

EDICIÓN ESPECIAL

EmpresaXXI

01 Junio 2026



CIBER SEGURIDAD





PEXELS-FERNANDO NARVAEZ

CONTEXTO SECTORIAL | LA SITUACIÓN EN EL MUNDO

LA IA REVOLUCIONA LA CIBERSEGURIDAD

LOS EXPERTOS SUBRAYAN QUE LAS ESTRATEGIAS BASADAS ÚNICAMENTE EN LA DETECCIÓN Y RESPUESTA A LOS CIBERATAQUES YA NO SON SUFICIENTES: SE IMPONE UN ENFOQUE PREVENTIVO

La incertidumbre geopolítica reinante en el mundo y las amenazas impulsadas por avances tecnológicos, como la Inteligencia Artificial (IA) o la computación cuántica, que amplían el frente de los ciberataques, obligan a replantear la estrategia de ciberseguridad de las organizaciones, según expertos del sector. En este sentido, la mayor parte de ellos coinciden al afirmar que, ante este nuevo escenario, los enfoques basados únicamente en detección y respuesta ya no son suficientes frente a amenazas que operan a velocidad de máquina, sino que la defensa debe evolucionar hacia una estrategia centrada en la prevención, capaz de anticiparse a los ataques antes de que se propaguen.

En su Security Report 2026, Check Point Software Technologies alerta de un entorno de amenazas cada vez más automatizado impulsado por la utilización de la IA por parte de

los ciberdelincuentes. Esta tecnología no solo contribuye a elevar el volumen de los ataques. También está transformando profundamente el modo en el que se diseñan, escalan y coordinan.

49%

**DE LAS EMPRESAS
NO PREVÉ MEDIDAS
POR CIBERAMENAZAS
DE LA CUÁNTICA**

Según el último informe elaborado por el proveedor de soluciones de ciberseguridad en la nube basadas en IA, a nivel global, más de 7.960 organizaciones vieron sus datos publicados en sitios de filtración gestionados por grupos de extorsión, lo que supone un incremento interanual del 53%. Y el

cuarto trimestre de este año se cerró con 2.473 víctimas, el dato más alto registrado hasta la fecha.

Nuevas tendencias

El informe destaca que, más allá del 'ransomware' (secuestro de datos), se está produciendo un cambio hacia campañas de ataque integradas y multicanal que combinan engaño humano y automatización a gran escala. Así, Check Point explica que los ataques impulsados por IA se vuelven más autónomos, con la integración de inteligencia artificial en los flujos de trabajo de ataque para acelerar el reconocimiento, la ingeniería social y la toma de decisiones operativas. Al mismo tiempo, subraya que la ingeniería social se expande más allá del correo electrónico, coordinando ataques a través de web, teléfono, navegadores, plataformas SaaS y herramientas de colaboración.

En este contexto de remode-

lación del panorama de riesgos, la última encuesta Global Digital Trust Insights 2026 de PwC, realizada a cerca de 4.000 directivos y responsables de tecnología de compañías de más de 70 países, revela que el 60% de los mismos sitúan a la inversión en ciberseguridad entre sus tres principales prioridades estratégicas para el año que viene, si bien también están implementando cambios en la ubicación de infraestructuras críticas (41%), en las políticas comerciales y operativas (39%) y en las pólizas de los ciberseguros (39%). Otras de las conclusiones que pone de manifiesto el estudio son, por un lado, que solo el 24% de las organizaciones invierte significativamente más en medidas proactivas, como monitorización, evaluaciones, pruebas y controles, y que la IA agentiva se encuentra entre las principales capacidades de seguridad basadas en esta tecnología que las organizaciones planean priorizar en el próximo año.

La UE, bajo el foco

En Europa, la Agencia de la UE para la Ciberseguridad, Enisa, pone de manifiesto en su último informe de amenazas cibernéticas que los ataques DDoS, que tienen como finalidad interrumpir el tráfico normal de un servidor, servicio o red sobrecargándolo con una avalancha masiva de tráfico de Internet, son el tipo de incidente predominante, mientras que el 'ransomware' se considera la amenaza de mayor impacto en la UE y el 'phishing' (60%), segui-

EL VOLUMEN DE LOS ATAQUES SE ELEVA Y SE TRANSFORMA EL MODELO EN QUE SE DISEÑAN Y ESCALAN

do de la explotación de vulnerabilidades (21%) se constituyen como los dos puntos de acceso para intrusiones. Además, a la cabeza de la lista de sectores atacados en la UE se encuentra la administración pública (38%), en segundo lugar se sitúa el sector del transporte (8%), seguido de la infraestructura y los servicios digitales (5%), las finanzas (5%) y la industria manufacturera (3%).

CIBERSEGURIDAD | CONGRESO

EL RETO DE PROTEGER LA FÁBRICA CONECTADA

CYBERINDUSTRY CONGRESS 2026 REUNIRÁ EN BILBAO DEL 16 AL 17 DE JUNIO A TODA LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Bilbao se convertirá los próximos 16 y 17 de junio en uno de los principales escaparates de la ciberseguridad industrial con la celebración del CyberIndustry Congress 2026 en el Azkuna Zentroa, un foro que reunirá a empresas tecnológicas, industria, expertos internacionales, *startups*, universidades e instituciones para analizar los nuevos

riesgos digitales que afronta la economía conectada.

Tras el éxito de su primera edición, el congreso busca consolidarse como una referencia estatal con creciente proyección internacional en un momento en el que la ciberseguridad ha dejado de ser un asunto reservado a departamentos técnicos para situarse en el centro de la competitividad industrial, la resiliencia empresarial y la soberanía tecnológica europea.

En el punto de mira

La edición de 2026 pondrá el foco en ámbitos especialmente sensibles para la continuidad operativa, como la protección de infraestructuras críticas, la ciberseguridad industrial, la seguridad de la cadena de suministro, la inteligencia artificial o el impacto de las nuevas normativas europeas, entre ellas el Reglamento CRA (Cyber Resilience Act).

El encuentro se articulará en torno a cinco grandes bloques temáticos centrados en geopolítica y sectores estratégicos, riesgos en sistemas conectados,

inteligencia artificial, regulación europea y ecosistema de innovación y talento. El programa incluirá también un espacio específico impulsado por la iniciativa europea Women4Cyber, reforzando la dimensión social y humana de la transformación digital.



CyberIndustry Congress 2026 conectará oferta y mercado.

CyberIndustry Congress conectará las necesidades reales de la industria con la oferta tecnológica en un contexto marcado por el aumento de las amenazas digitales y la creciente dependencia de sistemas conectados en sectores como energía, salud, administración, movilidad o fabricación avanzada.

ikerlan

MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

ESPECIALIZACIÓN MULTITECNOLÓGICA

- TECNOLOGÍAS DIGITALES E INTELIGENCIA ARTIFICIAL
- SISTEMAS ELECTRÓNICOS EMBEBIDOS Y CIBERSEGURIDAD
- ENERGÍA Y MECATRÓNICA



Where technology
is an attitude.

Somos un centro tecnológico enfocado en transferir tecnología a las empresas, formar a las personas y contribuir a la creación y puesta en marcha de nuevas empresas tecnológicas.

EUROPA | REGULACIÓN

LA CIBERRESILIENCIA, UNA PRIORIDAD INAPLAZABLE

LA CRA ESTABLECE REQUISITOS OBLIGATORIOS PARA LOS PRODUCTOS QUE INCLUYEN ELEMENTOS DIGITALES A LO LARGO DE TODO SU CICLO DE VIDA

La Ley de Ciberresiliencia, el Reglamento CRA (por sus siglas en inglés), se constituye como una de las normativas europeas más importantes en materia de ciberseguridad, ya que establece por vez primera requisitos de alta exigencia obligatorios para cualquier producto conectado a lo largo de todo su ciclo de vida y pone las bases para asegurar que la resiliencia en esta materia sea una prioridad, aumentando así la seguridad de los usuarios finales.

La CRA entró en vigor a finales de 2024, si bien la aplicación plena no se producirá hasta diciembre de 2027. El reglamento fija las condiciones necesarias para permitir el desarrollo de productos con elementos digitales seguros, garantizando que los equipos y programas informáticos se comercialicen con menos vulnerabilidades y que los fabricantes apuesten por la seguridad durante toda la vida del producto.

Esta ley afecta a una amplia gama de actores en el mercado digital, incluyendo fabricantes, tanto de dentro de la UE como de fuera de ella cuando sus productos se comercialicen en el mercado europeo, desarrolladores de 'software', distribuidores e importadores e, incluso, revendedores, siempre y cuando participen en el suministro de productos afectados en el mercado de la UE.

Según advirtió a este periódico el responsable de ciberseguridad de Ikerlan,

PROGRAMA DE ACCELERACIÓN DE ZIUR

El Centro de Ciberseguridad Industrial de Gipuzkoa, Ziur, puso en marcha el año pasado un programa de aceleración para anticipar la adaptación de las empresas a las exigencias europeas en materia de ciberseguridad, especialmente del reglamento CRA.

En seis meses, ha posibilitado el inicio del proceso de evaluación de 18 productos y servicios, un 25% de las evaluaciones previstas para este año. Además de las evaluaciones técnicas, Ziur incorpora actividades de formación, asesoramiento normativo sectorial, auditorías de componentes industriales y gestión de vulnerabilidades técnicas con el apoyo de tres laboratorios especializados en ciberseguridad industrial y un equipo de diez expertos en ciberseguridad OT, IoT e IoMT.

El programa se desarrolla con agentes tecnológicos y empresariales especializados en evaluación y certificación de ciberseguridad industrial, como telefónica, Thales, Orbik, Vicomtech, Ikerlan, Corporación Mondragon y AFM, entre otros.

David González, "en la práctica, muchas empresas industriales todavía están lejos de cumplir con estas exigencias" y, aunque su aplicación plena no se producirá hasta finales del próximo año, "los ciclos de desarrollo de producto son largos". En concreto, precisó que "la adaptación real requiere cambios profundos, desde la incorporación de prácticas de 'security by design' en el desarrollo, hasta la gestión de vulnerabilidades, actualizaciones seguras o trazabilidad del 'software'".

Productos conectados

Esta normativa afecta a cualquier producto de 'software' o 'hardware', así como a cualquier 'software' o 'hardware' no incorporado

al producto, pero introducido en el mercado por separado. Es decir, se aplica a todos los productos conectados directa o indirectamente a otro dispositivo o red. En cuanto a los requisitos obligatorios de ciber-

LA LEY ENTRÓ EN VIGOR EN 2024 PERO SU APLICACIÓN PLENA LLEGARÁ A FINALES DE 2027

seguridad exigibles a los fabricantes, abarcan desde la planificación hasta su mantenimiento, pasando por el diseño y el desarrollo. Y un punto importante es que estas obligaciones deben

cumplirse en todas las etapas de la cadena de valor. Por eso, la CRA no solo abarca a los productos finales, como teléfonos inteligentes o aplicaciones, sino también a los componentes, como chips y sistemas operativos.

Las empresas que venden productos de 'hardware' y 'software' deben garantizar que éstos se hayan diseñado con una seguridad fundamental, lo que incluye, por ejemplo, control de acceso, el uso de criptografía y actualizaciones automáticas. Además, los fabricantes deberán mantener sus productos durante el tiempo que se prevea su uso.

Evaluación de riesgos

Antes de sacarlo al mercado, el fabricante deberá realizar una evaluación de riesgos, a partir de la cual deberá definir cómo implementar los requisitos esenciales de ciberseguridad adecuados. Al finalizar el proceso, podrá colocar el marcado CE y añadir una declaración de conformidad a sus productos. Asimismo, tendrá que indicar el periodo de soporte. Tras su lanzamiento, deberá gestionar las vulnerabilidades durante el periodo de soporte indicado e informar sobre las que se estén explotando activamente.



La CRA no solo abarca a productos finales, sino también a componentes, como chips y sistemas operativos.

ESPAÑA | MERCADO

MOTOR DE ECONOMÍA DIGITAL

LA CIBERSEGURIDAD FACTURA 6.350 MILLONES DE EUROS Y EMPLEA A 165.000 PERSONAS

CIBERSEGURIDAD INDUSTRIAL, AL FINAL DE LA LISTA

La identidad, la nube y la protección del dato marcan la agenda inversora de los proyectos de ciberseguridad en España.

PRÓXIMOS PROYECTOS	% TOTAL	PRÓXIMOS PROYECTOS	% TOTAL
Servicios SOC/SIEM/Seg. gest.	32,8%	Segmentación/protección red	12,6%
Cloud Security	29,6%	Threat Intelligence	11,4%
Formación y Concienciación	23,2%	Ciberseguridad industrial	7,2%
Autenticación robusta	22,8%	Endpoint Security	6,4%
Consultoría de seguridad	21,8%	Email Security	3,6%
SASE	19,4%	Web Security	2,6%
DLP/IRM	18,0%	DNS Firewall	1,4%

Fuente: Barómetro del estado de ciberseguridad en España 2025 de LKS Next.

CRECE EL EMPRENDIZAJE EN CIBERSEGURIDAD

La facturación de las 403 empresas jóvenes de ciberseguridad en España supuso el 12% del total del sector en 2024.

	Nº EMPRESAS	FACTURACIÓN	%TOTAL
Sector Ciberseguridad	3.431	6.351	100%
Empresas jóvenes	403	745	12%
Emprendimiento	254	469	7%
En estudio	46	85	1%

Nota: Empresas jóvenes son aquellas de menos de 5 años. Fuente: Incibe

ESPAÑA ES EL CUARTO MERCADO DE EUROPA

Con un 2,8% de la facturación mundial y un 12% de la europea, España se posiciona como el cuarto mercado de ciberseguridad de Europa.

PAÍS	FACTURACIÓN	%TOTAL
Estados Unidos	60.565	26,8%
Europa	52.406	23,2%
Alemania	11.034	4,9%
Reino Unido	10.651	4,7%
Francia	6.680	3,0%
España	6.351	2,8%
MUNDO	225.972	100,0%

Facturación en millones de euros. Fuente Incibe.

La ciberseguridad se consolida como uno de los grandes motores del sector tecnológico en España con una facturación de 6.351 millones de euros, el 4,6% del sector TIC, que le posiciona como cuarto mercado europeo.

Según los datos del Estudio sobre la industria de la ciberseguridad en España 2025 elaborado por el Instituto Nacional de Ciberseguridad (Incibe), el sector de ciberseguridad cuenta con 3.431 empresas, el 4,5% de las compañías tecnológicas del país; genera casi 165.000 empleos, el 25,5% del sector TIC, y prevé crecer la ocupación a un ritmo del 14,3%/año hasta contabilizar con 282.000 empleados en 2029.

Desde Incibe constatan que la ciberseguridad “es ya uno de los sectores con más empuje de la economía digital española” con una creciente profesionalización y especialización, así como un papel cada vez más relevante en el ámbito de las TIC. En los últimos cinco años se han creado 403 empresas que concentran el 12% de la facturación

del sector, si bien se apoya en una base muy atomizada. De las 3.431 empresas, el 45% son microempresas, el 8% autónomos y el 5% son grandes compañías, aunque con una importante presencia en países como Portugal, Colombia, Alemania, Brasil y Chile.

Las empresas, a distintas velocidades

La ciberseguridad, sin embargo, afronta una coyuntura compleja. El Barómetro sobre el estado de la ciberseguridad en España elaborado por Secure&IT (LKS Next) constata que las empresas avanzan en su protección, pero a diferentes velocidades, viéndose influidas por la aceleración tecnológica, la

brecha del talento y la sofisticación de la ciberdelincuencia con un 26% más de incidentes. Según el estudio, el ransomware es la amenaza que más preocupa y la seguridad de los terminales (endpoint) la protección más extendida, con la ciberseguridad industrial al final de las prioridades frente a sectores como la sanidad, la energía o el transporte.

EL SECTOR REPRESENTA EL 4,5% DEL TOTAL DE LAS TICS



El estudio de Incibe parte de una encuesta a 517 empresas de la Confederación de Empresas TIC, Conetic.

LA RESILIENCIA INDUSTRIAL SE CONSTRUYE DE FORMA COMPARTIDA

La ciberseguridad industrial es ya un elemento clave de competitividad empresarial. Pero ya no se trata solo de proteger sistemas, sino de operar de forma segura y resiliente aún en escenarios de incertidumbre, fallo o ciberincidentes. Desde el Centro de Ciberseguridad Industrial (CCI) señalan que la estrategia de la industria debe evolucionar desde un enfoque único de protección

tecnológica hacia un modelo de ciberresiliencia operacional.

La ciberseguridad ya no es solo un problema técnico, sino un elemento estructural del negocio industrial, directamente relacionado con la continuidad operativa, la seguridad física, la cadena de suministro y la capacidad de decisión de las organizaciones.

Ante los retos de gobernanza de la ciberse-

guridad, conocimiento de entornos OT, menor dependencia crítica de terceros y mayor integración en procesos de digitalización desde el diseño, la resiliencia debe construirse de forma compartida entre operadores, fabricantes, integradores, proveedores tecnológicos e instituciones, donde la generación de capacidades sectoriales es tan importante como la propia tecnología.

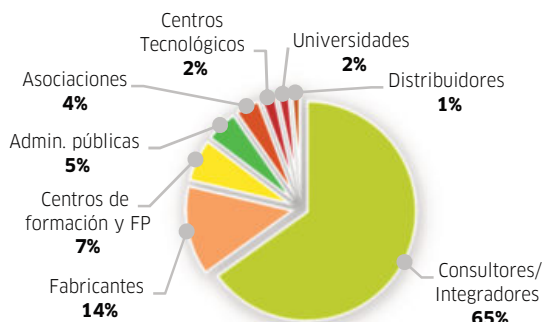
PAÍS VASCO | ECOSISTEMA

UNA RED EN EXPANSIÓN

EL ECOSISTEMA VASCO DE CIBERSEGURIDAD SE APOYA EN UNA BASE DE FABRICANTES QUE SE DIFERENCIA A TRAVÉS DE SOLUCIONES INNOVADORAS EN EL DESARROLLO DE ENTORNOS SEGUROS Y EL ANÁLISIS DE DATOS

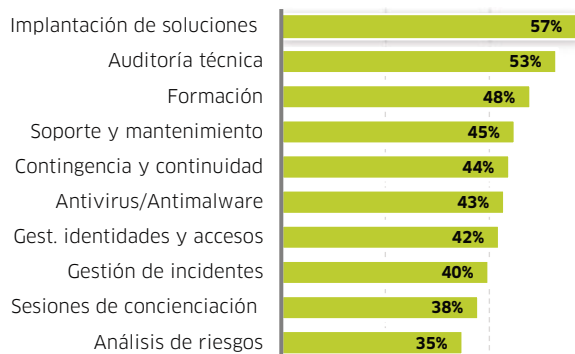
HETEROGÉNEO Y COMPLEMENTARIO

Los consultores/integradores componen, con 168 empresas, el grupo más numeroso entre los agentes del ecosistema vasco de ciberseguridad, seguidos de los fabricantes (35) y los centros de formación y FP (17).



TOP 10 PRODUCTOS Y SERVICIOS

La implantación de soluciones y las actividades de mantenimiento encabezan los servicios que desarrollan las empresas vascas del sector.



EVOLUCIÓN DEL ECOSISTEMA

El número de agentes ha ido creciendo de manera sostenida con un repunte entre 2016 y 2019, coincidiendo con la explosión de las operaciones online y la ciberdelincuencia.



Fuente: Grupo Spri.

El ecosistema vasco de ciberseguridad ha consolidado en los últimos años una estructura cada vez más diversa y complementaria, integrada por 258 agentes entre empresas, asociaciones, administraciones públicas, centros tecnológicos, universidades y entidades de formación.

Las empresas representan el núcleo principal del ecosistema, con 207 agentes que concentran el 80% del total. Predominan los consultores e integradores, que suponen el 81% del tejido empresarial, frente al 17% de fabricantes y un reducido 2% de distribuidores. La fisonomía empresarial evidencia la proliferación tanto de microempresas (45%) como de pymes (38%), mientras que las grandes compañías representan el 17%.

El sector incorpora también 59 startups y 14 EAPs (empresas innovadoras de alto crecimiento), configurando un tejido que evidencia el creciente peso de la ciberseguridad dentro de la transformación de la industria vasca.

En la base del entramado empresarial se sitúan los fabricantes, que desarrollan soluciones avanzadas en ciberseguridad como inteligencia de amenazas (CTI), Red privada Virtual (VPN) o rangos cibernéticos, que permiten a las compañías crear entornos de conexión seguros, simular campos de ciberbatalla u optimizar su protección a través del análisis de datos en tiempo real. Euskadi cuenta con un total de 35 fabricantes, que se reparten entre grandes empresas, como Panda, Grupo Igarle o SOC-E; pymes, startups y EAPs.

Mayoría de integradores

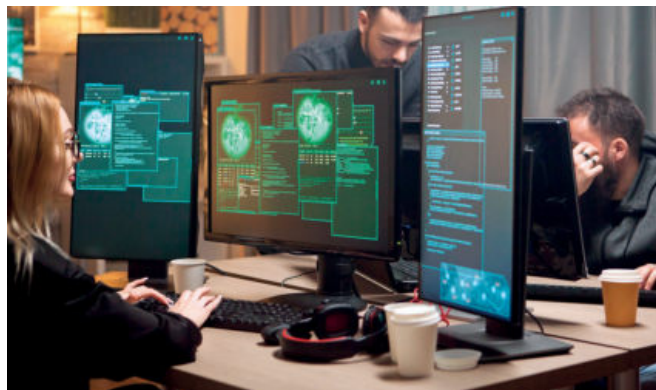
Los fabricantes encuentran eco en los consultores/integradores, que con 168 agentes constituyen un catálogo amplio de consultoras e ingenierías, encargadas de implementar las soluciones y desarrollar planes integrales tanto en pymes como en grandes operadores.

En cuanto a la oferta, en el ranking de los productos/servicios que más desarrollan las compañías vascas figuran la implantación de soluciones, auditoría técnica, formación, soporte y mantenimiento,

contingencia y continuidad y antivirus/antimalware.

El ecosistema ha crecido paulatinamente desde los primeros agentes surgidos en los años 70, década en la que apenas había una decena de empresas. Esta evolución ha contribuido a afianzar a Euskadi como polo de ciberseguridad con 79 empresas por millón de habitantes.

Con el fin de fomentar la colaboración en el sector, en 2020 se creó Cybasque, Asociación de Industrias de Ciberseguridad de Euskadi, impulsada por el Gobierno vasco, Spri y empresas del sector ICTA-GAIA, con 68 empresas asociadas.



El sector de la ciberseguridad ha crecido de manera exponencial.

EUSKADI EN LA DIANA

El ransomware registró un fuerte crecimiento en 2025 en Euskadi, con 35 ataques, un 40% más que el año anterior. Según los datos de Cyberzaintza, se concentraron en manufactura, retail y sector público. La explotación se focalizó en software de backup, transferencia de archivos y gestión remota, a través de exposiciones y vulnerabilidades comunes (CVEs) críticas de 2023-2025 como vectores principales. En ese sentido, las vulnerabilidades críticas y altas prácticamente se duplicaron, pasando del 24 al 48%. En cuanto a los ataques, creció su capacidad de desarrollo de exploits y la velocidad de explotación.



Cyberzaintza, fortaleciendo la ciberseguridad en Euskadi

La Agencia Vasca de Ciberseguridad-Cyberzaintza es un organismo público, adscrito al Departamento de Seguridad del Gobierno Vasco, creado para combatir, de una manera integral y transversal, las amenazas derivadas del uso de internet y las nuevas tecnologías en Euskadi. Alineado con la Estrategia de Ciberseguridad de Euskadi, el ámbito de actuación de los servicios de Cyberzaintza abarca la Prevención (evitar posibles incidentes de seguridad antes de que ocurran), Detección (identificación temprana de incidentes de ciberseguridad), Respuesta (servicios necesarios una vez se ha detectado un incidente de seguridad) y Gobernanza (establece las directrices y estructuras necesarias para gestionar la ciberseguridad de forma integral).

“Nuestro objetivo es promover y coordinar la ciberseguridad en el sector público vasco e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Administración pública, la ciudadanía y las empresas. Nues-

Cyberzaintza impulsa los planes de continuidad en materia de ciberseguridad frente a las emergencias informáticas

La Agencia Vasca de Ciberseguridad anima al 80% de empresas que aún tiene pendiente incorporarlos a sus planes de autoprotección “a ponerlos en marcha”

En una sociedad cada vez más conectada, los ciberincidentes constituyen una nueva amenaza en el ámbito de la seguridad ciudadana y las emergencias. Dentro del conjunto de empresas a las que, por su desempeño de actividades delicadas o potencialmente peligrosas, se les exige contar con planes de autoprotección ante emergencias, hay un grupo de compañías que tienen también la obligación de incorporar planes de continuidad en materia de ciberseguridad por la potencial afectación que tiene este ámbito en su funcionamiento. Se trata de las pertenecientes a los sectores de industria, energía, transporte, alimentación, agua, sanidad y finanzas, entre otros.

Las empresas sujetas a esta obligación deben cumplimentar un formulario orientado a recoger los principales aspectos de su plan de ciberseguridad y enviarlo, a través del registro electrónico general del Gobierno Vasco, a la Agencia Vasca de Ciberseguridad-Cyberzaintza, según la Orden del 7 de junio de 2024 del Consejero de Seguridad, que regula la elaboración de estos planes.

A punto de cumplirse el plazo máximo establecido en la Orden para realizar el trámite, coinciden-

do con la actualización cada dos años de los planes de autoprotección, Cyberzaintza advierte de que sólo un 20% de las empresas lo han cumplimentado. En ese sentido, anima a las compañías a ponerlo en marcha, “ya que, además de constituir una obligación, va a redundar en su propio beneficio”, indica Joseba Enjuto, director del Área de Auditoría y Gobierno del Riesgo de Cyberzaintza. “Los planes de continuidad preparan a las empresas para que, en caso de que un ciberincidente provoque un problema operativo que afecte a su producción, puedan continuar funcionando y evitar que ese problema se convierta en una emergencia”.

Guía para elaborar el plan

La Agencia Vasca de Ciberseguridad ha publicado en su web una ‘Guía de apoyo para la elaboración de un Plan de Continuidad en materia de Ciberseguridad’, orientada a facilitar a las empresas su desarrollo. “Básicamente cuenta con tres partes principales. En primer lugar, se trata de hacer una reflexión sobre cuáles son los sistemas informáticos importantes dentro de la organización e identificar, dentro de ellos, los críticos. A partir de ahí, es necesario elaborar un plan de reac-

ción ante una eventual parada de los sistemas. Finalmente, se ha de contar con un plan de recuperación, que establezca cómo volver a recuperar la actividad”, detalla el responsable. El plan también debe recoger actualizaciones periódicas y la realización de simulacros para ensayar su puesta en marcha. “Se trata de trasladar al mundo de la informática esa concienciación en torno a los protocolos de seguridad y los simulacros que hemos desarrollado el ámbito de las emergencias”, indica.

Una vez elaborado el plan, hay que cumplimentar y enviar a Cyberzaintza un formulario sobre sus características, que se puede descargar en su web. En relación con su condición de parte del mecanismo de reacción ante una emergencia de ciberseguridad, Cyberzaintza se vale de este formulario para ayudar a las empresas a resolver el problema. “Nos proporciona información crucial, como las personas de contacto en ese ámbito y las medidas de ciberseguridad con las que cuenta la empresa para resolver la contingencia”.



tra principal propuesta de valor es el desarrollo de medidas y acciones que fortalezcan la ciberseguridad en Euskadi”, detallan sus responsables.



PAÍS VASCO | PROGRAMA

LAS AYUDAS CRECEN EL TRIPLE

EL GRUPO SPRI DESTINARÁ ESTE AÑO 14 MILLONES DE EUROS A APOYAR LOS PROYECTOS DE CIBERSEGURIDAD DE LAS INDUSTRIAS VASCAS PARA AUMENTAR SU RESILIENCIA

El aumento de la conectividad de la industria a raíz de la incorporación de sistemas autónomos para la automatización de tareas y de la convergencia de los sistemas IT y OT para mejorar la eficiencia del proceso productivo ha multiplicado la vulnerabilidad de las empresas frente a los ciberataques. Para minimizar su exposición, el Gobierno vasco, a través del Grupo Spri, ha triplicado este año los recursos del programa de ayudas que puso en marcha en 2018 para mejorar el nivel de ciberseguridad de las empresas. Desde su lanzamiento hasta la actualidad, suma casi 3.000 actuaciones apoyadas, de un total de 2.300 compañías. Con una subvención media de 8.400 euros, los desarrollos respaldados han supuesto en total más de 60 millones de inversión privada.

El programa de ayudas de Ciberseguridad Industrial ha crecido en paralelo a las necesidades de protección de las empresas, pasando de en torno a un centenar de proyectos apoyados el primer año a los 555 del ejercicio pasado. El punto de inflexión se produjo en la pandemia, cuando el acceso remoto a los servidores de las compañías por efecto del teletrabajo y el despliegue de infraestructuras de comunicación en tiempo récord abrió una brecha en la ciberseguridad.

Ese aumento de la vulnerabilidad y de la participación empresarial en el programa ha venido acompañado de un fuerte refuerzo presupuestario. La dotación anual alcanzará este año los 14 millones de euros, más del triple que en 2025 y catorce veces superior a la de la primera convocatoria, que contó con un millón. Además, se ha elevado del 50% al 60% el porcentaje subvencionable del presupuesto global de los proyectos, con un máximo de 100.000 euros por empresa y año. La ayuda se calcula a partir de los gastos aprobados en consultoría e ingeniería, así como de las inversiones destinadas a hardware y software.

Del análisis de los proyectos aprobados

a lo largo del programa se pueden extraer conclusiones relativas a los sectores y las empresas que están invirtiendo en optimizar su ciberseguridad y a la tipología de los proyectos que están llevando a cabo.

En relación a los sectores, el 59% de los proyectos se enmarcan en la industria manufacturera. Figuran, a continuación, sectores como el de actividades profesionales científicas o técnicas, comercio al por mayor y al por menor, información y comunicación, construcción, y transporte y almacenamiento, que sin ser exactamente industriales ofrecen servicios conexos a la industria ligados al producto-proceso industrial.

Los proyectos relativos a la industria manufacturera, por su parte, se concentran en su mayoría en los subsectores de productos metálicos y maquinaria y equipo n.c.o.p., que, en general, engloban empresas de mecanizado y de MH.

Pymes y guipuzconas

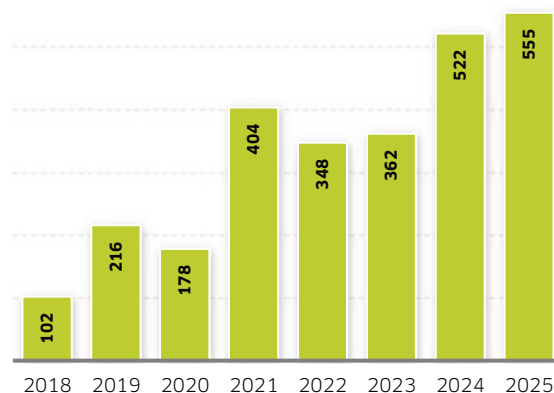
En relación a las empresas beneficiarias, las pymes concentran casi tres cuartas partes de los proyectos aprobados y casi el 50% promovidos por compañías guipuzcoanas.

Por tipología de proyectos, destacan los relativos al diseño y ejecución de nuevas arquitecturas de red para garantizar la segmentación entre entornos IT y OT; la monitorización de dispositivos de seguridad perimetral y de otros dispositivos industriales tales como *switches* o *firewalls*, entre otros, y la securización de los accesos remotos OT a los equipos industriales de la planta productiva requeridos para el mantenimiento de equipo, control y operación de los mismos. Por otra parte, uno de cada cinco proyectos aprobados están relacionados con la adopción de buenas prácticas y procesos de certificación dirigidos a la obtención y cumplimiento de normas de ciberseguridad industrial, en línea con la creciente presión regulatoria y los controles en forma de requisitos que están imponiendo determinados clientes a sus proveedores en sectores como automoción, aeronáutica o la propia administración pública.

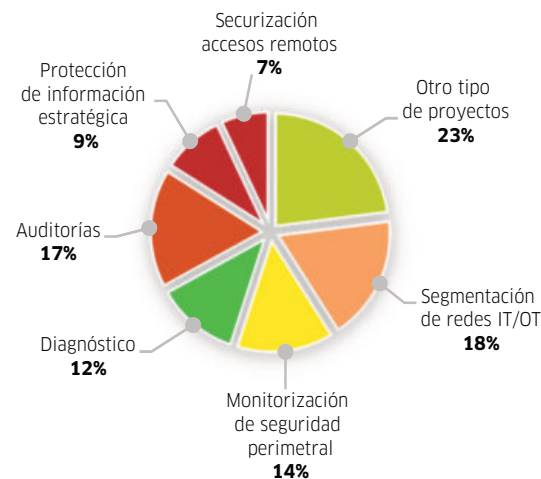
UN PROGRAMA CADA VEZ MÁS GRANDE

Los proyectos apoyados por el programa de Ciberseguridad Industrial del Grupo Spri se han multiplicado por cinco en sus nueve convocatorias.

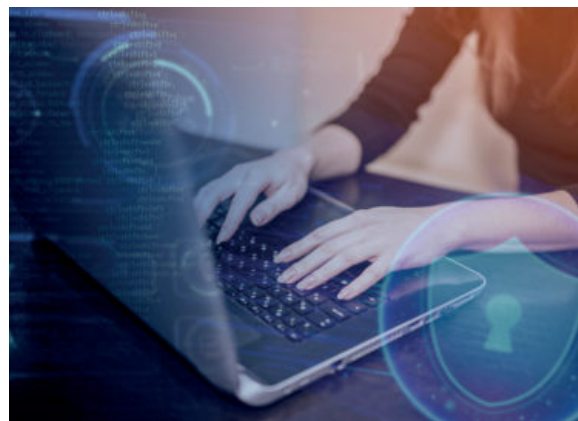
PROYECTOS APROBADOS POR CONVOCATORIA



TIPOLOGÍA DE PROYECTOS



Fuente: Grupo Spri.



La segmentación de las redes IT/OT es uno de los desarrollos más extendidos.

PROYECTOS | ESPACIOS DE DATOS

HACIA LA SOBERANÍA DIGITAL

EUSKADI AVANZA COMO REFERENTE EN ESPACIOS DE DATOS CON LOS PROYECTOS BCSSD Y CIBERDATA

Los espacios de datos de ciberseguridad están llamados a desempeñar un papel decisivo en los próximos años. La capacidad de intercambiar datos de forma segura y detectar riesgos antes de que se materialicen se perfila como uno de los grandes pilares de la futura ciberresiliencia industrial europea. Un ámbito en el que Euskadi ya ha comenzado a tomar posiciones con el desarrollo de infraestructuras propias como Baidata y el Espacio de Datos BCSSD.

Liderado por la empresa Perseus Ciberseguridad, junto a una decena de empresas vascas y el Clúster Gaia, el proyecto BCSSD ha supuesto la consolidación del primer espacio de datos de ciberseguridad industrial desarrollado en el País Vasco. Se trata de un espacio de datos descentralizado, confiable y seguro, en el que organizaciones del ecosistema industrial vasco compartan datos de ciberseguridad.

BCSSD HA TRAZADO UN ESPACIO DE DATOS SEGURO

Para su configuración, el consorcio se ha apoyado en la investigación de tecnologías, estándares y modelos de datos que faciliten el intercambio seguro y útil de información relacionada con amenazas IT y OT en entornos industriales. De este modo, BCSSD deja a la CAPV en una posición de ventaja de cara a los próximos pasos a dar en este ámbito, ya que además de aportar una arquitectura completa y operativa, brinda a las empresas un modelo de colaboración avanzada,

servicios de ciberinteligencia y un ecosistema tecnológico que puede servir de base para futuros espacios de datos en el ámbito de la ciberseguridad.

Ciberdata: centro demostrador

Dentro de esta apuesta por reforzar las capacidades digitales industriales, Gaia impulsa también Ciberdata, un centro demostrador de espacios de datos especializado en ciberseguridad.



Los espacios de datos jugarán un papel decisivo en la ciberseguridad.

dad, financiado por el Ministerio para la Transformación Digital y de la Función Pública. Su misión pasa por aprovechar el enorme volumen de información que genera el ámbito de la ciberseguridad para anticipar amenazas, mejorar la prevención de incidentes y reforzar la resiliencia digital de las organizaciones.

Alineado con los objetivos nacionales y europeos de soberanía digital y compartición segura de datos estratégicos, el centro demostrador de colaboración público-privada permite a empresas y organizaciones probar tecnologías y desarrollar casos de uso sobre infraestructuras basadas en estándares europeos como GAIA-X o IDS sin necesidad de desplegar plataformas propias.

Desde el pasado abril, Ciberdata ofrece acceso a infraestructuras y entornos de intercambio seguro de datos, así como servicios de consultoría, marketplaces de herramientas y programas de formación y certificación orientados al desarrollo de talento.

% 100 URA GARA SOMOS 100% AGUA

*Bizkaia etorkizunera egokituta zainduz, inbertituz eta mantenduz.
Cuidando, invirtiendo y manteniendo una Bizkaia adaptada al futuro.*



Bilbao Bizkaia Ur Partzuergoa
Consorcio de Aguas Bilbao Bizkaia
www.consorciodeaguas.eus





El proyecto Abedi aspira a transformar la forma en la que las empresas prueban y protegen sus sistemas industriales.

PROYECTO | SISTEMAS EMBEBIDOS

LA CIBERSEGURIDAD INDUSTRIAL QUE VIENE

UN CONSORCIO VASCO LIDERADO POR ORBIK CYBERSECURITY INVESTIGA UN NUEVO PARADIGMA PARA PROTEGER EQUIPOS INDUSTRIALES CON SOFTWARE EMBEBIDO

La creciente digitalización de la industria y el aumento exponencial de los ciberataques contra sus empresas e infraestructuras críticas están incrementando la presión sobre fabricantes y operadores de sistemas con software embebido, encargado de controlar procesos esenciales como líneas de producción, sistemas de señalización o mecanismos de seguridad industrial. Este escenario de amenazas, cada vez más complejo, está acelerando la necesidad de desarrollar nuevas tecnologías y capacidades de protección avanzada para entornos industriales, un desafío que abordará el proyecto Abedi durante los dos próximos años, anticipándose a la plena entrada en vigor del Reglamento Europeo CRA (Cyber Resilience Act) en 2027, momento en los fabricantes

estarán obligados a garantizar nuevos estándares de ciberseguridad.

Liderado por la empresa Orbik Cybersecurity, Abedi aspira a transformar la forma en que las empresas prueban, protegen y actualizan sus sistemas industriales mediante el desarrollo de una solución innovadora capaz de reforzar la respuesta frente a nuevas amenazas digitales de una forma más rápida, precisa y eficiente. Para ello, cuenta con un consorcio multidisciplinar que aporta capacidades complementarias para el desarrollo y validación de las tecnologías a investigar con la participación de CAF Signalling, Fagor Automation, Mondragon Assembly y Ormazabal como empresas tractoras. A ellas se suman, desde la Red Vasca de Ciencia, Tecnología e Innovación (RVCTI),

el Clúster Gaia, la Asociación de Industrias de Conocimiento y Tecnología de Euskadi, Ikerlan y Koniker. La colaboración entre todos estos agentes permitirá combinar experiencia industrial, capacidades tecnológicas y conocimiento científico para desarrollar soluciones de alto impacto para la industria vasca.

Protección avanzada

Orbik Cybersecurity desempeñará un papel clave en la definición y desarrollo de las principales líneas de investigación y actuación del proyecto, centradas en un nuevo paradigma de protección avanzada para sistemas industriales con software embebido. Para su concepción, investigará un novedoso sistema basado en entornos virtualizados de alta fidelidad para la simulación y validación re-

METAS PARA 2027

Disponibilidad del 99% en sistemas industriales gracias a diseños ciberseguros y actualizaciones seguras OTA.

Reducción del 80% del tiempo de respuesta ante incidentes de ciberseguridad.

Disminución del 70% de la intervención manual en la gestión de seguridad.

Eliminación del transporte físico de equipos, sustituidos por un laboratorio virtualizado de alta fidelidad.

Reducción del 50% de costes y tiempos en certificaciones, garantizando conformidad total con la normativa europea CRA.

mota de sistemas industriales capaces de replicar hasta el 95% de la operativa real. A la vez se desarrollarán mecanismos avanzados de ciberseguridad para la detección, prevención y respuesta ante amenazas digitales en entornos industriales, además de estudiar sistemas de actualización remota OTA (Over The Air) que permitan la evolución continua y segura del software y firmware sin interrumpir la actividad industrial.

Tecnologías clave

Como tecnologías prioritarias, en el proyecto se aplicará inteligencia artificial, big data, ciencia de datos, sistemas ciberfísicos y virtualización avanzada para automatizar procesos de análisis, monitorización y protección.

El papel de CAF Signalling, Fagor Automation, Mondragon Assembly y Ormazabal en Abedi se centrará en aportar casos de uso reales, conocimiento industrial y entornos de validación en sectores críticos. Y en el caso de las entidades de la RVCTI, sus roles estarán ligados a actividades de investigación aplicada, desarrollo tecnológico, validación de soluciones y transferencia de conocimiento.

UN SISTEMA DE SIMULACIÓN REPLICARÁ EL 95% DE LA OPERATIVA REAL

ENCUESTA | PROVEEDORES

UN ELEMENTO ESTRATÉGICO

LA IA, LA REGULACIÓN Y EL AUMENTO DE AMENAZAS ACELERAN LA INTEGRACIÓN DE LA CIBERSEGURIDAD

En un contexto marcado por el aumento y la sofisticación de los ciberataques, la presión regulatoria y las crecientes exigencias de seguridad de los fabricantes a toda su cadena de suministro, la ciberseguridad se ha convertido en un factor estratégico en la actividad de las empresas. Lo que hasta hace pocos años se percibía como una opción se ha convertido en un requisito ligado al propio diseño, fabricación y mantenimiento de los productos. Como señalan los responsables de Orbik Cybersecurity, Alias Robotics, Ayesa Digital y LKS Next, la industria evoluciona hacia modelos de protección continua en los que la ciberseguridad ya no solo es una cuestión tecnológica, sino también de competitividad y resiliencia.

► ¿Qué empresas están liderando la implantación de ciberseguridad?

Odei Olalde

CTO de Orbik Cybersecurity

Es verdad que tal y como es de esperar, las grandes empresas con presupuestos desorbitados tienen capacidades que otras empresas no tienen, y eso les convierte en referentes en innovación. No obstante, estamos viendo un crecimiento en las inversiones en innovación centrada en la ciberseguridad en el entramado de empresas industriales vascas que las posiciona muy por delante de los competidores. La industria ha tenido mucha relevancia en el País Vasco y eso se ha debido a la implicación e interés de las empresas que aquí se han formado en crear productos líderes en el mercado.

Endika Gil-Uriarte

CEO de Alias Robotics

Las empresas que operan infraestructuras críticas, entornos OT (Tecnología de las Operaciones) y sistemas ciber físicos complejos, como la robótica industrial y de servicios, están liderando esta necesidad de implantación. Estas organizaciones están incorporando IA y automatización para la ciberseguridad, ya que los enfoques tradicionales de auditoría manual no escalan. Además, muchas organizaciones industriales están evolucionando desde modelos de auditoría puntual hacia estrategias de validación y monitorización continua, impulsadas tanto por el aumento de las amenazas como por las nuevas exigencias regulatorias.

Álvaro Fraile

Director de Ciberseguridad de Ayesa Digital

Tradicionalmente, en la industria la prioridad absoluta siempre ha sido la continuidad operativa. Producción, calidad y eficiencia han marcado históricamente las decisiones tecnológicas. Sin embargo, la ciberseguridad está dejando de ser una variable secundaria porque hoy afecta directamente a esos tres elementos. Cada vez más compañías entienden que la ciberseguridad no compite con producción o costes, sino que protege precisamente la capacidad de producir. La tendencia actual es integrar la seguridad desde el diseño industrial y considerar el riesgo cibernético como un riesgo empresarial estratégico. Aun así, todavía existe una importante diferencia entre grandes corporaciones y pymes industriales. Mientras las grandes organizaciones ya manejan modelos maduros de gestión del riesgo, muchas empresas medianas siguen teniendo dificultades presupuestarias y de especialización.

Hugo Llanos

Director de Ciberseguridad Industrial (OT) de LKS Next

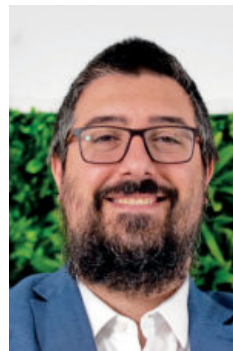
Aunque las grandes empresas están liderando actualmente la implantación de soluciones avanzadas de ciberseguridad, también se observa un importante crecimiento en la puesta en marcha de proyectos de ciberseguridad en pequeñas y medianas empresas, bien como respuesta al miedo de ser objetivo de un ataque o bien como necesidad debido a exigencias de terceros, dado que forman parte de cadenas de suministro.

Entre las tecnologías más implantadas en los entornos IT, seguimos avanzando con el despliegue de soluciones EDR/XDR, la incorporación de servicios de gestión y monitorización continua 24x7 (SOC) y soluciones de Zero Trust basadas en SASE, para dar respuesta a la protección de una compleja realidad de conectividad de los usuarios a servicios corporativos.

En el entorno OT el ritmo es más lento, aunque la segmentación y securización de redes industriales, mediante soluciones de protección adecuadas para estos entornos, sigue siendo lo más demandado. A continuación, estaría el despliegue de soluciones de monitorización “este-oeste” de la actividad

Odei Olalde

CTO de Orbik Cybersecurity



“LA INDUSTRIA VASCA ESTÁ INNOVANDO EN SEGURIDAD”

Endika Gil-Uriarte

CEO de Alias Robotics



“LA IA PERMITE REDUCIR EL TIEMPO DE RESPUESTA”

maliciosa que se produce en las propias redes.

► ¿Qué factores dificultan la adopción de este tipo de soluciones?

Odei Olalde

Las mayores barreras que vemos tienen que ver con la rentabilidad. El mercado OT se caracteriza por los requisitos funcionales y de seguridad de las personas, pero no por su ciberseguridad. Una inversión en esto no trae un retorno asociado tan claro como el que puede tener alguna funcionalidad o la optimización de ciertos procesos. Aún así, cada vez es más común ver cómo los clientes solicitan seguridad en sus productos y esto al final está repercutiendo en fabricantes y en las inversiones que están realizando. Esto y las nuevas regulaciones como la CRA son las principales causas de que se haya impulsado la ciberseguridad de forma global.

Endika Gil-Uriarte

Las principales barreras a las que se enfrentan son tres: la velocidad y sofisticación creciente de las amenazas, que obliga a operar prácticamente en tiempo real; el coste y la complejidad operativa del modelo tradicional, especialmente en entornos industriales donde las evaluaciones pueden afectar a la continuidad de la producción; y la escasez de expertos. Existe un déficit global de profesionales que entiendan tanto de protocolos industriales como de ciberataques.

Álvaro Fraile

El gran desafío no es únicamente tecnológico, sino cultural y estratégico. Muchas organizaciones industriales todavía continúan viendo la ciberseguridad como un coste o como una responsabilidad exclusiva del área IT, cuando en realidad se ha convertido en un elemento crítico de continuidad de negocio. En sectores industriales, un incidente ya no solo implica pérdida de datos. Puede detener líneas de producción, afectar a la seguridad física o comprometer cadenas de suministro completas. La buena noticia es que cada vez existe una mayor conciencia. El ecosistema vasco está acelerando inversiones en SOC, protección OT, monitorización industrial y modelos Zero

ENCUESTA | PROVEEDORES

(viene de la página XI)

Trust. Pero todavía queda recorrido en capacidades avanzadas de detección, resiliencia y preparación frente a amenazas impulsadas por IA.

Hugo Llanos

Las principales barreras siguen siendo la falta de recursos internos, la complejidad de integrar nuevas soluciones en entornos industriales 'legacy' y la dificultad de justificar inversiones preventivas en organizaciones que todavía perciben la ciberseguridad como un coste y no como un elemento estratégico de negocio. A esto se suma el aumento de requisitos regulatorios y la necesidad de garantizar la continuidad operativa en entornos donde cualquier parada tiene un impacto económico muy elevado.

► ¿Cómo está impactando la IA en la ciberseguridad?**Odei Olalde**

El uso de la IA es algo que ya tenemos normalizado a día de hoy. No es novedad ver cómo se utiliza en ambos bandos y es verdad que ha afectado bastante a la forma en la que tenemos que tratar la ciberseguridad. Por una parte, los ataques son más sofisticados, se encuentran vulnerabilidades y se explotan a unas velocidades que difícilmente pueden ser frenadas y la capacidad que puede tener un atacante depende de su capacidad computacional. Esto es verdad que funciona a la inversa, es decir, las vulnerabilidades se detectan antes, las herramientas cada vez son más sofisticadas y los productos y despliegues más resilientes.

Esto sobre todo ha afectado a la velocidad en la que se trabaja y se esperan resultados, lo que buscamos ahora son flujos optimizados que garanticen que los sistemas están seguros y sean resistentes a los ataques dirigidos que puedan llegar a cabo las propias inteligencias artificiales, de modo que al final han entrado como un arma de doble filo.

Endika Gil-Uriarte

El panorama ha cambiado radicalmente. El cibercrimen y los actores de estados-nación ya utilizan la IA para automatizar ataques, haciéndolos más veloces, sofisticados y masivos. En nuestras investigaciones hemos demostrado cómo sistemas robóticos conectados pueden convertirse en vectores de ataque si no se diseñan con criterios de seguridad desde el origen.

Desde el punto de vista de la solución, la premisa es clara: los defensores también necesitan operar con capa-

idades automatizadas e impulsadas por IA para responder a amenazas que ya actúan a velocidad de máquina. Tecnologías como CAI (Cybersecurity AI) y nuestros modelos especializados (alias1 y alias2) actúan como defensores autónomos. La IA aplicada a ciberseguridad permite reducir drásticamente los tiempos de análisis, validación y respuesta, especialmente en entornos críticos donde la capacidad humana por sí sola ya no puede escalar al ritmo de las amenazas actuales.

Álvaro Fraile

La industria vasca parte de una posición relativamente madura en comparación con otros entornos industriales europeos, especialmente por su fuerte tradición tecnológica, automatización de procesos y cultura industrial. Sin embargo, la irrupción de la IA ha cambiado completamente las reglas del juego. Hoy ya no hablamos únicamente de malware tradicional o ataques oportunistas, sino de amenazas automatizadas, hiperpersonalizadas y capaces de adaptarse en tiempo real. La IA está siendo utilizada tanto por defensores como por atacantes. Los ciberdelincuentes pueden generar campañas de *phishing* prácticamente indistinguibles de una comunicación legítima, automatizar vulneraciones o incluso manipular sistemas industriales mediante técnicas avanzadas de ingeniería social y análisis predictivo.

Hugo Llanos

La IA ha cambiado radicalmente el escenario de la ciberseguridad porque ha elevado el nivel de sofisticación y escalabilidad de los ataques. Los ciberdelincuentes ya utilizan IA para automatizar campañas de *phishing*, que son mucho más difíciles de identificar por parte de los usuarios; dotar de mayor adaptabilidad al *malware* para mutar y dificultar su identificación, o la realizar ataques de ingeniería social altamente personalizados. Por otro lado, y considerando la capacidad de la IA de analizar y contextualizar grandes volúmenes de información, está permitiendo a los atacantes identificar los vectores de ataque más efectivos con mayor rapidez y precisión. Al mismo tiempo, la IA se ha convertido en una herramienta muy importante para la defensa. El nivel de implantación actual ya permite detectar anomalías en tiempo real, automatizar tareas de respuesta, reducir falsos positivos y anticipar comportamientos maliciosos antes de que se materialicen en incidentes y, por lo tanto, mitigar o reducir notablemente el impacto de un ciberincidente.

► ¿En qué aspectos pondrá el foco su**compañía en el presente ejercicio?****Odei Olalde**

Nuestros esfuerzos durante este año están enfocándose en dos frentes. Por una parte, estamos trabajando con las empresas en el cumplimiento de la parte más inmediata de la CRA, la gestión y monitorización de vulnerabilidades que entra en vigor en septiembre. La necesidad de cumplir con los requisitos está suponiendo un esfuerzo para poder alcanzar en fechas los objetivos que se especifican.

Por otra parte, estamos centrando el resto de nuestras capacidades en adelantarnos a los requisitos con la entrada en vigor completa en diciembre de 2027. Para ello estamos empezando a analizar productos de clientes y viendo su grado de cumplimiento en cada uno de los requisitos que se han establecido.

Endika Gil-Uriarte

En 2026, nuestro foco comercial estará en escalar internacionalmente, llevando nuestra tecnología a nuevas industrias y sectores críticos, y expandiendo nuestro equipo de desarrollo de negocio para convertir la tracción actual en alianzas estratégicas a gran escala. A nivel tecnológico, lideraremos la transición hacia la 'Superinteligencia en Ciberseguridad'. Esto implica el despliegue de nuestros modelos alias2 y alias2-mini para defensa en local (on-premise) en infraestructuras críticas (testado y validado con éxito en ejercicios como Locked Shields 2026 de la OTAN). Y por último, continuaremos liderando la investigación y protección contra las vulnerabilidades críticas emergentes.

Álvaro Fraile

En 2026 veremos una clara evolución hacia modelos de ciberseguridad mucho más automatizados, inteligentes y orientados al negocio. El foco estará especialmente en cuatro grandes áreas. La primera será la protección de entornos OT e industriales, donde todavía existen grandes desafíos relacionados con sistemas *legacy* y convergencia IT/OT. La segunda será la aplicación de inteligencia artificial defensiva. Las organizaciones buscarán automatizar la detección, priorización y respuesta ante incidentes para reducir tiempos de reacción y compensar la escasez de talento. La tercera gran prioridad será el cumplimiento regulatorio. Normativas como NIS2, DORA o CRA obligarán a elevar significativamente los niveles de resiliencia y gobierno de la ciberseguridad. Y, finalmente, veremos una fuerte apuesta por modelos de soberanía digital y servicios gestionados euro-

ÁLVARO FRAILE

Dir. Ciberseguridad de
Ayesa Digital



**“LA TENDENCIA
ES INTEGRAR
LA SEGURIDAD
EN EL DISEÑO”**

peos, especialmente en sectores críticos donde la dependencia tecnológica se ha convertido en una preocupación estratégica.

Hugo Llanos

En 2026, el foco de Secure&IT está centrado en ayudar a las empresas a reforzar su ciberresiliencia, en un contexto marcado por el uso de la IA para fines maliciosos, el aumento de amenazas cada vez más sofisticadas, la presión regulatoria y la creciente digitalización de los entornos industriales. Estamos haciendo hincapié en la protección de entornos OT e infraestructuras críticas, la securización de la cadena de suministro y la mejora de las capacidades de detección y respuesta ante incidentes mediante la mejora de nuestros servicios avanzados de seguridad. Estamos trabajando intensamente en la integración de tecnologías basadas en IA para mejorar las capacidades defensivas, tanto en la identificación temprana, como en la protección y respuesta.

► ¿Están las empresas vascas preparadas para la entrada en vigor de la Ley de Ciberresiliencia (CRA)?

Odei Olalde

La respuesta a esta pregunta tiene contra-pregunta. ¿Está la CRA suficientemente clara como para que pueda ser cumplida? La verdad es que hay grises y cosas que no quedan del todo claras, aunque es verdad que poco a poco se están aclarando. El problema es que para las empresas invertir en cambios que no están claros no es una opción, cosa que hace que estas medidas tarden tanto en ser implementadas. Incluso la parte de monitorización tiene una norma que sigue estando en estado de corrección, estamos hablando de los requisitos específicos que debería cumplirse en septiembre de este mismo año. Volviendo al hilo, creo que las empresas están vigilando de cerca la norma y vemos una iniciativa muy marcada en alinearse a los requisitos, aunque quizás no al ritmo que se necesitaría para evitar los problemas de los tiempos ajustados. La inclusión de ciberseguridad en los productos industriales lo vemos como un factor diferenciador y competitivo en el mercado y estas regulaciones están acelerando estos procesos de hacer que nuestros fabricantes comprendan que la ciberseguridad puede llegar a tener una relevancia casi tan valorada como las propias funcionalidades.

Endika Gil-Uriarte

El tejido industrial, tanto a nivel vasco como europeo, se encuentra en plena carrera de adaptación. Normativas como la CRA, sumadas a la directiva NIS2 y el GDPR, suponen un cambio de pa-

radigma: la ciberseguridad se ha convertido en un requisito legal de 'seguridad por diseño' y soberanía del dato. Para el sector industrial, que cada vez integra más robótica y sistemas OT conectados, el impacto es inmenso. Los fabricantes y operadores industriales estarán obligados a garantizar que sus máquinas no son vectores de ataque ni de espionaje. La adaptación exige tecnologías que operen con una arquitectura centrada en la privacidad y la soberanía del dato, de forma que la información sensible jamás salga del perímetro industrial.

Álvaro Fraile

Existe una creciente preocupación y movimiento de adaptación, pero la realidad es que muchas organizaciones todavía están en fases iniciales de preparación. La Cyber Resilience Act supondrá un cambio profundo porque trasladará requisitos de ciberseguridad directamente al diseño, fabricación y mantenimiento de productos digitales e industriales. Ya no bastará con reaccionar ante incidentes: la seguridad deberá incorporarse desde el origen. Esto implicará nuevas exigencias en gestión de vulnerabilidades, actualización de software, trazabilidad, certificación y responsabilidad sobre productos conectados. Las grandes empresas industriales están avanzando más rápido porque ya disponen de equipos especializados y estrategias de *compliance* consolidadas. Sin embargo, muchas pymes todavía desconocen el impacto real que tendrá esta normativa sobre su operativa y su cadena de suministro.

Hugo Llanos

El impacto regulatorio será muy relevante para los fabricantes e integradores de productos, ya que la ciberseguridad pasa de ser un elemento opcional para convertirse en un requisito de diseño y cumplimiento. Esto obligará a fabricantes y proveedores industriales a incorporar la seguridad como un requisito más, lo que permitirá elevar los estándares de protección a toda la cadena de suministro. A medio plazo, esta también supondrá una oportunidad para aumentar la competitividad y confianza del sector industrial europeo.

► ¿Hasta qué punto limita la falta de talento la ciberseguridad industrial?

Odei Olalde

El del talento es un tema recurrente, y creo que el problema no es tanto del talento, sino de las expectativas que tenemos al contratar personas. Hay una creencia errónea de que una persona válida puede entrar y solucionar todos los problemas desde el principio. Esto no es así. Una persona puede alcanzar su potencial si se le guía y le apoya du-

rante su formación, si de verdad se hace un esfuerzo para formarlo. En mi experiencia en Orbik puedo afirmar que talento no nos falta, hemos ido formando e incluyendo en plantilla a gente que tenía recién terminados los estudios y nos hemos llevado más de una grata sorpresa con la iniciativa y lo que pueden llegar a aportar cuando se les da una oportunidad real. Así que creo que deberíamos dejar de esperar que nos solucionen los problemas y enseñarles a pensar cómo hacerlo, así es como generamos talento.

Endika Gil-Uriarte

La está limitando críticamente. Nos enfrentamos a una crisis global con casi 5 millones de puestos de ciberseguridad sin cubrir. En el ámbito industrial y robótico, esta brecha es aún más aguda porque requiere perfiles altamente especializados que entiendan la convergencia entre el mundo físico (OT/Robótica) y el digital (IT). Ningún equipo humano puede escalar lo suficiente para proteger los millones de dispositivos conectados en las infraestructuras actuales. Por ello, nuestra propuesta de valor con CAI es actuar como un 'multiplicador de talento'. Al automatizar las tareas más repetitivas, permitimos que los profesionales no expertos logren resultados de élite y que los pocos expertos disponibles se centren en la estrategia, democratizando así la ciberseguridad.

Álvaro Fraile

La escasez de talento es actualmente uno de los mayores riesgos para la ciberseguridad industrial. No solo faltan especialistas en seguridad, sino perfiles híbridos capaces de comprender simultáneamente entornos IT, OT e industriales. La protección de infraestructuras industriales requiere conocimientos muy específicos: protocolos industriales, automatización, sistemas SCADA, redes OT y operación de planta. Encontrar profesionales con esa combinación de experiencia es extremadamente complejo. Esta situación está provocando que muchas organizaciones dependan cada vez más de servicios gestionados, SOC's externos y automatización mediante IA.

Hugo Llanos

Considerando que existe una demanda creciente de perfiles profesionales capaces de gestionar la ciberseguridad, tanto de los entornos IT como OT, la oferta de profesionales con experiencia en ambos ámbitos sigue siendo insuficiente, lo que hace que muchas empresas industriales se encuentren con muy pocas capacidades de contratación de especialistas. Esto ralentiza notablemente la puesta en marcha de proyectos en el ámbito industrial.

HUGO LLANOS
Dir. Ciberseguridad Industrial LKS Next



"LA NUEVA LEY APORTARÁ PROTECCIÓN Y COMPETENCIA"



TECNOLOGÍA | TRANSPORTE

RUMBO A UN TRANSPORTE MARÍTIMO CIBERSEGURO

TECNALIA PARTICIPA EN EL PROYECTO EUROPEO WARRANT PARA REFORZAR LA PROTECCIÓN DE LOS SISTEMAS DIGITALES E INTELIGENTES EMBARCADOS MEDIANTE NUEVAS METODOLOGÍAS

El transporte marítimo, que mueve cerca del 90% del comercio mundial, se ha convertido en uno de los grandes desafíos tecnológicos y de seguridad de la nueva economía digital. La creciente dependencia de sistemas digitales, inteligencia artificial y tecnologías autónomas a bordo expone a los barcos a fallos de software y ciberataques capaces de comprometer la navegación y la seguridad marítima.

Para reducir su exposición a amenazas, TecNALIA participa en el proyecto europeo Warrant. El objetivo es impulsar el desarrollo de soluciones que garanticen operaciones marítimas más seguras, fiables y resilientes en un sector cada vez más digitalizado, avanzando hacia una nueva generación de transporte marítimo inteligente, autónomo y ciberseguro.

Con esa meta, el proyecto reúne desde el pasado abril a

doce entidades de ocho países para desarrollar una metodología común y una plataforma digital destinadas a reforzar la seguridad y la gestión de los sistemas embarcados durante todo su ciclo de vida. El principal valor añadido de Warrant reside en combinar seguridad operativa, ciberseguridad y resiliencia digital en una misma arquitectura tecnológica. Frente a otros enfoques centrados únicamente en automatizar o monitorizar procesos, la iniciativa incorpora

SIMULARÁ ATAQUES SOBRE SISTEMAS DE IA

herramientas avanzadas de simulación de riesgos capaces de anticipar fallos y vulnerabilidades antes de que se produzcan.

Si bien el proyecto se encuentra en fase de desarrollo, con vistas a finalizar en diciembre de 2027, ya han identificado beneficios potenciales, ya que una detección temprana de vulnerabilidades permite reducir incidentes de ciberseguri-

dad, disminuir costes operativos, evitar paradas no planificadas y mejorar la continuidad del negocio. También facilita la anticipación de fallos y la identificación de vulnerabilidades antes de que se conviertan en incidentes al proporcionar una mayor visibilidad sobre el estado de los sistemas y favoreciendo una toma de decisiones más informada. Asimismo, permite evaluar los modelos de inteligencia artificial antes de su despliegue, identificando debilidades en materia de ciberseguridad y aplicando medidas preventivas de forma temprana.

Rol de TecNALIA

TecNALIA participa en el proyecto Warrant como socio tecnológico especializado en ciberseguridad, aportando su experiencia en el desarrollo de soluciones avanzadas para la protección de sistemas digitales marítimos. Su actividad se centra en dos grandes objetivos: por un lado, la validación y mejora de la resiliencia de los sis-

temas de inteligencia artificial utilizados a bordo de los buques, contribuyendo así a garantizar su fiabilidad en entornos operativos complejos y expuestos a amenazas; y por otro, la mejora de la identificación de vulnerabilidades en los componentes de software embarcados, en toda la cadena de suministro, desde el fabricante, hasta su instalación final en un barco.

El centro tecnológico también tiene como objeto diseñar escenarios y herramientas para la simulación de ciberataques sobre sistemas de inteligencia artificial, como aquellos empleados en la detección de objetos, con el objetivo de evaluar su comportamiento frente a amenazas y reforzar su robustez y capacidad de respuesta.

Según avanzan desde TecNALIA, entre los primeros resultados previstos destacan nuevos enfoques para simular ataques a modelos de IA, especialmente en sistemas de detección de objetivos, con potencial de aplicación en otros sectores.

TECNOLOGÍA | ENERGÍA

I-DE BLINDA SUS REDES CON ORBIK E IKERLAN

LA EMPRESA DE DISTRIBUCIÓN ELÉCTRICA DE IBERDROLA REFUERZA LA CIBERSEGURIDAD CON UN LABORATORIO VIRTUAL PORTÁTIL PIONERO CREADO POR EL CENTRO Y LA STARTUP

i-DE, la empresa de distribución eléctrica del grupo Iberdrola, ha dado un nuevo impulso a la ciberseguridad de sus redes con un pionero laboratorio virtual portátil desarrollado por Orbik Cybersecurity e Ikerlan. Esta avanzada solución le permitirá mejorar la seguridad de los sistemas de control de sus subestaciones eléctricas en un contexto de creciente exposición a ciberamenazas y de mayores exigencias regulatorias.

El sistema se encuentra en el Global Smart Grid Innovation Hub de i-DE en Bilbao, donde la compañía dispone de una subestación eléctrica virtual para la realización de pruebas avanzadas. Durante la fase de validación, el laboratorio ha permitido automatizar más del 70% de los test de ciberseguridad susceptibles de ser mecanizados en Iberdrola, reducir de forma significativa los tiempos de evaluación y detectar vulnerabilidades en equipos comerciales previamente testados.

El proyecto se ha enfocado en la automatización de pruebas del *testbook* de Iberdrola, basado en el estándar internacional IEC 62443-4-2, referente clave para la protección de infraestructuras críticas como redes eléctricas, sistemas industriales y plantas de producción. Este avance cobra especial relevancia en un escenario marcado por nuevas normativas como la Ley europea de Ciberresiliencia (CRA), cuya aplicación

será obligatoria a partir de 2027, y por el incremento de vulnerabilidades en dispositivos electrónicos conectados.

Hasta ahora, estos ensayos se realizaban, mayoritariamente, de forma externa y manual, lo que implicaba altos costes, largos plazos y dificultades para escalar. Con esta nueva herramienta, Iberdrola podrá realizar pruebas internas de manera automatizada y reproducible, multiplicando su capacidad de evaluación y reduciendo significativamente los tiempos de homologación. “Con esta solución, Iberdrola podrá automatizar sus propios ensayos de ciberseguridad, obteniendo resultados objetivos y comparables, y avanzando hacia procesos certificables de forma más ágil y eficiente”, explica Oscar Saiz, del área de ciberseguridad de Ikerlan.

Orbik Cybersecurity ha desempeñado un papel clave en la definición e implementación de la capa de automatización y orquestación de las pruebas. Su director de operaciones, Borja Pérez, subraya que “la automatización de la evaluación de ciberseguridad supone un avance decisivo para la protección de infraestructuras

cesos, equipos y personas. Dentro de las diferentes líneas de acción, dada la evolución de los requisitos y nuevas directivas se detectó la necesidad de contar con un sistema de pruebas continuo que permita evaluar los equipos en cualquier fase de su ciclo de vida.

Tándem Ikerlan-Orbik

Como resultado de la colaboración entre Orbik Cybersecurity e Ikerlan, nace este laboratorio virtual, que refuerza la seguridad OT de las subestaciones, agiliza la validación de proveedores e impulsa la generación de conocimiento, con potencial aplicación futura al resto de equipos del grupo. Y es que la ciberseguridad de la red eléctrica se ha consolidado como uno de los grandes retos del sector energético.

Iniciativas previas como el proyecto Sec2Grid, impulsado por el Gobierno Vasco dentro del programa

Hazitek, y en el que participaron Ikerlan e Iberdrola junto a las principales empresas del sector eléctrico, ya evidenciaron la necesidad de avanzar hacia modelos más avanzados de detección y gestión de vulnerabilidades.

IBERDROLA PODRÁ AUTOMATIZAR SUS PROPIOS ENSAYOS



Investigadores de Ikerlan y Orbik Cybersecurity.

críticas, al permitir industrializar los procesos, mejorar la resiliencia frente a ciberataques y adaptarse a las exigencias regulatorias actuales y futuras”.

Para i-DE, la ciberseguridad no es una opción, sino una misión crítica e integrada en el ADN de todos los pro-

Con este nuevo laboratorio virtual, Iberdrola se posiciona como pionera en la adopción de soluciones avanzadas de ciberseguridad para infraestructuras eléctricas, mientras que Orbik Cybersecurity e Ikerlan refuerzan su papel como socios tecnológicos.

CERTIFICAR ES GENERAR CONFIANZA



La inteligencia artificial, el software y los sistemas digitales avanzan más rápido que nunca. Y los riesgos también.

En AENOR ayudamos a las organizaciones a certificar **sus sistemas de ciberseguridad, inteligencia artificial, calidad del software y de los datos, así como la seguridad en entornos digitales complejos.**

Porque la innovación sólo es sostenible cuando se apoya en criterios objetivos, una evaluación independiente y certificaciones reconocidas.



**Certificación para una
tecnología confiable**