# CIBERSEGURIDAD

## INFORME DE SITUACIÓN 2024

DISRUPTIVE Plataforma Tecnológica Española de Tecnologías Disruptivas

Ayuda PTR2022-001305 financiada por:
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
AGENCIA ESTATAL DE INVESTIGACIÓN

Secretaria técnica a cargo de:
APTE Asociación de Parques Científicos y Tecnológicos de España

# ÍNDICE

# INTRODUCCIÓN

En 2024, la ciberseguridad en España ha llegado a un punto crítico. La creciente sofisticación y frecuencia de los ciberataques ha obligado tanto a empresas como a organismos públicos a replantearse sus estrategias de protección ante un escenario digital cada vez más hostil. El incremennto del 190 % en ciberataques dirigidos al sector público, detectado en los primeros meses del año, refleja no solo la exposición creciente de las instituciones gubernamentales, sino también la falta de medidas preventivas adecuadas en sectores clave para la estabilidad y el bienestar social. Estos ataques han afectado gravemente a la infraestructura pública, comprometiendo datos sensibles y afectando la operativa diaria de servicios esenciales.

A nivel corporativo, el panorama no es más alentador. El 62 % de los ciberataques en España se concentra en sectores críticos como el tecnológico, financiero y público, lo que pone de manifiesto la vulnerabilidad de las infraestructuras de información y redes en estos ámbitos. Las empresas tecnológicas y financieras, que deberían estar a la vanguardia en términos de ciberseguridad, han sido especialmente afectadas por técnicas avanzadas como el ransomware, el phishing dirigido (spear-phishing) y las intrusiones a través de vulnerabilidades no parcheadas. Estos ataques no solo tienen un impacto económico, sino que también erosionan la confianza del público en la seguridad de los sistemas financieros y tecnológicos del país.

El hecho de que solo el 2 % de las organizaciones españolas cuenten con una infraestructura adecuada para mitigar ciberataques de gran envergadura evidencia una alarmante falta de preparación. Esta brecha en la ciberresiliencia se ve exacerbada por la adopción de nuevas tecnologías, como la inteligencia artificial y la red 5G, que si bien ofrecen mejoras en eficiencia y conectividad, también abren nuevos vectores de ataque. En particular, la expansión de la red 5G ha suscitado preocupaciones sobre la capacidad de las organizaciones para gestionar de manera efectiva los riesgos asociados con el aumento de la superficie de ataque y la interconexión de dispositivos del Internet de las Cosas (IoT). Estos dispositivos, en muchas ocasiones mal protegidos, se han convertido en un objetivo atractivo para los ciberdelincuentes que buscan comprometer redes y sistemas críticos.

En el plano del usuario final, los ciberataques también han tomado una dimensión alarmante. Durante el último año, el 60 % de los ciudadanos españoles admitió carecer de conocimientos suficientes para evitar ser víctimas de estafas online. Esta falta de concienciación y preparación ha generado un terreno fértil para la proliferación de fraudes y campañas de phishing, que han aumentado en complejidad, apuntando a objetivos tanto individuales como corporativos. Además, casi la mitad de los españoles ha sido objetivo de algún tipo de intento de fraude o estafa online en el último año, lo que resalta la vulnerabilidad de la población general en el ámbito digital.

En paralelo, la ciberseguridad se ha consolidado como un elemento estratégico en el plano geopolítico y empresarial. Las organizaciones que han adoptado soluciones avanzadas de seguridad están reconociendo que ya no es suficiente con desplegar firewalls y antivirus; la clave está en la ciberinteligencia y en la capacidad de anticiparse a los ataques mediante análisis predictivos y enfoques proactivos. La inteligencia artificial está comenzando a jugar un papel crucial en esta área, ayudando a las organizaciones a identificar patrones anómalos en sus redes y a reaccionar ante posibles incidentes antes de que escalen en ataques a gran escala.

Este informe de 2024 examina de manera exhaustiva los retos a los que se enfrenta España en el ámbito de la ciberseguridad, evaluando no solo las amenazas emergentes, sino también las oportunidades para fortalecer la ciberdefensa del país. La colaboración entre los sectores público y privado, la implementación de tecnologías emergentes, y una mayor concienciación y formación del usuario final, serán clave para afrontar los desafíos en un entorno digital cada vez más amenazante.

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

# TENDENCIAS

En 2024, el panorama de la ciberseguridad en España ha experimentado un notable cambio, impulsado por la intensificación de amenazas y la rápida evolución tecnológica. A continuación, se presentan las principales tendencias que han definido el estado de la ciberseguridad en el país:

- **Proliferación del Phishing y Ransomware Avanzado:**

El phishing continúa siendo uno de los vectores más prevalentes de ciberataques en España, con un aumento considerable en su sofisticación. Un informe reciente destaca que más del 50 % de los españoles ha sido objetivo de intentos de fraude online en el último año. Las tácticas de phishing han evolucionado, utilizando técnicas de ingeniería social más complejas que confunden a los usuarios, facilitando la infiltración en redes corporativas y personales.

Por su parte, el ransomware sigue ocupando un lugar destacado entre las ciberamenazas, impactando a organizaciones de todos los tamaños. Los ataques dirigidos a sectores clave como el tecnológico, financiero y público han incrementado, representando el 62 % de los incidentes reportados en 2024. Las empresas se enfrentan a demandas de rescates cada vez más elevadas y a daños reputacionales significativos.

- **La Inteligencia Artificial (IA) como arma de doble filo:**

La adopción de la IA se ha acelerado en el ámbito de la ciberseguridad, proporcionando herramientas de análisis predictivo y detección automatizada de amenazas. Sin embargo, al mismo tiempo, los ciberdelincuentes están aprovechando la IA para desarrollar ataques más precisos y difíciles de detectar. En 2024, solo el 2 % de las organizaciones españolas ha implementado estrategias adecuadas para defenderse contra ciberataques habilitados por IA, lo que demuestra la necesidad urgente de adaptar las defensas frente a estas amenazas emergentes.

- **Escasez crítica de talento en ciberseguridad:**

La falta de profesionales cualificados en ciberseguridad sigue siendo uno de los desafíos más apremiantes. Aunque la demanda de expertos en ciberdefensa se ha disparado, las organizaciones continúan luchando por cubrir vacantes. España necesita alrededor de 80.000 especialistas en ciberseguridad para 2024, pero el ritmo de formación no está a la altura de esta demanda. Esta brecha no solo afecta a las grandes empresas, sino también a las pymes, que tienen dificultades adicionales para atraer talento especializado.

- **Aumento de la Cibercriminalidad en el Sector Público:**

El sector público en España ha sido uno de los principales objetivos de los ciberdelincuentes en 2024, con un incremento del 190 % en ciberataques, lo que ha puesto de manifiesto las vulnerabilidades en la infraestructura crítica del país. Las instituciones gubernamentales, que manejan información sensible, han sido blanco de ataques que buscan desestabilizar sus operaciones y acceder a datos personales y financieros. Este fenómeno ha subrayado la necesidad de reforzar las estrategias de ciberseguridad en el ámbito público y de fomentar la colaboración internacional para mitigar riesgos globales.

- **Infraestructura 5G y nuevos riesgos**

La expansión de la red 5G en España ha abierto nuevas oportunidades de conectividad y eficiencia, pero también ha incrementado los riesgos de seguridad. Los ciberataques contra las redes 5G, especialmente en sectores como la salud y el transporte, representan una amenaza significativa. La interconexión de dispositivos IoT (Internet de las Cosas), que proliferan gracias a la infraestructura 5G, ha aumentado la superficie de ataque, obligando a las empresas a redoblar sus esfuerzos de seguridad.

- **Ciberseguridad como diferenciador competitivo**

La ciberseguridad se ha consolidado en 2024 como un factor clave en la competitividad empresarial. Más allá de su función tradicional de protección de activos, las organizaciones están comenzando a posicionarla como una ventaja competitiva frente a sus clientes y socios. Las empresas más resilientes en términos de ciberseguridad no solo protegen su reputación, sino que también mejoran la confianza del cliente, lo que se traduce en un valor agregado en sectores como el financiero y el tecnológico.

- **Las pymes, en la mira de los ciberdelincuentes:**

Las pequeñas y medianas empresas (pymes) siguen siendo extremadamente vulnerables a los ciberataques. En 2024, muchas de estas organizaciones continúan operando sin

Startups tecnológicas españolas, junto con grandes empresas de software, están estrategias de ciberseguridad robustas, lo que las convierte en un objetivo atractivo para los atacantes. Dado que una proporción significativa de las pymes españolas cierra sus puertas tras sufrir un ciberataque, la necesidad de soluciones accesibles y eficientes en ciberseguridad es más urgente que nunca.

- **Enfoque en la protección de infraestructuras críticas:**

La protección de infraestructuras críticas sigue siendo una prioridad estratégica para España. En 2024, las directrices europeas y los esfuerzos nacionales han continuado centrados en mejorar la resiliencia de sectores clave como la energía, el transporte y la salud. Los ataques a estas infraestructuras pueden tener consecuencias devastadoras, tanto a nivel económico como social, lo que ha llevado a un endurecimiento del marco regulatorio y a una mayor inversión en tecnologías de seguridad.

# ESTRATEGIA EN ESPAÑA

En 2024, la estrategia de ciberseguridad en España se ha intensificado, marcada por el creciente número y la complejidad de las amenazas cibernéticas. La adaptación de las políticas públicas y las medidas empresariales ha sido clave para enfrentar los desafíos emergentes. A continuación, se detallan los pilares fundamentales de la estrategia de ciberseguridad en el país durante este año:

- **Fortalecimiento del Marco Normativo**

El refuerzo del marco regulatorio ha sido un componente central en la estrategia de ciberseguridad de España en 2024. La aplicación y cumplimiento de la Ley de Ciberseguridad 5G ha ganado protagonismo, debido a las preocupaciones sobre la vulnerabilidad de la infraestructura crítica del país. Esta ley se centra en la protección de las redes 5G, que están impulsando la transformación digital y la conectividad en España. El aumento de los dispositivos IoT conectados a través de 5G ha expandido la superficie de ataque, por lo que las empresas y organismos gubernamentales han tenido que ajustar sus políticas de seguridad para minimizar los riesgos asociados.

Además, las directivas europeas como la NIS 2 han obligado a sectores clave, especialmente los de tecnología, salud, transporte y finanzas, a implementar controles de ciberseguridad más estrictos. La NIS 2 no solo amplía el ámbito de las empresas obligadas a cumplir con requisitos de ciberseguridad, sino que también establece sanciones más severas en caso de incumplimiento.

- **Colaboración Internacional y Público-Privada**

En 2024, la cooperación internacional y la colaboración entre el sector público y privado han sido pilares en la estrategia de ciberseguridad de España. La cooperación entre el Centro Criptológico Nacional (CCN-CERT) y organizaciones internacionales ha mejorado significativamente la capacidad de respuesta ante incidentes transfronterizos. En particular, se ha fortalecido la colaboración con Europol y otras agencias europeas, lo que ha permitido una reacción más rápida y coordinada frente a ciberataques masivos dirigidos a infraestructuras críticas

Por otro lado, la alianza entre el INCIBE (Instituto Nacional de Ciberseguridad) y empresas privadas ha jugado un papel crucial en la protección de sectores clave. Las empresas del sector financiero, tecnológico y sanitario han intensificado sus esfuerzos de colaboración para intercambiar información sobre amenazas, vulnerabilidades y soluciones de ciberseguridad. Un ejemplo destacado es el aumento en la colaboración público-privada en el sector sanitario, donde la protección de datos sensibles de pacientes se ha convertido en una prioridad estratégica.

- **Capacitación y Desarrollo de Talento**

La falta de profesionales especializados en ciberseguridad sigue siendo un desafío importante en España, donde se estima que para 2024 harán falta cerca de 80.000 especialistas en este campo. La respuesta a esta necesidad ha incluido una serie de iniciativas educativas y de formación diseñadas para cerrar la brecha de talento. El INCIBE ha continuado ofreciendo programas formativos y colaborando con universidades y centros de investigación para fomentar la formación de nuevos profesionales.

Asimismo, el gobierno español ha incentivado la creación de ciberacademias y ha promovido el desarrollo de bootcamps en ciberseguridad para proporcionar formación acelerada a aquellos interesados en entrar en el campo. La inclusión de módulos de ciberseguridad en los currículos de carreras técnicas y de ingeniería ha sido clave para garantizar que las futuras generaciones estén preparadas para hacer frente a las amenazas cibernéticas.

- **Adopción de Tecnologías Avanzadas**

La estrategia en 2024 también ha puesto un fuerte énfasis en la adopción de tecnologías avanzadas para mejorar las capacidades de ciberdefensa. La inteligencia artificial (IA) ha ganado terreno como una herramienta clave para identificar patrones anómalos y detectar amenazas en tiempo real. En particular, las empresas del sector financiero y tecnológico han comenzado a implementar IA para analizar grandes volúmenes de datos y predecir posibles ciberataques antes de que ocurran.

Sin embargo, los ciberdelincuentes también han comenzado a utilizar IA para desarrollar ataques más sofisticados. Esto ha obligado a las organizaciones españolas a actualizar constantemente sus tecnologías y estrategias defensivas. En este sentido, la inversión en I+D ha sido fundamental para la creación de soluciones de seguridad cibernética más robustas.

- **Protección de Infraestructuras Críticas**

Uno de los ejes centrales de la estrategia española ha sido la protección de infraestructuras críticas, que incluyen sectores como la energía, la salud, el transporte y las telecomunicaciones. En 2024, el número de ataques dirigidos a estas infraestructuras ha crecido considerablemente, con un aumento del 190 % en incidentes reportados en el sector público. Esto ha puesto en evidencia la necesidad de una mayor inversión en medidas preventivas y de respuesta rápida.

El gobierno ha impulsado la creación de SOC (Centros de Operaciones de Seguridad) regionales y sectoriales, que colaboran estrechamente con el CCN-CERT para monitorizar y responder a incidentes de ciberseguridad en tiempo real. Además, se ha incrementado el uso de tecnologías de cifrado y autenticación multifactor para proteger la infraestructura digital del país.

- **Incremento en la Concienciación y Ciberhigiene**

En 2024, la concienciación sobre ciberseguridad entre empresas y ciudadanos ha sido un área prioritaria en la estrategia española. Las campañas públicas y los programas de formación dirigidos tanto a grandes empresas como a pymes han sido claves para fomentar la adopción de buenas prácticas de ciberhigiene. Según informes recientes, más del 60 % de los españoles aún carece de conocimientos adecuados para evitar estafas online, lo que subraya la necesidad de una mayor educación digital.

Programas como Activa Ciberseguridad, impulsados por el INCIBE, han sido fundamentales para proporcionar asesoramiento y formación personalizada a las pymes, uno de los sectores más vulnerables a los ciberataques. Estos programas ofrecen diagnósticos de ciberseguridad gratuitos y recomendaciones específicas para mejorar las defensas de las empresas.

- **Respuesta y Recuperación ante Incidentes**

Finalmente, el fortalecimiento de la capacidad de respuesta y recuperación ante incidentes ha sido otro aspecto crucial de la estrategia en 2024. La creación de la Red Nacional de SOC, que integra a los principales centros de operaciones de seguridad del país, ha permitido una mejor coordinación en la detección y respuesta ante ciberataques a nivel nacional. El trabajo del CCN-CERT ha sido fundamental en este sentido, ayudando a mitigar los efectos de los ataques más graves y facilitando la recuperación de los sistemas afectados.

# RETOS Y OPORTUNIDADES

En 2024, España se enfrenta a un panorama cibernético complejo y desafiante, donde la expansión de la digitalización y la creciente sofisticación de los ciberataques exigen un enfoque robusto y dinámico en ciberseguridad. Este contexto presenta numerosos retos que el país debe superar, pero también brinda oportunidades clave para fortalecer su capacidad defensiva y de recuperación. A continuación, se detallan los principales retos y oportunidades que definen la ciberseguridad en España durante este año.

**Retos:**


## Aumento de la superficie de ataque con la expansión del 5G e IoT

LEl despliegue de la red 5G y la rápida adopción de dispositivos IoT han ampliado significativamente la superficie de ataque. Estos avances tecnológicos, aunque beneficiosos para la conectividad y eficiencia, han introducido vulnerabilidades críticas. Las infraestructuras más interconectadas, especialmente en sectores como salud, transporte y energía, son ahora más susceptibles a ciberataques dirigidos. Los atacantes tienen más puntos de acceso para comprometer redes, lo que complica la labor de asegurar la totalidad de los entornos digitales.

## Brecha de talento en Ciberseguridad

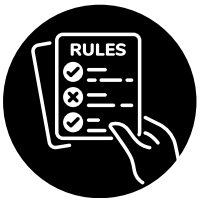
Uno de los desafíos más persistentes sigue siendo la escasez de profesionales especializados. En 2024, España se enfrenta a una brecha de talento que podría superar los 80.000 expertos necesarios para cubrir la creciente demanda en el sector. La falta de personal capacitado limita la capacidad de las organizaciones para detectar y responder a amenazas de manera efectiva, y supone un riesgo mayor para las empresas, especialmente en sectores críticos que requieren protección inmediata y constante. Las pymes, en particular, sufren este déficit con mayor intensidad.

## Vulnerabilidad de las PYMEs ante ciberataques

Las pequeñas y medianas empresas (PYMEs) siguen siendo un objetivo atractivo para los ciberdelincuentes. La mayoría de las PYMEs en España carecen de recursos adecuados para implementar sistemas de ciberseguridad robustos, lo que las convierte en blancos fáciles. Muchas de ellas aún operan sin estrategias claras de protección, lo que ha resultado en un aumento de los incidentes en este sector. Dado que un porcentaje significativo de las PYMEs españolas desaparece tras sufrir un ciberataque, abordar esta vulnerabilidad es crucial.

## Incremento de ataques dirigidos a infraestructuras críticas

El sector público y las infraestructuras críticas han sido blanco de un creciente número de ciberataques, con un aumento del 190 % en incidentes reportados en el primer trimestre de 2024. La protección de infraestructuras clave como la energía, el transporte y la salud sigue siendo un reto de gran envergadura. Las interrupciones en estos sectores pueden tener un impacto devastador en la seguridad nacional y en la calidad de vida de los ciudadanos, lo que subraya la necesidad de una mayor inversión en medidas preventivas y de recuperación rápida.




## Gestión del cumplimiento normativo

El cumplimiento de regulaciones como la Ley de Ciberseguridad 5G y la Directiva NIS 2 es otro desafío importante. Estas normativas imponen requisitos estrictos para mejorar las defensas cibernéticas, pero también exigen que las empresas actualicen sus infraestructuras tecnológicas y adopten nuevos enfoques de gestión de riesgos. Esto puede ser una carga para muchas organizaciones, especialmente las pymes, que a menudo carecen de los recursos necesarios para cumplir con todas las exigencias reglamentarias.

Oportunidades:

## Adopción de Inteligencia Artificial para la Ciberseguridad

La inteligencia artificial (IA) está emergiendo como una herramienta poderosa en la defensa cibernética. En 2024, cada vez más organizaciones españolas han comenzado a adoptar IA para la detección temprana de amenazas, análisis predictivo y respuesta automatizada. Esta tecnología tiene el potencial de reducir significativamente el tiempo de reacción ante ataques, mejorando la capacidad de las empresas para mitigar riesgos antes de que se materialicen en incidentes mayores. Además, la IA también puede ayudar a las empresas a optimizar sus recursos, priorizando las amenazas más críticas.

## Fortalecimiento de la colaboración público-privada

En 2024, la colaboración entre el sector público y privado ha sido un componente crucial para mejorar la ciberseguridad en España. La cooperación entre organismos como el INCIBE y empresas tecnológicas, financieras y sanitarias ha permitido compartir información sobre amenazas y desarrollar soluciones conjuntas. Este enfoque colaborativo ha demostrado ser efectivo en la detección y respuesta a ciberataques, especialmente en sectores críticos. A medida que la sofisticación de los ataques sigue creciendo, esta colaboración será clave para fortalecer las defensas nacionales.

## Formación y desarrollo de talento en Ciberseguridad

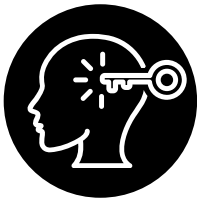
La creciente demanda de profesionales en ciberseguridad ofrece una oportunidad significativa para la formación y el desarrollo de talento. En 2024, el INCIBE ha intensificado sus esfuerzos para capacitar a nuevos expertos a través de programas de formación y certificación, así como colaboraciones con universidades y centros de investigación. Esto no solo ayuda a cerrar la brecha de talento, sino que también fomenta el desarrollo de profesionales altamente cualificados que puedan liderar la próxima generación de soluciones en ciberseguridad.

## Inversión en infraestructuras de resiliencia cibernética

La creación de la Red Nacional de SOC (Centros de Operaciones de Seguridad), que coordina la detección y respuesta a incidentes a nivel nacional, es una oportunidad clave para mejorar la resiliencia cibernética en España. Esta infraestructura permite una vigilancia continua de los sistemas críticos y facilita una respuesta rápida y coordinada ante ataques. Además, la inversión en nuevas tecnologías como cifrado avanzado y autenticación multifactor refuerza aún más la capacidad del país para protegerse contra ciberataques a gran escala.

## Crecimiento del mercado de soluciones de Ciberseguridad

El mercado de soluciones de ciberseguridad en España está en auge, impulsado por la demanda creciente de empresas que buscan protegerse contra amenazas cada vez más complejas. Las innovaciones en áreas como la protección contra ransomware, tecnologías de defensa perimetral y plataformas de gestión de incidentes ofrecen a las empresas nuevas formas de proteger sus activos y garantizar la continuidad de sus operaciones. Las empresas emergentes en el sector tienen una oportunidad única para crecer y posicionarse como líderes en el mercado global de ciberseguridad.



## Concienciación pública y Ciberhigiene

La educación y concienciación sobre ciberseguridad sigue siendo una oportunidad crítica. Aunque el 60 % de los españoles aún carece de conocimientos suficientes para evitar estafas online, las campañas de concienciación, como las lideradas por el INCIBE, están comenzando a tener un impacto positivo. El aumento de la ciberhigiene entre los usuarios finales es clave para reducir la exposición a ataques basados en ingeniería social, como el phishing, y para crear una cultura de seguridad más sólida en toda la sociedad.

En 2024, los retos y las oportunidades en torno a la ciberseguridad en España son complejos, pero ofrecen un camino claro para que el país consolide su liderazgo en este campo.

# ECOSISTEMA

En 2024, España ha fortalecido su ecosistema de ciberseguridad, logrando un equilibrio entre innovación, colaboración público-privada y la evolución tecnológica. El país sigue posicionándose como un referente europeo en seguridad digital, apoyado en un tejido empresarial robusto, un marco institucional dinámico y un enfoque integrador que une a grandes empresas consolidadas con startups emergentes. Este entorno permite desarrollar soluciones avanzadas en ciberseguridad para hacer frente a las crecientes amenazas globales y nacionales, en un contexto marcado por la transformación digital acelerada.

**Principales Actores Empresariales**

**1. Telefónica Tech Cybersecurity & Cloud**

Telefónica sigue consolidándose como uno de los principales actores en ciberseguridad, con una cartera de servicios que cubre desde la seguridad en la nube hasta la protección de redes empresariales críticas. En 2024, Telefónica ha destacado por integrar soluciones basadas en inteligencia artificial (IA) y machine learning en sus sistemas de ciberdefensa, mejorando la detección predictiva de amenazas en tiempo real. La compañía sigue ofreciendo protección a sectores estratégicos como el financiero y las telecomunicaciones, además de reforzar su presencia en el ámbito de la seguridad IoT, clave con la expansión del 5G.

**2. Indra**

Indra, con su vasta experiencia en ciberdefensa y seguridad, ha sido clave en la protección de infraestructuras críticas, un sector que ha visto un alarmante aumento de ciberataques en 2024. Sus soluciones avanzadas para sectores como energía y transporte han sido esenciales para mitigar riesgos y asegurar la continuidad operativa. Indra también ha jugado un papel activo en la colaboración con organismos gubernamentales para mejorar la protección del sector público, que ha sido uno de los más afectados por los ciberataques dirigidos este año.

**3. GMV**

GMV ha ampliado su liderazgo en seguridad espacial y defensa, enfocándose en soluciones para la protección de sistemas industriales y la infraestructura crítica en España. En 2024, GMV ha implementado tecnologías innovadoras para proteger los entornos industriales conectados, un sector que ha sufrido una ola de ataques dirigidos a sistemas de control operacional (OT). Su trabajo en ciberseguridad industrial ha sido crucial para salvaguardar fábricas inteligentes, cuya interconexión a través de IoT y 5G ha aumentado la exposición a vulnerabilidades.

**4. S21sec**

Otra empresa que ha tomado relevancia en 2024 es S21sec, una de las firmas líderes en servicios de ciberseguridad gestionada. Con una fuerte presencia en el mercado español, S21sec ha jugado un papel fundamental en la monitorización y respuesta a incidentes, trabajando en estrecha colaboración con el INCIBE y otras instituciones para proteger infraestructuras críticas y empresas del sector financiero. La empresa también ha desarrollado programas avanzados de formación para capacitar a las empresas en la detección de amenazas y en la gestión de incidentes de seguridad.

**5. Panda Security (WatchGuard Technologies)**

Panda Security, parte de WatchGuard Technologies, ha continuado destacando en el campo de la protección de endpoints y la seguridad en la nube. En 2024, la compañía ha lanzado soluciones de ciberseguridad diseñadas específicamente para pequeñas y medianas empresas (PYMEs), un sector altamente vulnerable en España. Con su enfoque en la automatización de respuestas a incidentes y la protección proactiva, Panda Security ha reforzado la defensa de miles de organizaciones, contribuyendo a elevar el nivel de protección general en el mercado español

**Startups Innovadoras y su Impacto en 2024**

- **CounterCraft**

CounterCraft ha seguido creciendo en 2024 como una de las startups más prometedoras en el ámbito de la ciberdefensa activa. Su tecnología de engaño y su enfoque en la inteligencia artificial han sido clave para identificar y neutralizar amenazas avanzadas en sectores como el financiero y el gubernamental. La empresa ha expandido su presencia internacional, pero sigue jugando un papel crucial dentro del ecosistema español, proporcionando soluciones innovadoras para empresas e instituciones gubernamentales.

- **Blueliv**

Blueliv se mantiene a la vanguardia de la inteligencia de amenazas en España y Europa. En 2024, ha mejorado sus capacidades de ciberinteligencia, utilizando grandes volúmenes de datos para prevenir ciberataques antes de que se materialicen. Su plataforma ha demostrado ser crucial para sectores como las telecomunicaciones y la banca, donde la rapidez en la identificación de amenazas es esencial para mitigar el impacto de ataques avanzados como el ransomware o el spear-phishing.

- **Devo**

Otra startup que ha captado atención en 2024 es Devo, una empresa especializada en el análisis de datos a gran escala y la gestión de incidentes de ciberseguridad. Devo ofrece a las empresas herramientas para analizar enormes cantidades de información en tiempo real, permitiendo la detección temprana de ciberataques. Su tecnología ha sido particularmente útil para organizaciones del sector tecnológico y financiero, donde los ataques sofisticados son una amenaza constante.

**Colaboración Público-Privada e Institucional**

El ecosistema español de ciberseguridad sigue beneficiándose de una estrecha colaboración entre el sector público y privado. Instituciones como el INCIBE y el CCN-CERT han reforzado su papel en la coordinación de las actividades de ciberseguridad a nivel nacional. En 2024, el INCIBE ha intensificado sus esfuerzos para apoyar a pequeñas y medianas empresas a través de programas como Activa Ciberseguridad, ofreciendo diagnósticos y recomendaciones personalizadas que han ayudado a mejorar las defensas digitales en un sector altamente vulnerable.

El CCN-CERT, por su parte, ha continuado liderando la protección de infraestructuras críticas mediante la Red Nacional de SOC, que ha jugado un papel clave en la monitorización y respuesta a ciberataques dirigidos al sector público, donde se ha observado un aumento significativo de incidentes. Esta colaboración entre el gobierno y las empresas privadas ha sido esencial para mitigar los riesgos y mejorar la resiliencia del país frente a las amenazas cibernéticas.

**Innovación y Apoyo al I+D en Ciberseguridad**

La inversión en innovación ha sido una piedra angular del ecosistema de ciberseguridad en España en 2024. A través de los fondos de Next Generation EU, el gobierno español ha fomentado el desarrollo de proyectos de investigación y desarrollo en ciberseguridad, centrados en tecnologías disruptivas como la inteligencia artificial, el análisis de big data y la protección de infraestructuras críticas. Este apoyo a la I+D ha generado un ecosistema donde tanto grandes empresas como startups pueden prosperar, desarrollando soluciones avanzadas que no solo protegen a las organizaciones, sino que también permiten anticiparse a las amenazas futuras.

# PROSPECTIVA

En el panorama actual, los riesgos cibernéticos representan una amenaza seria para la estabilidad global de las infraestructuras, afectando no solo a las cadenas de suministro y la estabilidad financiera sino también a la democracia misma, tal como lo indica el Foro Económico Mundial. Por su parte, el Fondo Monetario Internacional ha advertido que los ciberataques son una amenaza crítica para la estabilidad financiera mundial. En eventos de alta exposición, como los Juegos Olímpicos de 2024 en Francia, las autoridades lograron mitigar 140 ciberataques dirigidos contra el transporte, las telecomunicaciones, las infraestructuras deportivas y el propio Gobierno francés, evidenciando la capacidad de respuesta pero también la exposición a amenazas en infraestructuras críticas. Con esta situación en mente, las organizaciones deben plantearse un enfoque de ciberseguridad que contemple la adaptación y la prevención.

En este contexto, la digitalización de sectores como la sanidad, la industria 4.0 y las redes eléctricas ha resaltado la importancia de la seguridad en la infraestructura tecnológica crítica de España. Las actividades en el desarrollo de vehículos conectados demuestran cómo se pueden controlar o alterar elementos esenciales de los sistemas digitales, aumentando el riesgo de vulnerabilidades. La implementación de regulaciones en Europa para asegurar la infraestructura en vehículos, dispositivos médicos y otras tecnologías conectadas sigue avanzando, con el objetivo de que fabricantes y desarrolladores prioricen la seguridad desde el diseño, evitando la dependencia de soluciones de seguridad a posteriori que resultan menos efectivas.

La demanda de profesionales en ciberseguridad está en aumento. El Foro Económico Mundial ha estimado la necesidad de 4 millones de expertos adicionales en ciberseguridad a nivel global, mientras que en España se requieren 40,000 profesionales más en el sector. Sin embargo, el déficit actual en talento especializado ha derivado en una alta cotización de estos perfiles, incrementando los costes para las organizaciones y resaltando la necesidad de estrategias complementarias como la automatización de la ciberseguridad. En este ámbito, la inteligencia artificial (IA) juega un papel fundamental, aunque no está exenta de riesgos. La IA misma puede ser blanco de ataques, entre los cuales destacan los Poisoning Attacks, que buscan manipular tanto los modelos como los

datos de entrenamiento mediante el envenenamiento de datos. Estos ataques permiten degradar el rendimiento del sistema, modificar los resultados y dañar la reputación de las organizaciones. Dentro de estos ataques, uno de los métodos de mayor relevancia es el ataque Rocky, que manipula los datos generativos de los modelos de IA, exponiendo vulnerabilidades y comprometiendo información sensible.

El acceso a datos y el uso de modelos generativos se han convertido en vectores de riesgo adicionales. Actualmente, se pueden extraer datos personales de directivos y otras personas de interés mediante el análisis de grandes modelos de lenguaje público. La capacidad de introducir data poisoning en estos modelos plantea nuevos desafíos de seguridad, ya que los datos alterados afectan la integridad de los modelos y su utilidad en diversas aplicaciones, desde la administración pública hasta el sector empresarial.

La privacidad de los datos es otra área clave que enfrenta desafíos significativos. Europa ha adoptado tecnologías de base como blockchain para descentralizar la gobernanza de datos, promoviendo un uso controlado de la información. Sin embargo, a pesar de los esfuerzos, estos sistemas no garantizan la seguridad total en el intercambio de datos y dejan ciertas áreas expuestas a riesgos de privacidad. Para hacer frente a estos desafíos, la inteligencia artificial federada o Federated Learning ha sido explorada como una solución para entrenar modelos sin necesidad de transferir los datos de los usuarios a una ubicación centralizada. No obstante, esta tecnología también presenta vulnerabilidades. Los ataques de reconstrucción de datos y la inferencia de propiedades han demostrado ser efectivos para comprometer los datos de entrenamiento en sectores críticos, como el sanitario, donde un fallo en la seguridad de los datos puede tener consecuencias legales graves y sanciones financieras significativas.

Ante estos riesgos, se está avanzando en el desarrollo de la privacy-preserving computing, o computación que preserva la privacidad, que incluye técnicas como la computación multiparte y la criptografía homomórfica. Estas técnicas permiten realizar análisis y entrenamientos de modelos sin exponer datos individuales o parciales, protegiendo así tanto los modelos resultantes como los datos de entrenamiento utilizados. La aplicación de estas tecnologías en sectores como la energía eólica y la maquinaria industrial ha permitido a los fabricantes entrenar modelos con datos de usuarios sin comprometer la privacidad.

El diseño seguro, o Secure by Design, es otro concepto fundamental que se ha posicionado como pilar en la estrategia de ciberseguridad. Este enfoque promueve la integración de la seguridad en todas las fases de desarrollo, en lugar de añadirla como una capa posterior. La ausencia de seguridad desde el diseño ha sido un problema recurrente en la industria y la sanidad, y actualmente afecta también a tecnologías emergentes como los vehículos conectados y los implantes médicos. La incorporación de seguridad desde el diseño es esencial para garantizar la robustez de las soluciones tecnológicas en un entorno donde las amenazas cibernéticas evolucionan rápidamente.

En conclusión, las perspectivas futuras de la ciberseguridad apuntan a la necesidad de combinar tecnologías avanzadas con estrategias de formación y automatización. La colaboración internacional y la implementación de regulaciones de seguridad adaptadas a los nuevos desafíos tecnológicos serán esenciales para enfrentar las amenazas cibernéticas en un escenario donde la conectividad y el uso intensivo de datos redefinen la seguridad digital.

# CASOS DE USO

El 2024 ha marcado un año crucial para el avance de la Ciberseguridad en España, con nuevos desarrollos tecnológicos y normativos que buscan integrar a todas las personas en la era digital.

## Ciberseguridad Colaborativa: El rol de los programas de Bug Bounty en la protección empresarial

Los programas de bug bounty son una herramienta clave en ciberseguridad que permite a empresas detectar vulnerabilidades mediante la colaboración con hackers éticos.

Ofreciendo recompensas a expertos en seguridad, las empresas pueden identificar fallos en sistemas y aplicaciones antes de que sean explotados por ciberdelincuentes. Este enfoque colaborativo mejora la seguridad global de la empresa, al ampliar su red de expertos en ciberseguridad de un par de empleados a una red global de hackers éticos. Reduciendo así las vulnerabilidades mucho más rápido y reduciendo la posibilidad de sufrir un ciber ataque. En Secur0 ayudamos a las empresas a implementar estos programas de manera eficaz, ofreciendo acceso a una red de hackers éticos y gestionando todas las vulnerabilidades reportadas.

## Prueba de concepto para la detección de IoT impulsada por IA en redes cifradas

En el marco del proyecto ITEA ENTA (Encrypted Network Traffic Analysis for Cyber Security), el socio español del proyecto MTP busca empresas que participen en una prueba de concepto (PoC). El proyecto ENTA, en el que participan siete socios de Austria, Canadá, España, Suiza, Turquía y el Reino Unido, tiene como objetivo mejorar la ciberseguridad mediante la detección de dispositivos IoT inusuales dentro del tráfico de red cifrado. La solución desarrollada por MTP utiliza algoritmos de inteligencia artificial, en particular árboles de decisión, para analizar el tráfico cifrado.

## Prueba de concepto para la detección de IoT impulsada por IA en redes cifradas

Esta innovación mejora la detección de dispositivos IoT en las redes y alerta a los administradores sobre posibles vulnerabilidades, lo que permite respuestas rápidas y efectivas a las amenazas de seguridad. El enfoque proactivo de la solución identifica las comunicaciones de alto riesgo, lo que permite a las organizaciones implementar medidas preventivas antes de que las amenazas se intensifiquen. Como parte de la siguiente fase del proyecto, MTP invita a las empresas a participar en una prueba de concepto para validar la eficacia de la solución en entornos del mundo real.

Las organizaciones participantes tendrán la oportunidad de ser pioneras en esta innovadora solución de ciberseguridad y fortalecer sus defensas digitales. Aproveche esta oportunidad de estar a la vanguardia de la innovación en ciberseguridad y salvaguardar su negocio digital con las soluciones avanzadas de MTP.

## Fuzzing

Avanzando en la seguridad del software más allá del análisis estático. El fuzzing es una metodología dinámica de análisis de software que implica la inyección de datos aleatorios o semialeatorios en un programa, buscando descubrir posibles fallos, vulnerabilidades o puntos débiles que podrían ser aprovechados por ciberdelincuentes.

A diferencia del análisis estático, que escruta el código fuente sin ejecutarlo, el fuzzing simula condiciones reales de funcionamiento, lo que permite identificar problemas que de otra manera pasarían desapercibidos.
Esta capacidad para detectar errores en tiempo de ejecución convierte al fuzzing en una herramienta imprescindible para mejorar la seguridad del software y prevenir ataques.

## SINGULARITY

Multiverse desarrolla algoritmos cuánticos de detección de anomalías en entornos de ciber-engaño (phishing). Se generan modelos de aprendizaje automático no supervisado basándose en algoritmos cuánticos o redes tensoriales de inspiración cuántica. Teniendo en cuenta este contexto, se elabora el modelo en 3 etapas: un estudio detallado de la tecnología disponible, la creación de un modelo de detección de anomalías y un estudio del efecto de una línea de base limpia en los datos de entrenamiento para mejorar la eficacia del modelo.

Un analista conoce las vulnerabilidades conocidas que pueden ser explotadas, así como ciertas acciones que pueden activar una notificación de alerta como el intento de aumentar los permisos de un usuario o la inclusión de carpetas ocultas dentro de un software instalado. Sin embargo, un analista no sería capaz de detectar una vulnerabilidad desconocida, ni la extensión del ataque si no requiere de una de estas acciones que activarán la alerta.
El modelo de SINGULARITY es capaz de detectar cualquier ataque como anomalía sea conocido o no. Además, es capaz de filtrar los eventos por 'rareza', permitiendo al analista analizar los eventos más anómalos y reducir así el tiempo necesario para analizar todos los eventos

# ENLACES DE INTERÉS

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

Ciberseguridad: estos serán los principales peligros y amenazas en 2024

El 34% de los incidentes de ciberseguridad gestionados por el CCN-CERT en 2023 alcanzaron nivel de alta peligrosidad

Las claves de la ciberseguridad en 2024

Las empresas de tecnología, financieras y el sector público concentran el 62% de los ciberataques en España

El 60% de los españoles admite falta de conocimiento para evitar estafas 'online'

Consideraciones de ciberseguridad para 2024

La mitad de los españoles ha sufrido un intento de estafa online durante el último año

Aumentan en un 190% los ciberataques al sector público español en 2024

Los ciberataques en España son cada vez más frecuentes y más graves, según Seguridad Nacional

Solo el 2% de las organizaciones españolas pueden protegerse de forma completa de los ciberataques

La mitad de las empresas carece de una estrategia de ciberseguridad dedicada a la IA

Ciberseguridad: ¿riesgo u oportunidad?

La contraseña o la vida

¿Por qué están aumentando los casos de ciberataque en España?

Ciberataques en España se Intensifican en 2024: Empresas e Instituciones en Riesgo

'Phishing', un problema de ciberseguridad en auge: ¿cómo hacerle frente?

Alarma en TotalEnergies: Grave ciberataque pone en riesgo la información de más de 210.000 usuarios

Especialistas: Estos son los retos en ciberseguridad de la red 5G en el país

Del hackeo a la web de ticketmaster al robo de datos de la DGT y Decathlon: España, campeona de Europa en ciberataques

Cómo prevenir los ciberataques en una empresa: guía completa

Ciberseguridad, un aliado necesario en un año complejo

Informe realizado por la **Asociación de Parques Científicos y Tecnológicos de España (APTE),** entidad que gestiona la secretaría técnica de la **Plataforma Tecnológica Española de Tecnologías Disruptivas (DISRUPTIVE)** con la colaboración de su **grupo de trabajo de Ciberseguridad** durante durante el último trimestre de 2024

DISRUPTIVE Plataforma Tecnológica Española de Tecnologías Disruptivas

Ayuda PTR2022-001305 financiada por: MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · AGENCIA ESTATAL DE INVESTIGACIÓN

Secretaria técnica a cargo de: APTE Asociación de Parques Científicos y Tecnológicos de España