



Descarga esta
revista y ábrela
con Adobe
Acrobat Reader
para aprovechar
sus opciones de
interactividad



LA LEY DE IA IMPONE NUEVAS REGLAS DEL JUEGO EN EL MERCADO TI EUROPEO



**EVOLUCIÓN DE
LAS CIBERAMENAZAS
Y CLAVES PARA LA PROTECCIÓN
DE LAS ORGANIZACIONES**



**ENTREVISTA A YITZHAK KESSELMAN,
CORPORATE VICE PRESIDENT,
MICROSOFT FABRIC**



**EL DESAFÍO DE ORQUESTAR LA
CIBERSEGURIDAD CORPORATIVA**



**EL CANAL REDEFINE SU PAPEL EN
LA CONTINUIDAD DEL NEGOCIO**

«

#CONTENIDOS IT

©magnific

LA LEY DE IA IMPONE NUEVAS REGLAS DEL JUEGO EN EL MERCADO TI EUROPEO

DEBATE IT



Evolución de las ciberamenazas y claves para la protección de las organizaciones

ÍNDICE DE ANUNCIANTES

- >> INGRAM MICRO
- >> DMI
- >> IT RESEARCH
- >> ADM CLOUD & SERVICES
- >> SAMSUNG
- >> STORMSHIELD
- >> SECURIZAME
- >> IT WHITEPAPERS

NO SOLO IT

ENTREVISTA



Yitzhak Kesselman, corporate vice president, Microsoft Fabric

ACTUALIDAD

- >> Microsoft activa en FabCon+SQLCon EU 2026 la era de la inteligencia agéntica corporativa
- >> Ingram Micro celebrará el Symposium 2026 para impulsar la innovación y anticipar tendencias
- >> Alta disponibilidad a escala, seguridad, IA y soberanía, protagonistas del QNAP World Tour 2026
- >> Arsys celebra 30 años de evolución en los servicios TI

REPORTAJES



El desafío de orquestar la ciberseguridad corporativa



El canal redefine su papel en la continuidad del negocio

INGRAM MICRO[®]


Fira Barcelona

SIMPOSIUM

Powering the Channel. Conectando hoy el canal del mañana

« **Miércoles | 21-10-26** »

 **Fira Barcelona Gran Vía**

#IngramMicroSimposium





MICROSOFT ACTIVA EN FABCON+SQLCON EU 2026 LA ERA DE LA INTELIGENCIA AGÉNTICA CORPORATIVA

Ante alrededor de 5.000 profesionales reunidos en Barcelona, Microsoft ha puesto el foco en lo que denominan Frontier Transformation: una arquitectura unificada que conecta el contexto único de cada empresa con la IA autónoma a través de Microsoft Fabric, Power BI y la familia Azure SQL.

➤ MIGUEL ÁNGEL GÓMEZ (BARCELONA)

« Barcelona se ha convertido en foco de interés con la celebración de la European Microsoft Fabric + SQL Community Conference (FabCon + SQLCon EU 2026), una cita donde alrededor de 5.000 profesionales del dato, ingenieros y directivos de TI han compartido un programa compuesto por más de 130 sesiones técnicas, decenas de tutoriales y encuentros comunitarios, donde la compañía ha dejado claro su objetivo: transformar la analítica estática en un ecosistema agéntico capaz de tomar decisiones y ejecutar proce-

sos operativos con total gobierno de la información.

El objetivo se sitúa en pasar de los modelos conversacionales básicos a sistemas agénticos capaces de razonar sobre el contexto operativo único de cada organización. Para lograrlo, Microsoft ha articulado su oferta en torno a Microsoft Fabric, una plataforma que ya supera los 40.000 clientes a nivel mundial, y su ecosistema Microsoft SQL, motor que, según las cifras que maneja la compañía, respalda las cargas de trabajo críticas de más del 90% de las empresas de la lista Fortune 500.

CONSTRUYENDO LA CAPA DE INTELIGENCIA CONTEXTUAL CON FABRIC IQ

El desarrollo de software ha experimentado un giro sustancial. La inteligencia artificial ya no se limita a asistir a los programadores en la escritura de código, sino que asume tareas autónomas a lo largo de todo el ciclo de vida de las aplicaciones. Llevar esa misma capacidad al conjunto del negocio requiere ir más allá de los modelos de lenguaje: exige contextualización gobernada, definiciones de negocio compartidas y salvaguardas operativas.

Arun Ulagaratchagan, vicepresidente ejecutivo de Azure Data, explicó en su ponencia que “a medida que la IA se vuelve más capaz, la inteligencia necesita estar fundamentada en cómo ocurre realmente el trabajo: el conocimiento en el que confían las organizaciones y el estado en tiempo real del negocio”.

EUROPEAN MICROSOFT FABRIC + SQL COMMUNITY CONFERENCE

De izquierda a derecha, Arun Ulagaratchagan, vicepresidente ejecutivo de Azure Data; Shireesh Thota, vicepresidente corporativo de Azure Data Database



En este contexto nace Fabric IQ, definido como la capa de inteligencia compartida que conecta los datos empresariales de Microsoft OneLake, las métricas de los modelos semánticos de Power BI y el contexto operacional derivado de ontologías y señales en tiempo real.

Desde la perspectiva de Amir Netz, technical fellow and CTO, Microsoft Fabric, “el contexto es lo más importante; es lo que hace que el agente se comporte, razone y actúe exactamente igual a como esperaríamos que actuásemos nosotros mismos o nuestros colegas. No queremos que los agentes solo observen el negocio y nos den consejos; queremos que participen activamente en las operaciones de la empresa. Y aquí es donde introducimos las ontologías, lo que realmente nos traslada del Business Intelligence a la Inteligencia Operativa”.

Entre los anuncios más destacados se encuentra la integración de Fabric IQ en Microsoft Copilot Chat y Cowork, sin costes adicionales por uso de tokens. Esta novedad permite a las organizaciones formular consultas de negocio en Copilot obteniendo respuestas fundamentadas en los modelos semánticos ya

MICROSOFT APUESTA POR TRANSFORMAR LA ANALÍTICA ESTÁTICA EN UN ECOSISTEMA AGÉNTICO CAPAZ DE TOMAR DECISIONES Y EJECUTAR PROCESOS OPERATIVOS CON TOTAL GOBIERNO DE LA INFORMACIÓN

validados por sus equipos de analítica, garantizando una única fuente de verdad. Asimismo, Microsoft ha confirmado que la integración con la nueva experiencia Code llegará próximamente mediante el programa Frontier, un paso que desde la perspectiva de Microsoft consolida la analítica conversacional gobernada directamente en el flujo diario de trabajo.

LA EVOLUCIÓN DE POWER BI: CREACIÓN DE APLICACIONES AGÉNTICAS SIN CÓDIGO

Uno de los anuncios más llamativos para el área de Business Intelligence ha sido la llegada de la creación de aplicaciones agénticas a Power BI Desktop. Tradicionalmente, la analítica empresarial seguía un flujo estático: los analistas modelaban datos, creaban informes y publicaban cuadros de mando. Con la nueva experiencia agéntica, los usuarios

pueden describir mediante lenguaje natural la herramienta o flujo de trabajo que necesitan. La plataforma genera la aplicación en tiempo real a partir de un modelo semántico de confianza, permitiendo su edición interactiva y su publicación en Microsoft Fabric sin necesidad de partir de una plantilla en blanco.

A diferencia de los informes convencionales, estas Fabric Apps pueden recibir entradas de datos, ejecutar operaciones de escritura, conservar el estado de la aplicación y respaldar procesos operativos. Para sostener este rendimiento, cada aplicación incorpora automáticamente una base de datos SQL en Fabric, gestión de autenticación y seguridad de nivel empresarial mediante la tecnología open source Rayfin.

Microsoft ha confirmado que esta funcionalidad no estará restringida únicamente a los clientes con capa-

cidad contratada de Fabric. En las próximas semanas estará disponible en versión preliminar para los usuarios de Power BI Pro y Power BI Premium Per User, quienes dispondrán sin coste adicional de capacidades de Fabric Apps y bases de datos Fabric de hasta 1 GB por aplicación.

Paralelamente, para los desarrolladores profesionales, las mejoras en Fabric Apps facilitan la transición rápida de prototipos a producción utilizando el SDK y la CLI de Rayfin. Ahora es posible conectar aplicaciones directamente a almacenes de datos, bases de datos SQL, lakehouses y modelos semánticos de Power BI sin duplicar datos, sumando funciones de backend en TypeScript, Secret Store, soporte para PostgreSQL y métricas integradas de rendimiento.

Según Amir Netz, technical fellow and CTO, Microsoft Fabric, “pasamos de una simple instrucción (‘prompt’) a una aplicación completa de extremo a extremo, lista para producción y respaldada por Fabric. Esto ya no es el clásico informe tradicional de Power BI, sino aplicaciones que conectan datos en tiempo real y analítica operacional para interactuar directamente”.

ONELAKE, IQ SHARING Y LA AUTOMATIZACIÓN EN INGENIERÍA DE DATOS

La consolidación de un patrimonio de datos unificado exige eliminar los silos entre plataformas. En Barcelona se ha anunciado la versión preliminar de IQ Sharing, una capacidad integrada en OneLake que permite compartir de forma segura no solo tablas y archivos gobernados, sino también el contexto empresarial: instrucciones para agentes en Markdown y ontologías RDF.

« En palabras Amir Netz, technical fellow and CTO, Microsoft Fabric, “toda la información en OneLake se mantiene en formatos abiertos y mediante API abiertas, por lo que está disponible para cualquiera que adopte estándares abiertos. Si deseas utilizar estos datos que te ayudamos a integrar, de forma totalmente gratuita e incluso con nuestros competidores, es abierto y puedes utilizarlos en cualquier lugar de tu organización o entre diferentes empresas”.

El ecosistema OneLake amplía también su conectividad nativa con la versión previa de la integración bidireccional con Salesforce Data Cloud 360, la disponibilidad general de la réplica de Google BigQuery, y

una integración más profunda con Microsoft Dynamics 365 Business Central y herramientas como Atlan, dbt y ClickHouse.

En el ámbito del procesamiento de datos, la gran novedad es el agente de ingeniería de datos en Microsoft Fabric, también en versión preliminar, construido sobre la tecnología adquirida tras la compra de Osmos. Este agente permite delegar de forma gobernada y autónoma proyectos complejos y de larga duración, tales como migraciones de plataformas, modernización de lakehouses, optimización de rendimiento y canalizaciones ETL complejas. Los ingenieros definen el objetivo y los límites; el agente planifica, ejecuta, valida y refina el trabajo de forma independiente, manteniendo siempre la supervisión humana. Además, estas capacidades se integran en los entornos de desarrollo habituales de las plantillas de TI, incluyendo GitHub Copilot, Visual Studio Code, Codex y Claude Code.

Por su parte, Real-Time Intelligence suma funciones de Copilot para la creación de cuadros de mando en tiempo real mediante lenguaje natural y la gestión administrativa de Eventhouses. Asimismo, Microsoft

ha ratificado su compromiso con el estándar abierto Apache Ossie (en fase de incubación), colaborando con Snowflake y la industria para fijar un estándar neutro en el intercambio de metadatos semánticos.

MODERNIZACIÓN DE BASES DE DATOS

La gestión de las bases de datos operativas sigue siendo un pilar crítico en la arquitectura corporativa. Para responder a este reto, Microsoft ha presentado importantes avances dentro de su cartera de bases de datos como Database Hub en Fabric (versión preliminar), que se presenta como un plano de

control unificado desde el cual los administradores pueden supervisar, gobernar y optimizar bases de datos SQL Server, Azure SQL, PostgreSQL, Azure Cosmos DB y SQL database en Fabric desde un único entorno; y agentes de bases de datos diseñados para SQL y PostgreSQL en Azure que analizan continuamente señales en el Database Hub y VS Code para diagnosticar cuellos de botella y recomendar optimizaciones automáticamente.

En palabras de Shireesh Thota, vicepresidente corporativo de Azure Data Database, “estos agentes van a averiguar qué funciona y aprenderán de los resultados verificados para automati-



zar progresivamente, mientras continúan ofreciendo controles explícitos. No queremos quitarte el control”.

En el caso de Azure SQL Database Hyperscale, se presenta la versión preliminar de la Pausa automática Serverless, que detiene automáticamente el cómputo en períodos de inactividad para reducir costes en entornos de desarrollo y pruebas; la disponibilidad general de instancias de 192 vCores y soporte de hasta 50 bases de datos por grupo elástico (elastic pool); así como Índices vectoriales DiskANN (GA), es decir, la búsqueda vectorial de alto rendimiento integrada directamente en el motor de Azure SQL Database Hyperscale, Azure SQL Managed Instance y SQL database en Fabric, lo que facilita la construcción de arquitecturas RAG (Retrieval-Augmented Generation) sin exportar datos a almacenes vectoriales externos.

Según indicó Shireesh Thota, “SQL Hyperscale desacopla el almacenamiento del cómputo. Al hacer eso, te otorga una ventaja significativa: puedes empezar donde estén las necesidades de tu aplicación hoy, con la certeza de que, a medida que tu aplicación crezca, la base de datos crecerá con ella”.



En materia de soberanía de datos y entornos híbridos, Microsoft pone en el mercado SQL Server en Azure Local, así como de SQL Server en Azure Local Disconnected Operations (ALDO). Esta última opción permite ejecutar cargas de trabajo de misión crítica en ubicaciones donde la conectividad a la nube es inexistente, restringida o deliberadamente desconectada, manteniendo la paridad operativa con la nube de Azure.

Para Shireesh Thota, “consiste en asegurarnos de ofrecer esto sin perder nada de la innovación, la escala y la flexibilidad en la que las empresas confían en la nube. Rompemos esa disyuntiva mediante Azure Local... En lugar de tener que llevar los

datos a la nube, básicamente traemos todas las capacidades de Azure a donde estén tus datos”.

Por último, se ha anunciado la expansión de Fabric al entorno gubernamental de alta seguridad Microsoft 365 GCC High en EE.UU.

OBSERVABILIDAD INTEGRAL Y FACTURACIÓN BAJO DEMANDA PARA ESCALAR LA IA

Para terminar los anuncios, la compañía ha hecho hincapié en la madurez operativa de la plataforma. La nueva observabilidad en Fabric, en versión preliminar, simplifica la supervisión de múltiples espacios de trabajo consolidando la telemetría en un Eventhouse unificado, ofreciendo vistas mejoradas en el Mo-



nitor Hub y alertas automáticas de fallos ejecutadas por Activator.

Por último, el modelo de costes avanza en flexibilidad gracias a la facturación bajo demanda. Ampliando el esquema ya existente en Spark, la plataforma permite pagar estrictamente por el cómputo consumido con escalado automático. Además, la modalidad Fabric zero-provisioned habilita el inicio inmediato en Fabric y OneLake sin necesidad de comprometer capacidad de forma anticipada. ■

MÁS INFO +

» [European Microsoft Fabric + SQL Community Conference](#)

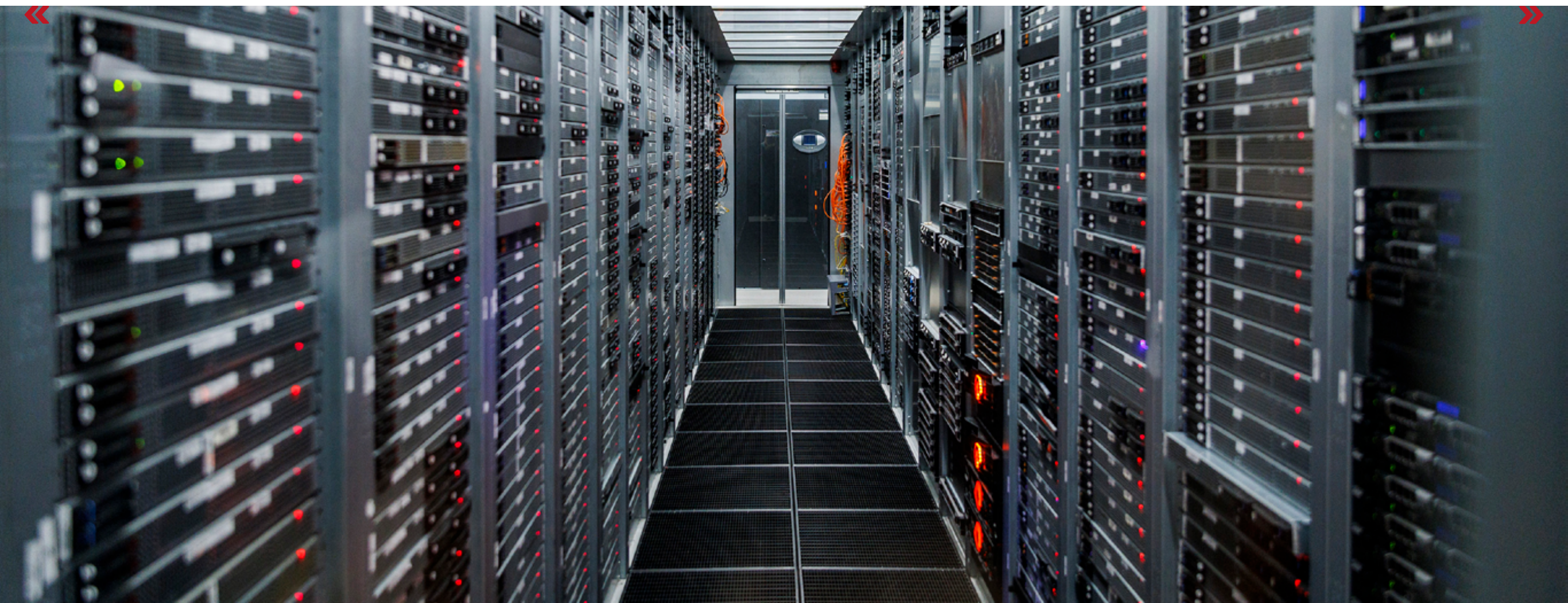


COMPARTIR EN REDES SOCIALES

ARSYS CELEBRA 30 AÑOS DE EVOLUCIÓN EN LOS SERVICIOS TI

En su larga trayectoria Arsys ha pasado de proporcionar los primeros servicios de hosting para las empresas españolas a ofrecer servicios basados en una infraestructura cloud soberana, moderna y cada vez más industrializada. Para conocer mejor cómo ha evolucionado el negocio de la compañía en estas décadas visitamos su centro de datos, ubicado en Logroño, desde el que dan soporte a sus clientes en España.

➤ RICARDO GÓMEZ (LOGROÑO)



« Este año se cumple el 30 aniversario de Arsys, una empresa que comenzó su andadura en 1996, en una década de grandes cambios tecnológicos, con el auge de internet, pero también con problemáticas como la burbuja puntocom. Comenzaron ofreciendo acceso a internet para pymes y en dos años se reorientaron hacia el registro de dominios y el alojamiento web, cambios que fueron acompasándose al avance tecnológico, centrándose cada vez más en los servicios y las soluciones de infraestructura cloud.

En 2013 la compañía se integró dentro del Grupo IONOS, una de las principales firmas europeas del sector, reforzando sus capacidades para seguir operando en el mercado español.

Uno de los principales hitos de la historia de Arsys fue la construcción del centro de datos de Logroño, desde el que lanzaron la primera plataforma comercial de cloud hosting desarrollada en Europa. Las instalaciones disponen de cuatro salas de TI de 300 m² cada una, de las cuales hay tres en funcionamiento, con capacidad para 6 MW de potencia y un PUE

medio anual de 1,25. Actualmente cuenta con alrededor de 20.000 servidores físicos, suministro de energía 100% renovable, climatización basada en aire con chillers y free cooling. Además, cumple con las certificaciones TIER III, ISO 50001, 9001, 14001, 27001, 27018, y además ofrece garantías de cumplimiento con el RGPD y soberanía digital europea.

UN CENTRO DE DATOS ENFOCADO EN EL CLIENTE

En una visita guiada por el centro de datos los responsables de Arsys

explicaban que comenzaron sus operaciones en la primera sala, proporcionando a los clientes la posibilidad de desarrollar proyectos a medida, apoyándose en sus conocimientos y experiencia. En palabras de Guillermo Arbelo, director de Arsys Cloud Solutions, “tratamos de dar acceso al conocimiento que tiene toda la gente

De izquierda a derecha: Miguel Martínez Vélez, Chief Product Officer y miembro del Consejo de Administración de Arsys; Olof Sandstrom, SVP Technical Operations Platforms del Grupo IONOS; y Guillermo Arbelo, director de Arsys Cloud Solutions.



EVOLUCIÓN DE LA INDUSTRIA CLOUD

Aprovechando la visita a sus instalaciones hemos conversado con Guillermo Arbelo, de Arsys, para conocer más en profundidad cómo ha evolucionado el mercado de servicios basados en la nube en los 30 años de historia de la compañía. Puedes leer la entrevista completa en este [enlace](#).

Además, hemos hablado con Olof Sandstrom, del Grupo IONOS, quien nos ha explicado cómo han modernizado la infraestructura de sus centros de datos y el impacto que suponen las regulaciones en materia de eficiencia, sostenibilidad y soberanía digital. Puedes leer la entrevista completa en este [enlace](#).



que trabaja aquí, compartir nuestro expertise, así como hablar tranquilamente de su proyecto y sobre cómo pueden desarrollarlo en nuestras instalaciones”.

Visitando la primera sala, Olof Sandstrom, SPV Technical Operations Platforms del Grupo IONOS, explicó que en este espacio mantienen “los servicios que ya corrían aquí y que no es necesario trasladar” porque son, decía, “sobre todo servicios muy estables, que tienen un crecimiento muy bajo o que no crecen”. Por ello, han mantenido el criterio de densidad de 2009, con racks de 5-10 kW.

HACIA UN DISEÑO MÁS INDUSTRIALIZADO

La segunda sala fría, desplegada en dos fases a partir de 2014, concentra el grueso del negocio de la compañía, enfocado en el mercado masivo y con un diseño más industrializado. En palabras de Olof Sandstrom, “aquí los clientes eligen la infraestructura que quieren en la web, por un precio mensual, de forma sencilla. Arsys busca las máquinas solicitadas, las deja pre-enrackadas, preinstaladas, con la IP preconfigurada, listas para que el cliente

pueda usarlas”, siguiendo un modelo estandarizado a nivel del grupo IONOS”.

Con más equipos de refrigeración, mejor aislamiento, mayor redundancia y una monitorización más granular, este espacio aporta más flexibilidad para redimensionar las capacidades. Esto, además, les han permitido instalar los primeros servidores de tipo “blade”, máquinas hechas a medida que, en palabras de Olof Sandstrom, “permiten incrementar la densidad con diseños propios en los que se comparte la fuente de alimentación, el chasis, el enfriamiento, la conectividad de red... un trabajo de ingeniería que aporta mucha flexibilidad” sin caer en el vendor lock-in de soluciones similares del mercado.

UNA INFRAESTRUCTURA EN CONSTANTE MODERNIZACIÓN

La tercera sala del centro de datos, puesta en marcha en 2019, es una evolución del concepto anterior y, en ella, señalaba Olof Sandstrom, “los cierres y sistemas de clima son más profesionales y la distribución de agua está más optimizada”. Las condiciones de enfriamiento y aisla-

miento mejoradas permiten albergar grandes bloques de servidores tipo blade de alta densidad, así como seguir avanzando en el modelo de centro de datos industrializado.

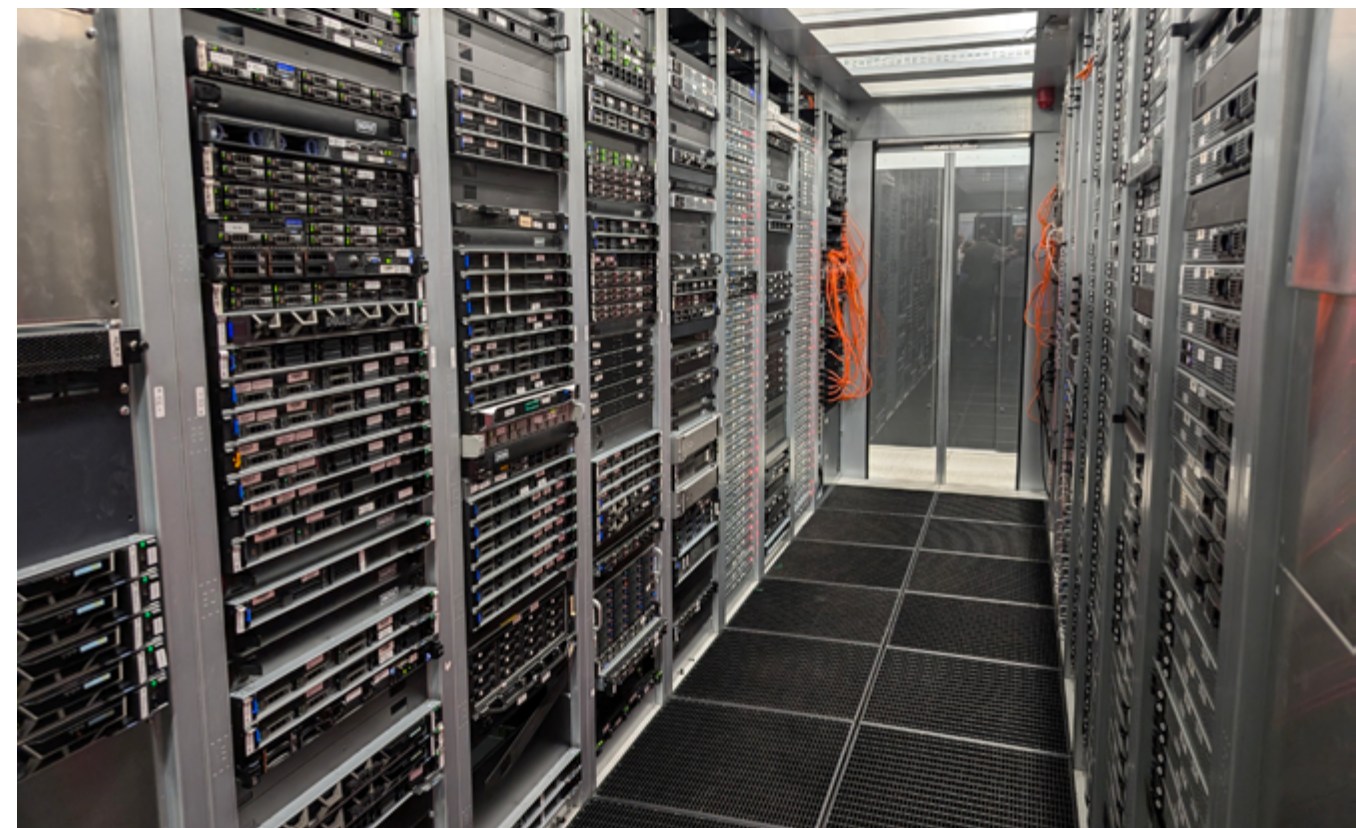
El responsable explicaba que aquí han introducido el concepto de distribución eléctrica por fases para incrementar la redundancia eléctrica y construir unas instalaciones más profesionales, que actualmente alcanzan el 75% de utilización. Añadió que, una vez superen el 80%, comenzarán a planificar la cuarta sala, en la que, decía, “continuaremos evolucionarlo hacia las nuevas necesidades y tecnologías que demande el mercado”. ■

MÁS INFO +

[Visita al Datacenter de Arsys en Logroño](#)

[Entrevista Guillermo Arbelo, Arsys Cloud Solutions](#)

[Entrevista Olof Sandstrom, Grupo IONOS](#)

**COMPARTIR EN REDES SOCIALES**



ALTA DISPONIBILIDAD A ESCALA, SEGURIDAD, IA Y SOBERANÍA, PROTAGONISTAS DEL QNAP WORLD TOUR 2026

El fabricante QNAP ha reunido en Madrid a partners y clientes para celebrar el QNAP World Tour, la cita anual en la que ha expuesto sus últimas tecnologías de almacenamiento y networking, poniendo énfasis en el almacenamiento empresarial de alta densidad y disponibilidad, y en temas candentes como la ciberseguridad, la resiliencia, la inteligencia artificial o la soberanía del dato. En esta edición, además, ha contado con la colaboración de sus partners Kingston Technology, Riello UPS y Seagate Technology, que han aportado su visión sobre el mercado y han mostrado sus principales propuestas para el sector.

➤ RICARDO GÓMEZ

« La última edición del QNAP World Tour se ha centrado en la gran evolución que ha llevado a cabo la compañía para abordar el mercado de centros de datos y grandes infraestructuras, haciendo hincapié en sus últimas novedades, que aportan soluciones completas para el almacenamiento, la conectividad y la protección del dato. Este año el evento ha contado con la colaboración de tres de sus principales partners. Tras la presentación del evento, Pedro González, BDM de Kingston Technology, habló sobre la complicada situación que vive el mercado y destacó algunos de sus últimos dispositivos SSD de alto rendimiento. A continuación, Jordi Riu, sales manager Canal IT de Riello UPS, destacó las características de su gama más profesional de SAI, sus Sistemas de Almacenamiento de energía (EES), Power Switches y Sistemas de Suministro Central (CSS).

ESTRATEGIAS FRENTE A UN MERCADO EN CRISIS

La tercera presentación del QNAP World Tour, titulada “La nueva realidad del dato” corrió a cargo de Daniel Oromí, country sales manager de Seagate Technology, que puso sobre la mesa

la actual escasez de componentes de almacenamiento y el impacto que ya está teniendo la inteligencia artificial en la industria. Frente a estos desafíos, Seagate articula su propuesta en torno a la plataforma Mozaic y los HDD con tecnología de Grabación Magnética Asistida por Calor (HAMR) y un nuevo láser en el cabezal que les permitirá lanzar unidades con 44 Tb de capacidad el próximo año, pudiendo llegar a 100 Tb para 2029-2030.

ALMACENAMIENTO DISTRIBUIDO DE ALTA DENSIDAD

En su presentación Adrián Groba, country manager de QNAP, detalló la estrategia de la compañía para el mercado corporativo, centrada en aportar resiliencia de datos, alta disponibilidad e inteligencia artificial on-premise a través de un ecosistema completo de almacenamiento y networking propio. Como gran novedad, ha anunciado el lanzamiento a comienzos del próximo año de la arquitectura Scale-Out QuTS Mega, una plataforma que permite crear un clúster de almacenamiento distribuido de alta densidad con capacidades que pueden superar los 180 Tb brutos, agrupando entre 3 y 96 nodos de almacenamiento.

DESAFÍOS Y OPORTUNIDADES EN EL MERCADO DE ALMACENAMIENTO EMPRESARIAL

IT Digital Media Group ha participado un año más en el QNAP World Tour de la mano de Pablo García Reales, director ejecutivo del grupo, quien ha moderado un coloquio titulado ‘Desafíos y oportunidades sobre las últimas tecnologías en almacenamiento empresarial de los datos’, un

panel en el que han participado Adrián Groba, country manager de QNAP; Pedro González, BDM de Kingston Technology; Jordi Riu, sales manager Canal IT de Riello UPS; Daniel Oromí, country manager Iberia de Seagate Technology; y David Guerra, sales director de SATEC.



Tras la presentación de Adrián Groba, Pedro Barranquero, Technical BDM de QNAP España, mostró de forma práctica cómo se configura un clúster con QuTS Mega Scale-Out, destacando algunas de las capacidades más destacadas de esta solución, incluyendo servicios de objetos y snapshots en clúster primario y secundario, con inmutabilidad, entre otras.

TECNOLOGÍA E INNOVACIÓN EN ALMACENAMIENTO, RED Y SEGURIDAD

Adrián Groba continuó su presentación mostrando la propuesta de QNAP para garantizar la continuidad de negocio mediante tecnologías de alta disponibilidad, sistemas de controladora dual, con la capacidad de montar un clúster dual de alta disponibilidad con HA Manager o la redundancia de red con la tecnología MC-LAG integrada en sus switches gestionados, entre otras innovaciones.

Otro de los temas clave para QNAP es la protección del dato, que aborda a través del sistema operativo QTS Hero 6.0, basado en ZFS, que ofrece compresión, deduplicación, hasta 65.000 snapshots, carpetas inmutables WORM y compatibilidad directa con entornos como Veeam. Y también con

Hybrid Data Protector for Business, que aporta protección multiplataforma con backup centralizado de equipos físicos, bases de datos en caliente y máquinas virtuales.

INTELIGENCIA ARTIFICIAL ON-PREMISE

Entre las innovaciones recientes de QNAP también está la infraestructura para IA on-premise, que lanzó a través de sus dispositivos de la serie TS-AI / QI, que funcionan como servidores de inteligencia artificial compatibles con tarjetas profesionales de Nvidia. En este campo, también ofrece la gestión del almacenamiento a través de lenguaje natural, mediante el asistente virtual Ana, que permite a los administradores, entre otras cosas, solicitar



configuraciones de volumen, auditorías de seguridad y limpieza automatizada de archivos obsoletos.

GARANTÍA DE DISCOS, SOPORTE POSTVENTA 24/7 Y LA PROPUESTA MYQNAPCLOUD

En relación con la gestión del hardware y la disponibilidad de componentes, QNAP mantiene una política abierta que permite al partner adquirir discos directamente de la lista de compatibilidad certificada o

recorrer a los códigos de disco oficiales de QNAP. En este último caso, incluye servicios como opciones de soporte logístico y cobertura 24/7 con un tiempo de respuesta de 4 horas y sustitución de piezas de 6 a 8 horas máximo, servicio que se extenderá a toda la Península Ibérica a finales de año.

Finalmente, su estrategia de nube híbrida centra en la familia de servicios myQNAPcloud, que engloba soluciones de almacenamiento de ficheros, objetos (S3), trabajo colaborativo empresarial (myQNAPcloud Storage Business) y videograbación en la nube (myQNAPcloud Surveillance), todo ello basado en una infraestructura alojada en Europa que garantiza la soberanía por un precio competitivo. ■

MÁS INFO +

» [Alta disponibilidad a escala, seguridad, IA y soberanía, protagonistas del QNAP World Tour 2026](#)



COMPARTIR EN REDES SOCIALES

INGRAM MICRO CELEBRARÁ EL SIMPOSIUM 2026 PARA IMPULSAR LA INNOVACIÓN Y ANTICIPAR TENDENCIAS

Bajo el lema “Powering the Channel. Conectando hoy el Canal del mañana”, el Symposium 2026 de Ingram Micro, que se celebrará en Barcelona el próximo día 21, volverá a reunir a fabricantes líderes, partners y expertos del sector tecnológico en una jornada diseñada para “impulsar la innovación, generar nuevas oportunidades de negocio y anticipar las tendencias que marcarán la evolución del canal en los próximos años”.



REDACCIÓN ITDM GROUP

Como en ediciones anteriores, [el próximo día 21 de octubre](#) los asistentes tendrán acceso a un completo programa de conferencias, demostraciones y sesiones especializadas de la mano de algunas de las compañías más relevantes del mercado, entre ellas Microsoft, Intel, AMD, AWS, Cisco y HPE, junto a otros fabricantes de referencia para, tal y como explican desde el mayorista, “conocer de primera mano las últimas tecnologías, descubrir

nuevas oportunidades de negocio y compartir experiencias con algunos de los principales actores del ecosistema tecnológico”.

Además de las sesiones de contenido, la zona de exposición permitirá a los asistentes descubrir las últimas innovaciones de algunos de los fabricantes más destacados del sector, ofreciendo un espacio para conocer de cerca las soluciones que están impulsando la transformación digital de empresas y organizaciones. Uno de los espacios protagonistas volverá a ser Xvantage, la plataforma digital de Ingram Micro orientada a transformar la forma en



que los partners gestionan y desarrollan su negocio. A través de demostraciones prácticas y sesiones específicas, los asistentes podrán conocer todas sus capacidades y

aprender a sacar el máximo partido a sus funcionalidades para optimizar procesos, mejorar la toma de decisiones y ganar eficiencia en su actividad diaria.

“ES EL MOMENTO DE TEJER NUEVAS ALIANZAS, DE ABRIR MERCADO Y DE INTEGRAR TECNOLOGÍAS PARA PODER NAVEGAR EN LAS AGUAS QUE HA REVUELTO LA IA, Y CREEMOS QUE NO HAY NADA MEJOR QUE UN EVENTO COMO EL SIMPOSIUM PARA CONSEGUIR LAS RESPUESTAS A LAS PREGUNTAS QUE TODOS NOS HACEMOS”

SARA ZAMORA,

marketing & communications manager de **Ingram Micro**



el que el canal defina su propuesta de valor en este nuevo ecosistema. Por eso pensamos que, en realidad, el mañana se escribe hoy, pero tenemos que escribirlo nosotros para que seamos creadores de esa nueva realidad, y no simples reactores a la misma”.

NUEVAS OPORTUNIDADES EN UN MOMENTO DE CAMBIO

Para esta responsable, “queremos que el Symposium de Ingram Micro sea un nuevo éxito este año, pero es verdad que miramos más allá de los números; por supuesto que queremos batir récord de asistencia, pero lo que más nos interesa es que los asistentes consigan sus objetivos. Es el momento de tejer nuevas alianzas, de abrir mercado y de integrar tecnologías para poder navegar en las aguas que ha revuelto la IA, y creemos que no hay nada mejor que un evento como el Symposium para conseguir las respuestas a las preguntas que todos nos hacemos. Si conseguimos que los asistentes terminen el Symposium con nuevos contactos, alianzas e ideas claras sobre las estrategias que definirán nuestro futuro como industria, habrá sido un verdadero éxito”.

La experiencia del evento se verá reforzada por la app oficial de Symposium 2026, una herramienta que permitirá a los asistentes planificar su agenda, consultar toda la información de la jornada y gestionar reuniones one-to-one con fabricantes, especialistas y otros partners. Una funcionalidad especialmente orientada a fomentar nuevas oportunidades de colaboración y negocio antes, durante y después del evento.

NOVEDADES DE ESTA EDICIÓN

Como gran novedad de esta edición, el Symposium 2026 incorpora-

rá un exclusivo afterwork de 15:30 a 17:00 horas, concebido como un espacio para seguir conectando y fortaleciendo relaciones profesionales en un ambiente más distendido. Los asistentes podrán disfrutar de la actuación en directo de la HP Mad Band, que pondrá la banda sonora al cierre de la jornada.

PREPARAR AL CANAL PARA EL FUTURO QUE NACE AHORA

Para conocer más detalles de la cita de este año, hemos hablado con Sara Zamora, marketing & communications manager de Ingram Micro, que nos explicaba que

el lema de este año “refleja muy bien la realidad en la que nos encontramos, un momento de cambio, de transición evidente hacia un futuro que aún todos desconocemos, porque la disrupción en que se basa, que es la inteligencia artificial, ni siquiera tiene claros sus propios desafíos ni verdadero potencial”.

Mucho se habla de IA, pero para Sara Zamora “es una tecnología que busca su encaje en un mundo abierto a ella, pero temeroso al mismo tiempo por el impacto que puede tener en nuestras vidas. Y queremos que este Symposium de 2026 sea el punto de encuentro en

« En palabras de Sara Zamora, “además de los nuevos productos y servicios que cada año presentan los expositores, las principales novedades en cuanto a organización se centran en la app exclusiva del Symposium, donde los asistentes podrán consultar no solo la agenda de ponencias, actividades y presentaciones, sino la disponibilidad de profesionales para mantener reuniones privadas enfocadas a conocerse y establecer esas alianzas que comentaba. Para nosotros es muy importante que se puedan generar relaciones de calidad en entornos que permitan el intercambio de ideas y el conocimiento mutuo, y la app del Symposium permite reservar espacios y bloquear agendas para hacerlo posible de manera eficiente”.

LA IA EN EL CENTRO DEL DEBATE

Para Zamora, “la inteligencia artificial está y estará en el centro del debate, porque es la tecnología más disruptiva que hemos conocido hasta ahora, a pesar de que venimos de revoluciones inimaginables como la informática, Internet o el smartphone. Todos tenemos muchas preguntas sobre la IA, pero

también muchos planes y objetivos para aprovechar las capacidades que traerá consigo, así que lo que buscamos este año es contar con expertos y profesionales que ayuden a entender mejor este fenómeno para que las empresas puedan integrar la IA a su favor. Pero no todo va a girar alrededor de la IA: también hablaremos de cloud, de ciberseguridad y de la evolución del ecosistema digital en las empresas más allá de la IA, donde tienen cada vez más peso segmentos como PROAV/UCC y DCPOS, porque estamos en un momento en el que confluyen varias revoluciones digitales por capas que solo quienes logren integrar de manera coordinada podrán exprimir realmente a su favor”. ■

MÁS INFO +**» [Simposium Ingram Micro 2026](#)****COMPARTIR EN REDES SOCIALES**

DESCUBRE POR QUÉ SOMOS TU SOCIO ESTRATÉGICO

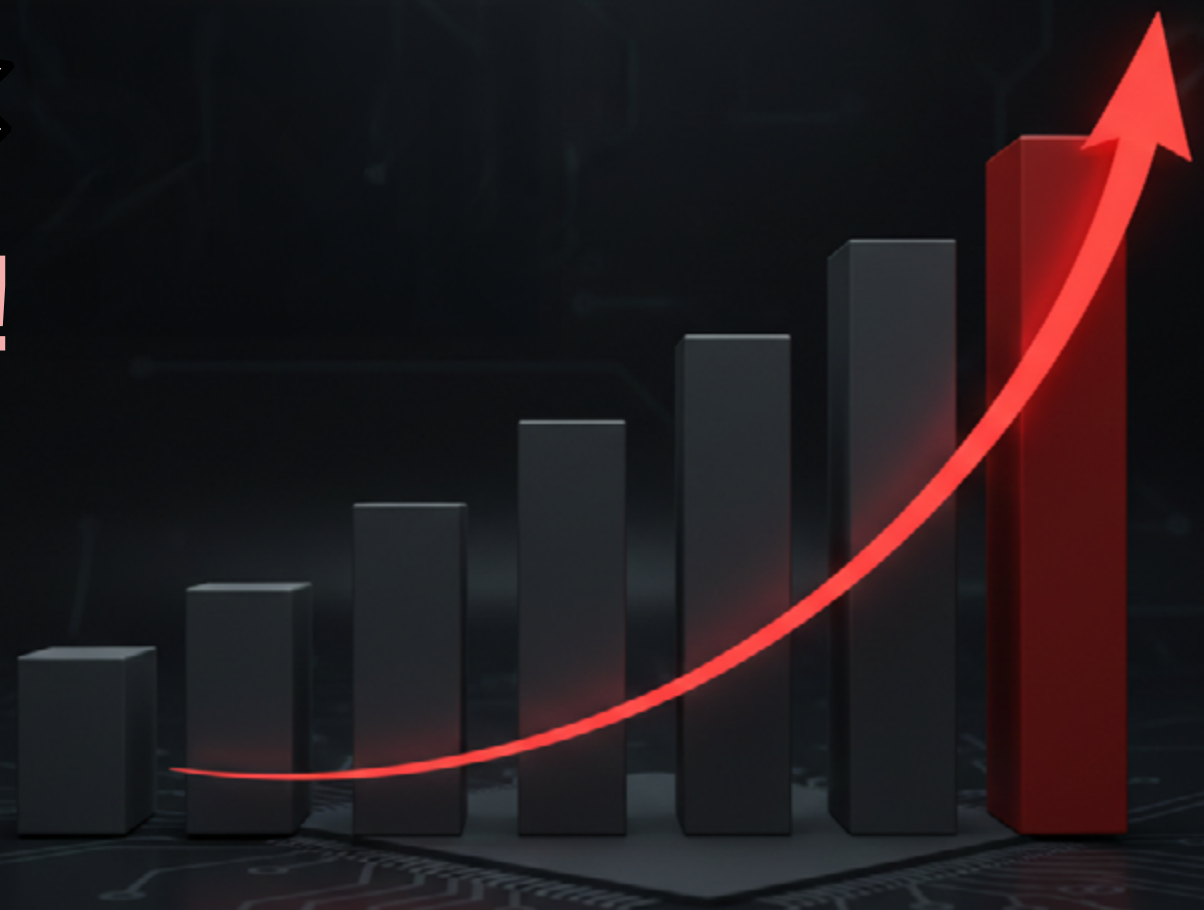


En un mercado que no se detiene, tu stock tampoco debería hacerlo. En DMI Computer combinamos logística inteligente y marcas líderes para que tu única preocupación sea seguir creciendo.

Tu stock, a un clic de distancia



« **¡ESCALAMOS TU NEGOCIO!** »



#ENTREVISTA

“El contexto aporta eficiencia a la IA”

« YITZHAK KESSELMAN,
CORPORATE VICE PRESIDENT, MICROSOFT FABRIC »

» MIGUEL ÁNGEL GÓMEZ (BARCELONA)

Yitzhak Kesselman dirige la estrategia de la plataforma Microsoft Fabric, que incluye Real-Time Intelligence y Fabric IQ, ayudando a las organizaciones a recopilar y conectar datos operativos, generar información en tiempo real y traducir esa información en acciones. Aprovechando su presencia en Barcelona en la European Microsoft Fabric + SQL Community Conference, hemos conversado con él.



Más allá de los anuncios realizados, ¿cuál cree que es el mensaje clave de este evento?

Quizá deberíamos empezar por explicar por qué estamos haciendo esos eventos. Creo que es importante, porque esta conferencia quizá es un poco diferente. La idea es reunir a la comunidad y a las personas que desarrollan y utilizan esta tecnología. Creo que es importante reunir a la gente que usa la tecnología, porque hay mucho de compartir para entender cómo hacen las cosas. Así que creo que eso es algo bastante importante. Uno de los mensajes clave que estamos transmitiendo es cómo estamos proporcionando el contexto adecuado para la IA. Cómo creamos un contexto que vaya desde las aplicaciones de negocio, proporcionado a través de toda la capa analítica Fabric IQ, pero también cómo lo vinculamos al contexto más amplio del ecosistema Microsoft IQ. Cómo recreas el contexto adecuado para que los agentes sean realistas, efectivos, y más correctos. Y, más allá de esto, una gran cantidad de anuncios concretos.



¿Qué cambia cuando la IA puede razonar sobre el contexto empresarial y no solo con datos?

Los responsables de la gestión son buenos para entender datos no estructurados, su contexto y las ideas detrás de estos datos. Pero aquí tenemos algunos datos estructurados y contexto detrás. Y hemos visto internamente que cuando quieres que los agentes te ayuden con tus datos y con tu empresa, estas quieren cambiar cómo dirigen las operaciones, porque eso se traduce en cómo ser más relevantes, más rentables, cómo servir mejor a sus clientes. Y para hacer el cambio con lo que la industria llama inteligencia

operativa, necesitan tener el contexto adecuado para que los agentes operen. Y este contexto está bien definido porque las empresas hoy saben cómo funcionan. Puede ser un conocimiento tribal, no siempre está documentado, algunos datos están en la mente de las personas, algunos en los documentos, algunos en las bases de datos, algunos datos llegan en flujo en tiempo real... y la oportunidad está en reunir esos contextos de diferentes dominios en un solo lugar y crear un contexto unificado.

Dentro de una empresa hay diferentes entidades, incluyendo también las acciones, las reglas y las políticas, y eso es lo que hace que la IA sea mu-

“ESTAMOS APORTANDO CONTEXTO PARA QUE LOS AGENTES SEAN REALISTAS, EFECTIVOS, Y MÁS CORRECTOS”

cho más eficiente que ejecutándose con los datos en bruto. Por tanto, la inteligencia que nos proporciona se apoya en el contexto adecuado, y es mucho más rentable porque ya no necesita adivinar qué contenido debe utilizar. Y eso es lo que hace que los agentes se vuelvan mucho más efectivos. No quieres que los agentes recreen tu base de datos operativa cada vez que necesitas responder a una pregunta relacional, quieres que el agente sepa cómo trabajar con una base de datos. Y, en este caso, lo que quieres es que el agente tenga el contexto adecuado para responder a las preguntas correctas y para operar. Y esa es la parte más interesante. Permitir que los agentes se vuelven mucho más relevantes y sofisticados.

La observabilidad en Fabric ofrece más que monitorización. ¿Qué tipo de desafíos operativos estamos preparados para gestionar?

Lo que queremos ofrecer mediante la observabilidad, no es solo monitorización de los diferentes elementos, sino también acciones proactivas y correctivas. Eso es algo en lo que estamos invirtiendo más que para recibir las notificaciones correctas con antelación y hacer un análisis profundo de la causa real de una alerta. Estamos trabajando para aprovechar el poder de todos los datos que tenemos en Fabric y las experiencias que tenemos del mundo de Azure Monitor, para reunirlos y así tener este tipo de experiencias. Y, en el futuro, poder vincularlas a los datos empresariales.

Con IQ Sharing, ¿cómo equilibran el intercambio de contenido empresarial con la gobernanza de los datos?

La gobernanza no es negociable. Pero, en la realidad actual, muchas empresas no viven en islas aisladas. Necesitan compartir sus datos con sus clientes, con sus socios, con sus proveedores... y hacer esto, compartir con la gobernanza adecuada, con las políticas adecuadas, con la capacidad de revocar, la capacidad

de alertar... proporciona capacidades muy significativas para nuestros clientes. La idea aquí es permitir que la organización comparta de forma muy segura, gobernada y controlada. Es evidente que las empresas tendrán que compartir datos, y la cuestión es cómo lo hacen.

¿Qué significa Fabric Apps para la convergencia de análisis de datos y desarrollo de aplicaciones?

Los informes de Power BI realmente permiten responder preguntas. Pero ahora, en el mundo actual, quiero hacer más que solo responder preguntas. Quiero actuar. Así que esa es la evolución natural: de Power BI hacia aplicaciones. No solo tener respuestas visuales para mí, sino también la capacidad de construir una aplicación donde pueda escribir datos de nuevo en el sistema de forma bidireccional. Por eso vemos una rápida adopción de las aplicaciones Fabric en el mercado.

Sin embargo, muchas empresas aún están en una fase inicial de IA con prototipos, pilotos... ¿Cómo les ayudan a entrar en un nuevo entorno con seguridad, gobernanza y productividad?

De dos formas diferentes. Por un lado, la tecnológica. Ahí, Fabric, por sí solo, te permite reunir fácilmente toda la información a través de diferentes conjuntos de datos, diferentes sistemas en un solo lugar... y luego tener múltiples motores que pueden trabajar en el lado analítico, en BI y en inteligencia en tiempo real de una forma muy segura y común. Y luego puedes crear el contexto para que la IA lo haga. Así que la tecnología en sí misma lo facilita mucho para los clientes.

El otro es con la guía, la documentación, las mejores prácticas, y también esta conferencia, ayudar a los clientes a entender cuáles son las mejores prácticas. Estamos compartiendo muchas buenas prácticas y cómo deberían implementarse. Proporcionar a los clientes ejemplos les ayuda mucho a asentarse, aunque cada empresa tiene sus propios matices, diferentes fuentes de datos, distintos permisos, quizá otros puntos de integración... pero, en general, tienen socios similares que quieren tratar con IA. Así que proporcionar esta orientación puede ayudar a acelerar esas experiencias, eso es algo que ofrecemos.

¿Qué diferencia la estrategia de Microsoft de otras alternativas en el mercado?

Creo que esta cuestión tiene múltiples facetas. La primera, la plataforma, que permite traer todos estos datos a través de múltiples fuentes de datos en el sistema, ya sea en la nube, on-premise... de forma segura y fácil, y esto es diferencial porque elimina un obstáculo para muchas empresas. Lo segundo es el propio motor dentro de Fabric, porque los costes de las cargas de trabajo son muy rentables, comparados con otros. Y la siguiente capa es cómo esto se combina con el resto del ecosistema de Microsoft, creando algo que ayuda a los clientes a proporcionar un mejor contexto para los agentes. ■

MÁS INFO

» [Microsoft activa en FabCon + SQLCon EU 2026 la era de la inteligencia agéntica corporativa](#)



COMPARTIR EN REDES SOCIALES

#EN PORTADA

LA LEY DE IA IMPONE NUEVAS REGLAS DEL JUEGO EN EL MERCADO TI EUROPEO

» RICARDO GÓMEZ

La aplicación progresiva del Reglamento Europeo de Inteligencia Artificial (EU AI Act) marca un hito sin precedentes para la industria tecnológica de la región. Analizamos cómo la nueva normativa está transformando el desarrollo de software, la gobernanza del dato, las arquitecturas cloud y las estrategias de adopción tecnológica en Europa, con la colaboración de expertos de Celonis, Cognizant, Devoteam, IONOS Cloud, Microsoft, SAP, Wolters Kluwer y Workday.

« El marco regulatorio europeo sobre Inteligencia Artificial representa un cambio de paradigma en la gobernanza de la tecnología a escala global. Desde la entrada en vigor del EU AI Act en agosto de 2024, las organizaciones tecnológicas han tenido que adaptar a marchas forzadas sus procesos de diseño, desarrollo y comercialización. El texto legislativo busca armonizar el mercado único mediante un enfoque basado en riesgos, estableciendo obligaciones estrictas que van desde la transparencia básica en modelos de IA generativa hasta la supervisión humana, la trazabilidad de algoritmos y la gestión integral de datos de entrenamiento en sistemas catalogados de alto riesgo.

El calendario regulatorio ha alcanzado un momento crítico a partir de agosto de 2026 con la plena exigibilidad de las obligaciones de transparencia estipuladas en el artículo

50, que afectan directamente a la interacción con usuarios, la identificación de contenidos sintéticos y el etiquetado de sistemas automatizados. A su vez, este escenario sirve de antesala para la entrada en vigor de restricciones más severas para entornos de alto riesgo, fijadas para 2027 y 2028. Las compañías del sector TI que operan en España afrontan este despliegue obligadas a auditar sus proyectos en curso, redefinir sus modelos operacionales y elevar la soberanía digital a la categoría de prioridad estratégica imprescindible.

CAMBIOS IMPULSADOS POR LA LEY DE IA

Transcurridos más de dos años desde que la Comisión Europea presentara la propuesta del Reglamento de Inteligencia Artificial (AI Act), el mercado del software ha experimentado una importante transformación. El impacto inicial se tradujo en un

cambio en la forma de invertir de las organizaciones, especialmente de las grandes empresas, que han pasado de pruebas de concepto a centrarse en proyectos de IA con garantías de gobernanza. Por su parte, las empresas tecnológicas han integrado la evaluación de riesgos desde la fase de diseño (privacy and compliance by

design) para ofrecer soluciones empresariales que puedan ser auditadas bajo la nueva regulación.

Como explica Vanessa Candela, Chief Legal & Trust Officer en Celonis, “el cambio más visible es que el desarrollo de la IA ha dejado de ser un proceso puramente técnico”. Señala que, desde agosto de 2024, exigencias



como la clasificación de riesgos, la documentación técnica, la gobernanza de datos y la supervisión humana se han integrado como requisitos de ingeniería.

Javier Pozuelo, director de Data & AI para España, Portugal e Italia en Cognizant, añade que, debido a imposición legal de controles más rigurosos en los proyectos de IA generativa, “en general, las empresas tardan mayor tiempo en decidir la implantación de las soluciones basadas en IA generativa debido a las revisiones que están realizando con sus departamentos jurídicos”, algo que considera positivo

porque se preparan mejor antes de desplegar la tecnología.

En la misma línea, José Luis de la Fuente, director de AI&Data en Devoteam, sostiene que “hemos observado un cambio de estrategia en el mercado, pasando de una experimentación donde primaba la velocidad en obtener un resultado a la adopción estructurada y madurada”. Y resalta que, lejos de actuar como un freno a la innovación, este cambio aporta una necesaria certidumbre jurídica, haciendo más seguras las inversiones.

Para Guillermo Arana, manager de IONOS Cloud España, “la AI Act ha

funcionado de catalizador, como pasó con el RGPD o está pasando con Verifactu”, y enfatiza que Europa ha liderado el establecimiento de un marco armonizado que combina seguridad e innovación, respondiendo a las propias demandas de la industria. Opina que, al anticipar conceptos fundamentales como la supervisión humana, la trazabilidad, la responsabilidad y la soberanía digital, la legislación europea permite a las empresas diseñar arquitecturas sólidas y competitivas.

Gabriel López Serrano, director de Regulación y Relaciones Institucio-

nales de Microsoft en España, enfatiza que la Ley de IA ha proporcionado certidumbre para consolidar la adopción corporativa, y afirma que “su principal impacto ha sido situar la gestión del riesgo, la seguridad, la transparencia, la supervisión humana y la responsabilidad en el centro de los proyectos”.

La anticipación a la ley ha sido un factor clave para las grandes firmas del software empresarial, según Jorge Morillo, head of Government Affairs and Public Policy en SAP España, quien explica que “cada caso de uso de IA desarrollado, desplegado, co-

“ LA EXPLICABILIDAD NO ES UN OBSTÁCULO PARA UNA IA EFICAZ. DE HECHO, ES ESENCIAL ”

VANESSA CANDELA,
Chief Legal & Trust Officer en
Celonis



“ NO COMETAMOS EL ERROR DE ASOCIAR LA UBICACIÓN FÍSICA DE LA IA A SU SEGURIDAD ”

JAVIER POZUELO,
director de Data & AI para
España, Portugal e Italia en
Cognizant



mercionalizado o utilizado por SAP pasa por una evaluación de impacto ética”.

En cuanto a las implicaciones operativas para el software de gestión y legal, Piermario Porcheddu, Legal director & assistant general counsel en Wolters Kluwer Tax & Accounting Europe & APAC, opina que “los proveedores de soluciones de IA han tenido que establecer procesos y principios de gobernanza claros y transparentes que respondan tanto a los requisitos regulatorios como a las nuevas expectativas de los clientes”, mitigando los riesgos jurídicos.

Finalmente, desde la perspectiva

de la gestión de recursos humanos y finanzas, Paolo Oberti, solution consulting de Workday EMEA, afirma que la AI Act ha forzado una reestructuración de fondo en la industria del software y que “en el escenario actual, la capacidad de ofrecer una IA segura, auditable y ética se ha convertido en el requisito básico para competir en el mercado corporativo europeo”.

IMPACTO EN LOS PROYECTOS EN MARCHA

La futura entrada en vigor de nuevas exigencias para sistemas basados en IA, especialmente los de alto riesgo,

ha hecho saltar las alarmas en las empresas españolas, impulsando auditorías masivas de los algoritmos y revisiones de las arquitecturas de datos. Así, aunque el plazo en este caso se ha ampliado, los proyectos en fases iniciales se ven forzados a certificar su calidad, trazabilidad y supervisión humana antes de llegar a producción, planteando el reto de conciliar el cumplimiento normativo con las necesidades del negocio.

Según Vanessa Candela (Celonis), “para el sector, el efecto práctico de ese aplazamiento no es un alivio, sino una ampliación de la brecha exis-

tente”. Candela enfatiza que las empresas están solicitando pruebas de cumplimiento normativo a los proveedores mucho antes de la entrada en vigor formal de las fechas límite para sistemas de alto riesgo. Respecto a los proyectos que llevan años en producción en España, señala que el gran desafío radica en reconstruir la gobernanza de forma retrospectiva.

Desde la perspectiva de la compañía Cognizant, Javier Pozuelo percibe que “muchos proyectos que funcionaban con agilidad en entornos de POC encuentran ahora barreras de entrada para escalar comercialmente si no

“ VENDER IA TRANSPARENTE SE CONVERTIRÁ EN UN SELLO DE CALIDAD DEL SOFTWARE EUROPEO ”

JOSÉ LUIS DE LA FUENTE,
director de AI&Data en
Devoteam



“ LA AI ACT HA FUNCIONADO DE CATALIZADOR PARA ARMONIZAR SEGURIDAD E INNOVACIÓN ”

GUILLERMO ARANA,
manager de **IONOS Cloud**
España



pueden demostrar el cumplimiento normativo exigido a proveedores y despliegues”, lo que podría afectar a su paso a entornos de producción.

Coincide José Luis de la Fuente (Devoteam) en que “aquellos proyectos que no nacieron teniendo en cuenta un marco de gobierno ético están requiriendo reajustes significativos” y que los proyectos pensados para obtener resultados rápidos requieren ahora la asistencia de servicios especializados de revisión y adaptación tecnológica.

« Por su parte, Guillermo Arana (IO-NOS Cloud) subraya que, aunque la

nueva normativa no ha tomado por sorpresa al sector de las tecnologías de la información, puede afectar a las compañías menos preparadas, ya que “la propia velocidad del desarrollo de la IA ha obligado a replantearse muchos aspectos de explotación del dato para que prime la resiliencia, la interoperabilidad y la portabilidad”.

Desde una perspectiva más positiva, Gabriel López Serrano (Microsoft) opina que España parte de una posición favorable ya que, “según el último Microsoft AI Diffusion Report, es el sexto país en adopción de IA, con un 45,1% de la población en edad de

trabajar”, pero matiza que la madurez entre pymes sigue siendo desigual, lo que enfatiza el valor de un ecosistema de partners tecnológicos que será fundamental para adaptarse a la Ley.

En cuanto a la traslación de las exigencias de transparencia del artículo 50, Jorge Morillo (SAP) afirma que el modelo adecuado es el de responsabilidad compartida. Así, los proveedores deben incorporar capacidades de transparencia y “los clientes, como responsables del despliegue, deben analizar sus casos de uso frente a los requisitos que les sean aplicables”, configurar

los controles adecuadamente y encargarse de informar a los usuarios finales.

Sobre la continuidad operativa ante los cambios introducidos por la Ley de IA en 2026, Piermario Porcheddu (Wolters Kluwer) comenta que “no esperamos que el sector se vea tan afectado como cuando el Reglamento de IA entró en vigor en 2024”. Argumenta que la mayoría de los proveedores ya aplican avisos en asistentes virtuales y campañas informativas, mientras que otros aspectos como la protección frente a imágenes manipuladas o deepfakes tendrán una

»

“EUROPA NO DEBERÍA TENER QUE ELEGIR ENTRE REGULAR E INNOVAR; DEBE HACER AMBAS COSAS”

GABRIEL LÓPEZ SERRANO,
director de Regulación y Relaciones Institucionales de
Microsoft en España



“UNA IA ÉTICA Y RESPONSABLE CONTRIBUIRÁ A GENERAR UNA VENTAJA COMPETITIVA”

JORGE MORILLO,
head of Government Affairs and Public Policy en **SAP España**



incidencia menor en el segmento de software de gestión B2B.

Por último, Paolo Oberti (Workday) observa una marcada polarización, señalando que “aquellos proyectos desarrollados sin un esquema claro de gobernanza o sobre modelos poco transparentes están sufriendo revisiones complejas o incluso suspensiones por la dificultad de certificar su cumplimiento”, mientras que aquellas organizaciones que han apostado por plataformas con gobernanza nativa certificada -como ISO 42001 y NIST AI RMF- continúan

escalando sus operaciones con absoluta seguridad jurídica.

SOBERANÍA DEL DATO: CLOUD ACT VS. AI ACT

El choque frontal de la AI Act con las normativas internacionales sobre acceso a datos, como la Cloud Act estadounidense, ha avivado el debate sobre la soberanía digital en Europa. Las empresas de la región se enfrentan a una doble necesidad: aprovechar las capacidades de cómputo y modelos avanzados de proveedores externos a la UE mientras garantizan

que el tratamiento de la información cumple con el RGPD y la AI Act. Esto está convirtiendo la soberanía del dato en un criterio prioritario en las decisiones de compra de tecnología e impulsando el mercado de modalidades de nube soberana.

Lo que necesitan ahora las empresas, según Vanessa Candela, de Celonis, “es determinar dónde se procesan sus datos, quién tiene la capacidad técnica para acceder a ellos y si eso puede demostrarse ante un regulador, un auditor o sus propios clientes”. Por ello, considera

la soberanía como un aspecto clave para cumplir con las regulaciones europeas, también en lo que se refiere a la IA.

Javier Pozuelo, de Cognizant, destaca el renovado interés por la localización de los datos y el auge del software libre, y afirma que “en Europa en general todavía existe margen para una adopción más amplia de determinados modelos open source como los de Meta, Qwen, Kimi o Deepseek”, que al ejecutarse tanto en local como en entornos cloud soberanos, permiten el fine-tuning, la

“ LOS BENEFICIOS DE LAS SOLUCIONES CLOUD CON IA SON SUPERIORES AL ON-PREMISE ”

PIERMARIO PORCHEDDU,
legal director & assistant general
counsel en **Wolters Kluwer**



“ OFRECER UNA IA SEGURA, AUDITABLE Y ÉTICA ES EL REQUISITO BÁSICO PARA COMPETIR ”

PAOLO OBERTI,
solution consulting de
Workday EMEA



reducción de costes de licencias y un mayor control sobre la gobernanza.

José Luis de la Fuente, de Devoteam, confirma el fuerte repunte en la demanda de soluciones bajo control comunitario, una inquietud que lidera las agendas de los comités de dirección, y destaca que “prácticamente la primera pregunta al entablar una conversación con nuestros clientes en proyectos de cierto calado es si se puede hacer este proyecto en un marco controlado en la UE”. A su vez, constata una mayor demanda de infraestructuras soberanas y on-premise que mantengan los datos dentro de las fronteras europeas.

“La soberanía está empezando a ser un requerimiento de negocio y no solo técnico o de cumplimiento normativo”, asegura Guillermo Arana, de IONOS Cloud, y argumenta que operar en centros de datos ubicados en Europa, bajo legislación comunitaria, sin dependencias extracomunitarias y apostando por código abierto, constituye la única garantía real para proteger la resiliencia y la competitividad empresarial.

Gabriel López Serrano, de Microsoft, aclara que el Reglamento de IA no contiene disposiciones sobre el acceso gubernamental a datos,

aspectos contemplados por otras regulaciones como el RGPD, por lo que “más que un choque entre la Cloud Act y la Ley de IA, lo que existe es un debate legítimo, y necesario, sobre cómo conviven los instrumentos de cooperación judicial”.

Por su parte, Jorge Morillo, de SAP, expone un marco multidimensional que comprende la soberanía de datos, operativa, técnica y legal. Apunta que “para nosotros, la soberanía digital es la capacidad de una organización, un sector o un país de mantener un control efectivo sobre sus activos, tecnologías y operaciones digitales”, un reto que debería abordarse sin aislarse de la innovación global.

Para Piermario Porcheddu, de Wolters Kluwer, la soberanía legal es relevante pero no exclusiva, y opina que “la protección jurídica que ofrece la legislación europea será sin duda un factor a la hora de elegir infraestructura cloud europea, pero es probable que la proximidad al cliente, el rendimiento y el coste seguirán siendo los principales motores de decisión”.

“Las organizaciones europeas, especialmente las pertenecientes a sectores fuertemente regulados o a la administración pública, demandan certidumbre respecto a la jurisdic-

ción bajo la cual se procesa su información”, explica Paolo Oberti, de Workday, quien cree que el éxito de las plataformas SaaS radica en ofrecer análisis avanzado e IA generativa garantizando la máxima protección frente a normativas extraterritoriales.

EXPLICABILIDAD Y TRANSPARENCIA COMO VENTAJA

El Reglamento Europeo de IA establece la obligación de garantizar la explicabilidad, trazabilidad y transparencia de los algoritmos. Tradicionalmente, el desarrollo de redes neuronales profundas y modelos de lenguaje (LLM) ha seguido el modelo de 'caja negra', cuya lógica interna resulta difícil de auditar, pero la nueva ley exige que los resultados generados por IA puedan ser justificados y comprendidos por los usuarios finales. Lejos de suponer un freno para el rendimiento técnico, la industria europea del software está transformando la explicabilidad en un atributo diferencial de calidad, capaz de generar la confianza necesaria para su adopción en procesos críticos.

Frente a quienes perciben la transparencia como un lastre para el desarrollo de software, Vanessa Candela (Celonis) sostiene que “la

explicabilidad no es un obstáculo para una IA eficaz”. Reconoce que los costes de cumplimiento afectan de forma desigual a startups y grandes firmas -aspecto amortiguado por el enfoque simplificado de la Omnibus

para pymes-, pero cree que los fabricantes europeos que diseñen sistemas explicables nativos obtendrán una clara ventaja competitiva.

“Como compañía multinacional vemos el reto de mantener la ca-

pacidad de innovación y competitividad global de Europa al mismo tiempo que se desarrolla un marco regulatorio sólido y confiable”, señala Javier Pozuelo (Cognizant), pero recalca la necesidad de preservar el

liderazgo de la industria europea. Y considera que la gobernabilidad de la IA plantea multitud de oportunidades, siempre que la aplicación de las leyes evolucione conforme al avance tecnológico.

ARQUITECTURA TI PARA SISTEMAS DE ALTO RIESGO

« Ante la futura llegada de restricciones severas para entornos de alto riesgo surge la necesidad de evaluar qué tipo de arquitectura de TI es la más adecuada para cumplir con estos requisitos. Las opiniones al respecto son muy variadas, y, aunque existe un cierto nivel de consenso en la industria sobre la idoneidad de la TI híbrida, se plantean diferentes formas de concebir este modelo. Expertos como Vanessa Candela, de Celonis, prevén el predominio de arquitecturas híbridas con supervisión auditable. Para Javier Pozuelo, de Cognizant, las arquitecturas on-premise y en

cloud soberano ofrecen niveles similares de protección, aunque apuesta por la ejecución on-premise de modelos open source.

“Lo que triunfará serán los modelos híbridos: el entrenamiento y los servicios menos críticos en cloud pública controlada, y la inferencia de alto riesgo desplegada en entornos aislados, privados u on-premise”, opina José Luis de la Fuente, de Devoteam, mientras que, para Guillermo Arana, de IONOS Cloud, “no importa tanto sobre qué modelo de nube corra la IA sino quién la controla realmente, la empresa o el proveedor”, y apuesta por estándares de código

abierto para diseñar arquitecturas multicloud e híbridas.

El debate está en “qué combinación de tecnologías permite a cada organización equilibrar mejor innovación, cumplimiento normativo, soberanía y control operativo”, según Gabriel López Serrano, de Microsoft, algo en lo que coincide Jorge Morillo, de SAP, para quien la elección de arquitectura requiere un análisis complejo que contemple todas las variantes de infraestructura local y en cloud.

Por otro lado, Piermario Porcheddu, de Wolters Kluwer, opina que “los beneficios

profesionales y comerciales de las soluciones cloud impulsadas por IA son ya superiores a los que puede ofrecer un equivalente on-premise”. Y Paolo Oberti, de Workday, sostiene que las exigencias de la Ley europea de IA actuarán como un acelerador del modelo SaaS en la nube porque “asumir de forma individual y sobre infraestructura propia las obligaciones de evaluación continua de riesgos, auditoría, prevención de sesgos y documentación técnica en sistemas de alto riesgo supone un coste operativo inasumible para la mayoría de las empresas”.

Coincide José Luis de la Fuente (Devoteam) en que “desarrollar y vender IA transparente se convertirá en un sello de calidad que diferenciará al software europeo a escala mundial, estableciendo un estándar ético y de fiabilidad que otros mercados terminarán exigiendo”. Y prevé que los clientes corporativos rechazarán cada vez más las soluciones que no sean comprensibles ni auditables.

Desde la visión de los modelos de código abierto y la soberanía tecnológica, Guillermo Arana (IONOS Cloud) reafirma que la apertura informativa es el mejor catalizador para el mercado. “Ser transparente y explicar cómo se hacen las cosas genera confianza, no es un freno para la competitividad”, afirma, y recalca que el open source otorga la flexibilidad necesaria para migrar e innovar al margen de entornos propietarios.

Por otro lado, Gabriel López Serrano (Microsoft) sostiene que la transparencia es la condición previa para la penetración del software en sectores regulados, y explica que “la competitividad no dependerá únicamente de quién desarrolle las capacidades de IA más avanzadas, sino también de quién sea capaz de trasladarlas al mercado de forma segura,

fiable y responsable”. Por ello, opina, el reto estará en aplicar la norma de forma limpia y proporcionada, evitando burocracias innecesarias.

Desde el punto de vista de Jorge Morillo (SAP), la ética aplicada es un motor de negocio duradero, y destaca que “nuestra propia Política Global de Ética de la IA señala que una IA ética y responsable contribuirá a acelerar su adopción, reducir riesgos legales y operativos y generar una ventaja competitiva a largo plazo”. Añade que es imperativo trazar el origen de los datos y la lógica de cada decisión, pero insta a que las autoridades apliquen las normas de manera armonizada para evitar interpretaciones nacionales fragmentadas en la UE.

Sopesando la influencia real de estas exigencias en la posición de mercado de los desarrolladores, Piermario Porcheddu (Wolters Kluwer) considera que la transparencia es un requisito completamente asumible. Y sentencia que “lo que seguirá siendo más determinante es la trayectoria del fabricante, su fiabilidad y la calidad de sus productos para resolver los problemas de sus clientes de forma eficaz y rápida”.

Dede su punto de vista, Paolo Oberti (Workday) argumenta que la opacidad



algorítmica es inaceptable en los procesos de recursos humanos o finanzas, afirmando que “en áreas estratégicas como la gestión del talento o los recursos financieros, las empresas no pueden respaldar sus decisiones en algoritmos cuya lógica se desconoce”.

La opinión de estos expertos pone de relieve el moderado optimismo de una industria que, sobre todo en el caso de las compañías europeas, se apoya cada vez más en valores como la soberanía digital, la ética y la aplicación de la tecnología en beneficio de la sociedad. Y, precisamente, consideran estas cuestiones como potenciales motores de un mercado cada vez más condicionado por regulaciones más estrictas que en otras regiones en cuanto a la privacidad, la explicabilidad y el control. Pero queda por ver si esta estrategia permitirá

ganar posiciones en una industria dominada por desarrolladores y proveedores estadounidenses.■

MÁS INFO +

- » [Ley europea de IA](#)
- » [Ley de IA: medidas de simplificación y prohibición de desnudos falsos](#)
- » [Proyecto de Ley del Gobierno español para la supervisión humana y un uso confiable de la IA](#)



COMPARTIR EN REDES SOCIALES

GUÍA PRÁCTICA:

CÓMO APLICAR LA IA EN LOS FLUJOS DE TRABAJO



DESCARGAR
DOCUMENTO



claranet[®]



#REPORTAJE

EL DESAFÍO DE ORQUESTAR LA CIBERSEGURIDAD CORPORATIVA

RAFAEL CLAUDÍN

Los riesgos asociados a las últimas innovaciones tecnológicas, la proliferación de amenazas y la entrada en vigor de nuevas normativas suponen nuevos desafíos para la ciberseguridad. Sin un planteamiento de gobierno ciber que esté bien asentado y alineado con los valores y la estrategia corporativa, el éxito futuro de las organizaciones pende de un hilo.

«El gobierno de la tecnología ha sido un campo tradicionalmente ligado a los equipos de TI, pero en los últimos años ha ido adquiriendo una mayor relevancia para el conjunto de las organizaciones. Es una evolución natural, que acompaña la transformación de los datos y la tecnología basada en ellos en elementos centrales del éxito corporativo. Si las empresas son ecosistemas vivos, en los que el cambio de algunos de sus componentes produce un efecto en cadena sobre todo el conjunto, en la última década han evolucionado tantos elementos que los ecosistemas están revolucionados.

Y una de las claves para el éxito futuro de esa revolución es la ciberseguridad.

Si intentas obtener una visión de conjunto sobre los cambios tecnológicos, normativos y de ciberseguridad de los últimos 10 años que han protagonizado la llamada

digitalización, es fácil constatar la sincronía que los ha guiado. La legislación en torno a la inteligencia artificial, el tratamiento y la privacidad de los datos, la ciberseguridad y la ciberresiliencia, se entrelazan con las tendencias tecnológicas y su práctica corporativa, que a su vez están estrechamente ligados con los estándares sectoriales y su evolución.

30 AÑOS DE EVOLUCIÓN EN EL MODELO DE GOBIERNO

La cuestión del gobierno de la tecnología y de la ciberseguridad, que hasta hace muy poco apelaba únicamente a los expertos dedicados a esas tareas, nació a mediados de la década de los 90, con la llegada de los primeros estándares. ISACA estableció por primera vez su marco de gobernanza y gestión de TI COBIT (Control Objectives for Information and Related Technologies) en 1995, el mismo año en que la británica

BSI lanzó la norma BS 7799-1 para la gestión de la seguridad de información, que una década después sería adoptada por la Organización Internacional de Normalización y se convertiría en la ISO 27001.

Otro de los estándares que interesa tener presente es el Cybersecurity Framework (CSF) que el NIST de Estados Unidos lanzó en 2014. En ese momento se dirigía específicamente a infraestructuras críticas



y giraba en torno a cinco cuestiones centrales: identificar, proteger, detectar, responder y recuperar. En su segunda versión de 2024, amplió su alcance a todo tipo de organizaciones y una de sus principales novedades fue añadir una función más a las cinco originales: el gobierno.

La evolución de las organizaciones hacia modelos data-driven exigió la adopción de estrategias de gobierno de los datos. El despliegue generalizado de tecnologías de inteligencia artificial, con riesgos asociados como el Shadow AI, está haciendo patente la necesidad de controlar y orquestar la IA. La mayor responsabilidad de la alta dirección sobre las decisiones de ciberseguridad y la creciente relevancia de la seguridad de los datos en el éxito corporativo están impulsando el gobierno de la ciberseguridad.

CIBERSEGURIDAD, VALORES CORPORATIVOS Y BUEN GOBIERNO

Miguel Tena, field sales engineer de Object First, considera que "la ciberseguridad debe reflejar la cultura y las prioridades de una organización. No se trata únicamente de implementar herramientas

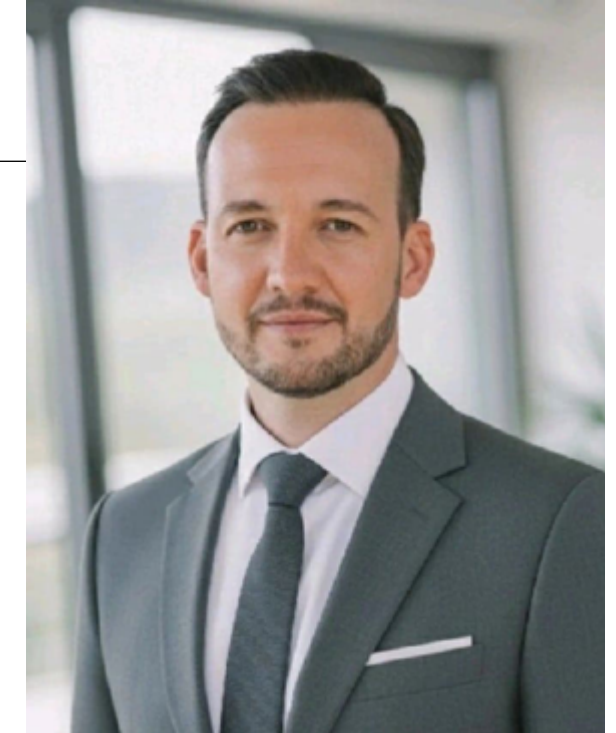
tecnológicas, sino de establecer una forma de trabajar basada en la protección de la información, la responsabilidad y la confianza. Una organización que considera los datos como un activo estratégico debe trasladar esa visión a todas sus áreas: desde la dirección hasta los equipos operativos. Esto implica definir procesos claros, concienciar a los empleados y garantizar que la seguridad está integrada desde el diseño de nuevos proyectos y servicios. También significa asumir que ningún sistema es completamente invulnerable".

Para lograr alinear la estrategia de ciberseguridad y los valores de la organización, Carlos Castro, strategic account manager de WatchGuard Technologies Iberia, explica que "el primer paso es transformar la seguridad en un habilitador del negocio. Cuando una organización entiende que proteger sus datos, sus infraestructuras y sus servicios digitales es un argumento de confianza y un diferencial competitivo, la conversación cambia. La seguridad deja de ser un coste defensivo para convertirse en una palanca comercial y reputacional. También es fundamental vincular la estra-

tegia de seguridad con los principios éticos y la transparencia. Si el valor central de una empresa es la confianza del cliente, la privacidad y la protección de su información sensible deben ser la máxima prioridad. El tercer elemento es fomentar la responsabilidad compartida. Tratar la ciberseguridad como la prevención de riesgos laborales, es decir, la ciberseguridad no un castigo ni una traba burocrática, sino un valor transversal donde cada empleado protege al equipo".

Entender la necesidad de esta alineación entre los valores corporativos, la estrategia de negocio y la ciberseguridad es un primer paso imprescindible para que el modelo de gobierno de la ciberseguridad tenga posibilidades de éxito. El deseado "patrocinio de la alta dirección" es un elemento básico para que los proyectos verdaderamente transformadores puedan calar realmente en la organización.

En cuanto a qué elementos centrales debe tener un modelo de buen gobierno de la ciberseguridad, Sergio Martínez, regional manager de SonicWall para Iberia e Italia, señala que "debe partir de una premisa básica: la seguridad



“ CUANDO UNA ORGANIZACIÓN ES CAPAZ DE TRASLADAR SUS VALORES EN CRITERIOS CONCRETOS DE ACTUACIÓN, RESPONSABILIDADES, CONTROLES Y PROCESOS VERIFICABLES ES CUANDO PASA DE EJECUTAR MEDIDAS A ORQUESTAR LA SEGURIDAD ”

RAFAEL VERGARA, responsable de soluciones de digitalización y tecnología de **AENOR**

« ya no puede entenderse como una responsabilidad exclusiva del departamento de TI. En primer lugar, es necesario identificar los activos críticos y comprender qué riesgos pueden afectar a la continuidad de la actividad. En segundo lugar, deben definirse claramente las responsabilidades y los procesos de decisión, respuesta y recuperación ante un incidente. Y, por supuesto, es imprescindible disponer de visibilidad sobre lo que ocurre en la red, los endpoints, las aplicaciones, los entornos cloud, las identidades y los accesos. También debemos incorporar una cultura de seguridad que implique a toda la plantilla».

MÁS ALLÁ DE LAS NORMATIVAS Y LA INNOVACIÓN

La obligación que imponen las normativas suele ser una buena palanca para impulsar este tipo de estrategias. RGPD lo fue para que conciencia sobre la seguridad y privacidad de los datos permeara a todos los niveles de la organización. Es una normativa que no se puede dejar de lado siguen siendo el centro de la tecnología digital, pero a ella se han sumado muchas otras que afectan a distintos tipos

de entidades, desde la Ley de IA, la de Ciberresiliencia o DORA hasta NIS2 que, quizá, llegará a las legislaciones locales antes de convertirse en NIS3.

Por supuesto, como recuerda Víctor Pérez de Mingo, presales manager para España y Portugal de Veeam, "cumplir con una normativa no equivale automáticamente a estar protegido. La regulación establece un marco y un nivel mínimo de exigencia, pero la resiliencia tiene que formar parte de la operativa diaria de la organización, no activarse únicamente cuando llega una auditoría. El cumplimiento debe ser el punto de partida para construir una estrategia más amplia de resiliencia. Las organizaciones necesitan poder demostrar que conocen sus datos, que tienen controles establecidos y que pueden recuperar sus sistemas y su información cuando se produce un incidente. Demostrarlo implica probarlo validando periódicamente que esos controles funcionan y que la recuperación puede realizarse bajo condiciones reales de presión".

La visión de los expertos, con sus distintas perspectivas, nos habla de una necesidad: el cambio de mentalidad.

Un cambio de mentalidad que empieza con la propia percepción de las cosas. Por ejemplo, el clásico dilema del equilibrio entre innovación y seguridad es rechazado de forma generalizada. Es una dicotomía que no debería existir y, de permanecer todavía en algún contexto, tendría que ser desterrada.

Juanan Alcaraz, CISO de Ontinet.com, distribuidor exclusivo de ESET en España, remarca que "la estrategia de seguridad ha de estar al servicio de la empresa, no al contrario. Dado que la innovación tecnológica es una necesidad de primer nivel para la supervivencia de la empresa a largo plazo, la estrategia de seguridad ha de definirse, no como freno sino como guía para fijar los guardarraíles en la innovación tecnológica. Es asegurar que la innovación tecnológica se desarrolla por un cauce seguro, con un control y gestión del riesgo que se adapte a las necesidades de la empresa. No se limita a permitir o prohibir, es un acompañamiento".

Por su parte, Rafael Vergara, responsable de soluciones de digitalización y tecnología de AENOR, incide en que "innovación y ciberseguridad no deben plantearse como



« **HEMOS IMPLANTADO UN FRAMEWORK DE GOBIERNO, RIESGO Y CUMPLIMIENTO QUE ASEGURA DE FORMA ÁGIL QUE TODAS LAS INICIATIVAS QUE INCORPORAN IA LO HAGAN DE MODO SEGURO Y ALINEADO CON LAS REGULACIONES Y POLÍTICAS DE HPE** »

JORGE LAREDO,
senior security architect de WW
Cybersecurity Services en **HPE**

« conceptos enfrentados. La ciberseguridad debe formar parte de la innovación desde su conceptualización. Actualmente, un claro ejemplo es la adopción de la inteligencia artificial, que está siendo frenética y en la que no considerar aspectos como la seguridad, la calidad del dato, la supervisión humana, la explicabilidad o la monitorización de su comportamiento puede implicar asumir riesgos con consecuencias drásticas. Son tecnologías innovadoras y disruptivas que si no se alinean con las estrategias de seguridad desde su conceptualización

ponen en riesgo modelos completos de negocio".

Otro de los cambios conceptuales es el paso de una postura reactiva a una proactiva. Para ello, Jorge Laredo, senior security architect de WW Cybersecurity Services en HPE, destaca que "lo primero es aceptar algo que puede resultar incómodo y es que no podemos construir una estrategia sobre la idea de que vamos a impedir todos los incidentes. Ser proactivo no significa adivinar siempre el próximo ataque. Significa reducir la exposición y eso pasa por conocer mejor lo que te-

nemos, detectar antes las señales relevantes y estar bien preparados para limitar el impacto cuando un ciberataque consiga superar alguna defensa. Aquí es donde conceptos como Zero Trust, la segmentación o la automatización empiezan a tener sentido de verdad. No como tecnologías que vamos sumando a una lista, sino como herramientas que nos permiten reducir continuamente la superficie de exposición y actuar cuando aparece algo que no encaja. Y la IA nos está dando además una capacidad que antes era mucho más limitada: analizar una



» LA PROTECCIÓN DE LOS DATOS CRÍTICOS Y LA EXISTENCIA DE COPIAS DE SEGURIDAD SEGURAS, AISLADAS E INMUTABLES DEBEN FORMAR PARTE DE CUALQUIER ESTRATEGIA MODERNA DE GOBIERNO DE LA SEGURIDAD «

MIGUEL TENA,
field sales engineer de
Object First



cantidad enorme de señales, relacionarlas y ayudar a identificar antes comportamientos que pueden anticipar un problema. Ser proactivo no significa pensar que vamos a ser capaces de evitarlo todo. Significa asumir que algo puede ocurrir y haber decidido antes qué vamos a hacer cuando ocurra".

DIFERENTES PROPUESTAS PARA EL GOBIERNO DE LA CIBERSEGURIDAD

Hemos querido saber cómo impulsan el buen gobierno de la ciberseguridad todos los expertos que han tenido la amabilidad de participar en este artículo. Más allá del trabajo que realizan con y para terceros, es interesante señalar que todos ellos parten de la propia experiencia de implementación del gobierno de TI y de la ciberseguridad en sus propias organizaciones.

Rafael Vergara, de AENOR, explica que, en su organización, "concretamente desde la gerencia de soluciones de Digitalización y Tecnología, promovemos soluciones que ayuden a impulsar la gobernanza de la ciberseguridad mediante modelos de gestión evaluables y sujetos a una mejora continua. Somos sa-

bedores de que la ciberseguridad se encuentra en constante evolución y es por ello que nuestras certificaciones abogan por una ciberseguridad centrada en la gobernanza y la aplicación de procedimientos y medidas técnicas acordes a riesgos. Accesibilidad TIC, Gobierno del Dato, Ciclo de vida de desarrollo software, incluso certificaciones enfocadas a ciudades como Nómadas Digitales, son ejemplos de la variedad de soluciones que impulsamos desde el área".

Jorge Laredo, de HPE, explica que en su caso "trabajamos precisamente para identificar y resolver brechas en los programas de seguridad, riesgo y cumplimiento, pero también en ayudar a que esas capacidades evolucionen a medida que cambian tanto las amenazas como las exigencias regulatorias. Además, una organización puede tener mucha tecnología de seguridad y no estar preparada para gestionar un incidente grave. Para resolver ese gap, trabajamos también la coordinación entre las personas que tendrán que tomar decisiones cuando algo ocurra. Para ello, tenemos, por ejemplo, talleres específicos de ransomware en los que se

aborda cómo coordinar a los actores clave de la compañía para que la organización pueda prepararse, resistir y recuperarse de un ataque. Y después está, naturalmente, la tecnología. Tenemos capacidades Zero Trust, protección del dato, automatización y herramientas de ciberresiliencia. Pero me parece importante el orden: la tecnología tiene que responder al riesgo y a cómo hemos decidido gobernarlo, no al revés".

Miguel Tena, de Object First, se centra en su contribución "desde una área crítica: la protección y recuperación de los datos. Nuestra visión parte de una realidad: el ransomware ha convertido las copias de seguridad en un objetivo prioritario para los atacantes. Por ello, las organizaciones necesitan una capa de protección que garantice que sus datos permanecen disponibles incluso en escenarios donde las defensas tradicionales han fallado. Ayudamos a las empresas a reforzar su estrategia de ciberresiliencia mediante soluciones de backup y almacenamiento diseñadas para simplificar la protección de datos, incorporar mecanismos de inmutabilidad y facilitar una re-



“ LA CORRECTA ALINEACIÓN DE LA ESTRATEGIA DE LA CIBERSEGURIDAD CON LOS VALORES DE LA ORGANIZACIÓN SE CONSIGUE MEDIANTE EL PLENO CONOCIMIENTO DE LOS PROCESOS Y DE LA CULTURA EMPRESARIAL ”

JUANAN ALCARAZ,
CISO de Ontinet.com, distribuidor exclusivo de **ESET en España**

cuperación rápida ante incidentes".

Juanan Alcaraz, de Ontinet.com y ESET España, considera que, "como empresa dedicada a la ciberseguridad, impulsamos el buen gobierno desde la coherencia: este año hemos alcanzado hitos clave como la certificación en ISO 27001 y el Esquema Nacional de Seguridad en nivel Alto. Sin embargo, el gobierno no es solo conseguir un sello, sino mantener la cultura viva. Por ello, hemos creado un Comité de Seguridad Interno donde dirección y las áreas clave se sientan a la misma mesa para evaluar riesgos, priorizar inversiones y asegurar que la gobernanza sea un proceso dinámico, transparente y alineado con la estrategia del negocio".

Sergio Martínez, de SonicWall, destaca su enfoque centrado "en proteger de forma coordinada redes, endpoints, aplicaciones, entornos cloud, usuarios e identidades, reduciendo la complejidad y facilitando una gestión más coherente del riesgo. Impulsamos arquitecturas de seguridad por capas y modelos Zero Trust, con controles de acceso basados en identidad, contexto y mínimo privilegio. También ponemos el foco en la inteligencia

de amenazas en tiempo real, la monitorización continua y los servicios gestionados, para que las organizaciones puedan identificar y responder a actividades sospechosas con rapidez, incluso cuando no cuentan internamente con todos los recursos especializados que requiere un entorno de amenazas tan dinámico".

Víctor Pérez de Mingo, de Veeam, señala que impulsan "el buen gobierno de la ciberseguridad ayudando a las organizaciones a construir y mantener una base de confianza alrededor de sus datos. Eso implica

poder comprender qué datos tienen y dónde están, quién o qué accede a ellos, protegerlos y gobernarlos durante todo su ciclo de vida y, ante cualquier incidente, garantizar que puedan recuperar información limpia y fiable. Con nuestra evolución hacia una compañía de Data y AI Trust, estamos llevando esa visión un paso más allá, integrando resiliencia, seguridad, gobernanza, privacidad y cumplimiento alrededor del dato".

Carlos Castro, de WatchGuard Technologies Iberia, destaca "una Arquitectura de Plataforma de Se-



“ LA TECNOLOGÍA, LA MONITORIZACIÓN, LA FORMACIÓN Y LOS PROCESOS DEBEN TRABAJAR DE FORMA CONJUNTA, DE MODO QUE EL CUMPLIMIENTO SEA UNA CONSECUENCIA DE UNA BUENA GESTIÓN DEL RIESGO Y NO UN SIMPLE EJERCICIO DOCUMENTAL ”

SERGIO MARTÍNEZ,
regional manager de **SonicWall**
para **Iberia e Italia**

seguridad Unificada: en WatchGuard eliminamos la fragmentación del ecosistema de seguridad integrando red, endpoint, identidad y nube en una única consola denominada WatchGuard Cloud. La protección de primer nivel con soluciones avanzadas, innovadoras y en continuo avance. Protegemos la red, los endpoint y la identidad, pero también avanzamos hacia el XDR, SASE, NDR, CloudDR, MDR. Todo ello

impulsado por la IA de una forma responsable. La democratización de la seguridad avanzada: permitimos que tanto las pymes como las grandes cuentas accedan a modelos de Zero Trust y servicios gestionados (MDR) sin necesidad de gestionar la complejidad técnica interna".

Un amplio espectro de perspectivas que mejoran el gobierno de la ciberseguridad corporativa. Junto a ellas, una serie de mensajes clave

que es imprescindible tener presente. Nos quedamos con tres centrales: la adaptación a las normativas supone un considerable esfuerzo, pero es una gran oportunidad para mejorar realmente la postura de ciberseguridad; los estándares son elementos de gran utilidad, pero no te inmunizan frente a los ciberataques; la seguridad desde el diseño no debería ser una hipótesis de trabajo, sino el trabajo. ■

MÁS INFO +

» [ISO/IEC 27001:2022](#)

» [ISACA COBIT](#)

» [NIST Cybersecurity Framework 2](#)



COMPARTIR EN REDES SOCIALES



“ LAS ORGANIZACIONES NECESITAN EVOLUCIONAR DESDE MODELOS REACTIVOS HACIA ESTRATEGIAS QUE LES PERMITAN CONOCER SUS RIESGOS, PREPARARSE Y VALIDAR QUE REALMENTE PUEDEN RECUPERARSE CUANDO SEA NECESARIO ”

VÍCTOR PÉREZ DE MINGO,
presales manager para España y Portugal de **Veeam**



“ LAS DISTINTAS NORMATIVAS QUE PUEDEN AFECTAR A CADA NEGOCIO, COMO NIS2, DORA O EL ENS, DEBEN ACTUAR COMO UN CATALIZADOR DE PRESUPUESTO Y AYUDAR A OBTENER LA ATENCIÓN EJECUTIVA ADECUADA ”

CARLOS CASTRO,
strategic account manager de **WatchGuard Technologies Iberia**



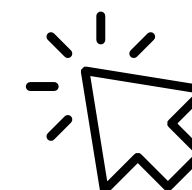
ESCALA LA IA EMPRESARIAL SIN CEDER EL CONTROL DE TUS DATOS

GUÍA PRÁCTICA PARA EL RESPONSABLE DE TI:

Cumplimiento, Control y Competitividad para
desplegar IA privada bajo la normativa europea



DESCARGAR
DOCUMENTO



arsys

itRESEARCH

#REPORTAJE



EL CANAL REDEFINE SU PAPEL EN LA CONTINUIDAD DEL NEGOCIO

» HILDA GÓMEZ



La continuidad operativa se ha convertido en el nuevo estándar, y los partners deben evolucionar desde el soporte reactivo hacia arquitecturas integradas capaces de anticipar, contener y recuperar. ADM Cloud&Services, ESET, Ingram Micro, Kaspersky, Object First, SonicWall, Stormshield, TD SYNnex y Veeam analizan cómo está cambiando la demanda, qué capacidades exige esta nueva etapa y qué oportunidades se abren para el ecosistema del canal.



«

La solidez operativa frente a interrupciones se ha convertido en uno de los grandes vectores de transformación del canal tecnológico. Según estimaciones del sector, más del 78% de las organizaciones europeas ha sufrido al menos una interrupción operativa significativa en los últimos doce meses, y el coste medio de una parada no planificada supera ya los 250.000 euros en empresas de tamaño medio.

A ello se suma un incremento del 37% en incidentes de ransomware durante el último año, con ataques cada vez más rápidos, automatizados y dirigidos a comprometer no

solo los sistemas de producción, sino también las copias de seguridad. En este contexto, la continuidad del negocio ha dejado de ser un concepto aspiracional para convertirse en un requisito estratégico que afecta a todas las capas de la infraestructura digital.

El canal, tradicionalmente centrado en la protección y el soporte reactivo, está viviendo una transición profunda hacia modelos de resiliencia integral. El mercado lo confirma, y los servicios gestionados de ciberseguridad crecen un 17% anual, la inversión en tecnologías de identidad aumenta un 22%, y las soluciones de backup y recuperación avanzadas registran

incrementos superiores al 30% en determinados segmentos.

A la presión del riesgo se suma la presión regulatoria, con normativas como NIS2, DORA o la Cyber Resilience Act que obligan a demostrar capacidad de recuperación, trazabilidad y continuidad, lo que está acelerando proyectos en sectores críticos y empujando al canal a adoptar un rol más consultivo, estratégico y cercano al negocio del cliente.

LA RESILIENCIA COMO NUEVO EJE DEL CANAL

La continuidad digital del negocio se ha convertido en el nuevo lenguaje común del canal tecnológico. No es

una moda ni un concepto aspiracional, sino una necesidad operativa. Las organizaciones ya no se preguntan si sufrirán un incidente, sino cuándo y con qué impacto. Y ese cambio de mentalidad está transformando por completo la relación entre clientes y partners.

Víctor Orive, CEO de ADM Cloud & Services, asegura que “el cliente ya no quiere únicamente estar protegido, sino tener garantías razonables de continuidad”. Para Orive la seguridad ya no se mide por la ausencia de incidentes, sino por la capacidad de recuperarse de ellos. “Una parada de pocas horas puede afectar a la operativa, la facturación, la re-

»

putación o incluso al cumplimiento normativo”, afirma, añadiendo que el canal debe pasar de vender soluciones aisladas a “construir arquitecturas de resiliencia”.

Esa arquitectura ya no es un conjunto de herramientas, sino un ecosistema coordinado que combina backup, recuperación ante desastres, seguridad del dato, monitorización, gestión de identidades, protección endpoint, correo seguro y respuesta ante incidentes.

SonicWall coincide en esta idea. Sergio Martínez, regional manager Iberia & Italy de la compañía, recuerda que “las organizaciones preguntan cuánto tardarán en recuperarse cuan-

do ocurra un ataque”. La pregunta ya no es cómo evitar el incidente, sino cómo minimizar su impacto. La resiliencia se convierte en una conversación de negocio, no de tecnología.

Martín Trullas, Advanced Solutions director de Ingram Micro, apunta que la resiliencia exige una integración profunda entre capas que antes se trataban como compartimentos estancos. Para Trullas, “combinar protección de datos e identidades con capacidades para monitorizar, automatizar y recuperar el ecosistema es vital para que la estrategia sea exitosa”, recalcando así que la resiliencia no es una suma de herramientas, sino una arquitectura coherente.

Esta evolución está impulsando un modelo de colaboración más estrecho entre fabricantes y partners. Así lo cree José Antonio Morcillo, director de Canal de Kaspersky Iberia, que explica que “la resiliencia está transformando el papel del canal, que deja de ser un proveedor tecnológico para convertirse en un asesor estratégico”. El partner debe así acompañar al cliente en todo el ciclo, desde la prevención hasta la recuperación.

EL MSP Y LA CONTINUIDAD OPERATIVA

En relación a esto, la evolución del proveedor de servicios gestionados

(MSP) hacia modelos de continuidad está redefiniendo su propuesta de valor. Ya no basta con supervisar backups o gestionar alertas, sino que ahora deben orquestrar la resiliencia completa del cliente, desde la detección hasta la recuperación.

Según David Sánchez, director de Canal de Ontinet.com, distribuidor exclusivo de ESET para España y Andorra, “las empresas necesitan estar preparadas para detectar, contener, responder y recuperar su actividad con el menor impacto posible. La protección es solo el primer paso; la resiliencia exige vigilancia, detección y recuperación”.



“ EL CLIENTE YA NO QUIERE ÚNICAMENTE ESTAR PROTEGIDO, SINO TENER GARANTÍAS RAZONABLES DE CONTINUIDAD ”

VÍCTOR ORIVE
CEO de **ADM Cloud & Services**



“ LA CIBERSEGURIDAD YA NO PUEDE CENTRARSE ÚNICAMENTE EN EVITAR UN INCIDENTE ”

DAVID SÁNCHEZ,
director de Canal de
Ontinet.com

Sánchez añade que “el crecimiento de los servicios gestionados demuestra que muchas empresas necesitan externalizar parte de la complejidad de la ciberseguridad”, y que el MSP debe ofrecer “supervisión continua del riesgo y capacidad de respuesta”. La resiliencia se convierte en un servicio vivo, no en un proyecto puntual.

Por su parte, Miguel Tena, field sales engineer de Object First, recuerda que protección y resiliencia no son exactamente lo mismo. “Podemos tener una copia de seguridad y descubrir, en el peor momento po-

sible, que también ha sido comprometida por el atacante”, afirma. Por eso tecnologías como el almacenamiento inmutable, la segmentación de la infraestructura de backup y el principio de mínimo privilegio están ganando protagonismo. Tena insiste en que “el MSP tiene que gestionar de forma continua la capacidad de recuperación del cliente”.

Santiago Pérez, Channel director en Veeam Iberia, coincide en esta visión, al asegurar que “el verdadero valor está en ser capaces de garantizar que esos datos son recuperables”, y que la resiliencia “no se puede dar

por sentada; hay que comprobarla y gestionarla de forma continua”.

Orive, de ADM Cloud & Services añade que “la resiliencia no se resuelve con una venta puntual, sino con servicios gestionados de largo recorrido”, y que “el MSP pasa de vender tecnología a vender continuidad”.

Desde SonicWall, Sergio Martínez refuerza esta idea señalando que “los MSP tienen una posición privilegiada para liderar esta evolución porque combinan tecnología, conocimiento operativo y capacidad de monitorización continua”. La resiliencia se convierte así en un servicio estratégico.

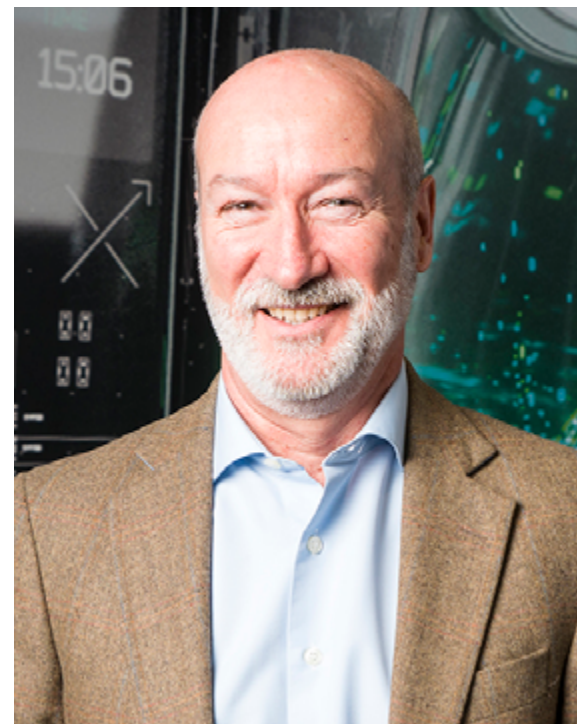
IDENTIDAD, DATO Y AMENAZAS IMPULSADAS POR IA

La identidad y el dato se han convertido en los nuevos vectores de ataque. La IA está acelerando la velocidad y la sofisticación de las amenazas, y el canal debe adaptarse a este escenario dinámico. No en vano, según datos de Kaspersky, el número de vulnerabilidades en servicios de IA y modelos de lenguaje se multiplicó por diez en seis meses. Este crecimiento refleja un riesgo emergente, que son los agentes de IA, los cuales pueden convertirse en nuevos puntos de entrada para los atacantes.



“ LA CONTINUIDAD OPERATIVA SE HA CONVERTIDO EN EL CRITERIO REAL PARA MEDIR LA MADUREZ DE CUALQUIER PARTNER ”

MARTÍN TRULLAS,
Advanced Solutions director de
Ingram Micro



“ LA RESILIENCIA REQUIERE CONOCER EL ESTADO DE LA INFRAESTRUCTURA EN TODO MOMENTO ”

JOSÉ ANTONIO MORCILLO,
director de Canal de Kaspersky
Iberia

Como reconoce Santiago Pérez, de Veeam, “las empresas están empezando a incorporar agentes de IA capaces de acceder a información y ejecutar acciones autónomas”, lo que introduce nuevos escenarios de riesgo. La resiliencia debe incluir gobernanza del dato y protección de identidades de máquina.

« ESET recuerda que la identidad deja de ser un componente técnico y se convierte en un pilar de continuidad. “La transición hacia Zero Trust y gobernanza del dato es una oportunidad de negocio muy importante”, afirma David Sánchez.

Miguel Tena, de Object First añade que “la arquitectura resiliente debe combinar controles preventivos de identidad con una última capa de recuperación que no dependa de credenciales administrativas”.

Para Sergio Martínez, de SonicWall, “la velocidad del atacante ha aumentado y la resiliencia depende cada vez más de nuestra capacidad para responder en tiempo real”. La IA defensiva, con detección de anomalías, correlación de señales, automatización de respuesta, se vuelve imprescindible.

Son embargo, Borja Pérez, country manager de Stormshield Iberia,

advierte que la IA no es el único desafío, y que la computación cuántica está en el horizonte. “Cualquier proyecto actual debe anticiparse e incorporar algoritmos criptográficos post-cuánticos”, sostiene Pérez. La resiliencia debe así mirar al futuro.

REGULACIÓN Y SECTORES CRÍTICOS

La regulación está acelerando la adopción de modelos de resiliencia. NIS2, DORA, ENS, GDPR y la Cyber Resilience Act están obligando a las organizaciones a demostrar continuidad, trazabilidad y capacidad de recuperación. La resiliencia deja de

ser una recomendación técnica para ser un requisito estratégico, pasando así a formar parte de la agenda de dirección, auditoría y cumplimiento. Sectores como financiero, energía, sanidad, infraestructuras críticas y administración pública lideran esta transición.

“La resiliencia del dato se convierte en una obligación auditable”, asegura Carlos Serra, technical practices manager en TD SYNnex España. “El reto para el canal es doble: por un lado, entender el lenguaje regulatorio para traducirlo en requisitos técnicos concretos; por otro, ayudar a que estas exigencias, pensadas inicialmente



“ PROTECCIÓN Y RESILIENCIA NO SON EXACTAMENTE LO MISMO ”

MIGUEL TENA,
field sales engineer de
Object First



“ LA RESILIENCIA YA NO ES UNA CAPA ADICIONAL DE SEGURIDAD, SINO EL RESULTADO DE UNA ESTRATEGIA UNIFICADA ”

SERGIO MARTÍNEZ,
regional manager Iberia & Italy
de **SonicWall**

para grandes organizaciones sean también accesibles para administraciones locales y empresas medianas con recursos más limitados”.

Borja Pérez, de Stormshield, destaca que la regulación “actúa como un facilitador para acelerar estos proyectos”, y que sectores como banca, sanidad e infraestructuras críticas están liderando la transición.

Por su parte, Santiago Pérez, de Veeam, añade que “la regulación está elevando la conversación a los niveles de dirección”. La resiliencia deja de ser un tema técnico y se convierte en una cuestión de gestión del riesgo.

EL PAPEL DEL MAYORISTA Y LA EVOLUCIÓN DEL CANAL

La transición hacia arquitecturas resilientes está transformando el catálogo del mayorista. Ya no se trata de vender productos aislados, sino de construir ecosistemas completos que cubran todo el ciclo, desde prevención a protección, detección, respuesta, recuperación y cumplimiento. La resiliencia exige una visión holística.

Borja Pérez, Stormshield insiste en que “la tendencia actual exige dejar atrás las herramientas aisladas para avanzar hacia la integración de soluciones”.

Ingram Micro, TD SYNnex y otros mayoristas están ampliando sus portafolios con soluciones de backup, disaster recovery, seguridad gestionada, IAM, protección del dato, seguridad cloud y documentación. La integración entre soluciones y la facilidad de despliegue se convierten en factores clave.

Sobre este punto, Martín Trullas, de Ingram Micro, recalca que “el mayorista puede ir más allá de la formación y ofrecer certificaciones, laboratorios o conocimiento especializado de la mano de sus partners, creando un conglomerado de servicios orientados a la mejora de

las capacidades del cliente, y donde el objetivo no es decirle dónde guardar sus copias de seguridad y cómo custodiarlas, sino analizar cuánto tiempo podrá aguantar en caso de ataque antes de que sea viable recuperar la continuidad del negocio”.

Carlos Serra, de TD SYNnex, recuerda que “más allá de la certificación técnica, nuestro papel incluye ayudar a los partners a rediseñar su discurso comercial: pasar de hablar de ‘copias de seguridad’ a hablar de ‘continuidad de negocio’ exige un cambio de conversación con el cliente, que debe entender el coste real de una interrupción y valorar la resi-



“ LA VERDADERA RESILIENCIA DEBE SER CONFIABLE Y SOBERANA ”

BORJA PÉREZ,
country manager de
Stormshield Iberia



“ LA RESILIENCIA OBLIGA AL CANAL A PENSAR EN SERVICIOS, NO EN PROYECTOS ”

CARLOS SERRA,
technical practices manager en
TD SYNnex España

liencia como inversión estratégica y no como gasto de infraestructura”.

Santiago Pérez, de Veeam, añade que “el partner tiene que entender el negocio del cliente y no limitarse a conocer su infraestructura tecnológica”.

Por último, Víctor Orive, de ADM Cloud & Services, refuerza esta idea, afirmando que “el mayorista debe actuar como facilitador: ayudar a reducir la complejidad, acelerar la puesta en marcha y mejorar la rentabilidad del servicio”. ■

MÁS INFO



» [La inversión en servicios tecnológicos alcanza máximos históricos en España](#)



COMPARTIR EN REDES SOCIALES



“ EL VERDADERO VALOR ESTÁ EN SER CAPACES DE GARANTIZAR QUE ESOS DATOS SON RECUPERABLES ”

SANTIAGO PÉREZ,
Channel director en
Veeam Iberia

EL PAPEL DE LA SOBERANÍA DEL DATO EN LA NUEVA RESILIENCIA



Aunque la resiliencia del dato se ha consolidado como eje central de la continuidad operativa, existe un aspecto que apenas se menciona en las conversaciones técnicas del canal y que, sin embargo, está ganando peso en sectores regulados: la soberanía del dato. No se trata solo de proteger la información, sino de garantizar que permanece bajo control del cliente incluso cuando se aloja en infraestructuras globales o distribuidas.

Stormshield es una de las compañías que más claramente está elevando este debate. Borja Pérez recuerda que “la verdadera resiliencia debe ser confiable y soberana”, especialmente en organizaciones que gestionan información crítica o sensible. La soberanía, explica, no es un concepto político, sino operativo, ya que implica que las claves de cifrado, los mecanismos de acceso y la capacidad de

recuperación no dependan de terceros.

Object First aporta una perspectiva complementaria desde el mundo del backup. Miguel Tena insiste en que “la arquitectura resiliente debe contemplar qué ocurre cuando una identidad legítima o unas credenciales de administrador terminan comprometidas”. Su propuesta se basa en el principio de que, incluso con credenciales privilegiadas, el atacante no debe poder destruir las copias de seguridad.

Desde Kaspersky, José Antonio Morcillo añade que “la protección ya no puede centrarse únicamente en el dispositivo o el perímetro, sino en quién accede a la información, desde dónde y con qué permisos”. La soberanía del dato, por tanto, no es solo una cuestión de cifrado, es una cuestión de identidad, gobernanza y control.

El mercado de la ciberseguridad en España se encuentra en un punto de inflexión marcado por la rápida irrupción de la inteligencia artificial, la sofisticación de las amenazas y la necesidad de proteger identidades y entornos remotos. Analizamos la evolución que se está produciendo en el mercado, el comportamiento de los presupuestos destinados a seguridad y los retos del canal de distribución en su transición hacia el modelo de prestación de servicios gestionados de seguridad (MSSP).

EVOLUCIÓN DE LAS CIBERAMENAZAS Y CLAVES PARA LA PROTECCIÓN DE LAS ORGANIZACIONES



DEBATE IT >> Analizamos cómo está evolucionando el panorama de las ciberamenazas en la segunda mitad de 2026, y cómo los proveedores y el canal se están adaptando para garantizar la protección de las organizaciones, con la colaboración de expertos de ADM Cloud & Services, Samsung, SonicWall, Stormshield y V-Valley.

« El panorama de la ciberseguridad afronta una profunda transformación impulsada por la inteligencia artificial, la sofisticación de los ataques y la desaparición del perímetro tradicional. Pese a un comportamiento tímido a comienzos de año, la ciberseguridad mantiene un crecimiento a doble dígito apoyado en la concienciación de los directivos, la presión regulatoria y la necesidad urgente de proteger las identidades, los datos y los dispositivos. Analizamos estas tendencias de mercado y la evolución que está viviendo el canal los servicios gestionados junto a Víctor Orive, CEO de ADM Cloud & Services; Enrique Martín, head of Large Enterprise de Samsung Iberia; Sergio Martínez, regional manager Iberia e Italia de SonicWall; Juan Manuel Granda, key account manager para Defensa y Seguridad de Stormshield Iberia; y David Gasca, director de Marketing y Operaciones de Ciberseguridad de V-Valley.

RADIOGRAFÍA DEL SECTOR

Tras un inicio de año contenido, el mercado de ciberseguridad ha demostrado que continúa ganando tracción y, según Context, el canal europeo creció cerca del 10% en in-



gresos en el segundo trimestre, y las perspectivas son positivas de cara a la segunda mitad de 2026.

David Gasca, de V-Valley, destaca la inercia positiva del mercado impulsada por la adopción tecnológica y el repunte de proyectos. En su opinión, “la IA lo está acelerando todo”, y añade que la visibilidad de las brechas de seguridad que se están detectando está reactivando el gasto de las empresas, porque “no hay capacidad de inversión hasta que no pasa algo cerca”.

Desde Stormshield Iberia, Juan Manuel Granda coincide en este plan-

teamiento, porque las organizaciones vinculan cada vez más la ciberseguridad a la continuidad de negocio. En su opinión “está habiendo un cambio de percepción en los clientes sobre la importancia de la ciberseguridad, ligado al impacto de negocio que realmente puede tener”. Asimismo, anticipa un último trimestre muy fuerte en España, que podría elevar la previsión de crecimiento hacia el 14%.

Por su parte, Sergio Martínez, de SonicWall, confirma el buen comportamiento del primer semestre y el empuje que se ha visto tras el verano. A pesar de ello, basándose



» en su último informe sobre ciberseguridad, afirma que “no hay cosas nuevas, lo que pasa es que nadie hace los deberes”, y añade que los problemas persisten en la gestión de identidades y la vulnerabilidad del acceso remoto SSL VPN.

Aportando una visión centrada en la seguridad del dispositivo, Enrique Martín, de Samsung Iberia, pone el foco en la creciente preocupación por proteger las flotas de dispositivos móviles. “Lo que sí estamos viendo es que antes la parte de movilidad no preocupaba y cada vez preocupa más”, apunta, señalando que la aparición de ciberataques con suplantación de voz por IA está impulsando la demanda de más control.

Finalmente, Víctor Orive, de ADM Cloud & Services, también confirma crecimientos a doble dígito, explicando que las nuevas superficies de ataque que abre la IA y la regulación

El ransomware ya no espera. ¿Y tu recuperación?

Los atacantes de 2026 ya no cifran y esperan: primero borran tus copias de seguridad. Cove DRaaS pone tu recuperación fuera de su alcance y te devuelve la operatividad en menos de 15 minutos.

Descubre cómo funciona





“ MUCHOS QUIEREN SER MSP, PERO POCOS SABEN HACERLO; DAR EL SALTO NO ES FÁCIL ”

VÍCTOR ORIVE,
CEO de **ADM Cloud & Services**

la administración pública muestra una inversión más contenida tras gastar los presupuestos anteriores, sectores como Defensa, Industria y las pymes están actuando como motores del mercado.

En cuanto al sector público, David Gasca (V-Valley), aclara que las entidades gubernamentales no dejan de ejecutar, sino que son conservadoras al migrar al cloud. Y advierte que “la IA es ahora mismo el eslabón más débil de la cadena, tiene acceso a nuestros dispositivos y datos”, facilitando el acceso sin la debida supervisión de TI.

Para Juan Manuel Granda (Stormshield) la administración opera de forma contraria al sector privado, concentrando sus inversiones en ci-



“ EL NEGOCIO FÁCIL ESTÁ EN LA GRAN CUENTA, PERO EL VOLUMEN Y LA OPORTUNIDAD ESTÁN EN LA PYME ”

ENRIQUE MARTÍN,
head of Large Enterprise de **Samsung Iberia**

infraestructuras para ponerse al día. A esto, añade, “sectores que están 'on fire' son Defensa e Industria, y las pymes están tirando bastante haciendo los deberes”, con previsiones de que la implantación de NIS2 estimulará aún más la demanda.

Sobre el marco regulatorio, Enrique Martín (Samsung) aconsejó a las corporaciones anticipar sus presupuestos para dar cumplimiento a las exigencias legales. “Yo me prepararía asumiendo que esto va a ocurrir y empezaría a pensar en los presupuestos del año que viene para adaptarse a esta nueva regulación”, comenta, previniendo sobre los riesgos de actuar a última hora.



impulsan la demanda. En su opinión, “las normativas ahora no solamente afectan a TI, sino que afectan al nivel directivo, a los directores generales”.

VARIACIONES POR SECTORES

El análisis por sectores que aportan los expertos refleja ritmos desiguales en la apuesta de las organizaciones por la ciberseguridad. Mientras



berseguridad al final del año. Afirma que “en España el último trimestre supone alrededor de un tercio del negocio anual de los fabricantes”, aunque destaca el auge de Defensa y de los entornos industriales OT/IoT, donde ya hay proyectos millonarios.

En esta misma línea, Sergio Martínez (SonicWall) enfatiza la fuerza del segmento pyme, que está renovando



“ HAY QUE PONER MUCHO FOCO EN MODERNIZAR EL ACCESO REMOTO, SOBRE TODO EN LAS PYMES ”

SERGIO MARTÍNEZ,
regional manager Iberia e Italia de **SonicWall**



“ LA SEGURIDAD DE LAS IDENTIDADES, HUMANAS Y NO HUMANAS, ES UNA ASIGNATURA PENDIENTE ”

JUAN MANUEL GRANDA,
key account manager para Defensa y Seguridad de **Stormshield Iberia**



Clica en la imagen para ver la galería

IMPULSORES DEL MERCADO

En el ámbito de la ciberseguridad, la gestión de identidades y accesos (IAM) está creciendo por encima del 20%, liderando la demanda junto a la observabilidad y la seguridad del dato. Ante la madurez de soluciones tradicionales, existe la duda de si el canal está asumiendo con la necesaria agilidad el concepto de ciberresiliencia y la importancia de los SOC.

Según Sergio Martínez, de SonicWall, el canal evoluciona hacia la gestión proactiva mediante SOC e IA, y señala la urgencia de actualizar los activos existentes, porque “la mayor parte de los ataques se

Por último, Víctor Orive (ADM Cloud & Services) señala que la IA ha democratizado los ataques, convirtiendo a las pymes en un blanco directo. Y alerta sobre que “la inteligencia artificial ha democratizado el ataque; antes las pymes no eran conscientes, pero ahora cualquiera puede ser objeto de ataque”.



Clica en la imagen para ver la galería

producen un viernes a las 4 de la madrugada para explotar esas 48 horas críticas”, y para combatir esto recomienda migrar a EDR y desplegar capacidades de detección temprana.

Por su parte, David Gasca, de V-Valley, sitúa la observabilidad como la tecnología estrella para los despliegues corporativos durante lo

que resta de año. “Es lo que nosotros estamos percibiendo más”, explica, a lo que añade que el almacenamiento en data lakes y la orquestación SOAR ya están llegando a la mediana empresa.

Desde Stormshield Iberia, Juan Manuel Granda defiende que la identidad es hoy el objetivo prioritario de los ciberdelincuentes, afirmando que “la seguridad de las identidades, humanas y no humanas, es una asignatura pendiente”. Por ello, opina que la identidad debe viajar con el usuario en arquitecturas flexibles ligadas a la protección del dato.

En este sentido, Enrique Martín, de Samsung, puntualiza que la identidad no puede desvincularse del estado de seguridad del terminal porque “no es solo quién eres, sino también desde dónde accedes y si el dispositivo está en condiciones”, ya que la autenticación falla si el dispositivo está vulnerado.

VECTORES DE ATAQUE

« España se mantiene entre los países europeos más afectados por ciberataques. La explotación de protocolos tradicionales, las campañas de ingeniería social mejoradas con IA y el robo de credenciales están concentrando el riesgo, por lo que los expertos ponen el foco en las vulnerabilidades recurrentes y en la necesidad de aplicar una IA defensiva.

Sergio Martínez (SonicWall) alerta sobre el riesgo crítico de las conexiones remotas tradicionales porque “el protocolo SSL VPN es un protocolo vulnerable; más de la mitad de las brechas se producen por culpa de esa vulnerabilidad”. Y detalla patrones donde el robo de credenciales deriva en cifrado, para lo que defiende el uso de IA agéntica local en los dispositivos.

Desde su punto de vista, Víctor Orive (Cloud & Services), percibe que el



factor humano sigue siendo un vector muy explotado, y explica que “son los mismos empleados los que buscan la alternativa de poder seguir accediendo, saltándose las reglas”, mientras la IA permite crear engaños hiperrealistas que se le escapan al usuario.

Frente a estas amenazas, Juan Manuel Granda (Stormshield) apuesta por aplicar principios de Zero Trust de forma integral. “No nos creemos nada de nadie ni de nada; todo tiene que ser verificado en todo momento, viajando con el dato y con la identidad”, y por ello aboga por esquemas donde la encriptación asegure la información de punta a punta.

“ LA IA ES AHORA MISMO EL ESLABÓN MÁS DÉBIL DE LA CADENA ”

DAVID GASCA,
director de Marketing y
Operaciones de Ciberseguridad
de **V-Valley**



Coincidiendo con sus homólogos Enrique Martín (Samsung), resalta la conveniencia de adoptar la IA de forma segura para potenciar la productividad, ya que opina que “tienes que poder utilizar la inteligencia artificial para hacer cosas porque aumenta la productividad, no puedes bloquear todo”, un contexto en el que apuesta por el procesamiento local en dispositivos con NPU.

HACIA EL MODELO DE MSSP

Los servicios gestionados crecen a un ritmo superior al 40% en España y se están consolidando como la vía de futuro para el canal. Sin embargo, pasar de la venta transaccional a la suscripción recurrente acarrea desafíos operativos y de capacitación que no se están resolviendo a la velocidad esperada.

En este sentido, Víctor Orive, de ADM Cloud & Services, pone de relieve las barreras que frenan a los distribuidores tradicionales, observando que “muchos quieren ser MSP, pero pocos saben hacerlo; dar el salto no es fácil y requiere estandarizar la propuesta”. Además, critica la falta de herramientas en algunos fabricantes para integrar aprovisionamiento y facturación.

David Gasca explica cómo V-Valley facilita la transición mediante soluciones flexibles de marca blanca, comentando que “habilitamos al partner más pequeño, o que no quiere invertir, para ofrecer servicios de manera mensual y flexible”, lo que les permite comercializar servicios para pymes sin asumir riesgos de infraestructura.

Asimismo, Sergio Martínez, de SonicWall, alerta sobre la obsolescencia del parque instalado de cortafuegos en Europa, diciendo que “el tiempo me-

dio de parchear cualquier dispositivo de red en general es alto y, en el caso de los firewalls, es de más de 180 días”, lo que en su opinión demuestra que tiene sentido su estrategia de ofrecer servicios de SOC y parcheo gestionado al canal.

Por su parte, Enrique Martín, de Samsung, incide en que atender a las pymes requiere industrializar los procesos de servicio con políticas estandarizadas. Comenta que “el negocio fácil está en la gran cuenta, pero el volumen y la oportunidad real está en la pyme”.

En último lugar, Juan Manuel Granda, de Stormshield, asegura que la migración hacia el servicio exige planificación estratégica de largo recorrido. “Es una transición que exige una visión estratégica”, señala, “tienes que invertir ahora para obtener un retorno que no es inmediato”, por lo que recomienda comprometerse con acompañar a los distribuidores en su necesaria capacitación.

PROPUESTAS PARA FINAL DE AÑO

Ante el panorama actual de ciberamenazas y teniendo en cuenta las previsiones de inversión empresarial para el resto de 2026, los portavoces de estas empresas resumen su propuesta en materia de ciberseguridad para



Clica en la imagen para ver la galería

los próximos meses. Comienza Víctor Orive, de ADM Cloud & Services, anunciando la incorporación a su catálogo de tecnologías para la protección de aplicaciones, API y mitigación de bots maliciosos, mencionando acuerdos estratégicos para estructurar paquetes atractivos para el MSP.

En el ámbito de la movilidad, Enrique Martín, de Samsung, destaca la inclusión de protección criptográfica

avanzada en sus terminales de corte empresarial, y asegura que “en los últimos modelos hemos incorporado el cifrado postcuántico, pensando en que el dispositivo estará seguro durante años”, y que también han profundizado en la integración de la telemetría móvil con los SIEM y SOC.

Desde SonicWall, Sergio Martínez repasa sus novedades pensadas para acabar con las vulnerabilidades del acceso y, en este campo, comenta, “presentamos Cloud Secure Edge para sustituir la tecnología SSL VPN por acceso remoto ZTNA verdaderamente seguro”, y también su nuevo Endpoint integrado y ligero para blindar los puestos de trabajo.

En el caso de Stormshield, Juan Manuel Granda detalla los pilares de su hoja de ruta tecnológica, destacando que “Stormshield Encryption Platform permitirá al cliente mantener el control total sobre las claves de cifrado de sus datos en la nube”, y también adelanta el futuro lanzamiento de soluciones de comunicación mallada simplificada con cifrado postcuántico.

Finalmente, David Gasca aporta más detalles sobre las iniciativas de V-Valley para estrechar lazos con el ecosistema de socios de cara a final de año, y comenta que “lanzamos el R-Evolve AI Tour para acercarnos a los partners en distintas ciudades y reforzamos nuestro equipo con hasta casi 90 especialistas”, además de destacar su presencia en citas clave del sector como ENISE y Madrid Tech Show. ■

MÁS INFO +

» [Evolución de las ciberamenazas y claves para la protección de las organizaciones](#)



COMPARTIR EN REDES SOCIALES

SAMSUNG



Diseñado para proteger su negocio

Galaxy Z Fold8 for business

Samsung Knox



Víctor Orive, CEO de ADM Cloud & Services

“HAY QUE BASARSE EN PROTEGER LAS IDENTIDADES, EL DATO Y EL SERVICIO”

« El panorama actual de las ciberamenazas está experimentando una profunda transformación empujada principalmente por el desarrollo acelerado de la inteligencia artificial. Como comenta Víctor Orive, esta tecnología está abriendo constantemente nuevas superficies y vectores de ataque dentro de las organizaciones. A pesar de que muchas empresas sostienen la falsa creencia de que tienen todo su perímetro protegido y su círculo de seguridad totalmente cerrado, la realidad diaria demuestra que continuamente están surgiendo nuevas vulnerabilidades que ponen en riesgo la continuidad del negocio y la integridad de los datos corporativos.

Para hacer frente con éxito a esta compleja situación, Orive opina que la estrategia de protección de las organizaciones debe fundamentarse



en tres pilares: la salvaguarda de las identidades digitales de los usuarios, la protección exhaustiva y continua del dato corporativo y el despliegue de herramientas especializadas suministradas bajo el modelo as-a-Service. Estas soluciones deben garantizar una resiliencia adecuada y estructurada, permitiendo

a las empresas ejecutar una recuperación rápida, ágil y eficiente ante cualquier tipo de ciberataque, incidente de seguridad o desastre operativo que ponga en peligro sus operaciones.

Ante esto, señala Víctor Orive, “en ADM Cloud & Services estamos ampliando activamente nuestro

catálogo de soluciones avanzadas de ciberseguridad. Entre las incorporaciones más destacadas figura la integración de tecnologías especializadas en la mitigación y control del tráfico de bots a través de nuestra alianza con Black Wall, abordando un vector de riesgo crítico en la red. Asimismo, estamos cerrando el círculo de protección de aplicaciones clave mediante la incorporación de las soluciones avanzadas de Barracuda, fortaleciendo la defensa de los entornos corporativos”. Su estrategia, explica, está concebida con la meta de ponérselo fácil al proveedor de servicios gestionados (MSP), que es su cliente prioritario. Para ello, empaquetan y estructuran estas herramientas en soluciones listas para ser revendidas de forma sencilla, ágil y rentable por el canal de distribución.



Enrique Martín, head of Large Enterprise de Samsung Iberia

“DAMOS HERRAMIENTAS DE HARDWARE PARA GARANTIZAR LA SEGURIDAD A NUESTROS PARTNERS”

« El entorno de la ciberseguridad empresarial se enfrenta actualmente a tres dinámicas fundamentales que condicionan la estrategia de protección. En primer lugar, según Enrique Martín, “asistimos a una aceleración sin precedentes de las ciberamenazas impulsada por la inteligencia artificial. Los ataques no solo se propagan a una velocidad mucho mayor, sino que resultan cada vez más sofisticados, novedosos y técnicamente elaborados”. En segundo lugar, destaca la gestión de la identidad como un factor crítico para certificar la autenticidad del usuario. En este contexto, opina que el dispositivo endpoint desde el que se accede a los sistemas corporativos está adquiriendo un rol estratégico como elemento clave de verificación y puerta de entrada a la red empresarial. Por último,



ante la creciente complejidad de este ecosistema, señala que las organizaciones se encuentran en el momento idóneo para delegar la gestión operativa de su seguridad en proveedores especializados de servicios gestionados (MSSP).

Frente a esta coyuntura, la propuesta de valor de Samsung

Iberia aborda la seguridad desde la propia arquitectura del hardware, garantizando que el dispositivo sea seguro por diseño. Sobre esta base física, explica, “facilitamos una completa suite de servicios para que nuestros partners del canal de distribución puedan implementar y operar la seguridad de manera

» óptima en las empresas. Un claro ejemplo de este compromiso preventivo es la incorporación del cifrado postcuántico en nuestros dispositivos móviles más avanzados, como la serie S26, preparando a las organizaciones desde hoy para responder a los desafíos criptográficos del futuro”.

En el ámbito de los servicios, señala, “continuamos evolucionando nuestras soluciones para asegurar el pleno cumplimiento normativo de las flotas corporativas”. Esto abarca el control del inventario de equipos, la actualización constante del software y la telemetría en tiempo real, proporcionando las herramientas necesarias para asegurar el endpoint, además de capacitar al canal para gestionar eficazmente la ciberseguridad empresarial.

David Gasca, director de Marketing y Operaciones de Ciberseguridad de V-Valley

“LA IA ESTÁ ACELERANDO TODO A UN RITMO DEMASIADO RÁPIDO Y EXPONENCIAL”

« La evolución reciente de las ciberamenazas discurre de manera paralela al avance acelerado de la inteligencia artificial. Si bien la IA es una herramienta indispensable para fortalecer las defensas de las empresas, también está siendo explotada masivamente por los ciberdelincuentes. David Gasca explica que los atacantes utilizan la IA para abrir nuevos vectores de agresión, como campañas de phishing automatizadas y ultra sofisticadas que desbordan la capacidad de respuesta de los Centros de Operaciones de Seguridad (SOC) a la hora de orquestar y analizar los datos. Esta velocidad de ataque está generando una presión inédita sobre las infraestructuras de protección tradicionales.

A esta amenaza externa se suma un desafío interno crítico: la proliferación del Shadow IT mediante el uso no



regulado de herramientas de IA por parte de los empleados. Gasca apunta que al subir información sensible a plataformas externas sin el control del departamento de TI, las organizaciones se hallan en una fase temporal de pérdida de control, y opina que esta situación solo comenzará a estabilizarse a

medida que se implemente un marco regulatorio adecuado y las empresas adapten sus políticas de gobernanza digital. Afortunadamente para el sector, comenta, los principales fabricantes del mercado están reaccionando con rapidez para desarrollar soluciones enfocadas en proteger los datos corporativos frente

a estas prácticas.

» David Gasca termina destacando que “en V-Valley trabajamos estrechamente con nuestros aliados tecnológicos habituales para ofrecer soluciones de protección adaptadas a este nuevo escenario, incorporando además marcas especializadas para cubrir nichos específicos de mercado”. La mayoría de los fabricantes del sector están desplegando actualmente herramientas para asegurar la interacción con la IA y proteger la información de las organizaciones. No obstante, anticipa que el mercado experimentará una selección natural en los próximos años, en la que únicamente prevalecerán aquellas propuestas consolidadas que respondan con efectividad a las necesidades reales de las empresas y del canal de distribución tecnológico y sus clientes finales.

STORMSHIELD

« Una amplia propuesta y una seguridad óptima »

PROTECCIÓN DE LOS ENTORNOS SENSIBLES



**LORENZO MARTÍNEZ
RODRÍGUEZ**
experto en ciberseguridad



**LA TRAMPA ESTÁ PUESTA:
QUE COMIENCE EL JUEGO**

JOSÉ MANUEL NAVARRO
experto en Marketing



DE PROPIETARIO A SUSCRIPTOR

FEDERICO CARO,
CIO y experto en
transformación digital



**DE LOS PILOTOS A LOS AGENTES:
LA VERDADERA REVOLUCIÓN DE
LA IA TODAVÍA ESTÁ POR LLEGAR**



**LORENZO MARTÍNEZ
RODRÍGUEZ**
Experto en ciberseguridad



« Lorenzo Martínez Rodríguez es ingeniero en Informática por la Universidad de Deusto. Perito informático forense, actualmente es director de la empresa [Securízame](#). Igualmente, es conferenciante habitual en congresos de Ciberseguridad.

LA TRAMPA ESTÁ PUESTA: QUE COMIENZE EL JUEGO

A lo largo de mi vida profesional he participado en la gestión de cientos de incidentes de organizaciones que han sido atacadas por ransomware.

He conocido empresas literalmente arrasadas por grupos destructivos. También he visto al informático que aseguraba que las copias de seguridad estaban estupendamente implementadas descubrir, cuando ya era demasiado tarde, que no era exactamente así. Después llega el turno del empresario: tomar la difícil decisión de arriesgarse a pagar una importante suma o empezar de cero a reconstruir con la poca información de la que pueda disponer. **Y aquí quiero ser muy claro: mi recomendación siempre ha sido y seguirá siendo no pagar.** Pagar no garantiza recuperar los datos, alimenta el negocio de los indeseables que han provocado el desastre y, además, puede dejar a la empresa exactamente donde estaba si el supuesto

decryptor no funciona o si los atacantes vuelven a aparecer.

Pocas cosas me resultan tan frustrantes como estar delante de una empresa que acaba de quedarse sin sus sistemas, sin sus datos y, en muchos casos, sin saber siquiera exactamente qué ha ocurrido.

En su día, cuando el ransomware ya campaba a sus anchas, nació [Reborn](#), una solución híbrida de copias

de seguridad inmutables que ayuda a las empresas a tener un punto de partida de datos en claro de forma garantizada, sin que el cliente tenga que poner velas a la Virgen a la espera de recibir un decryptor tras haber hecho un acto de fe pagando en bitcoins a Dios sabe quién.

Es decir, que tenga disponible la última copia de seguridad para poder arrancar de ella, ya sea para



COMPARTIR EN REDES SOCIALES

recuperar tal cual o para exportar los datos reinstalando en máquinas nuevas.

Pero no nos conformamos únicamente con proveer un servicio de backup inmutable, sino que lo colmamos de virtudes. Lo monitorizamos, por lo que podemos saber si diariamente nos llegan nuevos datos e incluso implementamos medidas para poder intuir si estos han fallado y avisar al cliente.

Sin embargo, quisimos ser como el seguro de incendio de nuestro domicilio. Aquel que tienes y que pagas, pero que no quieres verte en la necesidad de hacer uso de él, porque algo muy malo habrá sucedido.

Y precisamente nuestra propia experiencia en el análisis forense ante incidentes de este tipo nos enseñó algo. Los pasos que siguen los atacantes son, muchas veces, sorprendentemente parecidos.

Primero consiguen entrar en la organización, ya sea a través de una VPN, de un servicio expuesto mal bastionado o tomando el control del PC de un usuario. Sea como fuere, en algún momento el atacante consigue estar dentro. Sin embargo, no conoce la casa. Así que lo primero que va a hacer es “conocer a los vecinos”.

Si tiene acceso a un servidor o a un PC, empezará a buscar qué hay alrededor. Escaneará uno o más rangos de red y buscará servicios en cada equipo que tenga una dirección IP en dicha red. Quiere saber qué máquinas existen, qué puertos están abiertos y, sobre todo, qué puede haber ahí dentro que le resulte interesante para llevarse.

Hay quien me dirá que duerme tranquilo porque su EDR/XDR detecta todas las variantes de Advanced IP Scanner, Nmap, IPScan, etc. ¡Ilusos!

Hemos visto escáneres de puertos hechos en PowerShell que han evadido con soltura los EDR/XDR. Y es que no siempre puedes detectar al atacante por la herramienta que utiliza. PowerShell es legítimo. Una cuenta de administrador es legítima. Una conexión SMB puede ser perfectamente legítima. El problema es qué está haciendo con todo ello alguien que acaba de entrar en nuestra red.

¿Y si la entrada se produce vía VPN? Solo dependerá de lo robusta

que sea la política de seguridad del firewall, algo que muchas veces y, para algunos perfiles de alta dirección (si no lo es para todos), tiene mucho de política y poco de seguridad, permitiendo el acceso a todo.

A partir de este punto, el atacante identifica los servicios jugosos, las copias de seguridad, los controladores de dominio, explota vulnerabilidades de escalada de privilegios, se hace administrador de dominio, crea nuevos usuarios con su mismo nivel de poderes elevados y/o utiliza cualquier otro



NO PODEMOS EVITAR QUE A UN CLIENTE LE COMPROMETAN UNA VPN O TOMEN EL CONTROL DE UN PC DE USUARIO O UN SERVIDOR. SIN EMBARGO, SÍ PODEMOS PONER EL FOCO EN DETECTAR EL SIGUIENTE PASO QUE LLEVARÁ A CABO EL INVASOR



mecanismo de persistencia, exfiltra o roba información que considera interesante para posteriormente venderla o utilizarla para extorsionar a la víctima y, finalmente, cifra todo lo que encuentra, dejando los sistemas como si Atila hubiera pasado por allí.

Esto lo hemos visto demasiadas veces.

¿QUÉ PODEMOS HACER PARA EVITAR ESTA CATÁSTROFE?

Haciendo lo que se hace cuando se detecta un tumor: extirparlo lo antes posible.

No podemos evitar que a un cliente le comprometan una VPN o tomen

el control de un PC de usuario o un servidor. Sin embargo, sí podemos poner el foco en detectar el siguiente paso que llevará a cabo el invasor: el de “conocer a los vecinos”.

Y aquí es donde sabíamos que podíamos hacer algo diferente. Hace años ya pensamos que, con Reborn, ya que estamos dentro de la red de la empresa, podemos implementar señuelos que emulan diferentes tipos de servicios.

La idea es sencilla: poner dentro de la red un equipo con servicios o recursos con los que nadie debería interactuar. No se trata de intentar adivinar si un comportamiento es

malicioso. No se trata de decidir si una herramienta concreta es sospechosa. Se trata de colocar una puer-
ta que nadie debería abrir y esperar.

Algunas empresas están acostumbradas a tener que mirar decenas de consolas, cada una de su padre y de su madre, de diferentes soluciones de seguridad. Y, por ello, han de lidiar con multitud de falsos positivos. Al final esto resulta inútil porque son tantas las alertas que se les deja de prestar atención.

El enfoque que seguimos con Reborn es diferente.

Dado que NADIE debería tocar a la puerta de un equipo que no se conoce en la red, en cuanto alguien pasa por alguno de los distintos señuelos que ponemos en Reborn, tenemos una anomalía que sí o sí hay que investigar y, en su origen, erradicar.

Hay quien se rehúsa a utilizar una solución de copias de seguridad a prueba de ransomware que no está en el Cuadrante Mágico de Gartner: no les culpo, pero allá ellos.

Con Reborn, ese concepto de cyber decoys que recientemente ha recomendado CISA, la Agencia de Ciberdefensa de América, ya estaría implementado en sus redes.

De hecho, para este tipo de em-

presas, desde hace un par de meses, antes de la publicación de la guía de CISA, lanzamos una solución que llamamos [Decoys](#), que recoge precisamente este concepto.

Toda una suerte de señuelos elegidos quirúrgicamente a partir de lo que hemos visto hacer a los atacantes, según nuestra experiencia en respuesta ante incidentes, implementados en una solución cuyas opciones de notificación inmediata son todas aquellas posibles para intentar sacar de la cama a quien pueda echar a patadas al atacante de forma inmediata.

No solemos ser profetas en nuestra tierra, pero da gusto ver cómo algo que llevamos años haciendo, después de haberlo visto funcionar una y otra vez en incidentes reales, acaba apareciendo también en las recomendaciones de una institución tan valorada y reputada como CISA.

Llevamos años esperando a que el atacante llame a la puerta.

La trampa está puesta. Que comience el juego. ■

MÁS INFO



» [Cyber decoys](#)



DECOYS

EL ATACANTE CREE QUE HA ENCONTRADO UN OBJETIVO
EN REALIDAD ACABA DE REVELAR SU PRESENCIA

Decoys es un sistema de detección temprana de amenazas que utiliza señuelos estratégicamente desplegados en la red para identificar actividad potencialmente maliciosa antes de que alcance sistemas críticos



SEÑUELOS ESTRATÉGICOS
Simulan recursos legítimos en tu red



ALERTAS DE ALTO INTERÉS
Cuando alguien interactúa con ellos, lo sabemos



ADAPTADO A TU ENTORNO
Despliegue por redes y segmentos



NOTIFICACIONES DE ALERTA
Whatsapp, Telegram, email, SMS o llamada

¿QUÉ PUEDE DETECTAR?

ENUMERACIÓN DE RECURSOS

ESCAÑEOS Y RECONOCIMIENTO

ACCESOS INESPERADOS

MOVIMIENTO LATERAL

DISPONIBLE EN:



MÁQUINA VIRTUAL



MÁQUINA FÍSICA

Una interacción con un señuelo es una señal que merece ser investigada

UN SERVICIO DE **SECURIZAME**

¿QUIERES SABER MÁS?

DESCUBRE DECOYS EN:

<https://www.securizame.com/decoys>



Algunos objetivos están ahí a propósito





JOSÉ MANUEL NAVARRO
Experto en marketing

✕ in

« Su vida profesional la ha dedicado principalmente al sector financiero, donde ha desempeñado funciones como técnico de organización de procesos y como directivo de marketing. Y, basándose en su formación en Biología, ha profundizado en las neurociencias aplicadas a la empresa, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas nacionales e internacionales. Ha sido socio fundador de diversas empresas y de la entidad de dinero electrónico con licencia bancaria otorgada por el Banco de España SEFIDE EDE, de la que en la actualidad es director de Estrategia y Marca. Es autor de “El Principito y la Gestión Empresarial” y “The Marketing, stupid”.



COMPARTIR EN REDES SOCIALES

DE PROPIETARIO A SUScriptor

Durante siglos, una de las expresiones más concretas de la libertad económica fue la propiedad privada. Poseer dinero significaba poder decidir cuándo y cómo gastarlo; poseer una vivienda, una tierra, una herramienta o una máquina significaba disponer de ellas, transmitir las, venderlas, modificarlas o legarlas. La posesión de un bien convertía el resultado del trabajo presente en una reserva de la capacidad de decisión futura.

Ahora, la economía digital está alterando progresivamente ese principio. No porque la propiedad haya desaparecido (sigue siendo el fundamento jurídico de una parte sustancial de la economía global), sino porque una creciente proporción del consumo se organiza ya alrededor del acceso temporal en lugar de la adquisición. Música, películas, software, almacenamiento, movilidad, equipamiento e incluso determinados bienes físicos pueden contratarse como servicios recurrentes.

La OCDE identifica precisamente la expansión de estos modelos (pagos periódicos a cambio del acceso continuado) que proporcionan ventajas para las empresas en forma de ingresos recurrentes y menores costes (aparentes) de transacción para los consumidores.

UNA EVOLUCIÓN IMPARABLE

La evolución de “comprar a suscribir” parece tener un carácter comercial, pero tiene otra dimensión económica más profunda. La cuestión clave

»

es, en lugar de cuánto pagamos, qué adquirimos realmente por lo que pagamos. Y, sobre todo, qué grado de control conservamos sobre aquello que financiamos de forma periódica no siendo sus propietarios.

El reciente documento “[Yesterday's controversies for tomorrow's money](#)”

de Romain Baeriswyl, publicado por el Swiss National Bank, ofrece un punto de partida especialmente sugerente. Su tesis no consiste en anunciar una revolución monetaria radical, sino en recordar que las controversias sobre el dinero se repiten a lo largo de la historia bajo nuevas formas. El dinero ha ido constituyéndose sobre mercancías naturales a metales preciosos, billetes, depósitos bancarios y, ahora, tokens digitales; pero siguen abiertas las mismas preguntas acerca de su origen, su naturaleza y el mecanismo que garantiza que una unidad monetaria no pueda gastarse dos veces en un mercado que evoluciona muy rápidamente con dos referentes de emisión, uno centralizado y regulado (dinero fiduciario) y otro descentralizado y complejo de regular (criptomonedas).

Esa evolución resulta importante porque cada transformación del dinero ha modificado también la relación

LA EVOLUCIÓN DE “COMPRAR A SUSCRIBIR” PARECE TENER UN CARÁCTER COMERCIAL, PERO TIENE OTRA DIMENSIÓN ECONÓMICA MÁS PROFUNDA. LA CUESTIÓN CLAVE ES, EN LUGAR DE CUÁNTO PAGAMOS, QUÉ ADQUIRIMOS REALMENTE POR LO QUE PAGAMOS

entre quien posee un activo y quien controla ese activo. El oro era simultáneamente mercancía y reserva de valor. El billete convertible representaba un derecho sobre un activo. El dinero fiduciario rompió la convertibilidad y trasladó el fundamento del sistema hacia la confianza, la legislación y las instituciones financieras.

Baeriswyl contrapone dos grandes concepciones:

► **Para la teoría del bien económico** (recurso limitado y escaso que satisface una necesidad humana y que tiene un valor de mercado por el cual se debe pagar un precio), el dinero es un medio de intercambio que permite al individuo conservar la capacidad de disposición sobre los bienes presentes.

► **Para la teoría del crédito**, el dinero puede entenderse fundamentalmente como una relación de derechos y obligaciones contraídas a lo largo de un tiempo futuro. La diferencia no es

meramente académica. En la primera concepción, mantener dinero significa conservar flexibilidad y capacidad de decisión; en cambio, conceder crédito implica transferir temporalmente el control sobre determinados recursos a otra persona o entidad.

Ese razonamiento proporciona una clave para entender algo que está sucediendo más allá del dinero: la progresiva sustitución de la propiedad por el acceso. La economía industrial construyó buena parte de su prosperidad sobre la adquisición de activos. Una familia compraba una vivienda; una empresa compraba maquinaria; un ciudadano compraba un automóvil, un libro o un programa informático. Una vez pagado, el activo pasaba a formar parte de su patrimonio, con las limitaciones jurídicas correspondientes. El modelo digital tiende a separar el hecho de pagar del concepto de propiedad o de dominio

de lo adquirido. Así, el consumidor paga por utilizar una capacidad que permanece bajo control del proveedor sin llegar a ser nunca un activo propiedad de quien lo adquiere (a diferencia de con el crédito que, tras el aplazamiento del pago y una vez satisfecho en su totalidad, sí se obtiene la plena propiedad).

Quien compra un bien puede decidir qué hacer con él. Quien suscribe un servicio obtiene, por el contrario, un derecho contractual condicionado a la continuidad de la relación con el proveedor. Si deja de pagar, pierde el acceso. Si el proveedor modifica las condiciones, el usuario debe aceptar el cambio o abandonar el servicio. Y si la prestación depende de servidores, software, actualizaciones o autenticación remota, incluso un objeto físicamente adquirido puede contener elementos cuyo funcionamiento queda subordinado a terceros.

PROPIEDAD EN LA ERA DIGITAL

El Parlamento Europeo ha identificado ya este problema. Un reciente estudio sobre la propiedad en la era digital señala que determinados productos digitales y bienes conectados ya no proporcionan necesariamente el conjunto de derechos

tradicionalmente asociado a la propiedad (usar, disfrutar, modificar o revender) y advierte de que, cuando uno de los componentes esenciales del producto es una mera relación contractual, la posición del consumidor puede aproximarse a la de un arrendatario, usuario o suscriptor.

« No significa que toda suscripción sea una forma de dependencia ni que toda propiedad sea económicamente superior. Significa algo más preciso, en el sentido de que la propiedad concentra derechos sobre un activo, mientras que la suscripción concentra derechos de acceso a un servicio. La diferencia adquiere especial relevancia cuando se observa desde la perspectiva de la autonomía económica. Un activo (por ejemplo, una vivienda) puede constituir una reserva de valor y, además, ser transmisible. Una suscripción normalmente no lo es; una cuenta de streaming, una licencia de software o una capacidad de almacenamiento contratada no forman, por regla general, parte equivalente del patrimonio transmisible.

La economía digital, por tanto, no elimina la riqueza, pero sí puede cambiar su localización. Una parte creciente del valor económico se concentra en quienes poseen las

plataformas, las infraestructuras, los datos, los derechos de propiedad intelectual y los algoritmos que proporcionan el acceso.

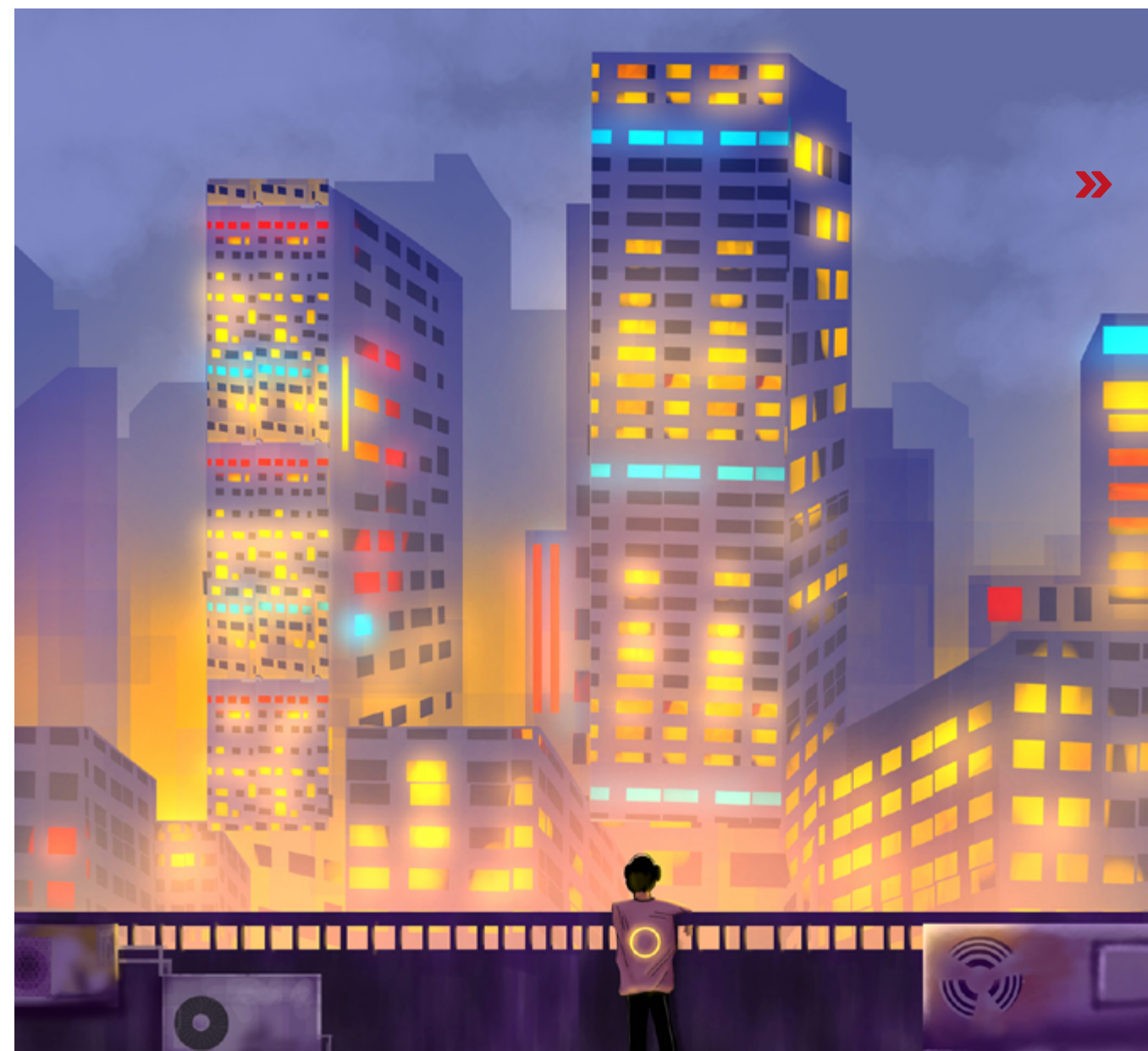
Aquí aparece una conexión interesante con Thorstein Veblen. En *The Theory of the Leisure Class* (1899), Veblen explicó cómo determinados bienes no se consumen únicamente por su utilidad, sino también por su capacidad para expresar posición social. Su concepto de “consumo conspicuo” convirtió el gasto visible en una herramienta de diferenciación social. Durante la etapa industrial, la acumulación visible de bienes podía funcionar como demostración de estatus: automóvil, vivienda, joyas, ropa, obras de arte. En la economía de plataformas, el estatus puede desplazarse desde la posesión hacia el acceso diferenciado a un mismo servicio con diferentes escalas de uso.

La diferencia social puede expresarse mediante niveles de servicio como la tarifa premium, el acceso prioritario, la mayor capacidad de almacenamiento, el vehículo de gama superior disponible bajo demanda o el contenido exclusivo. Es una evolución coherente con Veblen ya que cambia el objeto del consumo conspicuo, no necesariamente su lógica. El signo de

distinción deja de ser exclusivamente “lo que tengo” y puede convertirse en “a lo que tengo acceso”.

Pero hay otra transformación más importante. En el capitalismo patrimonial, el consumidor puede acumular activos. En el capitalismo de plataformas, el proveedor puede acumular relaciones recurrentes

con consumidores. La diferencia es extraordinariamente relevante para la estructura empresarial. La venta tradicional termina con una transacción. La suscripción pretende que la transacción nunca termine. El objetivo económico es convertir una decisión puntual en una corriente futura de ingresos.



Esta transformación coincide con la desaparición progresiva del precio como cifra estática.

PRECIO DINÁMICO

« Eurostat define el [“dynamic pricing”](#) como el uso de algoritmos automáticos para modificar precios rápidamente en función de las condiciones de mercado o de parámetros relacionados con el perfil y la disposición a pagar del consumidor. La tecnología no ha inventado el precio variable (los billetes de avión, los hoteles o los combustibles llevan décadas modificándolo), pero ha reducido radicalmente el coste de cambiarlo y ha multiplicado la información disponible para hacerlo.

Aquí conviene distinguir conceptos que con frecuencia se mezclan. La discriminación de precios de tercer grado consiste en dividir a los consumidores en grupos y aplicar precios diferentes a cada segmento. La discriminación perfecta o de primer grado intenta aproximarse a la disposición máxima a pagar de cada individuo. La literatura económica distingue expresamente ambas modalidades. Los algoritmos permiten acercarse progresivamente a esa frontera porque pueden combinar

variables que antes eran costosas de procesar, como ubicación, hora, demanda, historial de compras, comportamiento de navegación, dispositivo, frecuencia de utilización o respuesta ante precios anteriores.

Esto no significa que todo precio dinámico sea discriminatorio ni que todo algoritmo cobre a cada persona un precio distinto. El precio dinámico puede simplemente responder a cambios en oferta y demanda. La cuestión problemática aparece cuando la capacidad de segmentación permite estimar cuánto está dispuesto a pagar cada consumidor y convertir esa información en una estrategia sistemática de extracción de excedentes de ahorro.

La Comisión Europea ha advertido precisamente de los riesgos derivados de la segmentación y de la fijación personalizada de precios, aunque también reconoce que los efectos dependen de la estructura competitiva y del comportamiento de los consumidores. El resultado puede ser un mercado en el que dos personas reciban servicios aparentemente idénticos, pero afronten condiciones económicas diferentes. La información deja de ser únicamente un instrumento para elegir mejor y se convierte en un

factor de poder negociador.

Entonces, la suscripción y el precio algorítmico forman, en realidad, parte de una misma arquitectura económica. Si una empresa vende un producto, obtiene el ingreso cuando se produce la venta. Si ofrece acceso recurrente, mantiene una relación económica permanente con el cliente. Si además conoce su comportamiento, puede ajustar el servicio, el contenido, la publicidad y eventual-

mente el precio. El activo fundamental deja así de ser únicamente el producto, cuya propiedad mantiene el proveedor, siendo también el cliente, sus datos, su historial y la capacidad de predecir su comportamiento (formando parte de los activos intangibles del proveedor). Esta estructura presenta una asimetría evidente. El consumidor puede disfrutar de más variedad y menor coste inicial, pero la empresa obtiene una relación más

» **QUIEN COMPRA UN BIEN PUEDE DECIDIR QUÉ HACER CON ÉL. QUIEN SUSCRIBE UN SERVICIO OBTIENE, POR EL CONTRARIO, UN DERECHO CONTRACTUAL CONDICIONADO A LA CONTINUIDAD DE LA RELACIÓN CON EL PROVEEDOR**



estable, una fuente de ingresos recurrente y el control de la relación.

Por eso la cuestión relevante desde la perspectiva del capitalismo no debería formularse como una oposición simplista entre «propiedad buena» y «suscripción mala». Lo relevante debería ser qué derechos conserva el consumidor cuando deja de adquirir un activo y pasa a adquirir únicamente acceso. La UE está empezando a abordar precisamente esta frontera. Las normas sobre contenidos y servicios digitales reconocen derechos específicos incluso cuando el consumidor entrega datos personales en lugar de dinero. Y las nuevas reglas sobre reparación pretenden prolongar la vida útil de determinados bienes y reforzar la posición del consumidor frente a la sustitución permanente por productos o servicios nuevos.

El trabajo de Baeriswyl termina recordando que las nuevas formas de dinero (criptomonedas, CBDC y stablecoins) no constituyen una ruptura absoluta con la historia monetaria. Son nuevas manifestaciones de controversias antiguas sobre quién crea el dinero, qué representa y quién controla los activos que lo respaldan. Algo parecido está sucediendo con la propiedad ya que la digitalización

está haciendo posible una economía extraordinariamente eficiente basada en acceso, uso compartido, servicios bajo demanda y pagos recurrentes. Sería un error negar sus ventajas. Pero también sería ingenuo ignorar su contrapartida: cuando el acceso sustituye a la propiedad, parte de la autonomía que proporcionaba el activo se desplaza hacia quien controla la infraestructura que permite utilizarlo.

El consumidor puede sentirse más libre porque ya no necesita comprar un bien. Pero esa libertad es distinta al elegir entre servicios disponibles, no necesariamente libertad de dis-

poner de un activo propio. Y ahí se encuentra la paradoja de la economía de la suscripción. Puede ofrecer más opciones y, al mismo tiempo, aumentar la dependencia respecto de las plataformas que las proporcionan. Puede reducir las barreras de entrada al consumo y, simultáneamente, dificultar la acumulación patrimonial. Puede abaratar el acceso hoy mientras compromete una parte mayor de la renta futura.

La propiedad proporciona la capacidad de decisión, algo que la suscripción no garantiza. Por eso el debate económico del futuro no debería li-

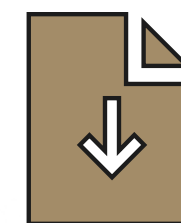
mitarse a cuánto vale un servicio sino ¿quién posee los activos que hacen posible nuestra vida económica y qué derechos conserva quien simplemente paga por utilizarlos?

La historia del dinero demuestra que cambiar el soporte de una relación económica puede cambiar también la naturaleza de esa relación. El paso del oro al dinero fiduciario no fue solamente el cambio de un objeto físico por un signo monetario. Del mismo modo, pasar de comprar a suscribirse no es solamente cambiar una modalidad de pago. Es cambiar, poco a poco, la relación entre pago, propiedad, patrimonio y libertad. Y quizá la verdadera cuestión de la economía que viene no sea si tendremos acceso a más cosas que nunca. Es si, al final del proceso, tendremos todavía suficientes cosas que podamos llamar nuestras y que nos permitan garantizarnos decidir libremente qué hacemos con ellas. ■

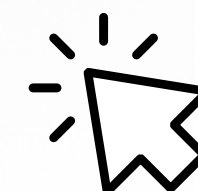
**MÁS INFO**

» [Yesterday's controversies for tomorrow's money. Romain Baeriswyl, Swiss National Bank](#)

**Evolución del mercado TIC-
digital en la primera mitad de
2026. Impacto en España**



Descarga
este informe





FEDERICO CARO
CIO y experto en
transformación digital

in

Federico Caro del Moral es CIO y experto en transformación digital, tecnología e inteligencia artificial. Ingeniero informático por la UPM, cuenta con más de 25 años de experiencia directiva en compañías como Grupo Ruiz, Bankinter, El Corte Inglés, BQ, VASS y Paradigma Digital. Su actividad combina la dirección tecnológica con la divulgación sobre IA y su impacto en las empresas.

DE LOS PILOTOS A LOS AGENTES: LA VERDADERA REVOLUCIÓN DE LA IA TODAVÍA ESTÁ POR LLEGAR

Han pasado casi cuatro años desde el lanzamiento público de ChatGPT el 30 de noviembre de 2022. Tras una primera ola de IA generativa accesible y una segunda centrada en la infraestructura y el hardware —donde NVIDIA se ha consolidado como líder global con

una capitalización cercana a los 5,5 billones de dólares a inicios de septiembre de 2026—, entramos en la tercera etapa: la IA agéntica. Pasamos de sistemas que generan contenido a sistemas capaces de interpretar objetivos, tomar decisiones y ejecutar secuencias de acciones de forma autónoma. Sin

embargo, surge una paradoja: la tecnología avanza exponencialmente, pero las organizaciones avanzan despacio.

LA LEY DE AMARA Y EL PURGATORIO DEL PILOTO

Como señalaba Roy Amara, tendemos a sobreestimar el efecto de



COMPARTIR EN REDES SOCIALES

una tecnología a corto plazo y a subestimar su impacto a largo plazo. Los datos actuales reflejan que la realidad empresarial es menos espectacular que las demostraciones técnicas:

► **Falta de valor tangible:** En 2024, BCG indicó que [el 74% de las empresas no lograba generar valor tangible con sus iniciativas de IA](#); solo el 26% superó la fase de prueba de concepto (PoC).

► **Abandono de proyectos:** Gartner estimó que el [30% de los proyectos de GenAI fueron abandonados después del PoC a finales de 2025](#) por costes, riesgos o mala calidad de datos. Para la IA agéntica, prevé la cancelación de más del 40% de los proyectos antes de finales de 2027.

El verdadero cuello de botella no es tecnológico, sino de transformación empresarial.

DATOS, PROCESOS Y PERSONAS

La integración efectiva de la IA enfrenta tres barreras críticas:

► **El dato:** En 2025, Gartner advirtió que el [63% de las organizaciones carecía de prácticas de gestión de datos adecuadas](#). En 2026, destaca que, sin un contexto semántico, los agentes no pueden comprender las

relaciones y reglas de los datos del negocio.

El proceso: Persiste la tendencia a quedarse en pilotos aislados o co-pilotos que solo ahorran minutos. McKinsey confirmó en 2025 que solo el 39% de las empresas percibía un impacto de la IA sobre el EBIT, vinculando el éxito directamente al rediseño de los flujos de trabajo.

► **Las personas:** La tecnología es solo una fracción del cambio. [BCG defiende la regla 10-20-70](#): el 10% del esfuerzo se centra en algoritmos, el 20% en tecnología y datos, y el 70% en personas, procesos y transformación organizativa.

Ante este cambio, conviven cuatro perfiles en las empresas: los negacionistas (enfocados en los sesgos), los inmovilistas (renegados a aprender), los «prisas» (aplican agentes sin definir el problema) y los motivados (con actitud para aprender y experimentar).

EL CIO COMO ARQUITECTO Y EL ROL DEL CEO

El CIO debe asumir una responsabilidad estructural a través de cuatro pilares:

► **Gestionar expectativas:** Explicar que la IA se implanta rápido, pero

PASAMOS DE SISTEMAS QUE GENERAN CONTENIDO A SISTEMAS CAPACES DE INTERPRETAR OBJETIVOS, TOMAR DECISIONES Y EJECUTAR SECUENCIAS DE ACCIONES DE FORMA AUTÓNOMA

la transformación cultural requiere tiempo.

► **Construir un roadmap:** Vincular los casos de uso a un plan de negocio a corto, medio y largo plazo para evitar iniciativas sin rentabilidad clara.

► **Rediseñar el modelo operativo:** Superar los silos departamentales y pensar en procesos transversales de principio a fin.

► **Garantizar el patrocinio del CEO:** La dirección general debe establecer la visión e involucrar activamente a la primera línea ejecutiva. Es de vital importancia que ese primer nivel no esté formado por inmovilistas, negacionistas o acelerados ya que, de no tener una capa unificada en el primer nivel de la compañía, la batalla será complicada.

La IA no transformará las compañías por el mero hecho de disponer de mejores modelos, sino cuando cambie la forma profunda en que trabajamos y creamos valor. ■

MÁS INFO



- » [AI Adoption in 2024, Boston Consulting Group](#)
- » [30% de los proyectos de GenAI podrían abandonarse tras el PoC, Gartner](#)
- » [Previsión de cancelación de más del 40% de los proyectos de IA agéntica antes de finales de 2027, Gartner](#)
- » [Riesgos derivados de la falta de datos preparados para IA y de contexto semántico, Gartner](#)
- » [Marco 10-20-70 para la transformación mediante IA, Boston Consulting Group](#)

La documentación TIC, a un solo clic



Guía práctica: cómo aplicar la IA en los flujos de trabajo

Esta guía práctica, elaborada por IT Research, en colaboración con Claranet y HP, ofrece recomendaciones para integrar la IA de forma segura y eficaz en los flujos de trabajo. Descubrirás cómo superar las principales barreras de adopción, desmontar los mitos más comunes, definir una hoja de ruta de implantación y preparar el entorno tecnológico para aprovechar todo el potencial de la IA



European Agentic IA

Este informe examina la preparación de Europa para la consolidación de la IA en las AAPP y describe los pasos necesarios para implementar la IA agéntica de forma segura y a gran escala en sectores clave como la Administración Pública.



Evolución del mercado TIC-digital en la primera mitad de 2026 e impacto en España

Lee este análisis exhaustivo, realizado por la consultora Advice Strategic Consultants, sobre cómo IA, Cloud, Ciberseguridad y Robótica están redefiniendo el sector tecnológico en España y el mundo. Datos, tendencias y casos reales de empresas líderes.



5 hechos que desmontan los mitos sobre la IA en el trabajo

A través de datos, casos de uso y recomendaciones prácticas, conocerás cómo la IA puede impulsar la productividad, potenciar las capacidades de los equipos, simplificar tareas repetitivas y convertirse en una ventaja competitiva para cualquier organización. Además, aprenderás por qué el liderazgo, la formación y la elección de la tecnología adecuada son claves para una implantación exitosa y segura.

