byte TI

349 · Junio 2026

Compliance inteligente:
automatización y analítica para el cumplimiento normativo

El CISO ante el reto de aplicar Zero Trust

Qué deberían hacer ahora las pymes con NIS2

COMPARATIVA
Servidores para el centro de datos

mkm PUBLICACIONES

N. 349 | ÉPOCA IV
Edita:
Publicaciones Informáticas MKM
Junio 2026.

MKM PUBLICACIONES
Managing Director
Ignacio Sáez (nachosaez@mkm-pi.com)

BYTE TI
Director
Manuel Navarro (mnavarro@mkm-pi.com)

Redacción
Alfonso Casas (acasas@revistabyte.es)

Coordinador Técnico
Regina de Miguel

Colaboradores
J. Palazón, I. Pajuelo, O. González, M. López, F. Jofre, A. Moreno, M. J. Recio, JJ. Flechoso, D. Puente, A. Herranz, C. Hernández.

Fotógrafos
P. Varela, E. Fidalgo

Diseño de portada
María Torre

Diseño y maquetación
María Torre

REDACCIÓN
Avda. Adolfo Suárez, 14 – 2 B
28660 Boadilla del Monte. Madrid
Tel.: 91 632 38 27 / 91 633 39 53
Fax: 91 633 25 64
e-mail: byte@mkm-pi.com

DEPARTAMENTO COMERCIAL
Directora comercial:
Isabel Gallego (igallego@mkm-pi.com)
Account Manager:
Laura Sierra (lsierra@mkm-pi.com)
Tel.: 91 632 38 27

DEPARTAMENTO DE EVENTOS Y COMUNIDAD
Coordinadora:
María Vicente (mvicente@mkm-pi.com)
Tel. 91 632 38 27

SUSCRIPCIONES
e-mail: suscripciones@mkm-pi.com

Revista mensual de informática
ISSN: 1135-0407

Depósito legal: B-6875/95

Carta del Director

Manuel Navarro Ruiz
Director de BYTE TI

Abordar el reto del compliance

Más allá de que los focos llevan un tiempo puestos en la IA, otras materias no deberían pasar desapercibidas. De hecho, cada vez hay un mayor interés por el compliance. El inusitado interés se debe a que la gran mayoría de las empresas, más allá de multas y sanciones que puedan recibir, es que han visto que puede ser una ventaja competitiva. Para ello es fundamental que tecnología y gobernanza trabajen de forma conjunta.

El impacto que está teniendo el compliance y su unión con TI está provocando que estemos yendo hacia el compliance inteligente, como afirma mi compañero Alfonso Casas en el tema de portada que llevamos este mes. En este sentido, automatización, analítica avanzada e IA están conviertiendo procesos reactivos en sistemas preventivos capaces de detectar anomalías y anticipar riesgos en tiempo real.

La obligación de demostrar cumplimiento continuo ante normas como DORA, NIS2 o el AI Act empuja a las empresas a integrar trazabilidad y monitorización permanente en sus flujos, no como un parche sino como columna vertebral del negocio. Al mismo tiempo, la irrupción de la IA dentro de las organizaciones obliga a replantear las responsabilidades Y es que el compliance habilita el uso responsable de la IA, y la IA amplía las capacidades del compliance. Sin embargo, la automatización mal alineada o implantada sin priorizar objetivos puede desperdiciar recursos y generar nuevos riesgos; hasta el 30% del coste de algunos proyectos se va en integrar workflows con sistemas documentales y aplicaciones corporativas. Por eso el enfoque debe partir del dato: gobierno, calidad, arquitectura y trazabilidad son prerequisitos para que la IA entregue valor verificable y explicable.

Aquí se produce una paradoja: la misma IA que ayuda a cumplir exige supervisión estricta. El principio human-in-the-loop, la trazabilidad de decisiones y auditorías periódicas son ineludibles cuando los modelos empiezan a tomar decisiones que afectan a operaciones críticas y reputación corporativa. Además, la transformación cultural y el upskilling de equipos serán tan determinantes.

En el contexto actual, es fundamental que las empresas sitúen a los datos y a la gobernanza en el centro y traten a la Inteligencia Artificial como una herramienta gobernada,. Si se utiliza como un atajo, el cumplimiento nunca supondrá una ventaja competitiva real.

Actualidad

Confluent Intelligence impulsa el data streaming para la IA en tiempo real

Londres ha acogido una nueva edición de Current 2026, el evento de referencia organizado por Confluent en torno al data streaming y la inteligencia artificial aplicada a los datos en tiempo real. Bajo el lema "Building Intelligent Systems on Real Time Data", la cita ha reunido a desarrolladores, ingenieros, expertos en datos y líderes tecnológicos de toda Europa para explorar cómo las organizaciones pueden pasar de sistemas de análisis pasivos a arquitecturas capaces de actuar de forma autónoma sobre información actualizada al instante.

El pistoletazo de salida lo dio Jay Kreps, CEO y cofundador de Confluent, con una presentación que marcó el tono de toda la jornada. Kreps comenzó agradeciendo el impulso de la comunidad open source que sostiene los proyectos de la compañía: más de 400 activos y más de 80 nuevas Kafka Improvement Proposals (KIPs) para Apache Flink desarrolladas a lo largo del último año, además de avances como Kafka Queues y los nativos Flink Agents.

El CEO también confirmó oficialmente que Confluent pasa a formar parte de IBM,

Jay Kreps, CEO y cofundador de Confluent durante la inauguración del evento.

afirmando que "IBM tiene una larga tradición como guardián del open source, demostrada con Red Hat y Linux. Esta integración nos permite acelerar nuestra inversión en la comunidad y en las capacidades del producto", señaló Kreps, que destacó además que la incorporación a IBM será un nuevo impulso para mantener la innovación.

El grueso de su intervención se centró en el cambio de paradigma que está viviendo la industria: la transición desde los sistemas de Business Intelligence tradicionales, donde las personas interpretan datos para tomar decisiones,

Actualidad

Confluent Intelligence impulsa el data streaming para la IA en tiempo real

hacia sistemas autónomos que cierran el ciclo por sí mismos y actúan en consecuencia. "El problema no es el modelo de IA, sino disponer del contexto real de los datos desordenados de la empresa", afirmó Kreps. En este sentido, señaló que en el desarrollo de IA moderna, los datos y el código son inseparables, y que la calidad del contexto que recibe un agente determina directamente la calidad de sus decisiones.

Kreps también alertó sobre dos patrones frecuentes pero problemáticos en la empresa: exponer directamente los agentes a los sistemas de producción, lo que conlleva riesgos de seguridad y dificulta la evaluación; y curar el contexto en data lakehouses para después cargarlo en bases de datos operacionales, un enfoque seguro pero que genera datos demasiado obsoletos para sistemas en tiempo real. La solución que propone Confluent es una arquitectura streaming-first que unifica el procesamiento batch y en streaming en un único flujo desde el desarrollo hasta la producción.

La IA lista para pasar a producción

Shaun Clowes, Chief Product Officer de Confluent, tomó el relevo para presentar las novedades concretas que materializan esa visión. Su intervención giró en torno a la disponibilidad general de varias capacidades dentro de Confluent Intelligence y Confluent Cloud, bajo una premisa clara: eliminar los obstáculos técnicos y regulatorios que impiden a las organizaciones llevar sus proyectos de IA al entorno de producción.

"En muchas empresas de zona EMEA, la complejidad de las normativas de privacidad de datos acaba frenando los proyectos de IA antes de que lleguen a producción. Confluent elimina estas barreras al integrar gobernanza de nivel empresarial directamente en los flujos de datos", explicó Richard Timperlake, Vicepresidente Senior de Ventas para EMEA, quien acompañó la presentación con una perspectiva de mercado relevante: según McKinsey, ocho de cada diez empresas consideran que las limitaciones en los datos son el principal obstáculo para escalar la IA agéntica.

Entre los anuncios más destacados figura la disponibilidad general del Real-Time Context Engine, una capa SQL rápida con caché sobre tablas respaldadas por streaming, expuesta a través del protocolo MCP para que agentes y aplicaciones puedan consultarla con muy baja latencia. Este motor evita las costosas transferencias entre sistemas y ofrece iteraciones sobre los conjuntos de datos de contexto de forma segura y evaluable, algo crítico para mejorar los resultados de los agentes de IA.

En el plano de la seguridad y la privacidad, Confluent presentó en forma de acceso anticipado una nueva función de anonimización automática de datos personales (PII) integrada directamente en Flink SQL, sin necesidad de código personalizado ni servicios externos. Se completa con soporte para Azure Private Link, que permite mantener las cargas de trabajo de IA fuera de la red pública mediante conexiones privadas a servicios como Azure OpenAI o Cosmos DB.

El reto de los agentes de voz

Durante la jornada, destacó la conversación que mantuvieron Sean Falconer, Head of AI en Confluent, y Alex Holt, Head of Forward Deployed Engineering en II ElevenLabs. Ambos coincidieron en que los dos grandes retos para desplegar agentes de voz en entornos empresariales son la latencia y la precisión del contexto.

No basta con que el modelo sea capaz: necesita acceder a información corporativa actualizada y relevante en tiempo real. "Hay que tratar a los agentes como código, con configuración, versionado, pruebas y monitorización", subrayó Holt, apelando al rigor de ingeniería necesario para llevar estos sistemas a producción de forma fiable.

Actualidad

V-Valley muestra su fortaleza en su V-Valley Tech Summit

V-Valley mostró en una nueva edición de su evento V-Valley Tech Summit toda su fortaleza. Este encuentro, celebrado en el Palacio de Congresos Lienzo Norte de Ávila es ya toda una referencia del ecosistema tecnológico nacional al reunir a los principales actores del sector para analizar las tendencias que están marcando la transformación digital de las empresas.

La inauguración contó con la participación de Javier Santaolalla, físico, divulgador científico y referente en comunicación tecnológica, quien ha sido el encargado de conducir y dinamizar el acto inaugural del congreso, acercando la tecnología y la innovación a todos los públicos con un lenguaje accesible y aportando una mirada cercana y divulgativa a la innovación. Uno de los momentos clave de la inauguración ha sido la mesa redonda "De la visión al impacto: cómo convertir la IA (y la innovación) en resultados medibles a través del ecosistema", en la que expertos de primer nivel de las compañías líderes Microsoft, NVIDIA, Templus, C1b3Wall y V-Valley, han analizado el papel de la inteligencia artificial y la innovación aplicada como palancas reales de negocio, así como la necesidad de colaboración entre fabricantes, partners, sector público y empresas.

Con esta nueva edición, el V-Valley Tech Summit refuerza su posicionamiento como el único evento del canal con contenido 100% tecnológico, centrado en soluciones avanzadas de alto valor y pensado por y para la comunidad tecnológica. Durante dos jornadas, más de 50 fabricantes y expertos del sector comparten visión, conocimiento y casos reales en torno a áreas clave como inteligencia artificial, ciberseguridad, cloud, data, infraestructura y soluciones híbridas, a través de un completo programa de ponencias, mesas redondas, demostraciones técnicas y espacios de networking. El evento puso también el foco en la ciberseguridad como prioridad transversal, la creciente adopción de modelos híbridos y la necesidad de partners cada vez más especializados, en un contexto de madurez del canal y demanda de soluciones tecnológicas avanzadas.

La elección de Ávila como sede del encuentro vuelve a situar a esta ciudad en el centro del mapa tecnológico nacional. La localidad castellana está haciendo en los últimos años un notable esfuerzo por consolidarse como sede de grandes encuentros profesionales, combinando innovación, patrimonio y proyección como destino de turismo de congresos y eventos.

FERNANDO JOFRE

Inteligencia por kilovatio

La IA avanza más rápido que la capacidad energética de los data centers. Por eso, en las últimas semanas hemos visto una oleada de anuncios que confirman una tendencia clara: **la próxima gran batalla tecnológica no es por la potencia, sino por la eficiencia**.

En abril de 2026, la startup Positron anunció una ronda de 230 millones de dólares para desarrollar chips de inferencia un **40% más eficientes**. Apenas unas semanas antes, Intel presentó **Crescent Island**, una GPU diseñada para maximizar el rendimiento por vatio en cargas de IA reales, parte de su estrategia de lanzar hardware de IA cada año. Europa también se mueve. Axelera AI aseguró **250 millones de dólares** para escalar sus chips "Europa", optimizados para inferencia eficiente en el edge. Y desde el ámbito académico, la Universidad de Cambridge publicó en **Science Advances** (abril–mayo 2026) un memristor capaz de reducir el consumo energético de la IA en **hasta un 70%,** un salto que podría transformar la industria.

Para la alta dirección el mensaje es inequívoco: la competitividad ya no dependerá solo de cuánta IA se despliega, sino de **cuánta IA puede ejecutarse por cada kilovatio disponible**. La eficiencia energética se convierte en la nueva métrica estratégica.

Actualidad

SAP sitúa a la empresa autónoma como eje de su estrategia de IA

SAP acaba de celebrar Sapphire 2026 donde ha presentado su hoja de ruta. Su propuesta parte de la idea de que la IA no debe limitarse a responder preguntas, sino a operar con contexto de negocio real y coordinar procesos dentro de la empresa. En un contexto en el que los agentes parecen que van a acabar con las labores que realizan los trabajadores, la compañía apuesta claramente por un modelo mixto. El lema de Sapphire 2026, "The Beginning of Better", es toda una declaración de intenciones sobre la propuesta de SAP que pasa por un modelo en el que asistentes y agentes de IA trabajan junto a las personas para automatizar tareas y liberar tiempo para poder realizar funciones de mayor valor añadido.

Por si no quedaba claro, Christian Klein, CEO de SAP, resumió esa ambición al señalar que, "en la empresa autónoma, los agentes gestionan la organización para que las personas puedan centrarse en lo que realmente importa". El punto de partida de la estrategia de la multinacional es SAP Business AI Platform, una base tecnológica que unifica SAP Business Technology Platform, SAP Business Data Cloud y SAP Business AI en un solo entorno. La plataforma incorpora SAP Knowledge Graph, una capa de contexto empresarial diseñada para que la IA trabaje con datos fiables, procesos reales y una visión más gobernada del negocio. La plataforma también permite integrar datos SAP y de terceros para eliminar silos y facilitar una visión unificada de la empresa.

SAP sostiene que este enfoque busca resolver una de las grandes limitaciones de la IA generativa como es su dependencia de información pública y la falta de contexto específico de cada empresa. La compañía afirma que su experiencia acumulada durante más de 50 años en procesos empresariales y ERP le permite conectar los modelos de lenguaje con la lógica operativa de las empresas.

En el núcleo funcional de la propuesta se encuentra SAP Autonomous Suite, que amplía las aplicaciones de finanzas, recursos humanos, cadena de suministro, compras y experiencia de cliente con agentes de inteligencia artificial. La compañía asegura que incorpora más de 50 asistentes Joule especializados y más de 200 agentes diseñados para ejecutar tareas concretas. También se han presentado nuevas capacidades como Joule Studio, una solución que permite crear agentes empresariales, aplicaciones y workflows basados en IA además de Industry AI, siete nuevas soluciones sectoriales autónomas, y ha mostrado cómo cambiará la experiencia de usuario con Joule Work, una nueva interfaz que permite interactuar con los sistemas empresariales mediante lenguaje natural.

MANUEL LÓPEZ

NeuroCuántica: ambigüedad inteligente más allá del ruido

La *NeuroCuántica* no es una disciplina cerrada ni una tecnología lista para adoptar. Es un concepto en evolución que describe la convergencia entre *modelos "neuroinspirados" y computación cuántica*: una forma de imaginar sistemas de IA capaces de combinar la eficiencia del cerebro con la capacidad de exploración masiva de los qubits. Es un marco para pensar lo que viene cuando el paradigma actual empieza a mostrar fatiga.

Porque la IA que hemos construido hasta ahora es hija del silicio: rígida, voraz, poderosa, pero profundamente mecánica. Aprende a base de datos y fuerza bruta, como quien memoriza sin comprender. Y, sin embargo, aspiramos a que intuya, generalice, imagine. Ahí es donde la NeuroCuántica se vuelve sugerente. No afirma que el cerebro sea cuántico, sino que la inteligencia —humana o artificial— necesita algo más que escalado. Necesita la capacidad de explorar sin destruir, de decidir sin agotar.

El silicio nos ha traído hasta aquí. El qubit puede llevarnos más lejos. Entre ambos se abre un territorio fértil donde la IA puede dejar de comportarse como un martillo gigantesco y convertirse en un instrumento más sutil, más eficiente, más cercano a la forma en que la naturaleza resuelve problemas.

Actualidad

IBM apuesta por nuevo modelo operativo de IA

IBM ha celebrado en Madrid su evento Think 2026, una cita que en esta edición, coincide con el centenario de la compañía en España. El encuentro ha servido para presentar sus últimas innovaciones orientadas a escalar la inteligencia artificial (IA) en entornos corporativos y reforzar la seguridad y gobernanza del dato.

Horacio Morell durante su intervención en Think 2026.

La jornada inaugural contó con la participación de Horacio Morell, presidente de IBM para España, Portugal, Grecia e Israel, y Ana Paula Assis, Senior Vice President y Chair de IBM EMEA y APAC. Morell repasó la trayectoria de la compañía en el país y subrayó el cambio de paradigma que supone la IA en el tejido empresarial. El máximo responsable de la compañía en nuestro país ha querido dejar claro durante su ponencia que "la IA ha dejado de ser un soporte para convertirse en el propio modelo de negocio. Nuestro objetivo es acompañar a las organizaciones para que la integren de forma segura, soberana y orientada a resultados".

El nuevo modelo operativo de IA

Uno de los ejes del evento fue la presentación del nuevo modelo operativo de IA de IBM, diseñado para facilitar el paso de iniciativas piloto a despliegues a gran escala. La propuesta se centra en la orquestación de agentes de IA y en su integración efectiva dentro de los procesos de negocio, con especial énfasis en la gobernanza, la seguridad y el control del dato.

En este contexto de nuevo modelo operativo de IA, Ana Paula Assis destacó que la ventaja competitiva ya no reside en el acceso a la tecnología, sino en su nivel de integración operativa. "Las organizaciones que lideren la IA empresarial serán aquellas capaces de desplegarla a escala bajo principios sólidos de gobernanza, especialmente en entornos regulatorios exigentes como el europeo", señaló.

Como parte de este enfoque, IBM anunció IBM Bob, un nuevo partner de desarrollo agéntico orientado a transformar el ciclo de vida del software. La solución permite acelerar la modernización de sistemas heredados, automatizar pruebas y reforzar la seguridad sin comprometer la velocidad de entrega.

Actualidad

IBM apuesta por nuevo modelo operativo de IA

Un auditorio lleno atendiendo a las diferentes ponencias.

Ana Gobernado, directora general de IBM Consulting para la región, puso el foco en el impacto organizativo de estos avances: "La IA introduce un 'equipo expandido' de agentes digitales que multiplica las capacidades del talento humano. Esto obliga a rediseñar procesos y adoptar un modelo de gobierno que garantice resultados tangibles".

Soberanía digital como prioridad estratégica

El temática de moda no podía faltar en el evento. Y es que, la soberanía del dato fue otro de los grandes temas abordados en Think Madrid. Según un estudio global de IBM, el 88% de los CEO españoles considera la IA soberana un factor clave para su competitividad y protección de datos. Para responder a este reto, la compañía anunció la disponibilidad general de IBM Sovereign Core, una plataforma que integra políticas de infraestructura y permite adaptar la gobernanza a los cambios regulatorios, al tiempo que prioriza la portabilidad de las cargas de trabajo en entornos híbridos.

Banca española: referente en adopción tecnológica

El evento también sirvió para mostrar casos de uso reales en el sector financiero, que se posiciona como uno de los más avanzados en la adopción de IA y computación cuántica en España.

- **BBVA:** Su Global CIO, Carlos Casas, abordó la estrategia del banco en computación cuántica y el papel de la IA en su transformación tecnológica, así como los nuevos modelos de arquitectura y relación con el cliente.
- **CaixaBank:** Luis Javier Blas, COO de la entidad, analizó la estrategia de IA y su experiencia con la Región Cloud de IBM en España, destacando su papel en la soberanía del dato.
- **Banco Santander:** David Cebrián (Head of AI Governance) y José Palacios (Data & AI Officer) profundizaron en los retos de gobernar la IA a escala dentro de grandes organizaciones.

La jornada se completó con el espacio Think Forum, donde los asistentes pudieron interactuar con demostraciones tecnológicas en vivo y conocer iniciativas de innovación de compañías como Telefónica, Grupo Carreras y Nestlé.

> **IBM Sovereign Core, es una plataforma que integra políticas de infraestructura y permite adaptar la gobernanza**

Actualidad

Unicaja mejora el control sobre la gobernanza con la IA

Unicaja avanza en la evolución de su modelo de ingeniería de software con la industrialización de la producción de código mediante capacidades aumentadas por inteligencia artificial generativa (IAG). Este enfoque busca escalar el desarrollo de sistemas en un contexto de creciente complejidad tecnológica y exigencia regulatoria, preservando el control interno sobre la arquitectura, la seguridad y el gobierno de la tecnología.

El modelo se apoya en la estandarización y factorización de los procesos de desarrollo, en el uso de IAG como herramienta de soporte, siempre con supervisión humana, y en la colaboración con un ecosistema estable de partners tecnológicos organizados por dominios, formado por IBM, NTT Data, Babel, GFT y Scalian, que complementan las capacidades internas del banco y operan conforme a los criterios y marcos definidos por Unicaja.

Control sobre la arquitectura tecnológica

Esta evolución de Unicaja forma parte del trabajo que la entidad viene desarrollando desde el inicio del Plan Estratégico 2025-2027, orientado a dotar a la ingeniería de software de mayor capacidad para acelerar la ejecución de proyectos, mejorar la eficiencia y facilitar la evolución de las plataformas, fundamentalmente las más tradicionales, conservando el control sobre la arquitectura tecnológica y el gobierno del uso de la IAG dentro del banco.

La incorporación de la IAG en los entornos de trabajo del equipo de Tecnología de Unicaja se está realizando de forma progresiva. En una primera fase, se ha desplegado Copilot como herramienta de apoyo a determinadas etapas de la ejecución de proyectos, como la toma de requisitos de negocio, la gestión de proyectos y la mejora de la calidad y consistencia de los entregables. Este despliegue ha ido acompañado de un proceso estructurado de gestión del cambio, orientado a facilitar la adopción de estas nuevas formas de trabajo y a generar buenas prácticas con impacto en plazos y productividad.

El eje central del modelo es la gestión centralizada del conocimiento, articulada a través de una plataforma propia desarrollada con el apoyo de modelos IAG seleccionados y validados por el equipo de IA del banco. Estos modelos han demostrado una alta eficiencia en el entendimiento y procesamiento de lenguajes de programación tanto actuales como legacy.

La plataforma interna de la entidad, denominada Rosetta, actúa como base común para proyectos nuevos y aplicaciones en uso, proporcionando criterios homogéneos de trabajo y un acceso ordenado y gobernado a la información funcional y técnica para los equipos internos y para los centros de ingeniería de los colaboradores seleccionados. De esta forma, contribuye a mitigar el riesgo operacional y de obsolescencia. Desde esta base, la incorporación de herramientas de programación se plantea como un paso inmediato, siempre con supervisión humana integrada en el proceso.

En 2025 se desarrolló el embrión de Rosetta mediante pruebas de refactorización de elementos tradicionales de la plataforma mainframe de Unicaja (JCLs). En estos pilotos se registraron ahorros de tiempo de programación superiores al 80% y un nivel de precisión del código refactorizado cercano al 100%. Durante 2026, se prevé incorporar a Rosetta, en distintas oleadas, aplicaciones de los diferentes dominios junto con los partners seleccionados, comenzando por las tecnologías más legacy y avanzando hacia las plataformas digitales y de datos. En el presente ejercicio se incorporarán aproximadamente 600 aplicaciones de negocio actualmente en producción en Unicaja.

Actualidad – Te interesa

España acelera en I+D para impulsar la Soberanía Digital de Europa

Telefónica, Arsys, OpenNebula Systems y Corporación MONDRAGON, las cuatro compañías españolas involucradas en el Proyecto Importante de Interés Común Europeo de Servicios de Infraestructura en la Nube (IPCEI-CIS), participaron en el encuentro Soberanía Digital y Edge dentro de los proyectos europeos IPCEI: la iniciativa 8ra. Esta jornada constató sus últimos avances en el proyecto 8ra, demostrando el potencial de España para liderar el desarrollo del continuo Cloud-Edge y habilitar una nueva generación de servicios digitales soberanos.

Con la coordinación de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales (SETELECO), el IPCEI-CIS desarrolla un ecosistema europeo de infraestructuras IT Cloud y Edge Computing interoperable, abierto y seguro, que refuerza el control del dato y facilita el desarrollo de servicios digitales más avanzados y soberanos. En la jornada, Jesús Marcos Morell, del gabinete de la SETELECO, destacó el valor de la colaboración público-privada en estas iniciativas de I+D: "Los IPCEI son una herramienta clave para la soberanía europea. Sin el impulso del Plan de Recuperación y una colaboración estrecha entre el sector público y el privado, España no podría participar en proyectos de esta magnitud. Nuestro objetivo es que este esfuerzo tenga un impacto real y duradero".

Por su parte, Luis Almansa, experto en Estrategia de Transformación TI en Telefónica España, se centró en la creación de nodos Edge y su capa de conectividad. "Estamos desplegando una red de nodos Edge a lo largo de todo el territorio nacional que transformará nuestras centrales en pequeños centros de datos de mínima latencia, creando el sistema nervioso de la nueva economía digital europea. Hasta el momento se dispone de 17 nodos con disponibilidad de infraestructura TI, donde los clientes sacarán provecho de sus prestaciones y bajas latencias para el despliegue de sus aplicaciones".

El proyecto de Arsys llegó por parte de Javier Arnáez, Manager del área de innovación Arsys Lab: "La soberanía del dato es el pilar de nuestro proyecto. Estamos creando una plataforma de orquestación, un ecosistema abierto y multiproveedor que elimine las incertidumbres actuales y refuerce la competitividad de la UE", explicó Arnáez. "Nuestro objetivo es claro: permitir a las empresas ejecutar sus aplicaciones y gestionar sus datos en nodos Edge cercanos con la máxima eficiencia, control y seguridad, garantizando que el valor del dato permanezca en Europa".

Participantes en la jornada "Soberanía Digital y Edge dentro de los proyectos europeos IPCEI: la iniciativa 8ra"

Por su parte, Michel Íñigo, senior Innovation & Technology Manager en Corporación MONDRAGON, puso el énfasis en la aplicación de estos desarrollos en el sector industrial: "Este proyecto nos permite desplegar soluciones de IA descentralizadas para optimizar la producción en tiempo real y acelerar la inteligencia en nuestras fábricas, respondiendo a la necesidad de máxima agilidad del sector".

Finalmente, la ponencia de OpenNebula Systems, a cargo de Alfonso Carrillo, Principal Edge Solutions Architect, y Pablo del Arco, Cloud & DevOps Innovation Engineer, se centró en su misión como proveedor europeo de tecnología Edge-Cloud: "Aportamos la capa de software de código abierto que simplifica la complejidad de la nube soberana multiproveedor, garantizando una gestión unificada y la portabilidad de las cargas de trabajo".

Actualidad – Te interesa

De consultoras tecnológicas a Frontier Companies: la transformación inevitable en la era de la IA

La transformación de la consultoría tecnológica ya no es una hipótesis: es un hecho medible. Los últimos datos del ecosistema Microsoft lo avalan con una base empírica poco habitual: 20.000 profesionales encuestados en múltiples mercados, billones de señales anonimizadas de Microsoft 365 y el análisis de más de 100.000 conversaciones reales con Copilot. La conclusión es clara: la inteligencia artificial está redefiniendo el trabajo y, con él, el modelo de negocio de las consultoras.

En este contexto, Microsoft introduce un doble concepto clave: Frontier Company y Frontier Partner. Las primeras integran la IA de forma transversal en su negocio; los segundos hacen posible esa transformación, acompañando a sus clientes desde la experimentación hasta la producción. Este mapeo marca un punto de inflexión para el canal TIC: ya no basta con implementar tecnología, es necesario operar capacidades de negocio basadas en IA.

Una nueva brecha competitiva y un cambio de modelo inevitable

Sin embargo, esta transición no avanza al mismo ritmo en todos los sectores. El último Work Trend Index de Microsoft muestra que solo algunas industrias —con Software y Tecnología a la cabeza, con un 10%— están empezando a consolidar este modelo. Así, emerge una nueva brecha: no entre quienes tienen acceso a la tecnología, sino entre quienes saben integrarla en procesos críticos y quienes permanecen en fase experimental.

La IA ya no se utiliza solo para tareas accesorias, sino cada vez más en actividades de alto valor como análisis, toma de decisiones y resolución de problemas

En paralelo, el análisis de más de 100.000 conversaciones con Copilot confirma un cambio cualitativo: la IA ya no se utiliza solo para tareas accesorias, sino cada vez más en actividades de alto valor como análisis, toma de decisiones y resolución de problemas. Este desplazamiento eleva el listón para las consultoras, que deben evolucionar desde la automatización hacia el rediseño del trabajo.

Hugo de Juan CEO de ENCAMINA

Esa evolución exige, además, coherencia interna. No se puede liderar la transformación de otros sin haberla abordado previamente dentro de la propia organización. Como explica Hugo de Juan, CEO de ENCAMINA —la tecnológica reconocida como Mejor Partner del Año de Microsoft en España—:

Actualidad – Te interesa

"No se puede acompañar a los clientes en una transformación que uno mismo no ha hecho antes; la credibilidad se construye demostrando adopción profunda, no solo conocimiento técnico. Pero mucho más allá de dar ejemplo, se trata de una transformación necesaria en un mercado que se expande en oportunidades, pero se comprime en tiempos y tarifas. Un mercado que necesita más agilidad y velocidad que nunca. Un mercado donde los nuevos entrantes serán competencia del status quo. Un mercado en el que queremos seguir siendo vanguardia e inspiración y, sobre todo, muy útiles a nuestros clientes".

Desde esta perspectiva, la adopción, la formación, la gobernanza y el cambio cultural dejan de ser elementos accesorios para convertirse en el núcleo del éxito. Y es precisamente ahí donde el papel del partner adquiere una nueva dimensión.

Del piloto a la producción: el verdadero rol del Frontier Partner

El punto de inflexión ya no está en probar la IA, sino en industrializarla. Como señala Iván Martínez Castillo, Director de Partners de Microsoft España:

"En la era agéntica, la diferencia no la marca quién adopta antes la tecnología, sino quién es capaz de integrarla con criterio, seguridad y visión a largo plazo. España ya ha demostrado su capacidad para adoptar la inteligencia artificial; ahora el reto es convertir ese liderazgo en valor sostenido para las organizaciones. Los Frontier Partners serán quienes hagan posible esa transición: socios tecnológicos capaces de acompañar a las empresas desde la experimentación hasta la producción, reduciendo riesgos, acelerando resultados y generando confianza".

> **Los Frontier Partners serán quienes hagan posible esa transición: socios tecnológicos capaces de acompañar**

Así, el valor diferencial de la consultora ya no reside en desplegar tecnología, sino en conectar negocio, adopción y ejecución de forma consistente. Esto se traduce en tres cambios clave: ventas orientadas a impacto, operaciones basadas en equipos híbridos humano-IA y un nuevo mercado de servicios gestionados y mejora continua.

Iván Martínez Castillo,
Director de Partners de Microsoft España

Convertirse en Frontier Company no consiste en llegar primero, sino en hacer el cambio de forma consistente y sostenible. En un entorno donde todo se acelera, la verdadera ventaja competitiva estará en quién sea capaz de transformar mejor —y antes— su propio modelo.

Más información: ENCAMINA

Actualidad – Te interesa

Cuando la IA escribe código, ¿quién responde?

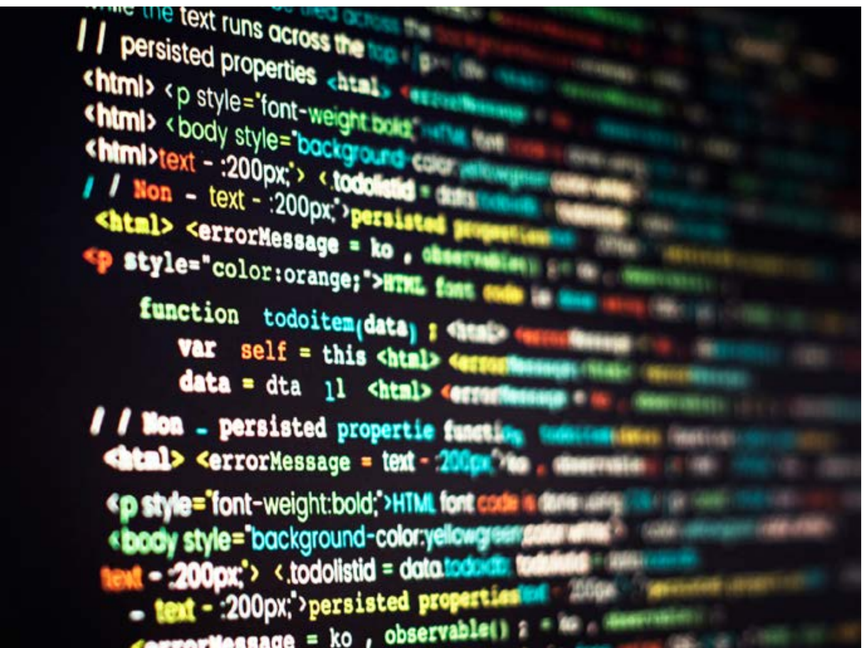
Se programa más rápido que nunca, pero la confianza en el código generado por IA cae. Más allá de la seguridad, en los sectores regulados la cuestión es quién responde por un código que casi nadie puede explicar.

La IA ya escribe software, pero el reto no es solo producir código más rápido, sino poder entenderlo, confiar en él y responder por sus efectos.

Según el Developer Survey 2025 de Stack Overflow, el uso de IA entre desarrolladores ha subido al 84%, mientras la confianza en sus resultados ha caído al 29%, frente al 40% del año anterior. Cuanto más se usa, menos se confía.

No es solo seguridad

El riesgo no está solo en el código que un equipo ve generar, sino en el que ya ha entrado en sistemas, librerías, dependencias o desarrollos subcontratados sin visibilidad suficiente sobre su origen ni sus controles.



Solo el 24% de las organizaciones evalúa a fondo la propiedad intelectual, las licencias, la seguridad y la calidad del código que genera la IA, según OSSRA 2026 de Black Duck. Sin control real, la trazabilidad falla cuando llega una auditoría.

También hay un riesgo legal: un asistente puede incorporar código sujeto a licencias no aceptadas por la empresa y convertirlo en un pasivo en una due diligence, una demanda o una auditoría.

Además, el código generado por IA introduce vulnerabilidades en el 45% de los casos, según Veracode, y los CVE atribuibles a IA que rastrea Georgia Tech se dispararon en 2026.

De programar a poder responder

«La primera ola de la IA en el desarrollo de software fue una cuestión de velocidad. La siguiente es una cuestión de confianza. No se trata de frenar la IA, sino de poder responder por lo que produce: saber de qué regla nace cada cambio, qué normativa cumple y cuál no. En un entorno regulado, eso no es un lujo; es la condición para poder desplegar», afirma Carlos Gutiérrez, Director de Go-to-market de h&k.

Para h&k, la clave es incorporar trazabilidad y gobierno desde el origen: saber de dónde nace cada línea, qué normativa cumple y quién responde de ella.

En 2026, el Reglamento de IA de la UE, el Cyber Resilience Act y, en finanzas, DORA refuerzan esa exigencia: la trazabilidad del software y el control sobre proveedores ya son una obligación.

La cuestión de fondo es cómo medir la calidad del código que genera la IA: no solo si compila o pasa tests, sino si cada decisión puede trazarse hasta su origen y mantenerse bajo control.

La pregunta ya no es si la IA puede escribir el código, sino si la empresa puede responder por él.

Actualidad – Te interesa

El Contracting en IT: un modelo de contratación que va al ritmo del negocio

Por VANESA PEÑA,
Senior Manager de Contracting & Outsourcing Services en Hays España

La agilidad se ha convertido en la nueva moneda de la competitividad tecnológica. Ya no gana solo quien más invierte en innovación, sino quien ejecuta cualquier avance antes que los demás, escalar sin grandes complejidades y adaptarse sin perder ritmo. En 2026, la agilidad ha dejado de ser una aspiración y el reto para los equipos IT es que, aunque las empresas quieren crecer más rápido, el acceso a talento especializado no avanza en síntonía.

Nuestra Guía del Mercado Laboral 2026 refleja esta tensión: el 81% de las empresas en España prevé ampliar sus equipos, pero el 93% reconoce dificultades para encontrar perfiles cualificados, una cifra récord que evidencia la magnitud del desafío. A ello se suma que un 72% planea aumentar salarios para competir por ese talento escaso, especialmente en áreas como desarrollo, cloud o ciberseguridad.

Ante este escenario, empieza a consolidarse una lógica distinta: la "plantilla mixta" donde conviven equipos internos con talento externo altamente especializado. El objetivo ya no es cubrir puestos, sino incorporar capacidades concretas justo cuando el proyecto las necesita. Además, este cambio no es solo organizativo, sino también económico, ya que el 56% de las empresas ya recurre a la contratación por proyectos como vía para ganar flexibilidad en costes de personal, transformando estructuras fijas en modelos más variables y adaptables.

En este punto, desde Hays creemos que el Contracting en IT se posiciona como una solución estratégica. Esta herramienta permite a las organizaciones activar talento experto cuando el negocio lo requiere, aportando flexibilidad y reduciendo la rigidez de las estructuras de contratación tradicionales. Además, facilita transformar costes fijos en variables, algo especialmente valioso en entornos de alta incertidumbre tecnológica.

Además, es un modelo clave en proyectos donde la velocidad es crítica: implementación de IA generativa, migraciones a cloud o refuerzos puntuales en ciberseguridad ante nuevas amenazas o regulaciones. Incorporar especialistas externos introduce conocimiento actualizado y perspectivas distintas que enriquecen a los equipos internos.

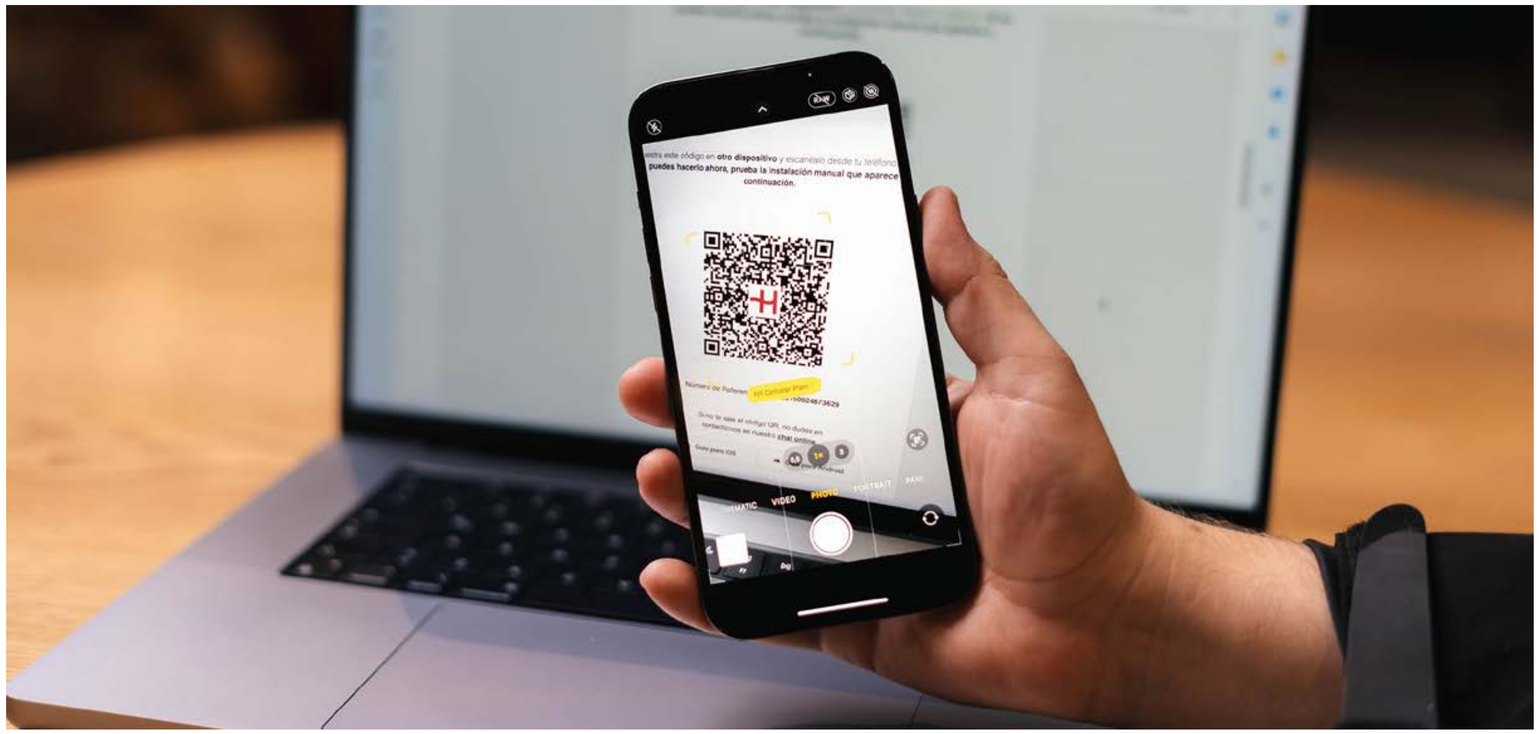
El Contracting encaja dentro de una transformación más amplia hacia modelos basados en capacidades. El 50% de las organizaciones ya utiliza modelos de proyecto para acceder a habilidades concretas en momentos puntuales, reforzando la idea de que el talento se activa, no solo se incorpora. En paralelo, desde Hays, detectamos que gana fuerza el enfoque de skills-based pay, donde la compensación se vincula directamente a competencias y resultados, consolidando una gestión más dinámica del talento.

Sin embargo, gestionar este ecosistema híbrido no es sencillo. La complejidad normativa o la coordinación entre talento interno y externo requieren una gestión precisa. Aquí es donde cobra relevancia la figura de un partner especializado, capaz de garantizar tanto la eficiencia operativa como el cumplimiento regulatorio.

Con todo, el foco está en la capacidad de construir organizaciones que respondan en tiempo real a la demanda del negocio. Y aquí, es donde el Contracting cobra sentido.

Actualidad – Te interesa

El mayor riesgo de seguridad no está en tu infraestructura. Está en cómo se conecta tu equipo al viajar



Un miembro de tu equipo acaba de aterrizar tras un vuelo intercontinental. Enciende el móvil. No tiene conexión. ¿Siguiente paso? Busca una red WiFi pública en el aeropuerto. En cuestión de minutos, podría estar exponiendo credenciales corporativas en una red insegura, o generando un coste innecesario por una simple notificación de "todo bien".

Para los responsables de IT, este escenario —cotidiano y aparentemente inofensivo— concentra varios de los riesgos más relevantes en la gestión de la conectividad internacional. Holafly for Business resuelve esta paradoja de nuestros días: aunque los viajes corporativos están plenamente integrados en la operativa de muchas compañías, la conexión a internet sigue dependiendo de soluciones reactivas como redes WiFi públicas, tarjetas SIM locales o planes de roaming tradicionales.

No olvidemos que, más allá de la tecnología, hay un componente humano clave. La necesidad de estar conectado no es sólo operativa, también es emocional. Así, un estudio publicado en Scientific Reports analiza la relación entre la interrupción del acceso a internet o al smartphone y un aumento de la ansiedad. ¿El resultado? Decisiones impulsivas y poco seguras.

Las redes WiFi en aeropuertos, hoteles o estaciones representan un vector de ataque cada vez más explotado. Según Zimperium Global Mobile Threat Report 2025, el 40% de las amenazas móviles están relacionadas con la red, una cifra significativa teniendo en cuenta que en 2025 se identificaron más de 5 millones de redes Wi-Fi públicas inseguras y que el 33% de usuarios se conecta a redes públicas no seguras. Para evitar este tipo de exposición, Holafly prioriza conexiones móviles cifradas, reduciendo la superficie de ataque y protegiendo el tráfico en movilidad.

"No se trata solo de trabajar mejor, sino de hacerlo con tranquilidad, sabiendo que todo funciona desde el primer momento", explica Alex Bryszkowski,

vicepresidente de B2B & Partnerships de Holafly. "Hoy acompañamos a más de 3.000 clientes en todo el mundo que han convertido el acceso a internet en una ventaja competitiva real".

Empresas como Remy Cointreau, Naturgy, Cuatrecasas o Esteve ya han comprobado el impacto de esta solución no solo en la productividad, sino también en la cultura corporativa. Facilitar el acceso a internet en movilidad permite mejorar la experiencia del empleado, favoreciendo la conciliación incluso durante los desplazamientos y reforzando aspectos clave como la retención del talento en entornos cada vez más globales.

Sencillez operativa con conectividad en más de 200 destinos

El modelo de despliegue de Holafly for Business también responde a las necesidades operativas de los departamentos de IT. La plataforma Holafly Business Center permite centralizar la asignación de eSIMs, automatizar la facturación y mantener una visibilidad global sobre el consumo. Esto no solo mejora el control, sino que reduce tareas manuales y facilita la toma de decisiones basada en datos, algo cada vez más necesario en entornos distribuidos.

> **La entrega de eSIM por email permite activar dispositivos de forma remota, sin logística ni tiempos de espera**

Además, la entrega de eSIM por email permite activar dispositivos de forma remota, sin logística ni tiempos de espera, alineándose con modelos de Zero Touch Provisioning, un enfoque que encaja con estrategias de sostenibilidad IT.

Este cambio no es solo tecnológico, sino operativo: Holafly for Business facilita la conectividad en más de 200 países como un servicio gestionado dentro del stack de IT, que garantiza seguridad e inmediatez y responde a una tendencia clara: para 2027, el 80% de los dispositivos corporativos serán eSIM-only.

Volviendo al inicio: tu empleado acaba de aterrizar. La diferencia entre una operación fluida y un riesgo potencial no está en lo que haga en ese momento, sino en las decisiones que se han tomado previamente desde IT.

Más información:
El primer plan de datos global del mundo diseñado para empresas

Actualidad – Te interesa

iRobot apuesta por una limpieza adaptada al hogar con la nueva generación Roomba®

La limpieza inteligente ha dejado de ser una cuestión tecnológica para convertirse en una experiencia ligada al diseño del hogar y a la rutina. En un contexto donde los espacios son más dinámicos y multifuncionales, iRobot ha ampliado su gama Roomba® para 2026 con una generación diseñada para las necesidades del hogar.

La nueva familia Roomba® incorpora mejoras en navegación, automatización y capacidad de limpieza, con diseño compacto. De hecho, varios modelos reducen hasta un 25 % su tamaño respecto a generaciones anteriores, permitiéndoles acceder con mayor facilidad bajo muebles en espacios de apenas 9 centímetros de altura.

Robots compactos para el mantenimiento diario

Dentro de la nueva gama, Roomba® 115 está pensado para quienes buscan una limpieza sencilla y eficiente en viviendas pequeñas. El modelo combina un formato compacto con una potencia de succión de hasta 15.000 Pa, diseñada para eliminar polvo, migas y suciedad diaria de forma rápida y silenciosa.

Además, su tamaño reducido permite limpiar zonas de difícil acceso y optimizar la limpieza en cada estancia gracias a la navegación inteligente, complementándose con la propuesta de productos compactos de la marca junto al recientemente Roomba® Mini.

Más potencia para hogares con más actividad

Para viviendas con mayor tránsito, mascotas o necesidades de limpieza más intensivas, iRobot amplía también la familia Roomba® Plus. Los modelos Roomba® Plus 415, 515, 575, 615 y 675 Combo combinan aspirado y fregado en una sola pasada, incorporando

Actualidad – Te interesa

iRobot apuesta por una limpieza adaptada al hogar con la nueva generación Roomba®

entre 20.000 y 30.000 Pa de potencia de succión.

Además, los modelos Roomba® Plus 615 y 675 Combo mejoran la experiencia de fregado gracias a un sistema de rodillo y pulverización de agua caliente a presión, diseñado para eliminar suciedad seca y manchas adheridas. El uso de agua caliente —de hasta 60 °C— contribuye también a mejorar la higiene de las mopas.

Navegación inteligente para adaptarse al hogar real

Uno de los principales avances de esta nueva gama está en la tecnología ClearView™ LiDAR de los modelos para mapear el hogar de forma rápida y precisa, permitiendo una limpieza más eficiente incluso en espacios complejos.

En los modelos más avanzados, como Roomba® Plus 575, 615 y 675 Combo, este sistema se combina además con reconocimiento visual mediante inteligencia artificial para detectar y esquivar objetos cotidianos como cables o zapatos sin interrumpir el recorrido.

La experiencia se completa con las bases AutoWash™, capaces de vaciar residuos, limpiar componentes y secar mopas y rodillos automáticamente, reduciendo al mínimo la intervención del usuario.

Roomba® Max: una experiencia más autónoma y discreta

Para hogares más amplios o con mayores exigencias de limpieza, la gama Roomba® Max incorpora los modelos Roomba® Max 715 y 775 con hasta 30.000 Pa de potencia de aspiración junto con sistemas avanzados de fregado y cepillos optimizados para la recogida de pelo de mascotas y limpieza de alfombras.

Con esta nueva generación, iRobot refuerza su apuesta por una limpieza inteligente más discreta, automatizada y adaptada a la realidad de los hogares actuales.

> **Las bases AutoWash™ vacían residuos, limpian componentes y secan mopas y rodillos automáticamente, reduciendo la intervención del usuario**

Actualidad – Te interesa

Nemix y el reto del edge AI: convertir proyectos piloto en infraestructura real

Muchos proyectos de inteligencia artificial en el edge fracasan por la dificultad de convertir una prueba de concepto en una infraestructura operativa, repetible y sostenible. Desde Nemix han observado cómo muchas organizaciones validan con éxito una primera instalación en una sede concreta, pero encuentran dificultades cuando el despliegue debe escalar a decenas de ubicaciones. En ese momento, las preguntas cambian: cómo actualizar modelos sin intervención física, cómo gestionar servidores remotos o qué ocurre cuando una sede pierde conectividad.

Hardware preparado para edge AI: soluciones Supermicro

Las nuevas plataformas edge de Supermicro basadas en procesadores AMD EPYC 4005 están diseñadas precisamente para este tipo de escenarios. Combinan capacidad de cómputo, bajo consumo y gestión remota integrada en formatos compactos preparados para operar fuera del CPD tradicional.

Uno de los aspectos más relevantes de estas plataformas es su flexibilidad física. Los sistemas pueden desplegarse en armarios de comunicaciones, oficinas técnicas, tiendas o entornos industriales donde un servidor tradicional simplemente no encaja.

El formato short-depth permite llevar capacidad de inferencia local a ubicaciones donde hasta hace poco era inviable desplegar infraestructura de IA, y los slots PCIe Gen5 permiten incorporar aceleradoras como las NVIDIA L4 o L40S cuando el caso de uso lo requiere.

Una de las ventajas prácticas es que toda la gama comparte el mismo ecosistema de gestión remota de Supermicro. Esto permite centralizar monitorización, despliegue de sistemas operativos, actualización de firmware y administración de BIOS sin necesidad de desplazamiento físico.

El reto aparece en la integración. Muchas organizaciones deben integrar estos sistemas sobre redes sin segmentación clara, políticas de seguridad pensadas únicamente para el CPD o herramientas de monitorización que no estaban preparadas para operar infraestructura distribuida.

En entornos universitarios, por ejemplo, Nemix ha observado cómo grupos de investigación que validaban modelos en un único equipo de laboratorio se encontraban sin respuesta cuando había que llevar esa inferencia a varias facultades o a campus distribuidos. El problema rara vez estaba en el modelo, sino en que la infraestructura y los equipos de IT no estaban preparados para operar servidores fuera del CPD.

El enfoque de Nemix

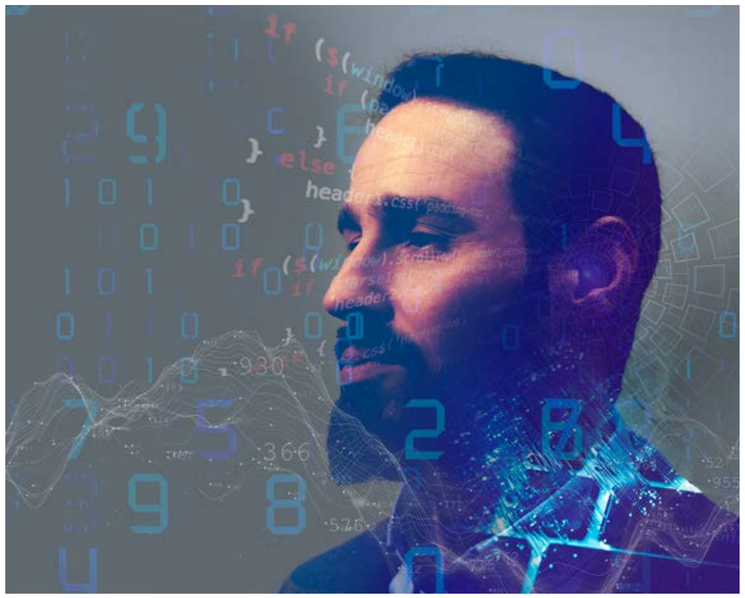
El trabajo de Nemix como integrador comienza antes de seleccionar la plataforma hardware. El análisis de la red, el modelo operativo y las necesidades de mantenimiento forman parte del diseño inicial del proyecto. A partir de ese diseño, Nemix configura e integra las soluciones Supermicro para simplificar la operación distribuida y minimizar la intervención manual.

Los proyectos de edge AI que siguen funcionando después del primer año son los que se diseñaron pensando en el día en que el técnico ya no puede ir a la sede.

Actualidad – Te interesa

Los dispositivos móviles son ya uno de los objetivos prioritarios del cibercrimen y del espionaje digital

Ricardo Barthel, CTO de OnRetrieval Group



Informes recientes señalan que los móviles han superado incluso al correo electrónico como principal vector de phishing, con tasas de interacción hasta un 40% superiores. Este escenario se agrava con la expansión del trabajo híbrido y remoto, que amplía la superficie de ataque y dificulta el control de dispositivos fuera de los entornos corporativos tradicionales. Frente a amenazas cada vez más sofisticadas —desde spyware avanzado hasta campañas de espionaje móvil y robo de credenciales—, las empresas buscan nuevas soluciones capaces de detectar ataques invisibles para las herramientas tradicionales de seguridad móvil.

Al mismo tiempo, amenazas avanzadas del nivel de Pegasus o Predator, antes reservadas a operaciones de alto nivel dirigidas contra gobiernos, periodistas o activistas, comienzan a democratizarse y a estar al alcance de actores menos sofisticados.

En este contexto, la colaboración entre OnRetrieval Group y Jamf busca ofrecer una nueva capa de protección especializada para dispositivos móviles, combinando tecnología avanzada de detección con capacidades forenses y de análisis experto. Conversamos con Ricardo Barthel, CTO de OnRetrieval Group, sobre esta alianza, sus implicaciones para el mercado y el futuro de la protección móvil avanzada.

¿Cuál ha sido la clave de la alianza entre OnRetrieval Group y Jamf?
La alianza surge de una complementariedad natural entre ambas compañías. Jamf aporta una tecnología altamente especializada en detección avanzada de amenazas móviles, especialmente a través de su solución Jamf Mobile Forensics (JMF), mientras que OnRetrieval Group contribuye con su experiencia en análisis forense y respuesta ante incidentes complejos.

Según explican desde la compañía, el mercado contaba hasta ahora con soluciones de gestión y protección móvil tradicionales, como MDM (Mobile Device Management) o MTD (Mobile Threat Defense), muy útiles para políticas de seguridad y amenazas convencionales, pero insuficientes frente a ataques sofisticados como Pegasus o Predator. La combinación entre la tecnología de vanguardia de Jamf y los servicios especializados de OnRetrieval Group permite cubrir precisamente ese vacío.

¿Qué valor diferencial aporta esta colaboración al mercado de la ciberseguridad?
El principal diferencial reside en la capacidad de detectar amenazas avanzadas que normalmente permanecen invisibles para las

Actualidad – Te interesa

Los dispositivos móviles son ya uno de los objetivos prioritarios del cibercrimen

herramientas tradicionales de seguridad móvil. Mientras que las soluciones convencionales pueden identificar malware común o amenazas básicas, la alta tecnología de Jamf está diseñada para localizar indicadores mucho más sofisticados relacionados con espionaje avanzado o cibercrimen dirigido.

Además, OnRetrieval Group complementa esta capacidad tecnológica con un servicio experto de análisis e investigación. La herramienta por sí sola ya ofrece una capacidad de detección muy potente, pero el valor añadido está en la interpretación avanzada de los resultados y en la capacidad de profundizar en la investigación cuando es necesario.

La compañía destaca además un aspecto clave: OnRetrieval Group es actualmente uno de los pocos proveedores oficiales MSSP (Managed Security Service Provider) de Jamf a nivel mundial certificados y habilitados para investigar amenazas dentro de esta plataforma, un reconocimiento especialmente relevante dentro del sector.

¿Por qué es especialmente importante ahora reforzar la seguridad móvil?
El auge del trabajo híbrido y remoto ha multiplicado la superficie de ataque de las organizaciones. El teléfono móvil se ha convertido en una herramienta crítica tanto para empleados como para directivos y, sin embargo, muchas compañías siguen protegiendo esta capa de forma insuficiente.

A ello se suma la evolución del panorama de amenazas. Según explican desde OnRetrieval Group, herramientas de ciberespionaje avanzado que antes estaban limitadas a gobiernos o actores altamente especializados empiezan a ser más accesibles. Amenazas recientes como "Coruna" o "Dark Sword" representan un ejemplo de esta democratización del cibercrimen sofisticado.

El riesgo ya no afecta únicamente a jefes de Estado o grandes figuras públicas. A medida que estas herramientas se hacen menos costosas y más accesibles, los potenciales objetivos se amplían hacia perfiles corporativos intermedios, empresas privadas y organizaciones estratégicas.

¿Cómo ayuda esta solución a empresas con modelos de trabajo híbridos o remotos?
La solución está diseñada precisamente para adaptarse a entornos distribuidos. Puede desplegarse tanto de forma remota mediante aplicaciones instaladas en los dispositivos como presencialmente mediante conexión física. Esto permite realizar inspecciones y análisis de forma continua sin importar dónde se encuentre el usuario.

Además de la capacidad forense puntual, la plataforma incorpora una capa preventiva mediante agentes instalados en los dispositivos que realizan escaneos continuos. Si detectan actividad sospechosa o indicios de compromiso, generan alertas automáticas para activar una respuesta rápida.

¿Qué sectores pueden beneficiarse más de este tipo de protección y qué futuro se avecina?
Aunque cualquier organización puede verse afectada, los sectores más expuestos son aquellos que manejan información crítica o sensible. Entre ellos destacan el sector financiero, la administración pública, defensa, seguridad y el ámbito legal.

Estos entornos son especialmente vulnerables tanto al espionaje industrial como a operaciones de cibercrimen avanzado o ataques vinculados a tensiones geopolíticas.

El mercado evolucionará rápidamente hacia una mayor especialización en protección móvil avanzada. El principal reto será seguir innovando al mismo ritmo que evolucionan las amenazas y anticiparse a ellas en un escenario donde el cibercrimen sofisticado es cada vez más accesible, asequible y frecuente.

Actualidad – Te interesa

Raphinha, selfies con IA y diseño ultraligero: así es el nuevo realme 16 5G

Cada vez son más los usuarios que buscan un smartphone capaz de seguir su ritmo diario sin renunciar al diseño, la cámara o la autonomía. En este contexto, realme ha presentado el nuevo realme 16 5G, un dispositivo que combina inteligencia artificial, fotografía avanzada y un diseño ultraligero pensado para quienes utilizan el móvil como una herramienta de creación y conexión.

La marca ha acompañado este lanzamiento con la incorporación de Raphinha como nuevo embajador de realme en Europa. El jugador brasileño del FC Barcelona protagoniza la campaña "Make it Raphinha, Make it realme", con la que la compañía refuerza su vínculo con una nueva generación de usuarios conectados al deporte, las redes sociales y la cultura digital.

Un diseño ligero con un rendimiento para los días más largos

Uno de los aspectos más diferenciales del realme 16 5G es su diseño. Con un peso de 181 gramos y un grosor de 8,1 mm, el dispositivo apuesta por una experiencia más cómoda y ligera sin comprometer la batería ni el rendimiento.

El terminal incorpora además el nuevo concepto Air Design, junto con un módulo horizontal "Camera Bar" para favorecer un agarre más cómodo y equilibrado. A esto se suma el acabado Aurora Wings, un efecto visual dinámico que genera reflejos en tonos azulados y dorados según la incidencia de la luz.

La experiencia visual se completa con una pantalla AMOLED de 120 Hz y hasta 4200 nits de brillo, diseñada para ofrecer buena visibilidad incluso en exteriores. Además, cuenta con certificación IP69, que proporciona una elevada resistencia frente al agua y el polvo. A nivel de autonomía, el dispositivo incorpora una batería Titan de 6550 mAh con carga rápida de 45W, diseñada para ofrecer usabilidad durante todo el día incluso en los más intensos.

Fotografía e inteligencia artificial para crear contenido en cualquier momento

La cámara es otro de los protagonistas del realme 16 5G. El dispositivo incorpora el sistema AI Portrait Master, con doble cámara de 50 MP y funciones de inteligencia artificial como AI Instant Clip o AI Edit Genie, diseñadas para crear y editar contenido de forma sencilla y personalizada.

Entre sus novedades destaca Selfie Mirror, una función que permite hacerse selfies con la cámara trasera para lograr imágenes de mayor calidad. Además, la tecnología LumaColor IMAGE optimiza automáticamente luces, sombras y detalles para conseguir retratos más naturales y realistas.

Raphinha, nuevo embajador de realme en Europa

Con esta alianza, realme refuerza su conexión con el fútbol europeo y con una generación que vive la tecnología y el deporte como parte de su rutina. La colaboración con Raphinha, uno de los futbolistas más destacados del momento, refuerza además la presencia de la marca en mercados como España, Italia, Francia y Polonia.

El jugador brasileño representa valores como autenticidad, creatividad y determinación, atributos que realme también traslada al nuevo realme 16 5G y a su apuesta por acercar tecnología avanzada a un público joven.

Actualidad – Te interesa

Seguridad y control de la IA en toda la empresa gracias a Prompt Security de SentinelOne

Case Study: 10x Banking

La empresa	10x Banking
País	Inglaterra
Sector	Fintech / Banca
Solución implementada	Prompt Security de SentinelOne
Resultados obtenidos	Adopción de la IA de forma segura, sin limitaciones

El Contexto

10x Banking es una plataforma bancaria cloud-native con sede en Londres, diseñada para modernizar la infraestructura bancaria y apoyar la innovación centrada en el cliente. Permite a las instituciones financieras abandonar los sistemas heredados en favor de un modelo SaaS que mejora la velocidad de comercialización y reduce costes. Construida sobre una arquitectura de microservicios con API REST y GraphQL, su plataforma 10x SuperCore procesa más de 100.000 transacciones por segundo por institución. Es utilizada por Chase UK, Old Mutual y Westpac, y ha sido reconocida por Celent por su innovación en banca cloud-native.

El Desafío: Garantizar la Seguridad de la IA sin frenar la Innovación

El equipo de seguridad de 10x Banking necesitaba permitir el uso de la IA sin bloquear sus funcionalidades, monitorizando de forma segura su utilización en toda la organización. Sus necesidades eran:

- Identificación en tiempo real de los datos sensibles compartidos con las herramientas de IA.
- Proteger los datos del acceso no autorizado sin interrumpir los flujos de trabajo.
- Obtener visibilidad sobre las actividades de IA no monitorizadas y los patrones de uso reales.
- Pasar de un enfoque reactivo de bloqueo de riesgos a la habilitación proactiva y segura de la IA.

La Solución

10x Banking seleccionó Prompt Security por sus funcionalidades orientadas a grandes empresas. La plataforma se implementó rápidamente en todos los endpoints mediante una extensión del navegador integrada con los servicios de identidad y seguridad existentes, sin requerir configuraciones manuales ni cambios en los flujos de trabajo. Prompt Security ofreció al equipo:

- Monitorización en tiempo real de las interacciones con la IA por usuario y departamento.
- Redacción y anonimización de datos sensibles antes de enviarlos a la IA.
- Detección de Shadow AI para una adopción segura en lugar de restricciones punitivas.
- Registros contextuales de todas las interacciones para garantizar la trazabilidad y el control.

Los Beneficios

Prompt Security es hoy un componente fundamental de la estrategia de IA de 10x Banking. La empresa continúa ampliando el uso de la IA de forma segura y eficiente, sin aumentar los riesgos ni generar obstáculos para sus equipos.

Comida BYTE TI

Gobierno de datos, ética y cumplimiento normativo

Manuel Navarro

Byte TI, junto con Arsys, organizó un encuentro en el que participaron Javier Paniagua, director de Tecnología y Proyectos en Risi; Iván Molina, subdirector general de Calidad e Innovación en la Consejería de Familia, Juventud y Asuntos Sociales de la Comunidad de Madrid; Rafael Claret Socorro, Head of Data Advanced Analytics en Acciona; Susana Olivares, manager de Preventa de Arsys Cloud Solutions; José Arbués, director del Centro de Inteligencia Institucional en la UCM; David Vaquero, CTO en Nationale-Nederlanden; y José Ignacio Guijarro, director general en The Whiteam Technology Services para hablar de la gobernanza del dato, la cultura interna, el impacto de la IA y el cumplimiento normativo, con una idea compartida: los datos son ya un activo estratégico y su protección exige implicación de la dirección, procesos claros y una visión común entre negocio, tecnología y legal.

El encuentro comenzó con la presentación de Susana Olivares, Manager de Preventa de Arsys Cloud Solutions, que explicó que "Arsys es una compañía europea de servicios de presencia en Internet, hosting gestionado, cloud computing y soluciones de infraestructura TIC que figura entre las compañías líderes en tecnología e innovación en Europa. Nuestro principal objetivo es impulsar la transformación digital y facilitar a las empresas todos los beneficios de la Nube. Para nosotros los datos son el activo más valioso de las empresas. Una brecha de seguridad puede afectar a la reputación y poner en riesgo el futuro de cualquier compañía. Protegerlos adecuadamente y garantizar su privacidad y disponibilidad es uno de los principales compromisos que tenemos con nuestros clientes. Por eso, los proyectos y soluciones alojados en nuestras instalaciones están avalados por las certificaciones de calidad ISO 9001, de seguridad ISO 27001 y el Esquema Nacional de Seguridad (ENS). La certificación Tier III garantiza que nuestro centro de datos es capaz de brindar el máximo nivel de rendimiento, fiabilidad, escalabilidad y disponibilidad y cumple con los más altos estándares de seguridad".

Javier Paniagua, director de Tecnología y Proyectos en Risi, afirmó que "hay gente que está haciendo cosas sin tener en cuenta el apartado de los datos, cuando es algo fundamental y por eso falla".

Por su parte, desde la administración pública, Iván Molina subdirector general de Calidad e

Comida BYTE TI

Gobierno de datos, ética y cumplimiento normativo

David Vaquero, CTO en Nationale-Nederlanden

Iván Molina, Subdirector General de Calidad e Innovación en la Consejería de Familia, Juventud y Asuntos Sociales de la Comunidad de Madrid

Javier Paniagua, Director de Tecnología y Proyectos en Risi

Jose Arbués, Director del Centro de Inteligencia Institucional en UCM

Innovación en la Consejería de Familia, Juventud y Asuntos Sociales de la Comunidad de Madrid insistió en que "el apartado de la cultura de los datos es bastante más difícil" y recordó que "detrás del dato hay una persona", una reflexión que conectó con la vertiente ética del encuentro. Rafael Claret Socorro, Head of Data Advanced Analytics en Acciona, por su parte, subrayó que "el aspecto de que la dirección esté involucrada y a favor de lo que aporta una gobernanza de datos es fundamental, porque si no existe el liderazgo por parte de la dirección, la cultura no arraiga".

José Arbués, director del Centro de Inteligencia Institucional en la UCM, apuntó que la dificultad no está solo en implantar herramientas, sino en lograr una organización orientada al dato: "En mi opinión es muy difícil conseguir que la organización esté orientada al dato. Es un aspecto extremadamente complejo". En esa misma línea, David Vaquero, CTO en Nationale-Nederlanden, explicó que "el apartado de la cultura es fundamental. En este sentido, cada empleado debe asumir una mayor responsabilidad sobre la información que maneja, en lugar de delegarla siempre en el departamento de TI". Tal y como consideraron la mayoría de los asistentes, la gobernanza no puede quedarse en un documento, sino que debe convertirse en una práctica estable y transversal.

Cultura y liderazgo

Uno de los ejes más repetidos fue que la cultura del dato no se impone solo con tecnología. Claret Socorro defendió que "los incentivos y el respaldo de la dirección son claves para que los empleados asuman nuevas rutinas", mientras Arbués resumió el objetivo práctico con una frase muy gráfica: "La parte del gobierno es más eficaz cuanto menos se ven. Es decir, cuando los procesos dejan de ser una fricción diaria, la gobernanza ya se ha integrado de verdad en la organización".

José Ignacio Guijarro añadió una visión muy realista desde la integración tecnológica: "El marco no vale si no le pones cierta inteligencia detrás". También advirtió de que en las empresas pequeñas "hablar de gobernanza del dato puede parecer una quimera, porque muchas personas no saben qué significa eso de la gobernanza del dato". En este sentido, Susana Olivares coincidió en que el reto no es solo técnico, sino también organizativo: "Las compañías suelen descubrir tarde que no tienen todas las áreas cubiertas y que necesitan reglas internas claras para evitar usos improvisados de la información".

Comida BYTE TI

Gobierno de datos, ética y cumplimiento normativo

IA, DORA y riesgo

La irrupción de la inteligencia artificial apareció como acelerador y, al mismo tiempo, como fuente de nuevos riesgos. Vaquero explicó que "DORA es fundamental en nuestro caso porque pone el foco en terceras partes y proveedores, algo decisivo en entornos donde el perímetro tradicional ya no existe". El CTO de Nationale-Nederlanden añadió que "el enfoque correcto pasa por reforzar el modelo de confianza cero", mientras Guijarro remarcó que primero hay que saber "qué datos son prioritarios y qué información puede comprometer realmente a la empresa".

José Ignacio Guijarro,
Director General en The Whiteam Technology Services

Rafael Claret Socorro,
Head of Data & Advanced Analytics en Acciona

Susana Olivares,
Manager de Preventa de Arsys Cloud Solutions

Por su parte, Rafael Claret señaló que "el boom de la IA está trayendo bastante problemas de gestión internos, pero también ventajas en la parte de gobierno de datos". En su experiencia, la IA ha ayudado a demostrar que sin datos de calidad no hay proyectos sostenibles. Iván Molina fue más crítico con la madurez organizativa y explicó que "falta compromiso de la alta dirección, algo que también comprobó al intentar impulsar un protocolo de IA agéntica que quedó obsoleto por falta de empuje interno".

CIO, CISO y DPO

Otro asunto central fue la relación entre las figuras del CIO, el CISO y el DPO. Arbués explicó que en su caso existe una separación funcional clara: "Yo tengo un CIO que implanta sistemas, CISO que protege y DPO que da la cobertura legal". También defendió que, en la práctica, la gobernanza del dato debe ser única, incluso en entornos multicloud, porque el riesgo más grave no siempre es la intrusión, sino la fuga de información. Vaquero coincidió en que la gestión del riesgo debe estar dentro del comité de dirección y no como una función secundaria. "Lo importante es que la política de datos esté impregnada en el comité de dirección", afirmó, al tiempo que explicaba que el DPO, aunque dependa del área legal, debe integrarse en el equipo de gobernanza del dato. Paniagua reforzó esta idea al recordar que el departamento legal es el que suele mover los presupuestos y que marcos como NIS2 ayudan a elevar la importancia de la seguridad a nivel ejecutivo. También se dejó claro que la regulación puede actuar como palanca de cambio. Susana Olivares, de Arsys, relató que el cumplimiento de DORA ha supuesto un reto para muchos clientes y proveedores, pero también una oportunidad para ordenar procesos y elevar el nivel de exigencia. En su opinión, "muchas empresas están descubriendo que, si no establecen un reglamento interno sobre IA, los empleados acaban usando herramientas por su cuenta para ganar productividad".

Finalmente David Vaquero insistió en que el core de muchas compañías ya son los datos, por lo que la gestión del riesgo no puede quedar fuera. Paniagua, por su parte, destacó que sectores como banca o seguros viven en un mundo plenamente digital y que la velocidad de adaptación se ha vuelto un factor competitivo.

Comida BYTE TI

El CISO ante el reto de aplicar Zero-Trust

Byte TI, junto con H&K y Sophos, organizó un encuentro en Sevilla en el que participaron Tomás Ávila, CISO del Ayuntamiento de Ayamonte; David del Río, director de TI en Dental Company; Roberto Bellamy, CIO y CISO en San Telmo Business School; Andrés Delgado, Head of Digitalization & Cibersecurity en BNZ Energy; Eder Barbosa, Modern Workplace & Security Manager en H&K; Alberto González, Director de Sistemas de la Información en Bogaris, e Iván Mateos, Senior Presales Engineer en Sophos.

Manuel Navarro

La conversación giró en torno al reto de implantar Zero-Trust en entornos reales, con especial atención al presupuesto, la simplicidad tecnológica, la formación del usuario, la cadena de suministro y el impacto de normativas como NIS2. Los portavoces de H&K y Sophos defendieron enfoques flexibles, basados en ecosistemas, navegador y servicios gestionados para reducir fricción y reforzar la seguridad.

Para ello, es fundamental la labor que realizan las empresas tecnológicas para ayudar a las empresas y organismos público a implantar una estrategia correcta. En este sentido, Eder Barbosa, Modern Workplace & Security Manager en H&K explicó que "H&K es una consultora tecnológica nacida de la fusión entre HSI y Kiteris, dos compañías con sólida trayectoria en consultoría y tecnología. De esta unión surge una nueva marca que reúne lo mejor de cada una: enfoque estratégico, cercanía con el cliente, excelencia operativa y una cultura tecnológica compartida. El resultado es que formamos un equipo diverso, resolutivo y comprometido, que multiplica la confianza de los clientes y el impacto de la tecnología en sus negocios".

Por su parte, Iván Mateos, Senior Presales Engineer en Sophos explicó que "nosotros somos una compañía que montamos ecosistemas. No pretendemos que alguien elija más de una solución y ahora estamos en un momento de soluciones de MDR y XDR supervisadas. Se está ampliando el modelo operativo agéntico al resto de su porfolio a través de Sophos Central. Las inversiones incluyen la integración de capacidades XDR y SIEM de última generación, la expansión de las capacidades de IA segura para la nueva generación de herramientas de IA para clientes y el lanzamiento de Sophos CISO Advantage en otoño de 2026, que proporcionará orientación estratégica en materia de seguridad a las

Comida BYTE TI

El CISO ante el reto de aplicar Zero-Trust

Alberto González,
Director de Sistemas de la Información en Bogaris

Andrés Delgado,
Head of Digitalization & Cibersecurity en BNZ Energy

David del Río,
director de TI en Dental Company

Eder Barbosa,
Modern Workplace & Security Manager en H&K

organizaciones que no puedan contratar directamente a un CISO. Cada una de estas capacidades opera sobre la misma base de agentes que Sophos MDR ha utilizado a lo largo del último año".

Los retos

Después de la presentaciones Tomás Ávila, CISO del Ayuntamiento de Ayamonte, puso sobre la mesa una de las principales barreras para determinados organismos del sector público como el suyo: "Los ayuntamientos de 25000 habitantes no somos ni grandes ni pequeños, contamos con un presupuesto reducido y además tenemos el problema de la contratación". Según explicó, cuando una solución se adjudica ya puede haber quedado desfasada, lo que complica todavía más avanzar hacia un modelo Zero-Trust. Ávila recordó además que la pandemia supuso un punto positivo de inflexión, porque "obligó a acelerar el trabajo en la nube para habilitar el teletrabajo y replantear la protección de identidades y dispositivos". Pero Ávila también advirtió de la dificultad de convencer a los usuarios cuando se introducen medidas que parecen más incómodas que visibles. "Hay muchos problemas para convencer a la gente de que estás protegiendo a las personas", señaló, y puso como ejemplo la implantación del doble factor, que al principio generó rechazo entre los funcionarios y después terminó normalizándose. Su reflexión encaja con una de las ideas repetidas durante el encuentro como es que la seguridad no fracasa solo por falta de tecnología, sino por falta de adopción.

Crecimiento y riesgo

David del Río, director de TI en Dental Company, explicó que su organización crece "a un ritmo de 25 clínicas por año, lo que obliga a integrar nuevas aperturas y adquisiciones con rapidez. Ese crecimiento genera una superficie de ataque muy amplia. Ahora tenemos 1000 XDR, 300 tablets y también hay que incluir a los smartphones. Es decir, es un parque muy grande que hay que proteger", afirmó. En su opinión, una empresa que crece tan deprisa se convierte en un objetivo prioritario para los ciberdelincuentes, por lo que insistió en no imponer soluciones sin entender antes la necesidad real del negocio.

Roberto Bellamy, CIO y CISO en San Telmo Business School, aportó una visión más pedagógica del problema. "En mi empresa somos ágiles, estables y no tenemos que cumplir determinadas normativas, porque somos pequeños y somos una fundación sin ánimo de lucro", indicó. Aun así,

Comida BYTE TI

El CISO ante el reto de aplicar Zero-Trust

reconoció que la debilidad sigue estando en el usuario y resumió su postura afirmando que "el Zero Trust es la radicalidad en ciberseguridad absoluta. Y me parece la opción correcta. Si hablamos de cero es que debe ser cero. No confiar en nadie y eso implica no establecer excepciones". Bellamy insistió en que la seguridad debe apoyarse en una cultura continua, no solo en herramientas, y explicó que conversa de forma habitual con los empleados para reforzar esa conciencia.

Iván Mateos,
Senior Presales Engineer en Sophos

Roberto Bellamy,
CIO y CISO en San Telmo Business Scholl

Tomás Ávila,
CISO del Ayuntamiento de Ayamonte

Usuario y cadena

Andrés Delgado, Head of Digitalization & Cibersecurity en BNZ Energy, destacó que el perímetro tradicional ya no existe como antes: "Antes el perímetro estaba establecido, pero con el entorno híbrido, el nuevo perímetro es el usuario". Para él, el reto está en combinar formación y control técnico, porque "poner al usuario todo tipo de trabas como el doble factor es fundamental". También alertó sobre la cadena de suministro, un frente que cada vez preocupa más a las compañías con estructuras complejas y proveedores subcontratados, especialmente cuando una mala praxis ajena puede acabar trasladando la responsabilidad a la empresa principal.

Por su parte, Alberto González, Director de Sistemas de la Información en Bogaris, describió una estrategia más orientada a la gobernanza. "Hemos empezado a preparar anexos de ciberseguridad para todos los contratos que se firman en la compañía", explicó, con especial atención a los acuerdos clave y a los procesos de licitación. También detalló que están definiendo una infraestructura común de seguridad para entornos OT e IT, con el objetivo de que toda la arquitectura encaje en el marco normativo de la compañía. Su posición es que "si un proveedor no cumple, no entra; y si afirma cumplir pero luego incumple, se le penaliza".

Gobernanza y cultura

A lo largo del debate apareció varias veces la idea de que Zero-Trust no es una herramienta aislada, sino una forma de ordenar el acceso, reducir la confianza implícita y obligar a revisar procesos, identidades y proveedores. Iván Mateos recordó que la propuesta de Sophos busca simplificar el acceso centralizando y mejorar la experiencia en el navegador, mientras que Barbosa de H&K defendió una consultoría que construye ecosistemas y evita forzar al cliente a multiplicar soluciones. En paralelo, los participantes coincidieron en que la formación es clave: "Hay que adoctrinar al usuario final de una forma sutil, independientemente de la herramienta que se utilice", resumió Barbosa.

El encuentro dejó también una advertencia sobre la gobernanza de la inteligencia artificial y la multiplicación de vulnerabilidades. En ese contexto, la mesa concluyó que el éxito de Zero-Trust depende menos del eslogan y más de la capacidad de combinar simplicidad, control, cultura y priorización. La última idea quedó bien resumida en una de las intervenciones finales de Andrés Delgado: "El empleado debe ser la prioridad porque las herramientas las tenemos."

Comida BYTE TI

El CISO ante el reto de aplicar Zero Trust y una correcta gestión de la ciberseguridad

El modelo de seguridad Zero Trust se ha consagrado como el nuevo estándar clave para poder afrontar las amenazas de ciberseguridad que sufren hoy en día las organizaciones. De alguna manera, se ha convertido en el nuevo estándar de facto para proteger entornos digitales híbridos y dinámicos. Según un reciente estudio publicado por DXC Technology bajo el título "The Trust Report: From Risk Management to Strategic Resilience in Cybersecurity", el 83% de las organizaciones que han adoptado un modelo Zero Trust han logrado reducir los incidentes de seguridad, contribuyendo a una disminución significativa de los costes de recuperación y del soporte técnico asociados a los ciberataques.

Alfonso Casas

Con el fin de conocer cómo lo están adoptando las compañías, la Revista Byte TI junto a ESET España y Ray Security que actuaron de patrocinadores, organizaron un almuerzo con expertos del sector bajo el título "El CISO ante el reto de aplicar Zero Trust y una correcta gestión de la ciberseguridad". En un contexto marcado por la sofisticación de las amenazas, la creciente digitalización y la apertura a nuevos entornos tecnológicos, garantizar la seguridad ya no es solo una cuestión técnica, sino también de continuidad de negocio.

La mesa redonda estuvo moderada por Ignacio Sáez, editor y director general de MKM

Comida BYTE TI

El CISO ante el reto de aplicar Zero Trust y una correcta gestión de la ciberseguridad

Alejandro Aliaga,
CTO de ESET España

Alfredo Delgado, Director de Transformación y Tecnología CIO CTO CISO de UMAS, Mutua de Seguros

Daniel Damas,
Head of IT Assurance & CISO en Nationale Nederlanden

David Hernan Gallardo, Subdirector Centro de Operaciones de Seguridad de la Información en MAPFRE

Publicaciones, a la que se unieron los siguientes CISOs y responsables de seguridad: Alfredo Delgado, director de Transformación y Tecnología, CIO, CTO, CISO de UMAS, Mutua de seguros; Daniel Damas, Head of IT Assurance & CISO en Nationale Nederlanden; David Moreno, CISO de Tendam Retail; Manuel Asenjo, CIO/CISO/CAIO en Ecija; David Hernan Gallardo, subdirector Centro de Operaciones de Seguridad de la Información en MAPFRE SA; Jaime Perea Amor, responsable de Gestión de Riesgos y Continuidad de Negocio en Carrefour; Alejandro Aliaga, CTO de ESET España; y Félix Prieto, Iberia & LATAM RSM en Ray Security.

Zero Trust y el cambio cultural que es necesario aplicar

Los participantes comenzaron exponiendo qué significa para ellos el concepto de Zero Trust y cuáles son los principales retos que supone su implementación. Un aspecto común para la mayoría de ellos comentó es que Zero Trust no es una tecnología nueva que se pueda adquirir e implantar de la noche a la mañana. Es, ante todo, una filosofía y un cambio cultural profundo que obliga a replantear cómo se gestionan los accesos, las identidades y los datos dentro y fuera de las organizaciones.

David Hernán Gallardo, subdirector del Centro de Operaciones de Seguridad de MAPFRE, resumió con claridad el núcleo del problema: la identidad se ha convertido en el nuevo perímetro. "En estos últimos años la seguridad de las compañías se ha centrado en ofrecer garantías de seguridad en la identidad, el nuevo perímetro, y es necesario securizar la identidad del usuario para proteger a la empresa de la mejor manera posible", señaló. A ello añadió la complejidad del legacy tecnológico y la necesidad de añadir capas de seguridad que, a menudo, generan reticencias entre los usuarios.

Para David Moreno, CISO de Tendam Retail, "Zero Trust no es una tecnología nueva. La filosofía de no fiarse de nadie y tener que orquestar lo que pasa en casa es algo básico. Es un cambio cultural de tecnología y del departamento de sistemas, pero no debe serlo para la compañía. Mi reto es que el impacto en el usuario sea mínimo y que lo perciba como una mejora".

Daniel Damas, CISO de Nationale Nederlanden, incidió en la dificultad de implementar este

Comida BYTE TI

El CISO ante el reto de aplicar Zero Trust y una correcta gestión de la ciberseguridad

David Moreno,
CISO de Tendam Retail

Felix Prieto,
Iberia&LATAM RSM en Ray Security

Jaime Perea Amor,
Responsable de Gestión de Riesgos y Continuidad de Negocio en Carrefour

Manuel Asenjo,
CIO, CISO y CAIO en Ecija

cambio cultural: "Es un cambio bastante difícil de implementar, de manera que trates continuamente de legitimar los accesos y segmentar los servicios. Los comportamientos de los usuarios son clave dentro de una política Zero Trust".

Por su parte, Alfredo Delgado, de UMAS, Mutua de Seguros, comentó que ve a Zero Trust como una oportunidad para las organizaciones: "Lo veo como una oportunidad y un cambio transformacional en la empresa. Obliga a que los usuarios se sensibilicen y cambien determinados procesos. Es también un cambio de gobierno que trasciende más allá de lo meramente tecnológico".

Alejandro Aliaga, CTO de ESET España, aportó una perspectiva integradora clave al debate, subrayando que la estrategia de Zero Trust no consiste en inventar algo nuevo, sino en poner en común tecnologías ya existentes con una visión unificada. "La estrategia de Zero Trust es coger muchas tecnologías que ya estaban y ponerlas en común para proteger el perímetro común, que quizás ya estaba difuminado. Por parte de los fabricantes, la estrategia pasa por hacer las cosas más sencillas y trasladar a la dirección cuáles son verdaderamente los riesgos para adoptar la tecnología adecuada. Hay que hacérselo fácil al usuario, fomentar el cambio cultural y que el usuario vea que no hay fricción", señaló.

Jaime Perea, responsable de Gestión de Riesgos en Carrefour, añadió la dimensión de la identidad y los roles como uno de los grandes retos operativos: "Gestión de identidades, por supuesto. Zero Trust exige una implicación por parte de toda la empresa para ser capaz de identificar los roles. Muchos roles implican mayor complicación." Y Manuel Asenjo, de Ecija, señaló que en su caso el dato del cliente es el verdadero centro de gravedad: "Para nosotros, Zero Trust es el dato del cliente.""

El inventario y la priorización de activos: la asignatura pendiente

Uno de los momentos que mayor interacción produjo fue el hecho de abordar la cuestión del inventario de activos. Llevan décadas siendo el punto de partida de cualquier estrategia de seguridad y, sin embargo, siguen siendo el talón de Aquiles de las organizaciones.

Comida BYTE TI

El CISO ante el reto de aplicar Zero Trust y una correcta gestión de la ciberseguridad

David Hernán Gallardo lo describió con precisión: "El inventario es la pieza fundamental para saber qué proteger. Con la llegada de DORA y demás regulaciones, parece que el inventario se ha quedado olvidado. Hemos protegido de forma tradicional todo lo de on-premise y con la adopción del cloud y el término time to market, se deja de lado y no se tiene control de la superficie global de ataque".

David Moreno, de Tendam Retail, no ocultó su frustración: "Llevo trabajando 30 años en temas de tecnología. Después de 25 años seguimos hablando de lo mismo: el inventario. No sabemos exactamente lo que hay. Las exigencias ahora son mayores y la tecnología más compleja de aplicar. Es un tema cultural". Una reflexión que encontró eco en Alfredo Delgado: "En el caso de DORA, es negocio con los datos de impacto el que tiene que definir y hacer un plan de continuidad para priorizar servicios", dijo.

En este punto, Félix Prieto, Iberia & LATAM en Ray Security, señaló un punto de vista diferenciador basada en el uso de la inteligencia artificial para resolver precisamente el reto de la priorización dinámica de activos y permisos. "Aplicando técnicas de algoritmo e IA podemos definir, en tiempo real, cuáles son los datos que están siendo usados y cuáles no. El 94% de los datos no son usados por las compañías. Desde Ray Security ayudamos al control de los accesos de forma dinámica, especialmente con los permisos que están abiertos y no autorizados, para que se revoquen, o para predecir futuros posibles permisos con técnicas de IA. Damos una especie de add-on al control y la securización para minimizar la superficie de riesgo de ataque".

La conversación derivó hacia el papel de la normativa como palanca de concienciación. Daniel Damas se mostró defensor de normativas como DORA y otras similares: "Vino a cambiar algo que antes era solo responsabilidad del CISO. Ahora, los directores son responsables, y los temas penales no van únicamente contra los CISOs. La conversación antes y después de DORA es muy diferente". Alejandro Aliaga, de ESET, reforzó esta idea señalando que la regulación debe hacerse a favor de las organizaciones: "Hay que exponérselo así a la alta dirección. La certificación te hace estar en un entorno de mejora continua para la organización".

El CISO: de su labor técnica a socio estratégico entre negocio y seguridad

Otro de los ejes del debate fue la evolución del rol del CISO. La ciberseguridad ha dejado de ser un asunto exclusivamente técnico para convertirse en una cuestión de negocio. Y eso exige un perfil diferente: capaz de hablar el idioma de la dirección, de traducir riesgos técnicos en impactos económicos y reputacionales, y de construir alianzas internas.

Jaime Perea lo explicó de la siguiente manera: "Es un problema de lenguaje. Los de sistemas no siempre son capaces de trasladar lo que realmente es necesario. El CISO ha cambiado porque tiene que hablar un idioma nuevo con soft skills". David Hernán Gallardo coincidió: "Cuando eres capaz de contarle a negocio lo que puede suceder, o con las auditorías internas que se realizan, es cuando puedes conseguir que el presupuesto sea mayor".

La transparencia también fue comentada entre los asistentes como un activo estratégico. Hernán Gallardo señaló que "la transparencia a la hora de gestionar un ataque y llevar a cabo una buena comunicación de lo que te pase también ayuda a afrontarlo con naturalidad. Nadie está exento de sufrirlo". Félix Prieto añadió que en las empresas donde ya se ha sufrido un ciberataque, la dirección es mucho más consciente, pero advirtió: "¿Y los que no han sido atacados? Hay empresas de gran calado con la idea de que a ellos no les va a tocar".

Para Alejandro Aliaga de ESET España, todos los procedimientos, la cultura y la comunicación a la alta dirección se vuelven fundamentales

Comida BYTE TI

El CISO ante el reto de aplicar Zero Trust y una correcta gestión de la ciberseguridad

para cualquier proceso. Cómo ellos quieren hacer esas inversiones para evitar la sensación de riesgo. "Tenemos que hacerles conscientes e implicarles hablando su idioma, con números, y exponiendo las consecuencias técnicas, legales y reputacionales".

Daniel Damas compartió una iniciativa concreta para concienciar desde dentro: "En la compañía realizamos simulaciones internas de ataques de ransomware para poner a prueba a los empleados, siendo desplegadas sobre 650 equipos. El mayor problema no es el CEO, que está muy concienciado, sino proviene de gerencia o de los departamentos de finanzas. "Alfredo Delgado añadió que en sus últimas campañas de phishing, todo el mundo suele caer en enlaces que simulan ser de OneDrive; "Zero Trust ha demostrado una alta eficacia a la hora de bloquear e impedir este tipo de ataques".

La cadena de suministro sigue siendo el eslabón más débil

La mesa dedicó especial atención a la gestión de terceros como uno de los vectores de riesgo más críticos y menos controlados. La cadena de suministro amplía la superficie de ataque de forma exponencial, y muchas organizaciones aún no han encontrado la manera eficaz de gestionarla dentro de su estrategia Zero Trust.

Jaime Perea fue muy descriptivo al respecto: "La cadena de suministro es tan fuerte como sus eslabones. Manejamos procesos críticos con contratos o negocio, y el problema es que el enemigo muchas veces está dentro porque no cumple con determinados requisitos y no se cambia. Cualquier regulación con gestión de terceros lo pone en el foco. Es imprescindible cuidar este apartado".

David Moreno explicó cómo Tendam está abordando esto tecnológicamente: "A día de hoy nos apoyamos mucho en la revisión y cumplimiento contractual, junto con una revisión anual esperando que el proveedor sea sincero, apoyado con auditorías. A nivel tecnológico, estamos reemplazando accesos punto a punto con navegadores protegidos y máquinas virtuales". Hernán Gallardo destacó que el problema se agrava con las pymes de la cadena de valor: "También están obligadas a cumplir con la normativa, y eso supone un problema mayor por contar con menos recursos".

Alfredo Delgado añadió una reflexión sobre la concentración que esto puede generar en el mercado: "Iremos al proveedor que ya esté en una lista verde de cumplimiento. La pequeña empresa, que carece de infraestructura adecuada, perderá competitividad".

Para Félix Prieto de Ray Security, los ataques vienen a través de terceros poco protegidos. "La empresa tiene que priorizar sus problemas a nivel de negocio y tener un rigor muy exhaustivo y dinámico utilizando técnicas de IA predictiva sobre todos los controles de acceso: qué tengo del pasado, qué no se usa, y con Zero Trust analizar qué puede venir en el futuro. Es un tema de priorización", enfatiza.

La IA generativa como el nuevo paradigma de riesgo y control

La última parte del debate se adentró en el territorio más disruptivo: la confluencia de Zero Trust con la inteligencia artificial generativa y los agentes autónomos. Un escenario que plantea desafíos radicalmente nuevos para la gestión de identidades y el control de accesos.

David Hernán Gallardo expuso una reflexión que caló entre los asistentes: "Los agentes no dejan de ser un empleado más de la organización, pero con funciones potenciadas y una mayor velocidad de ejecución. Operan en modo 24x7, con lo que el control y la monitorización deben ser constantes. Volvemos al problema de tener que controlar tanto a los humanos como a los agentes".

Daniel Damas fue más allá, planteando la complejidad técnica que esto supone: "Un comercial va con un agente de IA con acceso legítimo a información del cliente. Esto se

Comida BYTE TI

El CISO ante el reto de aplicar Zero Trust y una correcta gestión de la ciberseguridad

resuelve con tecnologías nuevas como Open FGA, una plataforma de código abierto diseñada para gestionar permisos y políticas de autorización complejas la cual se construye dinámicamente de la cartera del agente. Supone un paradigma nuevo para la compañía, meternos en las entrañas para que la IA sepa si la persona que está en el chat tiene acceso a nivel de registro". Y en cuanto a la protección frente a prompt-injection, Damas reconoció: "Todos los días hay una forma nueva de atacarte con la IA. Es potente en ambos sentidos".

Manuel Asenjo advirtió del escenario futuro: "Cuando los agentes de IA interactúen entre sí de forma autónoma —sin intervención humana en cada paso— los ataques de prompt-injection se volverán mucho más difíciles de detectar y contener, porque no habrá un humano que pueda identificar el comportamiento anómalo. Un agente podrá ser manipulado por otro agente malicioso pasando desapercibido".

Alejandro Aliaga, de ESET, recalcó el incremento de vectores de entrada que trae consigo la IA y la importancia de extender las medidas de seguridad ya existentes a estos nuevos contextos. "Ahora vamos a tener muchos más puntos de entrada: el correo electrónico, un asistente que resume los correos, una API que autorizas y que puede ser otro punto de entrada de ataque, librerías LLM de dudosa procedencia... Muchos de los problemas con IA podemos extrapolarlos a problemas que ya teníamos previamente. El problema base es el mismo, pero hay que usar las nuevas herramientas para combatirlo".

Félix Prieto, de Ray Security, cerró este bloque subrayando que Zero Trust, por sí solo, no es suficiente ante los retos que plantea la IA: necesita capas adicionales de control del dato. "Zero Trust es importante, pero no solo en acceso, sino en quiénes están accediendo a esos datos, con qué criticidad y en qué momento. Zero Trust pone herramientas de control, pero hay que controlar los datos de forma dinámica, especialmente con la llegada de la IA. Zero Trust necesita de otras capas a su alrededor que aborden también el control de acceso y la gestión del dato"

Alejandro Aliaga, CTO de ESET España, lanzó un mensaje de fondo que apunta a la gobernanza como principio rector: cada nueva tecnología que entra en la organización debe ser gobernada desde el primer momento, no prohibida. La ciberseguridad eficaz no pasa por bloquear la innovación, sino por controlarla con criterio. Félix Prieto, de Ray Security, incidió en la necesidad de un control dinámico y predictivo del acceso a los datos, especialmente en un entorno donde la IA amplía la superficie de riesgo de forma continua.

Conclusiones y puntos clave del debate

Aunque la mayoría de los responsables de TI reconoce el valor estratégico del modelo Zero Trust, su implementación total sigue siendo un proceso lento y desigual. Así, los CISOs identifican los sistemas heredados legacy como la principal barrera para su mayor adopción, tanto por la falta de interoperabilidad como por los costes de modernización que implica su sustitución o integración. A esta limitación técnica se suman factores organizativos.
En muchos casos, los departamentos de ciberseguridad operan de forma fragmentada respecto al resto de la estructura, lo que dificulta la coherencia en las políticas de acceso y control

Los participantes en la mesa dejaron claro que Zero Trust es un camino que exige visibilidad sobre los activos, control de las identidades y los datos, cultura organizativa orientada a la seguridad, y una conversación fluida entre los departamentos de tecnología y negocio.
En un entorno donde los agentes de IA, la computación cuántica y las amenazas persistentes avanzan a velocidad de vértigo, la pregunta ya no es si una organización será atacada, sino cuándo, y cuán preparada estará para poder responder.

Webinars BYTE TI

El impacto de la IA y los agentes autónomos en la empresa

Manuel Navarro

Gustavo Frega, Senior Academic Strategy & Business de ISACA, y Carlos Manuel Toledo, Chief Product Officer de Datadope, analizaron en un webinar el grado de madurez de la inteligencia artificial en la empresa, el salto del piloto a la implantación real, el papel de los agentes autónomos, el riesgo de una posible burbuja y la necesidad de combinar innovación con control humano.

El encuentro dibujó un panorama de avance real pero desigual donde las grandes compañías y los sectores que están muy digitalizados ya exploran despliegues ambiciosos, mientras que la pyme sigue moviéndose con más cautela y con menos capacidad para transformar procesos a gran escala. En ese escenario, los ponentes destacaron que la IA es una tecnología que empieza a tocar operaciones, modelos de negocio y estructuras organizativas, aunque todavía convive con expectativas sobredimensionadas y con demasiadas pruebas de laboratorio que no llegan a producción.

La primera idea que dejó el debate es que la madurez de la IA depende mucho del tamaño de la empresa y del nivel de ambición con que se adopta. Gustavo Frega, Senior Academic Strategy & Business de ISACA subrayó que "la IA ya forma parte del día a día empresarial, pero que las grandes corporaciones han avanzado mucho más rápido que el tejido pyme, especialmente en España, donde este último concentra la mayor parte del mercado. Esa brecha no solo refleja diferencias presupuestarias, sino también de cultura, de capacidad técnica y de velocidad para convertir la innovación en valor tangible".

Por su parte, Carlos Manuel Toledo, Chief Product Officer de Datadope, coincidió "en que muchas organizaciones han quedado atrapadas en la fase del piloto. El problema no es tanto experimentar como quedarse ahí, sin dar el paso hacia una implementación que resuelva dolores reales del negocio". Tal y como expuso Toledo, "la IA se está usando sobre todo para optimizar costes y tareas, pero aún son pocas las empresas que se plantean un cambio de modelo organizacional comparable al que en su día provocó la transformación digital.

Webinars BYTE TI

El impacto de la IA y los agentes autónomos en la empresa

Uno de los aspectos que caracterizan al uso de la Inteligencia Artificial en las empresas en la actualidad es el exceso de expectativas

Carlos Manuel Toledo,
Chief Product Officer de Datadope

Gustavo Frega,
Senior Academic Strategy & Business de ISACA

Agentes con control

Uno de los ejemplos que se pusieron durante la celebración del webinar es el de una startup que desarrollaba una agencia de viajes apoyada en agentes inteligentes casi autónomos, capaces de emitir tickets, recomendar viajes y sustituir parte del trabajo humano operativo. Toledo lo presentó como una muestra de cómo la IA puede habilitar modelos de negocio radicalmente distintos y centrados en desarrollar procesos más eficientes. Se trata de un planteamiento que Toledo lo comparó con los bancos digitales, que no eliminaron a las entidades tradicionales, pero sí obligaron a toda la industria a innovar y a rebajar fricciones para el usuario.

Aun así, Frega introduce un matiz decisivo: la autonomía total sigue necesitando supervisión humana. Aunque valora el potencial de estos modelos, defendió que "en ciertas tareas todavía debe existir una capa de control para evitar errores, sesgos o decisiones que no deberían dejarse completamente en manos de una máquina". En definitiva y tal y como expuso el portavoz de ISACA, "la IA avanza, pero la empresa no puede renunciar a los mecanismos de validación, trazabilidad y responsabilidad".

Uno de los aspectos que caracterizan al uso de la Inteligencia Artificial en las empresas en la actualidad es el exceso de expectativas. En este sentido, el portavoz de Datadope reconoce que existe inversión real en IA y que sus aplicaciones llevan años presentes en ámbitos como el reconocimiento facial o los algoritmos de recomendación, aunque la conversación pública se haya intensificado sobre todo desde la irrupción de la IA generativa. Tal y como expuso, "el mercado necesita distinguir entre automatización clásica e inteligencia artificial auténtica, porque no todo lo que se vende como IA responde a capacidades realmente inteligentes".

Para Frega, estamos en una especie de dejavu y sitúa la situación actual con la burbuja de las puntocom de principios de siglo. A su juicio, "la IA tiene el potencial de cambiar el paradigma de trabajo y de vida de forma tan profunda como lo hizo Internet, pero también arrastra tres riesgos que merecen atención: valoraciones desorbitadas, omnipresencia del etiquetado "powered by AI" y, sobre todo, costes crecientes de infraestructuras, centros de datos y energía". Su diagnóstico no afirma que la burbuja en torno a la IA ya exista, pero sí advierte de que puede formarse si la industria no ajusta promesas, gasto y resultados.

Webinars BYTE TI

El impacto de la IA y los agentes autónomos en la empresa

Ese punto de vista encuentró eco en Toledo, que insistió en que "el mercado está entrando en una fase de depuración del hype. Las compañías que sobrevivirán serán las que aporten inteligencia artificial real, con casos de uso útiles y medibles, no las que simplemente incorporen la etiqueta al discurso comercial". Tal y como expuso, "este filtro no es una mala noticia, sino una señal de madurez: el sector empieza a premiar más los resultados que las promesas".

Un ciclo más largo

Toledo insistió en que la inteligencia artificial "no es una novedad repentina, sino una tecnología con una trayectoria larga, con fases de avance, promesas excesivas y correcciones posteriores. La IA nació más o menos allá en los años 50, junto con la computación y ya atravesó el primer invierno de en los años 60-70, seguido de un segundo periodo de enfriamiento que se extendió hasta los años 90 aproximadamente". Tal y como explicó esa sucesión de entusiasmos y retrocesos sirve para contextualizar el momento presente y para evitar conclusiones apresuradas sobre el estado real de la tecnología.

A partir de ahí, el Chief Product Officer de Datadope, defendió que esta vez hay una diferencia esencial respecto a los ciclos anteriores: "Hoy es masivo, está en toda la sociedad y, además, ya estamos resolviendo casos reales". Según dijo, esa es la gran frontera con etapas pasadas, cuando buena parte de las promesas quedaban encerradas en el terreno académico. En su intervención, insistió en que no cree que se repita un escenario como los anteriores inviernos de la IA "precisamente porque ya no se trata solo de investigación o de expectativa, sino de usos concretos que están entrando en la vida empresarial y social", concluyó

> **Hoy la IA no vive en un laboratorio aislado ni es una promesa. Es una tecnología que ya ha demostrado capacidad de transformación**

Gustavo Frega, Senior Academic Strategy & Business de ISACA, recogió esa idea desde otra perspectiva y la conectó con el funcionamiento exponencial de las tecnologías emergentes. Señaló que "el arranque de herramientas como ChatGPT mostró una adopción masiva en muy poco tiempo", pero también advirtió de que el "uso real cae, aunque no lo haga en picado". Su observación no niega el valor de la tecnología, sino que invita a distinguir entre el impacto inicial y la consolidación posterior, cuando el entusiasmo se enfría y solo permanecen los usos verdaderamente útiles.

Frega también subrayó que, aunque los casos de uso hoy son "menos etéreos" que en la crisis de las puntocom, el riesgo sigue ahí si no se actúa con prudencia. Mencionó además la presión que están ejerciendo los "despidos masivos" y la sustitución de capital humano por agentes de inteligencia artificial, aunque matizó que ya se están viendo empresas que "están dando marcha atrás". Esa coexistencia de impulso y rectificación, según su lectura, es precisamente la señal de que el mercado todavía está buscando su equilibrio.

En ese marco, Toledo cerró el encuentro con una síntesis: "Hoy la IA no vive en un laboratorio aislado ni en una promesa futura, sino en una tecnología que ya ha demostrado capacidad para transformar sectores, productos y procesos. La historia de la IA avanza por ciclos, pero el actual parece más resistente que los anteriores porque está sostenido por casos de uso reales, una adopción transversal y una presión empresarial por resultados, no solo por expectativas".

Comparativa

Servidores para el centro de datos

El mercado de servidores para los centros de datos atraviesa una etapa de crecimiento excepcional, impulsada por el auge de la inteligencia artificial, la evolución de las infraestructuras cloud y la generalización de arquitecturas aceleradas mediante GPU. En este escenario, según datos del Worldwide Quarterly Server Tracker de International Data Corporation (IDC), los ingresos totales a nivel mundial ascendieron a 112.400 millones de dólares en el trimestre de 2025, un aumento del 61 % en comparación con el mismo período del año anterior. En cuanto a su distribución, diversos análisis coinciden en que los servidores rack siguen siendo la tipología dominante, con una cuota cercana al 47% gracias a su equilibrio entre densidad de cómputo, escalabilidad y compatibilidad con aceleradores GPU.

Evolución y adaptación

Los servidores se han convertido en un componente estratégico dentro de la infraestructura del centro de datos donde factores como el rendimiento, la eficiencia energética y la capacidad de adaptación determinan la idoneidad de cada arquitectura en un entorno en continua transformación.

Comparativa

Servidores para el centro de datos

Así, la propia definición de lo que es un servidor ha ido transformándose: ya no se entiende ni concibe solo como un sistema informático de propósito general capaz de ejecutar cualquier tipo de tarea, sino como una plataforma especializada para procesar cargas de trabajo específicas con la máxima eficacia posible.

Esta progresión ha venido acompañada de la consolidación de arquitecturas cada vez más diversas, donde la presencia de GPUs de alta densidad, memorias de elevado ancho de banda y sistemas de almacenamiento NVMe de baja latencia se han convertido en un elemento esencial de los diseños más avanzados, especialmente en entornos destinados a la inteligencia artificial y la computación de alto rendimiento.

Edge computing

El edge computing está trasladando parte del procesamiento de datos fuera del centro de datos tradicional, aproximándolo al lugar donde se generan. Este enfoque está impulsando la demanda de servidores compactos, robustos y energéticamente eficientes, capaces de operar en entornos como fábricas, hospitales, comercios o infraestructuras urbanas, a menudo con condiciones exigentes. Dentro de este contexto, el servidor deja de estar vinculado exclusivamente al CPD para convertirse en un recurso distribuido dentro de una arquitectura híbrida, en la que el procesamiento inmediato se realiza en el borde de la red, mientras que el centro de datos o la nube siguen asumiendo funciones de almacenamiento, coordinación y análisis a gran escala. Como resultado, se consigue reducir la latencia, optimizar el uso del ancho de banda y disminuir la dependencia de la infraestructura centralizada, sobre todo en aplicaciones que requieren una respuesta en tiempo real.

Eficiencia energética

Es otro de los grandes ejes al hablar de los servidores para el centro de datos y ello ha obligado a que los fabricantes replanteen sus estrategias de refrigeración, alimentación eléctrica y diseño térmico. En paralelo, la gestión de los servidores también se está simplificando gracias a modelos más automatizados y centralizados. Las plataformas unificadas, las actualizaciones gestionadas por políticas y los despliegues remotos sin intervención física reducen la complejidad, como en los entornos con muchos equipos distribuidos.

Comparativa

Servidores para el centro de datos

Cisco UCS C220 M8 Rack Server

La multinacional norteamericana propone un servidor en rack de 1RU y dos sockets diseñado para ofrecer un desempeño sólido en entornos de trabajo con un espacio limitado. Adecuado para una amplia variedad de cargas en el centro de datos como, por ejemplo, virtualización, colaboración y aplicaciones bare-metal, está equipado con los últimos procesadores Intel Xeon 6 que brindan dos características clave: nuevas capacidades de seguridad para máquinas virtuales y un mayor rendimiento con funciones aceleradas por inteligencia artificial.

En concreto, Cisco UCS C220 M8 Rack Server soporta hasta dos procesadores Intel Xeon 6700P o 6500P, con 32 ranuras DIMM (16 por CPU) que admiten una memoria DDR5 de hasta 6.400 MT/s para un máximo de 4 TB de memoria, o MRDIMMs de hasta 8.000 MT/s. Mientras, sus ranuras PCIe Gen5 garantizan una entrada/salida de alta velocidad para tarjetas de expansión, con capacidad para hasta tres slots half-height o dos full-height, además de ranuras dedicadas para RAID y conectividad mLOM/OCP 3.0. En la práctica, esto aporta a las empresas flexibilidad para distintas configuraciones y necesidades de rendimiento.

El servidor de Cisco destaca también por soportar hasta tres GPU single-wide, una característica útil para acelerar cargas de trabajo de inteligencia artificial y análisis de datos. A ello se suma un sistema de almacenamiento interno flexible, con capacidad para integrar hasta 10 unidades SFF SAS/SATA/NVMe U.3 o, en su defecto, con opción de hasta 16 unidades E3.S 1T NVMe conectadas directamente mediante PCIe Gen5 x4. ¿El objetivo? Combinar velocidad, densidad y escalabilidad en entornos empresariales exigentes. Y es que, en su conjunto, esta máquina proporciona una arquitectura de almacenamiento y conectividad versátil apoyada (entre otros) por un controlador RAID tri-modo modular de 24 Gbps compatible con SAS 4 y RAID de hardware NVMe, junto a un adaptador SAS HBA que aporta capacidad de adaptación en distintos escenarios de despliegue.

En el apartado de fiabilidad operativa, la presencia de fuentes de alimentación redundantes y hot-swap en diversas configuraciones de eficiencia (platinum y titanium), están orientadas a garantizar la máxima disponibilidad. Todo ello se complementa con las plataformas de gestión Cisco Intersight y Cisco IMC que admiten la administración centralizada del servidor tanto en modo standalone como en entornos híbridos y multicloud. Mientras tanto, los servicios Cisco Smart Net Total Care y Cisco Solution Support agilizan la resolución de incidencias en entornos multiproveedor frente al soporte estándar.

Por otro lado, este modelo extiende las capacidades del porfolio de servidores en rack Cisco UCS apostando por aceleradores integrados como Intel Trust Domain Extensions (TDX), Intel Data Streaming Accelerator (DSA), Intel QuickAssist Technology (QAT), Intel Advanced Matrix Extensions (AMX) e Intel In-Memory Analytics Accelerator (IAA); la finalidad es mejorar en términos de seguridad, rendimiento y eficiencia, y contribuir a los objetivos de sostenibilidad de las organizaciones.

Promete, finalmente, reducir los gastos operativos en energía, refrigeración y mantenimiento al consolidar servidores de generaciones anteriores en una plataforma más eficiente. Incluye garantía de hardware de tres años con reemplazo en el siguiente día laborable y 90 días de garantía de software.

Cisco

contacto

www.cisco.com/c/es_es

A consultar

Comparativa

Servidores para el centro de datos

Dell PowerEdge XE774X

La consolidación de cargas, la explosión de la IA generativa y la 'presión' por reducir el consumo energético están redefiniendo el centro de datos. En este contexto, la familia Dell PowerEdge ofrece a las empresas dos líneas claramente diferenciadas pero complementarias: la XE que está orientada a la aceleración de la GPU e IA a gran escala, y la R o formato enrackable tradicional optimizada para la virtualización, bases de datos y otros servicios de computación de propósito general.

Dentro de su portafolio para entornos de inteligencia artificial avanzada destacan los modelos de la gama PowerEdge XE774X, lanzados en la última generación de servidores Dell. En ella, los PowerEdge XE7740 y los PowerEdge XE7745 son opciones a valorar cuando el objetivo es maximizar la densidad de GPU y el rendimiento por rack, manteniendo al mismo tiempo la refrigeración por aire.

PowerEdge XE7740 y XE7745 son servidores 4U de dos sockets que han sido diseñados de manera específica para IA, GPU computing y computación de alto rendimiento (tecnología que se conoce también por las siglas HPC). Aunque comparten una arquitectura que es muy similar, se diferencian en la plataforma del procesador.

En este caso, los servidores XE7740 admiten hasta dos procesadores Intel Xeon 6 de nueva generación, con un máximo de 86 núcleos por CPU y 32 ranuras DDR5 RDIMM (hasta 4 TB de memoria a 6.400 MT/s). Por su parte, la configuración de los servidores XE7745 soporta hasta dos AMD EPYC 9005 de 5ª generación, con hasta 192 núcleos Zen 5 por CPU y 24 ranuras DDR5 RDIMM (hasta 3 TB).

Hecha esta aclaración, cabe señalar que ambos admiten configuraciones de GPU de alta densidad, con soporte para hasta 8 GPUs PCIe de doble ancho y 600 W —como NVIDIA RTX Pro 6000 Blackwell, H200 NVL o Intel Gaudi 3—, o bien hasta 16 GPUs de ancho simple (75 W) en escenarios orientados a una inferencia de muy alta densidad. Esta capacidad se complementa con hasta 8 unidades NVMe E3.S Gen5 en el frontal, con una capacidad total de hasta 122,88 TB, que están orientadas a alimentar estas cargas con baja latencia y alto ancho de banda.

En conjunto, esta arquitectura refuerza su propuesta de ofrecer máxima aceleración de IA en un chasis de 4U refrigerado por aire, sin necesidad de recurrir a configuraciones SXM más complejas ni a la refrigeración líquida. Esto

lo que hace es simplificar la adopción de IA en los centros donde las limitaciones de potencia por rack y de infraestructura de refrigeración suelen ser el principal condicionante; un enfoque que habilita casos de uso como el fine-tuning y despliegue de modelos de IA generativa, la inferencia de LLMs y modelos de visión con baja latencia, así como entornos HPC de GPU densa orientados a simulación, gemelos digitales o analítica avanzada.
En resumen, el XE7740 se posiciona para entornos estandarizados basados en Intel, mientras que el XE7745 eleva el techo de cómputo con procesadores AMD EPYC 9005, resultando adecuado para cargas mixtas que combinan procesamiento intensivo en CPU con aceleración mediante GPU.

Dell
www.dell.es
900 816 516
A consultar

Comparativa

Servidores para el centro de datos

HPE ProLiant DL145 Gen11

HPE participa en esta comparativa con un servidor para el centro de datos que viene con el procesador AMD EPYC (serie 8004) y que ha sido desarrollado para proporcionar un rendimiento fiable en el extremo, con amplia tolerancia a las temperaturas, filtración de aire, resistencia a las vibraciones, seguridad reforzada y gestión sencilla.

Entrando en detalle, el ProLiant DL145 Gen11 es un equipo edge que quiere garantizar a las compañías un rendimiento de clase empresarial, capacidades de aceleración de IA y una fiabilidad robusta, todo ello en un formato 2U silencioso y eficaz en costes. Con hasta 64 núcleos eficientes, soporte para PCIe Gen5, almacenamiento EDSFF de alto rendimiento y compatibilidad con GPUs NVIDIA RTX PRO 4500 Blackwell, permite que se aborden casos de uso como los siguientes: virtualización, la inferencia de la inteligencia artificial en el edge y cargas ligeras de IA generativa allí donde se generan los datos.

Posee, por otro lado, un diseño apto para operar en condiciones que son exigentes. En este sentido, cumple con la normativa MIL-STD-810H y brinda a las empresas que lo necesiten una opción de ultra-ruggedización que lo hace más resistente a condiciones o entornos especialmente difíciles. A este respecto, resulta adecuado para organizaciones de sectores que operan (entre otros) en el ámbito de la defensa, telecomunicaciones, retail, energía e industria, y que necesitan capacidades de computación edge seguras y resilientes sin comprometer el rendimiento ni la flexibilidad.

Con acceso frontal y totalmente integrado con HPE Compute Ops Management y HPE iLO, este servidor plug-and-play incorpora capacidades de autoconfiguración que permiten una provisión prácticamente sin intervención. Solo requiere de alimentación eléctrica y una conexión Ethernet para integrarse de forma segura en infraestructuras de edge computing distribuidas. A ello se suma que, al operar precisamente en el edge, el sistema reduce la dependencia de la nube central, lo que se traduce en una menor latencia y en una optimización del consumo de ancho de banda y conectividad. Por otro lado, sus dimensiones, de aproximadamente 38 cm de ancho y 40 cm de fondo, hacen que las opciones de instalación sean diversas, permitiendo su ubicación en armarios o racks, así como su montaje en la pared o su colocación en el escritorio.

En otro orden de cosas, HPE ha centrado sus esfuerzos en simplificar la gestión en entornos distribuidos. Esto supone ayudar a las empresas a desplegar, proteger y gestionar sus sistemas

en múltiples ubicaciones con facilidad. También estandarizar la gestión en toda la organización mediante una visibilidad global desde una consola unificada.

A nivel de seguridad, los datos se protegen frente a accesos no autorizados desde el momento en que el servidor se conecta y se autentica en la red. Por su parte, la seguridad multinivel protege tanto datos como dispositivos incluyendo: seguridad integrada con AMD Infinity Guard, AMD Secure Processor y arquitectura AMD 'Zen'; raíz de confianza en silicio de HPE, HPE iLO 6, IDevID y certificados de plataforma; y seguridad física del equipo con un kit de intrusión en el chasis, cierre del bisel y bloqueo Kensington.

HPE
911 237 104
www.hpe.es
A consultar

Comparativa

Servidores para el centro de datos

Huawei FusionModule2000

La participación de Huawei no viene de la mano de un servidor para el centro de datos como tal. En la era de la digitalización acelerada, la inteligencia artificial y el procesamiento de datos en el borde de la red, las empresas no siempre disponen del tiempo ni del espacio suficiente para construir un edificio dedicado exclusivamente a sus servidores. ¿Cómo desplegar entonces una infraestructura crítica sin realizar grandes obras? La respuesta de Huawei a este reto es el FusionModule2000, una solución de centro de datos modular inteligente que destaca por su capacidad para convertir prácticamente cualquier espacio de un edificio en un data center con todas las garantías de fiabilidad.

Su mayor logro es que propone un diseño todo en uno al integrar en una estructura modular los racks, el sistema de energía (UPS y distribución), el control de clima, la gestión de las baterías y la seguridad contra incendios, eliminando de este modo la necesidad de un suelo técnico elevado o techos con alturas especiales. Así, ya sea un antiguo almacén, una sala de juntas en desuso o una oficina estándar en un piso intermedio, este módulo se ensambla directamente sobre el suelo existente. La ventaja no es solo que una empresa reutiliza sus espacios físicos de inmediato, sino que ve reducidos los tiempos de despliegue hasta en un 50%.

Los tres ejes clave sobre los que se sostiene y articula FusionModule2000 son los siguientes: la fiabilidad continua con inteligencia artificial, la seguridad integral (tanto física como digital) y la eficiencia energética. En relación al primero, se apoya en su sistema de gestión inteligente iManager. Gracias a la tecnología de inteligencia artificial i3 (iPower, iCooling, iManager), el módulo realiza un mantenimiento predictivo: en lugar de reaccionar cuando un componente falla, el sistema detecta anomalías en las baterías o variaciones de temperatura antes de que causen una caída del sistema. A esto se añade una redundancia en alimentación y climatización, garantizando una disponibilidad del servicio del 99.999% según apunta la multinacional.

El FusionModule2000 cuenta, por otro lado, con un sistema de contención de pasillo cerrado (generalmente de pasillo frío o caliente) que aísla el entorno de los servidores del resto de la habitación. Además, incorpora estas otras medidas: control de acceso biométrico o por tarjeta en las puertas del módulo, videovigilancia las 24 horas y sistemas automáticos de extinción de incendios por gas que protegen el equipamiento sin dañar los componentes electrónicos.

Por último, uno de los mayores miedos de las empresas al instalar servidores en edificios comerciales es la factura eléctrica. Huawei lo resuelve optimizando el flujo de aire mediante el pasillo confinado, evitando que el aire frío se mezcle con el caliente. Sumado a sus sistemas de refrigeración In-Row (entre filas) que enfrían directamente la carga tecnológica, el FusionModule2000 logra reducir el PUE (Power Usage Effectiveness o Eficiencia en el Uso de la Energía) hasta un valor óptimo. Esto se traduce en un ahorro de energía de hasta un 30% en comparación con los centros de datos tradicionales.

Huawei

contacto

e.huawei.com/es

A consultar

Comparativa

Servidores para el centro de datos

Supermicro NVIDIA BlueField-4 STX

El proveedor integral de soluciones IT para IA, nube, almacenamiento y 5G/Edge presentó recientemente uno de los primeros servidores de almacenamiento de memoria contextual (CMX) de la industria. Lo hizo como parte de la arquitectura de NVIDIA STX que se anunció en la conferencia mundial NVIDIA GTC 2026 que tuvo lugar el pasado mes de marzo. Se trata de una nueva arquitectura de referencia modular desarrollada por NVIDIA con la intención de acelerar todo el ciclo de vida de la inteligencia artificial.

Aprovechando esta arquitectura STX, CMX está diseñado para abordar el desafío de las consultas de IA de larga duración y las cargas de trabajo agentivas de razonamiento en múltiples etapas (chain-of-thought), que requieren acceder a los tokens previos e intermedios asociados a la consulta del usuario. De este modo, la solución no solo acelera los resultados, sino que también reduce la energía que, de otro modo, sería necesaria para volver a calcularlos cuando se supera el almacenamiento local requerido para los tokens. Este almacenamiento de los tokens, denominado caché de valores clave (Key Value o KV cache) es gestionado por NVIDIA Dynamo, la capa de orquestación de inferencia de NVIDIA.

Desde el punto de vista técnico, este servidor de almacenamiento combina la CPU NVIDIA Vera y la SuperNIC NVIDIA ConnectX-9. La primera ha sido desarrollada para potenciar el aprendizaje por refuerzo (RL) y los sistemas de IA basados en agentes, optimizando el funcionamiento de código, las herramientas y los flujos de datos que van más allá del propio modelo de inteligencia artificial. Con núcleos de alto rendimiento, eficiencia energética y un elevado ancho de banda de memoria LPDDR5X, permite que los entornos de software se ejecuten hasta un 50 % más rápido con el doble de eficiencia que la infraestructura de CPU tradicional, lo que desbloquea la IA de agentes a escala. Por su parte, la tarjeta de red SuperNIC NVIDIA ConnectX-9 acelera las cargas de trabajo de computación de IA a gran escala gracias a su compatibilidad con velocidades de hasta 800 gigabits por segundo (Gb/s) por puerto, tanto sobre la tecnología de red InfiniBand como Ethernet. Asimismo, asegura una conectividad de red extremadamente rápida y eficiente que mejora el rendimiento de los sistemas destinados a fábricas de IA y plataformas cloud.

En otro orden de cosas, el servidor de Supermicro se basa en la introducción, el año pasado, del sistema JBOF Petascale all-flash impulsado

por NVIDIA BlueField-3, introduciendo así un nuevo enfoque para el almacenamiento. El punto de partida es JBOF, acrónimo de Just a Bunch of Flash, una matriz de almacenamiento all-flash inteligente que emplea una DPU (unidad de procesamiento de datos) para descargar y para acelerar las funciones tradicionalmente gestionadas por la CPU y la NIC, en comparación con los servidores de almacenamiento convencionales.

En este caso, JBOF integra una o varias DPU que se encargan, entre otros, de gestionar la conectividad de red, ejecutar la aplicación de almacenamiento y asegurar los medios de almacenamiento SSD. En cuanto a sus ventajas, destaca su mayor rendimiento y nivel de integración.

Nemix

902 400 888

nemix.es

A consultar

Conclusiones

Esta comparativa pone de manifiesto la madurez y la diversificación del mercado de servidores para el centro de datos. Y aunque todas las máquinas que participan son válidas y responden a las necesidades del entorno empresarial, las propuestas de HPE y Supermicro destacan ligeramente sobre el resto. La primera sobresale especialmente por su enfoque en el edge computing, la robustez en términos de diseño, la seguridad multinivel y la facilidad de despliegue en entornos distribuidos. Por su parte, Supermicro se posiciona como un referente en innovación para las infraestructuras de inteligencia artificial a gran escala, destacando por la adopción temprana de arquitecturas avanzadas como STX, la integración de tecnologías de NVIDIA y su orientación a cargas de trabajo de IA agentiva y almacenamiento de alto rendimiento

El resto de fabricantes representan asimismo opciones interesantes, sólidas y consolidadas. Cisco sugiere una plataforma equilibrada con gran capacidad de virtualización, alta flexibilidad de configuración y un ecosistema de gestión maduro. Dell, por su parte, se distingue por su potencia en entornos de inteligencia artificial y computación de alto rendimiento, sobre todo en configuraciones de alta densidad de GPU, aportando soluciones versátiles y muy orientadas a la escalabilidad.

Un caso particular es el de Huawei, cuya propuesta se basa en una solución de centro de datos modular. El FusionModule2000 integra toda la infraestructura en un único sistema, lo que permite convertir espacios convencionales en centros de datos funcionales. El propio armario IT del sistema cumple la norma IEC 60297-1 y ofrece un espacio adecuado y seguro para instalar los servidores.

Aspectos Destacados

Nombre de la solución	Cisco UCS C220 M8 Rack Server	Dell PowerEdge XE774X	HPE ProLiant DL145 Gen11	Huawei FusionModule2000	Supermicro NVIDIA BlueField-4 STX
Valoración	★★★★	★★★★	★★★★★	★★★★	★★★★★
Características clave	* Procesadores Intel Xeon 6: mayor rendimiento con funciones aceleradas por IA y nuevas capacidades de seguridad para máquinas virtuales. * Soporte GPU: hasta tres GPUs single-wide para acelerar cargas de trabajo de IA y análisis de datos. * Fuentes de alimentación redundantes e intercambiables en caliente: opciones platinum (1.050W DC y 1.600W AC) y titanium (1.200W AC y 2.300W AC) para máxima disponibilidad. *Cisco Intersight y Cisco IMC: gestión centralizada del servidor. * Unidades M.2 SATA intercambiables en caliente: mayor facilidad de servicio para las unidades de arranque, con soporte RAID por hardware.	* La gama se divide en dos modelos que son el XE7740 (Intel Xeon 6) y el XE7745 (AMD EPYC 9005 de 5ª generación) * Servidores 4U de dos sockets, diseñados específicamente para IA, GPU computing y HPC. * Chasis refrigerado por aire, sin necesidad de pasar a soluciones SXM más complejas o a una refrigeración líquida. * Inferencia de LLMs y modelos de visión con baja latencia. * Fine-tuning y despliegue de modelos de IA generativa.	* Equipado con procesadores AMD EPYC 8004 de 4ª generación. * Diseñado para entornos de extremo con condiciones hostiles, funcionando con temperaturas de -5 a 55ºC e incorporando filtración de aire para espacios con mucho polvo y tolerancia a las vibraciones. * Distintas opciones de montaje: pared, escritorio o rack. * Admite hasta tres GPU de ancho único. * Soporta de 8 a 64 núcleos y una potencia de diseño término (TDP) de hasta 200 W con AMD EPYC 8004.	* Solución para el centro de datos que convertierte prácticamente cualquier espacio de un edificio existente en un data center. * Diseño todo en uno. Integra en una estructura modular los racks, el sistema de energía , el control de clima, la gestión de baterías ... * Sistema de gestión inteligente iManager. * Seguridad integral, tanto física como digital. * Sus sistemas de refrigeración In-Row (entre filas) enfrían directamente la carga tecnológica.	* Uno de los primeros servidores de almacenamiento Context Memory (CMX) basado en la arquitectura de referencia NVIDIA STX para almacenamiento de IA. * Combina la CPU NVIDIA Vera y la SuperNIC NVIDIA ConnectX-9. * Basado en la matriz all-flash Petascale JBOF, equipada con NVIDIA BlueField-3. * Aborda el desafío de las consultas de IA de larga duración y las cargas de trabajo de IA agentiva con razonamiento en múltiples etapas. * No solo acelera la obtención de resultados, sino que también reduce la energía que, de otro modo, sería necesaria para volver a calcularlos cuando se supera el almacenamiento local requerido para los tokens.

Compliance inteligente:

automatización y analítica para el cumplimiento normativo

Por ALFONSO CASAS

La presión regulatoria, el auge de la inteligencia artificial y la necesidad de operar en tiempo real están impulsando una transformación profunda del compliance empresarial, forzando a las organizaciones a su adopción

Portada

Compliance inteligente: automatización y analítica para el cumplimiento normativo

> **Desde abajo, los equipos de cumplimiento ya experimentan con IA por su cuenta, muchas veces con shadow AI, porque les resuelve problemas reales del día a día"**
>
> **MARTA FOGLIACCO, AGGITY**

Vivimos en un mundo en el que la tecnología evoluciona a gran velocidad. El gran volumen de datos que manejan las organizaciones hace que los modelos tradicionales de compliance, basados en controles manuales y revisiones puntuales, resulten insuficientes. Es en este contexto donde la automatización y la analítica avanzada cobran todo el sentido permitiendo evolucionar desde un enfoque reactivo hacia un modelo más preventivo y predictivo, capaz de anticipar riesgos, detectar anomalías y facilitar el cumplimiento normativo en tiempo real.

Las organizaciones se ven en la necesidad de avanzar en capacidades como la analítica de datos, la automatización de procesos o la inteligencia artificial. Ayudados por estas tecnologías, pueden reducir tareas manuales, mejorar la eficiencia operativa y disponer de una visión más precisa y en tiempo real de los riesgos y del grado de cumplimiento normativo. Ya no basta únicamente con cumplir; las compañías también deben ser capaces de demostrar, de forma continua y objetiva, que cumplen con los requisitos regulatorios.

Diversos análisis llevados a cabo por empresas del sector revelan que hasta el 30% del coste total de un proyecto de automatización puede destinarse a integrar el motor de workflow con los sistemas documentales y otras aplicaciones corporativas. No se trata de una excepción, sino de una constante en proyectos donde contratos, facturas, expedientes o evidencias regulatorias forman parte central del proceso.

Principales factores que impulsan la adopción

La creciente complejidad regulatoria, la digitalización acelerada y el auge de la inteligencia artificial están transformando profundamente la forma en que las organizaciones afrontan el cumplimiento normativo. Lo que durante años fue concebido como una función de seguridad, ahora se está convirtiendo en

Portada

Compliance inteligente: automatización y analítica para el cumplimiento normativo

un elemento estratégico apoyado en automatización, analítica avanzada y modelos de IA capaces de monitorizar riesgos en tiempo real.

El resultado es el denominado compliance inteligente: un enfoque continuo, basado en datos y orientado no solo a cumplir normativas, sino a anticiparse a incumplimientos, reducir fricciones operativas y reforzar la capacidad de decisión de las empresas.

Normativas como DORA, NIS2 o el AI Act Europeo están acelerando la necesidad de implantar capacidades avanzadas de monitorización, trazabilidad y gestión de riesgos. "Ya no basta únicamente con cumplir; las organizaciones también deben ser capaces de demostrar, de forma continua y objetiva, que cumplen con los requisitos regulatorios", señala Sergio Postigo Collado, VP Consulting Delivery de CGI.

A esta presión normativa se suma otro fenómeno: la propia irrupción de la IA dentro de las organizaciones. Marta Fogliacco, Senior AI Consultant & Account Executive de aggity, explica que la transformación está siendo impulsada de manera simultánea desde la base y la dirección de las compañías. "Desde abajo, los equipos de cumplimiento ya experimentan con IA por su cuenta, muchas veces con shadow AI, porque les resuelve problemas reales del día a día. Y desde arriba, la alta dirección y el consejo piden respuestas cada vez más rápidas y mejor argumentadas sobre el estado del cumplimiento y de los riesgos", afirma.

Ese doble impulso está obligando a acelerar decisiones que muchas organizaciones llevaban tiempo posponiendo. Además, la relación entre IA y compliance empieza a ser bidireccional: la inteligencia artificial transforma la función de cumplimiento, pero al mismo tiempo el compliance se convierte en garante del uso responsable de la IA en el resto de la empresa.

Fernando Ranz, VP y Country Manager Iberia & Latam de Celonis, añade otro factor decisivo: la dificultad creciente de gestionar manualmente normativas y procesos cuando las compañías operan con múltiples sistemas y grandes volúmenes de datos. En este escenario, la automatización aporta visibilidad en tiempo real y reduce significativamente el riesgo de incumplimiento.

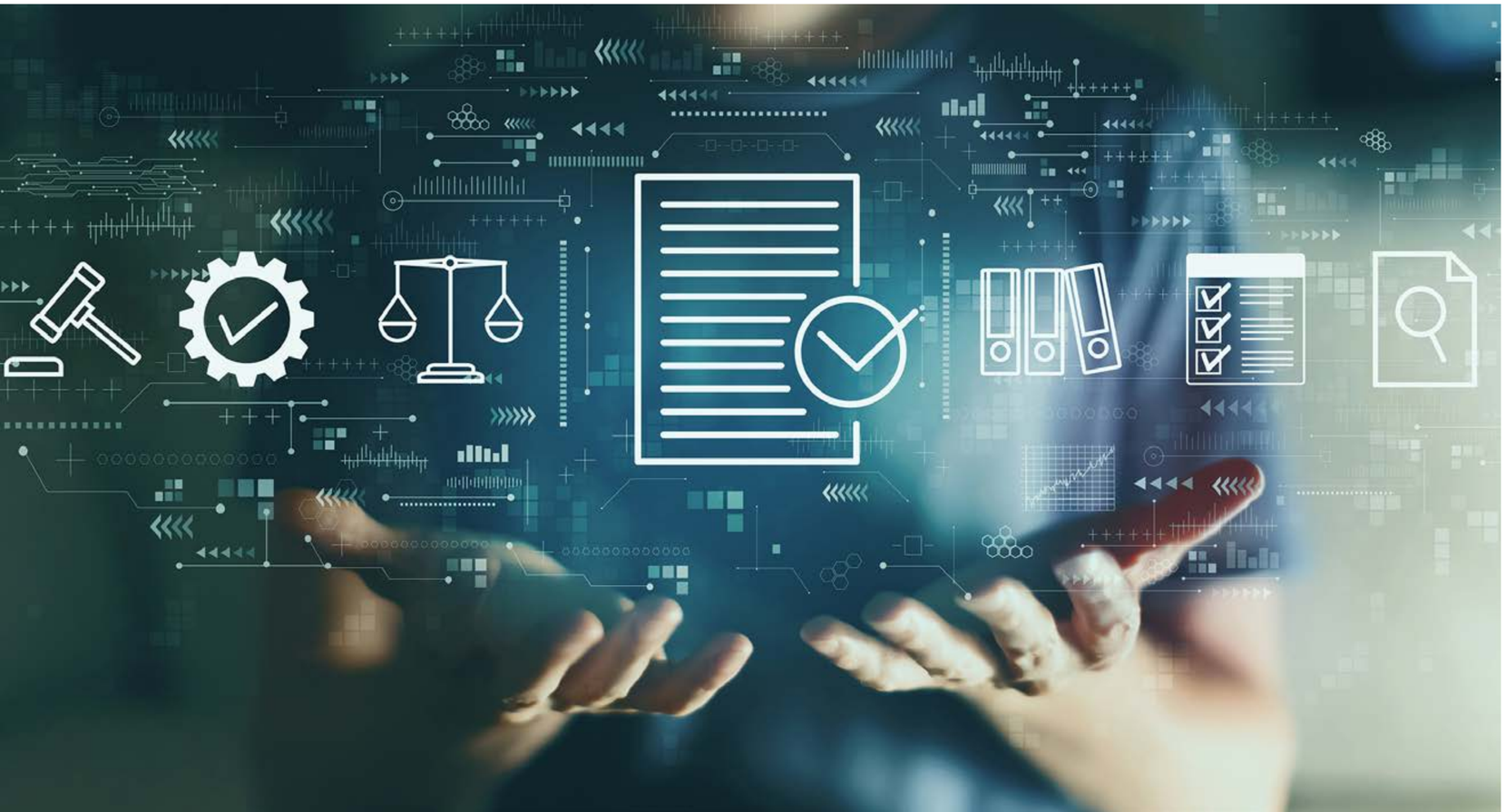
También está cambiando la percepción estratégica del compliance dentro de las organizaciones. Pedro Redondo Ballesteros, director ICT Business de Kyocera Document Solutions España, considera que el cumplimiento normativo "se está convirtiendo en un habilitador de negocio". Gracias a la analítica y al uso inteligente del dato, explica, las empresas no solo garantizan el cumplimiento, sino que

> **"El software puede incluso detener automáticamente determinadas operaciones si identifica riesgos regulatorios"**
>
> **FERNANDO RANZ, CELONIS**

Compliance inteligente: automatización y analítica para el cumplimiento normativo

mejoran procesos, refuerzan la seguridad y generan confianza entre clientes y socios.

Desde Indra Group, Javier Muñoz Lagaron, director de Desarrollo de Soluciones, Datos e IA, identifica además a los departamentos de compliance como una de las áreas que más rápidamente están adoptando herramientas de IA generativa, debido a su elevada carga documental y a la necesidad constante de interpretar y actualizar normativa. En su opinión, el reto ya no es tanto identificar casos de uso como gestionar adecuadamente el cambio cultural y el upskilling de los equipos.



Ventajas asociadas a la automatización

Los expertos coinciden en afirmar que uno de los principales errores es automatizar procesos sin priorizar los objetivos. El criterio clave pasa por identificar aquellas tareas repetitivas, críticas y con alta carga operativa donde la automatización pueda generar un mayor impacto y un retorno tangible.

Para aggity, el punto de partida debe ser escuchar a los propios equipos de compliance. "Dos preguntas funcionan muy bien: qué les frustra cada día y qué delegarían si pudieran tener un compañero más", explica Fogliacco. Ese ejercicio suele revelar rápidamente tareas susceptibles de automatización: revisión documental, recopilación de evidencias, controles regulatorios o verificación de información.

Celonis defiende una aproximación basada en datos reales de operación. Según Fernando Ranz, la monitorización continua de procesos permite detectar exactamente dónde se producen errores, retrasos o incumplimientos, facilitando así la automatización de los puntos de mayor riesgo.

En la misma línea, CGI considera prioritario automatizar procesos ligados a monitorización continua, gestión de riesgos, trazabilidad o supervisión de terceros. "La automatización no debe abordarse de forma genérica, sino alineada con las necesidades concretas de cumplimiento de cada organización", subraya Postigo.

Indra Group marca diferencias entre automatizaciones tácticas y transformaciones estructurales. Javier Muñoz explica que las

> **"Procesos que antes duraban semanas ahora pueden llegar a ejecutarse en horas"**
>
> **MIGUEL ÁNGEL GONZÁLEZ, APPIAN**

herramientas de copilotaje basadas en IA permiten generar mejoras rápidas y muy adaptadas al trabajo diario de los empleados, mientras que las transformaciones más profundas requieren la creación de Centros de Excelencia (CoE) capaces de coordinar perfiles técnicos, funcionales y de negocio.

Kyocera insiste en la necesidad de adoptar una visión end-to-end. "No se trata solo de automatizar tareas aisladas, sino de optimizar flujos completos integrando sistemas y datos", señala Pedro Redondo. En este punto, "nuestro enfoque en Kyocera pasa precisamente por integrar hardware, software y servicios dentro de un mismo ecosistema, permitiendo a las organizaciones tener control y visibilidad completa de sus procesos y avanzar en su posicionamiento como empresas más eficientes y seguras", puntualiza.

Tecnologías y herramientas con mayor impacto

Aunque la reducción de errores y el ahorro de tiempo son los beneficios más visibles, el impacto del compliance inteligente va mucho más allá de la eficiencia operativa.

Miguel Ángel González, VP South EMEA, Middle East & LATAM de Appian, resume esta transformación con una idea contundente: "procesos que duraban semanas ahora se ejecutan en horas". Como ejemplo, cita el caso de Acclaim Autism, organización sanitaria que logró reducir en un 83% el tiempo de admisión de pacientes gracias a la automatización documental y la extracción inteligente de datos.

La automatización también está cambiando el papel de los profesionales de compliance. Según González, muchas organizaciones están desplazando recursos destinadas a tareas administrativas hacia funciones de supervisión y análisis estratégico, aumentando así el valor añadido del área.

> **"Sectores como industria, energía, transporte o logística están teniendo que implantar capacidades avanzadas de monitorización y trazabilidad para adaptarse a nuevos marcos regulatorios"**
>
> **SERGIO POSTIGO, CGI**

Compliance inteligente: automatización y analítica para el cumplimiento normativo

En opinión de aggity, uno de los cambios más relevantes es que el compliance deja de actuar como un freno y pasa a ser un facilitador del negocio. "La información que llega al consejo deja de ser una foto y pasa a ser una visión continua del estado del cumplimiento y de los riesgos", destaca Fogliacco.

La capacidad predictiva es otro de los grandes avances. Fernando Ranz explica que las plataformas basadas en datos en tiempo real y simulación de escenarios permiten detectar posibles incumplimientos antes de que se produzcan. "El software puede incluso detener automáticamente determinadas operaciones si identifica riesgos regulatorios", afirma.

Indra Group destaca especialmente el potencial de la IA para procesar grandes volúmenes de documentación legal y normativa dispersa entre múltiples fuentes. Sin embargo, Javier Muñoz advierte de que el concepto "human-in-the-loop" seguirá siendo esencial: "son procesos críticos donde la IA no debe trabajar sola".

Desde CGI apuntan además que la automatización facilita el poder responder con mayor rapidez a auditorías, inspecciones regulatorias o cambios normativos, gracias al uso de sistemas capaces de operar de forma continua y con trazabilidad permanente.

El dato, el verdadero núcleo del compliance inteligente

Más allá de la IA generativa, los expertos opinan que el verdadero núcleo del nuevo compliance reside en la gestión del dato. "Gobierno del dato, calidad, arquitectura, trazabilidad. Sin esa base sólida ninguna IA va a dar lo que se espera", resume Marta Fogliacco.

La IA generativa está demostrando gran capacidad para analizar contratos, interpretar normativa o traducir requisitos regulatorios en controles operativos. Sin embargo, el machine learning tradicional sigue siendo fundamental para detectar anomalías, fraude o patrones sospechosos.

Appian apuesta por arquitecturas que combinan agentes inteligentes, automatización y capas de integración de datos capaces de conectar información de múltiples sistemas sin necesidad de moverla físicamente. Según Miguel Ángel González, la clave está en que "la IA opera con acceso a datos verificados, contexto normativo y reglas claras".

Desde Celonis opinan que el gran salto se produce cuando las herramientas de IA trabajan

directamente sobre datos conectados en tiempo real, permitiendo auditar procesos y predecir riesgos sin replicar grandes volúmenes de información.

Indra Group destaca el crecimiento de soluciones basadas en modelos RAG y agentes desplegados sobre plataformas de hiperescaladores como Microsoft, Google o AWS, los cuales resultan fáciles de integrar en los ecosistemas ya existentes. Estas herramientas permiten consultar normativa, contrastar documentación legal e identificar automáticamente posibles brechas regulatorias en contratos o acuerdos.

Kyocera recuerda además que el compliance también afecta a elementos frecuentemente olvidados, como la gestión documental y los sistemas de impresión. "La fuga de información en papel sigue siendo un riesgo real en entornos regulados", advierte Pedro Redondo.

En cualquier caso, existe unanimidad y todas las compañías coinciden en afirmar que la automatización solo resulta realmente útil cuando existe integración completa entre procesos, datos y herramientas de supervisión.

Sectores donde el impacto es más visible

Los sectores más regulados siguen liderando la adopción del compliance inteligente. Banca, seguros, sanidad o farmacéutico son algunos de los ámbitos donde la automatización ya está generando resultados tangibles. Sin embargo, varias compañías destacan que la expansión más acelerada se está produciendo precisamente en industrias con menor tradición regulatoria.

> **"Donde hay datos, regulación y necesidad de control, la automatización deja de ser eficiencia y pasa a ser un requisito operativo"**
>
> **PEDRO REDONDO, KYOCERA DOCUMENT SOLUTIONS ESPAÑA**

"Sectores como industria, energía, transporte o logística están teniendo que implantar capacidades avanzadas de monitorización y trazabilidad para adaptarse a nuevos marcos regulatorios", explica Sergio Postigo.

Indra Group identifica además importantes avances en empresas con grandes volúmenes de atención al cliente, como telecomunicaciones o Administraciones Públicas, donde la IA permite reducir tiempos de respuesta y ampliar la capacidad operativa de los equipos. "En estos ámbitos, se generan muchas eficiencias al ampliar la capacidad del equipo, reducir tiempos de atención y ofrecer un mejor servicio", subraya Javier Muñoz.

Celonis destaca especialmente el potencial en cadenas de suministro globales y fabricación industrial, donde la supervisión automatizada permite cruzar información de proveedores, compras y riesgos regulatorios en tiempo real.

Kyocera apunta también al creciente protagonismo de las pymes, impulsado por normativas relacionadas con facturación electrónica, protección del dato o cumplimiento fiscal. "Donde hay datos, regulación y necesidad de control, la automatización deja de ser eficiencia y pasa a ser un requisito operativo", resume Pedro Redondo.

La IA también necesita supervisión y regulación

La gran paradoja del compliance inteligente es que la misma IA que ayuda a garantizar el cumplimiento normativo debe ser, a su vez, regulada y supervisada. La Ley de Inteligencia Artificial de la Unión Europea (AI Act Europeo) aparece ya como uno de los principales marcos regulatorios llamados a redefinir la gobernanza tecnológica de las organizaciones. Las compañías deberán garantizar explicabilidad, supervisión humana, trazabilidad y control de

Compliance inteligente: automatización y analítica para el cumplimiento normativo

riesgos en muchos sistemas de IA considerados de alto impacto.

"El uso de la IA en compliance introduce una doble dimensión regulatoria", explica Sergio Postigo. "La IA puede mejorar la monitorización y la eficiencia, pero también debe ser gobernada para garantizar un uso ético, seguro y transparente".

Marta Fogliacco recomienda incorporar principios de IA responsable desde el diseño de los proyectos: gobernanza de modelos, trazabilidad de decisiones y supervisión humana en los puntos críticos. Según explica, cuando compliance participa desde el inicio en los proyectos de IA, la adopción resulta mucho más fluida y segura.

Appian establece tres pilares esenciales: responsabilidad humana garantizada, trazabilidad completa y acceso controlado a los datos. Celonis advierte, además, de los riesgos de utilizar modelos de IA genéricos sin reglas específicas de control: "la IA estándar opera en base a probabilidades", recuerda Fernando Ranz.

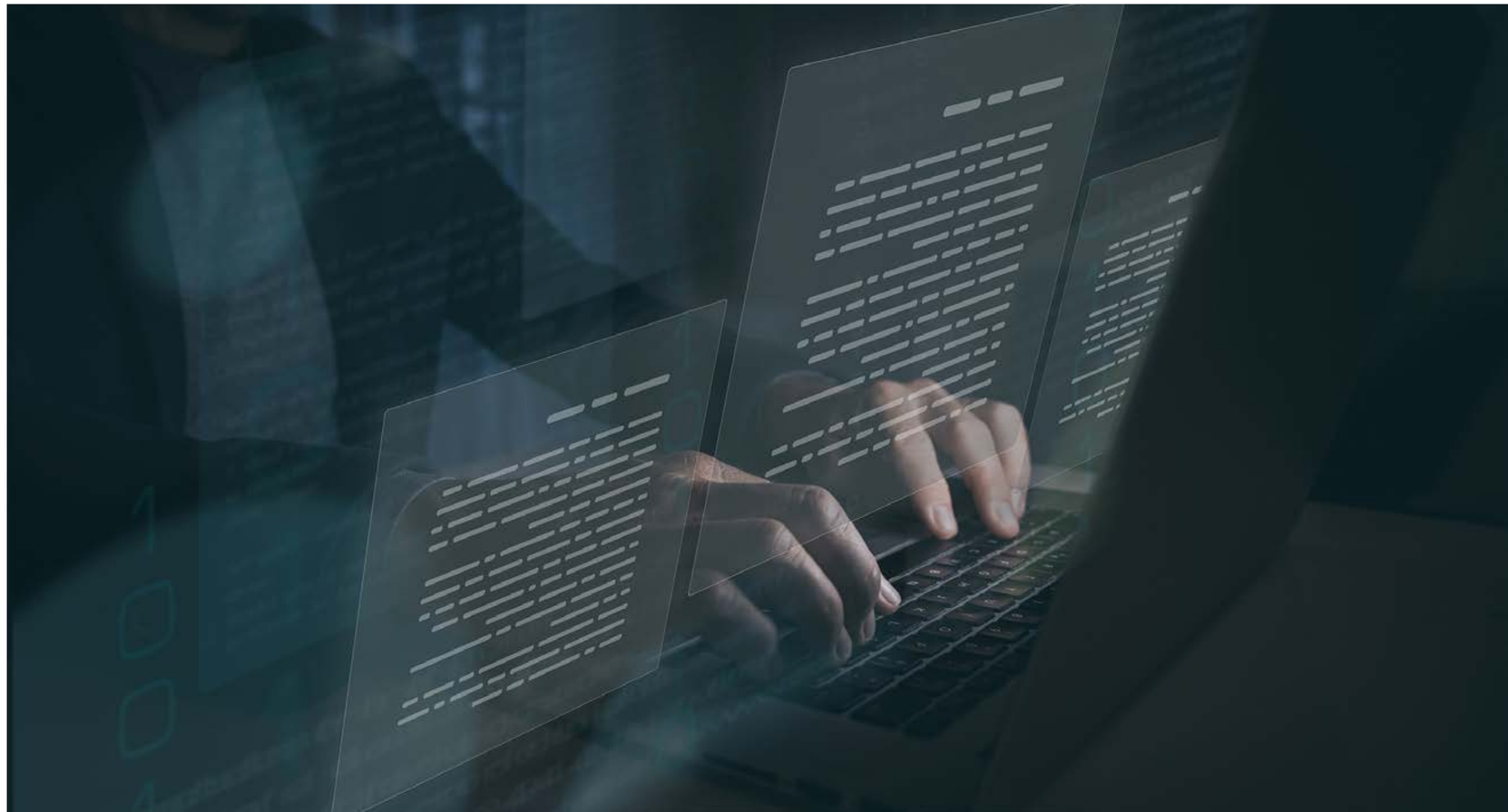
Indra Group insiste en que la confidencialidad y el riesgo reputacional hacen imprescindible mantener auditorías periódicas y supervisión humana constante sobre los sistemas automatizados.

La compañía ha detectado en el último año y medio un progreso generalizado en el uso de la IA para la agentivización de procesos en el puesto de trabajo, y la generativa en su sentido más amplio. "La introducción de la multimodalidad real en los modelos ha abierto también un nuevo horizonte de casos de uso. Si antes existían dudas sobre embarcarse en la realización de proyectos, ahora las conversaciones giran alrededor de cómo asegurar la correcta adopción y el cumplimiento normativo, lo cual denota que la IA ya está arraigando en buena parte de las compañías", concluye su directivo, Javier Muñoz.

Hacia un compliance predictivo e integrado

La evolución del sector con vistas al futuro apunta hacia modelos de compliance mucho más predictivos, automatizados e integrados directamente en los procesos de negocio. Uno de los grandes consensos es el paso desde revisiones periódicas hacia sistemas de monitorización continua capaces de detectar riesgos en tiempo real.

Para aggity, el futuro pasa también por la convergencia entre compliance, sostenibilidad y ciberseguridad bajo un mismo marco de riesgos



Compliance inteligente: automatización y analítica para el cumplimiento normativo

corporativos. Fogliacco advierte, sin embargo, de que muchas iniciativas de IA agéntica fracasarán si las organizaciones no redefinen adecuadamente sus modelos operativos y de gobernanza. "Los agentes se financian como tecnología, pero operan como workers, y sin una implantación clara de ownership, decision rights y accountability, los proyectos quedan huérfanos. La IA agéntica escala más rápido que sus guardarraíles, y el próximo capítulo no va de tecnología, sino de modelo operativo", enfatiza.

CGI prevé que la ciberseguridad y la regulación de la IA marcarán gran parte de la agenda futura del compliance, especialmente en sectores considerados críticos o de alto riesgo. Kyocera apunta hacia una integración total del cumplimiento dentro de los propios flujos operativos, apoyada en plataformas cloud y soluciones cada vez más verticalizadas por industria.

Indra Group estima que el futuro del compliance pasa por un fuerte crecimiento de herramientas capaces de automatizar la supervisión de modelos de IA y los procesos GRC (Governance, Risk & Compliance), facilitando tanto el control técnico como la gestión legal y documental. Appian, por su parte, identifica como tendencia estructural la democratización de la automatización. No obstante, Miguel Ángel González considera que el principal reto no será tecnológico, sino cultural. "El miedo laboral a ser reemplazado es real, pero la evidencia muestra que los empleados se reubican en nuevos puestos", afirma.

Expone además que la verdadera diferencia es convertir automatización en valor empresarial medible: "no solo números sino tiempo liberado, eficiencia mejorada, reducción de costes y mejora de compliance. En una era de regulaciones complejas, compliance inteligente es la ventaja competitiva del futuro", concluye.

La doble dimensión del compliance

La automatización y la inteligencia artificial están transformando definitivamente el compliance en una función estratégica para las organizaciones. El nuevo modelo ya no se limita a evitar sanciones o responder a auditorías, sino que aporta capacidad predictiva, agilidad operativa y una visión continua del riesgo. El área de cumplimiento deja así de percibirse como un obstáculo para convertirse en un habilitador del negocio y en facilitar la adopción segura de la IA.

Los expertos que han participado en el reportaje opinan que la tecnología por sí sola no basta. La calidad del dato, la gobernanza, la supervisión humana y la cultura organizativa seguirán siendo elementos críticos para que las compañías puedan tener éxito. En un entorno donde regulación y complejidad tecnológica avanzan al mismo ritmo, las organizaciones que logren

integrar automatización, analítica e IA dentro de una estrategia sólida de gobierno del dato estarán en mejor posición para competir a lo largo de los próximos años.

Como nos resume Marta Fogliacco de aggity: "Las organizaciones que entiendan esa doble dimensión, y aborden la transformación con una visión amplia, van a sacar ventajas reales. La tecnología actúa como un amplificador de lo que ya existe. Donde hay cultura sólida, los resultados son muy buenos. Donde la base es frágil, pone en evidencia los problemas que ya existían".

Mujeres TIC

Amaya Cerezo

Experta en Inteligencia Artificial

Fecha de nacimiento: 00/00/0000
Hijos: –
Aficiones: Correr, baloncesto, tocar el piano, leer
Formación: Matemáticas y un máster en Data Science

¿Cómo llegó al mundo TIC?
Mi llegada al mundo de las TIC fue un camino inesperado, casi de rebote, que comenzó cuando de niña, a pesar de tener claro mi desinterés por las letras, se me daban francamente mal las matemáticas. Sin embargo, el punto de inflexión llegó gracias a un profesor particular, que me enseñó matemáticas, física y química de una manera distinta. Al final logró que todo hiciera "clic" y me reveló un mundo divertidísimo y apasionante que me impulsó a orientar mi futuro hacia la tecnología.

De hecho, mi primera opción era estudiar informática, pero la nota de corte no me alcanzó. El destino hizo que acabase matriculándome en matemáticas (completado más tarde con un máster en Data Science), y hoy puedo decir que fue de las mejores cosas que he hecho en la vida. No solo aprendí las verdaderas matemáticas, sino que me amuebló el cerebro, me dio una estructura mental metódica, abierta y analítica para resolver problemas complejos.

El paso definitivo al sector de la inteligencia artificial llegó años después. Estaba en una posición muy cómoda en otra empresa, pero sentía que me faltaba aprendizaje. Decidí arriesgarme, vencer el miedo al cambio y ponerme a estudiar de nuevo mientras trabajaba para especializarme en IA y venirme a SAS. Me llamaron para una entrevista y, aunque no tenía una gran experiencia en ese campo específico, apostaron por mi actitud y mis ganas. Siete años después, sigo explorando un sector que no deja de fascinarme.

¿Qué es lo que más valora de su trabajo?
De SAS es que lo valoro absolutamente todo. Sobre todo, la confianza absoluta que depositan en mí. En SAS existe una cultura muy sana que te permite fallar, porque entienden que el error es la mejor vía para el aprendizaje y la evolución profesional. Te ponen a disposición todos los caminos posibles para que los explores y, si uno no funciona, te ayudan a buscar otra alternativa. Además, en mis siete años en la compañía he podido moverme por diferentes áreas. Es un entorno tan amplio y ofrece tanto que te

permite explorar constantemente y, lo que para mí es más importante, no dejar de aprender nunca.

En su opinión ¿qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?
Creo que el problema está en la base. Concretamente en cómo se enseñan las materias de ciencias en el colegio. Existe un rechazo generalizado hacia asignaturas como las matemáticas –a mí me pasaba– porque no se explican bien y, por tanto, no se entienden. Sin embargo, cuando consiguen transmitírtelas de una manera adecuada y logras comprenderlas, se te abre un mundo fantástico, ameno y sumamente divertido. Falta esa pedagogía inicial que rompa con la rigidez de la enseñanza tradicional. Si logramos que las niñas entiendan las ciencias desde el principio, perderán el miedo y se darán cuenta de que es un camino apasionante que no tiene por qué ser árido.

¿Cree que existe el "techo de cristal" en las empresas TIC? ¿Cuál debería ser la solución? ¿Una política de cuotas puede resolver el problema?
Aunque desconozco cuál es la realidad en otras compañías del sector, puedo afirmar que en SAS el techo de cristal no existe. Aquí lo único que premia es el talento, y las oportunidades se nos brindan con absoluta igualdad. Vivimos en un entorno de inclusividad real y transparencia total. Considero que una política de cuotas no solucionaría absolutamente nada en nuestro caso; la clave no está en imponer porcentajes, sino en integrar de forma natural políticas de igualdad transparentes basadas exclusivamente en el mérito y la capacidad de las personas, tal y como hacemos nosotros.

¿Qué dificultades se encontró usted para llegar a la posición que tiene actualmente?
Sinceramente, los únicos obstáculos reales que encontré fueron las barreras que me ponía yo misma. Si lo pienso bien, supongo que la mayor barrera fue el miedo, por lo que decía antes. Estaba en una empresa donde me sentía muy cómoda, pero que se me había quedado pequeña a nivel de aprendizaje y retos. Dar el salto significaba enfrentarse a la incertidumbre y salir de la zona de confort, y esa duda de "¿me quedo aquí porque estoy bien?" puede llegar a paralizarte. Sin embargo, decidí arriesgarme y, una vez tomada la decisión, el reto fue de puro esfuerzo. Tuve que estudiar y formarme en inteligencia artificial a la vez que trabajaba. Al final, la recompensa llegó cuando en mí vieron no solo el conocimiento técnico, sino, sobre todo, la actitud y las ganas de crecer, dándome la oportunidad que necesitaba y consiguiendo explotar muchas más cualidades que tenía y no sabía que tenía.

¿Cree que la conciliación de la vida laboral–familiar es el principal reto para las mujeres? ¿Qué habría que hacer para mejorar este apartado?
Rotundamente no. Para mí, plantear la conciliación como un reto exclusivo de las mujeres es un enfoque que carece de sentido. La conciliación de la vida laboral y familiar es una necesidad y un derecho que debe aplicar exactamente por igual tanto a hombres como a mujeres. Por lo tanto, no considero que deba etiquetarse como un problema femenino, sino como un desafío social y empresarial que nos afecta a todos.

¿Qué es lo que más valora de su empresa con respecto a la integración de la mujer?
Lo que más valoro es que la igualdad es una realidad cotidiana; jamás, desde el día en que entré hasta hoy, me he sentido diferente o en desventaja por el hecho de ser mujer. Pero más allá de esta normalidad, contamos con una iniciativa fantástica llamada WIN (Women in Network). Se trata de una comunidad interna de mujeres en la que organizamos multitud de actividades para conocernos, empoderarnos e intercambiar experiencias. Un aspecto clave de WIN es la mentoría cruzada, una iniciativa mediante la cual las profesionales más veteranas guían a las más jóvenes, y se crea una red de apoyo muy potente. Además, no es un entorno cerrado, colaboramos estrechamente con nuestros compañeros hombres en muchas de estas actividades, promoviendo una integración real y conjunta que enriquece a toda la compañía.

Un 35% de alumnos no logra ni acabar el bachillerato ni la FP equivalente, ¿está en la educación el problema de la falta de perfiles especializados?

Mujeres TIC

Amaya Cerezo, Experta en Inteligencia Artificial

Sin duda alguna, para mí el problema es de base y está en la educación. Las carreras STEM son complejas, exigen estructurar el cerebro de una manera determinada, además de desarrollar el sentido común y aprender a entender el porqué de las cosas. Ese moldeamiento mental no puede empezar en la adolescencia, es un proceso que debería iniciarse desde la etapa de parvulitos. Si no empezamos a entrenar y estructurar el cerebro de los niños desde que tienen tres o cuatro años para que se familiaricen con esta forma de pensar, es muy difícil que más adelante quieran enfrentarse a la exigencia de estas disciplinas técnicas.

¿Le han servido los estudios que hizo para realizar su labor actual?
Sí, estudiar Matemáticas ha sido lo que me ha abierto absolutamente todas las puertas en mi trayectoria profesional. Más allá de los conocimientos teóricos, esa carrera me dio la base y la estructura mental necesarias para enfrentarme a cualquier desafío tecnológico. A partir de ahí, con mucho esfuerzo personal por mi parte y algún que otro golpe de suerte, he conseguido llegar a donde estoy, pero no habría sido posible sin la carrera de matemáticas.

Solucione el problema de la educación en España...
¡Menuda pregunta! No soy ministra ni educadora, así que no tengo la receta mágica, pero sí tengo claro que la solución pasa por un cambio profundo en la base. Creo que hay que educar de otra manera, abandonando la rigidez actual. En mi día a día, cuando tengo que explicar conceptos complejos de inteligencia artificial, siempre intento hacerlo de la forma más sencilla posible y desde el principio, porque si empiezas a explicar por la mitad, la gente se pierde. Con la educación escolar ocurre lo mismo. En mi opinión, hay que enseñar a los niños a entender la vida y el mundo que los rodea desde lo más básico, de un modo mucho más intuitivo y flexible, para que el aprendizaje sea un proceso natural y no una imposición rígida.

Si tuviera que aconsejar a un joven qué estudiar de cara a obtener un futuro laboral estable, ¿por dónde le orientaría?
Aunque es evidente que las disciplinas ligadas a la inteligencia artificial están de moda y ofrecen un gran futuro, yo daría un paso más allá y le aconsejaría estudiar Matemáticas. Es probable que esté sesgada por mi propia experiencia, pero es una carrera que te aporta algo mucho más valioso que una formación técnica concreta; te da un cerebro diferente. Te enseña a ser más metódica, más perfeccionista, a tener una mente abierta y a encontrar soluciones creativas desde múltiples ángulos.

Si te limitas a estudiar una disciplina muy específica, como por ejemplo cómo hacer modelos de machine learning, tu conocimiento caducará cuando la tecnología avance hacia el deep learning o los grandes modelos de lenguaje. En cambio, una base sólida en matemáticas estructura tu mente de tal manera que adquieres la capacidad de comprender y adaptarte a cualquier tecnología disruptiva que surja en el futuro por ti misma.

¿Hacia dónde cree que va el sector TIC? En su opinión, ¿cuáles van a ser las tendencias que realmente van a transformar la sociedad?
Es evidente que el futuro más inmediato pasa por la consolidación de los chatbots, la sensórica, la robótica y la aplicación de la inteligencia artificial general en todos los ámbitos de nuestra vida cotidiana. Sin embargo, la verdadera transformación social no vendrá solo de las máquinas, sino de la revolución laboral que estas van a provocar. El gran "boom" de la IA va a generar muchos puestos nuevos de trabajo y perfiles profesionales que hoy apenas vislumbramos. La clave de esta transformación no estará tanto en la tecnología en sí, sino en cómo nos preparemos para asumir esos nuevos roles y tareas que surgirán a raíz de este avance tecnológico.

IA, automatización, robótica, ¿de verdad cree que el futuro pasa por las personas?
Definitivamente. Por muchos chatbots, robots o modelos de lenguaje que desarrollemos, una máquina jamás podrá replicar lo que es un ser humano.

Legalidad TIC

Odio y desinformacion digital

Por JAVIER LÓPEZ, SOCIO de ECIJA

La proliferación de la desinformación digital y los discursos de odio adquiere una dimensión notable a partir de la pandemia de la COVID-19, siendo en ese contexto cuando la Organización Mundial de la Salud (OMS) acuñó el término "infodemia" para denunciar la sobreabundancia de información falsa, engañosa o imprecisa que acompañó a la crisis sanitaria global. Asimismo, la Comisión Europea también advirtió sobre la creciente difusión digital de discursos racistas, alertando del papel de las plataformas digitales como amplificadores de narrativas polarizadoras. Esta preocupante tendencia no ha hecho sino consolidarse, como demuestran los episodios de desinformación estratégica vinculados al conflicto de Ucrania o a la escalada bélica en Oriente Medio, donde las fake news circulan a sus anchas como instrumento de influencia política y social.

En este escenario, resulta imprescindible abordar soluciones de carácter educacional en los ciudadanos que les permitan valorar adecuadamente el contenido que consumen, como el fact-checking y la alfabetización mediática, que son esenciales para combatir la manipulación informativa en Medios de comunicación y redes sociales, así como las exageraciones, tergiversaciones u omisiones que, aunque no encajen en la definición literal de información falsa, contribuyen a generar una realidad social alterada. Así, determinados hechos, personas o colectivos son mostrados como una amenaza para los valores supuestamente dominantes, sembrando la semilla del odio en el campo de la posverdad.

Para apoyar estas respuestas formativas, se han desplegado soluciones técnicas impulsadas por las propias plataformas digitales, como el bloqueo de contenidos, la suspensión de cuentas reincidentes o automatizadas y la inserción de advertencias visibles para advertir a los usuarios sobre la falsedad o inexactitud de un contenido, así como de su viralización. Pero lo cierto es que estas medidas muchas veces han pecado de inoperantes, además de generar cuestiones legales como la falta de transparencia, proporcionalidad y control democrático.

En España, en marzo de 2026 se presentó la herramienta HODIO (Huella del Odio y la Polarización), cuyo objetivo es medir el odio en las redes sociales con una combinación de datos empíricos, inteligencia artificial y revisión humana experta, como paso previo para acotarlo y combatirlo, bajo la premisa de que aquello que se mide deja de ser invisible. De esta forma, esta herramienta medirá específicamente

la presencia de discursos de odio y polarización y su capacidad de amplificación, es decir, no solo cuánto odio existe en cada red social, sino en qué medida este se transmite y viraliza.

Desde la perspectiva jurídica, el análisis de estos fenómenos exige la necesaria ponderación entre la libertad de expresión y el derecho a la información reconocidos en el artículo 20 de la Constitución Española, cuyo ejercicio se encuentra condicionado por el requisito de la veracidad, el límite del insulto y la vulneración el derecho al honor del artículo 18 de la Carta Magna. A nivel europeo se ha producido un reforzamiento del marco normativo contra las fake news mediante el Código de Prácticas sobre Desinformación de la Unión Europea, que en 2025 pasó de un modelo de autorregulación a un esquema de co-regulación, vinculado al Reglamento (UE) 2022/2065, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales (Digital Services Act).

Ello se suma al Reglamento (UE) 2024/1083 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, por el que se estableció un marco regulatorio común para los servicios de Medios de comunicación en el mercado interior, cuya finalidad es proteger el pluralismo mediático y limitar la concentración excesiva de propiedad. Y es que se ha detectado que plataformas globales como redes sociales y servicios de streaming han adquirido un poder significativo sobre la

> **Desde la perspectiva jurídica, el análisis de estos fenómenos exige la necesaria ponderación entre la libertad de expresión y el derecho a la información**

distribución de contenidos, de forma que se han convertido en los principales intermediarios con el público, por lo que resulta necesario adoptar medidas para combatir la desinformación y prevenir la injerencia, tanto pública como privada, en la línea editorial de los Medios.

Respecto a los recientes criterios jurisprudenciales para acotar los contornos del delito de odio en el entorno digital y analógico, por lo que se refiera a la homofobia, la Sentencia 89/2025 del Tribunal Supremo (Sala Segunda), de 5 de febrero de 2025, declaró que llamar "maricón" de forma denigrante a una persona homosexual no está amparado por la libertad de expresión; confirmando la condena por delito contra la dignidad de las personas del artículo 510.2 a) del Código Penal, subrayando que no existe un pretendido derecho al insulto y que tales expresiones transmiten un discurso que humilla, desprecia y discrimina a un colectivo por su orientación sexual.

En la misma línea, respecto a la xenofobia, la Sentencia 114/2026 del Tribunal Supremo (Sala Segunda), de 11 de febrero de 2026, confirmó la condena por delito de odio del artículo 510.2 a) del Código Penal y por amenazas leves del artículo 171.7 del mismo texto legal, en un caso de insultos racistas dirigidos contra el propietario de un local por razón de su nacionalidad y color de piel; estableciendo que expresiones como "negro de mierda" constituyen un ataque directo a la dignidad humana y una postulación de exclusión social incompatible con un Estado social y democrático de Derecho.

En consecuencia, el odio, tanto en la interacción directa como en el entorno digital, no puede considerarse una manifestación de la libertad de expresión, sino una forma grave de discriminación que atenta contra la dignidad humana y la igualdad, bienes jurídicos esenciales para la convivencia democrática. Por tanto, dada la tremenda capacidad de influencia en el pensamiento colectivo de los Medios de comunicación y las redes sociales, es fundamental combatir la desinformación en estos entornos para evitar la comisión de estos delitos.

Aplicación Práctica

La IA agéntica de Microsoft acelera el desarrollo de productos y servicios de BBVA

BBVA y Microsoft llevan más de un año trabajando conjuntamente en la introducción de la IA en el desarrollo de 'software', con el objetivo de impulsar nuevos productos digitales y mejorar los existentes. Ambas compañías están impulsando no solo la adopción de nuevas soluciones basadas en agentes de GitHub Copilot, sino toda una nueva forma de trabajar que está transformando los equipos y los roles de los programadores involucrados en la creación de productos tecnológicos.

Con cerca de 15.000 licencias de GitHub Copilot que ya usa el 70% de sus desarrolladores, el banco acorta los tiempos de entrega de sus desarrollos, acelera la modernización de su código y reorganiza sus equipos, ahora más centrados en la creación de valor.

Actualmente, las herramientas de IA están disponibles para los desarrolladores de todo el Grupo a través de una nueva plataforma global, a la que se han migrado más de 100.000 repositorios de código que dan soporte a múltiples productos y servicios. En estos entornos, el desarrollo, despliegue y mantenimiento de las aplicaciones se realiza siguiendo los más altos estándares de calidad y seguridad, garantizando además la trazabilidad necesaria para cumplir con las exigentes normativas del sector financiero. Este avance ha supuesto un hito clave al establecer un sistema estandarizado que permite integrar nuevas funcionalidades en los productos digitales y aplicar correcciones de forma automática y continua en los sistemas principales del banco, sin necesidad de realizar interrupciones o cortes en el servicio.

Tareas de coordinación de flujos de trabajo

El impacto de la IA también se refleja en la forma de trabajar de los equipos responsables de diseñar y evolucionar productos. Gracias al uso de IA agéntica de Microsoft, los ingenieros han pasado de ejecutar tareas manuales a coordinar flujos completos de trabajo de manera automática que van desde la generación de documentación técnica y funcional a la validación de proyectos o la gestión

Aplicación práctica

La IA agéntica de Microsoft acelera el desarrollo de productos y servicios de BBVA

de incidencias. Esto permite acelerar el ciclo completo de entrega de funcionalidades en los productos y reducir tareas repetitivas de bajo valor.

"Junto a Microsoft, estamos transformando la forma en la que se construye tecnología dentro de una gran organización. La incorporación de IA está permitiendo a nuestros equipos centrarse cada vez más en el diseño de soluciones y la toma de decisiones, evolucionando hacia un modelo de trabajo más estratégico y eficiente, con un único objetivo: acelerar la creación de productos financieros más rápidos, inteligentes y humanos para nuestros clientes", afirma Sergio Bonich, responsable Global de Desarrollo de Software en BBVA.

Este nuevo paradigma no solo permite desarrollar código con mayor velocidad y precisión, sino que también contribuye a la modernización del 'core' tecnológico de BBVA, es decir, las plataformas que soportan importantes transacciones y servicios operativos del banco y que sustentan sus principales productos. En este contexto, los proyectos orientados a refactorizar, migrar y modernizar este código histórico mediante herramientas de IA permiten acelerar procesos tradicionalmente complejos, mejorar la eficiencia en la evolución de los productos digitales y facilitar la transformación de sistemas críticos manteniendo los estándares de calidad, seguridad y continuidad operativa requeridos por el sector financiero.

"Desde Microsoft estamos trabajando con BBVA como socio estratégico en una transformación profunda, ambiciosa y transversal en todas las fases del ciclo de desarrollo de 'software', combinando innovación, seguridad y escala en el despliegue en todos los países donde opera BBVA y apoyando la evolución de sus productos digitales", indica Silvia Hernández, directora de clientes globales de Microsoft.

Innovación aplicada al desarrollo de software

BBVA fue la sede del evento GitHub EuroCats 2026 celebrado los días 19 y 20 de mayo. El encuentro reunió a más de 300 líderes y especialistas tecnológicos de toda Europa para compartir experiencias sobre el despliegue de inteligencia artificial en entornos corporativos altamente regulados y su impacto en el desarrollo de productos innovadores. La acogida de este evento refuerza el papel del banco como punto de conexión entre el ecosistema tecnológico y la innovación aplicada al desarrollo de 'software', los productos digitales y la inteligencia artificial.

La colaboración con Microsoft se enmarca en la estrategia de BBVA de apoyarse en un ecosistema de partners tecnológicos de referencia para acelerar su hoja de ruta de inteligencia artificial y el lanzamiento de nuevos productos. El banco cuenta con una hoja de ruta transversal basada en ocho líneas de trabajo, que contempla la adopción de la IA en la relación con los clientes, el trabajo de los gestores, en la gestión de riesgos, el desarrollo de 'software' y el día a día de los empleados para crear productos y servicios más personalizados, así como un banco más conversacional que acompañe a sus clientes en sus proyectos de vida y negocio.

Tendencias

Qué deberían hacer ahora las pymes con NIS2

Por JORGE MENDES,
fundador de Mencar Global Consulting · CISSP, CEH

España lleva más de 18 meses sin transponer NIS2. Mientras el BOE espera, los clientes grandes ya exigen a sus proveedores garantías de seguridad que la mayoría de pymes no puede demostrar. Cuatro acciones concretas para cambiar eso antes de que llegue la ley.

Imagina que uno de tus clientes más importantes te envía un cuestionario de seguridad de doce páginas. No tienes política de gestión de riesgos documentada. No tienes registro de incidentes. No sabes con certeza si los datos que gestionas están cifrados en tránsito y en reposo. El cuestionario tiene un plazo de dos semanas. Sin respuesta satisfactoria, el contrato se pone en riesgo.

Esta situación ocurre ya, hoy, en pymes españolas de todos los sectores. Y ocurrirá con mucha más frecuencia cuando la directiva NIS2 —la norma europea de ciberseguridad más ambiciosa de la última década— termine de desplegarse por la cadena de suministro.

La ley no ha llegado. Los efectos, sí

España lleva más de 18 meses en retraso en la transposición de NIS2. La directiva europea fijó el 17 de octubre de 2024 como plazo límite para que todos los Estados miembros la incorporaran a su derecho nacional. España no lo cumplió. El Anteproyecto de Ley de Coordinación y Gobernanza de la Ciberseguridad fue aprobado en Consejo de Ministros en enero de 2025, pero a fecha de hoy no ha sido remitido a las Cortes Generales. La Comisión Europea ya ha enviado un dictamen motivado que puede derivar en recurso ante el Tribunal de Justicia de la UE.

Este retraso no protege a nadie. Las grandes empresas y organismos regulados que sí están bajo el paraguas de NIS2 —o que se anticipan a su aplicación— ya exigen garantías de seguridad a sus proveedores. Y esto afecta directamente a PYMEs que, sobre el papel, no serían "entidades esenciales" ni "entidades importantes" según la directiva.

El efecto cascada: por qué NIS2 te afecta

NIS2 obliga a las entidades en su ámbito a gestionar los riesgos de seguridad de toda su cadena de proveedores y subcontratistas. Una empresa de software que vende a un banco tiene que acreditar que sus proveedores cumplen estándares mínimos. Un integrador logístico que trabaja con una gran distribuidora deberá demostrar que su acceso a sistemas está controlado. El cumplimiento se traslada escalón a escalón.

El mecanismo es directo: el cliente grande —sujeto a NIS2— traslada sus obligaciones hacia abajo en forma de cláusulas contractuales, cuestionarios, auditorías o requisitos de certificación. Si no los cumples, dejas de ser un proveedor elegible. No es una amenaza futura: ya ocurre en licitaciones del sector público, en contratos con corporaciones financieras y en sectores como la industria o la salud.

El número de incidentes gestionados por el INCIBE —el Instituto Nacional de Ciberseguridad— alcanzó los 122.223 en 2025, un 26% más que el año anterior. Al

mismo tiempo, casi la mitad de las pymes españolas invierte menos de 500 euros anuales en ciberseguridad, según el Barómetro de Digitalización de la pyme española elaborado por Gigas e Ipsos sobre 1.300 empresas. La brecha entre riesgo real e inversión en protección es enorme, y NIS2 —con o sin transposición formal— está acelerando su corrección desde arriba de la cadena de valor.

Cuatro acciones concretas, ordenadas de menor a mayor esfuerzo

La ventaja de actuar antes de que la ley esté en vigor es que puedes hacerlo a tu ritmo, sin la presión de un plazo regulatorio encima. Estas cuatro acciones generan valor inmediato independientemente del calendario legislativo.

Primera. Documenta lo que ya haces. La mayoría de pymes aplica controles de seguridad razonables sin haberlos registrado. Tener correo con autenticación reforzada, copias de seguridad automáticas o acceso restringido por perfiles no vale de nada ante una auditoría si no existe evidencia escrita. Dedica dos tardes a inventariar qué sistemas usáis, quién tiene acceso a qué y cómo salen los datos de vuestra red. Ese inventario es el punto de partida de cualquier evaluación de riesgos y el primer documento que pedirá un cliente que os audite.

Segunda. Haz un simulacro de cuestionario de cliente. Descarga el cuestionario de seguridad de alguna empresa grande de tu sector —muchos son públicos— y respóndelo honestamente. Las preguntas que no puedas contestar señalan tus brechas reales. Este ejercicio lleva menos de una jornada y produce un diagnóstico más útil que muchas auditorías formales, porque parte de las exigencias concretas del mercado, no de marcos teóricos.

Tercera. Define un protocolo mínimo de respuesta a incidentes. NIS2 exige notificar incidentes significativos en plazos muy ajustados: aviso inicial en 24 horas, notificación completa en 72. Sin un procedimiento escrito —quién decide, quién notifica, a quién— el tiempo se consume en caos interno. El protocolo no tiene que ser largo: dos páginas con los roles, los umbrales de activación y los contactos de notificación son suficientes para empezar, y te diferencian de forma inmediata ante cualquier auditoría.

Cuarta. Asigna un responsable de seguridad, aunque sea a tiempo parcial. La directiva establece que el órgano de dirección debe aprobar y supervisar las medidas de ciberseguridad. Esto no significa contratar un director de seguridad a jornada completa —para la mayoría de pymes no tiene sentido económico—, pero sí que alguien en la empresa debe ser el interlocutor de estas decisiones: el responsable de IT, el COO, o un asesor externo. Lo importante es que exista, que tenga autoridad real y que participe en las decisiones de negocio con criterio propio.

NIS2 establece de forma explícita que los miembros del órgano de dirección pueden ser considerados personalmente responsables por el incumplimiento de las obligaciones de seguridad de su organización. Las multas pueden alcanzar los 10 millones de euros o el 2% de la facturación mundial para entidades esenciales, y los 7 millones para las importantes. No son cifras abstractas: son el marco que España deberá incorporar en su legislación, más pronto que tarde.

Existe una tendencia comprensible a pensar que, mientras la ley no esté publicada en el BOE, no hay urgencia. Es un error de cálculo. Los clientes grandes no esperan al BOE para exigir garantías a sus proveedores. Los incidentes no esperan. Y cuando la ley llegue, los plazos de adaptación serán cortos para quienes no hayan empezado.

La ciberseguridad dejó de ser un problema técnico hace tiempo. Es una decisión de dirección que define, cada vez más, si una pyme puede seguir compitiendo en los mercados donde trabaja.

Tendencias

La fiebre del token y el espejismo de la productividad

Hay épocas en las que la tecnología se compra como antes se compraban las promesas: con ansiedad, con prisa y con la vaga intuición de que quedarse fuera saldrá más caro que entrar sin saber muy bien para qué. Estamos en una de esas épocas. La inteligencia artificial ha dejado de ser solo una herramienta para convertirse en una señal de estatus corporativo, en un indicador de modernidad y, cada vez más, en una métrica de supuesto rendimiento. Y ahí empieza el problema.

En Silicon Valley ya circula una idea que, observada con calma, resulta profundamente reveladora: además de salario, bonus y equity, algunas nuevas contrataciones empiezan a recibir capacidad de uso de IA, es decir, tokens. No solo como herramienta de trabajo, sino como parte del paquete de valor ofrecido al profesional. La escena es casi perfecta como síntoma de época. Antes se competía con oficina, acciones o flexibilidad. Ahora también con potencia de cómputo.

La pregunta no es si esto ocurrirá de forma más visible en las ofertas laborales. La pregunta importante es qué nos dice este movimiento sobre la forma en que empezamos a entender el trabajo técnico. Porque cuando el acceso a tokens se convierte en incentivo, y el consumo de tokens empieza a leerse como señal de productividad, el riesgo ya no es tecnológico: es conceptual.

Consumir más no equivale a producir más. Parece una obviedad, pero es precisamente el tipo de obviedad que suele desaparecer cuando una industria entra en estado de euforia. Si un desarrollador utiliza una gran cantidad de tokens de IA, lo único que sabemos con certeza es que ha utilizado una gran cantidad de tokens de IA. Nada más. No sabemos si ha resuelto mejor un problema, si ha reducido deuda técnica, si ha construido software útil o si simplemente ha desplazado a una máquina una secuencia caótica de pruebas, consultas, iteraciones irrelevantes y ocurrencias sin dirección.

Confundir consumo con resultado es uno de los errores más antiguos de la gestión. Ha ocurrido con las horas presenciales, con las líneas de código y con cualquier métrica que, por ser fácil

Tendencias

La fiebre del token y el espejismo de la productividad

de medir, termina pareciendo importante. Ahora el turno es de los tokens.

Y, sin embargo, el contexto invita a esa confusión. La inversión en inteligencia artificial está siendo una de las más grandes de la historia de la informática. Se construyen infraestructuras, se amplía capacidad de cómputo, se cierran acuerdos energéticos, se reorganizan cadenas de suministro y se tensiona el mercado entero para alimentar una expectativa de uso masivo. Todo parece preparado para un único desenlace: que el consumo crezca sin descanso.

Pero toda gran apuesta industrial necesita una demanda acorde. Y cuando esa demanda no llega al ritmo esperado, aparece la tentación de fabricarla culturalmente.

Por eso no sorprende que las grandes compañías del sector hayan convertido el uso de la IA en objeto de promoción constante. Influencers, campañas, demostraciones espectaculares, contenido patrocinado, tutoriales simplificados y una avalancha de mensajes diseñados para empujar a millones de personas a incorporar la IA a su vida cotidiana, aunque a veces el caso de uso sea poco más que una frivolidad simpática. El objetivo ya no es solo mostrar capacidad tecnológica, es normalizar el consumo. Hacerlo deseable. Hacerlo inevitable.

Y el dato acompaña esa tendencia: las plataformas de IA generativa gastaron más de 1.000 millones de dólares en anuncios digitales en Estados Unidos durante 2025, con un crecimiento del 125% respecto al año anterior. La cifra es importante no solo por su tamaño, sino por lo que anticipa. Cuando una industria necesita semejante presión comercial, no está únicamente educando al mercado. También está empujándolo.

Ahora bien, sería absurdo concluir de aquí que la IA no aporta productividad. Claro que puede aportarla. Bien utilizada, elimina tareas manuales, reduce fricción, acelera análisis, ayuda a explorar alternativas y libera tiempo para pensar mejor. Ese es su valor real: no sustituir criterio por potencia, sino quitar del medio trabajo repetitivo para que el talento humano se concentre en lo que de verdad importa.

El problema aparece cuando esa relación se pervierte y empezamos a premiar el uso por el uso. Cuando surge incluso una versión caricaturesca del fenómeno, como el tokenmaxxing: la maximización deliberada del consumo de tokens como demostración de actividad, sofisticación o rendimiento. Es difícil imaginar una metáfora mejor de nuestro tiempo: gastar más recursos para aparentar más valor, aunque el resultado no cambie sustancialmente.

Ahí conviene recordar una idea tan simple como incómoda: la potencia sin control sigue

Toda gran apuesta industrial necesita una demanda acorde. Y cuando esa demanda no llega al ritmo esperado, aparece la tentación de fabricarla

sin servir de nada. Y, en este caso, podríamos añadir algo más: la potencia sin conversión en producto útil tampoco.

Porque al final la productividad del desarrollo no debería medirse por lo que entra en la máquina, sino por lo que sale de ella con sentido de negocio. Si esa capacidad de IA se transforma en software pedido, necesario y alineado con objetivos reales, entonces estamos ante una mejora. Si no, estamos ante consumo decorado de innovación.

La unidad de medida no es el token. Es el producto software.

Lo que importa es cuánto software útil, funcional y valioso se genera. Y a partir de ahí sí emerge una métrica verdaderamente interesante: cuántos tokens han sido necesarios por unidad de producto software entregado. Ahí empezamos a hablar de eficiencia de verdad. Porque dos desarrolladores pueden producir el mismo resultado, pero si uno requiere mucho menos consumo de IA para lograrlo, entonces no solo es productivo: es más óptimo, más sostenible y probablemente más consciente de la herramienta que utiliza.

Ese es el cambio de enfoque que necesitamos. Dejar de admirar el gasto y empezar a evaluar la conversión. Dejar de medir combustible y empezar a medir movimiento. Dejar de confundir actividad con impacto.

La IA puede multiplicar la capacidad de los equipos. Pero no convierte automáticamente el despilfarro en progreso. Para eso sigue haciendo falta criterio, dirección y una manera seria de observar el resultado.

El producto software, al final, sigue siendo el rey. Y todo lo demás, tokens incluidos, solo tiene valor si logra ponerse a su servicio.

> **La IA puede multiplicar la capacidad de los equipos. Pero no convierte automáticamente el despilfarro en progreso**

Entrevista

Juan Carlos Sánchez de la Fuente, Vicepresidente Regional de Cloudera para España y Portugal

"Cloudera vende un framework, no los datos del cliente"

Manuel Navarro

El mercado de los datos y la inteligencia artificial avanza a una velocidad vertiginosa, pero no todas las empresas caminan al mismo ritmo. Cloudera afronta el presente ejercicio con la mirada puesta en la consolidación y el crecimiento en la región de Iberia. Entrevistamos a Juan Carlos Sánchez de la Fuente, Vicepresidente Regional de Cloudera para España y Portugal, para hablar sobre los objetivos de la compañía, la evolución técnica de su plataforma híbrida tras la compra de Tycoon, y la cruda realidad que revela su último informe Data Readiness.

Acaban de cerrar el primer trimestre de su año fiscal. Más allá de las cifras puras de facturación, ¿cuáles son los objetivos que se han marcado a medio plazo para la región de Iberia?
Nosotros arrancamos el año fiscal el pasado 1 de febrero con un propósito muy claro: seguir consolidando a Cloudera como la empresa líder en el mercado de España y Portugal. Nuestro objetivo es el crecimiento a doble dígito, y la línea que hemos conseguido durante este primer trimestre (Q1) mantiene esa tendencia positiva. Venimos de un año con unos excelentes resultados a nivel

Entrevista

Juan Carlos Sánchez, Vicepresidente Regional de Cloudera para España y Portugal

global, donde oficializamos el mejor año de la historia de la compañía. Esos datos históricos se replicaron tanto en la región de EMEA como en España. El mercado está respondiendo muy bien a la estrategia que marcamos hace unos años; mantenemos unos índices de confiabilidad muy altos y seguimos incrementando nuestra cartera de clientes con proyectos altamente estratégicos. Queremos seguir siendo un player fundamental en el ecosistema de los datos y la IA.

En el plano de producto, han anunciado mejoras importantes en su plataforma híbrida de datos e inteligencia artificial. ¿En qué consisten exactamente estas actualizaciones?
Durante los diferentes eventos Evolve que celebramos el año pasado, compartimos un roadmap bastante agresivo en cuanto a tiempos para la evolución de nuestra plataforma Anywhere Cloud. Esos tiempos se están cumpliendo. Estamos trabajando sobre los pilares de privacidad, seguridad y escalabilidad en entornos híbridos.

Gracias a la adquisición de la plataforma de Tycoon, esta nueva versión totalmente orquestada y montada sobre Kubernetes estará disponible a lo largo de este año 2026. Actualmente ya estamos avanzando en technical previews con clientes estratégicos que actúan como design partners. Esta evolución nos permitirá integrar soluciones de terceros de una forma mucho más ágil, actuando como un catalizador que solucione problemas históricos del mercado como los silos de información. Nuestra visión es ser integrales con el ecosistema del cliente mediante un único motor de ejecución, independientemente de dónde esté el dato: en el edge, en el cloud o en el on-premise.

> **Los comités de dirección son totalmente conscientes de la importancia del dato. Ya no es un mensaje que intentemos imponer los fabricantes**

Ha mencionado la compra de Tycoon, anunciada en agosto del año pasado. ¿Qué ventajas reales están experimentando ya los clientes en la gestión de Kubernetes con esta integración?
Cloudera ya ofrecía soluciones sobre Kubernetes, pero la adquisición de Tycoon nos ha dado un acelerador tecnológico para que la plataforma no dependa de terceros, sino que sea propia e integral en contenedores. No compramos Tycoon por su cartera de clientes o para incrementar el beneficio de forma inmediata; fue una adquisición puramente tecnológica para acelerar el producto.

A día de hoy, esto permite que nuestros Data Services (las experiencias de almacenamiento, ingeniería de datos, data warehouse o IA) funcionen de forma segregada pero totalmente interoperable. El cliente puede trabajar de manera independiente en cada prisma, pero todo montado nativamente sobre Kubernetes, lo que garantiza que la experiencia sea exactamente igual tanto en la nube pública como en la nube privada.

Usted suele defender que el dato ha dejado de ser un activo técnico para convertirse en el motor estratégico de las empresas. Sin embargo, en el día a día se sigue hablando de silos y desajustes organizativos. ¿Son las compañías realmente conscientes de este mensaje o se queda en mera teoría?
Los comités de dirección son totalmente conscientes de la importancia del dato. Ya no es un mensaje que intentemos imponer los fabricantes, sino que son los propios clientes los que saben que su diferenciación en el mercado pasa por gestionar bien su información. Ahora bien, una cosa es la teoría y otra la práctica. Nuestro último informe Data Readiness analiza precisamente este desfase. Los clientes entienden que para ser exitosos necesitan datos gobernados e integrados, pero la realidad nos demuestra que a la mayoría de las organizaciones les cuesta horrores gestionarlo. Aquellas que logran controlar y centralizar su dato están demostrando un impulso diferencial inmediato en sus casos de uso, sean o no de IA generativa.

Entrevista

Juan Carlos Sánchez, Vicepresidente Regional de Cloudera para España y Portugal

Sorprende un dato de ese informe: solo el 18% de las empresas afirma tener sus datos listos para la IA, y esa cifra cae al 9% en el sector financiero. ¿Por qué es tan bajo el nivel de preparación en un sector que vive precisamente del dato?
Las entidades financieras y bancarias avanzan en muchas iniciativas individuales de IA, pero cuando buscan una transformación centralizada y consolidada de su modelo de negocio, se topan con una enorme complejidad estructural. Un banco tiene múltiples cores de negocio: omnicanalidad, banca privada, banca corporativa etc. Históricamente, cada división ha tenido sus propias iniciativas, creando silos. Cuando el consejo de dirección intenta unificar todo para aplicar IA diferencial, se da cuenta de que esa consolidación no existe.

El informe refleja a más de 1.300 empresas de todos los tamaños. Lo que vemos es que a mayor envergadura y mayor antigüedad de la compañía, más complejidad hay para arrastrar la obsolescencia de los sistemas heredados. En cambio, las empresas fintech o firmas de servicios financieros que han nacido en los últimos 5 o 10 años con un enfoque puramente online no tienen que lidiar con ese histórico y se adaptan mucho más rápido.

Mirando el panorama en España, y más allá del sector financiero, ¿qué sectores diría que están mejor preparados?
Más que hablar de sectores específicos, el factor determinante es la era en la que han nacido: las nacidas en la era digital cuentan con una ventaja obvia. Cada sector regulado tiene su propia complejidad. Nosotros trabajamos en entornos altamente complejos como el sanitario, farmacéutico, telecomunicaciones, energía o retail. En todos ellos se repiten los mismos retos: la seguridad, la elasticidad, la privacidad y, muy especialmente en nuestro mercado actual, la soberanía del dato. Las empresas líderes necesitan una evolución tecnológica para que el dato sea el motor de la toma de decisiones, no un quebradero de cabeza regulatorio.

Otro de los grandes mantras actuales de Cloudera es que hay que "llevar la IA al dato y no el dato a la IA". ¿Me puede explicar este concepto de forma sencilla?
Para mí esta es la esencia y el gran elemento diferencial. Imagina que tus datos son un conjunto de bolígrafos de diferentes tamaños y colores guardados en tu despacho. Si utilizas una plataforma de IA tradicional, lo que te piden es: "Saca tus bolígrafos de ahí y tráemelos a mi entorno, que yo haré maravillas con ellos". En ese viaje, estás perdiendo el control perimetral de tu información.

Lo que Cloudera propone es lo contrario: mantén los bolígrafos en tu entorno seguro y bajo tu estricto control (ya sea en tu infraestructura o en tu cloud privada). Nosotros encapsulamos el modelo de IA y lo llevamos a donde están tus datos. El cliente mantiene el perímetro. No desarrollamos modelos propios; facilitamos la infraestructura para que puedas integrar el modelo que quieras, ya sea público o privado. Lo importante es que la IA se ejecute allí donde tú controlas el dato.

Cloudera es una empresa estadounidense y la legislación de este país genera cierta inquietud en Europa ante la posibilidad de que el gobierno pueda solicitar acceso a información confidencial. ¿Cómo garantizan a una empresa española que sus datos están 100% a salvo?
Es un matiz fundamental. Cloudera España es, efectivamente, una subsidiaria de Cloudera Inc., una compañía americana. Sin embargo, a nosotros no nos afectan normativas como la AI Act de la misma manera que a otros porque nosotros nunca gestionamos ni almacenamos el dato del cliente. Lo que vendemos es un framework, una plataforma de trabajo. Técnicamente nos es imposible acceder a la información de nuestros clientes. No tenemos que firmar contratos de uso de datos porque no tenemos acceso a ellos; el dato se queda siempre en la infraestructura del cliente. Es como si fuéramos un fabricante de coches: te vendemos el vehículo, pero nunca sabremos quién se monta en él. En cambio, cuando te llevas los datos a la infraestructura de otros proveedores de servicios en la nube, sí les estás entregando la custodia.

Cibercotizante

José Joaquín Flechoso
Presidente de Cibercotizante

MareNostrum el superordenador español que aspira al liderazgo europeo

La ampliación del superordenador MareNostrum del Barcelona Supercomputing Center (BSC) marca un punto de inflexión en la capacidad científica y tecnológica de España. No se trata únicamente de aumentar la potencia de cálculo, sino de consolidar una infraestructura estratégica que sitúa al país en la primera línea mundial de la supercomputación.

Esta actualización permitirá aumentar la capacidad de procesamiento de MareNostrum 5 casi en un 50%. Otro de los principales objetivos de la estrategia es la creación de un plan de modelos de lenguaje en castellano y lenguas cooficiales, ALIA, abiertos y transparentes y que eviten sesgos y mejoren la calidad de las aplicaciones.

El BSC será el coordinador técnico del plan de modelos del lenguaje, que será fundamental para fortalecer la diversidad lingüística del país y desarrollar aplicaciones multilingües con aplicaciones en la industria.

La ampliación del MareNostrum tiene un impacto directo en áreas críticas como la medicina personalizada, la genómica, el descubrimiento de fármacos, la simulación de proteínas o el análisis masivo de datos biomédicos. También abre nuevas posibilidades en la investigación climática, permitiendo modelos atmosféricos y oceánicos de ultra-alta resolución capaces de anticipar fenómenos extremos con mayor precisión. En sectores como la energía, la ingeniería o los materiales avanzados, el superordenador permitirá simulaciones más complejas y rápidas, acelerando la innovación industrial y la transición hacia tecnologías más eficientes y sostenibles. MareNostrum 5 forma parte de la iniciativa EuroHPC, la gran apuesta de la Unión Europea para construir una red de supercomputación que garantice independencia científica y competitividad global. En este contexto, España desempeña un papel protagonista al albergar una de las infraestructuras más potentes del continente y liderar proyectos de investigación en computación avanzada, IA y simulación científica. La ampliación del superordenador no solo atrae talento internacional, sino que consolida a Barcelona como un hub científico de referencia mundial. Su impacto se extiende también al tejido productivo, impulsando a empresas tecnológicas, startups y centros de innovación que encuentran en el BSC un aliado para desarrollar soluciones de alto valor añadido.