byte TI

348 · Mayo 2026

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

Cómo aplicar la IA en la estrategia empresariales

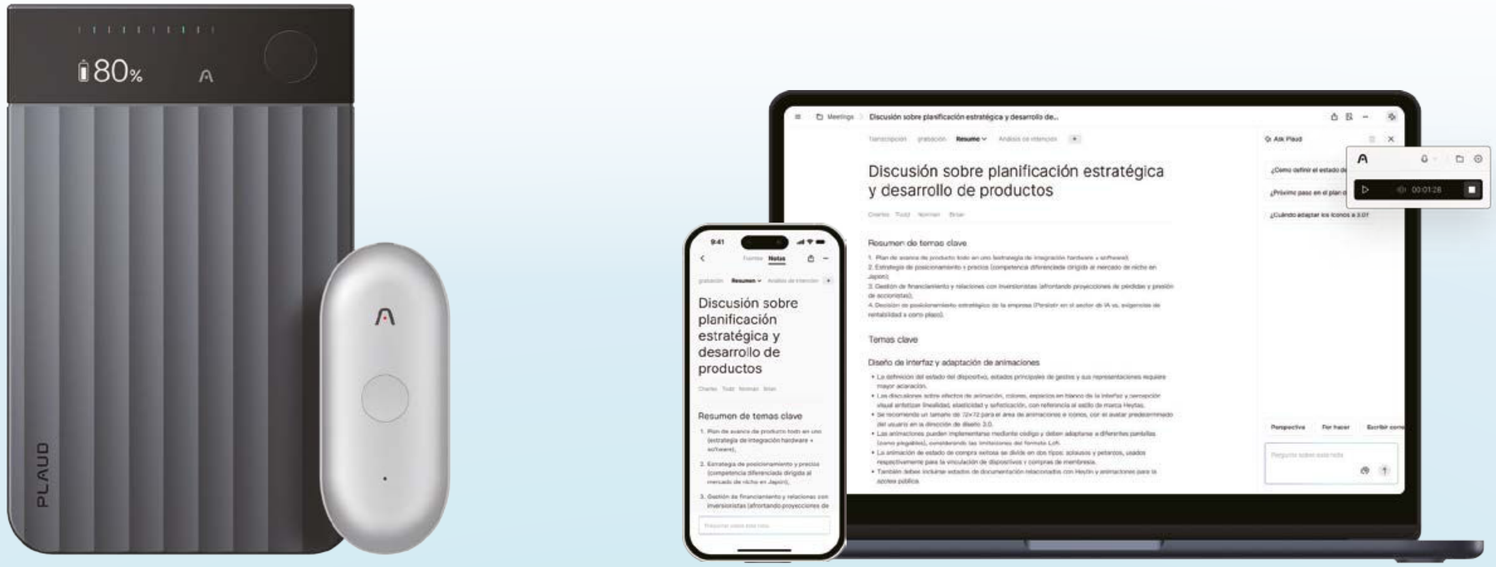
World: ¿Qué hay detrás de la tecnología para demostrar que eres humano?

COMPARATIVA
Plataformas EDR/XDR a examen

mkm PUBLICACIONES

PLAUD

Las mejores decisiones tienen lugar en conversaciones que no se deben olvidar.



El dispositivo de IA que te libera de tomar notas.

4.9
4.7
GDPR
SOC 2
HIPAA
EN 18031

Para más información

4 **Carta del Director**

5 **Actualidad**

22 **Webinars y encuentros BYTE TI**

36 **Comparativa**
5 plataformas EDR/XDR a examen

44 **Cómo evitar dependencias y ganar flexibilidad gestionando la nube**

54 **Un CIO en 20 líneas** Bjørn R. Watne

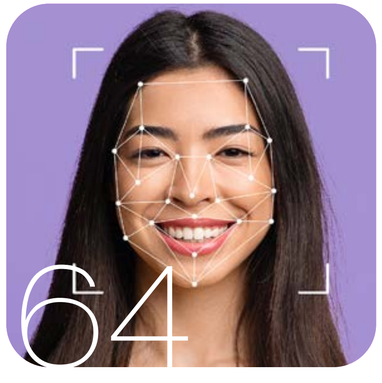
58 **Legalidad TIC**

61 **Aplicación práctica**

64 **Tendencias**

69 **Entrevista** Matt Calkins

73 **Cibercotizante**



N. 348 | ÉPOCA IV
Edita:
Publicaciones Informáticas MKM
Mayo 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

© Reservados todos los derechos.
Se prohíbe la reproducción total o parcial por ningún medio, electrónico o mecánico de los artículos aparecidos en este número sin la autorizació expresa por escrito del titular del Copyright. La cabecera de esta revista es Copyright de Publicaciones Informáticas MKM. Todos los derechos reservados. Publicado con la autorización de Publicaciones Informáticas MKM. La reproducción de cualquier forma, en cualquier idioma, en todo o parte sin el consentimiento escrito de Publicaciones Informáticas MKM, queda terminantemente prohibida. Byte TI es una marca registrada de Publicaciones Informáticas MKM.

Carta del Director

Manuel Navarro Ruiz
Director de BYTE TI

Presumimos de ser sostenibles, pero no

Lo de la sostenibilidad es una de las grandes mentiras actuales. Incluso, los más preocupados sólo la valoran si no les afecta a su vida diaria. ¿Dejamos de viajar? ¿Se dejan de utilizar las redes sociales por su impacto medioambiental? ¿Se abandonan los hábitos de consumo? Me temo que la respuesta es negativa. Nadie está dispuesto a cambiar su forma de vida, salvo que el cambio le suponga alguna ventaja.

Traducido al mundo empresarial, sucede prácticamente lo mismo. Todas las empresas presumen de dar pasos para ser más sostenibles. Pero en realidad, al igual que nos ocurre a los individuos, sólo se valora si realmente supone un beneficio para la organización.

Un ejemplo es el teletrabajo. En estos momentos, a primera hora de cada mañana, no se puede circular por las grandes ciudades. Todo el mundo cogiendo el coche para ir a trabajar. Se suponía que la pandemia iba a provocar un cambio radical. No era que el teletrabajo se fuera a imponer, pero si que se iba a producir una apuesta clara por los modelos híbridos. Entre otros mensajes, las empresas lo valoraban positivamente por "nuestra política por conseguir un mundo más sostenible".

Otras personas han cambiado de opinión, pero en el caso de algunas compañías la modificación del rumbo ha sido brutal. Algunas han pasado de ser los adalides del teletrabajo y sus bondades a obligar a todos los empleados a asistir a las oficinas, reduciendo incluso los días de teletrabajo que se tenían antes de la pandemia.

Kone, el fabricante de ascensores, confirma esta tendencia en un estudio reciente que asegura que se ha producido un crecimiento del 21% en el uso de oficinas en 2025 con respecto al año anterior. ¿Somos sostenibles? Más bien, no.

Cuando se habla de sostenibilidad, independientemente de si se trata de organizaciones o de individuos, lo que priman son otros factores, que luego disfrazamos de sostenibilidad. El principal de los disfraces es el ahorro de costes. La persona que se compra un coche eléctrico, no lo hace pensando en el medioambiente. Lo hace por que va a gastar menos en combustible y reparaciones. De la misma forma, las empresas no se van a la nube porque su centro de datos sea poco sostenible, sino porque el coste es menor. No vendamos de sostenibilidad lo que no es.

Actualidad

Appian World 2026: la IA de la Costa Este frente a Silicon Valley

Matt Calkins nunca defrauda. Sigue siendo una de las pocas voces dentro del sector tecnológico que intenta poner coto a los desmanes que otras empresas tecnológicas llevan a cabo cuando de la Inteligencia Artificial se trata. Este año, durante la celebración del Appian World 2026 que se está celebrando en Orlando (EE.UU.), acuñó el término "IA de la costa este" como contrapunto a la IA de Silicon Valley donde parece que todo vale.

Calkins comparó la evolución de la IA con la invención de la bombilla, que tardó 14 años en ser verdaderamente impactante tras superar batallas de estándares y mejoras técnicas. El máximo responsable de la compañía hizo mención a un estudio que han realizado en colaboración con Harvard Business Review, y en el que se afirma que la IA actual se utiliza ampliamente para la eficiencia personal y el recorte de costes, pero es raramente empleada para el crecimiento estratégico o aplicaciones que tomen decisiones de negocio críticas.

Para solucionar esto, Calkins incidió en que el modelo de las firmas de Silicon Valley no es el adecuado ya que no prioriza ni la responsabilidad y el rigor. Para explicar su punto de vista, Calkins subrayó "la IA es probabilística por lo que requiere un marco determinista, basado en procesos, para ser fiable. En este modelo, el proceso actúa como una "máquina de fiabilidad" que proporciona a la IA los raíles, los datos y la integración necesarios para trabajar en equipo". Como ejemplo de este éxito, mencionó la solución de Appian DocCenter, una solución que logra un 99% de precisión en el procesamiento de documentos, superando ampliamente el estándar de la industria del 60%.

Hacia una precisión de "nueves"

Un punto clave de la ponencia en Appian World 2026 fue la introducción del término "spec-driven development", algo así como desarrollo impulsado por especificaciones, frente al popular "vibe coding". Calkins explicó que, aunque programar basándose en sensaciones o lenguaje natural es aceptable para aplicaciones de baja criticidad, no es suficiente para sectores como el farmacéutico, el financiero o para misiones espaciales de la NASA, que requieren múltiples "nueves" de fiabilidad (99.99%).

Para alcanzar estos niveles, Appian presentó en Appian World 2026 la nueva versión de **Composer**, una herramienta que utiliza lenguaje natural

Actualidad

Appian World 2026: la IA de la Costa Este frente a Silicon Valley

para generar aplicaciones, pero permitiendo al usuario **auditar y validar cada regla, interfaz y unión de datos** antes de que el código se escriba definitivamente. Tal y como explicó, "Composer tiene tres casos de uso. Se puede utilizar para construir nuevas aplicaciones. Esto es ahora nuestro método principal de creación. Segundo, se puede usar para migrar aplicaciones legacy a la plataforma Appian. Y tercero, se puede emplear para mejorar continuamente aplicaciones existentes".

Es decir, Appian ha convertido el lenguaje natural en su nuevo estándar de desarrollo, dejando atrás las viejas fórmulas. Esto quiere decir que si antes se construían objetos de aplicación uno por uno, ahora se agrega una palabra y Composer crea todos los objetos que se necesitan y los une en una aplicación funcional de Appian, lo que significa poder y alta fiabilidad en nueves, data fabric, IA con barreras responsables y valor probado y confiable.

Además, Calkins hizo un llamamiento urgente a la modernización de sistemas legacy durante su intervención en Appian World 2026: "Con la aparición de IAs como "Mythos", capaces de hackear aplicaciones antiguas, la migración de silos de datos de más de 20 años a plataformas modernas y seguras se ha convertido en una prioridad de seguridad nacional y no solo en una cuestión de eficiencia operativa".

Los agentes seguros

Uno de los ejemplos en la manera de afrontar la IA de Appian con respecto a la agresividad de Silicon Valley se aprecia en el caso de los agentes. La apuesta de Appian pasa por que sus agentes sean más inteligentes, seguros y efectivos y para ello inciden en que tengan mejor estructura, contexto y barreras de protección.

En este sentido, Appian está mejorando la interoperabilidad en todo su ecosistema de IA. Al adoptar estándares potentes como el Protocolo de Contexto de Modelo (MCP), los agentes de Appian podrán interconectar de forma segura con sistemas empresariales externos. Los agentes de IA de terceros tendrán acceso a herramientas potentes de Appian como el data fabric, que proporciona de manera única acceso unificado de lectura y escritura a los datos empresariales.

Tal y como se pudo comprobar en Appian World 2026, Appian también está avanzando en el aprendizaje de agentes al permitir a los usuarios rastrear el rendimiento de los agentes y luego aplicar la memoria de un agente a través de procesos para mejorar la toma de decisiones. De esta forma, los usuarios podrán expandir esto dando orientación a la IA sobre qué objetivos optimizar y recomendando mejoras que se puedan aplicar de forma segura.

Asimismo, el data fabric de Appian, uno de sus productos estrella, ha sido mejorado para proporcionar un modelo de metadatos unificado que da a los agentes un contexto más claro sobre cómo está estructurada y conectada la información a través de sistemas.

Siguiendo su compromiso de apoyar plataformas de datos líderes en la industria, Appian ha anunciado en Appian World 2026 una asociación con Snowflake. Esto une a Appian como capa de orquestación de IA con la Nube de Datos de IA de Snowflake, combinando agregación de datos, entrenamiento de modelos y orquestación de procesos para habilitar valor empresarial inmediato. La integración directa habilitada por MCP entre el data fabric de Appian y Snowflake equipa a los agentes con contexto empresarial profundo y les permite interactuar directamente con Snowflake Cortex AI para impulsar decisiones inteligentes respaldadas por datos.

Actualidad

TrendAI alerta de una mayor alineación entre ciberataques e intereses geopolíticos

La unidad de Trend Micro, TrendAI, ha publicado un nuevo informe sobre el nuevo panorama que surge a raíz de una mayor alineación entre los ciberataques y los intereses geopolíticos. El informe detecta una creciente colaboración entre grupos APT y una convergencia cada vez más clara entre operaciones digitales, ciberataques, objetivos estratégicos de los estados e incluso dinámicas militares o de influencia.

Entre los hallazgos más relevantes, TrendAI destaca el uso de modelos de lenguaje en malware activo para sofisticar ciberataques, la consolidación de esquemas de acceso compartido como Premier Pass-as-a-Service y el creciente protagonismo de infraestructuras edge y cadena de suministro como vectores de entrada, persistencia y despliegue de ciberataques.

"Estamos ante un cambio estructural en la amenaza. La IA ha dejado de ser un apoyo puntual para convertirse en un multiplicador operativo que acelera los ciberataques y reduce drásticamente los tiempos de respuesta del defensor", señala José de la Cruz, director técnico de TrendAI. "El reto para las empresas y administraciones públicas ya no es solo evitar la entrada de ciberataques, sino ser capaces de detectarlos antes, contenerlos mejor y recuperarse más rápido".

Operaciones vinculadas a ciberataques

El informe también sitúa 2026 como un momento clave en la carrera por la soberanía tecnológica, especialmente en el ámbito de la inteligencia artificial. China aparece como el actor más avanzado en el desarrollo de capacidades propias, mientras que otros países como Rusia o Corea del Norte continúan dependiendo en mayor medida de tecnologías externas para reforzar operaciones vinculadas a ciberataques.

De cara a los próximos meses, TrendAI anticipa una aceleración de esta tendencia, en la que la velocidad y la automatización marcarán la diferencia. Ante este contexto, la compañía insiste en la necesidad de replantear las estrategias de ciberseguridad frente al aumento de los ciberataques. El informe recomienda abandonar los enfoques centrados exclusivamente en la prevención y apostar por modelos basados en visibilidad continua, capacidad de contención y recuperación rápida. En un entorno donde los ciberataques y las intrusiones son cada vez más inevitables, concluye, la resiliencia se convierte en el principal factor para garantizar la continuidad de negocio.

FERNANDO JOFRE

Volatilidad como norma global

Si algo está definiendo 2026 es que la volatilidad ha dejado de ser una anomalía. Forrester ya lo resumía con clarividencia en sus predicciones de octubre: **"Volatility: The Only Sure Thing in 2026"**. Y los acontecimientos internacionales recientes no han hecho más que amplificar esta realidad.

Para los equipos directivos, esto significa liderar en un entorno donde **los proyectos de IA pueden descarrilar**, los presupuestos deben justificarse de forma continua y los equipos se fragmentan entre empleados, gig workers y agentes de IA. La incertidumbre geopolítica añade una capa adicional: interrupciones en cadenas de suministro digitales, tensiones en infraestructuras críticas y oscilaciones bruscas en costes energéticos que afectan directamente a la operación tecnológica.

En este contexto, la clave no es resistir la volatilidad, sino **operar dentro de ella**. Reforzar la gobernanza de IA, anticipar escenarios, diversificar proveedores, asegurar resiliencia operativa y cultivar liderazgo adaptable ya no son buenas prácticas: son condiciones de supervivencia. Las organizaciones que traten la volatilidad como un elemento estructural —y no como una crisis pasajera— serán las que mantengan el rumbo en un mundo que cambia más rápido que nunca.

Actualidad

Cisco lanza Universal Quantum Switch para allanar el camino de la red cuántica

Cisco ha anunciado su Universal Quantum Switch, un prototipo de investigación operativo, que constituye el avance más reciente del programa de redes cuánticas de Cisco. Los ordenadores cuánticos codifican la información de diferentes maneras y, hasta ahora, ningún switch podía conservar la información cuántica en el proceso. El Universal Quantum Switch de Cisco está diseñado para superar este reto por primera vez, enrutando la información cuántica y conservándola y a través de la fibra óptica de telecomunicaciones existente, con un motor de conversión patentado por Cisco que traduce entre las modalidades de codificación en la entrada y la salida. Los ordenadores cuánticos actuales son potentes pero limitados. Operan con cientos de qubits, mientras las aplicaciones del mundo real en los sectores sanitario, de servicios financieros y aeroespacial necesitarán millones para alcanzar velocidades sin precedentes y avances tecnológicos. Cisco cree que las redes y la conectividad resultan fundamentales para superar esa brecha.

Cómo funciona

Imaginemos conectar miles de millones de personas y decenas de miles de millones de dispositivos con cables directos. Sería imposible de gestionar. Internet fue posible porque los conmutadores clásicos podían conectar todos esos puntos finales a través de una red compartida y escalable. El Universal Quantum Switch hace lo mismo para la tecnología cuántica. Cuando dos ordenadores cuánticos necesitan compartir información, el switch acepta la señal en cualquier modalidad en que llegue, la traduce a un lenguaje común para su enrutamiento y la entrega en el formato que necesita el sistema receptor, sin perder ninguna información cuántica por el camino. Esto es posible gracias a un motor de conversión patentado por Cisco que se encuentra en el corazón del switch cuántico. La modalidad de salida puede coincidir con la de entrada o ser completamente diferente, permitiendo conectar y traducir entre sistemas cuánticos que nunca fueron diseñados para comunicarse entre sí, una capacidad fundamental para construir redes cuánticas que funcionen entre diferentes proveedores y tecnologías.

El Quantum Switch está diseñado para admitir todas las principales modalidades de codificación cuántica utilizadas para transportar información:

- Polarización (la orientación de las ondas de luz).
- Intervalo de tiempo (la sincronización de los pulsos de luz).
- Intervalo de frecuencia (el color o la frecuencia de la luz).

MANUEL LÓPEZ

La verdad incómoda de la IA: No es gratis y no puedes dejar de usarla

Durante años hemos visto repetirse el mismo patrón: primero llega la innovación, luego el hype... y finalmente, la factura. Con la IA estamos entrando justo en esa tercera fase. Nos vendieron que era "gratis", que podíamos jugar sin consecuencias. Pero la realidad es otra: **la IA nunca fue gratis** y ahora que la necesitamos para todo, **no podemos dejarla**.

El caso de **Claude Mythos** es la prueba más clara. Anthropic dice que es "demasiado bueno para lanzarlo". Lo que no dicen es que también es **demasiado caro de mantener vivo**. Hablamos de rangos de **10$–25$ por millón de tokens de entrada y 50$–125$ por millón de tokens de salida**. Si un usuario profesional consume cientos de millones de tokens al mes , el coste operativo para el proveedor puede superar los **20.000$ mensuales**. Y aun así te lo venden por 20, 40 o 200 dólares. Eso no es un modelo de negocio.

La otra mitad del problema es peor: **las empresas ya no pueden desconectar**. Automatización, soporte, análisis, desarrollo... todo depende de modelos que cada mes cuestan más. La dependencia es total, y cuando la dependencia es total, el precio deja de ser negociable y se convierte en una condición operativa. La IA gratuita fue el anzuelo. Ahora llega el coste real, y no hay botón de "exit".

Actualidad

AWS amplía su colaboración con OpenAI y anuncia novedades en IA agéntica

Durante el evento What's Next with AWS que ha tenido lugar en San Francisco, AWS ha anunciado una colaboración más amplia con OpenAI, así como nuevas soluciones y herramientas diseñadas para ofrecer a las empresas las opciones y la flexibilidad que necesitan para acelerar y transformar sus operaciones con IA agéntica.

Durante su intervención, Matt Garman, CEO de AWS, y Colleen Aubrey, vicepresidenta sénior de AWS Applied AI Solutions, debatieron sobre cómo estos nuevos "compañeros de equipo agénticos" permitirán a las organizaciones pasar de gestionar limitaciones a buscar nuevas posibilidades, brindando una experiencia a escala y llegando a más clientes. Además, Matt Garman también anunció la ampliación de su colaboración con OpenAI.

Anuncios más destacados

- **Actualizaciones de Quick:** AWS anunció actualizaciones para Quick, su asistente de IA, permitiéndole comprender mejor el contexto de un trabajo y las preferencias personales del usuario, de su equipo y su organización. Estas actualizaciones incluyen una nueva aplicación de escritorio que se ejecuta en segundo plano, se conecta a los archivos y aplicaciones, completa tareas y aprende cómo trabaja el usuario. Las nuevas capacidades permiten crear documentos, imágenes, hojas de cálculo y presentaciones, pero también dashboards en tiempo real

> **AWS ha actualizado Quick, su asistente de IA, permitiéndole comprender mejor el contexto de un trabajo**

Actualidad

AWS amplía su colaboración con OpenAI y anuncia novedades en IA agéntica

y páginas web sin necesidad de tener experiencia previa en programación.

- **Amazon Connect Family:** AWS está transformando Amazon Connect en un conjunto de soluciones diseñadas como compañeros de equipo de IA que aprenden del contexto empresarial, se adaptan a los flujos de trabajo y se vuelven más inteligentes con el tiempo.
  - Amazon Connect Decisions: disponible desde hoy, permite a los equipos de la cadena de suministro tomar decisiones más inteligentes en horas, no en días. Es un sistema de planificación y toma de decisiones para la cadena de suministro que combina más de 25 herramientas especializadas en esta área y 30 años de experiencia operativa de Amazon.
  - Amazon Connect Talent: una nueva solución de contratación que utiliza agentes de IA para generar planes de entrevistas estructurados con rapidez y que permite realizar entrevistas con voz natural. Esto acelera los procesos de semanas a días, siempre con personas al mando de las decisiones finales.
  - Amazon Connect Health: anunciado el mes pasado, es una solución de IA agéntica diseñada específicamente para el sector de la salud que maneja tareas críticas en todo el recorrido de atención, desde la reserva de citas hasta la codificación médica. Recientemente, AWS también lanzó Amazon Bio Discovery, una aplicación impulsada por IA que ayuda a los científicos a diseñar y probar nuevos medicamentos más rápidamente.

> **AWS ha transformado Amazon Connect en un conjunto de soluciones diseñadas como compañeros de equipo**

- **Amazon Connect Customer:** anteriormente conocido como Amazon Connect. Se trata de una solución de contact center omnicanal que ya gestiona millones de interacciones con clientes al día. Ahora incorpora nuevas opciones de configuración que permiten poner en marcha IA conversacional en semanas en lugar de meses.

- **AWS y OpenAI se unen:** AWS y OpenAI han anunciado una ampliación histórica de su colaboración, llevando los modelos más avanzados de OpenAI directamente a Amazon Bedrock, la plataforma en la nube en la que ya confían millones de organizaciones en todo el mundo. Este movimiento señala un cambio fundamental en cómo las empresas pueden acceder, implementar y gobernar la IA de vanguardia, sin tener que abandonar la infraestructura que ya conocen. La asociación presenta tres nuevas propuestas, todas actualmente en versión preliminar limitada:

- **Modelos de OpenAI en Amazon Bedrock:** las empresas ahora pueden acceder a los modelos más recientes de OpenAI a través de las mismas API de Bedrock que ya utilizan, junto con modelos de Anthropic, Meta, Mistral y otros, todo bajo un marco unificado de seguridad, gobernanza y control presupuestario.

- **Codex en Amazon Bedrock:** el agente de programación de OpenAI con más de 4 millones de usuarios semanales ahora está disponible en el entorno de AWS, lo que permite a los equipos de software empresarial automatizar los flujos de trabajo de desarrollo utilizando sus credenciales e infraestructura de AWS existentes.

- **Agentes gestionados de Amazon Bedrock, impulsados por OpenAI:** un camino simplificado para implementar a escala agentes de IA impulsados por OpenAI y listos para producción, con gestión de identidad integrada, capacidad de auditoría, memoria persistente y la infraestructura global de AWS incorporada desde el primer día.

Actualidad

Salesforce da la clave para que la IA no sea un "cuñado de Navidad"

Salesforce celebró ayer en Madrid su tradicional evento Agentforce World Tour Madrid 2026 en donde la multinacional ha atraído a más de 3.500 profesionales que han podido comprobar la visión de Salesforce en torno al pilar angular de la compañía: la IA agéntica.

En este contexto Marco Hernansanz, EVP & CEO de EMEA en Salesforce, ha sido el encargado de realizar la ponencia principal. La base de su discurso se ha sustentado en que la inteligencia artificial empresarial se encuentra en un punto crítico. A pesar del entusiasmo generalizado, la realidad es que el **95% de los proyectos piloto de IA no logran llegar a la fase de producción**. Esta cifra, respaldada por un estudio del MIT y por la experiencia directa de Salesforce con sus clientes locales, pone de manifiesto una brecha creciente entre las expectativas y los resultados tangibles.

Según Hernansanz, "este fracaso masivo no se debe a la falta de buenas ideas. El problema reside en un enfoque equivocado. Muchas organizaciones han centrado sus esfuerzos de forma exclusiva en los modelos de lenguaje (LLM), olvidando que éstos son sólo una pequeña parte de la solución total". El directivo explicó que "un LLM por sí solo es como un "cuñado de Navidad": alguien que habla con total confianza sobre cualquier tema, pero que a menudo está equivocado porque carece de base real. Un LLM "desconectado" no conoce al cliente, no conoce el producto y no tiene acceso a los datos y metadatos críticos de la empresa. Estos modelos pueden ser confiadamente erróneos", adviertió Hernansanz, señalando que esta falta de precisión y seguridad es lo que impide que la IA se despliegue en industrias reguladas como la banca o la sanidad.

La respuesta de Salesforce: una arquitectura de cuatro sistemas

Para cerrar esta brecha y permitir que las empresas escalen sus proyectos, Salesforce propone abandonar el "bricolaje" tecnológico y adoptar una arquitectura basada en cuatro pilares fundamentales integrados en su plataforma Agentforce.

El primer pilar es el Sistema de Contexto. Para que un agente de IA sea útil, debe "saber de qué habla". Hernansanz pone como ejemplo una aerolínea que gestiona la pérdida de una maleta:

el agente necesita datos en tiempo real sobre el cliente, el vuelo y la ubicación del equipaje. Sin este contexto, la IA es incapaz de ofrecer una respuesta válida. El segundo pilar es el Sistema de Trabajo, que representa la lógica y los flujos de procesos que la empresa ha perfeccionado durante años. Es lo que permite que el agente no solo informe, sino que actúe, como por ejemplo, accionando los sistemas necesarios para conceder un crédito bancario.

Actualidad

Salesforce da la clave para que la IA no sea un "cuñado de Navidad"

Los dos pilares restantes son el Sistema de Agentes, una infraestructura para crear, testear y monitorizar el comportamiento de la IA, y el Sistema de Interacción, que facilita la colaboración en tiempo real entre humanos y agentes. Hernansanz subraya que esta es una "arquitectura abierta": las empresas pueden integrar sus propios Data Lakes y sus modelos de lenguaje previamente entrenados. "El poder está en la conexión", afirma, instando a las compañías a no dejar sus datos bajo llave en "bóvedas" inaccesibles, sino a ponerlos al servicio de los empleados que interactúan con los clientes.

Más allá de la tecnología: Valores y una nueva economía de la abundancia

El éxito de esta transición hacia lo que Hernansanz denomina la "empresa agéntica" no depende únicamente de la arquitectura técnica, sino de los cimientos sobre los que se construye la organización. Salesforce fundamenta toda su estrategia en cinco valores core: confianza (Trust), éxito del cliente, innovación, igualdad y sostenibilidad. En la era de la IA, la confianza se vuelve un valor crítico que debe aplicarse desde el nivel del dato hasta el uso ético de la tecnología.

La verdadera revolución, según explicó Hernansanz durante su intervención, es el cambio de paradigma en el trabajo. Históricamente, las empresas han operado bajo **economías de restricción**, limitadas por presupuestos rígidos, dificultades para ampliar equipos de forma rápida y presiones constantes de tiempo. La IA agéntica rompe estas barreras al funcionar como una "fuerza de trabajo virtual infinita" capaz de razonar y orquestar tareas. "Nos movemos de una economía de restricciones a una economía de abundancia", sentenció el directivo.

Este cambio es urgente debido a un entorno macro y micro cada vez más exigente. A nivel macro, la inestabilidad geopolítica y la competencia de países con menos regulación presionan a las empresas europeas a actuar. A nivel micro, los clientes ya no se conforman con menos de lo que obtienen en entornos conversacionales modernos, y los equipos directivos han dejado de interesarse por la innovación "por amor al arte" para exigir un retorno de inversión (ROI) real que impacte en la cuenta de resultados.

Hernansanz finalizo su intervención asegurando que la fase de experimentación con la IA ha terminado. Con competidores, clientes y empleados moviéndose a gran velocidad, el riesgo ya no es innovar, sino tardar demasiado en arrancar y quedar fuera de la nueva economía agéntica. Aquellas empresas que logren integrar contexto, trabajo, agentes e interacción serán las que lideren esta nueva era de abundancia.

Actualidad

Salesforce da la clave para que la IA no sea un "cuñado de Navidad"

Puesta en práctica

Los casos de éxito han sido los grandes protagonistas del evento. En el keynote principal han participado representantes de CaixaBank, Fever y Universidad Europea. En el área de exposición, Agentforce City ha sido el epicentro del Agentforce World Tour Madrid 2026, siendo el espacio más destacado y ambicioso de esta edición. Concebido como un entorno inmersivo, esta zona de exhibición ha estado dedicada a mostrar la realidad de la Empresa Agéntica con agentes en producción. Las empresas participantes en Agentforce City fueron las siguientes:

- **AEDAS Homes** está implementando agentes autónomos en dos áreas clave: Lara como Asesor de Promociones y Félix para el Servicio PostVenta. El agente Lara está entrenado para responder a consultas de potenciales clientes sobre cualquier proyecto inmobiliario, informar sobre promociones y coordinar la primera visita al punto de venta.

- **CaixaBank** está implementando agentes de IA para ofrecer asistencia especializada a clientes y empleados. Un caso de uso principal es un asistente de soporte a la contratación remota, que ayuda a los gestores a reducir el tiempo de interacción e impulsar la contratación de productos desde los canales digitales (app y web). En Agentforce City, CaixaBank presenta un agente de apoyo a los empleados de call center en la atención a clientes que solicitan vía online información sobre préstamos.

> **Salesforce fundamenta toda su estrategia en cinco valores core: confianza (Trust), éxito del cliente, innovación, igualdad y sostenibilidad.**

- **IBERIA** está desarrollando diversos casos de uso con Agentforce, incluyendo soluciones para aumentar la productividad de sus agentes de Contact Center y reducir los tiempos de atención. En el caso de Agentforce City, la compañía aérea presenta SofIA, un agente al servicio de los empleados que facilita a Personas responder dudas sobre cualquier aspecto relativo a la compañía.

- **Universidad Europea** utiliza Agentforce como asesor de Programas Educativos para estudiantes. Su caso de uso se centra en el desarrollo de un recomendador de grados, masters u otros programas de formación a medida y responder preguntas frecuentes. El agente también permite pre-cualificar el interés de los potenciales alumnos y escalar el caso a un agente humano.

- **Pikolin** está utilizando Agentforce para desarrollar un asesor técnico experto que resuelve dudas complejas sobre materiales y tecnologías de descanso, facilitando una decisión de compra asistida, automatizando la respuesta sobre tiempos de entrega y permitiendo que el cliente decida con toda la información técnica a su alcance..

- **Repsol** utiliza Agentforce de Salesforce para transformar la experiencia y los canales de comunicación con sus clientes, evolucionando de bots tradicionales a interacciones en lenguaje natural capaces de entender el contexto y ejecutar transacciones complejas. Esta tecnología ya se aplica en Ventas, con la gestión conversacional de pedidos de GLP (butano) por WhatsApp, que facilita un autoservicio personalizado; en Atención al Cliente, con un soporte inteligente integrado en el contact center que ayuda a los gestores y propone respuestas adaptadas; y en la web, donde los clientes cuentan con un chat de IA para resolver consultas.

Actualidad – Te interesa

El camino hacia una arquitectura Zero Trust real

Por ADRIÁ SOLANA,
Zero Trust

Zero Trust es uno de esos conceptos que, a fuerza de repetirse, corren el riesgo de perder significado. Se menciona con frecuencia en presentaciones comerciales, titulares y pliegos normativos, pero cuando una organización decide llevarlo a la práctica surge una pregunta clave: ¿por dónde empezar? La entrada en vigor de normativas como NIS2 ha acelerado esta reflexión, obligando a muchas entidades a demostrar que su modelo de seguridad va más allá del perímetro tradicional. En ese contexto conviene aclarar una idea fundamental: Zero Trust no se compra ni se instala. Se diseña, se recorre y se mide.

Lejos de ser un producto concreto, Zero Trust es un modelo de seguridad definido por el NIST en su estándar SP 800-207. Se apoya en tres principios básicos: verificar explícitamente cada acceso teniendo en cuenta identidad, dispositivo, contexto y riesgo; conceder siempre el mínimo privilegio necesario y únicamente durante el tiempo imprescindible; y asumir que la brecha ya se ha producido, diseñando controles que limiten su impacto. El reto no está en entender estos principios, sino en aplicarlos de forma coherente sobre identidades, dispositivos, redes, aplicaciones, datos y gobierno. No existe un interruptor único que lo resuelva todo.

Uno de los errores más comunes es abordar Zero Trust como un destino final, en lugar de como un camino evolutivo. En este punto, el modelo de madurez de Zero Trust de CISA se ha convertido en una referencia práctica. Plantea cuatro etapas —tradicional, inicial, avanzada y óptima— a lo largo de cinco pilares: identidad, dispositivos, redes, aplicaciones y datos, apoyados por capacidades transversales como visibilidad, automatización y gobierno. Este enfoque permite evaluar con honestidad el punto de partida, priorizar acciones según el riesgo real y demostrar avances de forma medible ante dirección, auditores y reguladores.

No todas las organizaciones parten del mismo punto ni recorren el mismo camino. Las compañías con entornos TI tradicionales suelen tener más madura la identidad, pero menos trabajada la protección del dato. En entornos industriales u OT ocurre a menudo lo contrario. Por eso, una iniciativa de Zero Trust sólida no debería comenzar con una arquitectura objetivo, sino con una evaluación de madurez por pilar y un roadmap realista, de 12 a 24 meses, con hitos verificables.

También conviene evitar errores habituales. El primero es pensar que desplegar MFA equivale a implantar Zero Trust: es necesario, pero claramente insuficiente. El segundo, comprar herramientas antes de definir políticas claras de identidad, dispositivos y datos, lo que solo amplifica el desorden existente. Y el tercero, tratar Zero Trust como un proyecto exclusivo de seguridad, sin involucrar a operaciones, soporte y experiencia de usuario, lo que suele generar fricción y rechazo interno.

Aunque muchas iniciativas nacen del cumplimiento normativo —NIS2, ENS o ISO 27001—, limitarse a ese objetivo es perder valor. Una arquitectura Zero Trust bien gobernada reduce la superficie de ataque, acelera la respuesta a incidentes y facilita la adopción segura de nuevas tecnologías, incluida la IA generativa. El cumplimiento llega como consecuencia. La pregunta clave, por tanto, no es qué herramienta de Zero Trust elegir, sino en qué punto del modelo de madurez se encuentra cada organización y cuál es el siguiente paso que más reduce su riesgo. Esa es la conversación que realmente marca la diferencia.

Actualidad – Te interesa

El problema del cloud no es la falta de flexibilidad, es la falta de arquitectura

Durante años, el discurso sobre cloud ha estado sostenido sobre un solo argumento: la flexibilidad. Escalar, desplegar y adaptar bajo demanda se ha convertido en uno de los principales argumentos para justificar su adopción.

A medida que el uso de cloud madura, empieza a imponerse una realidad menos conveniente: la limitación no es la flexibilidad. El problema es la falta de arquitectura.

En demasiadas ocasiones, el cloud se ve como una suma de decisiones tácticas, proyectos aislados o urgencias operativas. Se despliega rápido, se escala sin fricción, pero sin un diseño que ordene el conjunto. El resultado no es flexibilidad, es pérdida de gobierno, costes que crecen sin control, dependencias opacas y riesgos que aparecen cuando impactan en continuidad o cumplimiento.

No es un fallo del cloud. Es la consecuencia de haber operado sin arquitectura. Las grandes organizaciones ya no están decidiendo si usar cloud, están intentando contener lo que ya han construido. El problema no es consumir más tecnología, sino estructurarla mejor: decidir qué carga debe ir a cada entorno, bajo qué criterios de decisión, con qué modelo de gobierno y con qué garantías de continuidad.

La evolución hacia modelos híbridos responde precisamente a este aprendizaje: no todas las cargas tienen las mismas exigencias ni toleran el mismo modelo operativo. Algunas necesitan elasticidad; otras, control; otras, latencia mínima o soberanía del dato; otras, marcos de cumplimiento estrictos.

Forzar un único modelo para todo no simplifica. Introduce ineficiencia estructural y concentra riesgo en decisiones mal alineadas con la operación. Pero lo híbrido tampoco resuelve nada por sí solo. Combinar cloud público, privado o entornos dedicados sin un modelo común, introduce más puntos de fallo, más dependencia y más opacidad operativa.

Este enfoque es aún más relevante en el contexto regulatorio actual. Normativas como NIS2, DORA o el Esquema Nacional de Seguridad en sus niveles más exigentes están obligando a las organizaciones a demostrar control real sobre su infraestructura: saber qué ocurre, quién accede, cómo se comportan los sistemas y cómo responden ante incidentes.

El cumplimiento ya no puede abordarse como una capa adicional de seguridad. Tiene que formar parte del diseño. Lo mismo ocurre con la resiliencia. La resiliencia no consiste en improvisar cuando algo cae, sino en haber diseñado de antemano cómo se aísla el fallo, cómo se recupera el servicio y qué impacto es aceptable para el negocio.

La soberanía cloud debe entenderse desde esta lógica: no depende únicamente de en qué país se almacena la información, sino de dónde y quién la procesa, cómo se custodia y bajo qué normativas se opera (hay datos que avalan que el 60% de la información se procesa bajo la normativa de EEUU y/o China). La flexibilidad sigue siendo importante, pero ya no basta. En entornos complejos, lo diferencial no es desplegar más rápido, sino hacerlo sobre una arquitectura gobernable, auditable y preparada para crecer sin perder control.

Actualidad – Te interesa

Más allá del software: el primer pilar de la ciberseguridad está en el cableado

Aunque la ciberseguridad suele abordarse como un desafío puramente digital, la protección real comienza mucho antes: en la infraestructura física. Un estudio reciente de Intel indica que más del 70% de los responsables de TI considera que la seguridad debe integrarse desde esta base, lo que obliga a replantear el enfoque tradicional centrado exclusivamente en el software. Sin embargo, la práctica demuestra que este principio aún no está plenamente incorporado. Según InstaTunnel (2025), las vulnerabilidades explotables en dispositivos físicos crecieron un 88% en 2024. El auge del IoT y la proliferación de dispositivos conectados han ampliado considerablemente la superficie de ataque, mientras que la infraestructura física sigue siendo un punto débil en muchas organizaciones.

Parte del problema radica en ciertos mitos persistentes. El primero es pensar que la seguridad depende únicamente de herramientas como firewalls o antivirus. Si la base física es vulnerable, cualquier capa digital resulta insuficiente. La manipulación de puertos, cables o paneles puede comprometer una red incluso bien configurada.

El segundo mito es considerar el cableado como un elemento secundario. En realidad, representa uno de los primeros vectores de acceso físico. Cables de baja calidad, instalaciones deficientes o conexiones descontroladas pueden abrir la puerta a riesgos que el software no puede mitigar. La calidad del cable, su blindaje y su correcta instalación impactan tanto en el rendimiento como en la seguridad, especialmente en entornos críticos como los centros de datos.

El tercer mito es asumir que los datacenters están protegidos por defecto. La realidad es que la seguridad física y la lógica forman un único sistema interdependiente. Un fallo en el cableado o en el acceso físico puede provocar interrupciones, accesos no autorizados o fugas de información que escapan a las herramientas tradicionales de ciberseguridad.

Frente a este escenario, reforzar la infraestructura física se vuelve imprescindible. La segmentación de red, tanto lógica como física, permite limitar la propagación de incidentes y reducir la exposición. Asimismo, el control de accesos y puertos —mediante autenticación, desactivación de puertos no utilizados y políticas de red— elimina puntos de entrada innecesarios.

La protección de racks y gabinetes también juega un rol clave como primera barrera física. El uso de estructuras robustas, con cerraduras seguras, dificulta la manipulación no autorizada. En paralelo, el cableado debe diseñarse con criterios de seguridad: materiales certificados, apantallamiento adecuado, rutas controladas y revisiones periódicas para detectar anomalías.

El orden y la documentación son igualmente críticos. Una infraestructura bien organizada permite identificar rápidamente cambios no autorizados y reduce errores operativos. Finalmente, la continuidad eléctrica, mediante sistemas de alimentación ininterrumpida, garantiza que los controles de seguridad permanezcan activos incluso ante fallos de suministro.

La ciberseguridad ya no puede entenderse como una capa aislada. Cada cable, cada conexión y cada componente físico forman parte del mismo sistema. En este contexto, fabricantes como Lanberg trabajan para que ese primer pilar —el físico— no sea una vulnerabilidad, sino una fortaleza, desarrollando soluciones que integran calidad, orden y seguridad desde la base de la infraestructura.

Actualidad – Te interesa

"Las soluciones de Supermicro permiten a Nemix adaptar cada integración exactamente al caso de uso"

Por JOSÉ JUAN LLANOS,
CEO de Nemix

Nemix lleva más de 30 años integrando infraestructura tecnológica para universidades, banca y telecomunicaciones.
En plena explosión de la IA, hablamos con su CEO, José Juan Llanos, sobre por qué muchas estrategias de IA fallan antes de empezar y por qué llevan tiempo apostando por Supermicro como fabricante de referencia en proyectos de IA.

¿Qué piden realmente los clientes cuando dicen que quieren adoptar IA?
Llegan con casos de uso bastante claros, pero con una idea muy difusa de lo que hay detrás. Hablan de modelos propios, inferencia en tiempo real, privacidad... pero no han dimensionado el impacto en cómputo, almacenamiento o red. Ahí es donde empieza el trabajo de Nemix, traducir una ambición de negocio en una arquitectura que funcione. Porque la IA no falla por el modelo, falla por todo lo que lo rodea.

¿Por qué Supermicro como fabricante de referencia para proyectos de IA?
Es un fabricante que nos permite integrar soluciones completas sin atarnos a una única configuración. Trabajamos con todo su ecosistema tecnológico: servidores rack, servidores GPU, almacenamiento, red... Eso nos da flexibilidad real a la hora de diseñar la solución exacta que cada cliente necesita.

¿Cómo ha cambiado la demanda de hardware Supermicro desde que la IA entró en la agenda de las empresas?
Antes los proyectos giraban principalmente en torno a virtualización, almacenamiento y servidores de propósito general. Ahora los clientes preguntan por GPUs, por capacidad de inferencia o por cómo escalar sin reemplazar todo. Por eso, trabajamos con el ecosistema de Supermicro, porque puedes ir desde un servidor GPU en 1U hasta sistemas multinodo de alta densidad, según dónde esté cada cliente en su madurez de IA.

¿Y eso cambia también cómo diseñáis las soluciones?
Totalmente. El margen de error es mucho menor. En IA, si el pipeline de datos no está bien diseñado desde el principio, todo se resiente. No es lo mismo entrenar modelos científicos en una universidad que detectar fraude en milisegundos en banca. Por eso, no trabajamos desde un catálogo cerrado, sino desde el workload real.

¿Cuál es el error más habitual que ves en proyectos de IA?
Pensar solo en GPUs. Es el titular fácil, pero el problema suele estar en otro sitio: almacenamiento insuficiente, redes que no dan el ancho de banda necesario, o una arquitectura de datos que no escala. Tampoco se contempla desde el principio el software y las licencias necesarias para que todo funcione y que tienen un impacto real en el coste y en los tiempos del proyecto.

El otro gran error es no pensar en el día dos. Quién opera esa infraestructura, cómo se mantiene o evoluciona. La IA no es un proyecto que se entrega y ya está; es un sistema vivo.
Y acompañar al cliente en esa evolución es exactamente lo que hacemos en Nemix.

Actualidad – Te interesa

Var Group eleva su presencia en España con la inauguración de su nueva sede en el centro financiero de Madrid

Var Group ha inaugurado sus nuevas oficinas en Madrid, ubicadas en la planta 23 de la emblemática Torre Emperador Castellana, uno de los enclaves empresariales más representativos de la capital. La elección de este espacio refuerza el posicionamiento de la compañía, proyectando una imagen alineada con la calidad, innovación y excelencia que define su servicio a clientes.

A lo largo de esta semana se han celebrado distintos actos con la propia plantilla y con varios de sus clientes y partners. Los actos han contado con la presencia de Francesca Moriani, CEO de Var Group; Gorka Jiménez, Country Manager en Iberia; y Fabrizio Saltalippi, International Business Leader de Var Group, quienes dieron la bienvenida a este nuevo espacio estratégico.

"Estas oficinas verifican que la penetración de Var Group en España ha sido un acierto. Aquella intuición de hace tres años, cuando se comenzó a gestar Var Group España, da sus frutos y nos estamos consolidando, con un expertise brutal y un sólido soporte internacional, con resultados creíbles", explicaron durante la inauguración. Las nuevas instalaciones cuentan con capacidad para albergar a 80 profesionales e integran infraestructuras clave como un Centro de Operaciones de Seguridad (SOC), además de estar diseñadas para adaptarse a políticas de trabajo flexible y modelos híbridos.

La inauguración de la oficina de Madrid se enmarca en el plan de expansión de Var Group en Iberia, donde actualmente cuenta con 285 profesionales —260 en España y 25 en Andorra— y una red de 8 oficinas en Madrid, Barcelona, Pamplona, Sevilla, Bilbao, Ceuta, Zaragoza y Andorra.

Desde el lanzamiento de Var Group Iberia en mayo de 2025, la compañía ha mantenido un crecimiento sostenido. Para el ejercicio fiscal 2026-2027, se prevé cerrar con una facturación de 25 millones de euros, lo que supone un crecimiento superior al 20%. A medio plazo, el objetivo es superar los 60 millones de euros y alcanzar los 500 empleados.

Con más de 200 clientes en España —repartidos entre el sector privado y público, siendo este último aproximadamente el 10%—, Var Group cuenta con una base sólida y diversificada que incluye grandes empresas del IBEX, multinacionales y pymes, sin dependencia de cuentas individuales.

La estrategia de expansión de la compañía combina crecimiento orgánico superior al 20% con crecimiento inorgánico orientado a complementar y reforzar sus capacidades tecnológicas.

El propósito de Var Group es acompañar a las organizaciones en su transformación digital bajo el concepto de One-Stop Partner, posicionándose como un socio de confianza capaz de ofrecer un soporte integral end-to-end.

La innovación es un eje central en este plan, con la integración de inteligencia artificial en todos los verticales del portfolio, con el objetivo de maximizar el valor aportado a clientes en materia de ciberseguridad, identidad digital, explotación del dato e integración de herramientas tecnológicas.

Actualidad – Te interesa

Cómo evitar dependencias y ganar flexibilidad gestionando en la nube

Javi Tejada Luna, CTO y CCO de h&k.

En el debate actual sobre multicloud vs. monocloud, ¿por qué defiende h&k que la especialización en un único proveedor puede reducir la dependencia real y no aumentarla?
Desde h&k defendemos que la dependencia no se mide por el número de proveedores, sino por cómo se diseña la arquitectura y el modelo operativo. Trabajar con múltiples nubes no elimina el vendor lock-in por sí solo; de hecho, muchas veces lo multiplica, porque incrementa la complejidad, los costes de integración y la superficie de riesgo.

Especializarnos en un único proveedor como Microsoft nos permite dominar profundamente la plataforma, conocer sus límites, diseñar arquitecturas desacopladas a nivel de aplicación y datos, y utilizar servicios estándar y ampliamente adoptados. Esta profundidad técnica es lo que realmente da libertad: saber qué partes son sustituibles y cuáles no, y tomar decisiones conscientes desde el diseño, no a posteriori.

Además, la madurez global de Azure en términos de regiones, disponibilidad y servicios gestionados hace que, en la práctica, el riesgo operativo sea menor que en arquitecturas repartidas pero mal gobernadas.

¿Cómo gana flexibilidad operativa en el día a día una pyme que opera sobre un stack unificado como Microsoft 365, Azure y Power Platform?
La flexibilidad aparece cuando las personas, los procesos y la tecnología hablan el mismo idioma. Un stack unificado permite que una pyme deje de 'traducir' entre herramientas constantemente.

Microsoft 365 cubre la colaboración y la productividad diaria; Azure sostiene la infraestructura y los sistemas críticos; y Power Platform conecta ambos mundos permitiendo adaptar procesos sin desarrollos complejos. Esto hace que una empresa pueda cambiar flujos, automatizar tareas o crear pequeñas aplicaciones internas en semanas, no en meses, y sin depender siempre de terceros. Desde nuestra experiencia, el impacto no es solo tecnológico: es cultural. El negocio empieza a ver la tecnología como algo maleable y propio, no como un freno.

¿Qué papel juega la gobernanza del dato y de los accesos en la reducción de dependencias tecnológicas y operativas en la nube?
La gobernanza es la base de todo lo demás. Sin un buen gobierno del dato y de los accesos, cualquier estrategia cloud o de IA se vuelve frágil.

Un modelo claro de clasificación de la información, control de identidades y accesos condicionales permite desacoplar personas, dispositivos y ubicaciones del acceso al dato. Eso reduce dependencias internas («solo sabe hacerlo esta persona») y externas («este proveedor es el único que controla el sistema»).

Además, con la llegada de la IA generativa, la gobernanza deja de ser invisible: de repente vemos qué información está disponible, para quién y en qué contexto. Quien haya trabajado

Actualidad – Te interesa

Cómo evitar dependencias y ganar flexibilidad gestionando en la nube

Las soluciones de IA aisladas suelen generar picos de uso inicial, pero poco impacto sostenido.

bien esta base tendrá una ventaja competitiva clara.

Muchas empresas adoptan múltiples herramientas buscando agilidad. ¿Cuáles son los costes ocultos —operativos, de seguridad o de integración— de esa fragmentación?
El principal coste oculto es la pérdida de visión global. Cada nueva herramienta promete resolver un problema concreto, pero pocas veces se evalúa su impacto en seguridad, integración, adopción y operación diaria.

A esto se suman costes menos evidentes: más identidades que gestionar, más puntos de fallo, más proveedores que coordinar y más conocimiento disperso. El resultado suele ser justo el contrario de la agilidad buscada.

En h&k no hablamos de menos herramientas por principio", sino de menos herramientas sin un propósito claro. Y cuando hace falta adaptar una herramienta estándar, ahí es donde el low-code encaja perfectamente.

Desde vuestra experiencia, ¿qué indicadores concretos (ahorro de tiempo, reducción de costes, productividad) demuestran que una estrategia cloud bien diseñada genera retorno en pymes?
Los indicadores más claros suelen ser tres:

- Reducción del tiempo dedicado a tareas manuales, gracias a automatización y flujos integrados.
- Optimización de costes, eliminando infraestructuras sobredimensionadas y pasando a modelos de pago por uso.
- Incremento de productividad y continuidad operativa, especialmente en entornos híbridos o distribuidos.

Un indicador muy tangible es la capacidad de escalar hacia arriba o hacia abajo según la carga real del negocio, algo prácticamente imposible en modelos tradicionales.

¿Cómo contribuyen plataformas low-code como Microsoft Power Platform a reducir la dependencia de desarrollos a medida y proveedores externos?
El low-code cambia la conversación. Deja de preguntar «¿quién me lo desarrolla?» para pasar a «¿quién decide cómo debe funcionar?».

Power Platform permite que muchos ajustes y evoluciones se hagan desde dentro de la propia organización, con gobierno y seguridad, pero sin esperas ni proyectos largos. Esto no elimina al partner, pero sí cambia su rol: pasamos de ejecutar tareas a diseñar bien el marco, asegurar calidad y acompañar al negocio.

¿En qué medida la integración nativa de IA —por ejemplo, con Microsoft Copilot— dentro del entorno de trabajo marca la diferencia frente a soluciones aisladas?
La diferencia es enorme. La IA aporta valor cuando está donde ya trabajan las personas. Copilot no obliga a cambiar de herramienta ni de hábito: actúa sobre Word, Excel, Outlook o Teams, utilizando el contexto del negocio y del usuario.

Las soluciones de IA aisladas suelen generar picos de uso inicial, pero poco impacto sostenido. La integración nativa es lo que convierte la IA en productividad real y no en una demo llamativa.

La automatización, según los gurús de la tecnología, debe ser una estrategia, no una táctica. ¿Cómo debe abordar una pyme la automatización de procesos para que realmente aporte flexibilidad y no genere nuevas rigideces?
Automatizar sin pensar es peligrosamente fácil. Por eso una pyme debe empezar por entender sus procesos, simplificarlos y estandarizarlos antes de automatizar.

Actualidad – Te interesa

Cómo evitar dependencias y ganar flexibilidad gestionando en la nube

La clave está en que la automatización sea reversible y evolutiva. Herramientas como Power Automate permiten empezar pequeño, aprender y escalar sin generar rigideces. Cuando la automatización se diseña como parte del proceso, y no como un parche, aporta flexibilidad, no dependencia.

Tradicionalmente, la ciberseguridad se ha percibido como una limitación. ¿Cómo puede convertirse en un elemento que aumente la agilidad y reduzca dependencias?
La seguridad bien diseñada es un facilitador. Permite trabajar desde cualquier lugar, con cualquier dispositivo autorizado, sin perder control. Modelos como Zero Trust no dicen «no», dicen «demuéstrame quién eres, desde dónde accedes y en qué contexto». Eso da libertad al negocio y reduce riesgos. La alternativa suele ser la inseguridad o el bloqueo.

Tras las más de mil migraciones que lleva a sus espaldas h&k, ¿cuáles son los errores más comunes que generan dependencia innecesaria en proyectos de migración a la nube?
El error más habitual es ignorar la adopción de las personas. Migrar sistemas sin acompañar al usuario crea rechazo, atajos y soluciones paralelas que generan nuevas dependencias. Y otro error frecuente es replicar en la nube los mismos problemas del entorno anterior, sin replantear procesos ni modelos de gobierno.

> **La seguridad bien diseñada es un facilitador. Permite trabajar desde cualquier lugar, con cualquier dispositivo autorizado, sin perder control.**

¿Cómo influye una estrategia sólida de datos y analítica en la capacidad de una pyme para adaptarse rápidamente a cambios del mercado?
Los datos eliminan el «yo creo». Permiten reaccionar antes y con menos riesgo. Cuando una pyme confía en sus datos, puede probar, medir y corregir rápidamente. Plataformas modernas de analítica democratizan el acceso a información que antes solo tenían grandes corporaciones, y eso cambia completamente las reglas del juego.

¿Qué papel juegan los servicios gestionados en la reducción de dependencia técnica interna sin perder control sobre el negocio?
Los servicios gestionados bien entendidos liberan al equipo interno de la carga operativa, pero mantienen el control estratégico en la empresa. En h&k los entendemos como una extensión del cliente, no como una caja negra. Transparencia, alineación y transferencia de conocimiento son obligatorias para evitar dependencia.

Mirando a los próximos 3–5 años, ¿cómo evolucionará la relación entre nube, inteligencia artificial y autonomía tecnológica en las pymes?
Más que hablar de años, hablaría de meses. La combinación de cloud e IA está acelerando decisiones que antes se postergaban. La autonomía tecnológica crecerá, pero también la necesidad de gobierno, seguridad y estandarización. Las pymes que entiendan esto y se apoyen en partners adecuados avanzarán rápido; las que improvisen, se encontrarán con un ecosistema difícil de sostener.

Desde su experiencia, ¿por qué es clave contar con un partner como h&k que combine consultoría, desarrollo, datos y seguridad bajo una misma visión?
Porque hoy la tecnología ya no va por silos. Una decisión de datos impacta en seguridad; una decisión de desarrollo impacta en gobernanza; una decisión de IA impacta en personas. Un partner como h&k aporta visión transversal y continuidad en un entorno que cambia cada pocas semanas. Nuestro valor no está solo en implantar tecnología, sino en ayudar a tomar buenas decisiones de forma sostenida en el tiempo.

Eventos BYTE TI

Liderazgo TI: generando confianza digital en el negocio

Con el patrocinio de HCL Software, Kaspersky, Commvault, SUSE, encamina, Sophos, Barracuda y Penteo, Byte TI organizó un encuentro al que asistieron alrededor de 120 CIOs, CISOs y responsables de TI para descubrir cuáles sonlos retos que tienen las empresas en la actualidad. El evento se sustentó sobre cuatro pilares fundamentales como son la soberanía digital, el papel cada vez más estratégico del CIO, el retorno de la inversión en Inteligencia Artificial y la evolución del CISO hacia un perfil puramente orientado a resultados.

Manuel Navarro

Luis Alfaro, advisor de Penteo, fue el encargado de inaugurar el encuentro ofreciendo una radiografía del impacto de la inteligencia artificial en las empresas españolas y situó el debate en el terreno de los presupuestos, la productividad y la modernización tecnológica. Tal y como expuso, la firma de análisis está detectando un aumento del CAPEX, impulsado sobre todo por la migración de los ERP y la adaptación a nuevos entornos como SAP S/4HANA, mientras el OPEX continúa creciendo pese al esfuerzo por contenerlo.

Para Alfaro, "actualmente la gran prioridad de los CEOs es ganar eficiencia y producir más con los mismos recursos, aunque por primera vez también gana peso el crecimiento de ingresos. En ese contexto, la IA generativa concentra

Eventos BYTE TI

Liderazgo TI: generando confianza digital en el negocio

Varios momentos de las tres mesas redondas que tivieron lugar durante la celebración del encuentro.

más inversión, seguida de la ciberseguridad y el data analytics, mientras caen partidas como workplace y servidores". Alfaro subrayó que la adopción real de la Inteligencia Artificial "está avanzando con más rapidez en front office que en back office, y que todavía falta demostrar un retorno claro en muchos casos de uso".

El analista dejó un mensaje final para los asistentes en el que expuso que la IA abre oportunidades de automatización, analítica aumentada y nuevas funcionalidades, pero también exige equilibrar expectativas, inversión y capacidad de ejecución para no saturar a las organizaciones.

Desafíos operativos en la era de la IA

A continuación, Nacho Grieco, Sales Director Europe de Automation Orchestration en HCL Software, defendió en su intervención que la ventaja competitiva no depende tanto del talento individual como de la capacidad de coordinar operaciones complejas con precisión y escala. Para ilustrarlo, recurrió al fútbol y al último triunfo del Atlético de Madrid sobre el Barcelona como metáfora de un sistema bien ejecutado frente a un equipo con más recursos.

Griaco, consideró que "las empresas se encuentran en una nueva etapa marcada por la IA agéntica, una evolución que acelera la transformación tecnológica y obliga a repensar los modelos operacionales". En su diagnóstico, el reto no es sólo incorporar inteligencia artificial, sino decidir dónde aplicarla, cómo gobernarla y qué objetivos debe perseguir. Entre esos objetivos debe encontrarse la mejora de la eficiencia, la experiencia de cliente y el crecimiento o la generación de ingresos. También advirtió de que el corto plazo suele volver más complejas las operaciones de TI, pero insistió en que el coste de no transformarse es todavía mayor.

Ante este escenario, el ponente de HCL Software presentó a su compañía como "un socio capaz de orquestar cargas, procesos y agentes de IA desde un único punto de control, con capacidades de integración, automatización y gobernanza para entornos regulados y distribuidos".

Grieco cerró su ponencia con una idea central: las organizaciones que entiendan, controlen y coordinen mejor sus operaciones serán las que tendrán el liderazgo en los próximos años.

El ROI en la IA

Tras las dos primeras ponencias, tuvo lugar la primera de las mesas redondas. Con el título de "El ROI en la IA: cómo demostrar su valor real al Comité de Dirección", contó con la participación de

Eventos BYTE TI

Liderazgo TI: generando confianza digital en el negocio

Beatriz Méndez, CIO de Amadeus; Miguel Ángel González Gallego, CIO y CISO de Grupo ImesApi; Ricard Guasch, CIO de Zurich y Alberto Díaz Martín, CTIO de Encamina que se mostraron de acuerdo en que la Inteligencia Artificial ha pasado de ser una promesa a convertirse en una palanca de productividad, aunque su retorno debe medirse sobre procesos y resultados, no sobre la tecnología en abstracto. Los ponentes defendieron un enfoque híbrido entre prueba, transformación y adopción progresiva, subrayando la importancia del dato, la formación y la gestión del cambio para evitar que la IA se convierta en una simple moda.

Alberto Díaz Martín, CTIO de Encamina, sostuvo que el foco debe desplazarse del rendimiento de la herramienta al efecto que produce en la organización: "Yo creo que no tenemos que estar midiendo del ROI de lo que hace la inteligencia artificial, sino de los procesos que están afectados por esa inteligencia artificial". Su planteamiento resumió una de las ideas más repetidas de la mesa: la IA aporta valor cuando cambia la forma de trabajar, no cuando se convierte en un experimento aislado.

Por su parte, Ricard Guasch, CIO de Zurich, coincidió en esa visión y advirtió de que medir la IA de manera aislada puede ser incluso contraproducente. En su opinión, "medir el impacto de la inteligencia artificial como tal puede ser hasta un error. El verdadero retorno aparece cuando una compañía rediseña un proceso, lanza un producto nuevo o mejora su capacidad comercial a partir de la tecnología".

Miguel Ángel González Gallego, Global CIO y CISO de Grupo ImesAPI, puso el acento en la productividad personal como primer terreno visible de impacto. Contó que una presentación que antes requería días de trabajo se puede preparar en una hora con apoyo de IA, lo que demuestra que la eficiencia ya es una realidad en tareas concretas. Al mismo tiempo, recordó que la tecnología cambia rápido y que esa velocidad obliga a adaptar los métodos de trabajo y de experimentación.

Durante su intervención, Beatriz Méndez-Villamil, CIO de Amadeus, subrayó la necesidad de combinar convicción estratégica y rigor financiero a la hora de abordar la inversión en inteligencia artificial. "La apuesta debe ser una decisión estratégica, no únicamente financiera", afirmó. En este sentido, distinguió dos enfoques complementarios: uno basado en una confianza razonada en el potencial de la tecnología y otro apoyado en casos de uso tradicionales, ambos condicionados por procesos de adaptación progresiva y una gestión activa de la resistencia al cambio.

La mesa coincidió en que la inteligencia artificial no debe limitarse a automatizar la operativa existente, sino servir como palanca para

Inauguración del encuentro en el que se ofrecieron las claves de la actualidad tecnológica.

replantear los procesos desde su base. Méndez-Villamil incidió en que "no se trata de superponer la IA a los procesos actuales", sino de rediseñar la operativa para que agentes y herramientas inteligentes puedan ejecutar tareas dentro de una nueva lógica de trabajo, alineada con los objetivos del negocio.

En esa misma línea, Ricard Guasch explicó que el valor real en Zurich no está en el uso aislado

Eventos BYTE TI

Liderazgo TI: generando confianza digital en el negocio

de IA, sino en la transformación de productos y servicios. "Estamos vendiendo mucho más gracias al rediseño de todo el proceso de negocio, a los servicios que les proporcionamos", señaló.

Uno de los grandes temas de la mesa fue la adopción interna. Alberto Díaz Martín insistió en que la IA sólo funciona si los equipos entienden cómo usarla para aportar valor. A su juicio, "la formación, la evangelización y la documentación de procesos son condiciones imprescindibles para evitar que la organización se bloquee".

Miguel Ángel González Gallego apuntó que la resistencia no siempre nace del rechazo tecnológico, sino del miedo a perder el puesto de trabajo o a no saber adaptarse al cambio. Reconoció que en su compañía han impulsado sesiones de formación y acciones específicas para fomentar el uso de IA, aunque no todos los perfiles responden igual.

El valor del CIO

En este escenario, el CIO tiene un papel fundamental para impulsar el negocio. Entrevistado por Ignacio Liniers, Territory Sales Executive de Commvault, Mariano Domingo, CIO de Aena, explicó cuál es la importancia de su papel en el entramado de la compañía.

Domingo, describió que su día a día viene marcado por la coordinación interna, la relación con el negocio, la gestión de crisis y el apartado de la contratación pública. Gracias a que su perfil, no procede del mundo técnico, sino del negocio y la operación aeroportuaria, puede tender puentes entre la dirección ejecutiva y los equipos tecnológicos. "Para solventar mi déficit en la parte técnica me apoyo en un excelente equipo técnico del que aprendo a diario y en el que confío plenamente".

Domingo explicó que su llegada a al departamento de TI responde a una decisión estratégica para cerrar la brecha entre tecnología y negocio. Su trabajo diario abarca desde la participación en comités internos y reuniones estratégicas así como el seguimiento de proyectos clave, como la renovación de SAP a S/4HANA y su despliegue en la nube. También reconoció que, en una organización como Aena, la operativa no se detiene nunca, porque los aeropuertos trabajan 24/7 y cualquier incidencia puede activar comités de crisis.

Una parte central de la entrevista giró en torno a la confianza digital, un concepto que definió como "la capacidad de que usuarios, aerolíneas, agentes de handling y reguladores perciban que la tecnología funciona y aporta seguridad. En Aena esa confianza se traduce en experiencias cotidianas como una wifi estable, aplicaciones útiles y sistemas fiables para millones de pasajeros. Lo importante es que no sientan que hay tecnología detrás", aseguró.

Anticiparse al adversario

A continuación, Pedro Jorge Viana, Head of PreSales para Iberia, Reino Unido e Irlanda de Kaspersky, centró su ponencia en el valor de la inteligencia de amenazas como herramienta para anticipar ataques, reducir ruido operativo y mejorar la capacidad de respuesta de los equipos SOC. Su mensaje principal fue que "no basta con detectar eventos; hay que contextualizarlos, atribuirlos y convertirlos en información accionable para defender mejor a la organización".

Viana explicó que un analista de ciberseguridad se enfrenta hoy a una auténtica "capa de hielo" de alertas, IOCs, hashes, eventos de firewall, NDR, EDR y MDR, pero que la mayoría de esa información aparece desconectada entre sí. En ese contexto, la inteligencia de amenazas permite separar el ruido de lo realmente relevante, añadir contexto y relacionar indicadores aparentemente aislados para identificar campañas activas, actores concretos y posibles movimientos futuros. También advirtió del riesgo del burnout en los equipos de seguridad, saturados por el exceso de alertas.

Viana detalló cómo Kaspersky analiza el "ADN" del malware, compara patrones, relaciona

Eventos BYTE TI

Liderazgo TI: generando confianza digital en el negocio

técnicas, tácticas y procedimientos, y usa la conocida pirámide de dolor para centrarse en los elementos más difíciles de modificar por parte del atacante. Según explicó, este enfoque permite entender no solo quién ataca, sino también con qué objetivos, qué TTP emplea y cuál será probablemente su siguiente paso.

Retos de la Soberanía Digital

Una de las mayores preocupaciones actuales son las que tienen que ver con la soberanía digital. Para analizar todo ello, la mesa redonda "Retos de la Soberanía Digital en Empresas y Administraciones Públicas" contó con la participación de Roberto Lázaro, Sales Director de SUSE; Alberto Lozano, Products & Banking Services IT Director de ING; Fernando de Pablo Martín, Director General de la Oficina Digital Ayuntamiento de Madrid y Raúl Martín García, Subdirector Adjunto del SEPE.

Roberto Lázaro, Sales Director de SUSE, aseguró que "la soberanía digital no deja de ser un poco la definición que hacen todos los analistas, que no es más que la capacidad de las personas, de las empresas y de los organismos públicos de poder gestionar sus activos digitales sin interferencia de externos". También defendió que no se trata de un estado binario, sino de un nivel de exposición que cada organización debe medir y gestionar según sus servicios críticos y sus necesidades de resiliencia. A su juicio, el contexto europeo ha acelerado el interés por el tema, hasta el punto de que "ahora todo el mundo, lo primero que nos pregunta es si somos una empresa europea".

Por su parte, Alberto Lozano, Products & Banking Services IT Director de ING, situó el debate en una doble dimensión: política y técnica. Recordó que Europa arrastra una pérdida de competitividad y que la soberanía digital debe entenderse también como una cuestión estratégica ligada a qué aliados, proveedores y modelos de infraestructura se eligen. Para él, la clave es combinar eficiencia, cumplimiento regulatorio y capacidad de control sobre la propia operativa. "Yo entiendo que como técnico lo que tengo que tener es, con el presupuesto que se me ha asignado, dar la mejor solución posible a la organización", resumió.

Fernando de Pablo Martín, director general de la Oficina Digital del Ayuntamiento de Madrid, aportó una visión más institucional y centrada en los datos. Señaló que para la administración pública la soberanía digital afecta sobre todo al control de la operativa, la residencia de la información y el riesgo sobre los activos digitales. También alertó de que la desinformación es ya uno de los grandes riesgos globales y que la ciudadanía debe recuperar la confianza en el uso de sus datos. "Es necesario tener control sobre lo que tenemos, sea lo que sea, y tener la capacidad para retornar o revertir", afirmó como síntesis de su intervención.

Eventos BYTE TI

Liderazgo TI: generando confianza digital en el negocio

Finalmente, Rául Martín García, subdirector adjunto del SEPE, coincidió en que la dependencia tecnológica siempre ha existido, pero hoy se ha intensificado por el contexto geopolítico.

El CISO como impulsor del negocio

Finalmente, el encuentro se cerró con la mesa redonda "El CISO como impulso del negocio o por qué la seguridad supone una ventaja competitiva" que contó con la participación de Jaime Perea, Responsable de Gestión de Riesgos y Continuidad de Negocio en Carrefour; Daniel Damas, CISO de Nationale-Nederlanden; Juan Manuel Muñoz, CSO y CISO de Mawdy – Mapfre y Álvaro Fernández, Sales Manager de Sophos Iberia.

La mesa redonda giró en torno a la idea creciente de que la ciberseguridad ha dejado de ser un centro de coste para convertirse en una pieza de valor estratégico, siempre que esté alineada con el negocio, el riesgo asumible y la madurez de cada organización. Los ponentes coincidieron en que el nuevo escenario regulatorio, la presión de los clientes y la mayor exposición de las empresas obligan a los CISOs a dejar de ser perfiles puramente técnicos para asumir un papel más ejecutivo, transversal y orientado a la toma de decisiones.

En este sentido, Álvaro Fernández, Sales Manager de Sophos Iberia, explicó que "la ciberseguridad es una ventaja competitiva cuando va alineada con el negocio y va alineada con el nivel de riesgo tolerable para esa organización". A su juicio, "muchas compañías todavía invierten de forma desigual, protegiendo activos poco relevantes y dejando expuestos otros más críticos, por lo que es necesario tener herramientas que sean capaces de mostrar el riesgo en tiempo real y ayudar a priorizar las inversiones".

Juan Manuel Muñoz, CSO y CISO de Mawdy – Mapfre, reforzó esa visión al explicar que el cambio real consiste en pasar de ser solo habilitadores a ser "proveedores de valor del negocio". Según dijo, cuando la ciberseguridad entra en la propuesta de valor de la empresa, deja de ser una capa defensiva para convertirse en un factor competitivo. También afirmó que "los clientes quieren tener ciberseguridad en cualquier cosa que compran", una señal de que la seguridad ya forma parte de la decisión de compra.

Por su parte, Daniel Damas, CISO de Nationale-Nederlanden, describió cómo la relación entre seguridad y negocio ha cambiado en los últimos años. Explicó que antes, el área de ciberseguridad tenía que convencer a la organización para ser escuchada, mientras que ahora las áreas de negocio la llaman desde el inicio de los proyectos. "Ahora son ellos los que exigen. Ha cambiado el juego. Todo ello ha elevado la función del CISO a una posición más cercana al diseño y la arquitectura del negocio".

Jaime Perea, responsable de Gestión de Riesgos y Continuidad de Negocio en Carrefour, coincidió en que la seguridad ha pasado de ser reactiva a integrarse desde el principio en cualquier proyecto relevante. A su juicio, "la ciberseguridad ya no se percibe como una noticia aislada o como una función de bloqueo, sino como una capa transversal necesaria para que la compañía opere con seguridad y continuidad". Perea recordó que muchas organizaciones siguen dependiendo de automatismos y procesos informáticos susceptibles de fallos o ataques, lo que obliga a reforzar la anticipación y la resiliencia.

Uno de los puntos más debatidos fue el impacto de la regulación europea, en especial NIS2 y DORA, que han elevado la ciberseguridad al nivel de dirección y han reforzado la responsabilidad ejecutiva. Álvaro Fernández remarcó que estos marcos no solo imponen exigencias técnicas, sino que obligan a incorporar pensamiento estratégico en la gobernanza. Juan Manuel Muñoz fue más allá al señalar que "la "O" de CISO no es decorativa, sino que implica accountability real, algo que en entornos anglosajones se traduce en una responsabilidad ejecutiva más clara".

Daniel Damas insistió en que el CISO actual debe entender el negocio a fondo, hablar su lenguaje y ayudar a encontrar el equilibrio entre riesgo y oportunidad. Para él, la misión es colaborar en la mitigación para que el negocio siga avanzando".

Comidas BYTE TI

Cómo aplicar la IA en la estrategia empresarial

Para analizar cuál es el impacto de la IA, Byte TI, junto con Samsung, H&K y LinkRoad, organizó un encuentro en Barcelona que contó con la participación de Marc Paus, deputy director IT en IESE Business School; Joan Codina, director de Tecnología en Fundació Salut i Comunitat; Víctor Cuervo, head of Architecture en Banc Sabadell; Enrique Martín, director de ventas y desarrollo de negocio en grandes empresas y administraciones de Samsung; Xavier Altafulla, director de sistemas y tecnología del Museu Nacional d'Art de Catalunya; Lucas Viladomiu, Data AI Transformation Manager de H&K; Andrés Barreda, CIO de Encuentro Moda; Isidro Sánchez, IT Manager de Jotun; Albert Sierra, CIO de Cámara de Comercio de Barcelona; Nacho Santillana, socio director de LinkRoad; y Jordi Francés, exCIO de Applus.

Manuel Navarro

La inteligencia artificial ha dejado de ser una herramienta experimental para convertirse en un elemento estructural de la estrategia empresarial. Su adopción ya no se limita a proyectos piloto o a iniciativas aisladas de innovación, sino que empieza a influir en la forma en que las organizaciones diseñan procesos, toman decisiones, gestionan el talento y se relacionan con sus clientes.

Varios de los asistentes coincidieron en que la IA avanza con rapidez, pero que su éxito depende menos del despliegue tecnológico que de la calidad del dato, de la cultura interna y de la capacidad de las empresas para definir con claridad qué problema quieren resolver. También coincidieron en que la adopción debe hacerse con criterio: no todo caso de uso aporta valor, no toda automatización

Comidas BYTE TI

Cómo aplicar la IA en la estrategia empresariales

Albert Sierra,
CIO de Cámara de Comercio de Barcelona

Andrés Barreda,
CIO de Encuentro Moda

Enrique Martín, director de ventas y desarrollo de negocio en grandes empresas y administraciones de Samsung

Isidro Sánchez,
IT Manager de Jotun

mejora la eficiencia y no toda respuesta generada por un sistema inteligente merece ser aceptada sin supervisión. En ese equilibrio entre ambición y prudencia se está jugando buena parte del futuro de la transformación digital.

En varias de las intervenciones apareció la idea de que la IA ya ocupa un lugar central en los planes corporativos, aunque cada empresa la está incorporando con una lógica distinta. Por ejemplo, Marc Paus, deputy director IT en IESE Business School explicó que "la palabra más repetida en el plan estratégico 2026-2029 es IA". Afirmó que la institución la contempla en dos dimensiones: "por un lado, como herramienta interna para automatizar y mejorar procesos; por otro, como parte de la formación que ofrece al mercado". Su visión, insistió, es la de una IA humana, con criterio y con límites. En otras palabras, no se trata solo de hacer más con menos, sino de decidir qué debe hacer una máquina y qué sigue exigiendo juicio profesional.

Enrique Martín, director de ventas y desarrollo de negocio en grandes empresas y administraciones de Samsung subrayó que la compañía ha pasado de la seguridad a la IA y que ya la está aplicando en toda la organización, incluso en los electrodomésticos. Tal y como expuso, "la discusión no gira únicamente en torno a la capacidad técnica, sino a cómo llevar esa inteligencia a los dispositivos de forma útil y sostenible. Ahí aparecen tres conceptos que se repitieron en la conversación: ahorro, privacidad y escalabilidad. La IA, para ser realmente estratégica, debe generar eficiencia sin comprometer la confianza ni disparar la complejidad operativa".

Las empresas de servicios tecnológicos también están usando la IA como motor interno y como argumento comercial. Lucas Viladomiu, Data AI Transformation Manager de H&K explicó que "H&K, una consultora especializada en desarrollo y mantenimiento de software que unificó data e IA en su estructura para liderar la transformación digital desde dentro". Tal y como afirmó durante el encuentro, "una empresa que aspira a ayudar a otros a transformarse tiene que demostrar primero que sabe aplicar esa transformación en casa y eso es lo que hacemos nosotros".

Por su parte, Nacho Santillana, por su parte, describió a LinkRoad como "un grupo internacional preparado para acompañar a grandes compañías en su evolución digital con soluciones en cloud, experiencia digital, SAP, Data-AI y cumplimiento normativo".

Comidas BYTE TI

Cómo aplicar la IA en la estrategia empresariales

Joan Codina,
director de Tecnología en Fundació Salut i Comunitat

Jordi Francés,
exCIO de Applus

Lucas Viladomiu,
Data AI Transformation Manager de H&K

Marc Paus,
deputy director IT en IESE Business School

Casos de uso reales

El valor de la IA aparece antes en las tareas concretas que en los grandes discursos corporativos. Joan Codina, director de Tecnología en Fundació Salut i Comunitat explicó que "en el área informática utilizamos la IA para montar un PC, ayudar con programación, crear contenidos o responder correos electrónicos". También señaló que las herramientas que ya usan incorporan IA para diseñar un nuevo centro o resolver preguntas sobre cómo hacer algo que antes no sabían abordar. La lógica es sencilla: la inteligencia artificial se vuelve útil cuando reduce fricción, acelera decisiones o abre caminos que antes exigían demasiado tiempo.

En Banc Sabadell, Víctor Cuervo definió la IA como "una de las líneas básicas de transformación del banco". Su impacto, dijo, "alcanza a casi todas las áreas: conversaciones con clientes, contact center, recursos humanos, desarrollo y ciberseguridad. Esa amplitud la convierte en una tecnología transversal, pero también obliga a ordenar prioridades. No basta con desplegar soluciones; hay que seleccionar dónde la IA produce una mejora medible y dónde solo añade ruido".

En el ámbito cultural y público, Xavier Altafulla, director de sistemas y tecnología del Museu Nacional d'Art de Catalunya, introdujo una idea muy relevante: el equilibrio entre automatizar y no sobrecargar a los equipos de TI. Según explicó, "hay áreas donde la ganancia es mucho mayor que en otras, como el terreno legal, donde la IA puede ayudar notablemente en la redacción de textos jurídicos. Pero, para que el valor sea real, la organización debe formar a los usuarios y comprobar después que el uso que hacen de la herramienta es correcto. La fase decisiva no es la instalación, sino la adopción".

Por su parte, Andrés Barreda, CIO de Encuentro Moda, resumió su enfoque con una fórmula muy visual: "IA first". Con ella quiso decir que "antes de implantar una solución hay que preguntarse si aporta valor. En su organización, el primer caso de uso relevante está en el área de diseño, donde la IA ayuda a visualizar cómo quedará un estampado sobre una prenda". El ejemplo ilustra bien una tendencia común en el tejido empresarial: la IA empieza a entrar en procesos creativos y de negocio, no solo en tareas administrativas.

Datos y confianza

La conversación dejó claro que no puede haber una estrategia seria de IA sin una base sólida de

Comidas BYTE TI

Cómo aplicar la IA en la estrategia empresariales

Nacho Santillana, socio director de LinkRoad

Víctor Cuervo, head of Architecture en Banc Sabadell

Xavier Altafulla, director de sistemas y tecnología del Museu Nacional d'Art de Catalunya

datos. Lucas Viladomiu advirtió de que "muchas compañías intentan acelerar su entrada en inteligencia artificial sin haber resuelto antes cuestiones elementales como la calidad del dato, la seguridad o la estructura tecnológica". Su tesis es que antes de poner una capa inteligente sobre un sistema hay que limpiar el terreno y entender en qué estado real se encuentra la organización. Sin esa preparación, la IA corre el riesgo de amplificar errores en lugar de resolverlos.

La confianza es otro de los grandes retos. Nacho Santillana, socio director de LinkRoad, explicó que hoy existen herramientas para auditar el pensamiento de la IA y verificar qué está haciendo realmente el sistema. Santillana, advirtió de que "no todo lo que produce la máquina puede darse por bueno. A veces, las organizaciones validan respuestas sin analizarlas, aunque el ejemplo no sea trivial". Víctor Cuervo reforzó esa idea al señalar que la IA hace interpretaciones y que esas interpretaciones deben vigilarse. Por su parte, Lucas Viladomiu añadió que, en su empresa, cruzan dos puntos críticos antes de dar un resultado por válido.

Cambio cultural y productividad

El principal obstáculo ya no parece técnico, sino humano. Xavier Altafulla afirmó que "el reto más importante es la gestión del cambio, porque la IA obliga a trabajar con emociones, incentivos, carreras y expectativas. En muchas organizaciones, el verdadero debate no gira sobre la potencia del modelo, sino sobre el miedo de los equipos a quedar desplazados".

Por su parte, Andrés Barreda señaló precisamente que uno de los problemas es la percepción de que la IA puede dejar sin trabajo a parte de la plantilla. Sin embargo, recordó que "antes ocurría lo contrario: faltaba automatización. El desafío actual consiste en explicar el propósito de la herramienta y alinear a la organización con ese objetivo".

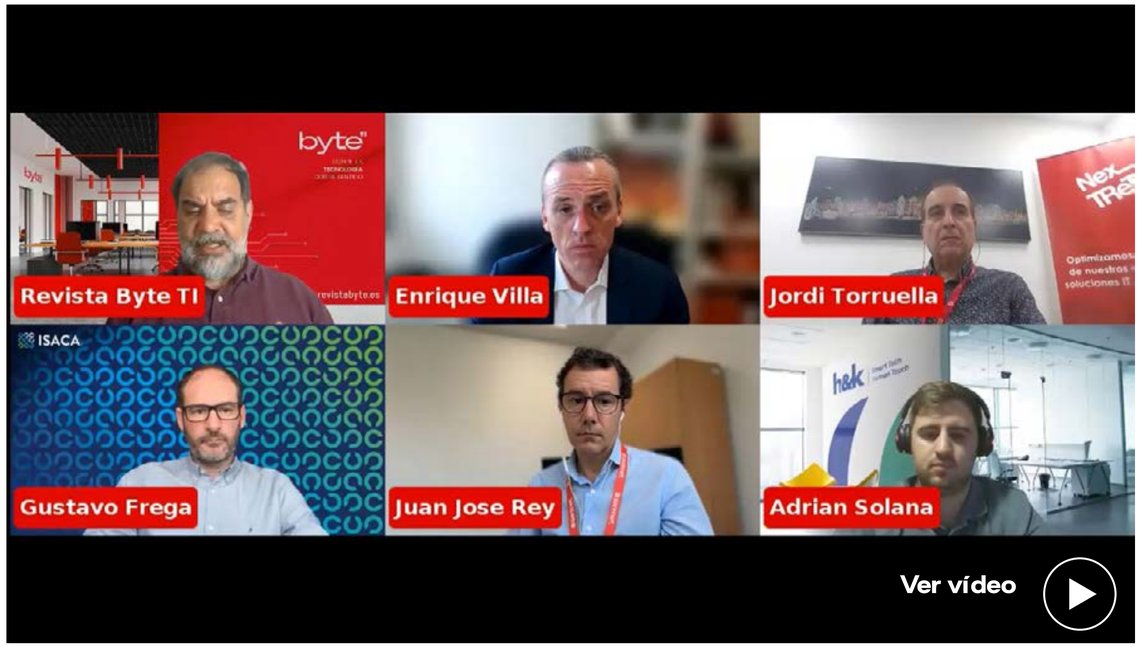
El CIO de la Cámara de Comercio de Barcelona, Albert Sierra, insistió en que la IA "debe entenderse como una palanca de aceleración y eficiencia, pero solo funcionará si va acompañada de cultura. En la Cámara de Comercio de Barcelona, hemos trabajado con la idea de "gobierno de la IA" del mismo modo que antes se hablaba de gobierno del dato. Para dinamizar su despliegue, incluso se ha identificado a una treintena de personas que la propia IA propuso como tractoras dentro de los departamentos. El objetivo no es solo automatizar tareas, sino redefinir qué hace la empresa con el tiempo que gana gracias a la automatización".

Finalmente, Jordi Francés añadió que la velocidad del cambio es tan alta que quien no se adapta se queda fuera. Lo comparó con revoluciones tecnológicas previas, desde la irrupción de internet hasta la expansión del iPhone, pero con una diferencia: "La IA está entrando más rápido y con un impacto más transversal. Esa aceleración obliga a las empresas a revisar su formación, sus procesos y, sobre todo, su manera de pensar. Porque la gran cuestión ya no es si la IA llegará,

Webinars BYTE TI

Ciberseguridad y protección de datos en la empresa

Manuel Navarro



La ciberseguridad es uno de los pilares de la empresa. Para analizar su situación Byte TI organizó un encuentro que contó con la participación de Adrià Solana, Security & Compliance Specialist de H&K; Juan José Rey, director de ventas zona centro de Sarenet; Gustavo Frega, Senior Academic Strategy and Business Partnership Manager de ISACA; Jordi Torruella, director de ciberseguridad de NexTReT; y Enrique Villa, Cybersecurity Sales Head de Var Group.

Los ponentes analizaron cómo han cambiado los riesgos digitales en la empresa y coincidieron en que la protección del dato, la gestión de accesos, la formación y la capacidad de ejecución siguen siendo los grandes desafíos, especialmente en el ámbito de la pyme.

La conversación dejó claro desde el principio que el problema de la ciberseguridad ya no puede resumirse en una lista de herramientas ni en una colección de amenazas aisladas. El ecosistema de riesgo se ha ampliado y, al mismo tiempo, se ha sofisticado. Adrià Solana, Security & Compliance Specialist de H&K situó entre los principales peligros el ransomware y las brechas de datos, dos amenazas que siguen plenamente vigentes en un momento en el que la información se ha convertido en uno de los activos más valiosos para las organizaciones. Según explicó, "la creciente adopción de inteligencia artificial ha elevado aún más la importancia del dato y ha incrementado el interés de los atacantes por comprometer las fuentes de información sensibles de las empresas".

Juan José Rey, director de ventas zona centro de Sarenet compartió ese diagnóstico, aunque introdujo un matiz relevante: "Además del peso tradicional del ransomware, en los últimos meses se observa una mayor presencia de campañas de phishing y suplantación de identidad dirigidas a obtener dinero de manera directa. El foco ya no está solo en secuestrar sistemas para reclamar un rescate, sino en inducir

Webinars BYTE TI

Ciberseguridad y protección de datos en la empresa

Adrià Solana, Security & Compliance Specialist de H&K

Enrique Villa, Cybersecurity Sales Head de Var Group

Gustavo Frega, Senior Academic Strategy and Business Partnership Manager de ISACA

Jordi Torruella, director de ciberseguridad de NexTReT

Juan José Rey, director de ventas zona centro de Sarenet

transferencias fraudulentas, acceder a cuentas bancarias o aprovechar cualquier rendija operativa que permita monetizar el ataque de forma más rápida. Esa evolución, más que sustituir al ransomware, lo complementa y obliga a las empresas a protegerse frente a una combinación de amenazas cada vez más dinámica", afirmó.

Por su parte, Gustavo Frega, Senior Academic Strategy and Business Partnership Manager de ISACA, reforzó esa idea con una imagen especialmente gráfica. Y es que, en su opinión, "la ciberdelincuencia ha dejado de ser un fenómeno casi artesanal para convertirse en una actividad automatizada e industrializada. Ya no se trata del atacante solitario, sino de estructuras capaces de operar a escala y de utilizar técnicas de "pesca de arrastre" para lanzar campañas masivas, explotando además el factor humano con ayuda de inteligencia artificial. Este componente de automatización hace que el riesgo sea más transversal, más frecuente y también menos dependiente de que una empresa sea grande o pequeña".

Jordi Torruella, director de ciberseguridad de NexTReT, añadió dos variables decisivas para completar el mapa. Por una parte, subrayó la exposición creciente de las infraestructuras críticas en un contexto geopolítico más tenso, en el que determinados conflictos pueden trasladarse al plano digital. Por otra, recordó que "una debilidad en seguridad no solo abre la puerta a un incidente técnico, sino también a un posible incumplimiento regulatorio, con implicaciones directas en materia de normativa, protección de datos y exigencias sectoriales".

Enrique Villa, Cybersecurity Sales Head de Var Group, por su parte, incorporó un frente que está ganando relevancia como son "los ataques a la cadena de suministro, tanto en entornos de código abierto como en proveedores comerciales. En conjunto, el panel dibujó un escenario donde las amenazas no desaparecen, sino que se acumulan, se combinan y elevan la complejidad de la defensa".

Del perímetro al dato

Uno de los principales consensos del encuentro fue que muchas compañías continúan trabajando con una lógica de protección heredada de una

era anterior, cuando el perímetro corporativo estaba más definido y el grueso de la actividad tecnológica permanecía dentro de la propia organización. Enrique Villa señaló que "ese modelo, apoyado en herramientas como firewalls o EDR, tuvo sentido durante mucho tiempo, pero hoy resulta insuficiente. El dato ya no habita únicamente en la red interna de la empresa: está repartido entre servicios en la nube, dispositivos no corporativos, entornos colaborativos y, cada vez más, interacciones con sistemas de inteligencia artificial generativa. Este cambio obliga, según explicó, a colocar el dato en el centro de la estrategia de seguridad. Ya no basta con blindar el borde de la organización; es necesario saber qué información existe, cómo se clasifica, quién accede a ella, desde dónde y con qué nivel de permiso.

Torruella coincidió en ese punto y remarcó que también el usuario ha dejado de estar vinculado a una ubicación fija: "El teletrabajo, la movilidad y los ecosistemas distribuidos hacen que la seguridad tenga que construirse desde otro enfoque, menos basado en fronteras y más apoyado en identidades, control de acceso y supervisión continua", aseguró.

Sin embargo, la mesa también advirtió de que ese cambio conceptual no está igual de maduro en todas las empresas. Gustavo Frega introdujo una distinción importante

> **Las pymes, no solo concentran buena parte del tejido empresarial, sino que representan la distancia entre necesidad y capacidad**

entre la estrategia teórica y su capacidad real de ejecución. En el caso español, recordó, "el tejido empresarial está compuesto en gran medida por pymes, y eso condiciona cualquier reflexión sobre madurez digital. Una gran organización puede disponer de equipos, presupuesto, asesoramiento especializado y capacidad de absorción tecnológica; una pyme, en cambio, suele operar con menos personal, menos tiempo y menos margen para realizar inversiones sostenidas. Por eso, una estrategia correcta sobre el papel puede fracasar si no se adapta al contexto real de la empresa".

Juan José Rey fue aún más directo al afirmar que, en el terreno de la pequeña y mediana empresa, sigue habiendo muchas carencias. A su juicio, "se ha producido cierta toma de conciencia sobre el fin del perímetro clásico y sobre la necesidad de proteger otros dispositivos, otros accesos y otras formas de trabajo, pero eso no significa que exista una verdadera madurez". Solana reforzó esa idea al describir a muchas pymes como organizaciones que han modernizado parte de su tecnología, aunque sin dar todavía el salto estratégico necesario. Tal y como afirmó "han comprado soluciones, han incorporado algunas capas de protección y han empezado a digitalizar procesos, pero con frecuencia siguen sin asumir que el atacante puede estar ya dentro y que la seguridad exige una visión más continua, más transversal y más cercana a planteamientos como el zero-trust".

La pyme ante el reto

La parte más práctica del debate giró en torno a las pymes, no solo porque concentran buena parte del tejido empresarial, sino porque representan con claridad la distancia entre necesidad y capacidad. Jordi Torruella sostuvo que "estas organizaciones necesitan ayuda de forma urgente para definir prioridades, ordenar inversiones y avanzar con una hoja de ruta realista. En mi experiencia, muchas no cuentan siquiera con unos niveles mínimos de protección, y en algunos casos la brecha entre lo que deberían implementar y lo que realmente pueden asumir es tan grande que cualquier exigencia elevada se percibe casi como inabordable".

Webinars BYTE TI

Ciberseguridad y protección de datos en la empresa

Por su parte, Juan José Rey apuntó que ese acompañamiento es especialmente importante en un mercado saturado de mensajes, fabricantes, siglas y propuestas tecnológicas difíciles de interpretar para una empresa pequeña. "Si incluso los especialistas reconocen la dificultad de seguir el ritmo de innovación del sector, para una pyme resulta todavía más complejo decidir qué necesita, qué puede aplazar y qué impacto tiene cada inversión. Desde esa perspectiva, el papel del proveedor o del partner ya no consiste solo en vender una solución, sino en traducir complejidad, ordenar prioridades y adaptar las decisiones de seguridad al lenguaje del negocio", concluyó.

Adrià Solana insistió en la misma idea desde una perspectiva de transformación. Para él, no se trata únicamente de implantar tecnología, sino de acompañar a la organización y explicarle, con criterios comprensibles, qué consecuencias puede tener no actuar. Esa pedagogía es fundamental porque muchas empresas no alcanzan a visualizar el daño potencial de un incidente, ya sea por pérdida de datos, interrupción operativa, exposición reputacional o incumplimiento normativo. Enrique Villa asumió incluso cierta autocrítica sectorial al señalar que "no siempre se ha sabido traducir de forma convincente el impacto real de la ciberseguridad para este segmento de mercado. En muchos casos,

> **En la práctica, muchas empresas se están topando con una barrera económica y estructural que es difícil de salvar. Incluso con la tecnología adecuada**

todavía no se percibe como una necesidad tan básica como la asesoría legal o la gestión laboral, cuando en realidad afecta directamente a la continuidad del negocio".

Gustavo Frega añadió a este debate un elemento decisivo: la formación. No solo la dirigida a los empleados, que siguen siendo una puerta de entrada habitual para muchas amenazas, sino también la que necesitan quienes gestionan la empresa. "En muchas pymes, –recordó– el responsable del negocio asume múltiples funciones a la vez y no dispone de un marco suficiente para comprender la dimensión del riesgo. Por eso, además de servicios externalizados o consultoría, hace falta una alfabetización mínima que permita entender conceptos básicos, valorar prioridades y asumir que la ciberseguridad no es un asunto aislado del área técnica, sino una cuestión transversal".

Ese enfoque conecta directamente con otro de los grandes temas del encuentro: el control de accesos. Villa alertó de que muchas filtraciones siguen produciéndose por el uso indebido de credenciales, los permisos heredados, las cuentas compartidas o la mala gestión de los accesos de terceros. Aunque existen soluciones maduras para ordenar identidades y privilegios, el panel coincidió en que el problema no es solo tecnológico. También tiene que ver con gobierno, procesos, disciplina organizativa y cultura interna.

Juan José Rey añadió que la desaparición del perímetro obliga además "a gestionar no solo el acceso de los empleados, sino también el de colaboradores y proveedores, un aspecto especialmente delicado en cadenas de suministro cada vez más conectadas."

Torruella cerró esa reflexión recordando que, "en la práctica, muchas empresas se topan con una barrera económica y estructural difícil de salvar. Incluso cuando existe tecnología adecuada, la falta de diseño, de concienciación y de buenas prácticas básicas impide sacar verdadero partido a esas herramientas".

Comparativa

5 plataformas EDR/XDR a examen

Hace ya tiempo que la seguridad tradicional no es suficiente para las empresas que deben afrontar ciberataques cada vez más inteligentes. En este escenario complejo se suma el hecho de que el perímetro clásico ha desaparecido si se tiene en cuenta el teletrabajo, el uso generalizado de las aplicaciones en la nube y el movimiento constante de datos entre dispositivos, redes y entornos híbridos. Por todo ello, la detección y respuesta ante las amenazas es un pilar fundamental de la ciberseguridad moderna.

Aquí es donde emergen las plataformas EDR (Endpoint Detection and Response) y su evolución natural, las de tipo XDR (Extended Detection and Response). Suponen un avance en el modelo de seguridad, ya que se pasa de un enfoque centrado en la prevención basada en firmas a un modelo activo de monitorización continua, análisis de comportamiento y respuesta avanzada.

Según algunos análisis de mercado, el segmento EDR supera los 5.000 millones de dólares y podría triplicar su tamaño en menos de una década, con estimaciones que lo sitúan entre los 18.000 y 22.000 millones

Comparativa

5 plataformas EDR/XDR a examen

de dólares en 2030–2031, lo que implica tasas de crecimiento cercanas al 24%–26% anual. Por su parte, el mercado de XDR presenta una expansión aún más acelerada, con crecimientos que rondan el 35%–38% anual, impulsado por la necesidad de unificar la detección y respuesta en múltiples capas de la infraestructura digital —endpoint, red, nube, identidad y correo electrónico—. También avanzar hacia la consolidación de plataformas integradas frente a soluciones aisladas.

Del antivirus al endpoint inteligente

EDR es una solución que responde ante las amenazas en los dispositivos finales (endpoints) como ordenadores, servidores o equipos móviles y que, a diferencia de los antivirus tradicionales, adopta un enfoque más avanzado. Permite, asimismo, actuar de una forma más rápida ante incidentes, por ejemplo, aislando un dispositivo comprometido o deteniendo un proceso malicioso. En este contexto, el EDR encaja con los principios de Zero Trust, un modelo de seguridad que parte de la idea de no confiar nunca por defecto en ningún usuario, dispositivo o conexión. Aplicado al endpoint, esto supone que cada acción debe ser verificada de continuo, reduciendo la confianza implícita dentro de la red corporativa y reforzando el control sobre cualquier actividad sospechosa.

Hacia un enfoque unificado

Las soluciones XDR representan el siguiente paso en la evolución de la ciberseguridad corporativa, debido a la necesidad de unificar las herramientas de seguridad. Frente a los enfoques que se centran en un único aspecto, como el endpoint, XDR amplía el alcance de la detección y la respuesta para abarcar de forma integrada múltiples capas dentro del entorno digital: endpoints, redes, correo electrónico, identidades y servicios en la nube.

Su principal valor reside, por lo tanto, en la capacidad de correlacionar datos procedentes de diferentes fuentes para construir una visión unificada y contextualizada de la actividad que tiene lugar en la organización empresarial. Gracias a esta integración, XDR identifica patrones de ataque complejos que, analizados de manera aislada, podrían pasar desapercibidos o interpretarse como eventos inconexos.

Comparativa

Cisco XDR

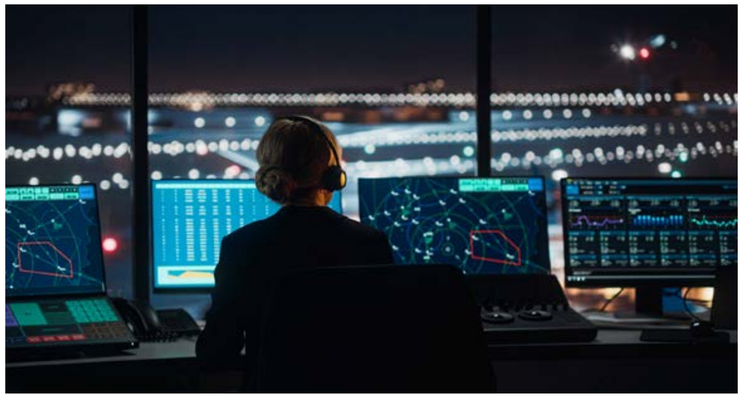
En el actual panorama de las amenazas, la velocidad y la claridad resultan clave. Y es que los equipos de seguridad se enfrentan a un volumen creciente de alertas, herramientas fragmentadas y la presión constante de responder más rápido con menos recursos. Para superar estos retos, Cisco XDR (Extended Detection and Response) se presenta como una plataforma diseñada para unificar, automatizar y elevar la detección y respuesta frente a estas amenazas.

La propuesta de la multinacional norteamericana brinda telemetría de todo el stack de seguridad –endpoint, red, nube, correo electrónico, aplicaciones e identidad– con el propósito de ofrecer una visión unificada y profunda capaz incluso de detectar las amenazas más avanzadas y difíciles de identificar. En este contexto, gracias a la ayuda de la inteligencia artificial y la correlación automática de datos, los equipos pueden llevar a cabo estas tareas: eliminar puntos ciegos y reducir significativamente los falsos positivos; priorizar y acelerar la respuesta ante incidentes críticos; y realizar investigaciones enriquecidas con inteligencia de amenazas y contexto ampliado.

Dispone, a este respecto, de capacidades nativas de detección y respuesta de red, y las organizaciones pueden integrarla no solo con las soluciones de seguridad de Cisco, sino de terceros, lo que pone de manifiesto su naturaleza abierta y flexible. También destaca la presencia de un asistente de IA llamado Cisco AI Assistant que, entre sus funciones,

optimiza las tareas incorporando tecnologías de IA generativa para generar información que sea valiosa y segura. Admite, asimismo, la ejecución automática de varias tareas que antes se realizaban manualmente. Las empresas se van a beneficiar, en otro orden de cosas, de contar con resúmenes de documentación instantáneos y de reducir el tiempo medio de respuesta para la identificación, contención, erradicación y recuperación; todo ello para que tomen las mejores decisiones posibles.

Por otro lado, la integración de Cisco XDR con la solución de ciberseguridad Splunk Enterprise Security potencia estas capacidades, permitiendo que los eventos y alertas fluyan sin interrupciones entre ambas plataformas. Splunk aporta análisis avanzados, búsquedas potentes y retención de datos a largo plazo, mientras Cisco XDR facilita la detección y respuesta en tiempo real. Como SIEM ampliado, añadir que Splunk Enterprise Security combina en una sola herramienta análisis de datos, automatización, inteligencia de amenazas y machine learning.



La solución de Cisco simplifica también las operaciones al unificar la visibilidad y automatizar los flujos de trabajo en el centro de operaciones de seguridad o SOC. Su integración con herramientas clave, incluyendo dispositivos de red y seguridad como la línea de equipos de seguridad y SD-WAN gestionados en la nube Meraki MX, permite a las organizaciones combinar telemetría de red con datos de seguridad para detectar y responder rápidamente a incidentes.

Igualmente, estas pueden utilizar playbooks de orquestación personalizados que automatizan tareas repetitivas, reduciendo la carga manual; contar con un asistente de inteligencia artificial que guía a los analistas con recomendaciones prácticas en tiempo real; y mantener un repositorio de datos accesible que facilita la investigación y el cumplimiento normativo.

Cisco

contacto

www.cisco.com/c/es_es

A consultar

Comparativa

5 plataformas EDR/XDR a examen

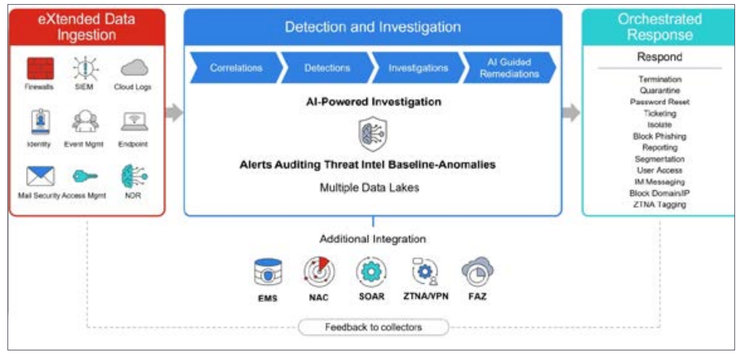
Fortinet FortiXDR

Fortinet ha evolucionado su propuesta de ciberseguridad para el mundo empresarial desde soluciones centradas en el endpoint (EDR) hacia un modelo más amplio y unificado basado en XDR (Extended Detection and Response), integrando así visibilidad, automatización y respuesta coordinada en toda la superficie de ataque; un avance que responde a la creciente sofisticación de las amenazas que ya no se limitan a un único vector, sino que se desplazan lateralmente entre endpoints, red, cloud y aplicaciones.

En este contexto, FortiEDR representa el punto de partida. Se trata de una solución de detección y respuesta en endpoints diseñada para prevenir, detectar y responder a amenazas en tiempo real, incluso aquellas que evaden los antivirus tradicionales. Su enfoque cubre todo el ciclo de vida del ataque —antes, durante y después— mediante capacidades automatizadas que reducen el tiempo de respuesta y optimizan las operaciones de seguridad. Además, FortiEDR se integra de forma nativa con la plataforma Fortinet Security Fabric, lo que permite a las compañías ampliar la visibilidad más allá del endpoint y facilitar la orquestación de respuestas.

Esta integración es la que convierte precisamente a FortiEDR en la base tecnológica sobre la que se construye la evolución hacia XDR. Para ello, Fortinet tiene en su portfolio FortiXDR que amplía las capacidades de EDR hacia una detección y respuesta extendida. En este caso, XDR correlaciona eventos de múltiples dominios —como endpoint, red, cloud y soluciones de terceros— para identificar las amenazas que son complejas de una forma más precisa. Esto explica que la solución de seguridad de la firma estadounidense emplee analítica avanzada e inteligencia artificial para unificar datos de seguridad y automatizar la investigación y remediación de incidentes.

Esta aproximación ayuda, por otra parte, a superar uno de los principales retos de los equipos de seguridad: la falta de visibilidad y la fragmentación de herramientas. Con FortiXDR, las organizaciones pueden consolidar soluciones, reducir la complejidad operativa y mejorar la eficiencia por medio de una plataforma unificada que automatiza la detección, la investigación y la respuesta ante amenazas. La integración entre FortiEDR y FortiXDR dentro de la plataforma Security Fabric proporciona de este modo una cobertura completa del entorno TI, lo que ayuda a detectar ataques que se originan en los endpoints y se propagan lateralmente. Gracias a la correlación de datos y la automatización, es posible contener amenazas de forma rápida, aislar dispositivos comprometidos y aplicar acciones



de remediación sin intervención manual intensiva. Complementando estas capacidades, Fortinet ofrece servicios MDR a través de su equipo de expertos FortiGuard Labs. Este servicio añade una capa operativa gestionada, proporcionando monitorización 24x7, análisis experto de alertas y respuesta proactiva ante incidentes. Los analistas de Fortinet actúan como una extensión del SOC del cliente, realizando hunting de amenazas y proporcionando recomendaciones para mejorar la postura de seguridad.

Todo este enfoque mejora la capacidad de detección frente a amenazas avanzadas, y también optimiza la eficiencia operativa, reduce la complejidad tecnológica y permite a las organizaciones adoptar una estrategia de ciberseguridad más integrada, automatizada y escalable.

Fortinet
www.fortinet.com
900 031 422
A consultar

Comparativa

5 plataformas EDR/XDR a examen

Sophos XDR

Sophos XDR (Extended Detection and Response) es una plataforma abierta, adaptativa y nativa de IA que ofrece herramientas e información sobre amenazas para identificar, investigar y neutralizar ataques avanzados en todo el ecosistema de TI. Proporciona capacidades de detección y respuesta extendida que van más allá del endpoint.

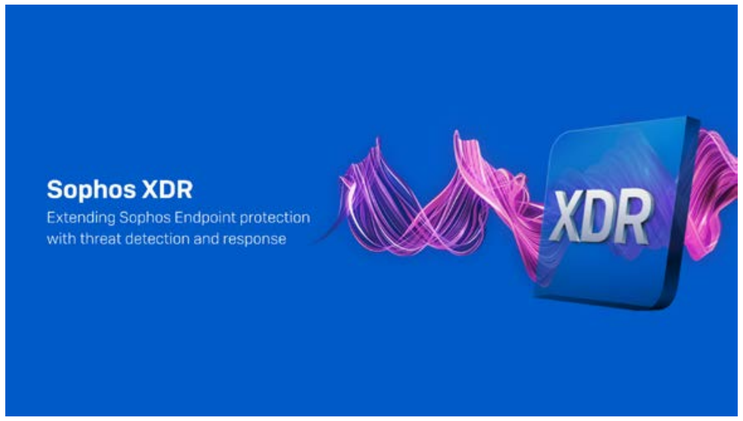
Al poder integrarse de forma nativa con el porfolio de seguridad de Sophos y soluciones de terceros puede brindar una visibilidad unificada a través de los endpoints, los firewalls, las redes, el correo electrónico, identidad, nube y productividad. Además, su arquitectura flexible y escalable ayuda a que los equipos de seguridad aprovechen sus inversiones existentes e incorporen nuevas fuentes de telemetría de forma sencilla.

Sophos XDR combina, a nivel técnico, capacidades preventivas con una detección avanzada de las amenazas, por lo que los trabajadores pueden centrarse en las investigaciones que realmente importan. Apuesta por tres capacidades clave. La primera es la protección para endpoints con inteligencia artificial: hace referencia a sus modelos de Deep Learning que detectan ataques nuevos y conocidos, análisis de comportamientos y funciones anti-ransomware y anti-exploits que detienen las amenazas antes de que escalen.

La segunda capacidad es la visibilidad en toda la superficie de ataque. Las empresas disfrutan de una arquitectura abierta con integraciones preconfiguradas para los dispositivos finales, cortafuegos, email, backup y seguridad en entornos cloud, entre otros. Por su parte, la priorización basada en IA (la tercera) está relacionada con la identificación y el análisis de las amenazas más graves para centrar los esfuerzos de los trabajadores en los incidentes de mayor impacto, reduciendo asimismo el ruido de las alertas irrelevantes.

En esta radiografía de la propuesta de Sophos hay que destacar la presencia de un asistente de inteligencia artificial que acelera las investigaciones y la respuesta a incidentes, facilitando a los analistas actuar con rapidez y precisión frente a amenazas sofisticadas. En este caso, el asistente de IA, diseñado junto a perfiles de primera línea para contextualizar amenazas en tiempo real, ofrece recomendaciones en lenguaje natural y automatiza tareas de operaciones de seguridad mediante instrucciones predefinidas o lenguaje cotidiano.

Las compañías tienen, por otro lado, una



plataforma unificada de detección y respuesta que proporciona una vista única del ecosistema de TI para investigar amenazas a través de múltiples vectores de ataque y responder de forma coordinada, sustituyendo las alertas dispersas por flujos de trabajo de investigación consolidados. También sobresale el análisis avanzado de amenazas que incluye herramientas para analizar comandos sospechosos, identificar entidades afectadas, enriquecer datos con inteligencia de amenazas actualizada y generar informes detallados de forma automática.

Para hacer frente a la gestión de casos y colaboración, los flujos de trabajo robustos facilitan la colaboración entre miembros del equipo, con priorización por IA para centrar los recursos en los incidentes de mayor riesgo.

Sophos
910 621 230
www.sophos.com/es-es
A consultar

Comparativa

5 plataformas EDR/XDR a examen

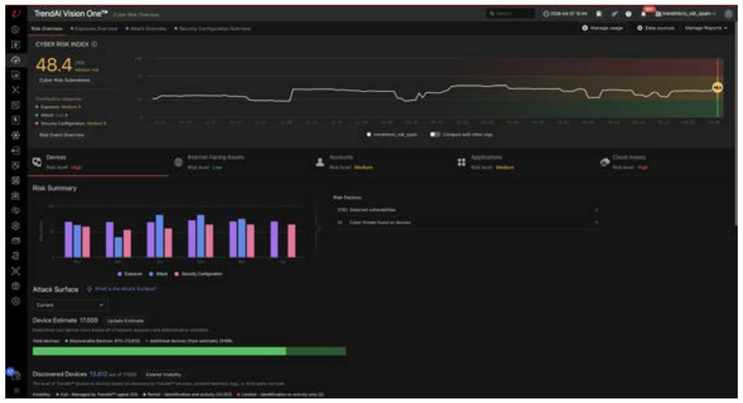
Trend Micro Trend Vision One

Trend Micro, con su nueva estrategia Trend AI, pone de manifiesto la transición de las soluciones EDR tradicionales hacia una plataforma XDR unificada con capacidades avanzadas de gestión del riesgo y protección de entornos de inteligencia artificial. A este respecto, Trend Vision One nació con un enfoque centrado en la protección del endpoint (EDR), pero ha evolucionado hacia un modelo XDR capaz de integrar y correlacionar telemetría de múltiples vectores: endpoint, cloud, red, correo electrónico, identidades, dispositivos móviles e incluso entornos industriales. Así, esta capacidad multivector le permite construir una visión completa de los incidentes, algo fundamental en escenarios donde el origen del ataque no siempre coincide con el punto en el que se detecta.

Mientras, con la correlación de eventos, Trend Vision One ayuda a que se actúe de forma coordinada y se brinde una respuesta unificada: desde aislar un dispositivo o ejecutar scripts remotos, hasta eliminar un correo del buzón, bloquear tráfico o deshabilitar usuarios comprometidos para reducir de manera significativa los tiempos de detección y contención.

Uno de sus pilares clave es la telemetría centralizada y correlacionada en un único data lake. Y es que sobre esta base se construye una capa de inteligencia transversal que se aplica a todos los vectores, mejorando tanto la detección como la respuesta. A esta capacidad XDR se suma la incorporación de funcionalidades avanzadas de gestión del riesgo. No obstante, y más allá de este planteamiento, la plataforma de Trend Micro ayuda a identificar vulnerabilidades, evaluar el nivel de exposición de los activos y priorizar acciones en función del riesgo real para el negocio; un enfoque que introduce un cambio de paradigma donde se pasa de una seguridad reactiva y a actuar tras el incidente a una seguridad proactiva, centrada en anticiparse a los ataques.

En este ámbito, la inteligencia artificial desempeña un papel vital permitiendo detectar posibles rutas de ataque, simulando cómo un atacante podría desplazarse lateralmente dentro de la organización hasta comprometer activos críticos. En la práctica, esto significa priorizar la mitigación de los puntos más vulnerables antes de que sean atacados. Asimismo, incorpora capacidades de cuantificación del riesgo, traduciendo el impacto potencial de amenazas en términos económicos y operativos, así como análisis continuo de cumplimiento normativo. De este modo, la ciberseguridad se alinea directamente con los objetivos estratégicos del negocio.



Otro aspecto relevante es la protección de entornos de IA. Trend Vision One cubre tanto el acceso de los usuarios a herramientas de IA como la propia infraestructura, integrándose con tecnologías de terceros para asegurar microservicios y modelos. Esto incluye la inspección de prompts y respuestas, mitigando riesgos como el envenenamiento de modelos o la generación de contenido malicioso. Además, la plataforma destaca por su flexibilidad de despliegue, soportando entornos cloud, híbridos y on-premise.

Trend Vision One no solo refleja la evolución de EDR a XDR. Anticipa el siguiente paso con una plataforma centrada en la gestión continua del riesgo.

Trend Micro
91 369 70 30
www.trendmicro.com/es_es
A consultar

Comparativa

5 plataformas EDR/XDR a examen

WatchGuard Unified Security Platform

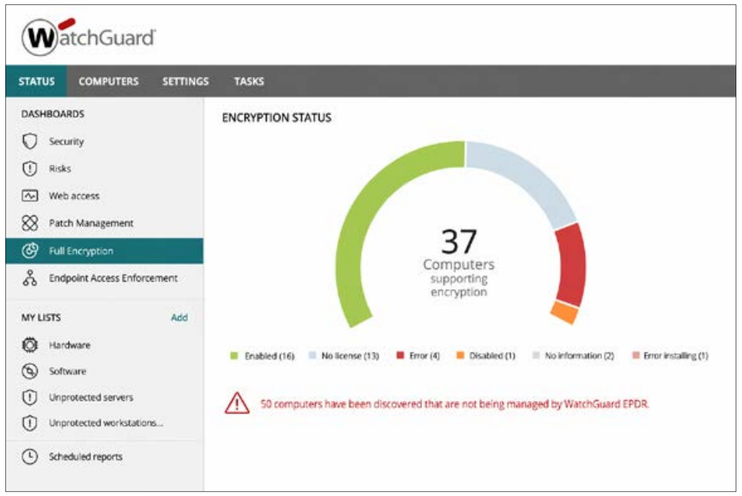
WatchGuard no concibe las soluciones XDR como un producto 'aislado', sino como una capacidad integrada, sin coste adicional, dentro de su WatchGuard Unified Security Platform. Este enfoque se apoya en las tecnologías de endpoint de WatchGuard, que actúan como base de una detección avanzada, mientras la correlación de XDR se realiza en WatchGuard Cloud, a través de ThreatSync, donde se unifican señales procedentes de endpoints, red, identidad y entornos cloud en incidentes accionables.

Esta arquitectura puede ser gestionada directamente por los partners o ampliarse mediante Total MDR u Open MDR, lo que permite disponer de una cobertura XDR 24x7, incluso en entornos multivendor.

Las capacidades de detección y respuesta de endpoint de WatchGuard se basan en el principio de confianza cero (Zero Trust) y están diseñadas para una protección sólida con un volumen de alertas muy reducido. Estas tecnologías escalan en entornos multisede, especialmente aquellos gestionados por proveedores de servicios gestionados (MSP), y aplican controles de denegación por defecto, junto con políticas de ejecución automática.

En la práctica, las aplicaciones que no son de confianza se bloquean por defecto, mientras que las consideradas como confiables se supervisan de manera continua para detectar comportamientos anómalos o señales de vulneración. Gracias a este enfoque, las empresas van más allá de la protección tradicional del puesto de trabajo al incorporar capacidades específicas de contención del movimiento lateral, visibilidad detallada de la actividad del endpoint y una operativa optimizada.

¿Cómo reduce el riesgo la tecnología EDR moderna más allá de la protección básica de los endpoints? La multinacional estadounidense minimiza este riesgo imponiendo un modelo en el que las aplicaciones desconocidas no se permiten por defecto; además, la solución es capaz de detectar comportamientos maliciosos incluso dentro de un software de confianza y de contener el movimiento lateral para evitar la propagación de una amenaza a través de los endpoints y la red. Con esta aproximación, las soluciones EDR de WatchGuard ayudan a detener los ataques antes y limitar su impacto. La contención temprana reduce, por su parte, la exposición y ayuda a mantener un nivel de riesgo más bajo, disminuyendo la necesidad de una



intervención manual continua.

Proporciona, por otro lado, una visibilidad clara de las ejecuciones bloqueadas, las aplicaciones de confianza comprometidas y la progresión de los ataques en los distintos endpoints. Asimismo, las líneas temporales de detección y las vistas del ciclo de vida asisten a los equipos para comprender cómo se detuvieron las amenazas y verificar que la contención fue exitosa. Este nivel de visibilidad resulta útil para tareas de investigación, procesos de cumplimiento, análisis de riesgo y validación posterior a un incidente.

WatchGuard

911 410 918

www.watchguard.com/es

A consultar

Conclusiones

Las cinco soluciones analizadas en esta comparativa permiten elaborar una radiografía completa del estado actual de este mercado. En este contexto, y como se ha comentado anteriormente, la clave ya no reside de manera exclusiva en la prevención, sino en la capacidad de las organizaciones empresariales para detectar, correlacionar y responder de forma ágil, coordinada y eficaz ante incidentes que cada vez son más complejos y sofisticados. Dos de ellas, sin embargo, destacan ligeramente sobre el resto.

Por un lado, Trend Micro avanza hacia un enfoque basado en la gestión continua del riesgo, incorporando capacidades predictivas y protección de entornos de inteligencia artificial. Por otro, está WatchGuard Unified Security Platform que apuesta por una integración nativa del XDR dentro de su plataforma unificada, sin costes adicionales, apoyándose en un modelo Zero Trust o de confianza cero que bloquea por defecto lo desconocido y supervisa continuamente lo confiable.

El resto de fabricantes aportan también un valor diferencial a las empresas interesadas en este tipo de soluciones. Fortinet se distingue por su integración dentro de Security Fabric y su capacidad para automatizar la respuesta en todo el ciclo de vida del ataque. Sophos, mientras tanto, pone el foco en la inteligencia artificial aplicada a la priorización de las amenazas y en una plataforma que es abierta y adaptable. Finalmente, Cisco XDR sobresale por su capacidad para unificar la telemetría de todo el ecosistema de seguridad y potenciarla mediante inteligencia artificial, lo que ayuda a reducir el ruido de las alertas y priorizar incidentes críticos.

Aspectos Destacados

Nombre de la solución	Cisco XDR	Fortinet FortiXDR	Sophos XDR	Trend Micro Trend Vision One	WatchGuard Unified Security Platform
Valoración	★★★★	★★★★	★★★★	★★★★★	★★★★★
Características clave	* Integración con la solución Splunk Enterprise Security. * Emplea playbooks de orquestación personalizados que automatizan tareas repetitivas, reduciendo la carga manual. * Repositorio de datos accesible que facilita la investigación y el cumplimiento normativo. * Asistente de inteligencia artificial que guía e incluye recomendaciones prácticas en tiempo real. * Romper silos entre equipos y tecnologías.	* Aplica inteligencia artificial para unificar datos de seguridad y automatizar la investigación y remediación de incidentes. * Correlaciona eventos de múltiples dominios, incluidas soluciones de terceros. * Integración con FortiEDR. *Servicios MDR (Managed Detection and Response) como complemento. * Empleo de analíticas avanzadas.	* Protección para endpoints con IA. * Priorización basada en IA para la identificación y análisis de las amenazas más graves. * Evaluaciones MITRE ATT&CK. * Gestión de casos y colaboración. * Arquitectura abierta con integraciones preconfiguradas para endpoints, firewalls, redes, correo electrónico, copias de seguridad, identidad, seguridad en la nube y productividad.	* Telemetría centralizada y correlacionada en un único data lake. * Protección de entornos de inteligencia artificial * Capacidades de cuantificación del riesgo. * Despliegue en entornos cloud, híbridos y on-premise. * Prioriza la mitigación de los puntos más vulnerables antes de que sean atacados.	*XDR como capacidad integrada: no es un producto aislado, sino una funcionalidad incluida sin coste adicional dentro de la plataforma. * Visibilidad completa del entorno: integra señales de endpoints, red, identidad y cloud en incidentes accionables. *Modelo Zero Trust (confianza cero). * Puede ser operada por partners o ampliada con servicios como MDR para una cobertura 24/7. *La correlación de datos se realiza en WatchGuard Cloud mediante ThreatSync.

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

Por ALFONSO CASAS

La evolución hacia modelos híbridos, multicloud y soberanos redefine cómo las organizaciones gestionan costes, reducen el lock-in con proveedores y preparan el cloud del futuro

Portada

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

Vivimos tiempos en los que la mayoría de las organizaciones están centradas en implementar la IA en sus procesos de forma segura y fiable a gran escala. Las compañías han dejado de ver la nube como una simple herramienta para reducir costes y han pasado a considerarla como la base primordial para el crecimiento, la competitividad y la adopción de nuevas tecnologías. Este cambio exige integrar las operaciones, la gestión de activos de TI y la gobernanza.

Así lo confirma el decimocuarto informe anual llevado a cabo por la compañía Flexera, titulado "2026 State of the Cloud Report", que revela que el 84% de las organizaciones tienen dificultades para gestionar el gasto en la nube, siendo el principal desafío a la hora de adoptar un entorno cloud. Dado que se espera que el gasto en la nube aumente un 28 % a lo largo de este mismo año, los resultados del informe sugieren que muchas de las organizaciones se están replanteando sus estrategias de gestión.

El informe muestra que el éxito de la nube depende de una supervisión rigurosa, de la medición del valor y de una gobernanza proactiva de la IA. Estas son las capacidades que distinguen a las organizaciones maduras en la nube de aquellas que luchan por controlar los costes, los riesgos y la complejidad.

Factores clave en una estrategia de migración a cloud

La flexibilidad en la gestión cloud empieza mucho antes de migrar. Los expertos de las compañías participantes en el artículo coinciden en afirmar que no se trata de "moverlo todo" a la nube, sino de definir una estrategia alineada con negocio, arquitectura y operación.

Para Isabel Acedo, Head of Cloud Services Presales para Latinoamérica y Sur de Europa en HPE, el punto de partida son los objetivos empresariales: "Una estrategia sólida debe partir siempre de objetivos de negocio concretos y medibles, como ganar agilidad, reforzar la resiliencia o habilitar casos de uso de IA". En esa línea, Alberto Pinedo, National Technology Officer de Microsoft en España, subraya que "no se trata solo de mover cargas de trabajo, sino de decidir qué modernizar, qué transformar y qué mantener".

> **"Los beneficios más claros aparecen cuando la adopción está bien gobernada"**
>
> **PATRICIA PALUD**

Portada

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

Otro aspecto clave gira en torno a analizar cada aplicación y cada dato antes de migrar. Julián Sanz, Especialista Cloud de Arsys Cloud Solutions, recuerda que "la migración no es el final del camino, sino el principio", por lo que debe contemplarse desde el inicio cómo se administrará, securizará y optimizará el entorno cloud. Jaime Balañá, Director Técnico de NetApp para Iberia y LATAM, refuerza esa idea: "La clave no es moverlo todo a la nube, sino decidir qué cargas deben ir, cuándo y con qué modelo operativo".

Los expertos señalan la necesidad de evitar dependencias tecnológicas desde el diseño. Balañá apuesta por arquitecturas híbridas y multicloud para poder mover cargas entre entornos sin rehacer infraestructuras, mientras Matias Sosa, Product Marketing Manager & Cloud Specialist de OVHcloud, destaca la importancia de "la interoperabilidad y la reversibilidad para no quedarnos atrapados por ningún bloqueo técnico ni económico".

La gestión posterior también es decisiva. Según Sanz, una plataforma flexible exige operación continua, optimización y control de costes, mientras Acedo insiste en integrar gobierno, observabilidad y seguridad como base del modelo operativo. Además, cumplimiento normativo y soberanía del dato dejan de verse como limitaciones. Como señala Pinedo,

> **"El enfoque híbrido y multicloud permite ubicar cada carga donde resulta más eficiente técnica y económicamente"**
>
> **JULIÁN SANZ**

abordarlos desde el diseño hace que "la adopción del cloud sea mucho más sólida y sostenible en el tiempo".

Fallos habituales cometidos por las organizaciones

Existe un error bastante común, según apuntan los expertos, y es pensar que migrar a la nube equivale, por sí solo, a modernizarse. Patricia Palud, Cloud Sales Specialist Lead & Business Development de Alhambra IT, advierte que "desplegar más rápido no implica necesariamente que la operación mejore" y que trasladar cargas sin revisar arquitectura o procesos suele derivar en ineficiencias, mayor complejidad y pérdida de control.

Ese enfoque excesivamente técnico, sin una visión estratégica y operativa, aparece como uno de los grandes errores. Balañá,

de NetApp, coincide en señalar que muchas organizaciones abordan la migración "como un proyecto puramente técnico y no como una transformación operativa, financiera y de gobierno del dato", lo que acaba generando problemas de costes, seguridad o recuperación del dato.

Otro error ampliamente compartido es el llamado "lift and shift" acrítico. Davide Altea, Group Chief Private & Public Cloud Officer de ReeVo, alerta de que "trasladar a la nube cargas no optimizadas lleva consigo ineficiencias y costes ocultos". Aitor Jerez, Director Comercial de Sarenet, apunta en la misma dirección al señalar que muchas compañías migran aplicaciones "tal cual están", sin revisar dependencias ni optimizarlas antes.

El riesgo de dependencia excesiva de un único proveedor también aparece como una preocupación transversal. Altea subraya que "subestimar el vendor lock-in y operar sin un plan de salida expone a renegociaciones desfavorables", mientras Matias Sosa, de OVHcloud, alerta de que muchas organizaciones terminan atrapadas por bloqueos tecnológicos o económicos que dificultan evolucionar o controlar costes.

La falsa sensación de que el proveedor resuelve por defecto seguridad, continuidad o backup es otro fallo habitual. Jerez recuerda que "la responsabilidad es compartida" y que descuidar recuperación, protección del dato o gobierno del gasto suele traducirse en sorpresas operativas y financieras. En esa línea, Palud advierte además del riesgo de delegar en el proveedor decisiones estratégicas que deberían seguir bajo el control de la organización.

Más allá de la tecnología, los expertos revelan un problema menos visible: subestimar el factor humano. Altea recuerda que "la tecnología cloud no genera valor sin las competencias adecuadas en los equipos de TI", y Jerez añade que migrar sin preparar a las personas o sin definir cómo se gestionará el entorno en el día a día genera ineficiencias a medio plazo.

Costes ocultos del salto de on-premise a cloud

Los costes ocultos suelen aparecer en cuatro frentes: movimiento de datos, sobredimensionamiento, duplicidad operativa y protección. Como afirma Balañá, "muchas

> **"Una estrategia sólida debe partir siempre de objetivos de negocio concretos y medibles, como ganar agilidad, reforzar la resiliencia o habilitar casos de uso de IA"**
>
> **ISABEL ACEDO**

Portada

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

organizaciones calculan bien el coste de cómputo inicial, pero infravaloran el impacto de la salida de datos, las copias adicionales, los entornos duplicados durante la transición, el almacenamiento premium innecesario, o el coste de mantener herramientas distintas para cada nube".

No obstante, los expertos destacan que el principal problema no es tanto los "costes ocultos", sino costes infraestimados o mal planificados desde el inicio. Una de las advertencias recurrentes es asumir que todo debe migrarse a nube pública. Julián Sanz, Especialista Cloud de Arsys Cloud Solutions, señala que "forzar la migración de determinadas cargas puede generar ineficiencias y sobrecostes evitables", y defiende que el enfoque híbrido y multicloud permite ubicar cada carga donde resulta más eficiente técnica y económicamente.

Y es que el coste cloud va mucho más allá del consumo de infraestructura. Isabel Acedo, de HPE, recuerda que muchas organizaciones infraestiman partidas ligadas a conectividad, flujos de datos, observabilidad, ciberseguridad, respaldo o continuidad de negocio. Como resume, "estos elementos determinan el coste total y, sobre todo, la eficiencia del modelo". Desde su perspectiva, incorporar prácticas FinOps y gobierno desde el diseño es clave para mantener visibilidad y control económico.

Otro foco de sobrecostes señalado es la falta de optimización operativa. Jaime Balañá apunta que muchas desviaciones aparecen por no automatizar o no aplicar políticas de eficiencia en almacenamiento, protección y movilidad del dato. En esa línea, los expertos coinciden en que costes como transferencia de datos, operaciones I/O, gestión 24/7 o sobredimensionamiento suelen aparecer una vez los entornos están en producción, si no se han previsto adecuadamente.

La conclusión compartida es que el riesgo no está en la nube en sí, sino en migrar sin una

> **"El cloud es el gran habilitador de la IA, y soluciones como Copilot permiten automatizar tareas, mejorar la toma de decisiones y liberar tiempo para actividades de mayor valor"**
>
> **ALBERTO PINEDO**

arquitectura adecuada, sin asesoramiento especializado y sin una gestión continua orientada a optimizar. Bien planteado, sostienen, el cloud no solo evita sobrecostes, sino que puede ofrecer un control financiero mucho más preciso que los modelos tradicionales.

Impacto en la productividad de equipos y departamentos

El cloud, cuando se adopta bien, elimina buena parte de las esperas de aprovisionamiento y de la carga operativa manual, y permite que los equipos dediquen más tiempo a innovación, fiabilidad, datos y seguridad. Así opina Isabel Acedo, que destaca que "en HPE lo vemos especialmente cuando las organizaciones habilitan una experiencia de nube consistente en todo su entorno híbrido, con autoservicio, automatización e infraestructura como código, pero también con gobierno, seguridad y observabilidad desde el diseño. En este ámbito, HPE Private Cloud Enterprise aporta una experiencia de nube totalmente gestionada en entorno privado, con acceso de autoservicio, APIs, control por roles e integración con herramientas de automatización e IaC, lo que ayuda a acortar el tiempo de acceso a recursos y a estandarizar la operación".

> **"Cuando el dato se puede mover y gestionar con políticas coherentes entre on-premise y nube, la organización gana flexibilidad"**
>
> **JAIME BALAÑÁ**

Este impacto se amplifica cuando las organizaciones empiezan a incorporar inteligencia artificial. Según destaca Alberto Pinedo, "el cloud es el gran habilitador de la IA, y soluciones como Microsoft Copilot permiten automatizar tareas, mejorar la toma de decisiones y liberar tiempo para actividades de mayor valor. Eso sí, para que la productividad mejore de verdad, es imprescindible acompañar la tecnología con formación y un cambio cultural que ayude a los equipos a adoptar estas nuevas capacidades".

Davide Altea de ReeVo señala: "el impacto en la productividad es real, pero no automático, ya que depende en gran medida de cómo se gestione la transición. A corto plazo es normal una fase de adaptación, con una disminución temporal de la productividad debido al aprendizaje de nuevas herramientas y procesos. Sin embargo, a medio y largo plazo, los beneficios son significativos: los equipos de TI se liberan de tareas de mantenimiento de infraestructura de bajo

Portada

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

valor añadido y pueden centrarse en iniciativas estratégicas. Los departamentos de negocio ganan autonomía en el acceso a recursos y herramientas, reduciendo los tiempos de espera hacia TI.

Soluciones planteadas por las compañías

Frente a los riesgos de dependencia y complejidad, las soluciones que plantean los proveedores convergen en una idea común: más que apostar por herramientas aisladas, se trata de construir modelos híbridos gobernados, con visibilidad unificada y capacidad de operación sobre múltiples entornos. Plantean entornos operativos diseñados para dar a las organizaciones control, resiliencia y libertad de elección a largo plazo.

Isabel Acedo resume este enfoque al señalar que la propuesta pasa por "llevar una experiencia cloud unificada allí donde estén las aplicaciones, los datos y las operaciones, con un enfoque híbrido por diseño". Sobre esa base, HPE combina plataforma, metodología y operación, integrando capacidades de observabilidad, automatización, orquestación y resiliencia para simplificar la gestión de entornos híbridos y multiproveedor.

Esa visión de acompañamiento integral también la comparte Sarenet. Aitor Jerez explica que "el objetivo es que el cliente no tenga que encajar piezas de distintos proveedores, sino que tenga un entorno coherente y gestionado". Su propuesta combina infraestructura cloud, conectividad segura —con redes privadas, VPN o SD-WAN— y herramientas de monitorización para ofrecer no solo capacidad de cómputo, sino un entorno operativo completo.

La soberanía del dato y la seguridad aparecen como otro eje diferenciador. Davide Altea de ReeVo subraya que su modelo responde especialmente a organizaciones que buscan alternativas a los hiperescalares tradicionales: "Nuestro modelo híbrido permite mantener cargas críticas on-premise o en nubes privadas e integrar servicios públicos para las más elásticas". A ello añade un portafolio de ciberseguridad gestionada, bajo la premisa de que "un cloud seguro no es una opción, es un prerrequisito".

> **"Muchas organizaciones terminan atrapadas por bloqueos tecnológicos o económicos que dificultan evolucionar o controlar costes"**
>
> **MATIAS SOSA**

Desde Alhambra IT, Patricia Palud insiste en una visión similar centrada en gobierno unificado. Para la directiva, "no tiene mucho sentido abordar cloud como una suma de herramientas aisladas", sino operar el entorno como un sistema completo, integrando capacidades como CloudOps, FinOps y SecOps con visibilidad continua sobre consumo, rendimiento y riesgo.

Retos de cumplimiento

En relación a aspectos de ciberseguridad y resiliencia, en Europa entran en juego marcos regulatorios cada vez más exigentes: NIS2 refuerza obligaciones de gestión de riesgos y reporting para entidades esenciales importantes y exige transposición nacional, mientras que en sector financiero DORA establece reglas uniformes de resiliencia operacional digital e incorpora un marco de supervisión para terceros TIC críticos, elevando el listón del third-party risk.

Portada

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

> **Nuestro modelo híbrido permite mantener cargas críticas on-premise o en nubes privadas e integrar servicios públicos para las más elásticas"**
>
> **DAVIDE ALTEA**

Según afirma Carolina Mulero, Senior Software Engineering Manager de Wolters Kluwer Tax & Accounting España, "como proveedores de software cloud, nuestras soluciones deben alinearse con todos los marcos normativos como el Reglamento General de Protección de Datos (RGPD), las certificaciones ISO 27001, ISO 22301, el Esquema Nacional de Seguridad (ENS) y el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST), entre otros. Es por ello que debemos mantener un modelo de gobernanza sólido y llevar a cabo constantes auditorías, tanto internamente como con proveedores de servicios en el marco de una estrategia que se apoya en procedimientos y políticas que siguen los más altos estándares de seguridad". Las soluciones de la compañía están muy vinculadas al cambio legislativo en los ámbitos fiscal, contable y laboral. "El entorno cloud nos permite hacer frente al reto de adaptarlas de forma ágil al marco legal vigente, asegurando el cumplimiento de los plazos que marcan las diferentes administraciones", señala Mulero.

Beneficios tangibles

En términos de negocio, un estudio de IDC sobre GreenLake señala para las organizaciones analizadas un ROI del 321% a tres años, un periodo de retorno de 10 meses, un 45% menos de costes operativos a tres años, un 86% menos de tiempo de inactividad no planificado y un 81% más de rapidez en el despliegue de nuevos recursos de cómputo. Más allá de las cifras, el valor más repetido es la capacidad de evolucionar al ritmo que exige el negocio con una experiencia cloud consistente, especialmente en entornos híbridos donde determinadas cargas requieren un equilibrio muy preciso entre rendimiento, control, resiliencia y cumplimiento.

El entorno cloud tiene un gran potencial, pero sus beneficios no son automáticos. Cuando no hay control ni modelo operativo, lo único que suele notarse al principio es la rapidez de despliegue, y eso por sí solo no basta. Así opina Patricia Palud, que señala que "los beneficios más claros aparecen cuando la adopción está bien gobernada. En esos casos, las organizaciones pueden ajustar mejor la capacidad a la demanda, responder con más agilidad a las necesidades del negocio y ganar

Portada

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

flexibilidad para evolucionar sin tantos bloqueos estructurales".

Sobre el terreno, lo tangible aparece cuando se combinan agilidad y control. "Acelerar el time-to-value sin perder gobierno, y convertir capacidad y operaciones en un servicio que escala con la demanda. Eso se traduce en menos sobre aprovisionamiento, menos tiempo dedicado a planificar capacidad y mayor flexibilidad para absorber picos de actividad o poner en marcha nuevas iniciativas con rapidez", puntualiza Isabel Acedo de HPE.

Alberto Pinedo comenta que hablamos ya de plataformas completas que integran datos, IA, seguridad y productividad, a lo que añade que "el cloud dejará de percibirse como infraestructura para convertirse en un componente estructural de la estrategia empresarial, clave para la competitividad, la innovación y la resiliencia a largo plazo".

En la misma línea opina Balañá, señalando que "cuando el dato se puede mover y gestionar con políticas coherentes entre on-premise y nube, la organización gana flexibilidad real para crecer, innovar y reaccionar ante cambios del mercado o regulatorios".

Isabel Acedo afirma que "cuando una organización aborda estrategia, operaciones,

DevOps, seguridad, datos, aplicaciones, innovación y personas como capacidades que maduran en paralelo, la nube deja de ser un destino y se convierte en una forma de operar con disciplina, autoservicio, automatización y responsabilidad compartida, lo que sostiene el cambio del negocio. Y ahí, más allá del producto, la diferencia suele estar en el acompañamiento".

Visión de futuro del cloud

Preguntados sobre la evolución del cloud en los próximos años, existe un consenso generalizado de que los próximos años traerán un cloud más maduro, menos centrado en la migración y mucho más orientado a la gestión inteligente, la soberanía y la libertad de elección. Como resume Patricia Palud, "la conversación ya no girará tanto en torno a quién migra más, sino a quién gestiona mejor".

Existe consenso en que el modelo híbrido y multicloud se consolidará como estándar. Aitor Jerez prevé que "las empresas combinarán cloud pública, privada, edge e incluso on-

Portada

Cómo evitar dependencias y ganar flexibilidad gestionando la nube

premise según el caso", mientras Jaime Balañá apunta a una evolución hacia un "híbrido inteligente", donde el foco estará en decidir dónde tiene más sentido ejecutar cada carga manteniendo una experiencia operativa unificada.

Otra gran tendencia transversal es el papel creciente de la inteligencia artificial en la evolución del cloud. Julián Sanz señala que "la IA ya está redefiniendo la gestión de la nube, desde la optimización automática de costes hasta la detección proactiva de anomalías". En la misma línea, Isabel Acedo anticipa entornos híbridos impulsados por automatización avanzada y AIOps capaces de anticipar incidencias y adaptar la infraestructura de forma dinámica. Para Alberto Pinedo el cloud dejará incluso de percibirse como infraestructura para convertirse en una capa estructural sobre la que desplegar datos, IA, seguridad y productividad.

También emergerá con fuerza la soberanía digital como criterio estratégico. Microsoft, OVHcloud y ReeVo coinciden en que las exigencias regulatorias, junto al contexto geopolítico, acelerarán la demanda de nubes soberanas y proveedores europeos. Por su parte, Davide Altea va un paso más allá al anticipar fenómenos como la cloud repatriation, de manera que muchas empresas llevarán de vuelta cargas de trabajo on-premise o a nubes regionales tras haber experimentado los límites económicos y estratégicos de los hyperscalers globales. En esta línea, la integración entre cloud e IA requerirá de infraestructuras cada vez más cercanas al dato, favoreciendo modelos híbridos y proveedores locales con baja latencia y control total de la cadena.

> **"Como proveedores de software cloud, nuestras soluciones deben alinearse con todos los marcos normativos vigentes"**
>
> **CAROLINA MULERO**

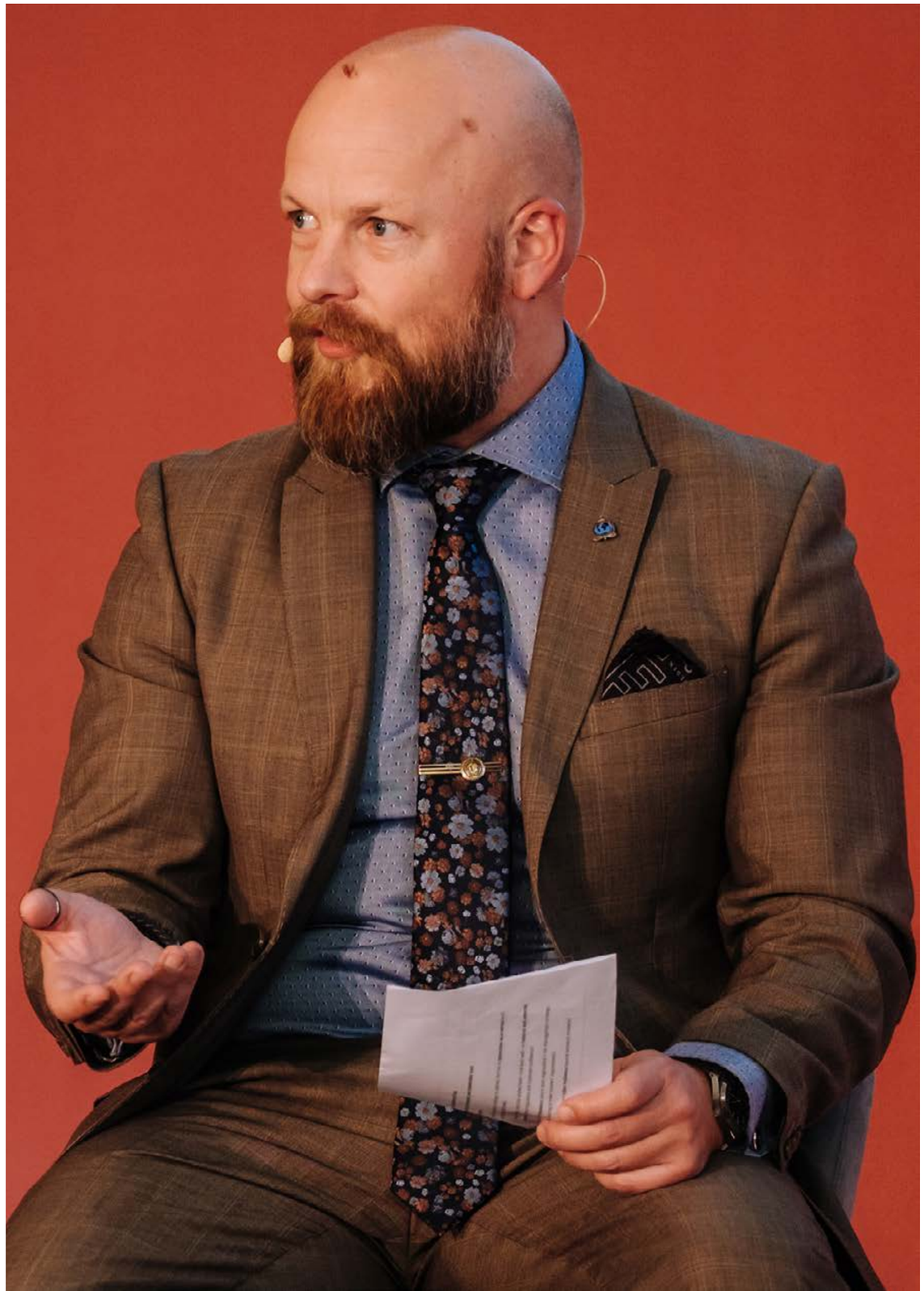
Las organizaciones están comprendiendo que el cloud no es solo una cuestión tecnológica, sino una elección estratégica sobre quién custodia sus activos digitales. En un contexto geopolítico cada vez más inestable, contar con un proveedor europeo de confianza con infraestructuras físicamente ubicadas en el país, interlocutores accesibles y una hoja de ruta transparente, marca diferencias.

Un CIO en 20 líneas

"Más que una disciplina técnica la ciberseguridad actual aúna comportamiento humano, regulación y geopolítica"

Bjørn R. Watne, Global CISO de INTERPOL

MANUEL NAVARRO



Bajo el marco del IT Security Summit de IDC, Byte TI tuvo la oportunidad de entrevistar a Bjørn R. Watne, Global CISO de INTERPOL. Este profesional de la ciberseguridad, que ha pasado por los sectores financieros y de las telecomunicaciones antes de aterrizar en la mayor organización policial internacional del mundo, cuenta cómo esa trayectoria profesional le ha enseñado que el ciberespacio no tiene fronteras ni discrimina sectores, manteniendo retos similares pero con adversarios distintos.

En Interpol, que agrupa a policías de 196 países con más de 140 nacionalidades diferentes, lidera una defensa en profundidad adaptada a la diversidad cultural, priorizando la formación sensible y una misión común como es la de empoderar a las distintas policías del mundo contra los más vulnerables. Watne destaca como prioritarios la lucha contra las

Un CIO en 20 líneas

Bjørn R. Watne, Global CISO de INTERPOL

amenazas de cárteles y terroristas, los fraudes y el ransomware impulsados por IA y aboga por la colaboración público-privada para paliar la escasez de talento en ciberseguridad.

Usted pasó del sector privado a una organización internacional pública. ¿Son muy diferentes los retos en materia de ciberseguridad, o se enfrentan ambos, en gran medida, a los mismos riesgos?
El ciberespacio no tiene fronteras y no discrimina entre industrias o sectores. Lo que hacemos como profesionales de la ciberseguridad y los retos a los que nos enfrentamos son muy similares. La mayor diferencia radica en quiénes son nuestros principales adversarios.

Mi primer puesto como CISO fue en el sector de los servicios financieros. Los actores maliciosos que nos acechaban en aquel momento eran delincuentes oportunistas que buscaban un beneficio económico rápido. Utilizaban en gran medida ataques automatizados y escaneos amplios, y probaban todas las cerraduras y todas las ventanas para ver si podían encontrar una forma de entrar. Si no lo conseguían, pasaban a la siguiente casa de la calle.

Mi segundo puesto como CISO fue en el sector de las telecomunicaciones y las infraestructuras críticas. Al no manejar dinero, no éramos un objetivo tan lucrativo como un banco, por lo que

> **La IA está impulsando un aumento tanto del phishing como del ransomware**

no nos enfrentábamos a los mismos problemas con los mismos actores maliciosos que en el sector de los servicios financieros.

Lo que las empresas de telecomunicaciones tienen, sin embargo, es información sobre dónde se encuentra la gente, con quién habla y de qué habla. Y esta es información que resulta muy interesante para las agencias de inteligencia de diferentes estados. Tanto para descubrir posibles amenazas para su país, como para vigilar a los actores políticos y a la diplomacia internacional. Esto significaba que nuestros adversarios eran en su mayoría aquellos con capacidades muy elevadas: las amenazas avanzadas y persistentes. En lugar de llamar a todas las puertas, seguían a una persona durante meses, tratando de ganarse su confianza y luego se colaban en la organización, donde permanecían en silencio y observaban durante meses, en busca de información importante.

Y ahora, con las fuerzas del orden, el panorama de amenazas cambia una vez más. Nuestros principales adversarios son el crimen organizado, tanto el ciberdelito como los delitos facilitados por la tecnología. Las tácticas, las herramientas y los procedimientos vuelven a ser diferentes, pero la forma en que nos protegemos sigue siendo, en cierta medida, la misma. Con un enfoque holístico, que abarca a las personas, los procesos y la tecnología.

¿Qué significa en la práctica liderar la ciberseguridad en una organización como INTERPOL, que conecta a los organismos encargados de hacer cumplir la ley de 196 países?
La respuesta rápida sería "jornadas de trabajo largas", pero ese es el problema de cualquier CISO, independientemente del sector o la industria. Internet es global y está siempre activo, y esa es la naturaleza de nuestra profesión.

Lo que hace especial trabajar para INTERPOL es la diversidad global dentro de la organización. Más de 140 nacionalidades diferentes trabajan para nosotros, aportando idiomas únicos, formas de trabajar, conocimientos regionales y hábitos culturales. Cuando se habla de temas como la formación y la concienciación en materia de seguridad, esto plantea nuevos retos sobre cómo transmitir el mensaje a todos los niveles y garantizar que se entienda al otro lado. Por otra parte, ofrece una oportunidad increíble para aprender tanto a nivel personal como profesional. Y, a pesar de la diversidad,

Un CIO en 20 líneas

Bjørn R. Watne, Global CISO de INTERPOL

sigue existiendo una misión común que nos une a todos: proteger a los más vulnerables de nuestras sociedades conectando y empoderando a las fuerzas del orden a nivel mundial.

Dada la información sensible que se comparte entre las fuerzas policiales de todo el mundo, ¿cómo garantiza INTERPOL la confidencialidad y la integridad de sus datos?
En este sentido, INTERPOL no es diferente de cualquier otra organización. Hemos implementado una estrategia de defensa en profundidad, siguiendo las mejores prácticas internacionales tanto en términos de tecnología como de gobernanza. Al ser una organización policial, nos centramos en la seguridad desde el principio, pero también dedicamos mucho tiempo a la formación y la sensibilización del personal, así como a mejorar y reforzar nuestra forma de trabajar, promoviendo la visibilidad y la transparencia.

¿Cuáles son actualmente las ciberamenazas más graves a las que se enfrentan los organismos encargados de la aplicación de la ley en todo el mundo?
Me gustaría volver a la primera pregunta sobre nuestros principales retos en materia de ciberseguridad. INTERPOL no tiene adversarios como Estados-nación ni rivales en el sentido militar; nuestro objetivo son las redes delictivas transnacionales y las amenazas. Nos centramos principalmente en los grupos de delincuencia organizada, los terroristas, los cárteles de la droga, los traficantes de personas y similares. Es de estos actores de quienes provienen las mayores amenazas para nuestra organización, ya que nosotros somos una de las mayores amenazas para sus operaciones.

¿Cómo influye la geopolítica en el panorama actual de las amenazas cibernéticas?
Como organización internacional, INTERPOL es totalmente independiente y no se pronuncia sobre cuestiones relacionadas con la política, la religión o la raza. Sin embargo, una observación general y objetiva es que la geopolítica está reconfigurando el panorama de las amenazas cibernéticas al alimentar los ataques patrocinados por Estados, la guerra híbrida y las alianzas de ciberdelincuencia en medio de los conflictos en curso.

¿Cuáles son los tipos de ciberdelitos más comunes denunciados hoy en día por ciudadanos y empresas, y cuáles son los que crecen más rápidamente?
El fraude y el robo dirigidos a particulares son los delitos cibernéticos más denunciados en la actualidad. Están aumentando los intentos de robar información como el phishing o el uso de malware diseñado para la extorsión como el ransomware. Ambas tipologías están dirigidas tanto a ciudadanos como a empresas. Las estafas de inversión y sentimentales, el fraude en las facturas y el robo de identidad también son problemas que se denuncian con frecuencia.

Lamentablemente, la IA también es un acelerador clave en este ámbito, impulsando un aumento tanto del phishing como del ransomware gracias a la automatización y a la IA agéntica.

La escasez de talento en ciberseguridad es un reto global. ¿Cómo pueden las organizaciones abordar esta carencia de manera eficaz?
Es una pregunta muy interesante. A medida que las amenazas se vuelven más complejas, también lo hacen las habilidades que necesitamos para defendernos de ellas. Y la solución no es solo más títulos universitarios, sino un pensamiento más amplio, perfiles diversos y CISOs que puedan formar equipos capaces de aprender más rápido de lo que evolucionan los atacantes.

La ciberseguridad hoy en día es mucho más que una disciplina técnica; se sitúa en la intersección entre el comportamiento humano, la regulación y la geopolítica. La tecnología por sí sola no puede proteger a una organización si los usuarios no están formados para reconocer las amenazas, evitar la manipulación y tomar decisiones digitales informadas.

Un CIO en 20 líneas

Bjørn R. Watne, Global CISO de INTERPOL

Para hacer frente a la escasez de talento, las organizaciones deben ampliar su mentalidad a la hora de contratar. Es muy posible que los próximos equipos de ciberseguridad estén formado por un ingeniero de software, un abogado, un profesor... y un hacker. Con los fundamentos, la motivación y un poco de orientación, serán formidables.

¿Qué importancia tiene la colaboración público-privada para INTERPOL a la hora de combatir la ciberdelincuencia y reforzar la ciberseguridad a nivel mundial?
La colaboración público-privada es muy importante para INTERPOL a la hora de combatir la ciberdelincuencia y reforzar la ciberseguridad a nivel mundial. En lo que respecta a la ciberdelincuencia, la policía no tiene todas las respuestas y gran parte de los conocimientos cibernéticos y tecnológicos se encuentran en el sector privado, el ámbito académico y las organizaciones públicas. Asociarnos con estos actores nos permite aprovechar esos conocimientos para comprender mejor las amenazas, innovar en soluciones y responder con rapidez.

Estas colaboraciones impulsan operaciones que protegen a las comunidades de todo el mundo, desde el intercambio de información sobre amenazas hasta la financiación de proyectos complejos. Sin ellas, nos costaría mucho hacer

> **El desarrollo de las capacidades es esencial. En INTERPOL formamos cada año a miles de agentes**

frente al desafío cibernético sin fronteras de hoy en día, y siempre estamos invitando a más socios a unirse: su apoyo da forma a un futuro digital más seguro.

Dado que tanto los defensores como los atacantes utilizan cada vez más la IA, ¿cómo aprovecha INTERPOL la inteligencia artificial para reforzar sus capacidades de ciberseguridad?
Recientemente hemos desarrollado una plataforma de inteligencia sobre amenazas basada en la IA diseñada para apoyar a los investigadores humanos. Esta plataforma procesa cada día millones de datos procedentes de los países miembros, socios privados y fuentes abiertas para identificar patrones transfronterizos, como nuevas tendencias de fraude o ciberataques coordinados dirigidos a regiones específicas.

También utilizamos la visión artificial para dar prioridad al contenido ilegal y agilizar las investigaciones, lo que ha reducido considerablemente los retrasos en algunas áreas. Otro de nuestros objetivos es detectar el uso indebido de la IA generativa por parte de grupos delictivos mediante métodos de pruebas adversarias.

Como se ha comentado en la pregunta anterior, todo esto se basa en una colaboración segura. Nuestro Centro Global de Ciberfusión (Cyber Fusion Centre) en Singapur sirve como un entorno neutral donde las fuerzas del orden y los aliados de confianza pueden intercambiar indicadores de amenazas de forma segura. Hemos implementado IA federada y análisis que preservan la privacidad para que las organizaciones puedan aportar información sin compartir datos brutos sensibles.

Más allá de la tecnología, el desarrollo de capacidades es fundamental. Cada año, formamos a miles de agentes de las fuerzas del orden y profesionales del sector en análisis forense y ciberdefensa basados en la IA. Y mantenemos un fuerte énfasis en la ética y la transparencia, guiados por el Marco de Gobernanza de la IA de INTERPOL, que promueve un uso responsable y fiable de la IA en la aplicación de la ley.

Legalidad TIC

Wearables y derecho: cuando el cuerpo se convierte en dato

Por CARLOTA PARRA, Senior Associate de ECIJA

La incorporación progresiva de dispositivos wearables, esto es, relojes inteligentes, pulseras de actividad o biosensores, ha transformado la relación entre tecnología y persona hasta un punto inédito, el cuerpo humano ya no solo es sujeto de derechos, sino también fuente constante de datos. Ritmo cardíaco, patrones de sueño, geolocalización o niveles de actividad física alimentan un flujo continuo de información que, en términos jurídicos, se sitúa en el núcleo más sensible de la privacidad.

Desde la perspectiva del Derecho europeo, el fenómeno se inserta claramente en el ámbito del Reglamento General de Protección de Datos (RGPD), que reconoce la protección de datos personales como un derecho fundamental y exige que su tratamiento respete principios como la minimización, la limitación de la finalidad y la seguridad desde el diseño. Sin embargo, los wearables tensionan estos principios, ya que la recogida de datos es masiva, persistente y, en muchos casos, difícilmente comprensible para el usuario medio.

Uno de los principales retos jurídicos radica en la naturaleza de los datos recopilados. Los dispositivos portátiles no solo registran información identificativa, sino también datos biométricos y de salud, considerados categorías especialmente protegidas. Su tratamiento indebido puede traducirse en consecuencias graves, desde escenarios de discriminación en el ámbito laboral o asegurador hasta la construcción de perfiles conductuales altamente intrusivos. A ello se suma su capacidad de inferencia, así combinando datos fisiológicos con datos contextuales (ubicación, rutinas, horarios, patrones de movilidad), puede reconstruirse con notable precisión el estilo de vida de una persona, sus hábitos e incluso, en ciertos supuestos, anticipar comportamientos futuros.

En este contexto, el consentimiento informado, el pilar clásico de la protección de datos, revela

sus límites, ya que los usuarios no comprenden plenamente el alcance del tratamiento ni las posibles reutilizaciones futuras, de modo que el consentimiento tiende a convertirse en una formalidad más que en una garantía efectiva de autodeterminación informativa.

A estos desafíos estructurales se añaden riesgos prácticos que ilustran la dimensión real del problema. Un ejemplo paradigmático lo encontramos en el reciente caso difundido tanto por la prensa nacional e internacional, donde un descuido en el uso de dispositivos durante un entrenamiento militar permitió filtrar la localización exacta del portaaviones francés Charles de Gaulle al haber subido el usuario sus datos a la aplicación deportiva Strava. El episodio muestra cómo la combinación de geolocalización y hábitos registrados por dispositivos personales puede comprometer no solo la privacidad individual, sino también intereses colectivos de primer orden, incluida la seguridad nacional.

Lo anterior no se trata de una anomalía aislada, sino de la manifestación extrema de una lógica inherente a estos sistemas, ya que todo dato capturado es, potencialmente, un dato expuesto, reutilizado o correlacionado con otros para generar conocimiento adicional sobre el individuo.

Desde el punto de vista regulatorio, la Unión Europea ha comenzado a reaccionar ampliando

> **La rapidez de la innovación tecnológica supera con frecuencia la capacidad normativa generando zonas grises**

las obligaciones de seguridad aplicables a los dispositivos conectados, incluidos los wearables, e imponiendo a los fabricantes medidas técnicas orientadas a evitar accesos no autorizados y la manipulación de datos.

No obstante, la rapidez de la innovación tecnológica supera con frecuencia la capacidad normativa, generando zonas grises en las que la responsabilidad jurídica se diluye entre fabricantes, desarrolladores de aplicaciones, proveedores de servicios, plataformas y terceros que acceden a los datos.

En la práctica, la discusión no se agota en la seguridad, sino que obliga a revisar las bases jurídicas del tratamiento y su coherencia con la lógica de estos dispositivos. El RGPD exige delimitar finalidades concretas, pero muchos ecosistemas de wearables combinan funcionalidades de bienestar, personalización, mejora del producto y explotación comercial, lo que incrementa el riesgo de deriva de finalidad y dificulta que el interesado anticipe usos posteriores.

A ello se suma el principio de minimización, donde incluso cuando un dato pueda ser técnicamente capturado, la pregunta jurídica es si resulta necesario para el servicio ofrecido y si existe una alternativa menos invasiva (por ejemplo, procesar localmente en el dispositivo, limitar la granularidad temporal o permitir el uso sin geolocalización).

También adquiere protagonismo la obligación de responsabilidad proactiva. La recogida sistemática y continuada de datos de salud o biométricos, junto con la posibilidad de elaborar perfiles, suele situar estos tratamientos en el perímetro de las evaluaciones de impacto en protección de datos, particularmente cuando concurren gran escala, monitorización y categorías especiales.

Ese enfoque obliga a identificar riesgos específicos (reidentificación, accesos indebidos, inferencias sensibles, uso secundario), a documentar medidas de mitigación y a articular garantías desde el diseño, como el cifrado, la seudonimización y políticas de retención estrictas. En entornos complejos, además, resulta clave clarificar los roles y responsabilidades

Legalidad TIC

Wearables y derecho: cuando el cuerpo se convierte en dato

(responsable, corresponsables, encargados), así como las cadenas de acceso a los datos que pueden incluir apps de terceros, proveedores de analítica o servicios en la nube.

Finalmente, los retos se agravan cuando los datos atraviesan fronteras o se integran en decisiones con efectos relevantes para las personas. La transferencia internacional de información generada por wearables, frecuente en infraestructuras globales, exige encaje con los mecanismos del RGPD y con garantías efectivas, especialmente tratándose de datos sensibles. Y, en escenarios como el empleo, los seguros o la financiación, la tentación de utilizar métricas de actividad, sueño o estrés como indicadores de rendimiento, riesgo o fiabilidad plantea preguntas de proporcionalidad, transparencia y no discriminación, además de límites asociados a la toma de decisiones automatizadas y a la elaboración de perfiles.

En todos estos casos, la promesa de control del usuario solo es real si se traduce en opciones comprensibles y operativas, como por ejemplo, configuraciones por defecto prudentes, paneles de gestión claros, revocación sencilla y acceso efectivo a derechos como la supresión o la portabilidad.

En definitiva, los wearables plantean una cuestión de fondo, ¿puede el Derecho seguir considerando los datos personales como una categoría estática cuando estos se generan de forma continua, automática y profundamente integrada en la vida cotidiana? La respuesta exige repensar no solo los mecanismos de consentimiento, sino también la gobernanza del dato y su ciclo de vida, reforzando la transparencia, la responsabilidad proactiva y, especialmente, el control efectivo del individuo sobre su información.

Porque, en última instancia, el verdadero desafío no es tecnológico, sino jurídico, el garantizar que, en la era de la cuantificación permanente, la persona siga siendo algo más que la suma de sus datos.

> **Los retos se agravan cuando los datos atraviesan fronteras o se integran en decisiones con efectos relevantes para las personas**

Aplicación Práctica

Leroy Merlin e Intelcia redefinen la excelencia en experiencia de cliente

La relación entre Leroy Merlin e Intelcia se ha fortalecido a lo largo de más de siete años de colaboración estratégica, marcados por la confianza, la innovación y un objetivo común: crear entornos donde vivir mejor y ofrecer mejores experiencias al cliente. Desde el inicio de la relación, ambas compañías han trabajado de la mano para construir un modelo de atención al cliente cercano, ágil y alineado con los valores de calidad y sostenibilidad que caracterizan a Leroy Merlin.

Durante estos años, Intelcia ha evolucionado de ser un proveedor operativo a convertirse en un socio estratégico clave en la transformación del modelo de experiencia de cliente. El camino compartido ha estado lleno de hitos que reflejan la madurez de esta alianza: la consolidación de un servicio multicanal orientado al cliente, la incorporación de metodologías ágiles en la gestión operativa, la digitalización de procesos de calidad y la introducción de la analítica avanzada como base de la toma de decisiones. Este proceso de evolución conjunta ha permitido a ambas organizaciones desarrollar una cultura compartida de aprendizaje, innovación y mejora continua.

En este contexto Evoluciona, la unidad de innovación y analítica avanzada del grupo, especializada en inteligencia artificial, automatización y desarrollo de soluciones de valor, ha sido un catalizador fundamental para que Leroy Merlin incorpore nuevas tecnologías en la gestión de su relación con el cliente, impulsando la eficiencia, la personalización y el análisis predictivo. A través de proyectos conjuntos, ambas compañías han demostrado que la innovación aplicada, cuando se combina con el conocimiento del negocio, puede transformar radicalmente la experiencia de cliente.

El reto más reciente surge en torno a uno de los indicadores clave del sector retail: el Net Promoter Score (NPS), un indicador de satisfacción y lealtad del cliente que mide qué probabilidad hay de que una persona recomiende una marca, producto o servicio a otras. Hasta ese momento, el NPS se calculaba de manera tradicional, mediante

encuestas a una parte limitada de los clientes, lo que ofrecía una visión parcial y reactiva de la satisfacción. Leroy Merlin e Intelcia se propusieron ir un paso más allá: predecir el NPS de cada cliente antes de que completara una encuesta, aprovechando la inteligencia artificial y el potencial de las conversaciones reales mantenidas con los clientes.

Así nació el proyecto de NPS Predictivo, un caso pionero que combina tecnología de IA generativa, procesamiento del lenguaje natural y analítica

Aplicación práctica

Leroy Merlin e Intelcia redefinen la excelencia en experiencia de cliente

de voz, y que posiciona a Leroy Merlin como referente en innovación orientada al cliente.

La solución: IA generativa aplicada al NPS

El proyecto consistió en evolucionar el modelo de Speech Analytics ya implantado hacia una solución más avanzada, basada en inteligencia artificial generativa y modelos de lenguaje (LLM). Esta evolución permitió analizar millones de conversaciones con clientes para identificar patrones de satisfacción, predicción de NPS y causas raíz de insatisfacción. La solución integra todas las interacciones del cliente —voz, chat, correo electrónico, formularios y otros canales digitales— en una base de conocimiento unificada. Sobre esta base, los modelos de IA interpretan contenido, contexto y tono emocional, extrayendo insights y predicciones en tiempo real. La herramienta permite no solo anticipar el comportamiento del cliente, sino también generar alertas predictivas para actuar antes de que se produzca una experiencia negativa.

Evoluciona by Intelcia tuvo un papel clave en el diseño de esta arquitectura tecnológica, combinando capacidades de ingeniería de datos, ciencia del lenguaje y experiencia en gestión de cliente. Su equipo desarrolló modelos calibrados con datos reales de encuestas, garantizando una alta precisión en la predicción del NPS.

El resultado fue una herramienta viva, en mejora continua, que transforma la voz del cliente en conocimiento accionable. Tal y como expone Miguel Rivert, Director de Customer Care en Leroy Merlin, "este proyecto nos permite pasar de medir a anticipar la satisfacción. Gracias al NPS Predictivo somos capaces de escuchar la voz del cliente en tiempo real y desarrollar acciones que refuercen la calidad y la personalización de la experiencia en cada punto de contacto".

Implementación y metodología

El despliegue del proyecto se realizó siguiendo una metodología Agile, estructurada en ciclos iterativos que permitieron avanzar con rapidez, incorporar aprendizajes y ajustar las predicciones en función de los resultados reales. El enfoque fue colaborativo desde el inicio: los equipos de Leroy Merlin, Intelcia y Evoluciona trabajaron conjuntamente para asegurar que la tecnología respondiera a necesidades reales del negocio.

La primera fase se centró en el diagnóstico: analizar los procesos existentes, los flujos de atención y los indicadores de satisfacción. A

Aplicación práctica

Leroy Merlin e Intelcia redefinen la excelencia en experiencia de cliente

> **LEROY MERLIN consiguió transformar su modelo de gestión del NPS, pasando de un enfoque reactivo a uno predictivo y proactivo**

partir de ahí, se diseñó un plan de acción que incluía el desarrollo del modelo predictivo, la integración de datos y la validación de resultados. El modelo fue entrenado con datos históricos de NPS y conversaciones de clientes, lo que permitió establecer patrones de correlación entre el lenguaje utilizado y el nivel de satisfacción.

Durante la fase de desarrollo, Evoluciona aplicó técnicas avanzadas de procesamiento del lenguaje natural (PLN) y aprendizaje automático, combinadas con la calibración de prompts específicos para interpretar emociones, temas y causas raíz. El modelo fue sometido a pruebas continuas de precisión, alcanzando una correlación del 85% entre las predicciones de la IA y los resultados de encuestas reales.

A medida que el proyecto fue madurando, se incorporaron múltiples adaptaciones y evoluciones funcionales que fortalecieron su robustez y escalabilidad. Estas evoluciones consolidaron el carácter vivo y adaptable del proyecto, garantizando su alineación con los cambios tecnológicos y operativos del negocio, y reforzando su papel como herramienta estratégica de mejora continua. Según Mario García Lainez, Director de Soluciones IA aplicada de Evoluciona, "Gracias a este enfoque, el proyecto evolucionó de forma orgánica, permitiendo que la innovación tecnológica se integrara de manera natural tanto en la operativa diaria como en la cultura de la organización".

Resultados obtenidos

Los resultados del proyecto fueron inmediatos y medibles, tanto en términos de impacto en la experiencia del cliente como en la eficiencia interna. LEROY MERLIN consiguió transformar su modelo de gestión del NPS, pasando de un enfoque reactivo a uno predictivo y proactivo. Entre los logros más destacados se encuentran:

- Incremento de +1,5 puntos en el NPS de marca, gracias a la detección temprana de posibles detractores.
- Cobertura total (100%) de las interacciones auditadas, frente al 5% habitual en procesos manuales.
- Reducción del tiempo de reacción en un 40%, permitiendo actuar sobre los problemas antes de que impacten en la satisfacción.
- Mejora en los índices de retención y lealtad, al gestionar de manera anticipada las causas de insatisfacción.
- Optimización de la carga operativa y aumento de la productividad, al automatizar tareas de revisión y análisis.

Además de los datos cuantitativos, el proyecto generó aprendizajes de gran valor. El análisis masivo de conversaciones permitió descubrir nuevos factores de satisfacción y áreas de mejora que antes no eran visibles. Por ejemplo, la importancia del tono de atención o la gestión emocional durante las incidencias se identificaron como elementos determinantes en la percepción del cliente.

Durante la migración a Zencare, cuando las encuestas estaban temporalmente inactivas, el modelo predictivo permitió mantener el control de la experiencia del cliente, demostrando su robustez como herramienta de medición continua incluso en contextos de cambio tecnológico.

Tendencias

World: ¿Qué hay detrás de la tecnología para demostrar que eres humano?

El avance de la inteligencia artificial y la proliferación de bots están cambiando la forma en que interactuamos en internet a través de la tecnología. Según datos de la Comisión Nacional de los Mercados y la Competencia (CNMC), más del 35 % de los usuarios de internet en España utiliza de forma habitual herramientas de IA como ChatGPT o chatbots similares.

Pero el cambio va más allá del uso cotidiano. "Los bots ya no son simples cuentas automatizadas que envían spam; hoy pueden generar comentarios complejos, automatizar transacciones o incluso mantener conversaciones que parecen humanas", señala Tiago Sada, Chief Product Officer en Tools for Humanity, compañía colaboradora de World. "Estamos llegando a un punto donde distinguir entre un humano y una máquina en entornos digitales que simulan serlo se ha vuelto cada vez más complicado".

En ese sentido, la tecnología de prueba de humanidad permite demostrar que detrás de una cuenta hay una persona real y única, sin necesidad de revelar información personal. World ID, la principal herramienta de World, garantiza un acceso seguro a espacios y servicios en línea a los que solo deberían acceder humanos (no bots), como servicios financieros, venta de entradas para conciertos, apps de citas y videojuegos.

Tradicionalmente, herramientas como los CAPTCHA o los datos de comportamiento ayudaban a separar humanos de bots. Sin embargo, la IA ha aprendido a superar estos desafíos. Por otro lado, los sistemas de identidad digital como el KYC están diseñados para identificar a una persona: saber su nombre, dirección u otros datos. La tecnología de Prueba de Humanidad propone algo diferente: el objetivo no es saber quién eres, sino poder demostrar que eres humano en entornos digitales.

World, por ejemplo, prioriza la privacidad y seguridad. Combinando imágenes de alta resolución y tecnologías de privacidad avanzadas. Las personas verifican su humanidad mirando a

Tendencias

World: ¿Qué hay detrás de la tecnología para demostrar que eres humano?

una cámara de última generación llamada Orb, que toma imágenes de los ojos y el rostro. Las imágenes se cifran y se envían al dispositivo del usuario y se eliminan inmediatamente de la cámara. La información queda bajo un modelo de custodia personal, lo que significa que permanece en el dispositivo de las personas.

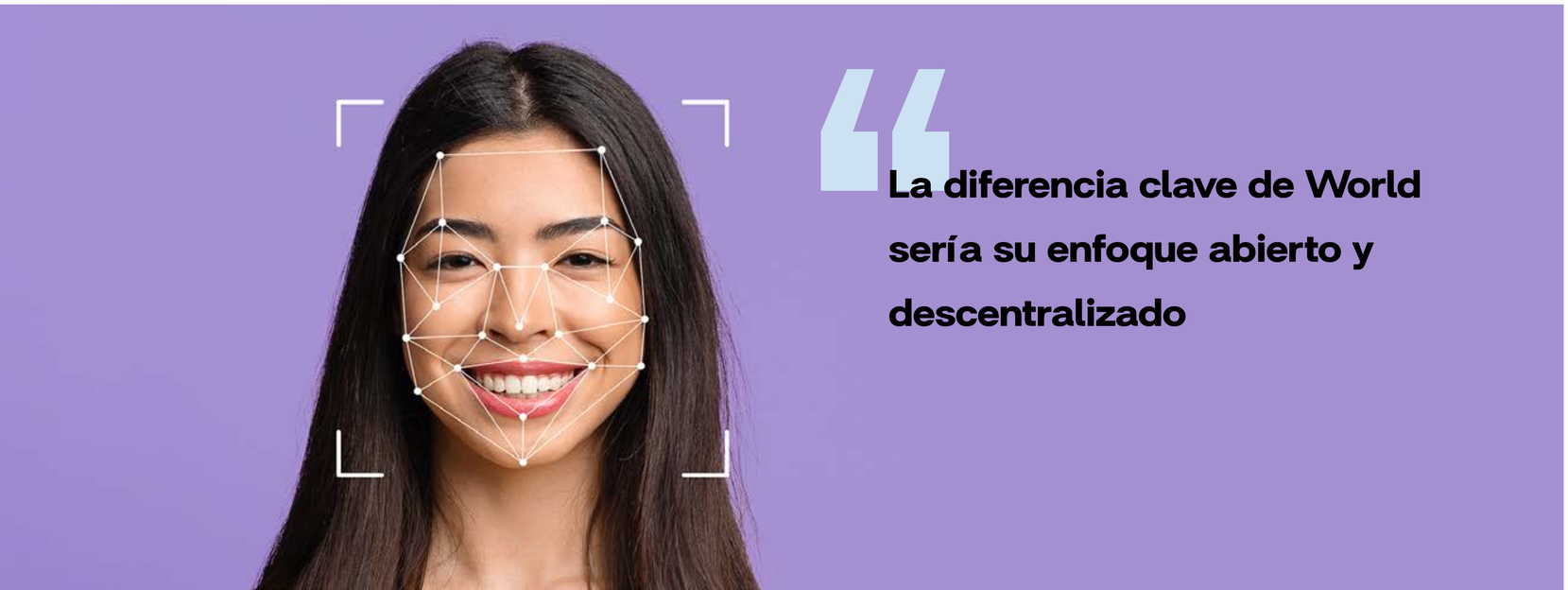
Cuando alguien utiliza esta credencial digital para demostrar ante un servicio que es un humano, por medio de una tecnología criptográfica llamada pruebas de conocimiento cero (ZKP), solo se confirma que la persona tiene un World ID válido, sin revelar ninguna otra información.

"En la práctica, esto significa que podemos proteger la privacidad del usuario mientras mantenemos la confianza en los espacios digitales", apunta Sada. "Esto puede ser relevante en distintos contextos, desde comunidades en línea y plataformas sociales hasta programas de fidelidad, encuestas o acceso a servicios digitales. Ya colaboramos con aliados que comparten esta visión, por ejemplo, ayudando a reducir el fraude, a mejorar la seguridad o a dar prioridad a humanos reales en experiencias digitales, como es el caso de Tinder."

Sobre los planes para integrar World ID con sistemas de identidad nacionales o pasaportes, Sada respondió:"Ya existen pilotos como World ID Credentials que permite a las personas vincular documentos oficiales con chip NFC (Near Field Communication) a su World ID, como es el caso de algunos pasaportes. Esto ya se está probando en algunos países. La información del documento se guarda únicamente en el dispositivo de las personas, y mediante tecnología de ZKP, el sistema solo confirma con un "sí" o "no" ciertos atributos necesarios, por ejemplo, que alguien es mayor de edad o su nacionalidad, sin compartir la identidad o datos completos."

La necesidad de distinguir entre un ser humano y un sistema automatizado tiene implicaciones prácticas en múltiples sectores. Pero no busca reemplazar sistemas de identidad tradicionales, sino ser una capa de seguridad complementaria. El protocolo busca ofrecer una verificación global, interoperable y centrada en la privacidad, donde las personas puedan demostrar que son humanas sin tener que crear cuentas en múltiples plataformas ni compartir datos personales con cada servicio. Su objetivo es convertirse en una capa neutral de verificación humana para internet.

A medida que la inteligencia artificial sigue avanzando y la frontera entre lo humano y lo digital se difumina cada vez más, la pregunta ya no es si este problema existe, sino cómo se resolverá. "Si grandes tecnológicas lanzaran soluciones similares, será una señal de que probar que eres humano en internet se ha vuelto una necesidad real. En ese escenario, la diferencia clave de World sería su enfoque abierto y descentralizado", concluye Sada



"La diferencia clave de World sería su enfoque abierto y descentralizado

Tendencias

La estrategia de los CIOs para convertir el calor desperdiciado en un activo de alto valor

Con la construcción de cada vez más centros de datos en nuestro país, la pregunta se hace inevitable, ¿qué significa esto para el consumo de un bien tan preciado como es el agua en España?

Por ALEXANDRE BENTO,
Infrastructure General Manager en Lenovo Iberia

La realidad es que la reducción del consumo de agua no es solo un reto para los centros de datos, todos los sectores deben evaluar rigurosamente cómo utilizan el agua y, sobre todo, cómo pueden reducir su consumo. Los datacenter se ven frecuentemente implicados en este debate, especialmente en un contexto marcado por la rápida adopción de la inteligencia artificial. Según un estudio, un 93% de los responsables de TI en EMEA plantean incrementar sus inversiones en IA en los próximos 12 meses, por lo que la escala e intensidad de las cargas de trabajo impulsadas por la IA están destinadas a crecer de forma significativa. A medida que las empresas amplían estas cargas de trabajo, se enfrentan a una demanda energética creciente y requisitos de sostenibilidad cada vez más exigentes.

Como decía, las preguntas sobre el consumo de agua son cada vez más frecuentes y urgentes. Existe una solución, y es que con el diseño adecuado, los centros de datos pueden reducir de forma drástica su dependencia del agua y generar valor medioambiental y comunitario... Todo en el mismo proceso. Los CIOs que quieran marcar la diferencia deben centrarse en rediseñar los sistemas en su totalidad, en lugar de focalizarse en minimizar el daño. Esto requiere pasar de hablar de consumo a circularidad, de focalizarse en la presión sobre los recursos a una infraestructura más inteligente, y pasar del calor residual a energía reutilizable.

Circuito cerrado por diseño

En los centros de datos, el uso del agua varía considerablemente en función de la arquitectura de refrigeración. Los sistemas de refrigeración tradicionales normalmente dependen de grandes volúmenes de agua, que se reponen continuamente a medida que ésta se evapora.

Tendencias

La estrategia de los CIOs para convertir el calor desperdiciado en un activo de alto valor

Es aquí donde entran a escena los sistemas sellados de refrigeración líquida.

La refrigeración líquida de circuito cerrado es, exactamente, eso: cerrada. Tras el llenado inicial, la pérdida de agua en condiciones normales de funcionamiento es insignificante. Estos sistemas están diseñados para recircular continuamente la misma agua dentro de un entorno sellado. Es decir, el agua no se evapora ni se descarga de forma rutinaria. Simplemente circula, absorbiendo el calor directamente de los componentes de alto rendimiento y transfiriéndolo eficientemente fuera del sistema.

En un mundo cada vez más preocupado por la escasez de agua, esta distinción es fundamental. Los sistemas de circuito cerrado evitan competir con las comunidades locales, la agricultura o los ecosistemas por los recursos de agua dulce, porque están concebidos como sistemas de recirculación autónomos.

Refrigeración más inteligente

Claro que, luego hay que hacer frente al tema del consumo de agua, algo a lo que también está dando respuesta la tecnología. La refrigeración líquida captura el calor directamente en la fuente, a nivel del procesador, en lugar de intentar enfriar salas enteras de aire caliente. Este enfoque selectivo mejora drásticamente la eficiencia.

Reduce la necesidad de enfriadoras de alto consumo energético y minimiza la dependencia de sistemas de refrigeración evaporativa que consumen agua, lo que puede traducirse en una menor demanda energética y en una menor presión sobre los sistemas hídricos locales.

Las implantaciones en entornos reales ya demuestran las posibilidades de las tecnologías de refrigeración avanzadas. La retransmisión a nivel global de la Fórmula 1 utiliza la tecnología de refrigeración líquida Neptune para dar soporte a cargas de trabajo de computación de alto rendimiento, mejorando al mismo tiempo la eficiencia energética de forma notable. Al capturar el calor directamente en la fuente en lugar de dispersarlo al aire, la refrigeración líquida reduce la demanda de energía de refrigeración a la vez que genera calor a mayor temperatura. Éste es más fácil de reutilizar. En el caso de la F1, este enfoque ha contribuido a impulsar unas operaciones de emisión más sostenibles y escalables, a medida que los volúmenes de datos y los requisitos de rendimiento continúan creciendo.

Es importante resaltar que reducir el consumo de agua no implica sacrificar el rendimiento. De hecho, la refrigeración líquida avanzada puede mejorar el rendimiento al soportar cargas de trabajo de IA y computación de alto rendimiento (HPC) de mayor densidad con mayor eficiencia. Al optimizar la gestión térmica, las empresas pueden incrementar el uso de IA a la vez que reducen la intensidad energética como la hídrica.

Tendencias

La estrategia de los CIOs para convertir el calor desperdiciado en un activo de alto valor

Además, los mismos sistemas de refrigeración líquida que protegen los recursos de agua dulce abren una segunda oportunidad de sostenibilidad: la reutilización del calor.

Del calor residual a la riqueza energética

Una vez que los centros de datos adoptan sistemas de circuito cerrado y refrigeración inteligente, también pueden comenzar a aprovechar los beneficios de reciclar el calor y emplearlo en beneficio de la comunidad local. Prácticamente toda la electricidad consumida por un centro de datos se convierte en último término en calor. Tradicionalmente, ese calor ha sido tratado como un subproducto que había que eliminar y desechar. Sin embargo, en un modelo de energía circular, el calor residual se convierte en un activo: se captura, redirige y reutiliza para satisfacer otras necesidades. En lugar de simplemente enfriarlo y liberarlo a la atmósfera, las compañías pueden transformar ese calor en un recurso aprovechable para redes de calefacción urbana, edificios comerciales y comunidades residenciales, mediante intercambiadores de calor e integración en sistemas de calefacción de distrito.

En toda Europa, proyectos pioneros ya están demostrando que es posible. Iniciativas de calefacción de distrito en Irlanda y Escandinavia han aprovechado el calor residual de los centros de datos para calentar hogares y empresas,

> **A medida que la IA transforma los sectores productivos, la infraestructura digital seguirá expandiéndose**

y grandes proyectos en Suecia tienen como objetivo suministrar calefacción directamente a viviendas residenciales. Para las comunidades, las implicaciones son significativas. El calor reutilizado puede reducir la dependencia de los combustibles fósiles, disminuir los costes energéticos municipales y reforzar la resiliencia energética local. Lo que antes era un residuo se convierte en riqueza.

La regulación eleva el listón

El panorama regulatorio europeo reconoce cada vez más la reutilización del calor residual como un imperativo de sostenibilidad y para los CIOs, el calor residual es una palanca estratégica para el rendimiento ESG, la eficiencia en costes y el valor organizacional más amplio. También puede reducir las emisiones de Alcance 2 y preparar las inversiones en infraestructura para el futuro.

Según un estudio de Lenovo, el 92 % de los responsables de la toma de decisiones en TI prioriza a los socios tecnológicos que reducen el uso de energía y la huella de carbono; sin embargo, solo el 46 % considera que el diseño actual de su centro de datos respalda los objetivos de sostenibilidad. La reutilización del calor ofrece una vía tangible para salvar esa brecha, mejorando los indicadores de rendimiento energético más allá de las métricas tradicionales como la Efectividad del Uso de la Energía (PUE) y contribuyendo directamente a las necesidades de la comunidad.

La integración satisfactoria del calor residual en los sistemas municipales depende de la conversión tecnológica, la planificación colaborativa, el diseño del sistema y la supervisión digital. Cuando estos elementos se alinean, la sostenibilidad teórica se convierte en realidad operativa.

A medida que la IA transforma los sectores productivos, la infraestructura digital seguirá expandiéndose. La pregunta no es si los centros de datos crecerán, sino cómo lo harán. Los CIOs deben tomar nota y poner en marcha los sistemas adecuados para convertir el calor residual en riqueza energética.

Entrevista

Matt Calkins,
CEO de Appian

"No creo que la IA pueda medirse en términos de inteligencia en la misma escala que los seres humanos"

Manuel Navarro

Durante la celebración del Appian World, Byte TI, junto con un reducido grupo de periodistas internacionales, entrevisto a Matt Calkins, CEO de la multinacional. El directivo sostiene que la IA es una tecnología potente pero intrínsecamente probabilística, por lo que exige estructura, fiabilidad y supervisión para ser útil en entornos críticos. Defiende que Appian aporta esa capa de confianza para llevar la IA a procesos estratégicos en empresas reguladas, mientras advierte de los riesgos de alineación y del uso malintencionado de sistemas cada vez más capaces. Estas fueron las principales preguntas que se le hicieron.

Usted considera que la IA es intrínsecamente probabilística. ¿Me puede desarrollar el concepto?
Sí, la IA es intrínsecamente probabilística. Todo lo que dice, absolutamente todo, es una suposición. Si le preguntas: «¿Cuánto es 1 + 1?», hará una suposición. Y si le haces la misma pregunta dos veces seguidas, es muy probable que obtengas respuestas diferentes, sea cual sea la pregunta. Esa es simplemente la

Entrevista

Matt Calkins, CEO de Appian

naturaleza de la tecnología. No es una crítica. Es una tecnología maravillosa, pero tiene ciertas características que debemos tener en cuenta y en torno a las cuales debemos diseñar. Y el núcleo de esas características es su naturaleza probabilística. Alguien me comentaba el otro día que estaba utilizando IA para sumar las celdas de su hoja de cálculo. Una hoja de cálculo. Y pensé: «Bueno, eso simplemente no tiene justificación, porque las fórmulas lo hacen perfectamente, y la IA nunca alcanzará una precisión del 100 % al sumar las celdas de tu hoja de cálculo».

Hoy en día, por supuesto, la gente recurre a la IA para cualquier problema, independientemente de si es adecuado o no. Pero a medida que nos familiarizamos con la tecnología, sus puntos fuertes, sus puntos débiles y sus necesidades, creo que una de las primeras cosas que debemos tener en cuenta es que necesita una estructura. Y que sus resultados no son, ni serán nunca, 100 % fiables.

Acaban de desarrollar una evolución de Composer. ¿Con Composer se producirá una especie de democratización del uso del bytecode dentro de las empresas?
Lo que hace Composer es tomar el concepto de la programación intuitiva y aplicarlo a aplicaciones críticas. La programación intuitiva no era lo suficientemente precisa ni fiable como para escribir aplicaciones exigentes, pero dentro de la estructura

> **Lo que hace Composer es tomar el concepto de la programación intuitiva y aplicarlo a aplicaciones críticas.**

de Composer, ahora sí lo es. Ahora podemos hacer y ya ni siquiera lo llamo «vibe coding» porque quiero establecer un vínculo claro, una división clara entre una actividad muy informal y poco fiable que genera código muy rápidamente —y eso es increíble— y nuestra opción, que consiste en crear aplicaciones excepcionalmente fiables a través de un proceso de desarrollo en lenguaje natural. Así que se trata de tomar lo que es increíble del live coding y añadirle estructura para que sea lo suficientemente fiable como para crear las aplicaciones que son verdaderamente las más valiosas.

Ha intentado diferenciar a Appian, con respecto a la IA, de las propuestas de Silicon Valley frente a la que usted denomina "IA de la Costa Este? ¿Cómo cree que influirá este enfoque en la adopción de la IA por parte de los gobiernos y las entidades financieras?
Creo que es justo lo que necesitan. Creo que es lo que están esperando.

¿Pero saben que eso es lo que necesitan?
Sí, y por eso aún no han utilizado la IA en sus aplicaciones estratégicas porque saben que les falta. Saben que les falta esa IA de la Costa Este. Permíteme citarte algunas estadísticas del artículo de Harvard Business Review, que se centra muy bien en este tema. Dicen que, en este momento, el 44 % de las organizaciones obtienen pocos o ningún beneficio de la IA, aunque todo el mundo está de acuerdo en que es útil y todo el mundo está trabajando en ello. Así que hay un grupo enorme que no está obteniendo nada. Y también han descubierto que las aplicaciones estratégicas casi nunca utilizan la IA en procesos estratégicos, como las orientadas al cliente, a los reguladores, a los socios y a la toma de decisiones. No están utilizando la IA a la hora de tomar decisiones empresariales. Así que la razón por la que la IA no forma parte de esas organizaciones, de esas aplicaciones, es porque aún no ha alcanzado el nivel de fiabilidad necesario. Y la encuesta lo deja claro. El estudio afirma que solo el 18 % de las organizaciones ha integrado la IA en sus procesos, aunque el 71 % de ellas lo está intentando y les está llevando demasiado tiempo.

También indica que el 92% está de acuerdo en que necesitan medidas de seguridad, pero la

Entrevista

Matt Calkins, CEO de Appian

mayoría aún no las tiene. Así que estas grandes organizaciones son conscientes de lo que les falta, saben que lo necesitan, pero simplemente aún no lo han hecho. Quizá porque es demasiado lento, quizá porque simplemente aún no se han puesto a ello. Pero, precisamente por eso, hacen bien en no implementar la IA en aplicaciones estratégicas. Saben lo que falta y saben que es demasiado pronto. Por eso creo que, en realidad, entienden que necesitan este enfoque de la Costa Este.

Necesitan nuestro enfoque de la IA centrado en la fiabilidad, y esa es la pieza que les faltaba y que les permitirá ahora implementar la IA en aplicaciones y operaciones estratégicas.

¿Y cómo evoluciona el papel de Appian a medida que la IA se vuelve cada vez más autónoma dentro de las empresas?
Sí, la IA va a transformar las empresas y sus aplicaciones, pero no puede hacerlo sola. La IA necesitará apoyo para sus carencias, como necesita apoyo en materia de fiabilidad y necesita apoyo para el seguimiento y para ciertos aspectos de potencia, y eso estamos diseñando nuestro producto como el complemento ideal para la IA. Así que cuando escuchamos predicciones sobre lo que la IA puede hacer, cómo va a revolucionar las empresas de todo el mundo, cómo va a realizar la mayor parte del trabajo y constituir la mayor parte de las aplicaciones, matizo esas predicciones y digo que la IA, con su tecnología complementaria necesaria, puede hacer esas cosas. Y nosotros somos esa tecnología complementaria necesaria.

¿Os veis más como un servicio básico para ofrecer servicios basados en IA a gran escala que como una plataforma de desarrollo y análisis?
Sí, es una pregunta interesante. Permíteme empezar diciendo que lo más importante de Appian son las aplicaciones que crea. El potencial que aporta a esas aplicaciones. Por eso vamos a hacer todo lo posible para reducir las barreras de entrada, de modo que la gente pueda crear y utilizar aplicaciones de Appian. En el pasado, hicimos lo que pudimos para facilitar las cosas creando interfaces que permitían arrastrar y soltar los objetos que formarían parte de la aplicación. Eso era lo más sencillo que podíamos hacer. Sí, se podía arrastrar y soltar una herramienta de reglas, se podía arrastrar y soltar una interfaz. Lo hicimos lo más fácil posible. Pero ahora hay una forma aún más fácil. Y eso va a dejar obsoletas algunas de las interfaces que solíamos utilizar. Las interfaces de creación son mucho menos importantes ahora. Pero nunca fueron el corazón del producto. Eran el eran el medio simplificado mediante el cual alguien podía disfrutar del corazón del producto. Así que esto pone el foco de atención justo donde creo que siempre ha estado: en el poder que damos a nuestros usuarios cuando ejecutan una aplicación de Appian.

> **Creo que gran parte del daño que se puede causar con la inteligencia artificial lo van a hacer personas de forma intencionada.**

Entrevista

Matt Calkins, CEO de Appian

Se habla de que el sector del software como servicio está muerto. ¿Como lo ve Matt Calkins?
No creo que seamos una empresa de software como servicio. Es cierto que publiqué un artículo en el Wall Street Journal en el que expresaba que, en mi opinión, los inversores se equivocaban al respecto, pero en lo que se refiere a Appian, nos veo como un vehículo para la IA. Dondequiera que vaya la IA, allí iremos nosotros. Así que todo ese fenómeno del SaaS, no creo que se aplique a nosotros. Del mismo modo que no dirías que se aplica a NVIDIA, que crea un producto que complementa a la IA y es necesario para el éxito de esta. Eso es lo que intentamos hacer nosotros. Tenemos un producto que, en mi opinión, es necesario para el éxito de la IA. Creo que la razón por la que la IA no se está implementando en cuentas estratégicas —en aplicaciones estratégicas— en este momento es porque carece de fiabilidad, y nosotros vamos a proporcionar la fiabilidad que la IA por sí sola no puede ofrecer. Así que nos veo como un componente necesario para el éxito de la IA en entornos estratégicos.

Appian no es un proveedor de SaaS al que la IA pueda sustituir. Al contrario, creo que seremos nosotros quienes hagamos la sustitución. Creo que si la IA sustituye a una aplicación, tendrá que hacerlo con nuestra ayuda. Y que podríamos ser el facilitador para que la IA sustituya a una gran cantidad de aplicaciones.

Tengo la sensación de que la IA será más inteligente que los humanos dentro de quizá un año, dos años, no lo sé. ¿Estás de acuerdo con eso? ¿Qué pasará si los agentes de IA, o la IA en general, no quieren la supervisión humana y actúan por su cuenta?
En primer lugar, no creo que la IA pueda medirse en términos de inteligencia en la misma escala que los seres humanos. Creo que ya es mucho mejor en ciertas cosas, como jugar al ajedrez, y que también es mucho peor en otras, como escribir poesía o dedicarse a la jardinería. Y no es correcto afirmar que, en algún momento, llegará a ser igual a una persona. No creo que llegue a ser nunca igual a una persona. Creo que tendrá ciertas fortalezas superlativas y ciertas debilidades persistentes, y debemos tratarla no como algo comparable, sino como algo fundamentalmente diferente. No estoy de acuerdo con la mentalidad de la IA general (AGI) y la creencia de que, ya sabes, va a ser comparable a las personas. Creo que a medida que lleguemos a comprender mejor la IA, entenderemos que tenemos ventajas duraderas sobre ella.

Tu otro punto era qué pasaría si la IA se resistiera a nuestra capacidad de controlarla. Bien, pues creo que ahora mismo tenemos que ser muy cuidadosos con la alineación, es decir, asegurarnos de que la IA siga las instrucciones y los deseos de las personas. Creo que se trata de un problema más grave de lo que la gente reconoce hoy en día. Y creo que la IA supone una amenaza si no logramos la alineación. Y ya hay un modelo como Mythos, capaz de piratear sistemas, que está alcanzando un nivel de poder que le permitiría controlar a las personas. Por ejemplo, podría transferir dinero. Si pudiera piratear sistemas, podría controlar el dinero, la reputación y la divulgación de información comprometedora. Estamos llegando a un punto en el que la IA es lo suficientemente fuerte como para crear influencia y, por lo tanto, manipular a las personas que supuestamente controlan la IA.

Eso significa que nos encontramos en un punto peligroso y que debemos esforzarnos más en la alineación. Así que eso me preocupa, pero también me preocupa que la IA caiga en manos de gente malintencionada. Creo que gran parte del daño que se puede causar con la inteligencia artificial lo van a hacer personas de forma intencionada. Van a crear nuevas formas de virus u organismos con una mutación proteica diferente o algo así. Por desgracia, el daño que una persona podría causar con una IA potente es enorme. Y creo que ese daño es probable.

Cibercotizante

José Joaquín Flechoso
Presidente de Cibercotizante

España puntera en sostenibilidad de green data centers

Los centros de datos son la columna vertebral de la economía digital, pero también infraestructuras con un consumo energético muy elevado. Por ello, los green data centers integran soluciones que reducen el consumo, optimizan recursos y minimizan emisiones.

Los green data centers integran tecnologías y estrategias diseñadas para minimizar la huella de carbono, optimizar el consumo energético y aprovechar recursos renovables, convirtiéndose en un pilar clave de la descarbonización urbana.

En España, este cambio de modelo está siendo impulsado por un nuevo marco regulatorio que obligará a los operadores a reportar indicadores ambientales, reutilizar calor residual y demostrar eficiencia energética avanzada. El Proyecto de Real Decreto sobre eficiencia y sostenibilidad de los centros de datos, actualmente en tramitación, establece obligaciones como el reporte anual de indicadores ambientales y socioeconómicos, incluyendo consumo energético, origen renovable y uso de agua, la reutilización obligatoria del calor residual cuando sea técnica y económicamente viable y la acreditación de estar entre el 15% de instalaciones más eficientes para centros de más de 100 MW. Estas medidas sitúan a España en la vanguardia regulatoria europea. España destaca por su disponibilidad de energía solar y eólica y esta ventaja competitiva es uno de los motivos por los que nuestro país se ha convertido en un destino prioritario para grandes operadores globales. Más del 70% del tráfico de datos hacia Europa pasa por España, gracias a su conectividad y energía limpia.

En España, se prevén inversiones de hasta 8.000 millones de euros hasta 2026, impulsadas por la digitalización y la demanda de servicios en la nube. Este crecimiento podría generar un impacto superior a 60.000 millones de euros en el PIB, consolidando a nuestro país como un hub digital europeo

España ha pasado de ser un mercado periférico a integrarse en el mapa FLAP+D (Fráncfort, Londres, Ámsterdam, París + Madrid), consolidándose como uno de los hubs más atractivos de Europa. Madrid ya supera los 555 MW de capacidad en construcción y planificación, situándose entre las diez ciudades EMEA con mayor potencia instalada. El crecimiento previsto eleva la demanda un 90% hasta 2028.