas, seguido de China (más de 5000). Recuperamos asimismo más de 1000 solicitudes internacionales (WO) registradas por via PCT (tratado de cooperación en materia de patentes) y casi 700 solicitudes para alcanzar la protección en la región europea. Otras jurisdicción importante es Corea del Sur (771 patentes).

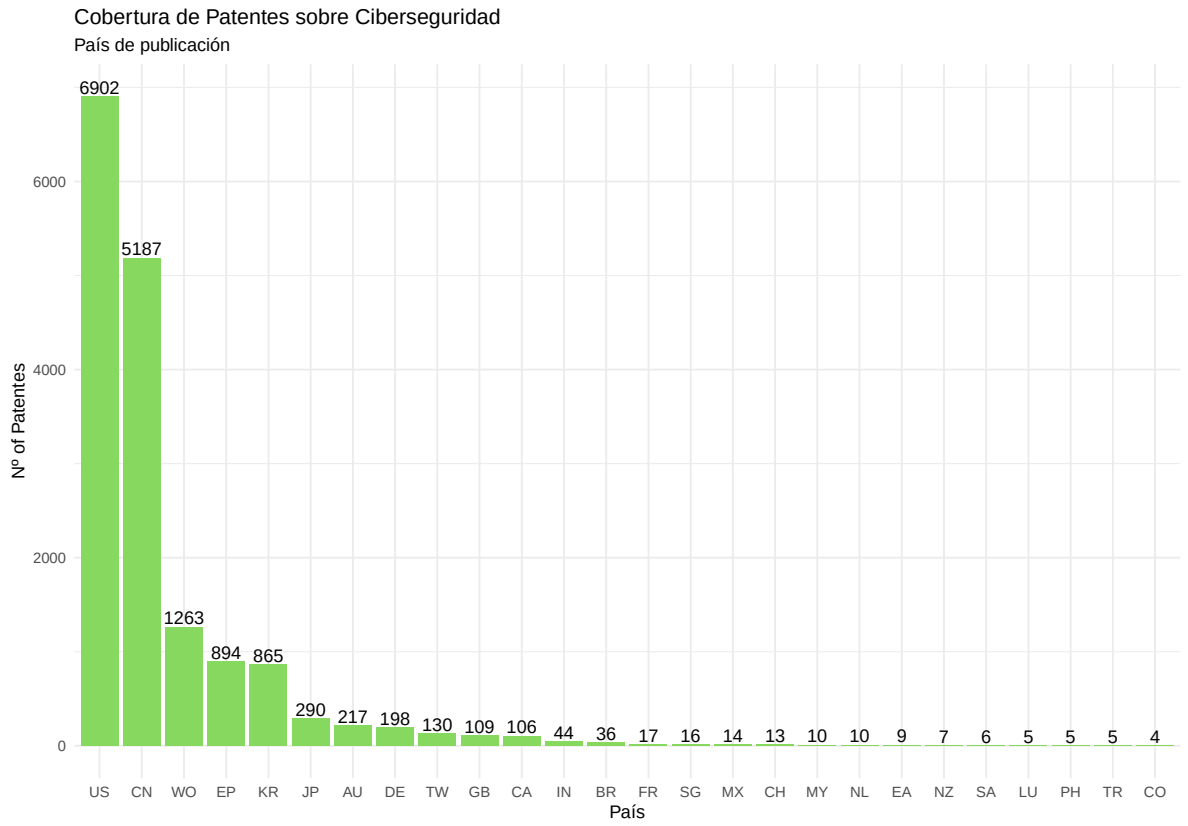


Figura 7: Principales países

Principales titulares españoles

En España, han patentado desarrollos en el ámbito de la ciberseguridad grandes empresas como **Telefonica** (que es el líder en número de invenciones patentadas), el **BBVA**; **Ge Renovables** o **Seat**.

Encontramos también empresas especializadas en ciberseguridad como **Gmv** con aplicaciones en IoT con IA; **Multiverse Computing**, AI inspirada en la cuántica; la alavesa **Alias Robotics**, especializada en seguridad robótica para empresas; **Wise Security Global** con sede en Madrid, que ofrece varias soluciones avanzadas de ciberseguridad; la consultora de Santander **Neuprotel** que desarrolla métodos de verificación y validación de usuarios.

Otras empresas españolas con patentes en el periodo estudiado son: **Arppa Tech**, en sistemas de asistencia remotos; **Tecteco**, que desarrolla métodos de identificación multifactor con datos biométricos (solución *Wefender*), **Koa Health** y **Neurologyca**, en el ámbito del monitoreo de la salud; la consultora **NTT Data** que trabaja en métodos seguros de transacción de datos; **Virustotal**; **Egarante**, con aplicaciones en el ámbito legal; Baintex y Dormakaba en

sistemas de protección de comunidades de vecinos e Italoiberica, en sistemas de seguridad para túneles y carreteras.

En cuanto a **centros de investigación y centros tecnológicos** con desarrollos patentados en España se identifica a la **Universidad de Vigo** -que en ocasiones colabora con el centro de I+D gallego **Gradiant**- como el principal titular, con varias invenciones patentadas en el periodo estudiado en métodos de encriptación de claves seguras (US11336442B2).

Otras Universidades como la Universidad de León, la Universidad de Sevilla, la de Alcalá Henares, la de Lleida, la Autónoma y la Politécnica de Madrid, la de Murcia, la de Oviedo, la UPC y la UPV. Francesc Guim Bernat, Investigador de La UPC, aparece como titular de varias patentes. Asimismo, encontramos patentes también de centros tecnológicos como Tecnalia (métodos de anonimización de logs de eventos, EP4235474A1), el Instituto Imdea Software de Madrid o el CTAG (Centro Tecnológico de Automoción de Galicia).

Principales áreas tecnológicas

Las clasificaciones de patentes permiten la identificación de principales subáreas tecnológicas en desarrollo dentro de la Ciberseguridad.

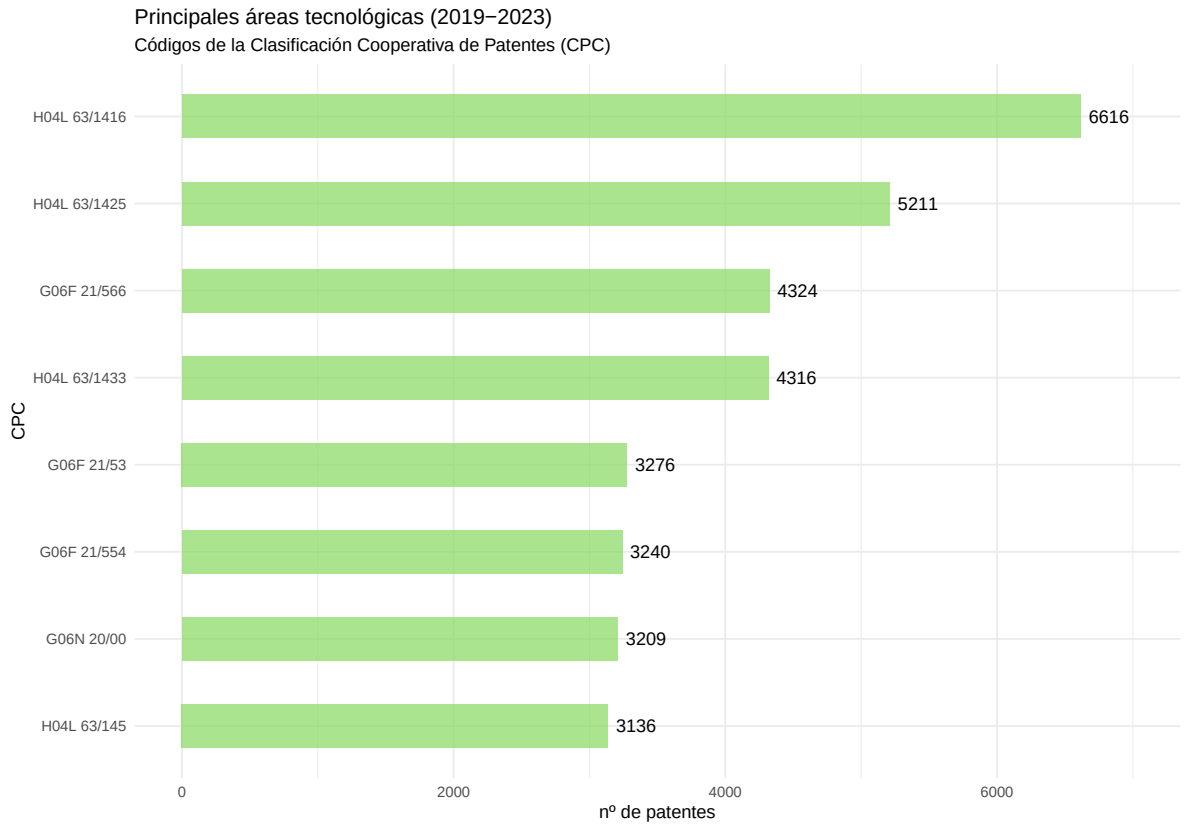


Figura 8: Principales áreas tecnológicas

Las principales se relacionan con:

- H04L 63/1416 *Event detection, e.g. attack signature detection*
- H04L 63/1425 *Traffic logging, e.g. anomaly detection*
- G06F 21/566 *Computer malware detection performed at run-time, e.g. emulation, suspicious activities*
- H04L 63/1433 *Vulnerability analysis*

La detección de eventos con **enfoques basado en firmas** (*attack signature detection*), a pesar de sus limitaciones, sigue siendo el área de mayor peso en las soluciones reivindicadas en los últimos años; se trata de un enfoque de ciberseguridad que identifica amenazas conocidas comparándolas con una base de datos de firmas predefinidas.

Son importantes asimismo otros sistemas de detección de anomalías, las emulaciones de actividades sospechosas y los análisis de vulnerabilidad.

Otras áreas relevantes son las **máquinas virtuales seguras** o ***sandboxes*** y el **aprendizaje automático**:

- G06F 21/53 *sandbox or secure virtual machines*
- G06F 21/554 *Detecting local intrusion or implementing counter-measures involving event detection and direct action*
- G06N 20 *Machine Learning*
- H04L 63/145 *Countermeasures against malicious traffic attacks involving the propagation of malware through the network, e.g. viruses, trojans or worms*

Por ejemplo, una patente de **Intel** (US12113902B2), otorgada a principios de octubre protege métodos de verificación escalable en un entorno confiable.

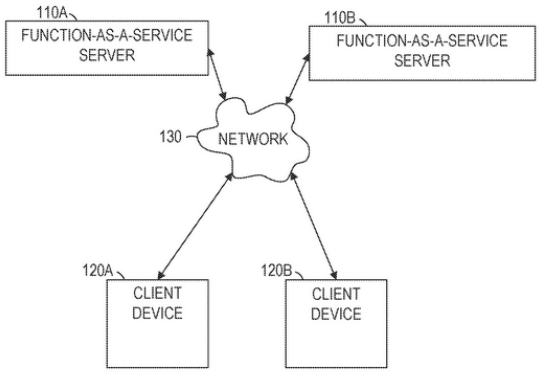


Figura 9: Patente de Intel: US12113902B2, Scalable attestation for trusted execution environments

La empresa de ciberseguridad basada en IA **Darktrace** -recientemente adquirida por la empresa de capital riesgo **Thoma Bravo** por 5.300 millones de dólares [3]- está más centrada en redes de conmutación de paquetes.

Intel, por su parte, focaliza sus desarrollos en unidades de control, mientras que **Knowbe4** destaca en computación basado en modelos biológicos (el área de aplicación asociada a la IA).

Tanto **Knowbe4** como **Darktrace** están trabajando en patentes sobre seguridad de correo electrónico. Asi por ejemplo, en 2022 se concedió una patente a Knowbe4 para un sistema que descubre mensajes peligrosos y alerta a los usuarios (US11343276B2).

[3] https://www.thomabravo.com/press-releases/thoma-bravo-completes-acquisition-of-darktrace

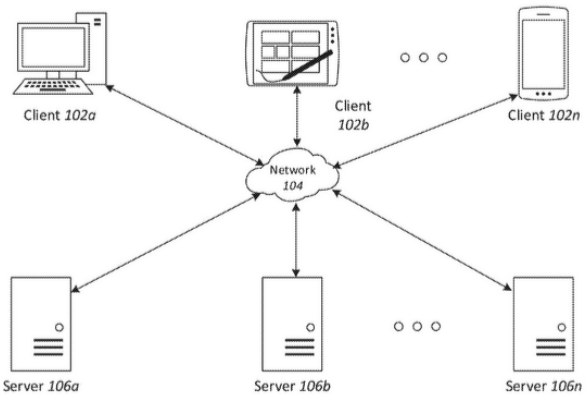


Figura 10: Patente de KNOWBE4 INC: US11343276B2, Systems and methods for discovering and alerting users of potentially hazardous messages

Evolución de las áreas tecnológicas

Observando detalladamente la evolución de las áreas tecnológicas podemos clasificarlas por aquéllas que muestran un interés sostenido en el tiempo, aquellas que emergen en los últimos años (sin apenas actividad previa) y aquéllas que muestran cierto decrecimiento:

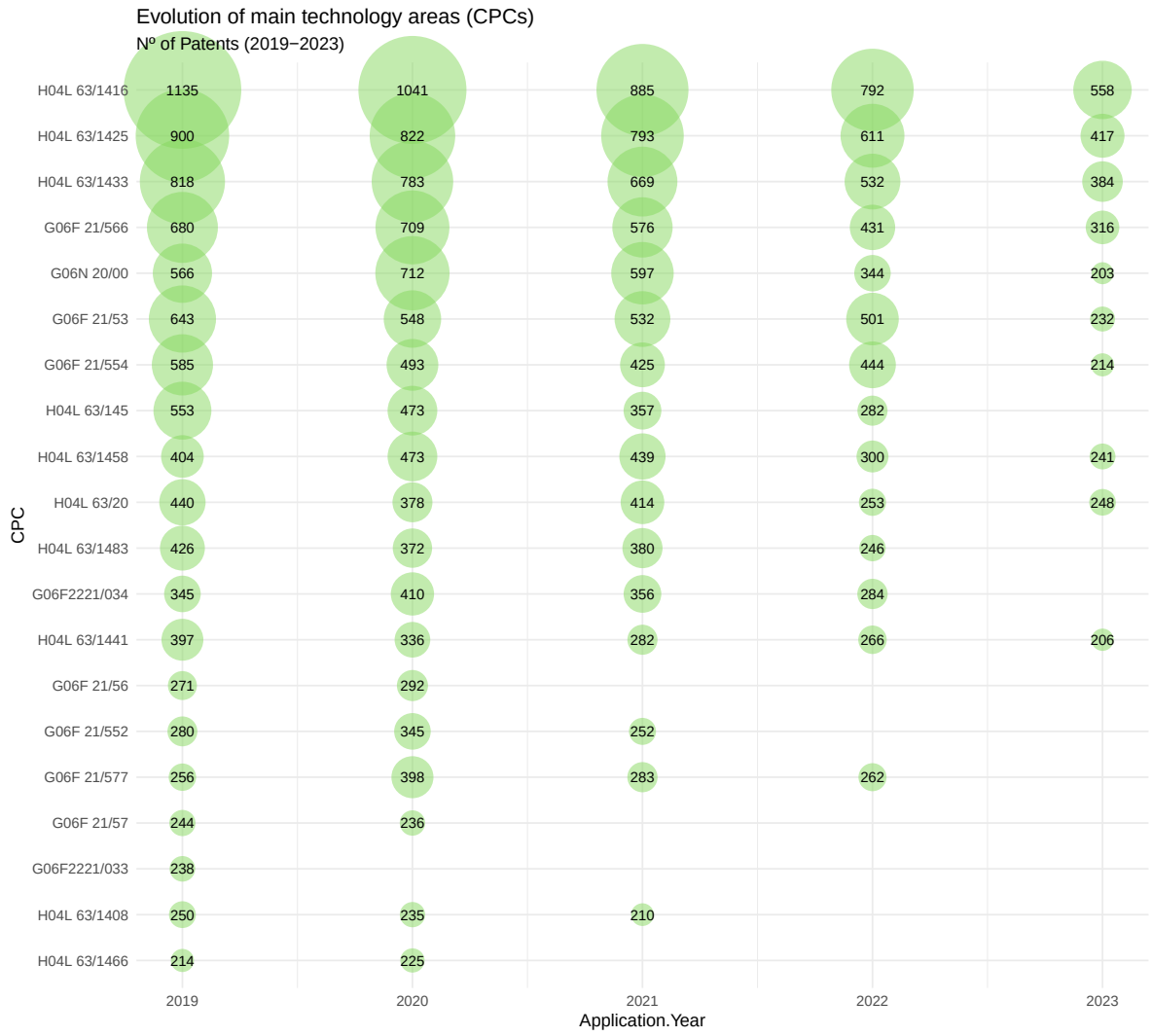


Figura 11: Evolución de las principales áreas tecnológicas

El **DDoS** (*Denial of Service*) es una de las áreas que muestra un interés sostenido en el tiempo. También se mantiene el interés por las políticas de seguridad de redes en general.

Áreas crecientes o de interés sostenido:

- H04L 63/1458 *Denial of Service*
- H04L 63/20 *network security policies in general (filtering policies)*
- H04L 63/14 *detecting or protecting against malicious traffic*
- H04L 63/1416 *Event detection, e.g. attack signature detection*
- H04L 63/1425 *Traffic logging, e.g. anomaly detection*
- H04L 63/1433 *Vulnerability analysis*

- G06F 21/566 *Computer malware detection or handling, e.g. anti-virus arrangements; Dynamic detection, i.e. detection performed at run-time, e.g. emulation, suspicious activities*

Áreas crecientes

Entre las áreas emergentes o que más crecen en los últimos años encontramos la **criptografía cuántica**, el reconocimiento de patrones, las arquitecturas de pagos, los métodos de protección jerárquica tipo anillos de memoria [4] y también las TIC para operaciones médicas remotas.

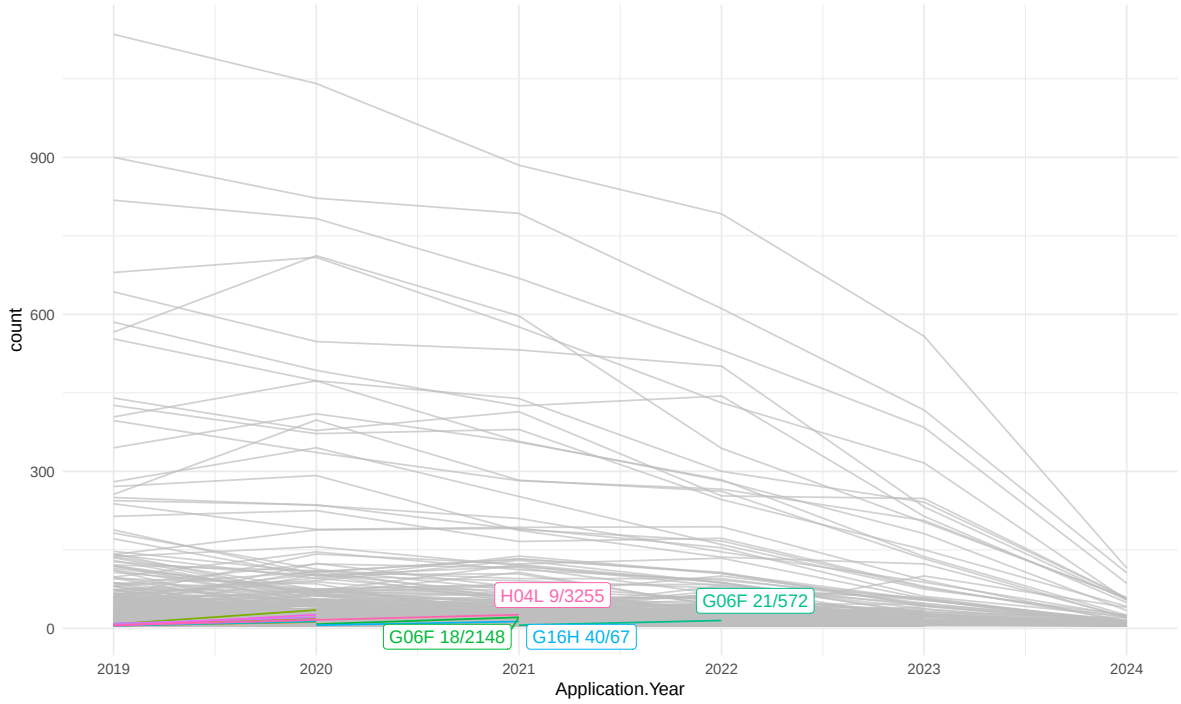


Figura 12: areas crecientes

Áreas crecientes:

- H04L 90/40 *Cryptographic mechanisms; Network security protocols*
- G06F 12/1491 *Protection against unauthorised use of memory or access to memory by checking the subject access rights, in a hierarchical protection system, e.g. privilege levels, memory rings*
- G06F 18 *Pattern recognition*

[4] https://en.wikipedia.org/wiki/Protection_ring

- G16H 40/67 *ICT for remote medical operation*
- H04L 9/0852 *Quantum cryptography (transmission systems employing electromagnetic waves other than radio waves, e.g. light, infrared; wavelength-division multiplex systems)*
- G06Q 20/407 *Payment protocols; Authorisation, e.g. identification of payer or payee, verification of customer or shop credentials; Review and approval of payers, e.g. check credit lines or negative lists; Cancellation of a transaction*

Principales áreas temáticas

Estudiamos las temáticas tratadas a partir del análisis contenido textual de todas las patentes en la colección estudiada.

Figura 13: Principales palabras en las patentes sobre Ciberseguridad

Asimismo, el recuento de palabras adyacentes -tomadas de dos en dos (bigrams)- nos permite una mejor percepción de los conceptos abarcados.

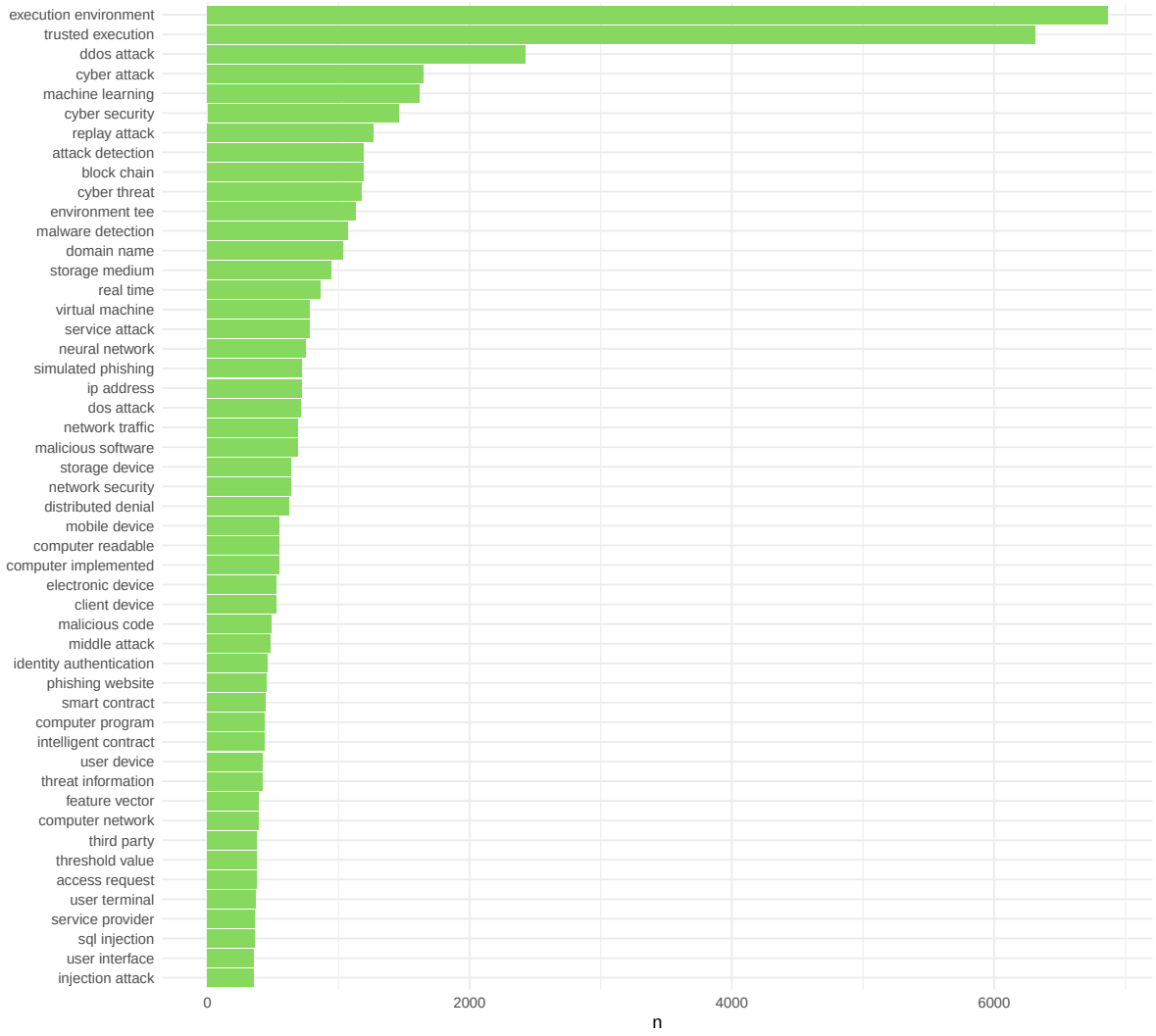


Figura 14: Principales conceptos (bigrams) en las patentes sobre Ciberseguridad

Como uno de los conceptos más frecuentes aparecen los **entornos de ejecución controlados** (*trusted execution environments*), el **Aprendizaje Automático** (*Machine Learning*), los **Ataques de replay** (o ataques de reproducción), un tipo de ataques de usurpación de identidad en la red en que el atacante intercepta una transmisión de datos y la repite y reenvia. Otros conceptos que aparecen son los **simuladores de phishing**, el DDoS, métodos asociados al **blockchain** y la criptografía o los **injection attacks** (ataques para explotar la vulnerabilidad de aplicaciones).

Principales palabras en las patentes sobre Ciberseguridad

El gráfico se genera representando una red de co-ocurrencia de palabras a partir de todas las palabras que aparecen en todos los resúmenes de patentes. El tamaño de las palabras es proporcional a su frecuencia de aparición. Las líneas que conectan las palabras representan las co-ocurrencias de palabras más frecuentes.

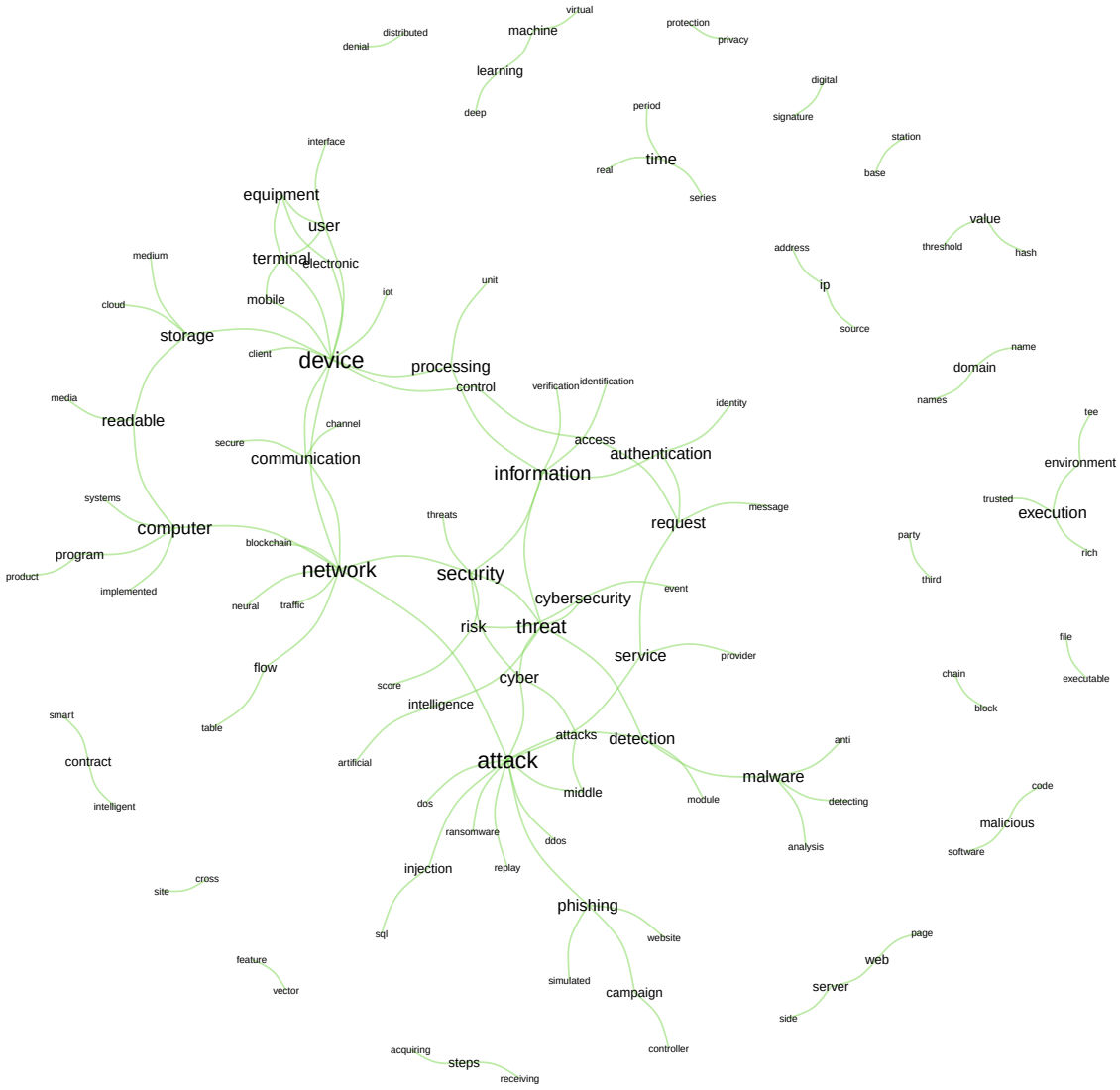


Figura 15: Red de co-ocurrencia de palabras en las patentes sobre ciberseguridad

Clústeres temáticos (topic clusters)

Con el objetivo de detectar y visualizar grupos de contenido significativos en el conjunto de datos recuperados, aplicamos técnicas de *topic modeling*, esto es, técnicas estadísticas que nos permiten descubrir grupos semánticamente similares en el texto que describe las invenciones patentadas [5]

Visualizamos los principales (10) términos, que describen cada cluster mediante un gráficos de barras de frecuencias de cada grupo distintivo.

De entre los grupos significativos que se derivan de todo el conjunto de patentes, observamos, por ejemplo, como en varios grupos temáticos (1,3), se aborda el tema de los ataques phishing, mientras que en otro grupo diferenciado (4) se tratan los ataques de denegación de servicio (DDoS) y en otro la encriptación y el blockchain (6).

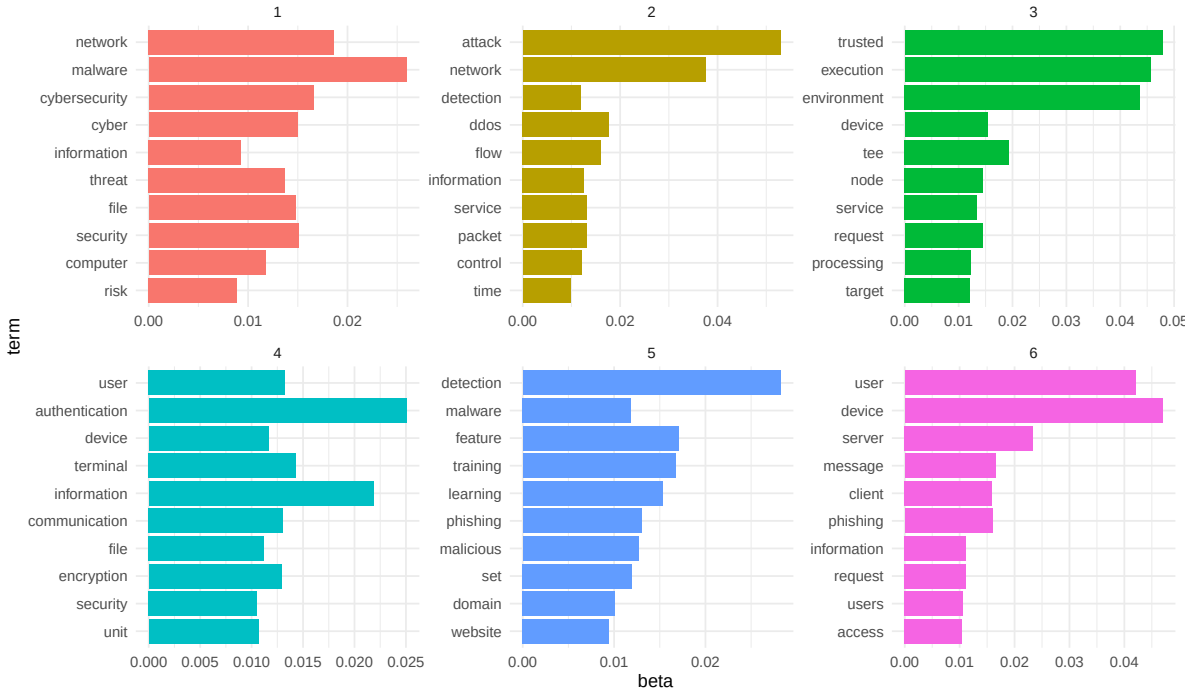


Figura 16: clústeres temáticos

[5] Una de las técnicas de modelado que se usan para este propósito es el algoritmo LDA (*Latent Dirichlet allocation*) https://en.wikipedia.org/wiki/Latent_Dirichlet_allocation. En LDA básicamente se asume que cada documento es una mezcla de un pequeño número de tópicos y que cada palabra en un documento (una patente, en nuestro caso) puede atribuirse a uno de estos tópicos; de este modo podemos especificar un número dado de tópicos o clústeres y usar LDA para generar grupos de tópicos y asignar palabras representativas de cada uno de estos tópicos. Con ello obtenemos una visualización de grupos temáticos representativos del conjunto de datos.

Según el tipo de ataque

Asimismo, analizamos, de entre el conjunto de invenciones recuperadas (todas las patentes publicadas en los últimos años, desde 2019 hasta hoy), la prevalencia en el tratamiento de los diferentes tipos de ciberataque.

De entre los más de 15.000 documentos de patentes revisados originalmente, más de un **8%** (1299) abordan directamente soluciones a ataques **phishing**; un **7,2%** (1150) abordan soluciones a ataques **DDoS**; el **ramsomware** es tratado en 642 patentes (un **4%**) y los ataques de **vectores** en 464 patentes (un **3%**).

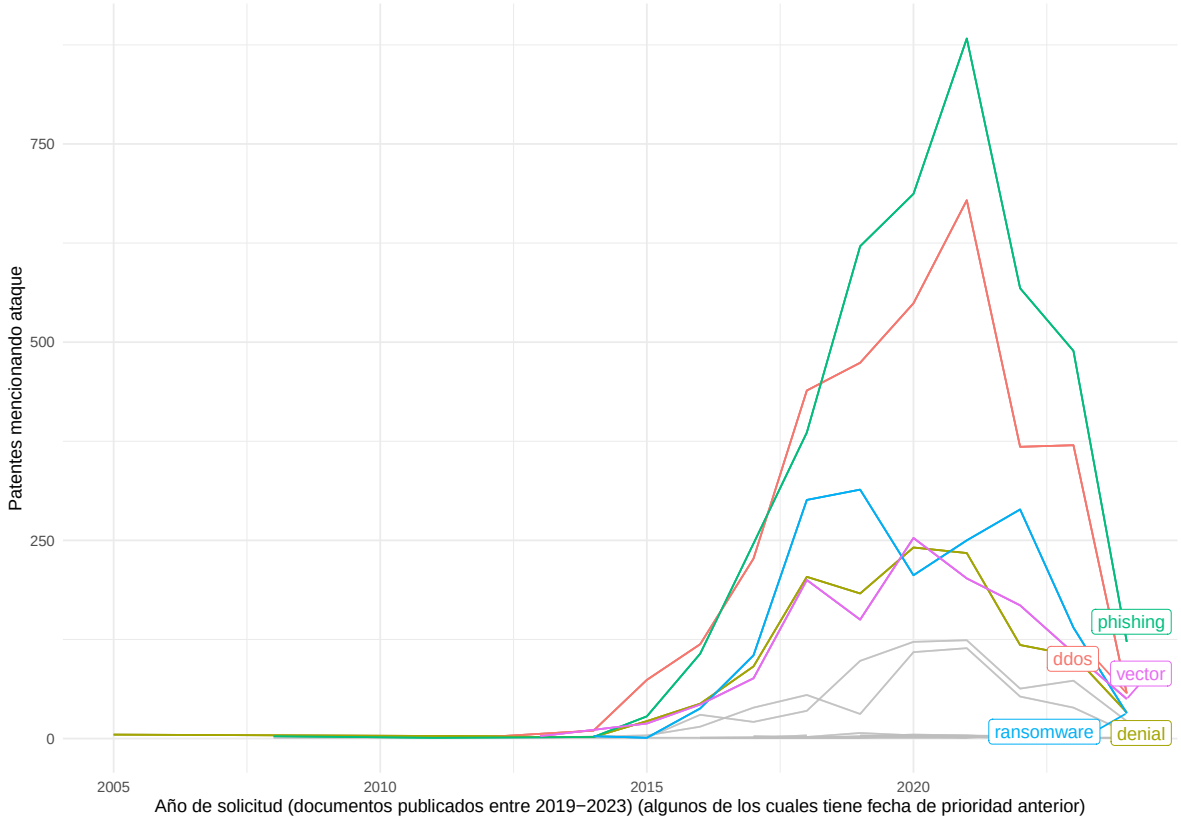


Figura 17: Menciones a los diferentes tipos de ataques en las patentes sobre ciberseguridad

La respuesta al ***phishing*** -una de las técnicas de ciberdelincuencia que más ha crecido y que es cada vez más personalizada- es uno de los problemas más tratados en las soluciones técnicas propuestas, seguido de los ***ataques DDoS*** o *Ataques de denegación de servicio* que implican la sobrecarga deliberada de un recurso o servidor web por parte de un atacante; así como los ataques que implican secuestro de información o ***ransomware***; también son reivindicadas y protegidas en las invenciones publicadas en los últimos años, las soluciones

técnicas para hacer frente a los ***vectores de ataque***, es decir, las rutas o métodos que utiliza un ciberdelincuente al intentar obtener acceso ilegítimo a un sistema de TI.

Principales áreas de especialización

A continuación se muestran las principales organizaciones titulares de patentes y las temáticas relacionadas con sus invenciones patentadas.

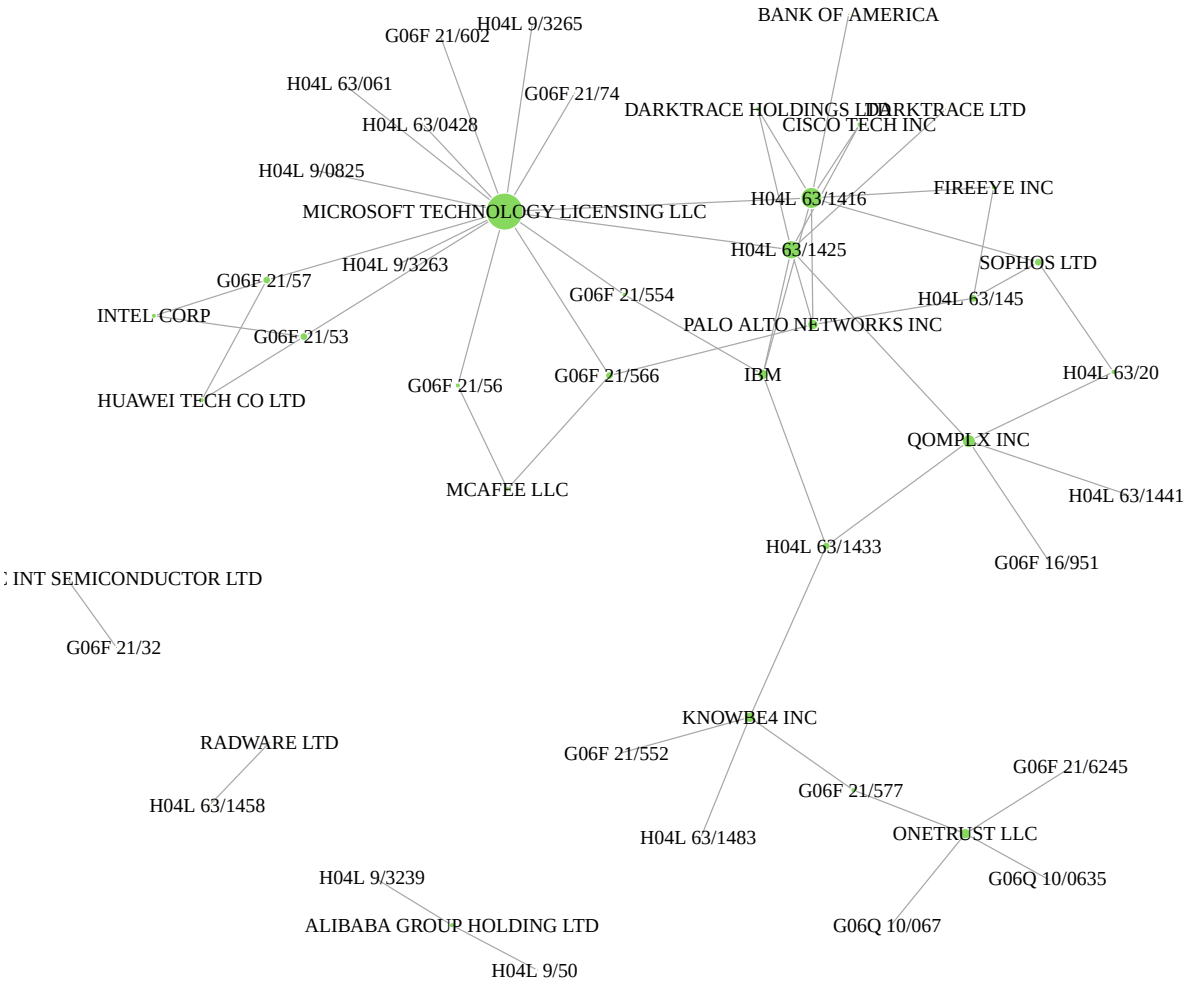


Figura 18: Áreas de especialización de los principales titulares

Trabajan en tecnologías de detección de eventos y en concreto en *attack signature detection* (H04L 63/1416) empresas como **Palo Alto Networks, Bank of America, Darktrace** o **Sophos**. **McAffee** destaca en métodos de detección dinámica de *Malware* (detección en *run-time*, p.e. mediante emulación de actividades sospechosas) (G06F 21/566); **IBM** en detección de tráfico malicioso y anomalías (*anomaly detection*) (H04L 63/1425).

Qomplx, por su parte, se diferencia en tecnologías para contrarestar ataques en mecanismos criptográficos (H04L 63/1441) en combinación con técnicas de *webcrawling* (G06F 16/951); **Cirrus** lo hace en identificación de usuarios usando datos biométricos (G06F 21/32) y **Radware** en contramedidas para *Denial of service* (H04L 63/1483).

Knowbe4 trabaja en contramedidas para trafico maliciosos, *phishing, pharming o web spoofing* (H04L 63/1483), detección de intrusiones con monitoreo a largo plazo (G06F 21/552) y evaluación de vulnerabilidades en el sistema de seguridad en computadores (G06F 21/577), área en la que también trabaja **Onetrust**, quien también ha patentado en modelado de recursos empresariales (G06Q 10/067).

Microsoft es fuerte, entre otros, en mecanismos criptográficos, sobre todo, usando *asymmetric-key encryption* o *public key infrastructure [PKI]*, tales como signaturas clave o certificados públicos clave (H04L 9/0825), ejecución de monitoreos de seguridad e integridad usando maquinas virtuales seguras o *sandboxes* (G06F 21) y arquitecturas de redes peer-to-peer (H04L 63/061).

Huawei se especializa en métodos de inicio seguro de computadores y actualizaciones de sistema seguras (G06F 21/57) y, como **Intel** y **Microsoft**, también patenta soluciones que involucran máquinas virtuales seguras o *sandboxes* (G01F 21/53).

Desarrollo de soluciones técnicas contra el Phishing

Lidera los desarrollos actuales de nuevas soluciones técnicas a problemas relacionados con el ***Phishing***, la empresa **Knowbe4**; Otras empresas como Microsoft, IBM, McAfee y Paypal, son también activas.

Empresas más especializadas que también estan desarrollando tecnología en relación a contrarestar el phishing son **Lookout** https://www.lookout.com de Abu Dhabi, la francesa **Vade Secure** https://www.vadesecure.com o la empresa de infrastructuras de acceso seguro **Netskope** https://www.netskope.com. Otras empresas relevantes en este ámbito de desarrollo son Sophos, Servicenow, Riskiq, Proofpoint, la china Dbapp Security, Shape Matrix, Sanofor o Fireeye.

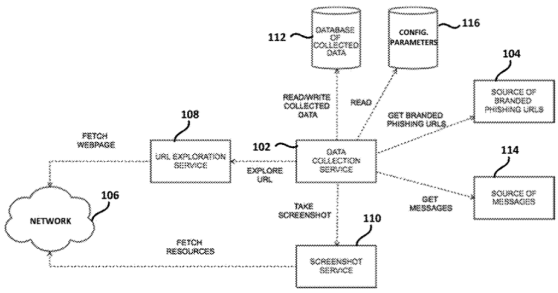


Figura 19: Patente de VADE SECURE INC: US11552993B2, Automated collection of branded training data for security awareness training

Desarrollo de soluciones técnicas contra el Ransomware

El ***Ransomware*** es un tipo de malware que se introduce en los equipos y dispositivos móviles conectados a Internet impidiendo el acceso a la información.

En cuanto a desarrollo actual de soluciones a problemas relacionados con el *Ransomware*, aparte de Microsoft -y grandes empresas como EMC, Dell, IBM, McAfee, British Telecomm, Amazon o Huawei- también aparecen activas otras empresas más especializadas, tales como la empresa especializada en ciberresiliencia en la nube **Rubrik** https://www.rubrik.com, **Datto** (hoy filial de **Kaseya.com** https://www.kaseya.com, del grupo de capital de riesgo **Insight Partners**) o la empresa de seguridad *zero trust* en la nube **Airgap** https://airgap.io.

Otras empresas con actividad significativa en este ámbito son **Palo Alto Neworks**, **Commvault**, **Acronis** y **Secuve**.

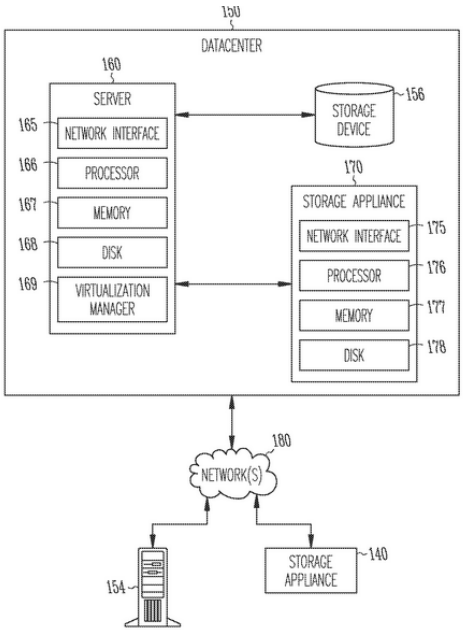


Figura 20: Patente de RUBRIK INC: US12019748B2 Application migration for cloud data management and ransomware recovery

Colaboraciones

El análisis del co-patentamiento -empresas que comparten titularidad en el registro de invenciones patentadas- nos permite detectar relaciones de cooperación en materia de desarrollo tecnológico.

Observamos como la mayoria de colaboraciones se dan entre empresas de un mismo grupo; así por ejemplo, Darktrace utiliza los nombres de titular *Darktrace Ltd* y *Darktrace Holdings* con los que aparece como co-titular en varias invenciones.

Symantec y **Nortonlifelock**, por su parte, comparten titularidad en varias patentes (Symantec también había copatentado con **Ca Inc**, hasta 2018); **Fireeye** lo hace en ocasiones con **Musarubra** (quien a su vez patenta con **McAfee**) y en otras con **Mandiant**; **Entit Software** con **Micro Focus** y **Qomplx** con **Fractal** https://fractal.ai empresa que aplica ML para detección de fraudes.

En China, **Alipay** patenta con la empresa de trazabilidad de blockchain **Ant Blockchain** de Shanghai https://www.antchain.net; el **China Construction Bank Corp** lo hace con **CCB Fintech** de Shanghai; **Xian Thermal Power Res Inst Co** con **Huaneng Group Tech Innovation Center Co Ltd**; la Canadiense **Bicdroid** https://bicdroid.com con **Baizhuo Information Tech Co Ltd** y **Baidu** con **Kunlunxin Tech Beijing Company Limited**.

En Israel, **Cognyte** https://www.cognyte.com copatenta con la empresa estadounidense de plataformas de IA **Verint Systems** https://www.verint.com.

Otras colaboraciones entre empresas y centros de investigación públicos se dan por ejemplo entre la **Universidad de Shanghai Electric Power** y **Shanghai Cloud Sword Information Tech Co Ltd**; en EE.UU. entre el **Battelle Memorial Institute** y la **Universidad de Arkansas** o entre **UIPCO LLC** y la asociación financiera y aseguradora **USAA**; **HP** ha colaborado con la **Universidad china de Nanyang Tech**; en Corea del Sur entre **SAMSUNG ELECTRONICS** y el centro **KIST** o entre **KOREA ELECTRIC POWER COR** y el **KNU INDUSTRY COOPERATION FOUND**.

En Europa, el **CEA** Francés copatenta con el Instituto Politécnico de la **Universidad de Grenoble**.

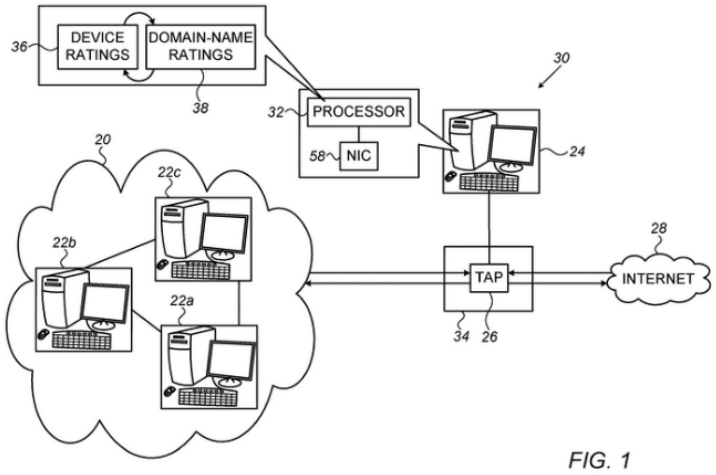


Figura 21: Patente de Cognyte y Verint Systems: US11888879B2, System and method for monitoring security of a computer network

Una de las patentes más citadas es la concedida en 2019 a la empresa aseguradora y financiera global **Aon**, relacionada con un sistema de evaluación del riesgo de ciberseguridad (US10387657B2). El sistema califica las vulnerabilidades dentro de la arquitectura tecnológica de una empresa después de identificar las características de la infraestructura y producir escenarios de amenazas. La patente de Aon ha sido citada, entre otros, por empresas como IBM, Samsung, Bank of America, Siemens o T-Mobile.

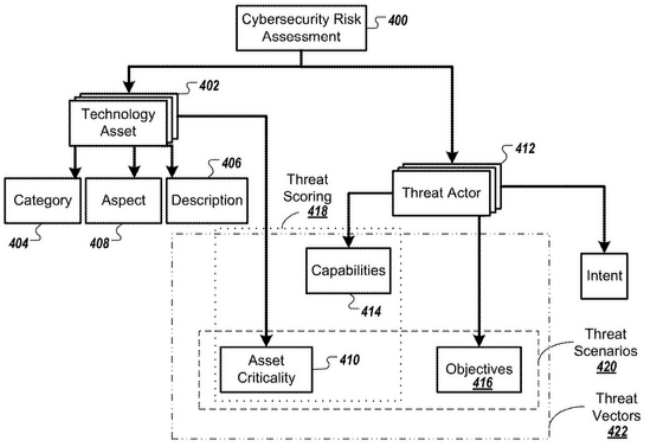


Figura 22: Patente de Aon: US10387657B2, Systems and methods for cybersecurity risk assessment

Mercado de la Ciberseguridad

La información tecnológica y estratégica proporcionada por el análisis de patentes, se ha completado con información secundaria obtenida a partir de diversas fuentes sectoriales y de mercado.

Se ha recopilado información distribuida en múltiples informes recientes[1] elaborados por centros de referencia en el sector, tanto a nivel internacional (ENISA, EIB, ECSO, WEF, ITU, etc.), como nacional (Incibe, ccn-cert, disruptive/apte, observaciber, cybasque, foro nacional de ciberseguridad, etc.), así como de empresas (Google, Cisco, Sonicwall, Knowbe4, Sealpath, SAP, etc.) y consultoras especializadas (Gartner, Forbes, Deloitte, Captsone, etc.), empresas de estudios de mercado, directorios, ferias (RSA, Ciber.gal, etc.) y foros de inversión (Venture in security, Pitchbook, etc.), páginas web corporativas, blogs especializados (hackernews, apwg, krebs), etc.

Tamaño y Proyecciones del Mercado

El mercado de la ciberseguridad es uno de los mercados de más rápido crecimiento en el mundo, liderado principalmente por la tendencia actual hacia una economía digital y la toma de conciencia de las vulnerabilidades que conlleva.

Según algunos estudios de mercado, como por ejemplo, el más reciente de Mordor Intelligence[2], alcanzó un tamaño global de 203.780 millones de euros en 2024 y crecerá hasta los 350.230 millones de euros en 2029 con una tasa de crecimiento anual del 11,4%.

[1] ver bibliografía al final del documento
[2] https://www.mordorintelligence.com/industry-reports/cyber-security-market

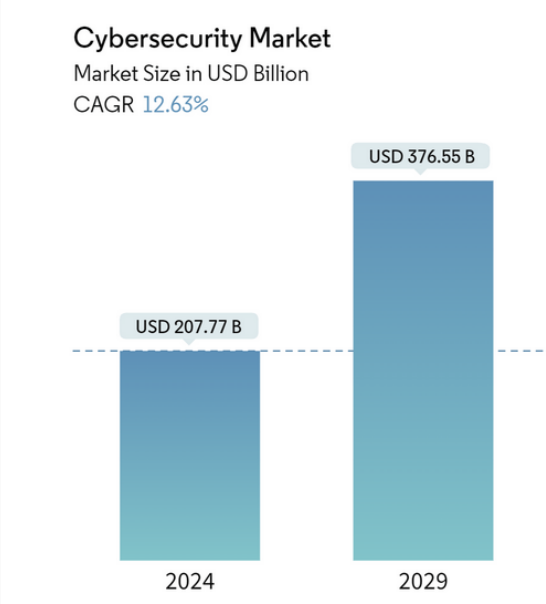


Figura 1: Mercado global de la ciberseguridad (2024-2029). Fuente: Mordor Intelligence

Fortune Business Insights[3] lo ha valorado en 193.730 millones de USD este 2024 y proyectó que crecería a unna TACC del 14,3% a alrededor de € 326.000 millones en 2028 y hasta 562.720 millones 2032. Según MarketsandMarkets[4] era de 190.400 millones de USD en 2023 y se proyecta que alcance 298.500 millones en 2028, con una tasa de crecimiento del 10,9%. Tambien Globaldata[5] apunta a una tendencia al alza. Para Cybersecurity Ventures[6], crecerá hasta 1 billón de dólares en 2030, frente a los 146.000 millones de dólares de 2022.

Segmentación

El mercado de la ciberseguridad puede segmentarse en varios submercados, entre ellos:

- Seguridad de puntos finales (*Endpoint security*)
- Seguridad de redes
- Seguridad en la nube

[3] https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
[4] https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
[5] Globaldata (30 de Agosto, 2022) Cybersecurity Market Size, Share & Trends Analysis Report by Type (Enterprise, Consumer), Product (Security Consulting, Managed Service Providers, Identity & Access Management), Vertical, Enterprise Size, Region, and Segment Forecasts, 2022-2026 https://www.globaldata.com/store/report/cybersecurity-market-analysis
[6] https://cybersecurityventures.com/cybersecurity-almanac-2024

- Gestión y control de identidades y accesos (IAM)[7]
- Respuesta a incidentes e inteligencia de amenazas
- gestión y monitorización de eventos e información de seguridad (SIEM) [8]
- Consultoría en ciberseguridad y servicios de gestión de la seguridad

Impulsores de crecimiento

En cuanto a los principales impulsores del mercado, el principal es el creciente número de ciberataques y violaciones de datos[9]

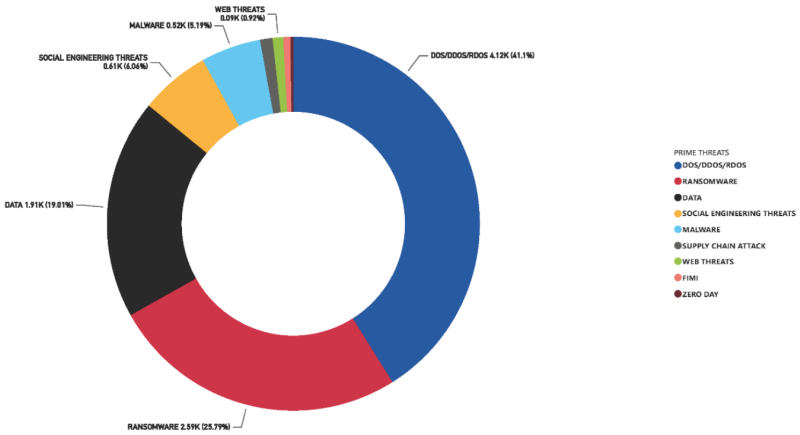


Figura 2: Principales incidentes. Fuente: Enisa

Otros impulsores son:

- La adopción de la computación en la nube, los dispositivos IoT y otras tecnologías emergentes está creando nuevas vulnerabilidades que hay que gestionar.
- La creciente importancia de la protección de datos y el cumplimiento de regulaciones como GDPR, HIPAA (en el ámbito médico) y PCI-DSS (en el ámbito de los pagos electrónicos).

[7] https://www.microsoft.com/es-mx/security/business/security-101/what-is-identity-access-management-iamhttps://www.microsoft.com/es-mx/security/business/security-101/what-is-identity-access-management-iam
[8] https://www.ibm.com/es-es/topics/siem
[9] https://cybersecurityventures.com/cyberwarfare-report-intrusion

Tendencias

- El cambio hacia soluciones de seguridad basadas en la nube es cada vez más popular.
- La ciberseguridad como servicio (MSS[10]) está cada vez más extendida, con muchos proveedores que ofrecen servicios de seguridad gestionados.

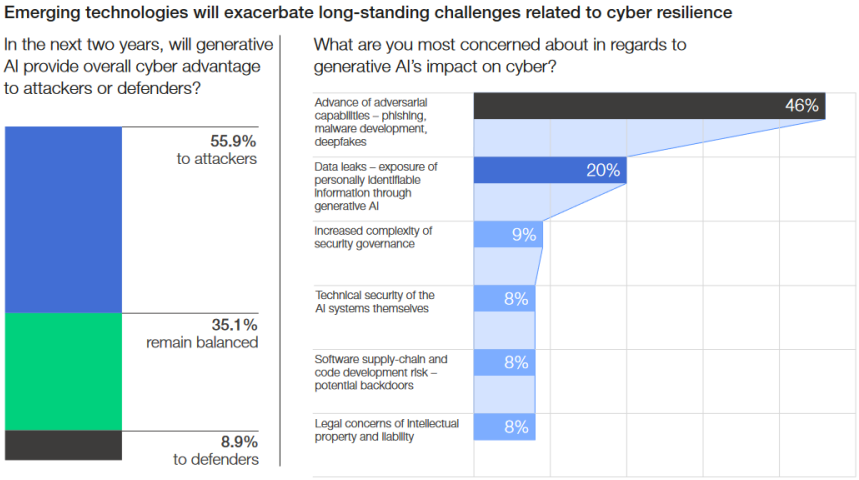


Figura 3: La IA generativa plantea riesgos considerables para la ciberresiliencia. Fuente: WEF

- La inteligencia artificial (IA) y el aprendizaje automático (ML) se están utilizando para mejorar las capacidades de detección y respuesta a amenazas.

Los actuales avances en tecnologías autónomas de operaciones en sistemas computacionales que utilizan la IA (sistemas que automatizan tareas humanas en entornos informáticos) -pensemos por ejemplo, en los nuevos frameworks para construir aplicaciones que usan la IA con grandes modelos de lenguaje (LLM) y que gestionan programas y archivos en un entorno computacional, tales como Computer Use de Anthropic o Cursor- plantean nuevos retos y dificultades en la identificación de identidades y pueden suponer una amenaza para la ciber-resiliencia.

Mercado laboral

El mercado laboral de la ciberseguridad está creciendo rápidamente, y se espera que el número de ofertas de trabajo aumente un 34% entre 2022 y 2025[11].

[10] https://www.deustoformacion.com/blog/ciberseguridad/ciberseguridad-como-servicio
[11] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031

Las habilidades de ciberseguridad más demandadas incluyen:

- Pruebas de penetración
- Respuesta a incidentes
- Inteligencia de amenazas
- Seguridad en la nube
- Inteligencia Artificial (IA) y Aprendizaje Automático (*Machine Learning*, ML)

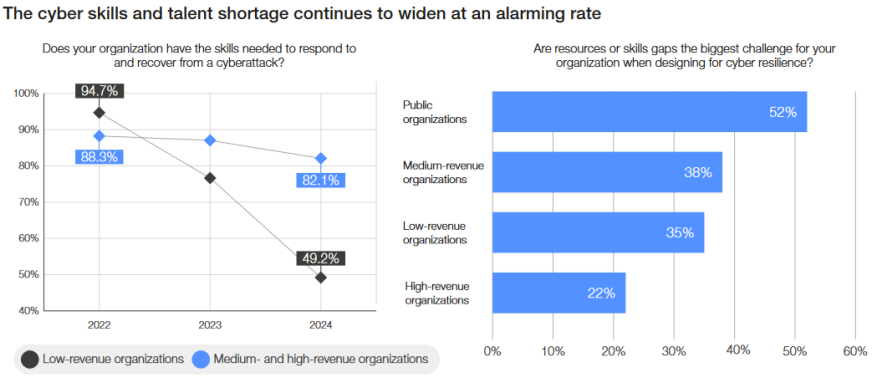


Figura 4: Creciente escasez de competencias y talentos cibernéticos. Fuente: WEF

En España, según un estudio que elaboró Observaciber[12] en 2022, la cifra de profesionales que buscaban empleo en ciberseguridad en 2021 ascendía a 39.072 y la previsión es que se incrementen hasta los 42.283 en 2024. El número de profesionales necesarios en ciberseguridad se elevaba a 63.191 empleos, mientras que en 2024 superará los 83.000.

Análisis Competitivo y Tendencias del Mercado

Los países con los mercados de más rápido crecimiento se concentran en el área de Asia-Pacífico (con una CAGR esperada del 19,6%), con Europa y América del Norte caracterizadas por tasas de crecimiento medias (9,1% y 7,8%, respectivamente)[13]

[12] https://www.incibe.es/incibe/sala-de-prensa/demanda-talento-ciberseguridad-doblara-oferta-2024-alcanzar-cifra-mas-83000
[13] https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf

Comparación regional y proyecciones

Se espera que América del Norte mantenga una importante cuota de mercado. Los clústeres de San Francisco, Washington y el vínculo tecnológico con Israel configuran el ecosistema de ciberseguridad de EE.UU. como uno de los más potentes del mundo. En esta región el mercado de la ciberseguridad se estimó en 124.000 millones de USD en 2022 y se proyecta que alcanzará 243.000 millones en 2027, con una tasa de crecimiento del 10,9[14].

El mercado en Asia, por su parte, se ha estimado en 34.000 millones de USD en 2022 y se proyecta que alcanzará los 64.000 millones en 2027, con una tasa de crecimiento del 11,5%. El reciente estudio de Mordor apunta a cuotas de crecimiento del mercado del 21.31% en China y del 18.33% en India.

Finalmente, en Europa se estimó en 43.000 millones de USD en 2022 y se proyecta que alcanzará los 73.000 millones en 2027, con una tasa de crecimiento del 9,5%.

[14] <https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html

Principales Empresas

Empresas Líderes en América

Algunas de las empresas norteamericanas más importantes en el mercado de la ciberseguridad son:

- Palo Alto Networks (Estados Unidos) https://www.paloaltonetworks.com
- Cyberark (Estados Unidos/Israel) https://www.cyberark.com
- Check Point (Estados Unidos/Israel) https://www.checkpoint.com
- McAfee (Estados Unidos) https://www.mcafee.com
- Symantec/Gen Digital/Broadcom (Estados Unidos) https://www.broadcom.com
- Trend micro (Estados Unidos) https://www.trendmicro.com
- CISCO (Estados Unidos) https://www.cisco.com
- IBM Security (Estados Unidos) https://www.ibm.com/data-security
- Microsoft (Azure Security) (Estados Unidos) https://azure.microsoft.com/es-es/explore/security
- Amazon Web Services (AWS Security) (Estados Unidos) https://aws.amazon.com/es/security
- Fortinet (Estados Unidos) https://www.fortinet.com
- Barracuda networks (Estados Unidos) https://www.barracuda.com
- Splunk Inc (Estados Unidos) https://www.splunk.com/
- F5 Networks Inc (Estados Unidos) https://www.f5.com
- Arcserve https://www.arcserve.com
- Aqua security (Estados Unidos) https://www.aquasec.com
- Sysdig (Estados Unidos) https://www.sysdig.com
- Oracle (Estados Unidos) https://www.oracle.com/security

Empresas Líderes en Asia

Algunas de las empresas más importantes en el mercado de la ciberseguridad en Asia son:

- Huawei (China) https://www.huawei.com
- Kaspersky Lab (Rusia) https://www.kaspersky.com
- Astra Security (India) https://www.getastra.com/

- Fujitsu (Japón) https://www.fujitsu.com/es/themes/security
- Manageengine (Arabia Saudita) https://www.manageengine.com
- Dbapp Security (China) http://www.dbappsecurity.com.cn
- Bluedon (China) http://bluedon.com
- Antiy Labs (China) https://www.antiy.net
- Bugbank (China) https://www.bugbank.cn
- Bangcle (China)https://dev.bangcle.com
- Qi An Xi Technology (China) https://en.qianxin.com
- Beijing ThreatBook Technology (China) https://threatbook.cn
- Feitian (China) https://www.ftsafe.com
- New H3C Technologies (China) https://www.h3c.com
- Seirim (China) https://seirim.com
- I-sprint (Singgapur) https://www.i-sprint.com
- Fortinet (Estados Unidos/Japón) https://www.fortinet.com
- Juniper Networks (Estados Unidos/China) https://www.juniper.net
- Cisco (Estados Unidos/China) https://www.cisco.com
- Symantec/Gen Digital/Broadcom (Estados Unidos/Japón) https://www.broadcom.com

Empresas Líderes en Europa

Algunas de las empresas más importantes en el mercado de la ciberseguridad en Europa[1], [2] son:

- Sophos (Reino Unido) https://www.sophos.com
- Darktrace (Países Bajos) https://darktrace.com
- Acronis (Suiza) https://www.acronis.com
- Avast (República Checa) https://www.avast.com
- Siemens (Alemania) https://www.siemens.com
- Check Point (Israel/Reino Unido) https://www.checkpoint.com
- Palo Alto Networks (Estados Unidos/Reino Unido) https://www.paloaltonetworks.com
- IBM Security (Reino Unido) https://www.ibm.com/data-security
- Cyberark (Israel/Francia) https://www.cyberark.com
- Symantec/Broadcom (Estados Unidos/Francia) https://www.broadcom.com
- Barracuda networks (Estados Unidos/Austria) https://www.barracuda.com
- Astra Security (India/Irlanda) https://www.getastra.com
- Fujitsu (Japón/Alemania) https://global.fujitsu
- Dell (Estados Unidos/Irlanda/Alemania) https://www.dell.com
- Infoguard (Suiza) https://www.infoguard.ch
- Hacken (Estonia) https://hacken.io

[1] https://www.mordorintelligence.com/industry-reports/europe-cybersecurity-market/companies
[2] https://cybermagazine.com/cyber-security/top-10-cyber-security-companies-in-europe

- SecurityHQ (Reino Unido) https://www.securityhq.com
- Bridewell (Reino Unido) https://www.bridewell.com
- Bitdefender (Rumania) https://www.bitdefender.com
- SEON Technologies (Hungria) https://learn.seon.io
- Stormshield (Francia) https://www.stormshield.com
- F-secure (Finlandia) https://www.f-secure.com
- Alluriy (Suecia) https://allurity.com

Tendencias en Europa

La Regulación General de Protección de Datos (RGPD) de la UE ha impulsado la demanda de soluciones de seguridad para ayudar a las organizaciones a cumplir con las normas de protección de datos. La Directiva Europea NIS2[3] quieren hacer que la privacidad de los datos sea una prioridad en las organizacioes[4].

El crecimiento del Internet de las Cosas (IoT) en Europa ha creado nuevas vulnerabilidades y oportunidades para ciberamenazas.

Tendencias en Asia

El crecimiento de las compras electrónicas y pagos digitales en Asia ha creado nuevas vulnerabilidades para ciberamenazas.

La creciente utilización de servicios en la nube impulsan la demanda de soluciones de seguridad en este ámbito.

Tendencias en EE.UU.

El crecimiento de las transacciones digitales y el comercio electrónico también en América del Norte ha impulsado la demanda de soluciones de seguridad que puedan proteger datos sensibles.

El crecimiento del Internet de las Cosas (IoT) y los servicios en la nube crean nuevas vulnerabilidades para ciberamenazas.

[3] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[4] https://www.redseguridad.com/especialidades-tic/normativa-y-certificacion/ens-prepara-a-las-entidades-para-cumplir-con-la-directiva-nis-2_20241122.html

Inversiones y operaciones conjuntas (M&A) recientes

La alta demanda de productos y servicios en el sector de la ciberseguridad se está materializando en consumidores individuales que apoyan a empresas más tradicionales de antivirus y detección de amenazas, mientras que nuevas empresas impulsadas por la IA son respaldadas por inversores de capital de riesgo [5].

Han invertido en ciberseguridad firmas de capital de riesgo generalistas a nivel global, tales como Andreesen Horowitz, Sequoia Capital, Accel, Sands Capital, Alumni Ventures, Gaingels, Lightspeed Management, Ten Eleven ventures, Bessemer Venture Partners, Cyberstarts, y otros[6].

La inversión en el sector, por tanto, parece que se está recuperando tras un crecimiento plano el año previo en financiación de capital riesgo; en lo que va de 2024 se ha recaudado, según apunta Pitchbook[7], 8.800 millones de dólares, en camino de superar el total de 10.900 millones de dólares del año anterior.

Entre las inversiones realizadas en los últimos años [8], cabe destacar, por ejemplo, los 1.400 millones de USD por parte del grupo **Blackstone** en **Palo Alto Networks**.

A nivel de adquisiciones este año, por ejemplo, han sido noticia la compra de **Venafi** (de la firma de inversión **Thoma Bravo**) por parte de **CyberArk** por 1.54 mil millones de USD, mientras que **Thoma Bravo** por su parte ha adquirido a **Darktrace** por 5.3 mil millones.

Otras adquisiciones destacadas han sido la compra de **Noname** por parte de **Akamai**; de **Egress** por parte de **Knowbe4**; de **Foretrace** por parte de **Flare**; de **Avalor** por parte de **Zscaler**; de **Arculus** por parte de la británica **Bridewell**; **Stackpath** por parte de **Gcore**; de **Flow Security** por parte de **Crowdstrike**; de **Bearer** por parte de **Cycode**; de **Vade** por parte de **Hornetsecurity Group**; de **Kolide** por parte de **1Password**; de **CTCI** por parte de **Armis**; de **Veritas** por parte de **Cohesity**; de **Elevate Security** por parte de **Mimecast**; de **Trustware** por parte de la empresa del Grupo Chertoff, **MC² Security Fund**; de **Authomize** por parte de **Delinea**; de **Helios** por parte de **Snyk**; de **Security Shift** por part de la australiana **5G Networks** o la division de ciberseguridad de HoganTaylor Technology por parte de **Staley Technologies**.

La creciente tendencia a realizar operaciones conjuntas (M&A) se espera que también continúe en los próximos años: por ejemplo, la adquisición de 4.3 mil millones realizada por Silver Lake Partners con **SonicWall** que a su vez ha comprado a **Banyan Security**; la fusión de **LogRhythm** y **Exabeam** o la de **DNV** con **Nixu** y **Applied Risk**, entre otras.

---

[5] Informe Sectorial de Ciberseguridad de enero de 2024 de Capstone https://www.capstonepartners.com/wp-content/uploads/2024/01/Capstone-Partners_Cybersecurity-Sector-Report_January-2024-1.pdf

[6] Venture in security (2023) Generalist VC firms in cybersecurity https://ventureinsecurity.net/p/generalist-vc-firms-in-cybersecurity

[7] Pitchbook 2024 Information Security Overview https://pitchbook.com/news/articles/cybersecurity-private-equity-deals-us-europe https://pitchbook.com/news/reports/2024-information-security-overview

[8] https://www.csoonline.com/article/1298623/top-cybersecurity-ma-deals-for-2024.html

En Europa

En Europa, el Banco Europeo de Inversiones (BEI) está abordando activamente los retos de inversión a los que se enfrentan las empresas europeas de ciberseguridad para fomentar el crecimiento del sector. Su propuesta de Plataforma Europea de Inversión en Ciberseguridad (European Cybersecurity Investment Platform, ECIP[9]) pretende abordar el déficit de financiación y apoyar la expansión de las empresas europeas de ciberseguridad. El ECIP ofrecería una gama de servicios financieros y no financieros, incluidas inversiones de capital, asistencia técnica e iniciativas de desarrollo de ecosistemas. La estrategia de inversión del ECIP prioriza las soluciones vinculadas a la soberanía de los datos, como el cifrado, la seguridad en la nube, la autenticación multifactor (MFA), la gestión de accesos privilegiados y la detección y respuesta a incidentes. Se ha comprometido una inversion de 1600 millones de Euros hasta 2027.

A nivel privado, ha habido inversiones recientes de varias firmas de Capital de Riesgo activas en Europa, tales como **Adara Ventures** (p.e. en la empresa italiana de formación en ciberseguridad Cyber Guru[10] este año o en CounterCraft en 2020), **Accel Partners**[11] (en Blackpoint Cyber[12] en 2023) o **33N Ventures** (p.e. en la empresa de ciberseguridad para IoT Exein y en la empresa de centros de comando impulsados con IA StrikeReady este año[13]), entre otras.

En España

En España el ecosistema emprendedor es respaldado por empresas de VC tales como:

- JME Ventures (Madrid)
- Kibo Ventures
- Caixa Capital Risc
- Inveready (Donostia)
- Orza (Donostia)
- all iron ventures (Bilbao)
- Easo ventures
- Talde Private (Bilbao)
- stellum capital
- Anzu Partners,
- Baron Capital

[9] https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf
[10] https://www.adara.vc/news/cyber-guru-raises-25m-series-b
[11] https://www.reuters.com/business/finance/vc-firm-accel-raises-650-mln-invest-ai-cybersecurity-startups-2024-05-13
[12] https://fintech.global/2023/06/09/bain-capital-and-accel-invest-190m-in-cybersecurity-provider-blackpoint-cyber
[13] https://www.essential-business.pt/2024/07/19/33n-ventures-leads-investment-in-exein-and-strikeready

Asimismo a nivel corporativo, han habido iniciativas en el ámbito de la ciberseguridad por parte de empresas como Iberdrola (Fondo Perseo)[14] o el Banco Santander (alianza con Forgepoint Capital International FPCI)[15].

A nivel público, en Euskadi se han destinado 3,5 millones en ayudas a la Ciberseguridad destinadas a fortalecer a las empresas vascas[16].

Empresas de ciberseguridad en España

El entorno competitivo de las empresas especializadas de ciberseguridad en España es bien nutrido y dinámico (existen alrededor de 1800 empresas[17]).

Los servicios de seguridad -según apuntan estudios recientes de IDC[18] o Statista[19] - dominan el mercado, con un volumen de unos 1.780 millones de dólares en 2024 y un crecimiento estimado del 6,67%, hasta alcanzar los 4.250 millones de dólares previstos para 2029.

En este informe se han identificado algunas de las principales empresas hoy activas en ciberseguridad en España, recopiladas a partir de varias fuentes tales como el catálogo de Empresas del Incibe [20] y otros directorios[21] y listados[22], [23], [24]:

Prestando servicios o invirtiendo en el ámbito de la ciberseguridad en España encontramos a grandes multinacionales españolas (Telefonica Cybersecurity Cloud, Iberdrola, Banco Santander); así como varias sedes de compañias tecnológicas internacionales (Ibm Global Services España, Konica Minolta, Talio, Izertis); Grandes consultoras tecnológicas (Deloitte, ey, Capgemini España Sl, accenture, kpmg, atos, Dxc, pwc); grandes empresas españolas especializadas en ciberseguridad (sia/indra, innovate/Mnemo, Seidor, Softeng, mtp, ibermatica, Eulen, Panda, S21sec, Zerolynx, Cuatroochenta), así como un abundante número de empresas especializadas pequeñas y medianas.

Como ejemplos de empresas atualmente activas en ámbitos tecnológicos innovadores, **Wise Security Global**, parte del grupo italiano Var group, trabaja en el ámbito de las soluciones

[14] https://www.iberdrola.com/innovacion/programa-internacional-startups-perseo/porfolio-inversiones
[15] https://www.santander.com/es/sala-de-comunicacion/notas-de-prensa/2022/10/santander-y-forgepoint-capital-anuncian-una-alianza-estrategica-para-impulsar-la-inversion-y-la-innovacion-en-ciberseguridad
[16] https://www.spri.eus/es/ciberseguridad/impulsa-la-ciberseguridad-en-tu-pyme-mediante-la-implantacion-de-servicios-soc-y-obten-los-certificados-de-ciberseguridad-mas-exigentes
[17] https://www.incibe.es/emprendimiento/publicaciones/blog/pilares-del-emprendimiento-en-ciberseguridad-en-espana
[18] https://atlastecnologico.com/inversion-dispersa-baja-y-fragmentada-en-una-europa-cibertibia
[19] https://www.statista.com/outlook/tmo/cybersecurity/spain
[20] https://www.incibe.es/empresas/herramientas/catalogo-de-ciberseguridad
[21] ENS https://gobernanza.ccn-cert.cni.es/certificados
[22] https://microhackers.net
[23] https://financialmagazine.es
[24] https://www.tarlogic.com/es/blog/empresas-de-ciberseguridad

de Identidad Descentralizada y ha sido reconocida por Gartner[25] como un referente en este campo; la donostiarra **Multiverse Computing** trabaja en el desarrollo de métodos inpirados en la cuántica para clusterización de datos de seguridad; **Sealpath** es una empresa bilbaína de software de seguridad que colabora con varios partners a nivel nacional e internacional y ha participado en estudios de tendencias del sector[26].

tier8 es una empresa de Madrid especializada en analisis del comportamiento humano y fallos de seguridad y concienciación. **Zerolynx** es otra empresa con sede en Alcorcón y presencia Europa enfocada a la Ciberseguridad, la Inteligencia y la Seguridad Patrimonial corporativa.

En Aragón, la empresa **Arasafe Ciberseguridad SL** de Zaragoza, ha desarrollado herramientas contra el ransomware y adquirió recientemente a VUNKERS IT EXPERTS, SL (Lleida).

En Cantabria, la consultora **Neuprotel** ha patentado métodos de verificación y validación de usuarios.

En la C. Valenciana, **Sofistic** https://sofistic.com, la empresa de ciberseguridad de **Grupo Cuatroochenta** https://cuatroochenta.com desarrolla en colaboración con INCIBE un sistema de gestión de alertas de ciberseguridad basado en IA. **Sofistic** está especializada en infraestructuras críticas, banca y salud, ofrece protección preventiva y proactiva, apoyándose en el software de los fabricantes líderes en el mercado. Cuenta con SOC (Security Operations Center) propio 24/7 para ofrecer servicios de gestión, detección y respuesta a incidentes de ciberseguridad (MDR, managed detection and response) a empresas e instituciones en Latinoamérica y España. **Cuatroochenta** es la compañía tecnológica matriz, que desarrolla e implanta software cloud y ciberseguridad para mejorar el rendimiento de las organizaciones. Con 12 oficinas propias en España y América Latina (con especial implantación en Colombia y Panamá) y cotiza desde 2020 en BME Growth, el mercado bursátil español de empresas emergentes

Cloud Levante es otra empresa valenciana de soluciones avanzadas en la nube, inteligencia artificial y ciberseguridad y **nethits**, proveedor global de soluciones TIC para hoteles.

La catalana **GMV** ha patentado tecnologías de seguridad para el IoT usando IA (EP4280534A1).

Otras empresas a tener en cuenta son **Izertis**, grupo con sede principal en Londres y varias sedes en España que presta servicios relacionados con la adopción de la IA en ciberseguridad y **S21sec**, empresa pionera en ciberseguridad con sede en Bilbao (que fue adquirida en 2020 por Thales).

Hay muchas otras empresas activas hoy en España en el sector de la ciberseguridad. En Catalunya, por ejemplo, existen alrededor de 495 empresas de ciberseguridad[27], entre desarrolladores de software y consultoras.

[25] https://www.wisesecurity.com/News/News/Identidad-Descentralizada-Hype-Cycle-Gartner
[26] https://www.sealpath.com/es/blog/2024-ciberseguridad-tendencias-expertos
[27] https://ciberseguretat.gencat.cat/ca/empresa/proveidors-ciberseguretat/index.html

Startups

Asimismo, identificamos numerosas startups activas en el ámbito de la ciberseguridad; por ejemplo en Euskadi[28], [29] **Ironchip** ha desarrollado una solución protección de la identidad mediante tecnologías de IA y geolocalización; **Nymiz**, es una empresa bilbaína de anonimización de datos; **Alias Robotics**, ha recibido financiación del EIC[30] para ofrecer servicios de ciberseguridad para robótica a empresas; **Barbara IoT**, que desarrolla aplicaciones industriales de edge computing e IA; **Eurocybcar** y **Cybentia**, centradas en ciberseguridad para vehículos; **Developair**, software embebido con IA; **Brave Corporation**, empresa bilbaína de pagos con blockchain ; Osane Consulting/**Zerolynx** (Vitoria-Gasteiz/Madrid), entre otras.

Otras startups españolas destacadas[31] son **Occentus Network** que ofrece servicios y soluciones de ciberseguridad gestionada; **Zepo** focalizada en formación de empleados sobre ciberseguridad utilizando simulaciones (similar a Knowbe4); **A3Sec** especializada en la detección, prevención y reacción ante incidentes de ciberseguridad; **BLOOCK** startup de Barcelona que ofrece herramientas de protección de sistemas de información para empresas, utilizando tecnologías descentralizadas; **ByteHide** que ofrece soluciones para creación de software seguro y contra la ingeniería inversa y el robo de datos; **authUSB** de Vigo, que desarrolla dispositivos de protección o **shaadow.io**, con tecnología propia patentada de fuga de documentación (que tiene alianza con Ironchip[32]). **IriusRisk**, de Zaragoza es otra startup que ha obtenido recientemente premio de emprendimiento femenino.

[28] Libro Blanco de la Ciberseguridad en Euskadi 2024 https://www.spri.eus/es/ciberseguridad/libro-blanco-de-la-ciberseguridad-en-euskadi-2024

[29] Up!Euskadi https://startup.spri.eus/dashboard

[30] https://news.aliasrobotics.com/asegura-unada-prestigiosa-financiacion-del-eic

[31] https://www.red.es/es/actualidad/noticias/cinco-empresas-ciberseguridad-segunda-edicion-desafia-nueva-york

[32] https://gaia.es/eu_ES/blog/noticias-asociados-13/post/ironchip-y-shaadow-io-generan-una-solucion-inteligente-para-la-encriptacion-documental-678

Centros de Referencia

Centros de Referencia en América

- **National Security Agency** (NSA), (Estados Unidos) https://www.nsa.gov
- **Cybersecurity and Infrastructure Security Agency** (CISA), (Estados Unidos) https://www.cisa.gov
- **National Institute of Standards and Technology** (NIST), (Estados Unidos) https://www.nist.gov
- **CSET** (Center for Security and Emerging Technology) de la Georgetown University's Walsh School of Foreign Service https://cset.georgetown.edu ofrece analisis basados en datos sobre implicaciones en seguridad de las tecnologías emergentes.
- **CIA** (Central Intelligence Agency) https://www.cia.gov
- **Canadian Center for Cybersecurity** (Canadá) https://www.cyber.gc.ca
- **National Cybersecurity Consortium** (NCC),(Canadá) https://cyber-center.org
- **Portal brasileiro da Cibersegurança** https://ciberseguranca.igarape.org.br del Instituto Igarapé (Brasil) https://igarape.org.br think tank nacional.

Centros de Referencia en Asia y Oriente Medio

- **Ministerio de Defensa de Corea del Sur** (MND) (Corea del Sur) https://www.mnd.go.kr
- **Ciberadministración de China** (CAC), (China) https://www.cac.gov.cn.
- **Indian Computer Emergency Response Team** (CERT-IN), (India) La CERT-In es el equipo de respuesta a emergencias de ciberseguridad en la India https://www.cert-in.org.in
- **Ministerio de Defensa de Japón** (MOD), (Japón). El MOD es el centro de referencia para la ciberseguridad en Japón https://www.mod.go.jp
- **National Cyber Security Agency** (NCSA) (Qatar) https://ncsa.gov.qa.

Centros de Referencia en Europa

- **European Cybersecurity Competence Centre** (ECCC), constituida por 27 centros, uno en cada estado miembro https://cybersecurity-centre.europa.eu/index_en

- **European Union Agency for Cybersecurity** (ENISA) https://www.enisa.europa.eu
- **European cybersecurity Organization** (ECSO) https://ecs-org.eu
- **Plataforma Octopus** del Consejo de Europa (cDE) https://www.coe.int/en/web/octopus plataforma de cooperación e intercambio de información en cuestiones de cibercrimen y evidencia electrónica.

Instituciones nacionales[1]:

- **INCIBE** (España), Instituto Nacional de ciberseguridad https://www.incibe.es
- **GCHQ** (Reino Unido), El Government Communications Headquarters es uno de los centros de referencia más importantes en Europa para la ciberseguridad. Se encarga de proteger la seguridad nacional del Reino Unido y es conocido por sus habilidades en el análisis y la mitigación de ciberamenazas. https://www.gchq.gov.uk
- **Bundesnachrichtendienst** (BND), (Alemania) Servicio de inteligencia alemán https://www.bnd.bund.de.
- **National Cyber Security Agency** (NCSC), (Países Bajos): Centro de referencia para la ciberseguridad en los Países Bajos https://english.ncsc.nl
- **Nationall Cybersecurity and Intelligence Authority** (NCSC), (Suiza) https://www.ncsc.admin.ch/ncsc/en/home.html
- **Federal Chancellery of Austria in cooperation with the Austrian Research Promotion Agency** (Austria) https://www.ncc.gv.at
- **Centre for Cybersecurity Belgium (CCB)** (Bélgica) https://ccb.belgium.be
- **Ministry of Electronic Governance** (Bulgaria) https://egov.bg/wps/portal/egov/en/your%20europe/home
- **Croatian Academic and Research Network** (CARNET)(Croacia) https://www.carnet.hr/en
- **Digital Security Authority** (DSA), (Chipre) https://dsa.cy/en
- **National Cyber and Information Security Agency** (Republica Checa) https://nukib.gov.cz
- **The Danish Business Authority** (Dinamarca) https://danishbusinessauthority.dk
- **Estonian Information System Authority** (RIA), (Estonia) https://www.ria.ee/en
- **Finnish Transport and Communications Agency Traficom's National Cyber Security Centre** (NCSC-FI), (Finlandia) https://www.kyberturvallisuuskeskus.fi/en/homepage
- **Agence nationale de la sécurité des systèmes d'information** (ANSSI), (Francia) https://cyber.gouv.fr
- **National Coordination Centre for Cybersecurity - Federal Office for Information Security** (BSI), (Alemania) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/NKCS/nkcs_node.html
- **National Cybersecurity Authority of Greece** (Grecia) https://cybersecurity-centre.europa.eu/greece-ncc_en

[1] National coordination centers https://cybersecurity-centre.europa.eu/nccs-0_en

- **NCC Eyvör** (Islandia) https://cybersecurity-centre.europa.eu/news/ncc-eyvor-national-cybersecurity-coordination-centre-iceland-2023-11-29_en
- **Governmental Agency for IT Development** (KIFÜ), (Hungria) https://kifu.gov.hu/main-page
- **National Cyber Security Centre** (NCSC), (Irlanda) https://www.ncsc.gov.ie
- **Agenzia per la Cybersicurezza Nazionale** (ACN), (Italia) https://www.acn.gov.it/portale
- **Ministry of Defence** (MOD), (Latvia) https://www.mod.gov.lv/en
- **National Cyber Security Centre, Ministry of National Defence** (Lituania) https://www.nksc.lt/en
- **National Cybersecurity Competence Center** (NC3) (Luxemburgo) https://nc3.lu
- **Malta Information Technology Agenc** (MITA), (Malta) https://mita.gov.mt
- **The Netherlands Enterprise Agency** (RVO), (Países Bajos) https://business.gov.nl
- **Norwegian National Security Authority** (Noruega) https://nsm.no/en
- **National Cybersecurity Department** (Polonia) https://www.gov.pl/web/digitalization/cyber-security-department
- **Centro Nacional de Coordenaçao** (Portugal) https://www.cncs.gov.pt/en/ncc-pt-centro-nacional-de-coordenacao
- **Centrul Național de Coordonare** (Rumanía) https://ncc.gov.ro/1/centrul-national-de-coordonare
- **Cyber Security Competence and Certification Centre** (KCCKB), (Eslovaquia) https://cybercompetence.sk/en
- **Government Information Security Office** (Eslovenia) https://www.gov.si/en/state-authorities/government-offices/government-information-security-office -**Swedish Civil Contingencies Agency** (MSB) (Suecia) https://www.msb.se

Otros centros de referencia en España

Aparte del **Incibe**, otros centros de referencia en el sector a nivel nacional y regional son:

- **Centro Nacional de Inteligencia**, CNI https://www.cni.es/ca
- **Centro Criptológico Nacional**, CCN https://www.ccn.cni.es/index.php
- **CCN-CERT** https://www.ccn-cert.cni.es Computer Emergency Response Team del CCN.
- **Centro nacional de Protección de infraestructuras críticas**, CNPIC https://cnpic.interior.gob.es
- **Redes Territoriales de Especialización Tecnológica** (RETECH) https://espanadigital.gob.es/medida/retech-redes-territoriales-de-especializacion-tecnologica
- **Agencia Española Protección de Datos**, AEPD https://www.aepd.es
- **Plataforma Tecnológica Española de Seguridad Industrial**, PESI https://http://www.pesi-seguridadindustrial.org
- **Centro de Seguridad TIC de la Comunidad Valenciana** (CSIRT-CV) https://www.csirtcv.gva.es
- **Agència de Tecnologia i Certificació Electrònica** (ACCV) https://www.accv.es/va

- **Ciberseguridad Galicia** (foro Ciber.Gal y Centro CEC en creación) https://ciberseguridadegalicia.gal/es
- **Agencia de Ciberseguridad de Cataluña** https://ciberseguretat.gencat.cat/ca/inici/index.html
- **Cybersecurity Innovation HUB** (Castilla y León) https://www.cyberdih.com/
- **SPRI Cybersaintza** https://www.ciberseguridad.eus (Euskadi)
- **ZUIR** - Centro de ciberseguridad industrial de Gipuzkoa https://www.ziur.eus
- **Fundación IDIS** https://www.fundacionidis.com
- **CyberMadrid** https://www.cybermadrid.org/
- **Agencia de Ciberseguridad de la Comunidad de Madrid** (en creación) https://www.comunidad.madrid/transparencia/unidad-organizativa-responsable/agencia-ciberseguridad-comunidad-madrid
- **Andalucía CERT** https://www.juntadeandalucia.es
- **TÜV SÜD** https://www.tuvsud.com proveedor internacional de soluciones de calidad, seguridad y sostenibilidad especializado en certificación, auditoría, ensayo, inspección, asistencia técnica y formación.
- **Oficina de Seguridad del Internauta** (OSI, Incibe) https://www.incibe.es/ciudadania
- **Centro Seguridad TIC de la Comunidad Valenciana** (CSIRT) https://www.csirt.es
- **Agència Balear de Digitalització, Ciberseguretat i Telecomunicacions** (IB Digital) https://www.caib.es/webgoib/agencia-balear-digitalitzaci%C3%B3-ciberseguretat-telecomunicacions

A nivel de Investigación y Desarrollo en España, la **Red de Excelencia Nacional de Investigación en Ciberseguridad**, RENIC https://renic.es ha creadò el Mapa de I+D+I en ciberseguridad que permite conocer el quién es quién en investigación en ciberseguridad en España (toda la información de los equipos de investigación del ecosistema investigador nacional en ciberseguridad).

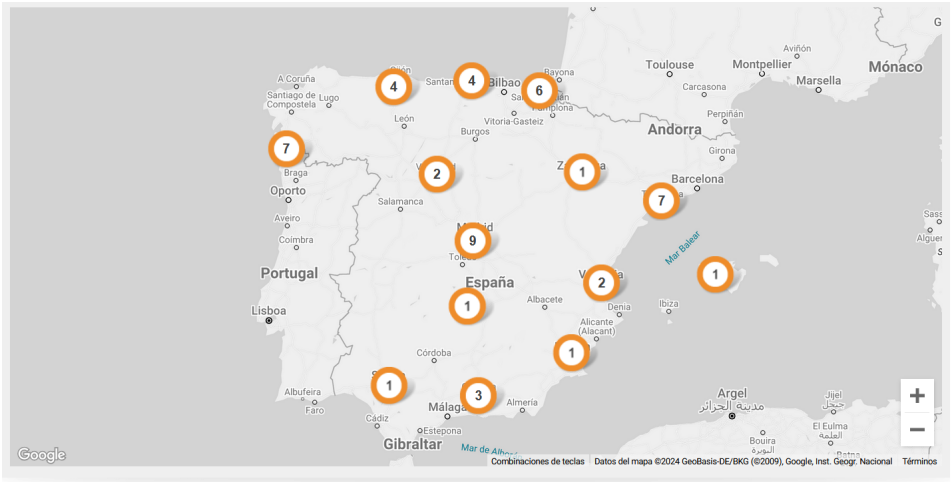


Figura 1: Mapa I+D+I en ciberseguridad. Fuente: renic.es

Perspectivas Futuras y Recomendaciones

En la actualidad, la IA y los grandes modelos de lenguaje (LLM) está siendo utilizada para crear emails o *phishing* elaborados con un lenguaje y un nivel de credibilidad extraordinariamente convincente que hacen mucho más difícil de detectar. También puede escribir código para crear malware.

Pero la buena noticia es que al mismo tiempo la IA y los LLM permiten analizar grandes volúmenes de datos de logs de *firewalls* o archivos de detección de intrusiones y también permite la automatización de tareas como el escaneo de vulnerabilidades o el triaje de incidencias.

La IA, además, posibilita el desarrollo de código y software más seguro, pero, eso sí, debe entrenarse en base a los diferentes tipos de ataques y estar actualizada.

La creciente integración de la IA en la ciberseguridad es inevitable y se volverá más profunda y compleja en las próximas décadas. La IA ofrece el potencial de avances significativos en la forma en que se detectan, previenen y responden a las ciberamenazas.

Recomendaciones y mejores prácticas

En cualquier caso, aprovechar el potencial de la IA en la ciberseguridad requerirá un enfoque estratégico holístico:

- **Integración de los equipos de ciberseguridad e IA**: Establecer una sólida colaboración entre los equipos de ciberseguridad e IA será crucial para garantizar el desarrollo de soluciones de IA que satisfagan necesidades de seguridad específicas
- **Formación continua y mejora de las competencias**: La rápida evolución de las ciberamenazas y la tecnología de IA requiere una formación continua para los profesionales de la ciberseguridad. Esta formación debe incluir tanto las capacidades como las amenazas asociadas a la IA generativa
- **Diseño de sistemas robustos y resistentes**: Los sistemas que integran IA deben estar diseñados para ser robustos y resistentes para resistir condiciones adversas, recuperarse rápidamente de fallos o ataques y manejar circunstancias impredecibles

- **Calidad y seguridad de los datos**: La eficacia de los sistemas de IA depende en gran medida de la calidad, la relevancia y la seguridad de los datos con los que se entrenan. Garantizar la integridad de los datos e implementar las medidas de seguridad adecuadas es primordial
- **Consideraciones éticas y regulaciones**: A medida que la IA se integra más profundamente en la ciberseguridad, es crucial abordar los desafíos éticos y regulatorios. Las cuestiones de responsabilidad, equidad y privacidad deben considerarse cuidadosamente, y se deben desarrollar y mantener regulaciones apropiadas
- **Adopción gradual y pruebas (en *sandboxes*)**: Se recomienda implementar sistemas basados en IA de forma gradual en entornos controlados o sandboxes antes de la implementación a gran escala. Esto permite la identificación y resolución de problemas en un entorno controlado
- **Colaboración e intercambio de inteligencia**: Compartir información sobre amenazas, vulnerabilidades y mejores prácticas dentro de la comunidad de ciberseguridad es esencial para mantenerse a la vanguardia de las tácticas de ciberdelincuencia en evolución. Hará falta ser mucho más proactivos y anticipativos y estar al muy día de las nuevas amenazas.

Direcciones Futuras en Investigación y Desarrollo

Esta naturaleza cada vez más compleja y dinámica de los ciberataques, junto a la rápida evolución de la IA requiere de una investigación y desarrollo continuos para crear soluciones efectivas y proactivas.

Áreas clave de Investigación y desarrollo en curso

- **Sistemas de ciberdefensa autónomos**: se espera que la IA desempeñe un papel clave en la creación de sistemas de defensa autónomos capaces de identificar, analizar y responder de forma independiente a las ciberamenazas. Los investigadores están desarrollando sistemas de IA que van más allá de la detección de amenazas y puedan **responder automáticamente a los incidentes** de seguridad. Estos sistemas tomarían decisiones en tiempo real sobre cómo mitigar o neutralizar las amenazas sin intervención humana. Los enfoques de detección de intrusiones basados en aprendizaje automático (*Machine Learning-Based Intrusion Detection*) y los desarrollos que aprovechan el **aprendizaje profundo** para la **detección de ataques sofisticados en tiempo real** toman cada vez más relevancia, ya que se constata las técnicas tradicionales basadas en firmas ya no son suficientes para detectar ataques nuevos o modificados (*zero-day attacks*).

- **Aprendizaje continuo y vigilancia del entorno**: Los futuros sistemas de IA podrán aprender continuamente de nuevos datos y experiencias, lo que les permitirá adaptarse a las amenazas emergentes y mejorar su rendimiento con el tiempo
- **IA explicable (XAI)**: La IA explicable o XAI[1] es un área de investigación importante, cuyo objetivo es hacer que las decisiones de IA sean transparentes y comprensibles. Comprender por qué un sistema de IA toma una decisión específica con respecto a la detección de amenazas o la respuesta a incidentes es crucial para la confianza y la confiabilidad en estos sistemas.
- **IA cuántica**: A medida que la computación cuántica se vuelve más frecuente, se espera que surja la IA cuántica, que ofrezca velocidades de procesamiento sin precedentes y la capacidad de manejar problemas de seguridad actualmente intratables.
- **Colaboración humanos-máquina**: El futuro de la ciberseguridad probablemente contará con sistemas colaborativos en los que humanos y máquinas trabajen juntos, combinando la experiencia humana con la potencia de procesamiento y las capacidades analíticas de la IA, para crear una defensa más robusta.
- **IA perimetral**[2]: El uso de la IA en los dispositivos periféricos, tales como sensores de dispositivos de IoT, permitirá la detección y respuesta a amenazas en tiempo real en el perímetro de la red (es decir, combinando IA y Edge computing[3]), sin depender constantemente de la infraestructura de la nube.
- **Seguridad de Aplicaciones**: El hackeo de aplicaciones se esta volviendo uno de los principales vectores de accion en brechas de seguridad [4], por tanto, este segmento es uno de los que está acaparando mayor atención por parte de los inversores.
- **Seguridad 5G** El desarrollo de las redes 5G networks amplían los campos de ataque y implican muchos más puntos de entrada, por lo que presenta nuevos desafíos de seguridad que deben ser mucho más integrales.
- **Blockchain** tecnologías blockchain están siendo usadas por una variedad de aplicaciones de cybersecuridad. La tecnología blockchain puede ser utilizada para proteger la integridad de los datos, garantizar la autenticidad de los usuarios y proporcionar una mayor transparencia en la gestión de la seguridad. Empresas como **Slowmist** https://www.slowmist.com ofrecen soluciones en este ámbito.
- **Aprendizaje federado**: este enfoque permite que los modelos de IA se entrenen en dispositivos o servidores descentralizados mientras se mantienen los datos locales, lo que mejora la privacidad. Ello es especialmente relevante para las aplicaciones de ciberseguridad, en las que la confidencialidad de los datos es primordial.

[1] https://www.ibm.com/es-es/topics/explainable-ai
[2] https://www.ibm.com/es-es/topics/edge-ai
[3] https://www.ibm.com/es-es/topics/edge-computing
[4] https://www.barracuda.com/products/application-protection

Recomendaciones futuras de investigación y desarrollo

Las mayoría de fuentes consultadas recomiendan varias áreas para futuras investigaciones y desarrollos:

- Formalizar los **marcos de certificación para una IA fiable**: Establecer normas de certificación claras para las tecnologías, los productos y los servicios de IA es esencial para garantizar su fiabilidad, seguridad y uso ético. En Europa la Ley de IA[5] recientemente aprovada, es el primer marco jurídico sobre IA que aborda los riesgos de la IA y ofrece a los desarrolladores e implementadores de IA requisitos y obligaciones bastante claros en relación con los usos específicos de la IA. En EE.UU. organizaciones como Rand Corporation están explorando mecanismos de autorregulación, como iniciativas de etiquetado y códigos de conducta para las aplicaciones de IA.
- **Vigilancia de amenazas emergentes**: A medida que la tecnología de IA evoluciona, también lo hacen las amenazas que plantea. La investigación debe centrarse en comprender y mitigar las amenazas emergentes, especialmente las que surgen de los últimos avances tecnológicos. Esto requiere un monitoreo constante del panorama de amenazas y un enfoque proactivo para la investigación de seguridad
- **Desarrollo de herramientas de IA explicables**: Herramientas como LIME y SHAP[6] ya están contribuyendo a una IA explicable.
- **Promoción de la privacidad y la ética**: La investigación debe abordar las implicaciones éticas y de privacidad del uso de la IA en la ciberseguridad. La privacidad no debe sacrificarse por la seguridad. El desarrollo futuro debe centrarse en garantizar que las soluciones de IA se diseñen e implementen teniendo en cuenta la privacidad y las consideraciones éticas
- **Realización de pruebas y validaciones rigurosas**: Antes de implementar soluciones basadas en IA en entornos del mundo real, es crucial realizar pruebas y validaciones exhaustivas. Esto garantiza que las soluciones sean sólidas, fiables y capaces de gestionar las amenazas del mundo real
- **Incentivar la innovación**: Los gobiernos y las organizaciones privadas deben ofrecer incentivos para la innovación en ciberseguridad e IA, bien en forma de subvenciones, concursos o programas de reconocimiento para fomentar la investigación, el desarrollo y la creación de nuevas soluciones.

[5] https://digital-strategy.ec.europa.eu/es/policies/regulatory-framework-ai
[6] https://www.datacamp.com/es/tutorial/explainable-ai-understanding-and-trusting-machine-learning-models

Recomendaciones para Empresas e Investigadores

Según apuntan informes recientes como el de Sonicwall[7] y otros[8], en 2024 han augmentado de forma considerable el ransomware y los ataques DDoS double dipping [9] (tipo de ataque que implica dos ataques consecutivos). También han augmentado los ataques en la *supply chain*, esto es, ataques a proveedores con quienes nos relacionamos y que nos afectan (aunque no nos ataquen a nosotros, podemos recibir las consecuencias de ataques sufridos por proveedores más débiles dentro de nuestra red de suministro y operativa y hay que poder gestionarlos); por ello se enfatiza la necesidad de asegurar la protección de los sistemas CI/CD [10] que los desarrolladores utilizan para crear sofware y que los ciberdelincuentes pueden usar para focalizarse en componentes de terceros[11]; en este sentido, algunas de las principales recomendaciones, pasan, entre otros aspectos, por:

- Implementar un **plan de respuesta al ransomware**
- Incrementar la **seguridad del correo electrónico** de negocio (BEC) (Aunque el ransomware acapara los titulares de los medios, los ataques de Compromiso del correo electrónico de negocio son mucho más numerosos)
- Priorizar la rápida **aplicación de parches** (la aplicación regular de parches es esencial, ya que mitiga las vulnerabilidades y reduce el riesgo de explotación por parte de los cibercriminales - que atacan a una velocidad alarmante).
- Desarrollar una **estrategia de privacidad de datos sólida**. Implementar medidas de Identificación multifactor (MFI) (Sigue siendo común ver organizaciones que no implementan MFA, lo cual facilita drásticamente los ataques)
- **Proteger los sistemas y datos en la nube** (p.ej. con medidas como el Security Service Edge (SSE)[12] y la Arquitectua de red Zero Trust (ZTNA)[13])
- **Proteger el ecosistema de IoT** en expansión y la convergencia IT-OT[14], exige un enfoque de múltiples capas.
- Invertir en la **formación del personal en ciberseguridad** (La mayoría de las brechas de ciberseguridad incluyen algún grado de error humano. La mejor forma de combatir estos

[7] Informe semestral de Ciberamenazas 2024 de SonicWall https://www.sonicwall.com/es-mx/resources/white-papers/mid-year-2024-sonicwall-cyber-threat-report
[8] https://blogs.salleurl.edu/es/tendencias-en-ciberseguridad-2024-lo-que-debes-sabe
[9] https://insights.cybcube.com/en/ransomware-and-the-double-dipping-trend
[10] continuous integration and continuous delivery/continuous deployment
[11] https://www.paloaltonetworks.com/cyberpedia/what-is-ci-cd-security
[12] https://www.netskope.com/es/security-defined/security-service-edge-sse
[13] https://www.paloaltonetworks.es/cyberpedia/what-is-zero-trust-network-access-ztna
[14] https://www.redseguridad.com/especialidades-tic/convergencia-it-y-ot-la-ciberseguridad-en-un-mundo-interconectado_20241120.html

errores es reducir las oportunidades y aumentar la formación. Los empleados deben ser conscientes de las amenazas y saber cómo protegerse)

- Los **ejercicios de ciberseguridad**, para probar y mejorar la preparación de las organizaciones en función de los marcos establecidos y ayudar a las organizaciones a comparar su postura de seguridad y priorizar los esfuerzos de mejora.
- Invertir en **soluciones de seguridad basadas en IA**
- La **vigilancia tecnológica y el monitoreo proactivo** de la tecnología para mantenerse informado y a la vanguardia frente a las amenazas que surgen constantemente y las soluciones innovadoras.
- Mejorar el **alineamiento entre el negocio y la participación de la Dirección** [15]

Asimismo, los aspectos básicos de protección y seguridad para el usuario medio siguen siendo primordiales:

- **asegurar las redes** (gestión de pasaportes fuertes, actualizaciones, usar firewalls, etc.)
- **proteger la identitad** (sistemas de autentificación fuertes, enfasis en la autentificación multifactor (MFA), estar alertado contra phishing)
- **control de los dispositivos** (drivers y software actualizados con los últimos patches de seguridad y controlar los settings de seguridad) datos (encriptacion de datos, vigilar el uso compartido online, backups regularmente, etc.)
- **application workloads** (apps actualizadas, leer los permisos que aceptamos y asegurar el origen oficial de las apps que usamos)
- El **elemento humano** (formación en ciberseguridad y ciber-resiliencia, monitoreo continuo de nuevas tecnologías y amenazas y tener un plan para gestionar emergencias).

Visión a Largo Plazo y Sostenibilidad

La mayoría de los estudios esbozan una visión a largo plazo de un futuro digital seguro y resiliente impulsado por la IA, el cual requiere un enfoque colaborativo y proactivo que implique, entre otros:

- **Inversión en I+D**: La investigación y el desarrollo continuos en IA y ciberseguridad son esenciales para impulsar la innovación, abordar las amenazas emergentes y descubrir nuevas soluciones

[15] https://www.deloitte.com/es/es/services/risk-advisory/research/estado-ciberseguridad.html

- **Abordar la brecha de habilidades**: Los esfuerzos para abordar la creciente brecha de habilidades en ciberseguridad son cruciales. Esto incluye la promoción de programas de educación y formación, la mejora y el reciclaje profesional de los profesionales existentes y el fomento de una cultura que fomente las carreras de ciberseguridad
- **Cooperación y regulaciones internacionales**: El desarrollo de estándares y regulaciones globales para el uso ético y responsable de la IA en la ciberseguridad es primordial.
- **Fomentar una cultura de ciberseguridad**: Promover la concienciación sobre la ciberseguridad y las mejores prácticas entre las personas y las organizaciones es esencial para crear un entorno digital más seguro

Impacto potencial en la industria y la sociedad

Se espera que la adopción generalizada de la IA en la ciberseguridad tenga un impacto significativo tanto en la industria como en la sociedad en su conjunto:

- **Mejora de la seguridad de las empresas**: las soluciones de ciberseguridad impulsadas por la IA pueden ayudar a las empresas de todos los tamaños a mejorar su postura de seguridad, proteger sus datos y sistemas, y mitigar los riesgos de forma más eficaz.
- **Transformación de las funciones de los profesionales de la ciberseguridad y nuevas oportunidades de empleo**: Al automatizar las tareas rutinarias, la IA puede liberar a los profesionales de la ciberseguridad para que se centren en retos más complejos y estratégicos. Al mismo tiempo, la creciente demanda de experiencia en IA y ciberseguridad conducirá a la creación de nuevas oportunidades de trabajo en estos campos, impulsando el crecimiento económico.
- **Protección mejorada de las infraestructuras críticas**: la IA puede desempeñar un papel fundamental en la protección de las infraestructuras esenciales frente a los ciberataques, garantizando la estabilidad y la seguridad de los servicios vitales.
- **Mayor confianza en el mundo digital**: Al fomentar un entorno digital más seguro, la IA puede contribuir a generar confianza en el mundo digital, promoviendo el crecimiento económico y el progreso social.

Si se consiguen abordar estos retos, se anticipa un futuro en el que los sistemas impulsados por IA puedan adaptarse y aprender en tiempo real, lo que lleva a una mejor protección contra las amenazas en evolución. Se espera que estos sistemas reduzcan los tiempos de respuesta a incidentes y mejoren la capacidad de prevenir violaciones antes de que ocurran.

Algunas Conclusiones

Resumen de Hallazgos Clave

Se ha realizado una revisión sistemática de las principales tecnologías que están siendo desarrolladas en el ámbito de la Ciberseguridad, a partir de la información contenida en las invenciones protegidas por patentes en todo el mundo, seguido de una la revisión de otras fuentes de mercado y estudios secundarios recientes, con el fin de ofrecer un panorama actualizado de los últimos avances, tendencias y actores clave a tener en cuenta en el sector.

Principales áreas de desarrollo tecnológico

Fruto de la exploración tecnológica, hallamos que las principales áreas de desarrollo tecnológico que se han venido llevando a cabo en los últimos años se relacionan con la detección basada en firmas (*attack signature detection*) (que a pesar de sus limitaciones -los ataques son cada vez más mutantes- es una de las áreas principales de desarrollo); la detección de anomalías; la emulación de actividades sospechosas; el análisis de vulnerabilidades; las contramedidas a los ataques distribuidos de denegación de servicio (DDoS); las máquinas virtuales seguras o *sandboxes* y el Aprendizaje Automático.

Son áreas de desarrollo que han ganado mayor relevancia en los últimos años:

- La **criptografía cuántica**,
- El **reconocimiento de patrones**,
- Las **arquitecturas de pagos**
- Las **TIC para operaciones médicas remotas**

Los principales **actores globales en ciberseguridad** en cuanto a desarrollo de tecnología son grandes empresas tecnológicas como Microsoft e IBM y grandes empresas especializadas en cibersecuridad, tales como Palo Alto Networks, McAfee, Sophos, FireEye, CrowdStrike, Qomplx, Radware; empresas de telecomunicaciones tales como Huawei, British Telecom o Nippon Telegraph y empresas de servicios financieros tales como Bank of America o Capital One.

Por **tipo de ciberataque** identificamos que un 8% de los desarrollos patentados abordan directamente soluciones a ataques *phishing*; un 7,2% plantean soluciones técnicas a ataques *DDoS*; el *ramsomware* es tratado un 4% y los ataques de *vectores* en 3%.

Lideran los desarrollos actuales de nuevas soluciones técnicas a problemas relacionados con el ***phishing*** empresas como Knowbe4, Microsoft, IBM, McAfee, Paypal, Lookout, Vade Secure, Netskope, Sophos, Servicenow, Riskiq, Proofpoint, la china Dbapp Security, Shape Matrix, Sanofor, Fireeye, entre otras.

En cuanto a I+D actual en relación al ***Ransomware***, son activas Microsoft, EMC, Dell, IBM, McAfee, British Telecomm, Amazon, Huawei, Rubrik, Datto/Kaseya, Airgap, Palo Alto Neworks, Commvault, Acronis o Secuve.

Trabajan específicamente en desarrollos de aplicaciones de la **IA para Ciberseguridad** empresas como IBM, Tencent, Samsung, Baidu, la corporación State Grid China, la aseguradora Ping An, Huawei, Microsoft, así como numerosos centros de investigación chinos como la Universidad de Zhejiang, entre otras muchas.

En España, empresas como Sofistic, empresa de ciberseguridad de Grupo Cuatroochenta, desarrolla en colaboración con INCIBE un sistema de gestión de alertas de ciberseguridad basado en IA.

En **Criptografía y Ciberseguridad** operan empresas como Microsoft, Wiz, Qomplx, Saudi Arabian Oil, Aramco, Fireeye, Proofpoint, Bank Of America Battelle Memorial Institute, Google, Trend Micro, As0001, Bitsight Tech, Expel, Honeywell, Sands Lab, Senseon Tech, Capital One, Rapid7, Revelstoke Security, Fractal Ind, Mandiant) y específicamente en nuevos desarrollos relacionados con **Criptografia Cuántica** encontramos a empresas como: Lucomm Tech, IBM, Lacework, Microsoft, Atombeam, Pure Storage, Bitsight Tech, GE, Revelstoke Security, Intel, At&T, Vmware o Zscaler.

En España, empresas como la donostiarra Multiverse Computing, proponen la aplicación de métodos basados en IA e inpirados en la cuántica para clusterización de datos.

En **ciberseguridad para operaciones remotas de salud** tienen desarrollos patentados empresas como Biotronik, Advanced Neuromodulation Systems, Fenwal, Cilag, Hoffmann La Roche, Dexcom Lifelens Tech,Quantaira, Thirdwayv, Zoll Medical Corp, dexcom, Acorai, Bayer Healthcare, Cohere Health, Ethicon o Fresenius.

En España, la spin-off de telefónica KOA Health aplica sistemas de ciberseguridad específicamente en aplicaciones de tratamiento de la salud mental.

Principales tendencias del Mercado

Fruto de la revisión de las tendencias del mercado, encontramos que toman relevancia en los últimos años aspectos tales como:

- **La IA y el aprendizaje automático**: El aprendizaje automático (ML) se utiliza cada vez más para la detección y respuesta a amenazas, ofreciendo una identificación proactiva de vulnerabilidades y actividades maliciosas. Sin embargo, tal y com se ha apuntado,

la IA también puede ser explotada por los atacantes (la IA cada vez se utiliza más, por ejemplo, para aumentar la efectividad de los ataques de *phishing*, con mensajes cada vez más personalizados y multifacéticos), lo que requiere una cuidadosa consideración.

- El **Cifrado resistente a la cuántica**: En EE.UU. la aprobación por parte del NIST[1] de algoritmos de cifrado resistentes a la cuántica supone un enfoque proactivo para abordar las futuras amenazas que plantea la computación cuántica, salvaguardando la infraestructura digital. Se espera que la criptografía postcuántica (PQC) empiece a ser adoptada pronto, incluso antes de su estandarización, como una solución basada en software que funcione en sistemas convencionales para proteger los datos de futuros ataques cuánticos[2].
- El **enfoque de confianza cero** (*zero trust*)[3]: El modelo de confianza cero, que está ganando terreno, hace hincapié en la verificación y validación de todas las acciones, incluso por parte de los usuarios autorizados, subrayando el principio de "no confiar en nadie, verificarlo todo".
- La **privacidad de los datos como prioridad**: La creciente concienciación de los consumidores y las estrictas normativas como el RGPD están impulsando a las organizaciones priorizar la privacidad de datos. Ello incluye la implementación de soluciones tecnológicas relacionadas con la gestión de derechos digitales. Recientemente, la *Ley de Ciberresiliencia* [4] impone estándares obligatorios para el diseño, el desarrollo, la producción, la entrega y el mantenimiento de los productos digitales comercializados en el mercado de la UE, con la finalidad de mitigar las ciberamenazas.
- **Asegurar el IoT**: La proliferación de dispositivos IoT requiere mayores medidas de seguridad. La implementación de protocolos de seguridad estandarizados, estándares de cifrado universales y certificaciones de seguridad obligatorias es crucial.
- **Seguridad en la nube**: A medida que aumenta la adopción de la nube, la seguridad de los entornos en la nube es primordial. Los atacantes se dirigen a las vulnerabilidades de la infraestructura en la nube, lo que exige estrategias de seguridad sólidas para la protección de datos. Gartner predice que la seguridad en la nube crecerá un 24.7%.
- **Arquitecturas de nube híbrida**: Estos sistemas se enfocan en la integración fluida entre la infraestructura local y la nube. En las estructuras organizacionales de hoy, donde el intercambio de información de dentro y fuera es cada vez más difuso, los modelos de

[1] https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards
[2] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2023/m06/from-ai-to-quantum-innovating-for-a-better-world.html
[3] https://www.forbes.com/councils/forbestechcouncil/2024/11/13/the-rise-of-zero-trust-cybersecurity-and-trust-in-it
[4] https://www.redseguridad.com/actualidad/ley-ciberresiliencia-ue-ciberseguridad-europa_20241121.html

nube híbrida ofrecen flexibilidad y escalabilidad, al tiempo que permiten a las organizaciones mantener el control sobre los datos confidenciales, logrando un equilibrio entre seguridad e innovación .

Implicaciones para el Sector y Recomendaciones

Perspectivas Futuras

En un entorno de alta complejidad, gran inestabilidad geopolítica y en plena transformación digital de las empresas (que implica un incremento de su dependencia tecnológica al estar cada vez más hiperconectadas), sumado al boom actual de la inteligencia artificial, los ciberataques, cada vez más sofisticados,se han convertido en uno de los principales riesgos para cualquier organización y que pueden impactar drásticamente en su integridad.

En este contexto, ser capaces de incorporar soluciones basadas en inteligencia artificial (IA) de una forma eficiente y controlada, se está volviendo un reto primordial en las estrategias de ciberseguridad de las organizaciones, que deben ser cada vez más integrales, proactivas y resilientes. Será más importante que nunca invertir en formación del personal, en cultura sobre ciberseguridad y en vigilancia tecnológica y monitoreo proactivo de la tecnología para ser capaces de asimilar y aprovechar las nuevas tecnologías y mantenernos siempre informados y actualizados frente a amenazas cambiantes y soluciones innovadoras.

Referencias

Bibliografía y Fuentes Consultadas

- Caldwell (2021) Cybersecurity Patent Landscape https://caldwelllaw.com/news/cybersecurity-patent-landscape-2021
- CCN-CERT IA_35-23 Ciberamenazas y Tendencias (Noviembre 2023) https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7188-ccn-cert-ia-35-23-ciberamenazas-y-tendencias-edicion-2023/file.html
- CCN-CERT BP-30 Aproximación a la Inteligencia Artificial y la ciberseguridad (Octubre 2023) https://www.ccn-cert.cni.es/es/informes/informes-ccn-cert-publicos/7195-ccn-cert-bp-30-aproximacion-a-la-inteligencia-artificial-y-la-ciberseguridad-1/file.html
- ENISA Threat Landscape 2024 (19 de Septiembre, 2024) https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
- European Cybersecurity Investment Platform (19 Octubre, 2022) https://www.eib.org/en/publications/20220206-european-cybersecurity-investment-platform
- Foro Nacional de la Ciberseguridad(2022) Informe sobre la industria e investigación española en ciberseguridad https://www.observaciber.es/sites/observaciber/files/media/documents/industria-investigacion-ciberseguridad-2022.pdf
- ITU (2024) Global Cybersecurity Index https://www.itu.int/hub/publication/d-hdb-gci-01-2024
- IS decisions blog (21 de Noviembre, 2023) Exploring the evolving landscape of cybersecurity patents and innovations https://www.isdecisions.com/en/blog/it-security/cybersecurity-innovations-patent-landscape
- Keri Pearlson hbr (Julio, 2024) When Cyberattacks Are Inevitable, Focus on Cyber Resilience https://hbr.org/2024/07/when-cyberattacks-are-inevitable-focus-on-cyber-resilience
- Observaciber (Incibe y Ontsi) https://www.observaciber.es
- Pitchbook 2024 information security overview https://pitchbook.com/news/reports/2024-information-security-overview

- Surveilling the Masses with Wi-Fi-Based Positioning Systems 23 May 2024 https://arxiv.org/abs/2405.14975
- The Washington post (Julio, 2024) A fatal program update: How CrowdStrike crashed global computer system https://www.washingtonpost.com/technology/2024/07/19/bosd-outage-microsoft-crowdstrike
- Venture in security (2023) Generalist VC firms in cybersecurity https://ventureinsecurity.net/p/generalist-vc-firms-in-cybersecurity
- Venture in society (2022) Global cybersecurity startup ecosystem map: a founder's guide https://ventureinsecurity.net/p/global-cybersecurity-startup-ecosystem
- WEF Word Economic Forum (16 de Enero, 2024) Global Cybersecurity Outlook 2024 https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

Enlaces a Recursos Adicionales

- ECSO Market radar https://ecs-org.eu/activities/market-radar
- Cisco 2023 Cybersecurity Readiness Index https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html
- Preparedness and Resilience Enforcement for Critical Infrastructure Cascading Cyber-physical Threats and effects with focus on district or regional protection https://cordis.europa.eu/project/id/101021668
- Forbes (14 de Noviembre, 2024) Companies Need To Invest In Digital Resilience https://www.forbes.com/councils/forbesfinancecouncil/2024/11/14/beyond-cybersecurity-why-companies-need-to-invest-in-digital-resilience
- ECSO (2 de Octubre, 2024) White Paper: Cyber Exercise Scenario Development https://ecs-org.eu/?publications=white-paper-cyber-exercise-scenario-development
- Grupo Gimeno destaca en el evento GoDigital con una ponencia sobre Ciberseguridad de Alto Impacto https://www.grupogimeno.com/grupo-gimeno/grupo-gimeno-destaca-en-el-evento-godigital
- Hacker news Cyber Attack News https://thehackernews.com/search/label/Cyber%20Attack
- LISA News https://www.lisanews.org
- GenAI's Impact on Cybersecurity https://www.informationweek.com/it-leadership/genai-s-impact-on-cybersecurity
- WEF Word Economic Forum(16 de Enero 2024) Estas son las tendencias cibernéticas que los líderes tendrán que navegar en 2024 https://es.weforum.org/stories/2024/01/estas-son-las-tendencias-ciberneticas-que-los-lideres-tendran-que-navegar-en-2024
- Top 10 resources about the business of cybersecurity (27 de Octubre, 2023) https://ventureinsecurity.net/p/top-10-resources-about-the-business
- cyber security intelligence https://www.cybersecurityintelligence.com

- Vulnerability database https://vuldb.com
- Informe semestral de Ciberamenazas 2024 de SonicWall https://www.sonicwall.com/threat-report
- Pitchbook (8 de Julio, 2024) IPO Watchlist: The cybersecurity startups most likely to go public https://pitchbook.com/news/articles/ipo-watchlist-cybersecurity-startups
- Cybasque (2023) Caracterización del sector de la ciberseguridad en Euskadi https://www.cybasque.eus/web/content/3113474
- Redes Territoriales de Especialización Tecnológica (RETECH) https://www.incibe.es/retech
- Ciberseguridad https://ciberseguridad.com Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas
- Krebs on security https://krebsonsecurity.com
- Deloitte (18 de Abril, 2024) El estado de la ciberseguridad en España https://www.deloitte.com/es/es/services/risk-advisory/research/estado-ciberseguridad.html
- cybersecurity intelligence https://www.cybersecurityintelligence.com
- LISA Institute https://www.lisainstitute.com
- Campus Internacional de Ciberseguridad https://www.campusciberseguridad.com
- Directiva Europea NIS2 https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- Red seguridad https://www.redseguridad.com
- FIRST, Global Forum of Incident Response https://www.first.org
- Trusted Introducer https://www.trusted-introducer.org
- SANS Empowering Cyber Security Practitioners & Teams https://www.sans.org
- APWG https://apwg.org
- ENS Gobernanza de la ciberseguriddad nacional CNN-CERTT-CNI https://gobernanza.ccn-cert.cni.es/certificados
- Venture Radar Top Quantum cryptography Companies https://www.ventureradar.com/keyword/Quantum%20cryptography
- Cuadernos de seguridad https://cuadernosdeseguridad.com