CIBERSEGURIDAD

Informe de situación 2023

DISRUPTIV
Plataforma Tecnológica Española de Tecnologías Disruptivas

Ayuda PTR2022-001305 financiada por:
MINISTERIO DE CIENCIA E INNOVACIÓN
AGENCIA ESTATAL DE INVESTIGACIÓN

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

ÍNDICE

INTRODUCCIÓN

En 2023, el paisaje de ciberseguridad en España ha experimentado desarrollos significativos en respuesta a las crecientes amenazas y desafíos. Según datos recientes, el Instituto Nacional de Ciberseguridad (INCIBE) gestionó **un total de 107.500 incidentes** durante el 2022, lo que representa un incremento del 15% en comparación con el año anterior. De estos incidentes, el 34% estuvo relacionado con ataques de malware, lo que sugiere un aumento constante en su prevalencia. Paralelamente, el Centro Criptográfico Nacional identificó 80.000 incidentes, lo que implica un **aumento del 16% con respecto a 2021.** Es preocupante observar que los incidentes críticos vieron un alza del 130% en comparación con el año previo, evidenciando un paisaje de amenazas más agresivo.

El ransomware ha continuado siendo un punto focal de preocupación. Durante la primera mitad de 2023, esta forma de ataque ha causado estragos en varias instituciones públicas y privadas, reafirmando la necesidad urgente de una acción concertada. Como consecuencia, España ha **reforzado su participación en iniciativas internacionales para combatir colectivamente el ransomware,** reconociendo su potencial para socavar la soberanía de los estados y la seguridad económica.

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.

INTRODUCCIÓN

El Informe de Seguridad Nacional resalta la ciberseguridad como un desafío crucial en todas las tecnologías digitales disruptivas. Se prevé que el uso de la inteligencia artificial (IA) para optimizar los ciberataques y cometer actividades delictivas seguirá incrementándose. La red 5G, aunque promete revolucionar la conectividad, enfrenta retos significativos en términos de seguridad, especialmente en lo que respecta a vulnerabilidades en la cadena de suministro y a la protección contra injerencias externas.

El Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU. ha dado pasos adelante con la aprobación de los primeros algoritmos de cifrado resistentes a la computación cuántica, una medida que busca preparar la infraestructura digital para las futuras amenazas. Además, la ciberseguridad se ha convertido en un pilar fundamental para el desarrollo seguro de la tecnología blockchain y sus aplicaciones.

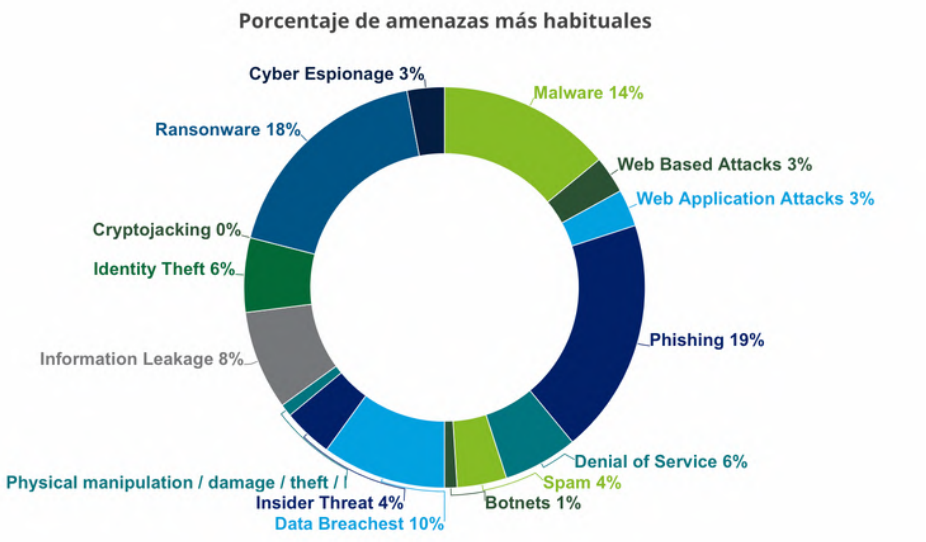
En el ámbito legislativo, España ha convalidado **la Ley de Ciberseguridad 5G,** reforzando el marco de seguridad para el despliegue y la explotación de las redes 5G. A nivel europeo, la aprobación de la directiva NIS 2 y el acuerdo político sobre la Directiva relativa a la resiliencia de las entidades críticas son testimonio del compromiso con el fortalecimiento de la infraestructura crítica ante las amenazas cibernéticas. Ver enlace.

INTRODUCCIÓN

Para las PYMES, la situación es especialmente crítica, ya que según Telefónica Cyber Security Tech, el 60% de las pequeñas y medianas empresas que sufren un ciberataque **desaparecen en menos de seis meses** tras el incidente. Este dato resalta la importancia de una ciberseguridad robusta para la supervivencia empresarial en la era digital.

El informe de Deloitte sobre el estado de la ciberseguridad en España subraya que, además del ransomware, las principales amenazas para las empresas incluyen el **phishing, el malware y los ataques a aplicaciones web.** La gravedad de estas amenazas se ve reflejada en el gráfico proporcionado, donde el **phishing lidera con un 19%,** seguido de cerca por el ransomware con un 18% y los ataques de malware con un 14%.

Esta introducción sienta las bases para un análisis más detallado de las tendencias actuales, los retos y oportunidades, y el ecosistema de ciberseguridad en España en 2023, que se desarrollará en las siguientes secciones de este informe.



Fuente: Estado de la ciberseguridad en España (Deloitte)

TENDENCIAS

En 2023, el escenario de la ciberseguridad en España se ha visto marcado por una serie de tendencias emergentes que están **configurando la estrategia y las operaciones** de las organizaciones en todos los sectores. A continuación, se presentan las tendencias más significativas:

Aumento del ransomware y phishing: 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.

Ciberseguridad como factor de diferenciación empresarial: Las empresas españolas han comenzado a valorar la confianza en sus proveedores de seguridad por encima del precio y de la tecnología que ofrecen. Las inversiones en ciberseguridad no solo buscan proteger los activos sino también actuar como un valor agregado en la propuesta de valor a los clientes.

Escasez de talento especializado: La demanda de profesionales cualificados en ciberseguridad está superando la oferta, con una estimación de que para 2024 serán necesarios 80.000 especialistas en este campo en España. Las empresas y las instituciones educativas están llamadas a **cerrar esta brecha de talento.**

Adopción de Inteligencia Artificial: La IA está emergiendo como una herramienta poderosa tanto para la mejora de la eficiencia en los procesos de detección y respuesta ante incidentes como para la realización de actividades maliciosas más sofisticadas.

TENDENCIAS

Fortalecimiento del marco normativo y colaboración internacional: La convalidación de la Ley de Ciberseguridad 5G y la implementación de la directiva NIS 2 evidencian una fuerte tendencia hacia un marco normativo más sólido y una mayor cooperación internacional para hacer frente a las ciber amenazas.

Preocupación por la protección de infraestructuras críticas: Las directivas europeas y las iniciativas nacionales se han enfocado en aumentar la resiliencia de entidades críticas, lo que ha resultado en una mayor atención a la seguridad de infraestructuras clave como la energía, el transporte y la salud.

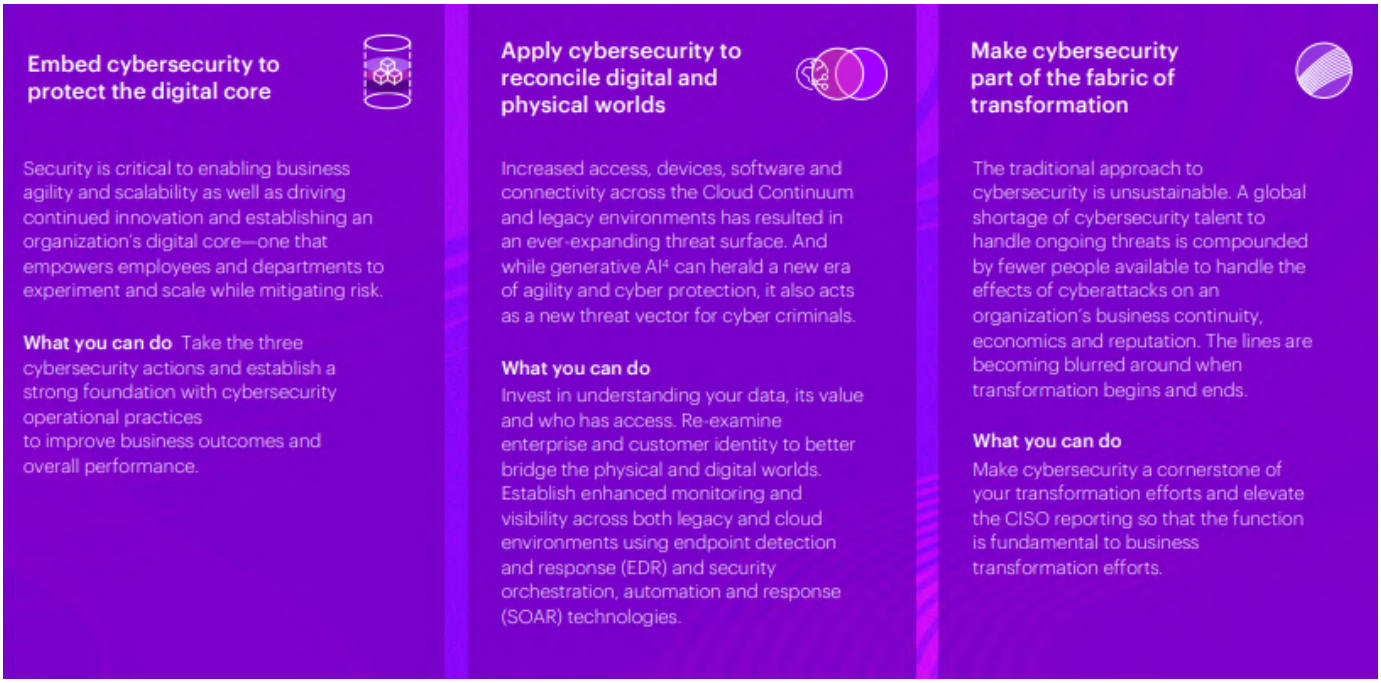
Ciberseguridad en la Industria 4.0: La integración de sistemas de control operacional y tecnologías de la información ha conducido a una mayor preocupación por la seguridad en entornos industriales. Esto incluye la necesidad de proteger la cadena de suministro y la producción contra interrupciones y espionaje.

Servicios de emergencia y asesoramiento: La creciente complejidad de la ciberseguridad y la proliferación de amenazas han llevado a un aumento en la demanda de servicios de emergencia y asesoramiento especializado, como se refleja en programas como Activa Ciberseguridad y el apoyo del INCIBE.

TENDENCIAS

Desafíos de la ciberseguridad para PYMES: Las pequeñas y medianas empresas siguen siendo particularmente vulnerables a los ataques, con un alto porcentaje de ellas desapareciendo tras un incidente. Esto subraya la importancia de estrategias de ciberseguridad accesibles y efectivas para este segmento del mercado.

Estas tendencias señalan una evolución en la percepción y el enfoque de la ciberseguridad en España, indicando un avance hacia la **madurez y la integración de la ciberseguridad** en la gestión de riesgos empresariales y las políticas públicas.



Fuente: Informe Estado de resiliencia en ciberseguridad 2023 (Accenture)

TENDENCIAS

ENISA Threat Landscape 2023

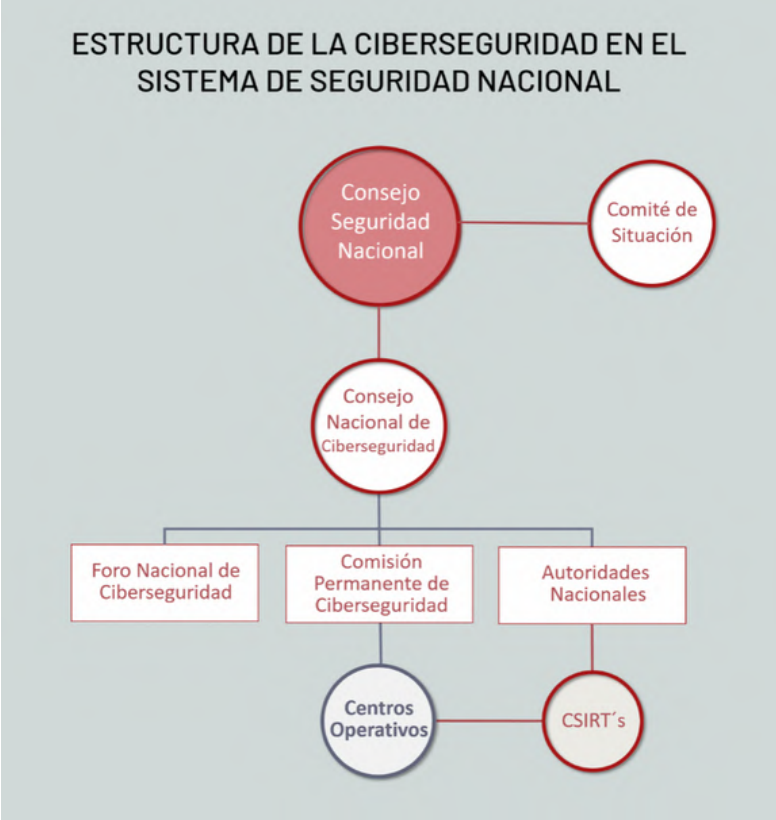
El documento "ENISA Threat Landscape 2023" proporciona un análisis exhaustivo de las tendencias actuales en materia de ciberseguridad, centrándose en las principales amenazas, actores de amenazas, vulnerabilidades y sectores impactados. Los hallazgos clave incluyen:

- Aumento significativo en la variedad y cantidad de ciberataques, influenciados por eventos geopolíticos como la guerra en Ucrania.
- Ransomware y DDoS como las principales amenazas, con un notable incremento en el uso de ransomware.
- Profesionalización de los actores de amenazas y uso de tácticas avanzadas para infiltrarse en los entornos y extorsionar a las víctimas.
- Incremento de la ingeniería social y ataques de phishing, con la IA emergiendo como una técnica clave.
- Ataques a la cadena de suministro, con un enfoque en el uso de empleados como puntos de entrada.

El informe detalla cómo estos desarrollos afectan a varios sectores, enfatizando la importancia de estrategias de mitigación adaptadas y una comprensión profunda del paisaje de amenazas. Puedes acceder al documento completo aquí.

Adicionalmente, el informe "Ciberamenazas y Tendencias" del CCN-CERT ofrece una visión detallada de las ciberamenazas y tendencias actuales, incluyendo la evolución de las tácticas de ciberataques y las recomendaciones para fortalecer la seguridad cibernética. Este informe es una fuente valiosa para comprender las dinámicas actuales en el ámbito de la ciberseguridad. Para más información, se recomienda revisar el documento completo en CCN-CERT IA_35-23 Ciberamenazas y Tendencias.

ESTRATEGIA EN ESPAÑA



La estrategia de ciberseguridad en España durante el año 2023 ha estado caracterizada por un enfoque multidimensional que abarca la prevención, detección, respuesta y recuperación ante incidentes cibernéticos. A continuación, se detallan los pilares fundamentales de esta estrategia:

Marco normativo reforzado: La implementación de la Directiva NIS 2 ha establecido requerimientos de seguridad más estrictos, como los experimentados por compañías del sector de las telecomunicaciones que han debido ajustar sus protocolos y herramientas de seguridad para cumplir con los nuevos estándares de la Ley de Ciberseguridad 5G.

Cooperación Internacional y Público-Privada: Se ha evidenciado en la colaboración entre el INCIBE y la Fundación IDIS, trabajando conjuntamente para fortalecer la ciberseguridad del sector sanitario, marcando un precedente en el compromiso con la seguridad de datos sensibles de pacientes.

ESTRATEGIA EN ESPAÑA

Desarrollo de talentos en Ciberseguridad: El lanzamiento de programas de formación por parte del INCIBE y las alianzas con universidades para ofrecer cursos especializados en ciberseguridad buscan reducir la brecha de especialistas en el sector, con el objetivo de alcanzar los 20.000 profesionales necesarios para 2025.

Adopción de tecnologías avanzadas: El uso de IA en la detección de amenazas se ve reflejado en la colaboración de empresas como Check Point, que han integrado tecnologías avanzadas para combatir sofisticados ataques de ransomware, mostrando un aumento del 20% en la actividad del grupo Lockbit3.

Protección de infraestructuras críticas: La iniciativa de #017ENISE organizada por el INCIBE es un ejemplo de la consolidación de esfuerzos para asegurar infraestructuras críticas, reuniendo a expertos y profesionales para discutir innovaciones y tendencias en ciberseguridad.

Incremento de la concienciación y formación: Programas como Activa Ciberseguridad, dirigidos a pymes, reflejan el esfuerzo por mejorar la comprensión y gestión de la ciberseguridad a nivel empresarial, proporcionando diagnósticos y planes de acción personalizados.

Promoción de la Ciberhigiene: Campañas de concienciación y herramientas como el servicio 017 de INCIBE enfocadas a educar a ciudadanos y empresas sobre prácticas seguras en línea, son claves para promover una cultura de ciberhigiene robusta y efectiva.

ESTRATEGIA EN ESPAÑA

Respuesta y recuperación: El establecimiento de la Red Nacional de SOC demuestra la capacidad de reacción coordinada y casi inmediata ante incidentes, con el objetivo de bloquear cualquier actividad sospechosa en tiempo real y a nivel nacional.

Innovación y I+D en Ciberseguridad: La inversión en proyectos de I+D+i financiados por fondos Next Generation EU y la Iniciativa Estratégica de Compra Pública Innovadora (IECPI) muestra el compromiso con la innovación y el desarrollo de soluciones avanzadas de ciberseguridad.

Red Nacional de SOC: La creación de esta red, que integra los SOC de todos los organismos públicos, evidencia la mejora en la capacidad defensiva del país, siendo un ejemplo claro el trabajo del CCN-CERT en la colaboración con diversos SOC de diferentes magnitudes. En la red también participa el sector privado (ver enlace).

Redes Territoriales de Especialización Tecnológica (RETECH) Ciberseguridad (enlace Redes Territoriales de Especialización Tecnológica (RETECH) | ED2026 | INCIBE), se trata de una iniciativa estratégica del país para el desarrollo del ecosistema de ciberseguridad (capacidades, industria, I+D+i, talento, etc.), que con la coordinación del Instituto Nacional de Ciberseguridad de España (INCIBE), entidad dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, **reunirá en su primera fase a 15 comunidades autónomas con un presupuesto inicial de 149 millones de euros**, en esta línea de actuación. Este programa se enmarca en la Agenda España Digital 2020-2026.

- RETECH Ciberseguridad será además un modelo de colaboración entre INCIBE y las CCAA para el desarrollo de la ciberseguridad en sectores productivos estratégicos relevantes.

ESTRATEGIA EN ESPAÑA

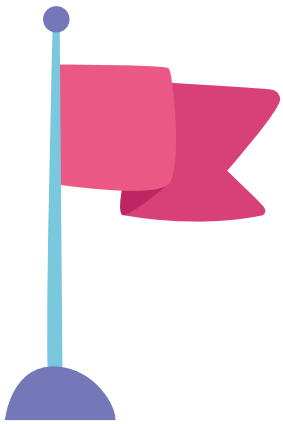
- Esta estructura de RETECH, con la participación de las CCAA y sus ecosistemas de ciberseguridad, formarán parte de la Comunidad Nacional Española en torno al Centro Europeo de Competencia en Ciberseguridad, donde INCIBE actúa como Centro de Coordinación Nacional (NCC-ES).

En todo este contexto, las universidades y el mundo de la investigación, deberán jugar un rol destacado. Sin I+D+i no hay ciberseguridad, y sin ciberseguridad no hay transformación digital.

- Castilla y León dispone en su **estrategia de especialización Inteligente 2021-2027**, de una prioridad para la especialización en ciberseguridad (Castilla y León una apuesta por la fabricación inteligente y la ciberseguridad), y como instrumento para su ejecución define un **Iniciativa Emblemática en ciberseguridad**, donde se recogen de forma centralizada todas las actuaciones en ciberseguridad, que se abordarán principalmente en el marco del proyecto "Red Argos" del Programa RETECH incluido en el punto anterior (ya en el anterior periodo de programación se ejecutó otra iniciativa emblemática en ciberseguridad por valor de 24Millones€). Enlace: Iniciativas Emblemáticas RIS3 2021-2027 | Ciencia y Tecnología | Junta de Castilla y León (jcyl.es).

- Desde el Instituto de Competitividad Empresarial de Castilla y León, en el marco de la **Estrategia de Emprendimiento e Innovación de Castilla y León 2027 (EEI 27)**, que será **la hoja de ruta compartida por los agentes del ecosistema** de emprendimiento e innovación , en su Linea Estratégica 3, Castilla y León con la trasformación digital, se incluye una medida **estratégica en ciberseguridad** como **herramienta esencial para abordar esta transformación digital segura de las empresas** (medida 35) Enlace: Estrategia de Emprendimiento e Innovación de Castilla y León 2027 (EEI 27) | Empresas | Junta de Castilla y León (jcyl.es)

RETOS Y OPORTUNIDADES



En 2023, España se encuentra en un **punto crítico** en el ámbito de la ciberseguridad.

A medida que la digitalización penetra en todos los aspectos de la vida empresarial y social, la protección contra los ciberataques se ha convertido en un componente indispensable de la estrategia nacional. Este panorama presenta **tanto desafíos complejos como oportunidades únicas** para fortalecer las defensas y capacidades en ciberseguridad del país.

RETOS

Adaptación al rápido cambio tecnológico: La ciberseguridad en España enfrenta el desafío constante de mantener el ritmo frente a tecnologías emergentes, como el 5G, la IA y el blockchain.

Brecha de competencias y recursos: La necesidad de profesionales especializados en ciberseguridad es urgente, especialmente cuando el INCIBE estima que se necesitarán 80.000 profesionales en el campo para 2024.

Gestión de la Ciberseguridad en PYMEs: Las pequeñas y medianas empresas, a menudo con recursos limitados, luchan por implementar estrategias efectivas de ciberseguridad.

Seguridad de datos en infraestructuras críticas: Proteger sectores vitales como la salud y la energía contra ciberataques sigue siendo un reto significativo.

RETOS Y OPORTUNIDADES

Implementación de nuevas normativas

La implementación de nuevas normativas en España en materia de ciberseguridad en 2023 debe contemplar la integración de leyes europeas significativas. Entre ellas, se destaca el Acto de Resiliencia Cibernética (CRA) de la Unión Europea, que establece requisitos obligatorios de seguridad para fabricantes y minoristas de productos y software con componentes digitales. Este acto se enfoca en garantizar la seguridad a lo largo del ciclo de vida del producto y mejorar la confianza del consumidor.

Además, la Ley de Inteligencia Artificial (IA) de la UE propone un marco regulador para sistemas de IA, clasificándolos según su nivel de riesgo y estableciendo obligaciones para proveedores y usuarios. Esta ley busca garantizar la seguridad, transparencia y no discriminación de sistemas de IA, asignando responsabilidades específicas según el nivel de riesgo.

Estas legislaciones, especialmente el CRA, que se espera entre en vigor en 2024, y la Ley de IA, refuerzan la necesidad de adaptación y actualización constante en los protocolos y sistemas de seguridad de las organizaciones españolas.

Para más detalles sobre el CRA, puedes visitar EU Cyber Resilience Act. Para más información sobre la Ley de IA, consulta Ley de IA de la UE.

RETOS Y OPORTUNIDADES

OPORTUNIDADES

Programas de Asesoramiento como Activa Ciberseguridad: Iniciativas como el programa "Activa Ciberseguridad" de la Secretaría General de Industria y de la PYME ofrecen asesoramiento especializado y planes personalizados de ciberseguridad, abriendo puertas para que las PYMEs mejoren su resiliencia digital.

Colaboración entre Entidades Públicas y Privadas: La colaboración entre el INCIBE y entidades como la Fundación IDIS destaca la oportunidad de compartir recursos y conocimientos para fortalecer la ciberseguridad nacional.

Inversión en formación y desarrollo de talento: La creciente demanda de expertos en ciberseguridad presenta una oportunidad para invertir en formación y desarrollo de talento especializado.

Innovación y desarrollo tecnológico: La adopción de tecnologías avanzadas, como la IA en la detección de amenazas, ofrece oportunidades para mejorar la eficiencia y efectividad en la ciberseguridad.

Fortalecimiento del Marco Legal y Normativo: La adaptación a las nuevas regulaciones puede actuar como catalizador para que las empresas revisen y fortalezcan sus estrategias de ciberseguridad.

Concienciación y educación: Campañas de sensibilización y programas educativos sobre ciberseguridad pueden crear un entorno digital más seguro para todos los usuarios.

RETOS Y OPORTUNIDADES

Iniciativas de Apoyo del INCIBE: La línea de ayuda gratuita del INCIBE y su apoyo constante a las empresas proporcionan una base sólida para la gestión de la ciberseguridad.

Creciente mercado de Ciberseguridad: El aumento de la demanda de soluciones de seguridad ofrece un mercado en crecimiento para empresas innovadoras en el sector.

Estrategias de resiliencia ante incidentes: El desarrollo de la Red Nacional de SOC enfatiza la importancia de la capacidad de respuesta y recuperación ante incidentes.

Inversión en I+D+i: La financiación de la UE y el compromiso del gobierno español con proyectos de I+D+i en ciberseguridad alientan la innovación y el desarrollo de nuevas soluciones.

La Unión Europea está trabajando en el Acto de Resiliencia Cibernética, un nuevo marco legal para aumentar la seguridad de los productos y software con componentes digitales. Este acto establecerá requisitos obligatorios de ciberseguridad para fabricantes y minoristas, cubriendo todo el ciclo de vida del producto.

Aborda la falta de seguridad cibernética en muchos productos y la dificultad para los consumidores y empresas de determinar qué productos son seguros. Se espera que entre en vigor a principios de 2024, exigiendo que los productos conectados a internet lleven el marcado CE para indicar el cumplimiento de los nuevos estándares.

Para más información, puedes visitar el sitio web de la Unión Europea sobre el futuro digital.

RETOS Y OPORTUNIDADES

Una oportunidad notable en el ámbito de la ciberseguridad en España en 2023 es la colaboración entre empresas privadas, como la ampliación de la alianza entre **Accenture y Google Cloud.** Esta asociación se enfoca en mejorar la resiliencia en ciberseguridad para las empresas, integrando la inteligencia artificial generativa específica de seguridad de Google Cloud en el servicio Managed Extended Detection and Response (MxDR) de Accenture.

Esta colaboración busca potenciar la protección de activos críticos frente a ciberamenazas, utilizando tecnologías avanzadas y compatibles con plataformas de seguridad comunes y otras nubes.
Fuente: Accenture y Google Cloud amplían su alianza

Estos retos y oportunidades subrayan la importancia de una **estrategia proactiva y adaptativa** en la ciberseguridad de España en 2023. Con el apoyo adecuado y la implementación de programas como "Activa Ciberseguridad", el país puede mejorar su postura de seguridad y convertirse en un modelo de resiliencia cibernética.

ECOSISTEMA

España ha emergido como un ecosistema caracterizado por un tejido empresarial innovador, una sólida colaboración entre el sector público y privado, y un compromiso a nivel nacional con la seguridad digital.

Este paisaje está marcado por la sinergia entre empresas consolidadas y startups emergentes, apoyadas por un marco institucional que fomenta la innovación y la especialización en el campo de la ciberseguridad.

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

Incibe es designado en septiembre centro como Centro de Coordinación Nacional del Centro Europeo de Competencia en Ciberseguridad.
El Centro Europeo de Competencias en Ciberseguridad es una iniciativa europea que se enmarca dentro de las políticas europeas en ciberseguridad y que tiene como objetivo crear un ecosistema industrial y de investigación sobre ciberseguridad interconectado a escala de la UE, mejorando la cooperación entre las partes interesadas para hacer el mejor uso posible de los recursos y conocimientos técnicos existentes en esta materia en toda Europa. Con este fin se crea una red europea de Centros Nacionales de Coordinación (NCC) compuesta por 27 centros.

ECOSISTEMA

RENIC: La Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), promovida por INCIBE, es una asociación sectorial que engloba centros de investigación y otros agentes del ecosistema investigador en ciberseguridad de España. RENIC tiene como fin principal fomentar la investigación científica, el desarrollo tecnológico, la innovación, la trasferencia de conocimiento y tecnología a la industria y el desarrollo de proyectos de I+D+i en el sector de la ciberseguridad en España.

ObservaCIBER: es un nuevo espacio de encuentro especializado en ciberseguridad que, ante la creciente demanda de información sobre este ámbito por parte de la ciudadanía y las empresas, pretende por un lado, poner en valor el trabajo que vienen desarrollando los diferentes actores y por otro, conectar el conocimiento desarrollado por la administración en esta materia facilitando su comprensión. Su objetivo es aumentar la cultura de la ciberseguridad facilitando el acceso a la información y fomentando su calidad.

ECOSISTEMA

Woman4Ciber Spain: Women4Cyber Spain (W4C Spain) es una iniciativa que nace con el objetivo de convertirse en un referente en el impulso y visibilización del papel de la mujer en ciberseguridad en España, así como la diversidad de género en el sector.
La Asociación es el capítulo español de Women4Cyber.eu, fundada por la Organización Europea de Ciberseguridad (ECSO), y la primera asociación de mujeres en ciberseguridad en España que cuenta con respaldo europeo.

Dentro del ecosistema de ciberseguridad en España, destaca el emprendimiento femenino en **empresas tecnológicas como IriusRisk, authUSB y shaadow.io.** Estas compañías, lideradas por mujeres, están contribuyendo significativamente al avance en el campo de la seguridad informática. IriusRisk se especializa en la gestión proactiva de riesgos de seguridad en aplicaciones, mientras que authUSB se centra en la seguridad de dispositivos USB. Por su parte, shaadow.io ofrece soluciones innovadoras en el ámbito de la protección de datos y la privacidad.

Málaga Hub de Ciberseguridad: Málaga se está posicionando como un gran hub de ciberseguridad. A la instalación de la Agencia Digital de Andalucía y el Centro de Ciberseguridad de Andalucía se le suma la apuesta que han hecho por la capital de la Costa del Sol empresas privadas del sector de la tecnología como Vodafone (con su centro tecnológico para toda Europa que creará 600 empleos cualificados), Google (con su centro de ciberserguridad), Telefónica (con el campus de programación que impulsa su Fundación en colaboración con la Junta), Dekra, Ericcson y o la Fundación Instituto Ricardo Valle.

ECOSISTEMA

Otros hub de ciberseguridad: Asimismo, destacan también otros puntos del mapa español como:

- **Centro Vasco de Ciberseguridad (BCSC):** Este centro, situado en el País Vasco, se centra en la investigación y el desarrollo en ciberseguridad.
- **Centro Regional de Innovación Digital de Castilla-La Mancha (CRID):** Situado en Castilla-La Mancha, se dedica a impulsar la innovación digital y la ciberseguridad en la región.
- **Agencia de Ciberseguridad de Cataluña:** Enfocada en fortalecer la seguridad digital en Cataluña.
- **Agencia de Ciberseguridad de la Comunidad de Madrid:** Recientemente creada para reforzar la ciberseguridad en Madrid.
- **Centro de Excelencia en Ciberseguridad de Galicia (CEC):** Ubicado en A Coruña, este centro se enfoca en la investigación y desarrollo en ciberseguridad.
- **Centro Criptológico Nacional (CCN):** Con sede en Madrid, depende del Centro Nacional de Inteligencia (CNI) y se especializa en la protección de la información clasificada.
- **EuskalCERT:** Es el equipo de respuesta a incidentes de ciberseguridad del País Vasco.
- **Cybersecurity Innovation Hub:** En Valencia, es un centro que promueve la innovación y el desarrollo empresarial en el ámbito de la ciberseguridad.

ECOSISTEMA

EMPRESAS LÍDERES EN CIBERSEGURIDAD

Telefónica Cyber Security Tech: Esta firma ha consolidado su posición como líder en el desarrollo de estrategias de ciberseguridad, con soluciones que abarcan desde la infraestructura de TI hasta la seguridad IoT, respaldando a una amplia gama de industrias.

Indra: Con una reputación internacional, Indra ofrece soluciones de seguridad avanzadas, marcando pautas en proyectos de defensa y protección de infraestructuras críticas.

GMV: Especializada en sistemas seguros, GMV lidera el camino en la protección de infraestructuras críticas y ofrece innovaciones en el ámbito espacial y de defensa.

STARTUPS INNOVADORAS EN CIBERSEGURIDAD

IriusRisk: startup de ciberseguridad aragonesa ubicada en el Parque Tecnológico Walqa consigue 29 millones de euros en una ronda liderada por Paladin Capital Group. La empresa se fundó en Aragón por Stephen De Vries y Cristina Bentué.

CounterCraft: Esta startup destaca por su enfoque proactivo en la defensa cibernética, con plataformas que utilizan estrategias de engaño para identificar y neutralizar amenazas.

Blueliv: Con una propuesta basada en la inteligencia frente a las amenazas cibernéticas, Blueliv proporciona análisis y datos críticos para prevenir ataques.

ECOSISTEMA

Made of Genes: Aunque centrada en la biotecnología, ha desarrollado métodos de ciberseguridad para asegurar datos genéticos y médicos sensibles.

Feedzai: Esta empresa ha ganado reconocimiento por su solución antifraude que utiliza la biometría y el comportamiento del usuario en línea.

Hdiv Security: Orientada a la seguridad en el desarrollo de aplicaciones, ofrece herramientas para la protección desde las fases iniciales de programación.

COLABORACIÓN Y APOYO INSTITUCIONAL

La colaboración es una piedra angular del ecosistema español de ciberseguridad. Las startups trabajan de la mano con empresas establecidas, beneficiándose de programas de aceleración y del respaldo institucional. Programas como **Activa Ciberseguridad de SGIPYME y EOI** demuestran el enfoque estratégico nacional para fortalecer las capacidades de ciberseguridad en empresas de todos los tamaños.

El panorama español en 2023 refleja un enfoque integral hacia la ciberseguridad, donde la innovación y la cooperación entre diferentes actores del mercado se unen para formar un ecosistema resiliente. La presencia de instituciones gubernamentales y la participación activa de las empresas subrayan la **prioridad que España concede a la ciberseguridad** en el contexto de una economía y sociedad cada vez más digitalizadas.

CASOS DE USO

A continuación os mostramos algunos de los ejemplos de casos de uso que DISRUPTIVE ha ido recopilando y que puedes consultar con más detalle pinchando aquí

Ethical Hacking Penetration Test - Cloud Levante

Adam Riese, una empresa emergente del Grupo W&W centrada en revolucionar el mercado de los seguros, ha realizado una prueba de penetración de hacking ético para mejorar su seguridad en línea. La prueba pretende identificar vulnerabilidades desde la perspectiva de un atacante y reforzar las defensas de la red. Las tareas clave del equipo de ciberseguridad incluyen el mapeo de la red, la identificación de vulnerabilidades, la explotación y la elaboración de informes.

DYNABIC - TECNALIA

DYNABIC es un proyecto Horizonte Europa que comenzó en Diciembre de 2022 y tiene 3 años de duración. El proyecto investiga sobre el uso de gemelos digitales para la mejora de la ciber resilencia de sistemas críticos, a través de la evaluación continua de los ciber riesgos del sistema y la protección y adaptación del sistema frente a amenzas ciber-físicas.

Aplicación de la Blockchain en IoT - Universidad de Málaga

Falta de seguridad en los dispositivos IoT, para control y gestión de las Smart City, con la Blockchain damos solución al problema.

CASOS DE USO

A continuación os mostramos algunos de los ejemplos de casos de uso que DISRUPTIVE ha ido recopilando y que puedes consultar con más detalle pinchando aquí

SECBLURED - LAUDE Canarias

El proyecto SecBluRed - Aproximación holística a la ciberseguridad en el IoT Industrial, plantea diversas líneas de investigación industrial que tratan de dar respuesta a diversos retos a los que la industria española se tendrá que enfrentar en los próximos años. Se trata de un proyecto financiado dentro del Programa Misiones GG.EE. 2022 del CDTI. Edosoft (ahora LAUDE Canarias) participa como miembro del consorcio, liderado por MTP, con el objetivo de investigar nuevas aproximaciones para la mejora de la seguridad en las comunicaciones entre nodos de una red IIoT contemplando un escenario post-cuántico; así como en la aplicación de analítica de datos e inteligencia artificial para la mejora de la gestión de la información y los eventos de seguridad en las plataformas de gestión de IoT industrial (IIoT).

PIACERE - TECNALIA

Para fortalecer la evolución de la automatización de la infraestructura y avanzar en el concepto de infraestructura como código, es imperativo equipar a los ingenieros de DevSecOps con herramientas y un entorno de desarrollo comparables a los disponibles para los desarrolladores de software tradicionales. (1/2)

CASOS DE USO

A continuación os mostramos algunos de los ejemplos de casos de uso que DISRUPTIVE ha ido recopilando y que puedes consultar con más detalle pinchando aquí

PIACERE - TECNALIA

El proyecto PIACERE H2020 se enfoca en mejorar la eficiencia y seguridad en el desarrollo y operación de infraestructuras de software, aplicando el enfoque de DevSecOps. Permite tratar la infraestructura de software como se maneja el código de aplicación, desde la definición de requisitos hasta el diseño, implementación, y monitoreo. PIACERE utiliza técnicas de modelado, plantillas y automatización, integrando herramientas de inspección de seguridad para verificar la validez y confiabilidad del código tanto en diseño (SAST) como en operación (DAST), utilizando entornos de prueba y técnicas avanzadas como el procesamiento de lenguaje natural (NLP) para la detección de anomalías. (2/2)

Brokel - TECNALIA

Brokel es una plataforma avanzada para compartir y analizar datos sensibles de forma segura entre diversas organizaciones. Utiliza técnicas de preservación de la privacidad, como criptografía avanzada, para asegurar la soberanía de los datos compartidos. Ofrece herramientas para integrar datos existentes, normalizarlos en un formato común y coordinar la explotación conjunta de datos. Actualmente, Brokel se está probando en diversos sectores como la sanidad, industria, energía y gobierno, a través de proyectos piloto tanto nacionales como internacionales.

ENLACES DE INTERÉS

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

Las empresas españolas incrementan inversión en ciberseguridad frente a ataques cada vez más críticos y dañinos

INCIBE y la Fundación IDIS firman un convenio para impulsar la ciberseguridad en el sector sanitario

Seguridad Nacional sugiere que el Código del Buen Gobierno en Ciberseguridad aplique no solo a cotizadas

Más de un 60% de las empresas españolas afirma haber recibido un mayor número de ciberataques en 2023

La IA y la ciberseguridad se disparan como riesgos globales

En la primera mitad de 2023 han aumentado un 8% los ciberataques mundiales

Empresas españolas elevan inversión en ciberseguridad frente a ataques cada vez más críticos y dañinos

Google anuncia seis estrategias de ciberseguridad en sus servicios

Éxito absoluto de #017ENISE como evento internacional de ciberseguridad

INCIBE y Fundación IDIS se unen para impulsar la ciberseguridad en el sector sanitario

Ciberseguridad en la administración local: un desafío legal y tecnológico

ENLACES DE INTERÉS

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

INCIBOT: la nueva herramienta de INCIBE para la ciberseguridad

Los 7 puntos vitales en la ciberseguridad de las cadenas de suministro

IA generativa y ciberseguridad: un binomio con riesgos y beneficios para las empresas

La ciberseguridad en España pide más de 20.000 expertos

Conferencia sobre la situación actual de la red 24/7 y la lucha contra la ciberdelincuencia en el marco de la UE

Ciberseguridad en pymes españolas: un estudio revela la cruda realidad

Pymes ante el reto de la ciberseguridad: cómo afrontar los riesgos sin recursos de las grandes

NIS2: ciberseguridad y resiliencia, de la teoría a la práctica

Copilot está a punto de despegar: retos en cuanto a la ciberseguridad

El lado oscuro del IoT: un nuevo estudio revela alarmantes amenazas para la privacidad y la seguridad en los hogares inteligentes

Solo el 61% de los equipos de ciberseguridad cuentan con personal suficiente

La ciberseguridad, el elefante en la habitación de las empresas

El reto de la ciberseguridad

ENLACES DE INTERÉS

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

Carme Artigas inaugura la conferencia anual europea sobre habilidades en ciberseguridad

El Foro Nacional de Ciberseguridad presenta nuevos trabajos

Sobre ENISA - Agencia de la UE para la Ciberseguridad

La Red Nacional de SOC: plataforma del CCN-CERT

Ciberseguridad industrial: retos y estrategias

Una al día: Blog de Hispasec sobre ciberseguridad

Nueva convocatoria de ayudas Activa Ciberseguridad para pymes

Inauguran el Centro de Seguridad de Andalucía en Málaga

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 el último trimestre de 2023

DISRUPTIVE Plataforma Tecnológica Española de Tecnologías Disruptivas

Ayuda PTR2022-001305 financiada por: MINISTERIO DE CIENCIA E INNOVACIÓN · AGENCIA ESTATAL DE INVESTIGACIÓN

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