Observatorio de Defensa y Seguridad

Cátedra de Ciberseguridad

Informe de Prospectiva 2024

RED HORIZONTES ISDEFE

Madrid, 28 de noviembre de 2024

TABLA DE CONTENIDOS

FIGURAS

TABLAS

1. INTRODUCCIÓN

1.1. OBJETIVO DEL INFORME

Nuestro informe tiene como objetivo revelar las principales tendencias y predicciones de ciberseguridad para el próximo año: desde el auge de la IA en la ciberseguridad hasta la creciente importancia de la seguridad móvil, profundizaremos en lo que depara el futuro para este sector crítico.

De acuerdo con la Estimaciones de Cybersecurity Ventures, el impacto del cibercrimen, en términos de daños a las víctimas, habría superado los 8 billones de dólares durante 2023, con expectativas que ven 10 billones como posible objetivo para 2025. En 2015, este volumen de negocio se cuantificó en el orden de 3 billones dólares.

Se trata de cifras objetivamente extraordinarias, que sitúan al cibercrimen como una auténtica industria a escala global capaz de competir directamente con el PIB de las naciones más poderosas del mundo. En una clasificación ideal, el cibercrimen ocuparía de hecho el tercer lugar, precedido sólo por gigantes como Estados Unidos y China.

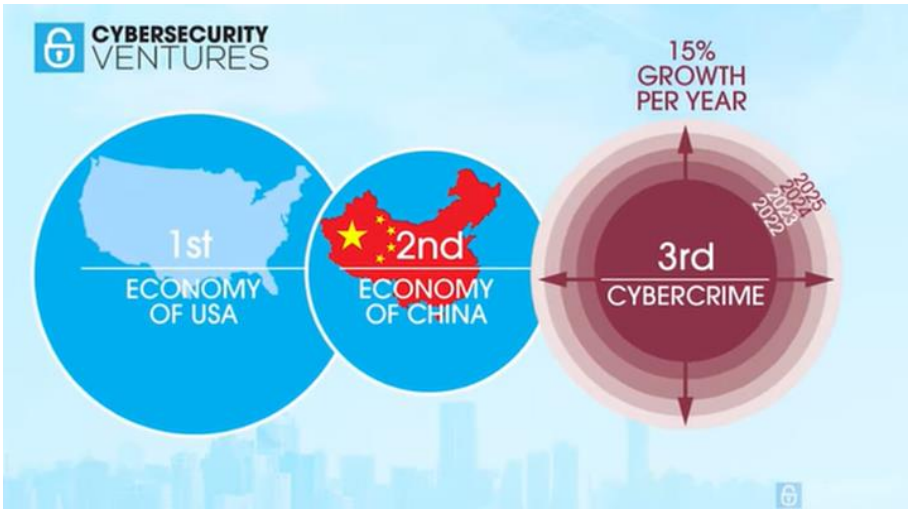


Figura 1. Estimaciones Cybersecurity Ventures.[1]

Este informe de prospectiva forma parte de los trabajos realizados por la Cátedra de Ciberseguridad ISDEFE-UAH (Universidad de Alcalá) dentro del Observatorio de Defensa y Seguridad de la Red Horizontes ISDEFE en 2024.

1.2. CONTEXTO

A medida que nos adentramos en el año 2024, el ámbito de la ciberseguridad se tambalea al borde de un cambio transformador. Las ciberamenazas no sólo están aumentando en frecuencia, sino que también se están volviendo más sofisticadas, desafiando los paradigmas de seguridad tradicionales. En este panorama

[1] https://cybersecurityventures.com/cybersecurity-almanac-2023/

https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Última consulta en marzo de 2024

digital en rápida evolución, comprender las tendencias futuras es una cuestión de previsión y necesidad de preparación.

Para ejemplificar la rápida evolución del entorno podemos analizar el informe de ENISA (Agencia para la Ciberseguridad de la Unión Europea) llamado “IDENTIFYING EMERGING CYBER SECURITY THREATS AND CHALLENGES FOR 2030 MARCH” [01] de marzo de 2023 que, aunque con una visión a más largo plazo (2030), seguramente haría más hincapié en algunos de las amenazas y tendencias que expone, como la número 10, habiendo pasado solo un año desde su publicación.

Figura 2. Top 10 Amenzas Emergentes para el 2030 [01]

Podremos usar como base los informe de la propia ENISA sobre lo ocurrido en 2023 [02] y el del Centro Criptológico Nacional [03], como punto de partida para tratar de predecir lo que pasará en 2024.

Figura 3. Panorma de Amenzas de ENISA[02]

Antes de adentrarnos en lo que pensamos que sucederá en 2024, hagamos primero una ligera retrospectiva en aquello que ha sucedido en el año 2023.

2. FACTORES DE INFLUENCIA

Sin ánimo de ser exhaustivos, vamos a tratar de identificar los principales factores que pueden influir en el futuro del sector de la Ciberseguridad tanto positiva como negativamente. Algunos podrán encuadrarse en más de uno de los tipos que hemos determinado.

2.1. FACTORES NORMATIVOS

Sabemos que la ciberseguridad es un ámbito en constante transformación y evolución, fuertemente influenciado por un marco normativo cada vez más complejo y exigente. Estos marcos legales de obligado cumplimiento dependen del país y del sector en el que opere una institución u organización y establecen los requisitos mínimos que deben cumplir para proteger sus sistemas, datos y la privacidad de los usuarios.

La normativa y legislación suele ser de ámbito nacional, pero puede venir generada por una transposición de una norma emanada de algún organismo internacional con el que se tengan acuerdos de cumplimiento obligatorio.

Entre otras muchas de carácter sectorial, creemos que las que más están impactando y lo seguirán haciendo en el futuro son las siguientes por su carácter generalizado:

- Directiva NIS2. Esta directiva europea establece requisitos más estrictos para la seguridad de las redes y sistemas de información en sectores críticos y establece nuevas normas de notificación de incidentes.
- RGPD/GDPR: Aunque enfocado en la protección de datos personales, tiene implicaciones directas en la ciberseguridad al exigir medidas técnicas y organizativas adecuadas para proteger la información. Es uno de los más estrictos en cuanto a privacidad y seguridad de datos. Obliga a las empresas a proteger los datos personales de los ciudadanos de la UE y a notificar cualquier brecha de seguridad. El impacto que ha tenido en las organizaciones desde su aparición ha sido muy importante.
- ENS: El Esquema Nacional de Seguridad es una normativa que tiene por objetivo establecer la política de seguridad en la utilización de medios electrónicos relacionados con la administración pública, y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. El ámbito de aplicación del Esquema Nacional de Seguridad comprende todo el sector público, los sistemas de información de entidades del sector privado cuando presten servicios a entidades del sector público y los sistemas que traten información clasificada.
- AIA: El Reglamento Europeo de Inteligencia artificial (AIA, Artificial Intelligence Act) busca regular los usos de la Inteligencia Artificial para limitar los riesgos que de ellos se derivan. Su ámbito de aplicación se extiende a: proveedores de sistemas de IA que se pongan en servicio o comercialicen dentro de la UE o cuya salida se utilice en la UE, independientemente de su origen; y a usuarios de los mismos, considerando usuarios a quienes explotan esos sistemas, y no a los afectados.
- DORA: Es la norma que establece obligaciones en materia de ciberseguridad a las empresas del sector financiero (banca y seguros) pero, también, a todas las empresas que les prestan servicios relacionados con IT y de aquí que trascienda al ámbito propio de aplicación como le sucede al Esquema Nacional de Seguridad.

2.2. FACTORES GEOESTRATÉGICOS

La ciberseguridad no es asunto meramente técnico, sino que está profundamente vinculado en el contexto geopolítico y geoestratégico global. Las relaciones internacionales, los conflictos, la competencia económica y las políticas nacionales influyen significativamente de manera diversa y compleja en el panorama de las amenazas cibernéticas

- Conflictos y tensiones internacionales. En todas sus múltiples facetas. Guerra hibrida, guerra cibernética, espionaje industrial, propaganda y desinformación, ataques a infraestructuras críticas, pero también en forma de cibercrimen organizado operando a escala global
- Tratados Transnacionales. La ciberseguridad es un desafío global que requiere una respuesta coordinada a nivel internacional. Los tratados y alianzas como la OTAN, la UE y tratados internacionales sobre ciberseguridad pueden fortalecer la cooperación y la defensa mutua contra ciberamenazas. Estas alianzas permiten compartir información y recursos para mejorar la ciberseguridad global.

2.3. FACTORES ECONÓMICOS

Al igual que con los factores geoestratégicos, tenemos que insistir en el carácter no exclusivamente técnico de la ciberseguridad. Al contrario, está, por ejemplo, profundamente influenciada por factores económicos que moldean las amenazas, las respuestas y las políticas a nivel global.

- Regulación y Cumplimiento. Las leyes y regulaciones sobre protección de datos y ciberseguridad pueden imponer costes adicionales a las empresas para asegurar el cumplimiento. Las sanciones pueden restringir el acceso a tecnologías críticas y aumentar la vulnerabilidad.
- Coste de los Ciberataques. Pérdidas financieras directas: Robo de dinero, fraude electrónico, extorsión por ransomware. Daño a la reputación: Pérdida de clientes, disminución de la confianza en la marca. Costes de recuperación: Gastos en sistemas de seguridad, investigaciones forenses, tiempo de inactividad.
- Concienciación y Formación. Las organizaciones deben invertir en tecnologías y personal capacitado para proteger sus sistemas.

2.4. FACTORES TECNOLÓGICOS

La constante y rápida evolución de las tecnologías emergentes, como la inteligencia artificial y el Internet de las cosas (IoT), requiere inversiones constantes para mantenerse al día con las nuevas amenazas.

- IA. La inteligencia artificial se utilizará tanto para variar la tipología de los ataques como para mejorar las defensas. Los atacantes utilizarán la IA para automatizar ataques, evadir las defensas y desarrollar malware más evasivo. Habrá más ataques sofisticados, pero no mayor sofisticación en los ataques. Por otro lado, se utilizará para mejorar la detección de amenazas, la respuesta a incidentes y la automatización de tareas de seguridad, detectando patrones de comportamiento anómalos y respondiendo a amenazas en tiempo real.
- Redes 5G. Las redes 5G permitirán nuevas aplicaciones y servicios, pero también aumentarán la superficie de ataque. Mejorará la velocidad y la conectividad, pero introduciendo nuevas vulnerabilidades debido a la mayor cantidad de dispositivos conectados y la complejidad de la infraestructura.
- La computación y la transmisión cuántica están ya revolucionando la criptografía, planteando riesgos significativos con la rotura de los sistemas de cifrado actuales.

- IoT/IIoT. La difusión de estos dispositivos creará una superficie de ataque más grande y expondrá a las organizaciones a nuevos riesgos. Además, muchos dispositivos IoT tienen vulnerabilidades de seguridad inherentes, lo que los convierte en objetivos fáciles para los atacantes. Complicándose todo en el sector industrial donde podría afectar a infraestructuras críticas.
- La nube ofrece ventajas en términos de agilidad y costes, pero también introduce nuevos riesgos, como la pérdida de control sobre los datos. La responsabilidad de la seguridad en la gestión de accesos y la protección de datos sensibles tendrá que ser compartida entre el proveedor de la nube y el cliente.

2.5. FACTORES POLÍTICOS

Las decisiones y acciones de los gobiernos, las relaciones internacionales y los intereses geopolíticos tienen un impacto significativo en el panorama de las amenazas cibernéticas. Ya hemos hablado en epígrafes anteriores sobre la influencia de la legislación y regulaciones, así como de la importancia de la cooperación internacional.

FACTORES DE INFLUENCIA	
Factores normativos	*RGPD, NIS2, DORA, ENS, AIA*
Factores geoestratégicos	*Conflictos Internacionales, Tratados Transnacionales.*
Factores económicos	*Regulación y Cumplimiento, Coste de los Ciberataques, concienciación y Formación*
Factores tecnológicos	*IA, 5G, Computación Cuántica, IoT/IIoT, Computación en la nube*
Factores políticos	*Legislación y Regulaciones, Cooperación Internacional*

Tabla 1. Resumen de factores de influencia en el sector de la Ciberseguridad.

3. IDENTIFICACIÓN DE TENDENCIAS

3.1. TENDENCIAS ACTUALES

En su “Balance de Criminalidad” [04], correspondiente al segundo trimestre del año 2023, el Ministerio del Interior sostiene lo siguiente:

“como hecho asociado a la penetración y el uso de internet en España (en especial en las crecientes formas de comercio y compras online) que se observa desde hace ya algunos años y de manera muy significativa desde 2016, se ha producido un incremento de las modalidades de criminalidad agrupadas bajo el concepto de cibercriminalidad, sobre todo un fuerte incremento de las estafas cometidas por medios informáticos”

En concreto, la criminalidad aumentó en España un 5,9% en el año 2023 arrastrada por el alza de la ciberdelincuencia, que fue del 25,5%.

Según este informe el año 2023 cerró con cerca de 2,5 millones de infracciones penales, de las que casi dos millones corresponden a la delincuencia convencional (un 2,1 % más que en 2022) y 470.388 son ciberdelitos.

De ellos, el 90% son estafas informáticas, que crecen un 27% con respecto al año anterior. Interior destaca que en 8 años este tipo de estafas han aumentado un 508%, dado que en 2016 apenas se registraron 70.178.

Esto no hace más que confirmar lo que ya predecía el Allianz Risk Barometer en su encuesta que incluía todos los posibles riesgos y situaba en primer lugar los Ciberincidentes.

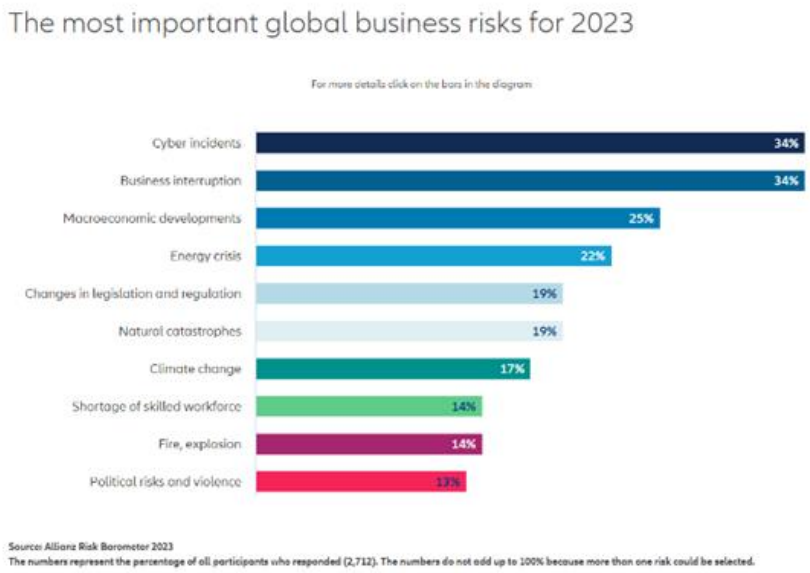


Figura 4. Riesgos más importantes en 2023[2]

[2] https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html#download

Última consulta en marzo de 2024.

En todo caso el cibercrimen es un problema global. Ningún país del mundo está inmune a ser atacado. Veamos aquí cuales son los 10 principales países afectados por ciberataques en 2023 según SentinelOne [05]. España se sitúa en el top 10

Figura 5. 10 principales países afectados por ciberataques en 2023 [05]

Podemos ver en la Figura 6 los sectores que han estado más en el punto de mira de los atacantes a nivel mundial.

Estos sectores se suelen elegir en base a tres factores claves: 1. La importancia de sus datos y su reputación. 2. La capacidad y voluntad potencial para pagar un rescate. 3. El estado general de la seguridad del objetivo

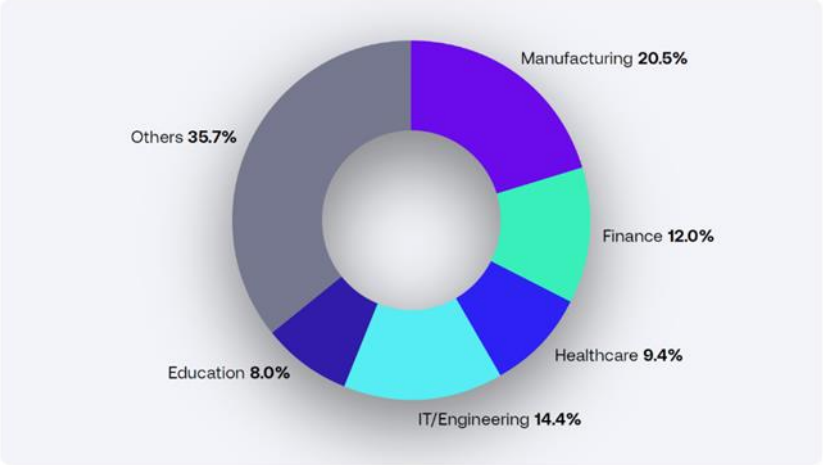


Figura 6. Sectores en el punto de mira [05]

Por lo que respecta a España, el 2023, se ha visto marcado por una serie de tendencias emergentes que han configurado la estrategia y las operaciones de las organizaciones en todos los sectores.

Fundamentalmente se ha comprobado un aumento del ransomware y phishing[3]:

Consistentemente con los años anteriores, el ransomware sigue siendo una de las amenazas más frecuentes y dañinas. Los ataques de phishing también han aumentado, convirtiéndose en el vector más común para la infiltración de sistemas, evidenciando la necesidad de reforzar la formación en concienciación de seguridad.

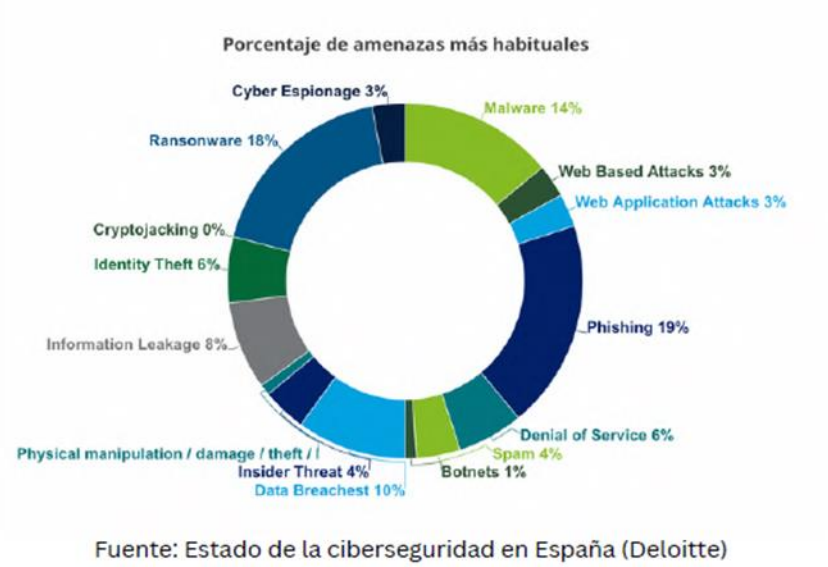


Figura 7. Estado de la Ciberseguridad en España[3]

3.2. TENDENCIA EMERGENTES

Elegimos, precisamente, como tendencias emergentes también estas dos (ransomware y phishing), aunque desde hace años sean una realidad, porque la aparición en escena de la IA Generativa, está haciendo que el número de actores que las utilizan en sus ciberdelitos aumente considerablemente

Y, por supuesto, también incluiremos la IA pero no solo la generativa si no también, y de manera muy importante, la IA clásica (predictiva/discriminativa).

3.2.1. RANSOMWARE

Los ataques de ransomware, en los que los ciberdelincuentes cifran datos críticos y solo liberan la contraseña de descifrado después de pagar un rescate, son ahora más temidos que nunca. Según la

[3] https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html

Última consulta en marzo de 2024

encuesta The State of Ransomware 2023, realizada por el proveedor de seguridad Sophos [06] entre 3.000 ejecutivos de TI de 14 países, el 66% de las empresas se vieron afectadas por al menos un ataque de ransomware el año pasado. De estos ataques, el 76% resultó en datos cifrados y en el 30% de los casos, incluso hubo robo de datos.

En particular, las tácticas de extorsión múltiple están aumentando. En otros informes sobre Ransomware publicados los ciberdelincuentes cometieron robo de datos en un promedio del 70 % de los casos (a mediados de 2021, la tasa era solo del 40 % en promedio). En aproximadamente el 50% de los ataques de Ransomware encontrados por el Equipo de Respuesta a Incidentes de la Unidad 42 de Palo Alto Networks, la causa fue una "superficie de ataque desprotegida".

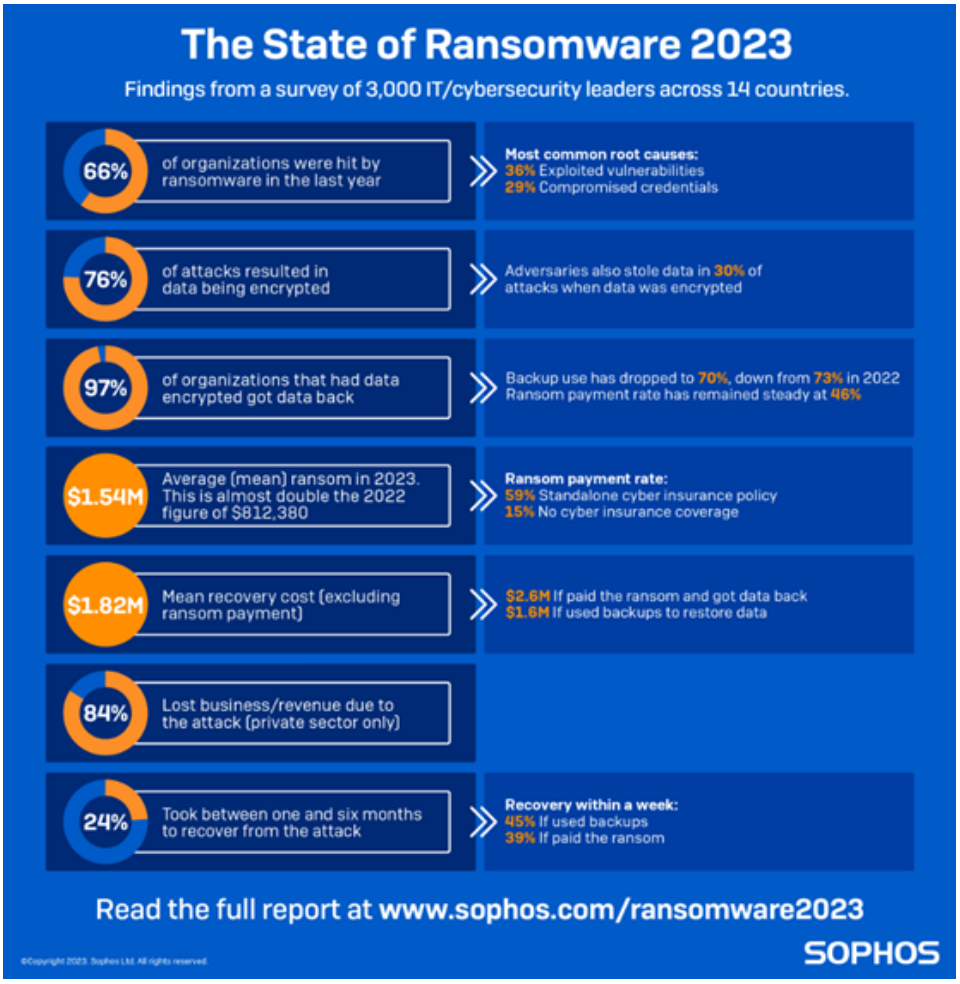


Figura 8. Estado del Ransomware en 2023 [06]

El “Watchtower. Intelligence-Driven Threat Hunting Endo of Year 2023” de SentinelOne [05] nos da el siguiente ranking de grupos dedicados al Ransomware en 2023.

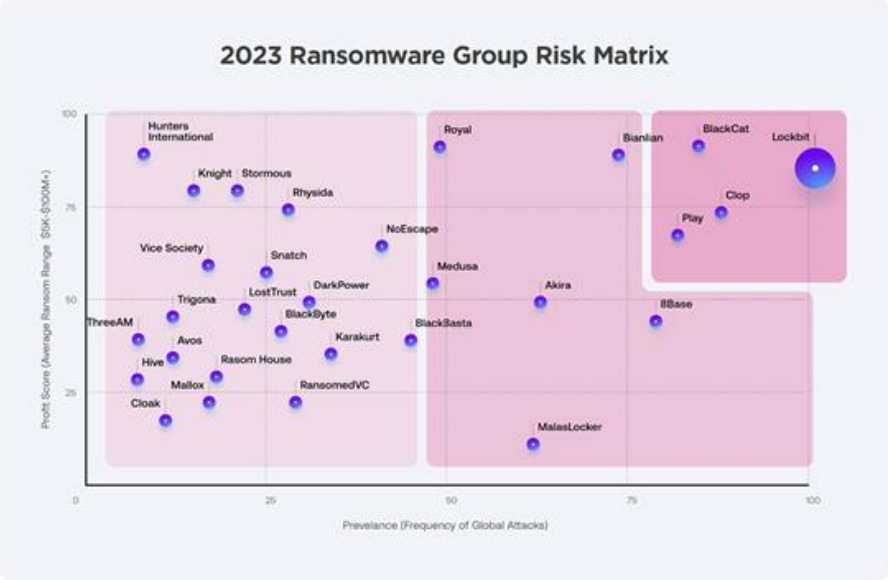


Figura 9. Grupos de Ransomware [05]

3.2.2. PHISING

Según la revista IT Digital Magazine en su sección de Seguridad [4], los ataques por correo electrónico durante 2023 aumentaron un 222%

España es uno de los tres países que fueron objetivo de más ataques de malware en el último trimestre de 2023.

España ocupa el 10º puesto entre los países con un mayor porcentaje de URLs maliciosas bloqueadas en diciembre de 2023, con un 13,4%.

Según datos de Check Point Research las empresas más suplantadas durante el último cuatrimestre del año pasado serían:

- El portal de Internet y servicio de correo electrónico Yahoo (20%), a través de emails que anunciaban premios falsos.
- La empresa de logística internacional DHL (16%), cuya suplantación se produjo sobre todo alrededor del Black Friday.
- La compañía tecnológica multicanal conocida por todos, Microsoft (11%).
- El buscador más famoso de Internet, Google (5,8 %).
- La red social profesional LinkedIn (5,7%).
- El servicio de transferencia de archivos WeTransfer (5,3%).
- La plataforma de streaming Netflix (4,4%).

[4] https://www.itdigitalsecurity.es/actualidad/2024/02/los-ataques-por-correo-electronico-durante-2023-aumentaron-un-222

Última consulta en marzo de 2024

- Otra empresa de logística que opera a nivel mundial, FedEx (2,5 %),
- La firma de servicios financieros HSBC (2,3 %).
- El servicio de mensajería instantánea WhatsApp (2,2%).

En cualquier caso, como podemos ver en la web del Anti-Phishing Working Group (APWG) en su Phishing Activity Trends Reports [5] la tendencia ha seguido siendo al alza.

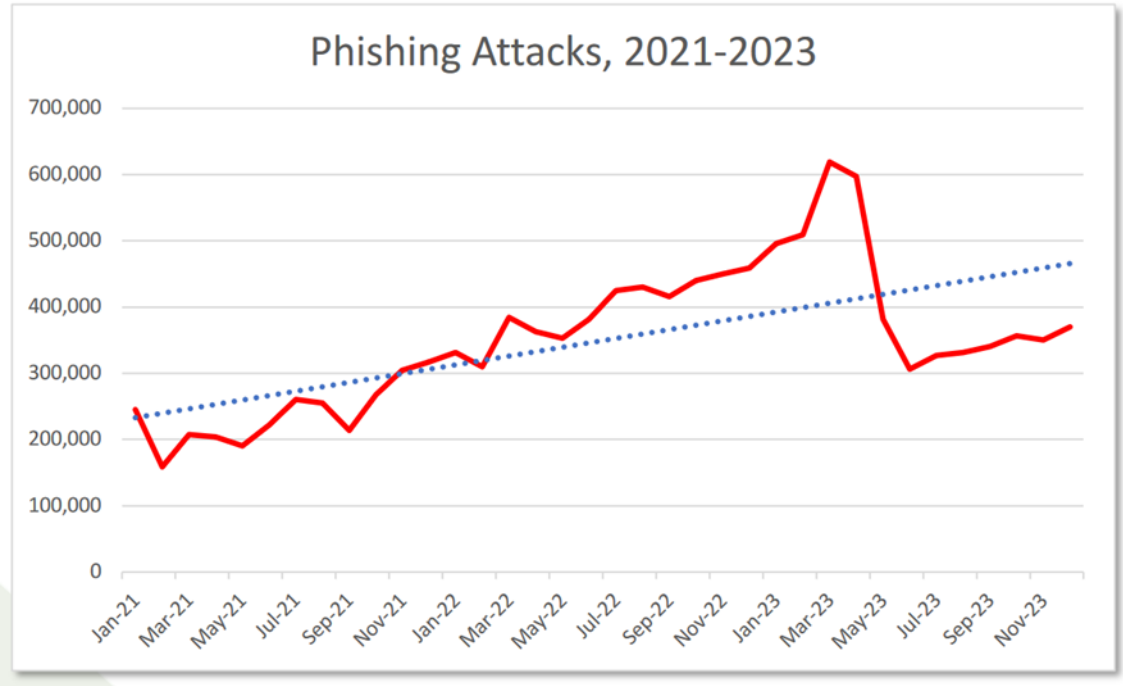


Figura 10. Tendencia en los ataques de phising[5]

3.2.3. INTELIGENCIA ARTIFICIAL

La inteligencia artificial, tradicional y generativa, ha asumido progresivamente un papel tan crucial en el campo de la ciberseguridad que sería simplista considerarla una tendencia "de lista" proyectada para 2024. Ya durante 2023 parecía evidente que la IA es cada vez más utilizada tanto por atacantes y defensores de sistemas y datos para completar sus respectivas actividades. Podemos ver un muy buen resumen en su Informe de Buenas Prácticas del CCN-CERT titulada “Aproximación a la Inteligencia Artificial y la Ciberseguridad” de octubre de 2023. [07]

[5] https://apwg.org/trendsreports/

Última consulta en marzo de 2024

4. ESCENARIOS FUTUROS

Conforme el mundo se vuelve más digitalizado e interconectado, la oportunidad de sufrir ataques es mayor que nunca. Además, el aumento de las nuevas tecnologías y las crisis geopolíticas alimentan los ciberataques y los hacen más efectivos. Como resultado, en 2024, la pregunta para muchos ya no será si se verán afectados, sino cuándo.

Veamos un top 10 de posibles escenarios futuros seleccionados por nosotros a la vista y lectura de numerosos informes que se citan en cada caso y teniendo muy presente también el número 158 de febrero de 2024 de la Revista SIC titulado: “Ciberataques 2024: la ciberdelincuencia se afila los dientes”[6].

4.1. INTELIGENCIA ARTIFICIAL Y CIBERSEGURIDAD

Con la introducción de la IA en todos los segmentos del mercado, esta ha traído enormes cambios en la ciberseguridad. La IA ha sido fundamental en la creación de sistemas de seguridad automatizados, procesamiento del lenguaje natural, detección facial y detección automática de amenazas. Sin embargo, también se utiliza para desarrollar malware y ataques inteligentes para eludir los últimos protocolos de seguridad en el control de datos. Los sistemas de detección de amenazas habilitados por IA pueden predecir nuevos ataques y notificar a los administradores sobre cualquier violación de datos al instante.

La carga cada vez más pesada que supone implementar nuevas tecnologías y mantener la ciberseguridad con un número de empleados fijo o cada vez menor se traduce en que cada administrador debe ocuparse de más cosas. Afortunadamente, la inteligencia artificial y la automatización avanzan con rapidez, lo que permite pasar de la gestión y configuración de dispositivos individuales a la definición de políticas para todo el parque y su aplicación automática y coherente

“En 2026, la tecnología de inteligencia artificial generativa (GenAI) representará el 20 % de la configuración inicial de la red, lo que supone un aumento desde casi cero en 2023”.[7]

Según Radware en su informe “2024 Global Threat Analysis Report” [08] lo que puede ocurrir es lo siguiente:

“Si bien los LLM (Large Language Models y, más específicamente, los Generative Pre-Trained Transformers) pueden mejorar la productividad y la sofisticación hasta cierto punto, en última instancia están sujetos a sus datos de entrenamiento. Los LLM no se limitan a lenguajes naturales, sino que también se destacan en reproducir y generar lenguajes de programación. Los actores de amenazas menos capacitados pueden aprovechar los LLM para crear scripts de ataque o malware más complejos, pero estos ataques y piezas de malware aún están limitados por el conocimiento incorporado en el modelo LLM. Por lo tanto, el aumento de la sofisticación radica más en la cantidad de ataques con una sofisticación promedio más alta que en su complejidad y sofisticación inherentes.”

[6] https://revistasic.es/revista-sic-numero-158/

Última consulta en marzo de 2024

[7] Gartner®, Research Hoja de ruta estratégica para las redes empresariales. Brown, Munch, Leibovitz y Lerner, octubre de 2023.

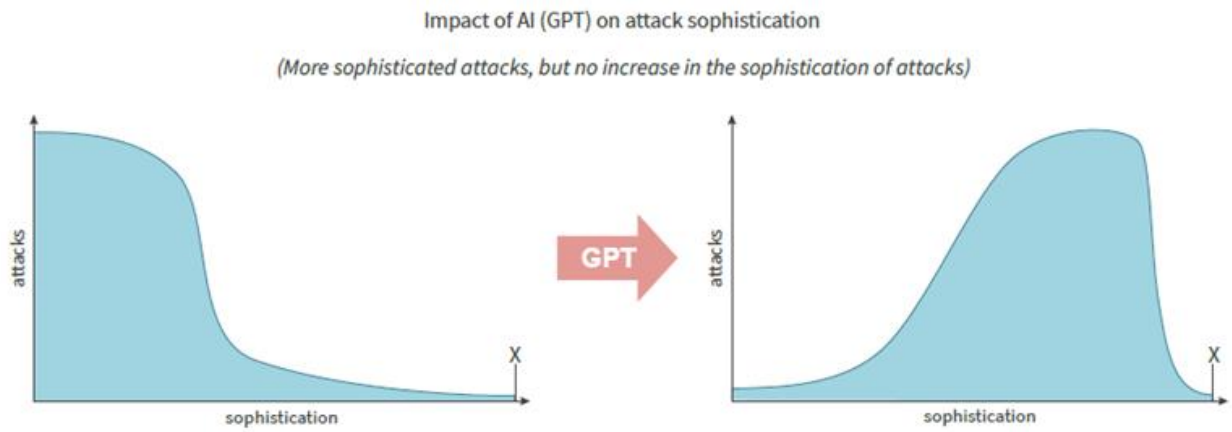


Figura 11. Impacto de los LLM en los tipos de ataques [08]

4.2. COMPUTACIÓN Y TRANSMISIÓN CUÁNTICA. SU IMPACTO EN LA CIBERSEGURIDAD.

Aunque aún en sus fases iniciales, la computación cuántica ha empezado ya a tener un impacto en la ciberseguridad. Las organizaciones pioneras comenzarán a experimentar con la tecnología para mejorar la seguridad de sus datos, preparándose para futuras amenazas cuánticas.

Se espera que el mayor uso de la computación y la transmisión cuántica sea uno de los riesgos cibernéticos en 2024. Los ordenadores cuánticos pueden romper los métodos de los criptógrafos clásicos, lo que genera posibles amenazas cibernéticas. Por lo tanto, los expertos en ciberseguridad deberán adoptar algoritmos criptográficos resistentes a los cuánticos para proteger los datos confidenciales de futuros ataques cuánticos, adoptar criptografía postcuántica para proteger la integridad y la confidencialidad de los datos, y desarrollar e implementar métodos criptográficos resistentes a los cuánticos.

Ya, a principios de 2023, el Institute for Business Value de IBM en su informe titulado “Security in the quantum computing era The risk is real, the need is now” [09] prevenía sobre múltiples facetas que se van a ver afectadas.

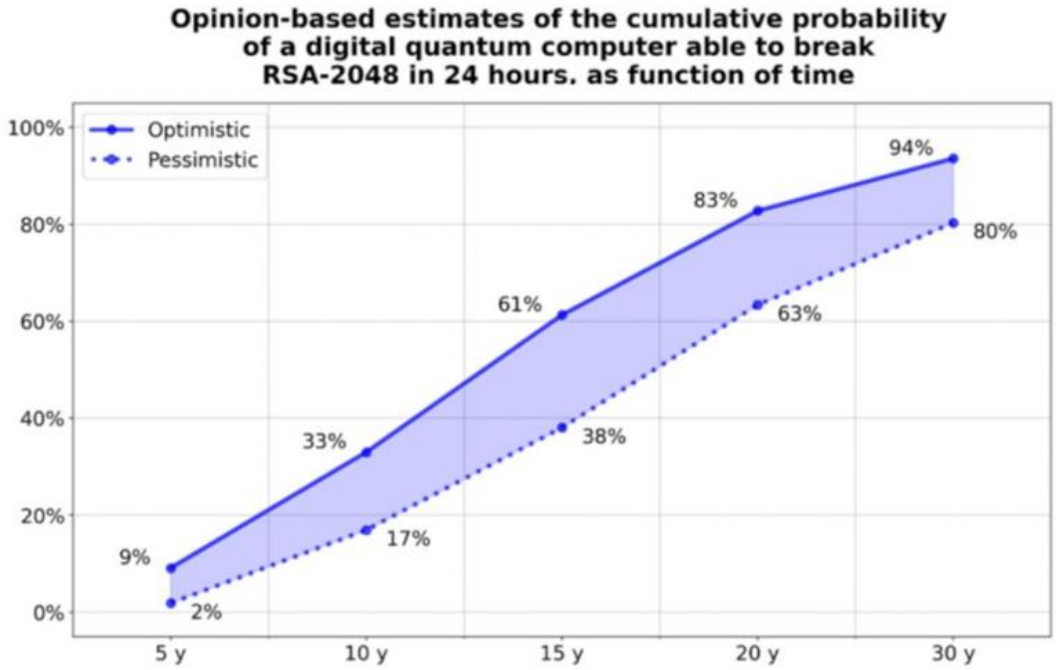


Figura 12. Probabilidad de romper RSA 2048 en 24 horas [09]

Vemos también como actores fundamentales en la utilización de las tecnologías para desestabilizar otros países y acoger a cibercriminales están invirtiendo fuertemente en Computación Cuántica[8].

[8] https://www.newtral.es/tecnologias-cuanticas-que-son-y-por-que-los-paises-invierten-en-ellas/20221027/#google_vignette

Última consulta en marzo de 2024

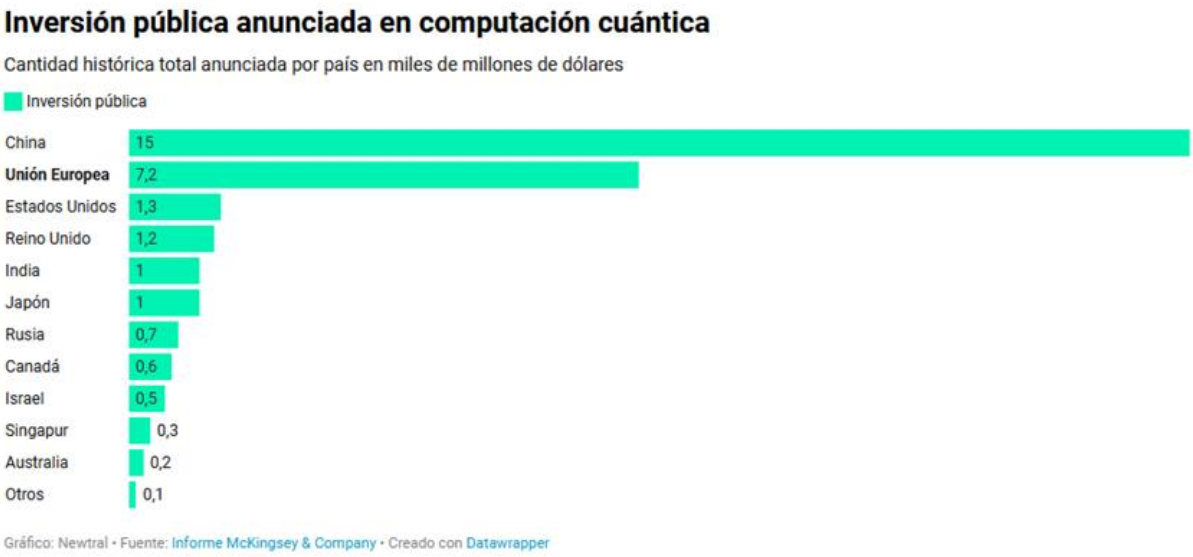


Figura 13. Inversión pública en computación cuántica6.

4.3. DISPOSITIVOS MÓVILES

En el informe de “Pronóstico de Ciberseguridad de Google Cloud para 2024” podemos leer: [9]

“En 2024, anticipamos que los ciberdelincuentes o estafadores continuarán empleando tácticas novedosas de ingeniería social, como simular servicios de ayuda doméstica, mensajes de cuentas falsas en redes sociales, bancos o funcionarios gubernamentales y alertas emergentes falsificadas para engañar a las víctimas e instalar aplicaciones maliciosas en sus dispositivos móviles.”

Esto, unido al continuo aumento del número de dispositivos móviles [10], así como de sus diferentes usos, hace que vayan a ser el objetivo casi número uno en cuanto a tipo de dispositivo.

Los ciberdelincuentes están trasladando el campo de batalla a nuestros teléfonos y tabletas.

Tenemos que prepararnos para un aumento de los problemas móviles, desde malware hasta troyanos bancarios que apuntan estratégicamente a nuestros datos de inicio de sesión. Prepararse para ataques de phishing en los que los ciberdelincuentes intentan manipularnos para que usemos nuestros datos de inicio de sesión auténticos en sitios engañosos.

Nuestros dispositivos móviles albergan un tesoro de información personal y financiera. Pensemos en las repercusiones de una infracción, desde el robo de identidad y el fraude financiero hasta el acceso no autorizado a sus datos más confidenciales. A medida que nos adentramos en el año 2024, proteger nuestros dispositivos móviles es primordial.

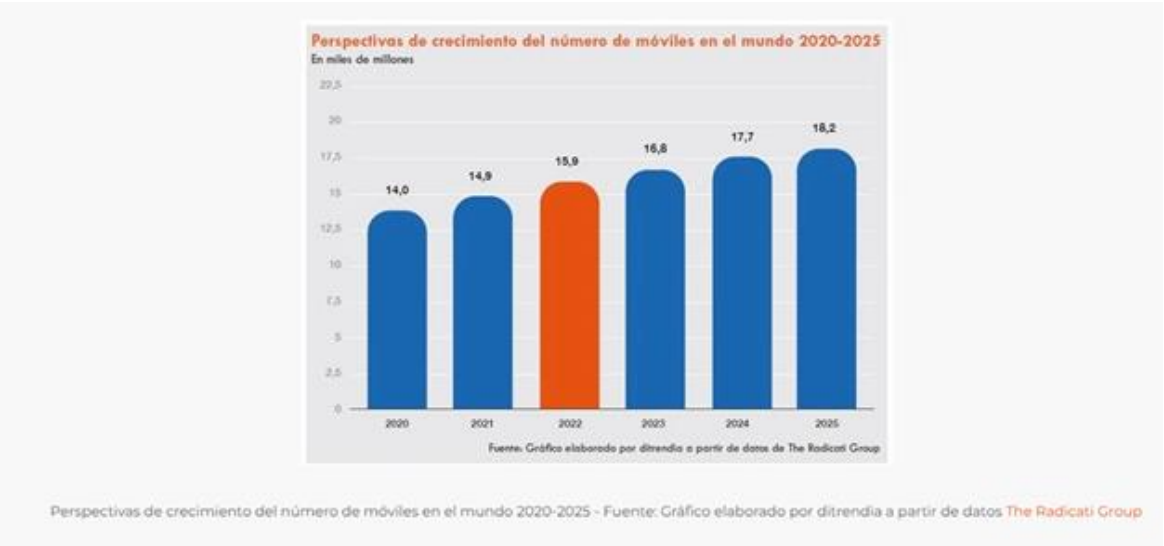


Figura 14. Crecimiento de número de móviles [10].

[9] https://cloud.google.com/resources/security/cybersecurity-forecast?hl=es

Última consulta en abril de 2024

[10] https://mktefa.ditrendia.es/blog/estadisticas-sobre-m%C3%B3viles-2023

Última consulta en marzo de 2024

4.4. SEGURIDAD IOT E IIOT EN LA ERA DEL 5G.

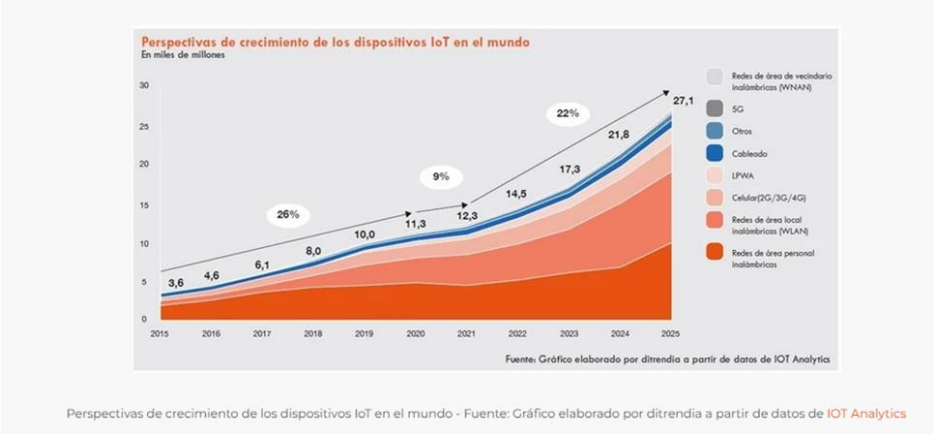
De cara a 2024, el Internet de las cosas (IoT) sobre todo en su faceta industrial (IIoT) sigue creciendo exponencialmente, creando interconexiones entre un número cada vez mayor de dispositivos. Sin embargo, esta expansión trae consigo una serie de desafíos de seguridad. La diversidad y ubicuidad de los dispositivos de IoT e IIoT los convierten en objetivos atractivos para los ciberataques, y su naturaleza interconectada puede generar vulnerabilidades generalizadas.

Los sistemas IoT son prácticos, rápidos de configurar y sencillos de utilizar, hasta el punto de que su uso está muy extendido incluso en entornos domésticos. La desventaja es que los ciberdelincuentes conocen muy bien y son muy hábiles para explotar esas situaciones, sobre todo con las credenciales de acceso obsoletas, que los usuarios finales a menudo pasan por alto.

Según datos proporcionados por la empresa TUVRheinland, en la actualidad hay aproximadamente 42 mil millones de equipos conectados por IoT y se espera que este número aumente hasta 76 mil millones en 2035 con el consiguiente riesgo añadido.

En 2024, la atención se centrará principalmente en mejorar la seguridad de IoT a través de diversas herramientas. Se esperan avances significativos en el desarrollo de protocolos de seguridad más sólidos y estandarizados para dispositivos IoT. Esto podría incluir estándares de cifrado universales y certificaciones de seguridad obligatorias para nuevos dispositivos. Otra área de mejora podría ser la integración de algoritmos de IA y ML en los sistemas de IoT. Estas tecnologías pueden monitorear patrones inusuales que indican una infracción, lo que permite una respuesta más rápida a las amenazas.

Además, es probable que se ponga más énfasis en educar a los usuarios sobre la seguridad de IoT. A medida que los usuarios sean más conscientes de los riesgos potenciales y las mejores prácticas, la seguridad general de las redes de IoT mejorará. Finalmente, es posible que veamos un aumento en el uso de la tecnología blockchain para centralizar y proteger las redes de IoT, haciéndolas menos vulnerables a los ataques dirigidos a sistemas centralizados. En general, estos avances apuntan a un ecosistema de IoT más seguro y resiliente en 2024.



Perspectivas de crecimiento de los dispositivos IoT en el mundo - Fuente: Gráfico elaborado por ditrendia a partir de datos de IOT Analytics

Figura 15. Crecimiento de dispositivos IoT[11].

[11] https://mktefa.ditrendia.es/blog/estadisticas-sobre-m%C3%B3viles-2023

Algunas vulnerabilidades de IoT e IIoT a considerar:

- Ataques a instalaciones y software de gestión de edificios que pueden mantener sin disponibilidad de electricidad, agua y energía a una ciudad entera. Los atacantes pueden llevar a cabo ataques de ransomware extremadamente dañinos, dejando vulnerables las aplicaciones de IoT.
- Comunicaciones no seguras
- Protocolos de red inseguros
- Protocolos de red obsoletos, sin cifrar o configurados incorrectamente

De ello se deduce que los profesionales de la ciberseguridad tendrán que proteger cada vez más los dispositivos IoT e IIoT, con soluciones ad hoc para cada tipo de dispositivo. Además, será cada vez más necesario proteger la transmisión, el almacenamiento y la gestión del ciclo de vida de los datos.

Por lo tanto, para prevenir las vulnerabilidades de IoT e IIoT, las organizaciones deberían:

- Utilizar la autenticación más segura disponible en cada dispositivo
- Asegúrese de que los dispositivos IoTe IIoT nunca utilicen la contraseña predeterminada de fábrica
- Adoptar un enfoque de “confianza cero” (Zero-Trust) que sufrirá una transformación de un modelo de seguridad de red puramente técnico a un enfoque más integral y adaptable, facilitado por la integración de autenticación continua en tiempo real basada en IA y monitorización de actividad.

4.5. ESCASEZ DE TALENTO: COMPETENCIAS Y FORMACIÓN.

Como viene sucediendo en los últimos 10 años, en 2024 la demanda de profesionales cualificados en ciberseguridad superará ampliamente la oferta, lo que representa uno de los mayores obstáculos para lograr objetivos de resiliencia cibernética. La formación y el desarrollo de talento son esenciales para cerrar esta brecha.

Ya en el año 2017 en el Cuaderno de Estrategia 185 del IEEE-DSN titulado Ciberseguridad: la cooperación público –privada [10], en las conclusiones del capítulo octavo dedicado a la "Capacitación profesional y formación especializada en ciberseguridad" nos hacíamos eco de la más que palmaria escasez de profesionales en materia de Ciberseguridad y evidenciábamos que ya entonces no se trataba de un problema nuevo. Toda esta situación, en vez de solucionarse, ha empeorado con el tiempo porque las necesidades han seguido aumentando a un ritmo mayor.

En 2022, en su blog tecnológico, la compañía acens [12] señalaba lo siguiente:

"En 2024 España necesitará 83.000 profesionales más en ciberseguridad"

Y mostraba en una gráfica muy significativa sobre cuáles eran los principales efectos negativos de la escasez de talento de ciberseguridad en las empresas.

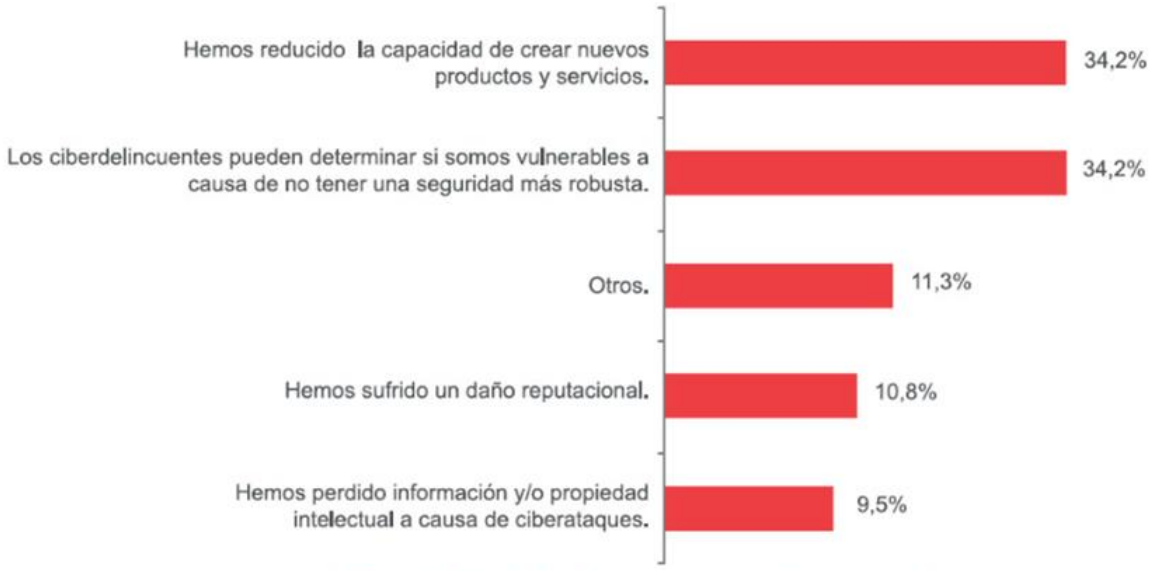


Figura 23. Principales efectos negativos de la escasez de talento de ciberseguridad en las empresas

Figura 16. Efectos de la escasez de talento[12].

[12] https://blog.acens.com/informes/en-2024-espana-necesitara-83-000-profesionales-mas-en-ciberseguridad/

4.6. REGULACIÓN.

En cuanto a aspectos normativos y legislativos, 2024 va a ser también un año notable para la ciberseguridad. La creciente preocupación por la protección del ciberespacio como espacio global común y por los riesgos derivados de uso indiscriminado de la IA se verán materializadas en diversas normativas de ciberseguridad que creen un marco común para aumentar la resiliencia de sistemas concretos y específicos. Normas como la Directiva NIS2, IT-SiG 2.0, NIST Cybersecurity Framework, CSA-iot, TEC in India, la Ley de Cibersolidaridad para el 2024 o la nueva regulación de la IA recientemente aprobada.

El "Cumplimiento" va a seguir jugando un rol crucial en guiar las iniciativas de ciberseguridad que las organizaciones afronten

Figura 17. Modelo de Ciberseguridad y Privacidad de AENOR

El bufete de abogados GARRIGUES, [11] en su informe sobre las novedades legales que se avecinan en este año (en algunos casos ya han aparecido en 2023 pero se tienen que implementar y aplicar durante 2024), en el apartado de "Economía Digital" destaca, entre otros menos relacionados con la ciberseguridad, los siguientes reglamentos y directivas:

- Data Act, Reglamento sobre normas armonizadas para un acceso justo a los datos y su utilización. Regula el acceso por parte de los usuarios y otros terceros a los datos generados por productos y servicios
- Reglamento de Inteligencia Artificial
- Reglamento e-IDAS 2, que regula la identidad digital se ha consensuado en el mes de noviembre y se publicará a comienzos de 2024.

- Reglamento sobre el Espacio Europeo de Datos Sanitarios, que regula la historia clínica digital europea y los usos primario y secundario de los datos de salud.
- Directiva NIS 2, cuya transposición al ordenamiento jurídico de cada estado termina en octubre de 2024.
- Reglamento DORA, obligatorio y directamente aplicable desde enero de 2025. Es la norma que establece obligaciones en materia de ciberseguridad a las empresas del sector financiero (banca y seguros) y a todas las empresas que les prestan servicios relacionados con IT.
- Reglamento de Mercados en Criptoactivos (MiCA)

4.7. CIBERSEGUROS.

El mercado de seguros es conocido por sus fluctuaciones. Un mercado duro indica que las primas están aumentando y la cobertura se está restringiendo, mientras que un mercado blando indica que las primas están disminuyendo y la cobertura se está ampliando. Tras una fuerte corrección en el mercado de seguros cibernéticos en los últimos años, caracterizada por el aumento de primas y la restricción de cobertura, el mercado está comenzando a suavizarse.

Con más participantes en el mercado y aseguradoras con ambiciosos objetivos de crecimiento cibernético, se espera que la competencia proporcione un alivio muy necesario a las crecientes primas que la industria ha estado viendo.

Ya en febrero de 2023 ENISA en su informe “Demand side of cyber insurance in the EU. Analysis of challenges and perspectives of OESs” [12] anticipaba lo que luego otras fuentes del sector asegurador han venido a confirmar.

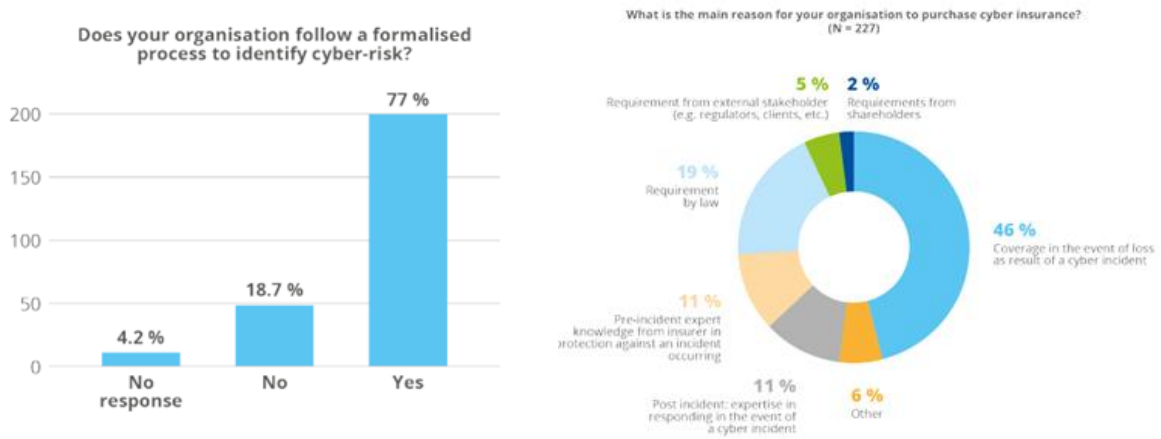


Figura 18. Ciberseguros [12]

Según el Blog de Innovación para el sector asegurador Future by inese:

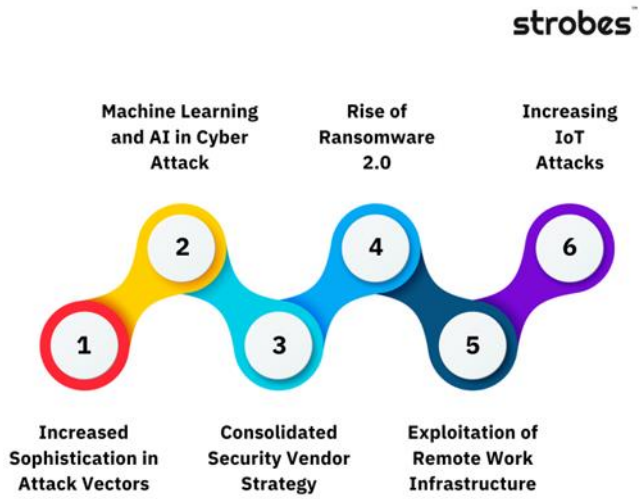
“El mercado mundial de los ciberseguros se prepara para otro año de crecimiento en 2024, pero los expertos advierten del aumento de los riesgos que acechan bajo la superficie. Tras registrar un crecimiento récord en 2023, con un aumento vertiginoso de los volúmenes de negocio de los ciberseguros en todo el mundo, el último Insurance Risk Monitor de OAC, prevé una trayectoria similar para 2024”.

Como viene sucediendo ya en los últimos años, la ciberseguridad ya no trata solamente de prevenir ataques; ahora es una cuestión de gestionar el riesgo. En 2024, los trabajos en torno a la ciberseguridad se centrarán en términos cuantitativos de riesgo, convirtiéndose en un tema crítico de discusión para juntas directivas y equipos de gestión.

4.8. RANSOMWARE.

El ransomware sigue siendo la amenaza número uno y plantea enormes desafíos para gobiernos, empresas y sociedad. Como decíamos más arriba, los ataques de Ransomware han sufrido un significativo incremento durante el año 2023 y se espera que la tendencia continue acentuando la necesidad de medidas proactivas tales como la monitorización en tiempo real, la securización de los dispositivos finales y la adopción de planes de respuesta inmediata ante ataques de este tipo.

En su top 6 de tendencias en Ciberseguridad para el 2024 la compañía de ciberseguridad de ámbito mundial Strobes [13]señala el ascenso de lo que denomina Ransomware 2.0:



Dice dicho artículo:

“La prevalencia del ransomware ha dado un giro más amenazador. Más allá del cifrado de datos, los actores de amenazas ahora están participando en la exfiltración de datos, creando un escenario de doble amenaza: bloqueo de datos y posible violación de datos.”

Un informe de Panda Security analiza el aumento de la **doble extorsión** en los ataques de ransomware. Tradicionalmente, el ransomware se centraba en la extorsión única cifrando los datos de una organización y exigiendo un rescate por una clave de descifrado. Sin embargo, los grupos de ransomware ahora han evolucionado para exfiltrar los datos de las víctimas a una ubicación externa antes del cifrado. Luego, amenazan con filtrar o publicar los datos si no reciben el rescate, creando así un escenario de doble extorsión. Este enfoque se aprovecha cada vez más, ya que resulta más rentable. Los datos robados no sólo son valiosos para sus legítimos propietarios sino también para otros ciberdelincuentes, lo que los convierte en un activo para la monetización y la venta en la dark net.

[13] https://strobes.co/blog/cybersecurity-trends-2024-lessons-from-2023-predictions-to-watch-out-for/ Última consulta en abril de 2024.

Un informe de Security Boulevard analiza cómo la naturaleza fundamental del ransomware ha pasado del cifrado a la exfiltración de datos, lo que significa que las prácticas tradicionales de copia de seguridad y recuperación de datos ya no serán una protección suficiente.

Conforme las organizaciones criminales que operan en el mundo del ransomware adoptan modelos de negocio "como servicio" en la dark net, los atacantes de todos los niveles pueden participar y los ciberdelincuentes pueden comprar toda la infraestructura de ransomware en dicha web oscura.

Por tanto, se espera para el año 2024 una tendencia al aumento del ransomware de doble extorsión e incluso de triple extorsión con tres capas para conseguir sus objetivos:

- Cifrado
- Amenaza de publicación de datos sensibles
- Presionar utilizando tácticas como DDoS y otras, por ejemplo, si la organización atacada dispone de copias de seguridad y se niega a pagar.

4.9. PHISHING DE NIVEL SUCESIVO.

Se espera que aumente la sofisticación de los ataques de ingeniería social, que manipulan a los usuarios para otorgarles acceso no autorizado a los sistemas. El uso de herramientas de IA generativa, ejemplificadas como ChatGPT, facilita la capacidad para más personas de emplear estrategias más sofisticadas y personalizadas en sus ataques.

Como resultado, se espera que la prevalencia de ataques “deepfake” aumente en el futuro con la finalidad de:

- Difundir información errónea
- Manipular elecciones
- Realizar ataques de ingeniería social
- Cometer robo de identidad
- Cometer fraude financiero
- Conseguir que la gente revele información protegida
- Convencer a la gente para que participe en el robo financiero
- Dar acceso a los delincuentes a las redes de la empresa

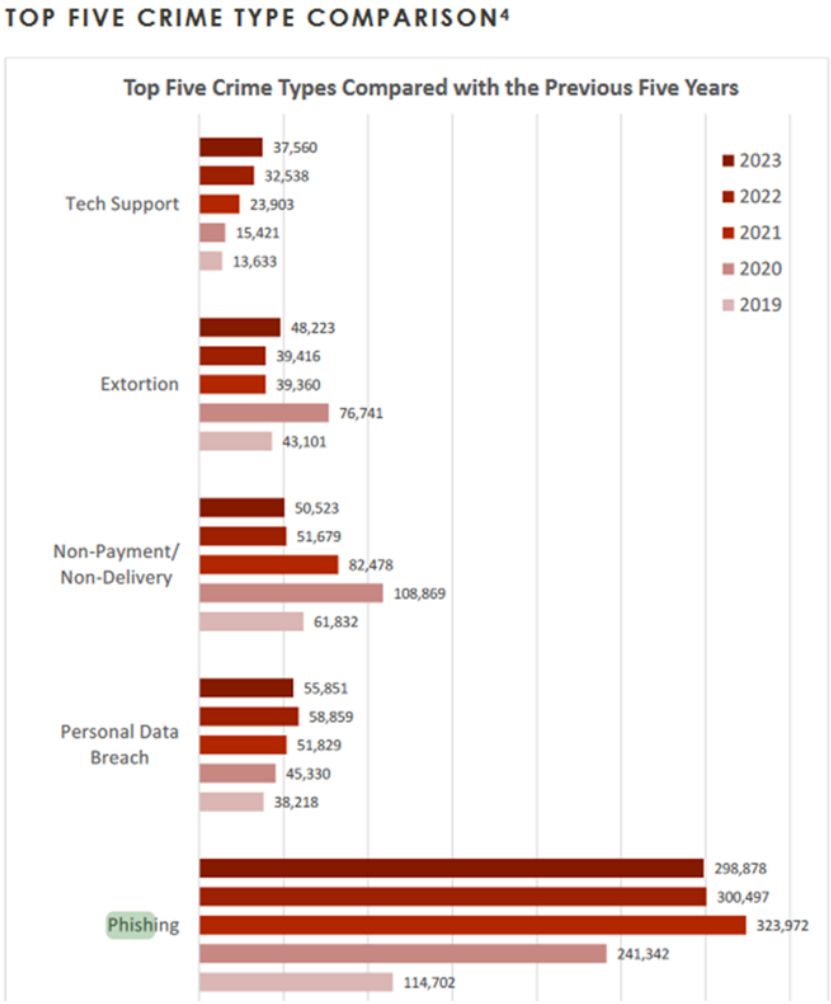


Figura 19. Comparativa del Top 5 por tipos de Cibercrimen [13]

El principal objetivo al abordar este problema se tendrá que centrar en:

- Fortalecimiento de los procedimientos de cumplimiento relacionados con la autorización de pagos
- Usar autenticación multifactor
- Promover la concientización en toda la organización y brindar educación integral.
- Uso de inteligencia artificial e implementación de principios de confianza cero.

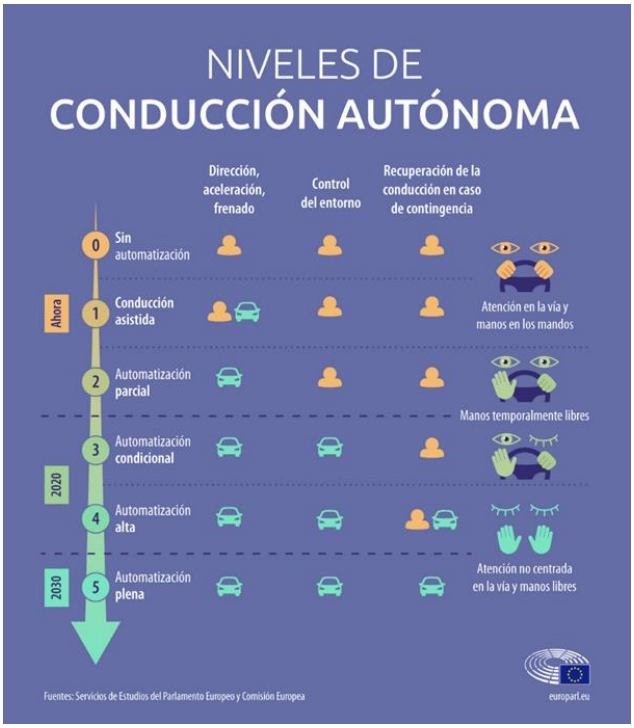
Como dato significativo y curioso hay que señalar que el FBI en su Internet Crime Report 2023 [13] destaca, si, el Phising como el tipo de cibercrimen más utilizado con diferencia, pero con una tendencia a la baja en los dos últimos; esto en contra de los datos de muchos otros proveedores de soluciones de ciberseguridad que, como mostramos en la Figura 10 han mostrado un crecimiento constante.

4.10. CIBERSEGURIDAD EN LOS VEHÍCULOS AUTÓNOMOS.

El avance de la digitalización, la conducción autónoma y una mayor conectividad plantean nuevos desafíos para la ciberseguridad de los automóviles.

Hoy en día, los vehículos modernos vienen equipados con software automatizado que crea una conectividad perfecta para los conductores en aspectos tales como el control de crucero, sincronización del motor, bloqueo de puertas, airbags y sistemas avanzados de asistencia al conductor. Estos vehículos utilizan tecnologías Bluetooth y WiFi para comunicarse, lo que también los abre a varias vulnerabilidades o amenazas de piratas informáticos. Se espera que en 2024 aumente el control del vehículo o el uso de diferentes sistemas con un mayor uso en vehículos automatizados. Los vehículos autónomos utilizan un mecanismo aún más complejo que requiere estrictas medidas de ciberseguridad.

La DGT estima que el próximo año podría salir adelante un Real Decreto que regule la circulación de vehículos con sistemas autónomos de nivel 4 y 5. Estará basado en documentos, normas y regulaciones más antiguos tanto de ENISA [15] como de las Naciones Unidas [16].



Expertos estadounidenses en ciberseguridad[14] han descubierto alarmantes brechas de seguridad en los sistemas informáticos empresariales y de backend de marcas de automóviles conocidas como BMW, Porsche y Mercedes. Estas brechas no sólo afectaron a los vehículos privados, sino también a los vehículos de emergencia como coches de policía y ambulancias. No sólo pudieron controlar las luces y los claxón, sino también abrir y cerrar las puertas del coche y arrancar los motores. Además, podían copiar datos del vehículo, restablecer configuraciones y, en algunos casos, incluso acceder a las redes internas de los fabricantes.

[14] https://samcurry.net/web-hackers-vs-the-auto-industry/

Última consulta en marzo de 2024

5. PROPUESTA DE ACCIONES RECOMENDADAS

La prevención de ciberataques es una tarea compleja pero que debe ser constante y que requiere un enfoque multidisciplinar. Se deben tomar medidas tanto a nivel personal como organizacional.

Por otro lado, siguen y seguirán siendo las mismas que se vienen recomendando a nivel nacional e internacional, pero con un enfoque que tenga en cuenta los nuevos escenarios tanto tecnológicos como sociales.

Como sabemos, la ciberseguridad es un proceso continuo, y no una solución única. Es fundamental mantenerse actualizado sobre las últimas amenazas y adoptar nuevas medidas de seguridad a medida que surgen.

- **Inversión en ciberseguridad**: Las organizaciones deberán invertir más en tecnologías y personal capacitado para proteger sus sistemas. Podría ser interesante incluso incluir a los seguros como ayuda para cubrir los costes de un incidente cibernético.

- Hay que adoptar una postura de **seguridad proactiva**: Anticipar las amenazas y tomar medidas preventivas.

- Se desarrollarán **políticas de seguridad** claras y concisas, asegurándose de que todos los empleados las conozcan y las cumplan

- **Cooperación público-privada**: La colaboración entre gobiernos y empresas es esencial para combatir el cibercrimen.

- **Formación y concienciación**: Los empleados son la primera línea de defensa. La formación de los usuarios es fundamental para prevenir ataques.

- **Resiliencia**: Las organizaciones deben desarrollar planes de recuperación para minimizar el impacto de los incidentes. Tienen que elaborar un plan detallado para responder a incidentes de seguridad y ensayarlo regularmente.

- **Medidas Tecnológicas**: Hay que mantener todos los sistemas operativos, aplicaciones y software de seguridad actualizados con los últimos parches de seguridad (actualización constante de software). Hay que utilizar contraseñas robustas y diferentes para cada cuenta. Además de utilizar la autenticación multifactor (MFA) y, a ser posible, un gestor de contraseñas. Es esencial realizar copias de seguridad de los datos de forma regular y guardarlas en un lugar seguro y utilizar software y herramientas de seguridad. El uso de “cortafuegos” y la segmentación de la red también se han demostrado utilísimos para limitar el impacto de un posible ataque.

En resumen, la tecnología es un factor clave en la ciberseguridad, tanto para los atacantes como para los defensores. Las organizaciones deben mantenerse al día con las últimas tendencias y adoptar un enfoque proactivo para proteger sus sistemas y datos.

6. CONCLUSIONES

En conclusión, las organizaciones son cada vez más “biónicas”, combinando tecnología y recursos humanos.

- Es fundamental adoptar un enfoque holístico, con una alta dirección que promueva una cultura corporativa fuerte, ágil y flexible, facilitando el aprendizaje entre pares, el debate abierto y la formación continua. El objetivo es crear organizaciones “robustas”, capaces de predecir y abordar los riesgos cibernéticos, **garantizando la ciberesiliencia**.

- Las nuevas tecnologías ayudarán a los equipos de seguridad, pero también pueden **hacer aumentar la superficie de ataque**.

- En 2024, el mundo rápidamente evolutivo de la **IA generativa** proporcionará a los atacantes nuevas formas de conducir campañas de phishing convincentes y operaciones de información a gran escala. Sin embargo, los defensores podrán usar las mismas tecnologías para robustecer la detección, respuesta y atribución de adversarios, y más ampliamente reducir el esfuerzo, abordar la sobrecarga de amenazas y cerrar la creciente brecha de habilidades.

7. ANEXOS

7.1. REFERENCIAS

01] ENISA. European Union Agency for Cybersecurity. Identifying Emerging Cyber Security Threats and Challenges for 2030. March 2023. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

[02] ENISA. European Union Agency for Cybersecurity. Enisa Threat Landscape 2023. October 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[03] CCN-CERT. Ciber_Amenazas y Tendencias. Noviembre de 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

[04] Ministerio del Interior. Balance Trimestral de Criminalidad. Segundo Trimestre 2023. https://www.interior.gob.es/opencms/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Balance-de-Criminalidad-Segundo-Trimestre-2023.pdf

[05] SentinelOne. “Watchtower. Intelligence-Driven Threat Hunting Endo of Year 2023”. 2024. https://www.sentinelone.com/resources/watchtower-end-of-year-report-2023/

[06] Sophos. The State of Ransomware 2023. https://www.sophos.com/en-us/content/state-of-ransomware

[07]CCN-CERT. CCN-CERT BP/30. “Aproximación a la Inteligencia Artificial y la Ciberseguridad”. Octubre de 2023. https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/7190-ccn-cert-bp-30-aproximacion-a-la-inteligencia-artificial-y-la-ciberseguridad/file.html

[08] Radware. “2024 Global Threat Analysis Report” Analysis of the most significant cybersecurity events and trends of 2023. 2024. https://www.radware.com/threat-analysis-report/

[09] IBM. Informe de IBM Security in the quantum computing era The risk is real, the need is now. Publicado en 2023 https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption

[10] IEEE-DSN. Instituto Español de Estudios Estratégicos-Departamento de Seguridad Nacional. Cuadernos de Estrategia 185. Ciberseguridad: la cooperación público-privada. Marzo de 2017. https://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2017/Cuaderno_185.html

[11] Garrigues. 2024: Las novedades legales más relevantes a las que deberán prestar atención las empresas en España. Diciembre de 2023. https://www.garrigues.com/sites/default/files/noticias/files/espana_2024_las_novedades_legales_mas_relevantes_a_las_que_deberan_prestar_atencion_las_empresas.pdf

[12] ENISA. Demand side of cyber insurance in the EU. Analysis of challenges and perspectives of OESs https://www.cde.ual.es/wp-content/uploads/2023/04/demand-side-of-cyber-insurance-in-the-eu-TP0422095ENN.pdf

[13] FBI. Federal Bureau of Investigation. Internet Crime Complaint Center. Internet Crime Report 2023 https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[14] SoSafe GmbH. "Tendencias en ciberdelincuencia 2024" Lo último en ciberamenazas y en buenas prácticas de seguridad. 2024. https://sosafe-awareness.com/es/recursos/informes/tendencias-ciberdelincuencia/

[15] ENISA. European Union Agency for Cybersecurity. Cyber Security and Resilience of smart cars Good practices and recommendations. December 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars

[16] ECEUN. Economics Commission for Europe - United Nations. Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system. March 2021. https://op.europa.eu/en/publication-detail/-/publication/a5081378-8079-11eb-9ac9-01aa75ed71a1

7.2. ACRÓNIMOS

AIA	Artificial Intelligence Act – Reglamento Europeo de Inteligencia Artificial.
CCN	Centro Criptológico Nacional
DORA	Digital Operational Resilience Act
ENS	Esquema Nacional de Seguridad
ENISA	European Union Agency for Cybersecurity – Agencia Europea de Ciberseguridad
IA/AI	Inteligencia Artificial / Artificial Intelligence
IEEE-DSN	Instituto Español de Estudios Estratégicos-Departamento de Seguridad Nacional.
IoT/IIoT	Internet de las Cosas / Industrial
INCIBE	Instituto Nacional de Ciberseguridad
NIS Directive	Directiva de Seguridad de Redes y Sistemas de Información (EU)
NIST	Instituto Nacional de Estándares y Tecnología (USA)
RGPD/GDPR	Reglamento General de Protección de Datos