byteTI

353 · Noviembre 2026

Trabajo colaborativo.
La nueva experiencia del empleado

La importancia de automatizar procesos

Como preparar la red empresarial para la IA

COMPARATIVA
Soluciones de gestión de identidades

mkm PUBLICACIONES


itera
AI Day
19 NOVIEMBRE
10:00 h
ARCADE
TECH AI | RACING | NETWORKING
¡Inscríbete ahora!
Con el patrocinio de:
aws
udemy

4 **Carta del Director**

6 **Actualidad**

30 **Webinars y encuentros BYTE TI**

49 **Comparativa**
Soluciones de gestión de identidades y accesos

57 **Trabajo colaborativo. La nueva experiencia del empleado**

65 **Mujeres TIC** Maica Aguilar

69 **Un CIO en 20 líneas** Miguel Ángel Melero

72 **Legalidad TIC**

74 **Aplicación práctica**

76 **Tendencias**

80 **Entrevista** Ramón Valiente

83 **Adoptado digital**















N. 352 | ÉPOCA IV
Edita:
Publicaciones Informáticas MKM
Noviembre 2026.

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

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

Redacción
Alfonso Casas (acasas@revistabyte.es)

Coordinador Técnico
Regina de Miguel

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

Fotógrafos
P. Varela, E. Fidalgo

Diseño de portada
María Torre

Diseño y maquetación
María Torre

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

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

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

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

Revista mensual de informática
ISSN: 1135-0407

Depósito legal: B-6875/95

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

Carta del Director



Manuel Navarro Ruiz
Director de BYTE TI

Hacia dónde evoluciona el puesto de trabajo

El puesto de trabajo atraviesa una metamorfosis sobre la que hay una infinidad de pronósticos, no siempre acertados. Los "culpables" de esta situación tienen nombre: la inteligencia artificial, los agentes autónomos y la automatización avanzada. Todas ellas están redefiniendo la experiencia del empleado, desplazando el foco desde la mera acumulación de herramientas digitales hacia la integración estratégica en los procesos de negocio.

Como señala el exhaustivo artículo de Alfonso Casas en nuestra portada de este mes, ya no nos encontramos en la era de una IA receptiva que solo responde consultas, sino ante una tecnología ejecutiva capaz de asumir tareas complejas, coordinar acciones y liberar tiempo operativo. Este cambio de paradigma transforma la naturaleza de la colaboración. Las dinámicas laborales tradicionales, estructuradas entre personas, evolucionan hacia un entorno híbrido donde los profesionales interactúan en espacios comunes junto a asistentes y agentes inteligentes.

En este entorno, se puede apreciar que no siempre el dinero lo puede todo. De hecho, las empresas más innovadoras no son las que realizan desembolsos millonarios sin rumbo, sino las que identifican procesos concretos para automatizar tareas repetitivas y potenciar las habilidades humanas.

Han sido muchos los empresarios que han visto en la IA, la oportunidad para reducir la factura de nóminas. Y se han dado de bruces con la realidad porque no se trata de sustituir el talento, sino de amplificar la creatividad, el pensamiento crítico y la toma de decisiones estratégicas.

La tecnología y concretamente la Inteligencia Artificial va a tener mucho que decir en los próximo años, pero el verdadero reto al que se van a enfrentar las empresas no va a ser exclusivamente tecnológico, sino cultural y organizativo. Tanto las más grandes como las pequeñas y medianas empresas están llamadas a rediseñar sus modelos operativos para pasar de administrar aplicaciones aisladas a gestionar objetivos de negocio.

Creo que facilitar entornos colaborativos fluidos, acompañados de formación continua y un enfoque de gobernanza centrado en la persona, marcará la diferencia entre la saturación digital y la eficiencia colectiva.

myQ X

Digitalizar es mucho más que dejar atrás el papel

Se trata de hacer que la impresión y el escaneado se adapten a la forma de trabajar de las personas, con menos tareas manuales y mayor control. MyQ X 10.3 incorpora nuevas funciones para procesar documentos, revisar documentos escaneados y liberar trabajos de impresión desde el navegador. Todo para simplificar el trabajo diario y avanzar en la digitalización de tu organización.



myq-solution.com

Actualidad

El avance hacia futura infraestructura digital europea

OVHcloud y CGI, a través de su filial CGI France Défense et Spatial, anuncian la firma de un contrato multimillonario de 30 meses con la Agencia Espacial Europea (ESA) para contribuir a la realización de "Digital Earth Observation", el sistema de información de la ESA para la observación de la Tierra. Se trata de una infraestructura digital estratégica y soberana, diseñada para reunir datos, servicios y capacidades de procesamiento relacionados con esta aplicación.

Digital EO tiene como objetivo abrir nuevos usos de los datos satelitales para la comunidad científica, las entidades públicas, las empresas y los ciudadanos, acercando cada vez más las innovaciones derivadas de la Observación de la Tierra a la vida cotidiana.

Con más de 500 petabytes de datos satelitales previstos para 2035, gestionar eficientemente esta información y aprovechar plenamente su potencial representa un desafío creciente para las futuras misiones de la ESA, además de constituir un objetivo estratégico para la soberanía digital de Europa.

Desarrollo, distribución y gobernanza de algoritmos

Para responder a esta necesidad, la ESA ha emprendido Digital EO, un proyecto a gran escala destinado a la creación de un sistema digital descentralizado, escalable y resiliente. El objetivo es ofrecer un entorno soberano basado en un nuevo paradigma para gestionar de manera eficiente grandes cantidades de datos heterogéneos, junto con los recursos de computación e inteligencia artificial. El sistema permitirá reunir infraestructuras nacionales y europeas, apoyando al mismo tiempo el desarrollo, la distribución y la gobernanza de algoritmos, aplicaciones y servicios innovadores en el ámbito científico, público, comercial y en beneficio de los ciudadanos.

"Digital EO nos permitirá dar un paso más en la forma en que se gestionan y utilizan los datos de observación de la Tierra. Junto con CGI y OVHcloud, desarrollaremos y gestionaremos un sistema europeo innovador y soberano, capaz de respaldar esta ambición y proporcionar un apoyo duradero a los programas de la ESA y de la Comisión Europea, como Copernicus y DestinE", afirma Nicolaus Hanowski, Head of EO Mission Management and Ground Segment Department de la ESA.

Para convertir a Digital EO en una plataforma capaz de responder a las necesidades del futuro, el uso del cloud es fundamental. OVHcloud pondrá a disposición una plataforma cloud



Actualidad

El avance hacia futura infraestructura digital europea

soberana y estable, que combina recursos de computación, almacenamiento y redes con servicios cloud gestionados. El sistema se implementará inicialmente en el centro de Europa (en Italia, Francia y Alemania), y contará con servicios de soporte gestionados desde Polonia, pudiendo ampliarse posteriormente a otros países europeos y a Canadá. Además, OVHcloud contribuirá activamente a la evolución del sistema a largo plazo, garantizando su rendimiento, resiliencia y un constante alineamiento con las necesidades de los usuarios.

«Europa debe tener el pleno control de las infraestructuras que respaldan sus programas más estratégicos. Con Digital EO, ponemos nuestra experiencia en el cloud soberano al servicio de la ESA, permitiéndole desarrollar soluciones innovadoras para procesar, almacenar y aprovechar los volúmenes cada vez mayores de datos de observación de la Tierra, en beneficio de la investigación, la industria y las comunidades de usuarios operativos. Todo ello garantizando los más altos niveles de rendimiento, resiliencia y seguridad. Nuestra ambición es clara: crear un Digital EO europeo sólido y soberano, capaz de evolucionar con el tiempo al ritmo de las necesidades y ambiciones de la ESA», declara Octave Klaba, CEO y fundador de OVHcloud.

Desarrollo científico

En el centro de esta infraestructura, Digital EO constituirá el núcleo tecnológico y operativo.



CGI se encargará de la fase de ideación e integración, y contribuirá a la realización de Digital EO permitiendo a las organizaciones gestionar sus datos, servicios y usuarios. Además, ofrecerá soporte a usuarios y desarrolladores, contribuyendo con la mejora continua del sistema.

«Con Digital EO, ponemos nuestra experiencia en el sector espacial y en plataformas digitales críticas al servicio de una ambición estratégica para Europa. Gracias a la combinación de nuestras competencias en ciberseguridad, datos e inteligencia artificial, ayudamos a la ESA a crear una plataforma soberana, sólida y escalable, capaz de generar valor duradero a partir de los datos satelitales y acelerar la innovación en el ecosistema europeo», concluye Didier Thérond, presidente de CGI en Francia.

Al poner en común las infraestructuras y las inversiones, Digital EO debe permitir acelerar la innovación, el desarrollo científico y la industrialización de servicios y aplicaciones basados en la observación de la Tierra, contribuyendo al mismo tiempo a reforzar la soberanía digital europea y a preparar los futuros programas de la ESA.

Actualidad

El malware supera al phishing como principal amenaza basada en DNS

El malware ha superado al phishing como principal amenaza basada en DNS en el primer semestre de 2026, tras pasar del cuarto puesto en el segundo semestre de 2025 al primero en solo seis meses. Es una de las principales conclusiones del H1 2026 DNS Threat Intelligence Report, el nuevo informe de EfficientIP elaborado a partir del análisis de más de 150.000 millones de transacciones DNS diarias.

La actividad diaria de malware se cuadruplicó entre enero y abril, al pasar de un mínimo de 8,0 millones de detecciones diarias a un pico de 32,6 millones, y se mantuvo cerca de ese nivel hasta junio. En conjunto, el volumen total de señales de amenaza DNS creció un 24% respecto al segundo semestre de 2025, de 11.180 millones a 13.850 millones de detecciones. El malware, por su parte, casi se duplicó en el mismo periodo, hasta alcanzar 3.840 millones de detecciones, y representó buena parte de ese incremento general.

Los atacantes prepararon la infraestructura

El informe identifica además una secuencia clara en los datos DNS que permite ver cómo los atacantes estaban preparando la infraestructura del repunte de malware semanas antes de su activación. En febrero, la actividad de algoritmos de generación de dominios, conocidos como DGA por sus siglas en inglés, fue la primera señal, con un crecimiento mensual del 24,2%.

En marzo, los dominios recién observados aumentaron un 56,8% y la actividad maliciosa comenzó a acelerarse, con un incremento del 73,1%. En abril, ambas señales alcanzaron su máximo de forma simultánea: los dominios recién observados crecieron otro 92,1% y la actividad maliciosa un 86,8%, coincidiendo con el pico de malware del semestre. El informe también analiza varias familias de algoritmos de generación de dominios y muestra que algunas infraestructuras maliciosas pueden seguir generando actividad incluso después de que los registros de dominio expiren o tras periodos de aparente inactividad. P

Al tiempo, el phishing muestra cambios relevantes. Su volumen general descendió un 10 % en el primer semestre de 2026, pero los objetivos cambiaron de forma notable entre sectores. Las marcas de logística y mensajería pasaron del séptimo al tercer puesto entre los sectores más atacados, con una cuota de detecciones que se multiplicó por 3,4, del 4,0 % al 13,6 %, impulsada en gran medida por una única campaña activa surgida a finales de junio.

FERNANDO JOFRE



24 horas para reaccionar

Durante años, las empresas han gestionado las vulnerabilidades con una mezcla de procedimientos internos, prioridades y urgencias. Desde el pasado 11 de septiembre, en Europa el reloj corre también por obligación. El Cyber Resilience Act establece que los fabricantes deben comunicar las vulnerabilidades de sus productos que estén siendo explotadas activamente y determinados incidentes graves. La primera alerta debe realizarse en un plazo máximo de 24 horas y la notificación completa, en 72. Las obligaciones afectan a productos con elementos digitales comercializados en la UE,

Puede parecer otro requisito regulatorio, pero sus implicaciones van más allá. Para reaccionar en 24 horas hay que saber qué productos tenemos, qué componentes incorporan, qué vulnerabilidades les afectan y quién toma las decisiones cuando aparece un problema. Para CIOs y CISOs, eso convierte el inventario, la gestión de vulnerabilidades y la coordinación interna en algo más que buenas prácticas. Son capacidades que tendrán que funcionar cuando empiece la cuenta atrás. Las principales obligaciones del reglamento llegarán en diciembre de 2027, pero las relativas a la notificación ya están vigentes. Porque en ciberseguridad podemos tener muchos procedimientos. La verdadera prueba empieza cuando solo tenemos 24 horas.

Actualidad

El 81 % de los CIOs confía en la IA para ahorrar costes, aunque solo el 6% la ha desplegado

La IA está dejando de ser una herramienta de apoyo para convertirse en un elemento que modifica cómo se distribuyen las tareas en las empresas. El reto para los CIOs es el de cómo reorganizar los equipos, las responsabilidades y las competencias alrededor de ellas.

Esta transformación también está generando nuevas tareas para las personas. Un reciente estudio del IBM Institute for Business Value señala que el 80 % de los responsables de RR. HH. considera que la adopción de IA está creando un "trabajo invisible" para los empleados, relacionado con validar recomendaciones, corregir errores, aportar contexto o gestionar excepciones. El mismo estudio sitúa la capacidad para supervisar, validar y corregir los resultados de la IA entre las competencias más importantes para la fuerza laboral.

De incorporar IA a reorganizar el trabajo

El estudio de LiceoTIC sobre el mercado del talento IT muestra la magnitud de la expectativa de las empresas: el 81 % de los CIOs espera que la IA sea la principal vía de ahorro durante los próximos tres años, especialmente a través de la automatización de tareas administrativas, el soporte IT y la gestión documental. Sin embargo, solo un 6 % de las organizaciones ha conseguido desplegar la IA a gran escala, mientras que el resto se encuentra todavía evaluando casos de uso o desarrollando proyectos piloto.

El impacto de la IA no se limita a los departamentos que utilizan tecnología: también afecta directamente al propio sector IT. La generación de código, las pruebas, la documentación, el análisis de datos o determinadas tareas de soporte pueden automatizarse progresivamente, modificando el contenido de puestos que hasta ahora constituían una vía habitual de entrada al mercado laboral. Los primeros efectos ya se observan en el mercado de trabajo. Según un estudio de Gartner publicado en julio, el 22 % de los responsables de RR. HH. afirma que al menos un directivo de su organización ha dejado de contratar perfiles de entrada debido a la automatización mediante IA. Gartner advierte de que la respuesta no debería ser eliminar estas posiciones, sino rediseñarlas para que los profesionales junior puedan asumir antes tareas de mayor valor y desarrollar las competencias que necesitarán en un entorno de trabajo con IA.

Para el sector tecnológico, esto plantea un reto específico: cómo mantener las vías de entrada y desarrollo profesional de programadores y técnicos IT jóvenes cuando algunas de las tareas tradicionalmente asociadas a los primeros años de carrera empiezan a automatizarse. El cambio no implica necesariamente una desaparición de estos perfiles, sino una evolución de sus funciones y de las competencias que se les exigirán.

Nuevas competencias

En este escenario, las capacidades más valiosas serán aquellas que permitan trabajar con sistemas de IA y, al mismo tiempo, aportar lo que estos no pueden resolver por sí solos: criterio, pensamiento crítico, capacidad de supervisión, resolución de problemas y toma de decisiones.

El estudio de IBM apunta precisamente en esta dirección: mientras los CHROs sitúan el pensamiento crítico y el juicio humano entre las capacidades prioritarias, una parte de los empleados teme que el uso intensivo de IA pueda provocar una pérdida de determinadas habilidades. Para los CIOs, esto implica pasar de definir puestos exclusivamente por las tareas que realizan a analizar qué combinación de personas, tecnología y capacidades necesita cada proceso.

Actualidad

SUSE ofrece a las empresas control soberano sobre la IA agéntica con NVIDIA



SUSE ha mostrado al mercado nuevas capacidades para que las empresas puedan adoptar soluciones de IA privada para entornos empresariales, manteniendo el control operativo, la seguridad y la gobernanza de sus sistemas. SUSE refuerza así la seguridad empresarial de los agentes de IA autónomos mediante la integración de la nueva arquitectura de referencia NVIDIA OpenShell en SUSE AI Factory con NVIDIA.

Esta arquitectura combina NVIDIA Vera Rubin para la inferencia de modelos, CPU NVIDIA Vera que ejecutan OpenShell para la ejecución de agentes y DPU NVIDIA BlueField-4 que ejecutan NVIDIA Sentry, basado en NVIDIA DOCA, para la monitorización independiente del sistema anfitrión y la aplicación de políticas directamente en el silicio.

Entorno controlado para ejecutar los agentes

Como partner de lanzamiento de la arquitectura de referencia OpenShell, SUSE contribuye al desarrollo de una arquitectura abierta y a escala industrial para crear, aislar, supervisar y gobernar agentes de IA autónomos con seguridad de nivel empresarial. Mediante el uso de entornos aislados de Kubernetes y pasarelas de API, junto con OpenShell, SUSE AI Factory con NVIDIA proporciona un entorno controlado que regula la ejecución de los agentes sin comprometer el máximo rendimiento. Entre sus principales capacidades se incluyen:

- **Gobernanza activa basada en el modelo zero trust:** Los proxies de supervisión inspeccionan continuamente el tráfico de los agentes, autorizan el acceso de acuerdo con las políticas definidas y bloquean las solicitudes de red no autorizadas para ayudar a evitar la extracción de código o datos.
- **Soberanía de los datos y cumplimiento normativo:** Permite ejecutar código de agentes dentro del perímetro corporativo, con políticas de acceso que restringen la transferencia de propiedad intelectual empresarial y conjuntos de datos propietarios fuera de la infraestructura privada.
- **Modelo de costes predecible:** El despliegue privado de modelos, mediante el uso de microservicios NVIDIA NIM, elimina las tarifas por token de las API públicas de terceros y permite planificar la inversión en infraestructura en función de una capacidad predecible.

Disponible con SUSE AI Factory con NVIDIA, la última versión incorpora seguridad para agentes basada en el modelo zero trust a través de la arquitectura de referencia NVIDIA OpenShell, junto con SUSE Linux Enterprise Server (SLES) para NVIDIA. La solución está diseñada para ofrecer compatibilidad inmediata con las plataformas de silicio de próxima generación de NVIDIA.

En conjunto, estas innovaciones proporcionan una base unificada, preparada para entornos empresariales, que permite a los desarrolladores crear aplicaciones de IA y agentes autónomos listos para producción; a los equipos de ingeniería de plataformas, desplegarlos; y a los departamentos de TI empresariales, gobernarlos en cualquier tipo de infraestructura.

SLES para NVIDIA permite a las empresas acelerar las cargas de trabajo de IA con acceso inmediato a las últimas innovaciones de hardware de NVIDIA, incluida la infraestructura NVIDIA Vera Rubin.

Actualidad – Te interesa

La IA convierte la soberanía digital en una decisión estratégica

La infraestructura cloud hace tiempo que dejó de ser una prestación puramente tecnológica. Es el fundamento arquitectónico sobre el que operan la economía, la administración y, cada vez más, la Inteligencia Artificial. Quién controla esta infraestructura influye en la capacidad de acción estratégica de las empresas, e incluso de economías nacionales completas.

El Cloud Computing se percibe con frecuencia, y de forma errónea, como una mera provisión técnica de capacidad de cómputo y almacenamiento. Sin embargo, las plataformas cloud estructuran hoy procesos centrales de la economía y la administración, desde el almacenamiento de datos, pasando por el entrenamiento de IA, hasta las arquitecturas de seguridad.

Así pues, la infraestructura digital ya no es un tema puramente tecnológico, sino un factor estratégico para la capacidad de acción económica y política. Quien implementa datos centrales y sistemas de IA en plataformas ajenas, establece dependencias a largo plazo. Las decisiones que se toman hoy determinan el margen de maniobra de los próximos cinco años.

Dependencias estructurales

El mercado de infraestructuras cloud está dominado hoy por unos pocos grandes proveedores. Plataformas como Amazon Web Services, Google Cloud o Microsoft Azure ponen a disposición de las empresas no solo infraestructura, sino ecosistemas completos de herramientas de desarrollo, plataformas de datos y servicios de IA. Para las empresas esto ofrece ventajas, pero al mismo tiempo, se generan dependencias estructurales que a menudo solo se hacen visibles cuando es necesario un cambio de proveedor.

Una parte sustancial de esta dependencia resulta del marco jurídico: los datos alojados en proveedores estadounidenses están sujetos al derecho extraterritorial de EE. UU. incluso en centros de datos europeos. El CLOUD Act permite a las autoridades estadounidenses el acceso, con independencia del lugar donde se encuentre el servidor.

A esto se añade la "fuerza gravitatoria de los datos". La capacidad de cómputo sigue a los datos en la práctica. Cuando grandes volúmenes de datos se encuentran en una plataforma, sobre



La IA convierte la soberanía digital en una decisión estratégica

ella se construyen también los flujos de trabajo de análisis e IA. Un cambio de proveedor se convierte así en un gran proyecto de migración técnica con los costes y riesgos correspondientes.

La geopolítica como gobernanza de TI

Lo que durante mucho tiempo se consideró un debate de compliance, es hoy realidad operativa. El bloqueo de servicios del Tribunal Penal Internacional o las inestabilidades en la política comercial demuestran que las decisiones cloud son decisiones de gobernanza. Quién está técnicamente vinculado, pierde margen de maniobra en tiempos inestables.

Un estudio de techconsult para IONOS CLOUD entre 200 empresas europeas subrayaba este cambio de conciencia: el 88% de las empresas valoraban el control completo sobre su stack de IA (infraestructura, modelos y datos) como "muy importante". Para el 45% este aspecto era especialmente crítico. Reducir dependencias de proveedores externos y limitar riesgos como el acceso de terceros estados a los datos era, para la mayoría, una exigencia permanente.

La IA aumenta la necesidad de soberanía

Con la integración de la Inteligencia Artificial en los procesos de negocio, la decisión sobre la infraestructura resulta aún más trascendente para las empresas. Los sistemas de IA aprenden de los datos. Quien introduce datos en sistemas externos cede potencialmente la soberanía sobre su activo más valioso.

El estudio de techconsult hace estas afirmaciones tangibles. El 58% de las empresas encuestadas quiere excluir expresamente que sus datos sean utilizados para el entrenamiento de modelos de IA externos. El 71% exige regulaciones contractuales claras sobre la soberanía de los datos, así como el cumplimiento consecuente del RGPD, ISO 27001 y la protección básica de TI del BSI.

Al mismo tiempo, los datos muestran hacia dónde se dirige el viaje estratégico: el 87% de las empresas atribuye a los modelos de IA de código abierto un papel central en el futuro. Los modelos abiertos permiten intervenciones más profundas en la lógica del modelo, son operables con independencia de las estructuras de API y permiten una visión completa del código y los datos de entrenamiento.

Por otra parte, los principales desafíos al vincular modelos de IA con datos empresariales son: falta de experiencia con arquitecturas RAG (71%), integración en sistemas legacy como ERP o



Actualidad – Te interesa

La IA convierte la soberanía digital en una decisión estratégica

> **Tener en cuenta la soberanía como principio de diseño de la infraestructura asegura una verdadera capacidad de acción empresaria**

CRM (68%), protección frente al Data Poisoning (66%), construcción de infraestructura técnica e integración de datos (66%), garantía de que los datos de la empresa no se utilicen para el entrenamiento de modelos (63%), protección frente a Prompt Injection (63%), protección de las interfaces API (63%), separación clara entre modelo de IA, historial de consultas y almacenamiento de datos (62%), control sobre los espacios de almacenamiento y procesamiento (56%) y gestión de control de acceso y permisos (54%).

La regulación crea el marco pero no la infraestructura

En Europa, la Ley de IA, el Data Act y el RGPD definen estándares importantes. Pero la regulación por sí sola no reemplaza una base tecnológica propia. Para las empresas esto significa que el compliance es necesario, pero no suficiente. La pregunta real es si la infraestructura sobre la que corren sus datos y sistemas de IA está efectivamente bajo su control o al menos bajo jurisdicción europea. Según el estudio de techconsult, las empresas prefieren proveedores europeos para la operación de sus cargas de trabajo de IA con un 48%, claramente por delante de los hiperescaladores con un 32%.

IONOS CLOUD: Infraestructura soberana como principio de diseño

Exactamente esas son las exigencias que IONOS CLOUD tiene ancladas como principio de infraestructura. La soberanía no es un reclamo publicitario, sino un estado auditado. El fundamento arquitectónico lo conforman centros de datos propios en Europa, sin exposición al US CLOUD Act y con una arquitectura nativa de RGPD.

Para una operación de IA soberana, IONOS CLOUD pone a disposición los siguientes elementos concretos:

- Recursos GPU: basados en NVIDIA para cargas de trabajo de alto rendimiento.
- AI Model Hub, una plataforma de IA soberana para acceder a los principales modelos Open Source para generación de texto e imágenes.
- IONOS CLOUD MCP Server, para conectar tu IA con tu infraestructura cloud donde tus datos permanecen seguros bajo soberanía europea.
- Plena conformidad con el RGPD sin uso de datos para entrenamiento de modelos externos.
- Colaboración soberana sin pérdida de control gracias a Nextcloud Workspace.
- IONOS Momentum, un ecosistema de IA soberano y europeo, desarrollado especialmente para pequeñas y medianas empresas. La plataforma combina modelos de IA modernos, automatizaciones, aplicaciones e infraestructura cloud segura en una solución centralizada y conforme con el RGPD.

En definitiva, la decisión sobre la infraestructura se ha convertido en una decisión estratégica y hace tiempo que dejó de ser una cuestión puramente tecnológica. La estrategia cloud de una empresa determina quién tiene acceso a los datos y si la empresa sigue siendo capaz de actuar en tiempos geopolíticamente convulsos.

Tener en cuenta la soberanía como principio de diseño de la infraestructura asegura una verdadera capacidad de acción empresarial y otorga la capacidad de decidir, cambiar y configurar desde una posición de control propio.

Actualidad – Te interesa

EMASESA impulsa su digitalización consiguiendo resiliencia estructural mediante Continuidad de Negocio, Protección Inmutable y Modernización del Data Center de la mano de IaaS365

EMASESA, Empresa Metropolitana de Abastecimiento y Saneamiento de Aguas de Sevilla S.A., es la entidad que gestiona y administra el ciclo integral del agua en Sevilla capital y once municipios de su área metropolitana. Su objetivo es ofrecer un servicio público de calidad, con un compromiso de transparencia e información permanente a la ciudadanía.



A nivel tecnológico, EMASESA dispone de dos centros de datos, ubicados en la capital andaluza comunicados entre sí mediante red propia, lo que le permite desplegar servicios en uno u otro indistintamente y, en caso de desastre, usar uno de ellos para seguir funcionando sin perjuicio por el que quedase inoperativo. Además, en ellos, alojan importantes equipos y entornos de conmutación que constituyen, en su conjunto, un sistema de misión crítica para la infraestructura de comunicaciones y servicios telemáticos de la entidad.

"La transformación digital de EMASESA exige disponer de una infraestructura tecnológica resiliente, segura y preparada para responder a los desafíos actuales y futuros. Nuestro objetivo no era únicamente renovar tecnología, sino construir una plataforma que sirva de base para la digitalización de procesos, la explotación avanzada de los datos, la automatización de operaciones y la incorporación progresiva de nuevos servicios digitales para la organización", comenta Rafael Manuel Martínez Torres, Jefe del Departamento de Infraestructuras TIC de EMASESA.

"La situación de partida que teníamos era, por un lado, que ambos CPDs estaban basados en un esquema de tres capas, en el cual los recursos de cómputo, almacenamiento y conectividad teníamos que administrarlos separadamente y donde convivían tecnologías muy diversas, de distintos fabricantes, que nos provocaban una operación compleja y nos dificultaban la gestión técnica y administrativa. A esto se unía, por otro lado, la criticidad de los servicios que estábamos prestando y se prestan desde dichos centros tecnológicos, lo que hacía imprescindible mejorar el plan de continuidad de negocio adaptándolo a las necesidades actuales", añade Rafael.

En este contexto, el organismo confió en IaaS365 para llevar a cabo un proyecto para dotarles de resiliencia con dos objetivos. Primero, evolucionar la infraestructura existente adoptando un nuevo modelo innovador, eficiente, seguro y holístico que permita simplificar la administración de los sistemas y el despliegue de nuevos servicios tanto en la plataforma TI local como en la nube. Y, segundo, contar con un servicio de copias de seguridad de los datos y del software que conforman dicha arquitectura tecnológica, que les permita restaurar la situación ante cualquier tipo de problema físico o lógico en los sistemas.

"Desde IaaS365 se trabajó de forma alineada con las exigencias actuales de EMASESA para plantear una solución resolutiva para el presente

y también de cara a su evolución futura. El proyecto ha incluido dos retos muy interesantes. Se ha llevado a cabo la prestación de los servicios de suministro, instalación y puesta en servicio de una infraestructura hiperconvergente (HCI) que sustituirá a toda la arquitectura x86 actual del organismo. Con este cambio, la entidad va a poder simplificar la gestión de sus centros de proceso de datos, mejorar su seguridad, centralizar la gestión y les permitirá además el crecimiento lineal de la plataforma TI. Y el segundo reto ha sido dotarles de un sistema de copias de seguridad escalable, que les permita el crecimiento en capacidad de cómputo y almacenamiento, sin necesidad de desechar ningún componente ya existente", comenta Rosalía Lima, Regional Account Manager para la zona de Andalucía de IaaS365.

Por su parte, la arquitectura hiperconvergente propuesta cumple con requisitos muy importantes para el correcto funcionamiento de EMASESA. Así, cuenta con un módulo que permite, mediante software, definir firewalls para el control y filtrado granular de las comunicaciones entre máquinas virtuales y aplicaciones. Es compatible con su solución existente de copias de seguridad y con el refuerzo que se ha hecho de la misma. Está preparada para la orquestación de contenedores basada en Kubernetes. Y mejora el sistema de monitorización mediante la automatización de muchas de las tareas TI.

Y, en cuanto a la nueva solución de copias de seguridad, el proyecto les va a dotar de una plataforma distribuida, escalable y de alta disponibilidad que no permita el acceso indebido a los datos salvaguardados y que cuenta con almacenamiento interno. Van a contar además, con inmutabilidad de los datos ante ataques de tipo Ransomware. Les va a proveer de alertas en caso de mal funcionamiento de la solución del tipo que no se estén guardando los datos de forma adecuada, problemas hardware, problemas de rendimiento, etc. Y, también, van a recibir informes sobre el funcionamiento de dicha plataforma, lo que les va a permitir ser proactivos y tomar mejores decisiones.

Para IaaS365, este proyecto es una solución que ejemplifica a la perfección la habilitación de la transformación digital y adopción de nuevas tecnologías para adaptarse a la realidad actual TI. Con la modernización de EMASESA en ambos entornos, la entidad se coloca a la cabeza en innovación institucional volcada a la mejora de los servicios al ciudadano consiguiendo sus objetivos de simplificar la gestión de sus Data Centers, automatizarlos, prepararlos para necesidades y crecimiento futuro y dotarles de mayor seguridad e inmutabilidad.

Con esta iniciativa, IaaS365 consolida su papel como partner tecnológico de referencia, acompañando a EMASESA en todo el proyecto de principio a fin. A los servicios de suministro, instalación y puesta en marcha de ambos retos, se han unido también el de formación al personal del organismo para el correcto uso de las tecnologías implantadas, así como el de mantenimiento y servicio de atención al usuario para contar con un soporte experto personalizado de cara a resolver posibles dudas o incidencias.

EMASESA está encauzando la gestión de sus servicios TI a un modelo de procesos que garanticen la disponibilidad y la mejora continua y con este proceso de digitalización marca un punto de inflexión innovador que la prepara para afrontar el entorno TI tan cambiante.

Al contar con IaaS365 como socio tecnológico para este proyecto, EMASESA consolida una arquitectura tecnológica moderna, segura y preparada para afrontar los futuros retos de una gestión cada vez más digitalizada del ciclo integral del agua. La modernización de sus centros de datos y el fortalecimiento de sus capacidades de continuidad y protección del dato constituyen un paso fundamental dentro de una estrategia más amplia orientada a convertir la tecnología en un elemento impulsor de la eficiencia operativa, la sostenibilidad, la innovación y la mejora continua de los servicios prestados a la ciudadanía.

Actualidad – Te interesa

h&k reduce más de un 50% los costes de mantenimiento de aplicaciones mediante ingeniería agéntica

La compañía presenta los primeros resultados obtenidos con Ariadna, un modelo que combina inteligencia artificial, conocimiento estructurado y supervisión humana para acelerar el desarrollo sin perder control ni trazabilidad

La aplicación de la inteligencia artificial al desarrollo de software ha estado marcada en los últimos años por la capacidad de generar código de forma más rápida. Sin embargo, en las aplicaciones empresariales, una parte importante del coste no está únicamente en programar; sino más bien en comprender los sistemas existentes, localizar conocimiento, analizar dependencias, evaluar el impacto de los cambios y coordinar el trabajo entre diferentes equipos.

Precisamente, tras varios meses de validación en proyectos reales, h&k ha medido el impacto de su modelo de ingeniería de software agéntica en proyectos de mantenimiento y evolución de aplicaciones existentes. En concreto, ha obtenido reducciones superiores al 70% en los tiempos de desarrollo y al 50% en los costes, junto con una mejora del 30% en la calidad y seguridad del software entregado. Estos resultados se han obtenido frente a un modelo de desarrollo tradicional y utilizando analizadores estándar como referencia.



Los resultados ponen el foco en una cuestión que va más allá de la velocidad de generación de código. El mantenimiento de una aplicación exige conocer las reglas de negocio, las decisiones acumuladas durante años, sus dependencias y las consecuencias que puede tener cada modificación. En sistemas complejos, buena parte del esfuerzo se dedica precisamente a reconstruir ese contexto antes de realizar cualquier cambio.

Reducir el trabajo de bajo valor

El ahorro obtenido por h&k no procede únicamente de utilizar inteligencia artificial para generar código. El modelo busca reducir actividades de bajo valor como la búsqueda

Actualidad – Te interesa

h&k reduce más de un 50% los costes de mantenimiento de aplicaciones

> **Una mayor eficiencia en el mantenimiento puede hacer viables proyectos que anteriormente no lo eran**

de información, la reconstrucción manual del contexto de una aplicación, el análisis de impacto, la repetición de tareas o los traspasos de conocimiento entre equipos.

Para ello, h&k utiliza Ariadna como habilitador de este modelo de trabajo. La plataforma estructura previamente el conocimiento relacionado con cada aplicación para que la IA pueda operar sobre un contexto delimitado, reutilizable y trazable. De este modo, la tecnología puede concentrarse en las tareas de ejecución mientras se mantiene la supervisión humana en las decisiones de validación y aprobación. "La mejora no viene solo de escribir código más rápido; sino de reducir todo el tiempo que dedicamos a entender qué hay que cambiar, dónde hacerlo y qué impacto puede tener", explica Carlos Gutiérrez, Product Lead de Ariadna en h&k.

Esta aproximación resulta especialmente relevante en el mantenimiento y evolución de sistemas existentes, donde conservar el conocimiento de la aplicación a medida que se introducen cambios permite disminuir la dependencia de personas concretas y evitar que una parte del trabajo tenga que repetirse en cada intervención.

Más proyectos viables y menos deuda técnica

La reducción de tiempos y costes tiene implicaciones directas para las organizaciones. Una mayor eficiencia en el mantenimiento puede hacer viables proyectos que anteriormente no resultaban rentables, facilitar la modernización de aplicaciones heredadas y reducir la acumulación de deuda técnica.

También permite liberar recursos internos para dedicarlos a iniciativas de mayor valor, al tiempo que las compañías pueden abordar procesos de transformación tecnológica sin que el crecimiento de las necesidades de desarrollo implique necesariamente un aumento proporcional de los equipos.

En la práctica, el modelo se está aplicando tanto al mantenimiento y evolución de sistemas existentes como a procesos de modernización de aplicaciones heredadas, donde resulta necesario recuperar y estructurar conocimiento acumulado durante años en el código y la documentación.

Mejora de todo el ciclo de vida

Para h&k, la evolución de la inteligencia artificial aplicada al software está entrando en una nueva fase. Después de una primera etapa marcada por las herramientas capaces de producir código con mayor velocidad, el siguiente reto pasa por mejorar la eficiencia del conjunto del ciclo de vida de las aplicaciones.

El objetivo es, por un lado, acelerar el desarrollo; y por otro, reducir el coste total de construir, mantener y evolucionar software durante años, conservando al mismo tiempo la trazabilidad sobre las decisiones, el conocimiento de negocio y el control sobre los cambios. En este contexto, h&k plantea la ingeniería agéntica como una forma de combinar automatización, inteligencia artificial y conocimiento estructurado sin eliminar la intervención humana de aquellas decisiones que requieren validación, responsabilidad y criterio.

Tras una primera fase de validación con clientes durante el verano de 2026, h&k ha comenzado recientemente la comercialización de Ariadna, especialmente orientada a organizaciones que gestionan sistemas heredados o trabajan en entornos donde la documentación, la trazabilidad y el control sobre los cambios son especialmente relevantes.

Actualidad – Te interesa

Racks de 10 pulgadas: cuándo elegir una infraestructura de red compacta

Por Federico Ansón,
Country Manager de Lanberg en la Península Ibérica

En oficinas pequeñas, comercios y espacios técnicos reducidos, instalar un armario rack convencional de 19" no siempre resulta práctico. Aunque las necesidades de conectividad siguen creciendo, el espacio disponible para alojar los equipos de red suele ser limitado. En estos casos, los racks de 10" ofrecen una alternativa compacta para organizar la infraestructura sin sobredimensionar la instalación.

La elección del rack influye en la accesibilidad a los dispositivos, la gestión del cableado y las posibilidades de mantenimiento. Por eso, más alláw de las dimensiones, conviene analizar qué equipos se van a instalar, cómo se accederá a ellos y si será necesario ampliar la red en el futuro.

¿Cuándo tiene sentido utilizar un rack de 10 pulgadas?

Estos formatos resultan especialmente útiles en pequeñas oficinas, establecimientos comerciales, instalaciones domésticas avanzadas y espacios donde se necesita centralizar routers, switches, paneles de conexión y otros componentes compatibles.

Su principal ventaja es el aprovechamiento del espacio, pero no es la única. Una instalación bien organizada permite identificar conexiones con mayor facilidad, reducir errores durante las intervenciones y mantener los equipos accesibles.

Antes de elegirlo es necesario comprobar la compatibilidad de los dispositivos, la profundidad disponible, la capacidad de carga y las necesidades de ventilación.

Diseños abiertos para facilitar la instalación

La estructura del rack también debe responder al entorno. Mientras que los armarios cerrados ofrecen una barrera física frente al acceso no autorizado, los modelos abiertos permiten acceder directamente al cableado y a los equipos desde diferentes lados.

Esta configuración puede resultar interesante en instalaciones interiores controladas, especialmente cuando se realizan



modificaciones o ampliaciones frecuentes. En esta línea, Lanberg ha incorporado a su catálogo la serie Open Rack 10", disponible en versiones de 4U, 6U y 9U, con opciones de instalación en pared o sobre una superficie de trabajo.

Su estructura abierta, los puntos de fijación para organizar cables y los paneles perforados facilitan el montaje, la circulación del aire y las operaciones de mantenimiento.

Elegir una infraestructura compacta demuestra el correcto conocimiento del espacio, la selección de componentes compatibles y la prevención en el acceso a los equipos.

En definitiva, el mejor rack es el que responde a las necesidades reales de cada instalación, tanto en su configuración inicial como en futuras intervenciones.

Más información sobre las soluciones Open Rack 10" de Lanberg.

Actualidad – Te interesa

Elige la infraestructura Supermicro que tu empresa necesita con Nemix

La elección de un servidor depende de las aplicaciones que ejecutará, del rendimiento que requiere la empresa y de sus planes de crecimiento. No necesita la misma infraestructura una organización que busca consolidar su entorno de virtualización que otra que desarrolla proyectos de inteligencia artificial (IA) o HPC. La gama H15 de Supermicro, basada en procesadores AMD EPYC de sexta generación, ofrece distintas configuraciones para responder a estos escenarios.

Los sistemas H15 incorporan procesadores de hasta 256 núcleos y 512 hilos, memoria DDR5 y conectividad PCIe 6.0. Estas prestaciones permiten abordar cargas exigentes, desde aplicaciones empresariales y bases de datos hasta entornos cloud y servicios de IA. Para aprovecharlas, es fundamental elegir una configuración acorde con los requisitos de cada proyecto.

Las familias Hyper y CloudDC incluyen servidores de 1U y 2U con diferentes opciones de procesamiento y expansión. Permiten consolidar cargas de trabajo, renovar plataformas de virtualización o ampliar la capacidad de los centros de datos. Algunas configuraciones admiten hasta cuatro GPU de doble ancho, lo que facilita ejecutar determinadas cargas de inferencia sin recurrir a sistemas dedicados exclusivamente a la aceleración.

Para proyectos que requieren mayor capacidad de aceleración, Supermicro ofrece sistemas específicos para GPU. Su catálogo incluye equipos con hasta diez aceleradores PCIe y plataformas con ocho aceleradores, disponibles con opciones de refrigeración por aire o líquida. La elección depende de factores como el volumen de datos, la memoria necesaria y los requisitos de las tareas de inferencia o entrenamiento.

Adaptar la infraestructura a cada carga de trabajo exige evaluar las prioridades antes de invertir. Una configuración sobredimensionada puede elevar los costes sin aportar un beneficio proporcional, mientras que una insuficiente puede limitar el rendimiento y dificultar futuras ampliaciones. Nemix ayuda a las empresas a encontrar ese equilibrio. Como integrador de infraestructuras tecnológicas, analiza los requisitos de cada proyecto y configura soluciones a medida. La integración se realiza en una sala limpia con clasificación ISO 8.

Con más de 30 años de experiencia en integración de sistemas, Nemix ofrece soporte técnico especializado durante todo el proyecto, desde la selección de la arquitectura hasta la puesta en marcha. El objetivo es proporcionar una infraestructura ajustada a las aplicaciones de cada empresa, validada antes de su instalación y preparada para adaptarse a la evolución de sus cargas de trabajo.



Actualidad – Te interesa

"Sangfor es una compañía global, pero queremos ser también un socio cercano"

Teamo Chen, Deputy Country Manager en Sangfor Technologies



Teamo Chen, Deputy Country Manager de Sangfor Technologies, se traslada a Madrid para liderar la expansión del fabricante en la Península Ibérica y Polonia. La compañía, que alcanzó 1.200 millones de dólares en 2025 y dedica más del 20% de sus ingresos a I+D, proyecta crear un equipo de 20 profesionales en tres años. Tras los cambios en el mercado de virtualización, Sangfor propone su infraestructura hiperconvergente como alternativa estratégica.

Después de más de once años en Sangfor y de haber desarrollado buena parte de su carrera en Asia-Pacífico, ¿qué le llevó a trasladarse personalmente a Madrid para dirigir los mercados de España, Portugal y Polonia?
Durante estos once años he tenido la oportunidad de participar activamente en la expansión de Sangfor en Asia-Pacífico. En Hong Kong, Macao y Taiwán construimos relaciones muy sólidas con nuestros socios locales y alcanzamos una facturación anual de 22 millones de dólares en 2025.

Sin embargo, mi decisión de trasladarme a Madrid no responde únicamente a una oportunidad empresarial. Existe también una conexión personal y familiar con España. Me gusta mucho el idioma y estoy estudiando español; incluso uno de mis hijos lo eligió como tercera lengua en su colegio de Hong Kong. Además, soy un gran aficionado al tenis y admiro especialmente a Rafael Nadal y Carlos Alcaraz.

Lo que más me atrajo de España fue la cercanía, la energía y la mentalidad abierta de la gente. Por eso, venir a Madrid no representa para mí una asignación temporal, sino un compromiso real con el país.

Desde el punto de vista empresarial, nuestra presencia directa transmite un mensaje claro: Sangfor considera España un centro estratégico para su desarrollo en Europa. Contar con la dirección sobre el terreno nos permite acelerar la toma de decisiones y conectar directamente las necesidades del mercado local con nuestros equipos globales de ingeniería y desarrollo.

Cuando las empresas españolas y portuguesas seleccionan una nueva plataforma tecnológica, valoran especialmente la estabilidad del fabricante y su capacidad de innovación. ¿Qué respaldo global ofrece Sangfor?

Actualidad – Te interesa

Teamo Chen, Deputy Country Manager en Sangfor Technologies

Sangfor alcanzó en 2025 unos ingresos globales de 1.200 millones de dólares y dispone de presencia directa en más de veinte países. Además, destinamos anualmente más del 20 % de nuestros ingresos a investigación y desarrollo.

Este compromiso con la innovación también cuenta con reconocimiento internacional. En el Gartner Magic Quadrant for Server Virtualization Platforms de 2026, Sangfor fue posicionado como Visionary. Asimismo, nuestra solución de infraestructura hiperconvergente mantiene una valoración de 4,9 sobre 5 en Gartner Peer Insights y un 100 % de disposición a recomendar, según los datos publicados actualmente en la plataforma.

Combinamos, por tanto, la estabilidad de una compañía tecnológica global con una elevada capacidad de innovación y una presencia local cada vez mayor.

¿Cómo plantea utilizar España como base para desarrollar el negocio en la Península Ibérica? ¿Qué compromisos concretos está asumiendo Sangfor en materia de equipo local y capacitación técnica?
Hemos definido junto con la dirección del grupo una hoja de ruta de localización a tres años. Durante el primer año estableceremos un equipo inicial de seis profesionales. En el segundo año prevemos ampliarlo hasta doce y, en el tercero, alcanzar una organización local de veinte personas, con capacidades comerciales, técnicas y de servicio.

> **Un número creciente de empresas está evaluando alternativas para sus cargas de trabajo virtualizadas**

El equipo se contratará principalmente en España y Portugal. Queremos incorporar profesionales que conozcan el idioma, la cultura empresarial y las necesidades específicas de los clientes de ambos países.

No obstante, nuestra estrategia va más allá de aumentar nuestra propia plantilla. Queremos transferir conocimiento al mercado y capacitar a ingenieros locales, arquitectos de nuestros socios y equipos técnicos de clientes.

Para ello, estamos impulsando programas de formación, certificaciones oficiales y proyectos piloto en los que los profesionales puedan trabajar directamente con nuestra tecnología. Nuestro objetivo es crear un ecosistema local preparado para diseñar, desplegar y mantener infraestructuras de nueva generación con un alto grado de autonomía.

El mercado europeo de virtualización está atravesando una transformación importante después de la adquisición de VMware por Broadcom. ¿Qué implica esta situación para las empresas españolas y qué alternativa propone Sangfor?
Los cambios en los modelos de licenciamiento y el incremento de los costes han hecho que muchas organizaciones sean más conscientes de los riesgos asociados a la dependencia de un único fabricante. Como resultado, un número creciente de empresas está evaluando alternativas para sus cargas de trabajo virtualizadas. Las organizaciones españolas necesitan opciones sólidas, predecibles y respaldadas por fabricantes con capacidad tecnológica y presencia local. Nuestro objetivo es ofrecer al mercado ibérico una alternativa de primer nivel, reconocida por Gartner y respaldada directamente por un equipo establecido en España.

Durante los próximos tres años centraremos especialmente nuestra estrategia en la infraestructura hiperconvergente. Sangfor HCI ofrece un modelo de costes competitivo, herramientas para facilitar la migración y una arquitectura diseñada para

proporcionar disponibilidad, rendimiento y resiliencia empresarial.

Además, nuestros clientes y socios tendrán acceso directo a ingenieros locales en Madrid. Esta proximidad es fundamental para reducir los riesgos de los proyectos, acelerar su puesta en marcha y ofrecer una atención más cercana.

A medida que consolidemos esta posición, incorporaremos progresivamente otras capacidades de nuestro catálogo, especialmente en ciberseguridad, para que nuestros socios puedan ofrecer propuestas más completas a sus clientes.

Para finalizar, ¿cómo resumiría el compromiso de Sangfor con España y con el conjunto del mercado ibérico?

El éxito de un fabricante solo es posible cuando también tienen éxito sus socios, sus clientes y la comunidad técnica local. Mi equipo y yo queremos trasladar al mercado español la misma entrega y perseverancia que representan Rafael Nadal y Carlos Alcaraz dentro de una pista de tenis. Mi traslado a Madrid, el aprendizaje del idioma, nuestro plan para crear un equipo local de veinte profesionales y la inversión en capacitación y certificación demuestran que nuestra apuesta es de largo plazo.

Sangfor es una compañía tecnológica global, pero queremos ser también un socio cercano y accesible para las empresas españolas y portuguesas. Venimos a ofrecer una alternativa sólida y reconocida internacionalmente, acompañada de recursos locales y de un compromiso real con el desarrollo del ecosistema tecnológico ibérico.

Estamos aquí para desarrollar capacidades locales, trabajar como un único equipo y crecer juntos.



> **El éxito de un fabricante solo es posible cuando también tienen éxito sus socios, sus clientes y la comunidad técnica local**

Actualidad – Te interesa

"La ventaja de VASS es global: anticipamos en España los retos que ya estamos resolviendo en más de 20 países"

Patricio Novoa, Chief Commercial Officer de Industria, Energía, Telco, Media, Products & Retail en VASS

Patricio Novoa, Chief Commercial Officer de Industria, Energía, Telco, Media, Products & Retail en VASS, analiza los retos tecnológicos de las empresas, la importancia de la especialización sectorial y el valor de contar con un socio tecnológico con experiencia internacional.

Regresa a VASS en un momento de transformación para el sector tecnológico. ¿Qué le ha llevado a iniciar esta nueva etapa y cuáles son sus principales objetivos?
Regresar a VASS tiene un significado especial para mí. Es una compañía que conozco bien, en la que he compartido grandes proyectos y, sobre todo, con profesionales a los que admiro.

Pero también regreso porque creo que VASS tiene algo que hoy es especialmente valioso: una trayectoria de más de 25 años en el sector tecnológico, un profundo conocimiento de sus clientes y una dimensión internacional que nos permite desarrollar proyectos en mercados muy diferentes. Mi objetivo es reforzar precisamente esas fortalezas. Estar cada vez más cerca de nuestros clientes, comprender mejor sus



desafíos y conectar todo el conocimiento y las capacidades de VASS con las necesidades reales de sus negocios.

VASS está reforzando su orientación al cliente y su especialización sectorial. ¿Cómo se traducirá esta estrategia en la relación con las empresas?
El modelo de relación entre las empresas y sus socios tecnológicos ha cambiado, y la inteligencia artificial lo ha acelerado. Los clientes ya no buscan a alguien que implante soluciones: buscan a quien entienda su negocio, conozca su industria y les ayude a decidir dónde invertir.

Con la IA, esto es todavía más evidente. Los modelos están al alcance de todos; la diferencia está en saber aplicarlos a los procesos, los datos y la regulación de cada sector. Un agente de IA que optimiza el mantenimiento de una planta industrial no tiene nada que ver con uno que gestiona la atención al cliente de un operador de telecomunicaciones o la previsión de demanda de una energética. Por eso nuestra apuesta es reforzar la especialización sectorial. Queremos hablar el lenguaje de nuestros clientes, entender sus prioridades y llevarles casos de uso de IA que ya han demostrado su valor en su propia industria, no soluciones genéricas.

Es algo que forma parte de nuestra manera de trabajar. Hemos acompañado a grandes organizaciones en distintas etapas de su transformación y hemos construido relaciones basadas en la cercanía y la confianza. La IA no cambia eso; lo hace más necesario.

Actualidad – Te interesa

Patricio Novoa, VASS

La inteligencia artificial está en el centro de las estrategias empresariales. ¿Estamos ante una verdadera transformación o todavía existe demasiada expectativa alrededor de esta tecnología?
Las dos cosas son ciertas. La inteligencia artificial está cambiando la forma de trabajar y de competir de las empresas, pero también ha generado expectativas que no siempre se han traducido en resultados.

Durante los últimos años hemos visto muchas pruebas de concepto y muchos pilotos. Hoy la pregunta en los comités de dirección ya no es qué puede hacer la IA, sino qué está haciendo por mi negocio. Y esa pregunta exige otra forma de abordarla. Ya no se trata de incorporar tecnología porque esté disponible o porque sea tendencia, sino de empezar por el problema: dónde puede aportar valor, qué proceso mejora, cómo se mide su impacto y cómo se lleva de un piloto a la operación real de la compañía.

La inteligencia artificial tiene que dejar de ser una promesa tecnológica para convertirse en una realidad de negocio. A eso, en VASS, lo llamamos Transformación Inteligente.

¿Qué barreras están encontrando las compañías a la hora de trasladar la inteligencia artificial a sus operaciones?
La fase de pruebas ya ha pasado. La mayoría de las grandes compañías ya han comprobado que la IA funciona; el reto ahora es escalarla. Y es ahí donde aparecen las verdaderas barreras.

> **VASS nació en España, pero hoy somos más de 4.000 profesionales con presencia en más de 20 países y operaciones en más de 50**

La primera es que un piloto puede funcionar con datos preparados para la ocasión, pero llevarlo a toda la operación exige datos fiables, integrados y gobernados. Muchas organizaciones descubren en ese momento que su base de datos no está lista.

La segunda son los procesos y las personas. Escalar la IA no es desplegar una herramienta, es rediseñar cómo se trabaja. Si los procesos no cambian y los equipos no se forman, la tecnología se queda en la superficie.

Y la tercera es la gobernanza. Con los agentes de IA, que ya no solo recomiendan sino que actúan, hay que definir quién supervisa, qué se automatiza y cómo se cumple con marcos como el AI Act europeo. Sin eso, ninguna compañía seria escala. El reto ya no es demostrar que la IA funciona, sino hacer que funcione en toda la organización.

VASS es una compañía española con una importante presencia internacional. ¿Qué aporta esa dimensión global a sus clientes?
Es uno de nuestros grandes elementos diferenciales. VASS nació en España, pero hoy somos más de 4.000 profesionales con presencia en más de 20 países y operaciones en más de 50. Esa dimensión no tiene valor por sí misma. Lo que la hace valiosa es el conocimiento que genera. Trabajamos en mercados con distintos niveles de madurez tecnológica, marcos regulatorios y realidades de negocio, y lo que aprendemos en cada uno lo compartimos con todos.

Hay retos que vemos primero en otros mercados y que después llegan a España, y otros en los que España va por delante y esa experiencia la llevamos fuera. Esa circulación del conocimiento nos permite anticiparnos, saber qué funciona y qué no, y evitar que nuestros clientes empiecen de cero.

Ser global no es estar en muchos países, es compartir lo que aprendemos en todos ellos. Y eso nos permite combinar la cercanía de un socio local con las capacidades de una compañía internacional.

Actualidad – Te interesa

Patricio Novoa, VASS

> **Vemos un gran recorrido en casos de uso de IA como el mantenimiento predictivo y la planificación de intervenciones en industria**

¿Podría poner algún ejemplo que refleje esa capacidad de VASS para abordar proyectos complejos a escala internacional?
Trabajamos con grandes compañías e instituciones internacionales en proyectos donde la tecnología resulta estratégica y la capacidad de ejecución es determinante.

Un ejemplo es nuestro trabajo para la OTAN, para la que hemos desarrollado su plataforma digital pública, nato.int, incluyendo capacidades de gestión de activos digitales para sus comunicaciones.

También contamos entre nuestros clientes con compañías como Telefónica, Iberdrola, Repsol y Renault, referentes en sectores muy distintos. Son ejemplos de la diversidad de industrias con las que trabajamos y de la amplitud de los desafíos tecnológicos que conocemos. Junto a ellas, colaboramos con instituciones europeas y otras grandes organizaciones internacionales.

Estas relaciones y proyectos reflejan nuestra capacidad para trabajar en entornos complejos, coordinar equipos internacionales y responder a exigencias de calidad, seguridad y continuidad operativa. La experiencia adquirida en cada sector y mercado nos permite aportar soluciones contrastadas a nuevos desafíos.

La IA necesita datos fiables, procesos integrados y sistemas que ya funcionen. Por eso vemos un gran recorrido en casos de uso como el mantenimiento predictivo y la planificación de intervenciones en industria, la resolución automática de incidencias en telecomunicaciones, la optimización de la operación de activos en energía o la personalización de cada interacción con el cliente en retail.

Para mí, esa es una de las grandes fortalezas de VASS: podemos llevar a cada cliente el conocimiento adquirido en otros mercados y aplicarlo a su evolución hacia la IA. La IA no se construye desde cero: se escala sobre lo que ya funciona.

Es responsable de verticales como Industria, Energía, Telecomunicaciones, Media y Retail. ¿Qué necesidades tecnológicas comparten estos sectores y dónde están sus principales diferencias?
Más que por sectores, yo los analizaría por su modelo de relación con el cliente, porque ahí están los denominadores comunes.

En los negocios B2C, como el retail o la comercialización de energía, el consumidor está en el centro y el reto es conocerlo, personalizar cada interacción y fidelizarlo. En los B2B, como la industria, la prioridad es la eficiencia, la fiabilidad de los activos y la relación a largo plazo. Y en los B2B2C, como el gran consumo, el reto es conocer al consumidor final sin ser dueño de la venta, colaborando con la distribución y aprovechando mejor los datos.

Pero la realidad es cada vez más híbrida. Las operadoras de telecomunicaciones encuentran hoy su mayor potencial de crecimiento en el negocio con empresas. Los medios viven a la vez de su audiencia y de sus anunciantes. Y en energía, cada vez más clientes, sobre todo empresas, ya no solo consumen energía: también la producen.

Y hay algo que lo cambia todo: el cliente B2B ya espera una experiencia digital y fluida como la del B2C, y el negocio B2C necesita la eficiencia operativa del B2B para proteger su margen. Ese cruce es hoy el gran denominador común, y es ahí donde la IA y los datos marcan la diferencia.

Actualidad – Te interesa

Patricio Novoa, VASS

En un mercado tan competitivo, ¿qué debe ofrecer una consultora tecnológica para diferenciarse?
Creo que el sector de la consultoría tecnológica tiene que hacer autocrítica. Durante años hemos hablado demasiado de capacidades, plataformas y tecnologías, y poco de los problemas que realmente necesitaban resolver nuestros clientes. Hoy el mercado exige resultados y una comprensión mucho más profunda del negocio.

Para mí, la diferenciación se construye sobre tres factores: conocimiento del negocio, capacidad de ejecución y confianza. La tecnología es imprescindible; lo decisivo es entender las prioridades del cliente y acompañarle desde la identificación del problema hasta el resultado.

Y hay otro factor que para mí es clave: la capacidad de simplificar. En VASS hablamos de Complex Made Simple, y no es un claim de marca, es una forma de trabajar. Las organizaciones ya conviven con suficiente complejidad: sistemas heredados, regulación, presión sobre costes y, ahora, la IA. Nuestro papel es hacer que la tecnología sea más sencilla de adoptar, de integrar y, sobre todo, de convertir en resultados. Simplificar lo complejo no significa hacer menos, sino saber hacer mejor las cosas.

La velocidad del cambio tecnológico obliga a las empresas a tomar decisiones constantemente.

> **Parece increíble, pero todavía hay organizaciones que eligen primero una tecnología y después buscan dónde aplicarla. Eso lo hemos visto con la IA**

¿Cómo pueden evitar invertir en tecnologías que no aporten valor?
Empezando por el problema y no por la tecnología. Parece evidente, pero todavía hay organizaciones que eligen primero una tecnología y después buscan dónde aplicarla. Con la IA lo hemos visto mucho: pilotos que funcionan, pero que no responden a una prioridad real del negocio y nunca llegan a escalar. El proceso tiene que ser el contrario: identificar el problema, entender su impacto y elegir la solución más adecuada. Y definir desde el principio cómo se va a medir el éxito. Si el objetivo es mejorar la productividad, reducir tiempos o aumentar ingresos, los indicadores tienen que estar claros antes de invertir, no después.

En un contexto en el que aparecen nuevas tecnologías cada semana, contar con un socio que aporte criterio es tan importante como contar con capacidades técnicas.

Para terminar, ¿qué le gustaría que los clientes identificaran con esta nueva etapa de VASS?
Queremos que nuestros clientes sepan que, cuando trabajan con VASS, tienen a su lado un equipo que conoce su negocio y que puede aportarles la experiencia de proyectos desarrollados en distintos países e industrias.

Es algo que forma parte de nuestra identidad y que nuestros clientes conocen y valoran. Muchas de nuestras relaciones se han construido acompañándoles durante años, respondiendo a nuevos retos y demostrando resultados.

Muchos de los desafíos que hoy empiezan a plantearse en España ya los hemos abordado en otros mercados. Esa experiencia nos ayuda a anticiparnos, reducir riesgos y llegar antes a soluciones que funcionan.

Para mí, esa es una de las grandes ventajas de trabajar con VASS: sumar el conocimiento internacional a la cercanía y al compromiso de un equipo que entiende las necesidades de cada cliente.

Actualidad – Te interesa

MyQ X 10.3: un nuevo paso en la digitalización de los flujos de trabajo



La digitalización no consiste solo en pasar los documentos del papel al formato digital. Se trata de facilitar las tareas cotidianas, ayudar a las personas a trabajar de forma segura y reducir el tiempo dedicado a los procesos rutinarios. La impresión y el escaneado siguen formando parte de este proceso y deben facilitar la forma de trabajar de las personas, no convertirse en un obstáculo.

MyQ ayuda a las organizaciones a gestionar la impresión y los flujos de trabajo documentales en oficinas y entornos de trabajo híbridos. Gracias a las experiencias de usuario personalizadas, la liberación segura de los trabajos de impresión y los flujos de escaneados prácticos, los empleados pueden acceder a las funciones que necesitan sin complicaciones innecesarias. Al mismo tiempo, los equipos de TI pueden gestionar los dispositivos, los usuarios y la actividad de impresión desde un sistema centralizado.

MyQ X 10.3 amplía esta base con nuevas funciones que responden a los retos cotidianos relacionados con los documentos y facilitan los siguientes pasos en la digitalización de los flujos de trabajo.

Con MyQ Document Processor, los documentos escaneados pueden procesarse directamente desde los flujos de escaneado de MyQ X. La solución permite aplicar OCR, convertir documentos a formatos como Word y Excel, separar archivos y eliminar páginas en blanco. Estas funciones pueden reducir la manipulación manual después del escaneado y ayudar a los empleados a preparar los documentos para la siguiente fase de su trabajo.

Para las organizaciones que necesitan un mayor control sobre la digitalización, Scan Review incorpora un paso de verificación antes de archivar los documentos. Los revisores autorizados pueden comprobar los documentos escaneados y sus metadatos, aprobarlos o rechazarlos y contribuir a un proceso controlado de creación de registros digitales. Esto resulta especialmente relevante cuando la integridad y la trazabilidad de los documentos son importantes.

Release Station responde a otro reto del entorno de trabajo. No todas las impresoras disponen de un terminal MyQ integrado, pero eso no significa que deban quedar fuera de un sistema de liberación controlada de trabajos de impresión. A través de una interfaz web, los usuarios pueden autenticarse, seleccionar una impresora y liberar los trabajos que ya han enviado a imprimir. MyQ X 10.3 también incorpora una compatibilidad mejorada con Windows Protected Print (WPP) mediante IPP pass through, que permite utilizar funciones compatibles de los dispositivos, como el grapado y la perforación, al imprimir con Windows Protected Print.

Estas funciones responden a necesidades diferentes, pero comparten un objetivo práctico: ayudar a las organizaciones a gestionar los procesos documentales con mayor control y, al mismo tiempo, facilitar las tareas cotidianas de los empleados.

Digitalizar no significa eliminar la impresión del entorno de trabajo. Significa asegurarse de que la impresión y el escaneado se integren en la forma en que las personas trabajan, reduciendo la manipulación innecesaria y aplicando los controles adecuados a los documentos.

Actualidad – Te interesa

Seidor obtiene la AWS Migration & Modernization Competency

El reconocimiento valida la experiencia técnica de SEIDOR y su éxito demostrado con clientes en proyectos de migración y modernización cloud sobre Amazon Web Services (AWS)

La consultora tecnológica SEIDOR ha obtenido la AWS Migration and Modernization Competency, un reconocimiento a su experiencia técnica y al éxito demostrado con clientes en proyectos de migración y modernización cloud. Esta competencia de AWS valida la especialización de la compañía en proyectos de migración de alto volumen y alta exigencia técnica.

Esta competencia reconoce la capacidad de SEIDOR para acompañar a las organizaciones en iniciativas de adopción cloud que implican un elevado volumen de servidores, aplicaciones y cargas de trabajo. Valida la experiencia de la compañía desde el assessment inicial y la definición de la estrategia hasta la planificación, ejecución, operación y optimización de entornos sobre AWS.

La obtención de la AWS Migration and Modernization Competency permite a SEIDOR acceder a fondos del Migration Acceleration Program (MAP), así como a soporte técnico especializado y recursos específicos. Esto ayuda a estructurar el proceso de adopción, priorizar las cargas de mayor impacto y alinearse con el marco AWS MAP.

La adopción cloud implica revisar arquitecturas, dependencias entre sistemas, modelos de seguridad, continuidad operativa, gobierno del dato y criterios de eficiencia de costes. La obtención de la AWS Migration and Modernization Competency posiciona a SEIDOR como AWS Partner con experiencia especializada para ayudar a los clientes a adoptar la nube y transformar sus aplicaciones, reducir costes de licencias, optimizar costes operativos y mejorar rendimiento, agilidad y resiliencia.

La obtención de la AWS Migration and Modernization Competency se suma al estatus AWS Premier Tier Services Partner y a la AWS DevOps Competency, reforzando su



Actualidad – Te interesa

Seidor obtiene la AWS Migration & Modernization Competency

especialización en AWS. La relación de SEIDOR con AWS refleja un compromiso sostenido con el desarrollo de capacidades avanzadas en cloud, automatización, operaciones, migración y gestión de entornos tecnológicos a escala.

Según Eduard Bonet, Director de Cloud & IT Infrastructure en SEIDOR, "la AWS Migration and Modernization Competency confirma la madurez de nuestra práctica cloud y la capacidad de nuestros equipos para abordar migraciones de gran volumen con una metodología contrastada. Para nuestros clientes, supone poder avanzar hacia la nube con el soporte técnico de SEIDOR como AWS Partner validado y acceder a herramientas, beneficios y programas específicos que les permiten afrontar estos proyectos con mayor seguridad, planificación y continuidad operativa".



Migración cloud en entornos críticos

La migración cloud requiere combinar visión estratégica y ejecución técnica. En muchos casos, las organizaciones deben decidir qué cargas deben migrarse, cuáles necesitan modernizarse antes de avanzar, qué aplicaciones requieren una evolución progresiva y qué sistemas deben permanecer en modelos híbridos durante un periodo de transición.

El enfoque de SEIDOR incluye servicios especializados de assessment, diseño de arquitecturas cloud, construcción de landing zones, migración de aplicaciones, automatización de despliegues, observabilidad, FinOps, seguridad y resiliencia operativa. Esto ayuda a estructurar el proceso de adopción, reducir la incertidumbre técnica y acompañar a los clientes desde la fase de análisis hasta la operación recurrente.

> **La obtención de la competencia demuestra la capacidad de SEIDOR para trabajar con organizaciones que necesitan evolucionar sus plataformas**

La obtención de la AWS Migration and Modernization Competency demuestra la capacidad de SEIDOR para trabajar con organizaciones que necesitan evolucionar sus plataformas tecnológicas sin comprometer la continuidad del negocio. Para ello, SEIDOR combina metodología, equipos certificados, conocimiento sectorial y experiencia acumulada en proyectos internacionales.

La relación de SEIDOR con AWS desde 2016

SEIDOR empezó a trabajar con AWS en 2016. Desde entonces, la compañía ha obtenido la AWS IoT Competency, la AWS DevOps Competency, la AWS SAP Competency y la AWS Migration and Modernization Competency, reforzando su especialización en AWS. SEIDOR también participa en el AWS Solution Provider Program y en el AWS Well-Architected Partner Program.

SEIDOR ha completado más de 800 proyectos para más de 300 clientes en AWS, cuenta con más de 150 certificaciones oficiales de AWS en sus equipos profesionales y con más de 10 programas, competencias y validaciones de servicios de AWS.

Comida BYTE TI

Cómo escalar la IA conectando datos, procesos y tecnología



Alfonso Casas

Las empresas afrontan el reto de llevar la inteligencia artificial más allá de los proyectos piloto, con modelos que garanticen seguridad, control de costes y retorno de inversión.

La inteligencia artificial (IA) se ha convertido en una prioridad empresarial, pero trasladar sus capacidades a los procesos críticos y extender su uso a toda la organización continúa planteando importantes desafíos. La fragmentación de los datos, la gobernanza, la ciberseguridad y el control de los costes son algunos de los obstáculos que deben superar las compañías para obtener resultados tangibles.

Para analizar estos retos, Byte TI organizó un almuerzo en colaboración con Appian en el que participaron Miguel Amérigo, jefe corporativo de I+D e Innovación en OHLA; Ángel Nebrera, Broad Markets Senior Account Executive en Appian; Manuel Miranda, director de IT en FCC; Juan Luis Blasco, director of IT Operations en Acciona; David Gómez, Broad Markets Account Executive en Appian; Juan Pedro Gozalo, Head of Hyperautomation en entidad financiera; y Laura Baus, CISO en Vodafone. Manuel Navarro, director de Byte TI, moderó el encuentro.

Nebrera abrió el debate explicando que Appian desarrolla plataformas para integrar inteligencia artificial, datos y procesos, con el objetivo de mejorar la eficiencia operativa y trasladar ese impacto a los resultados empresariales. Desde su perspectiva, la IA aislada difícilmente alcanza todo su potencial. "Para que aporte valor, debe tener datos y procesos a su alrededor", señaló. La compañía apuesta por incorporar estas capacidades a las automatizaciones empresariales para resolver problemas concretos.

David Gómez coincidió en que el objetivo no consiste en incorporar IA por el mero hecho de hacerlo, sino en ayudar a las organizaciones a resolver grandes desafíos mediante una plataforma que permite diseñar, automatizar y optimizar procesos de principio a fin. La clave está en conseguir que la tecnología funcione

Comida BYTE TI

Cómo escalar la IA conectando datos, procesos y tecnología



Ángel Nebrera,
Broad Markets Senior Account Executive en Appian



David Gómez,
Broad Markets Account Executive en Appian



Juan Luis Blasco,
director of IT Operations en Acciona



Juan Pedro Gozalo,
Head of Hyperautomation en entidad financiera

dentro de la operativa empresarial y pueda escalar con garantías.

De la experimentación al despliegue empresarial

La primera cuestión planteada fue en qué punto se encuentran las compañías en la adopción de la IA y cuáles son las principales barreras para extender su utilización. Aunque las organizaciones han avanzado a ritmos diferentes, todas comparten la necesidad de pasar de los proyectos experimentales a soluciones sostenibles.

Juan Pedro Gozalo explicó que ya disponen de algunos proyectos en producción y han definido un marco normativo para gobernar el uso de la IA. En el sector financiero, la regulación y las reglas internas condicionan especialmente su implantación. La entidad trabaja con distintas soluciones y apuesta por combinar modelos en función de las necesidades de cada proceso. El siguiente paso pasa por revisar la operativa interna para identificar oportunidades de automatización y avanzar hacia modelos agénticos.

En OHLA, Miguel Amérigo describió una evolución desde los primeros pilotos, iniciados tras la aparición de ChatGPT, hasta una estrategia corporativa más estructurada. En 2025, la compañía unificó sus líneas de trabajo para coordinar la implantación y el despliegue tecnológico de estas iniciativas.

Su estrategia se articula en tres ejes. El primero, denominado "cimientos", se centra en la productividad cotidiana, con herramientas como Microsoft Copilot y acciones de formación que han involucrado a más de 1.000 personas. El segundo aborda la hibridación de procesos y la construcción de una plataforma agéntica gobernada. El tercero reúne proyectos de IA avanzada vinculados a necesidades específicas, como la gestión de residuos, la economía circular o el diseño generativo.

Amérigo destacó que la principal dificultad ya no consiste en encontrar aplicaciones potenciales, sino en escalarlas. "El problema no es identificar casos de uso. Ahora la barrera está en el tema de costes y gestión", afirmó. Convertir una prueba en una solución corporativa exige resolver cuestiones relacionadas con los accesos, la seguridad, la reutilización de componentes y los modelos de consumo.

En FCC, Manuel Miranda subrayó que innovación

Comida BYTE TI

Cómo escalar la IA conectando datos, procesos y tecnología



Laura Baus,
CISO en Vodafone



Manuel Miranda,
director de IT en FCC



Miguel Amérigo,
jefe corporativo de I+D e Innovación en OHLA

y tecnología trabajan integradas en el mismo equipo. La compañía ha establecido un marco de gobierno y un comité de IA, y durante los últimos doce meses ha avanzado en la transformación de procesos. No obstante, señaló dos dificultades: establecer mecanismos de control adecuados y priorizar los proyectos con criterios que permitan medir el valor aportado.

Juan Luis Blasco, por su parte, puso el foco en la adopción por parte de los empleados. "Mientras algunos incorporan estas herramientas con naturalidad, otros se muestran más reticentes", señala. Desde su experiencia en Acciona, considera necesario reforzar la ingeniería de software alrededor de la IA y formar a los equipos de negocio para que puedan identificar oportunidades, acelerar sus ideas y convertirlas en soluciones reales.

Gobierno y ciberseguridad, condiciones para escalar

La extensión de la IA multiplica las posibilidades de automatización, pero también los riesgos derivados de un uso descontrolado. La gobernanza se convirtió así en uno de los principales ejes de la conversación, especialmente al abordar cómo facilitar la innovación sin perder el control corporativo.

Laura Baus, CISO de Vodafone, explicó que la compañía trabaja en la mejora de procesos y en la incorporación de agentes de IA, aunque considera que los desafíos más complejos en materia de ciberseguridad están todavía por llegar. La capacidad de estas tecnologías para potenciar los ataques obliga a preparar las infraestructuras y revisar los procedimientos de defensa.

"La IA se tiene que atajar con IA", afirmó Baus, quien defendió la integración de la monitorización en la operativa para identificar amenazas y gestionar las actualizaciones de seguridad con el menor impacto posible en el negocio. También reclamó que los equipos de seguridad participen desde el principio en los proyectos, de manera que los desarrolladores dispongan de componentes seguros para construir soluciones sin dejar la protección para el final.

La preocupación no se limita a los ataques externos. El uso de herramientas de IA ajenas al entorno corporativo puede provocar filtraciones por desconocimiento o negligencia. Miranda advirtió de que, en actividades como la gestión medioambiental y del agua, las empresas manejan información especialmente sensible y relevante. Aunque los ciberataques le preocupan, considera que las fugas provocadas por malas prácticas de los empleados representan un riesgo igualmente importante.

Amérigo coincidió en la necesidad de reforzar la responsabilidad individual. No todos los trabajadores son conscientes de las implicaciones de introducir información corporativa en herramientas externas. Por ello, OHLA trabaja en difundir normas internas sencillas y fáciles de comprender. Además, cuando un agente

Comida BYTE TI

Cómo escalar la IA conectando datos, procesos y tecnología

desarrollado por un empleado empieza a utilizarse en otros departamentos, resulta necesario incorporarlo a una plataforma que permita gobernarlo, compartirlo y controlar su uso.

Miranda añadió que cualquier solución que vaya a extenderse a más empleados debe someterse a regulación interna y certificación. La intervención de TI es fundamental para comprobar que cumple las normas, evitar duplicidades y garantizar su mantenimiento.

Gozalo defendió que las reglas de uso, la ciberseguridad, el cumplimiento normativo y la arquitectura deben definirse antes de implantar las soluciones. "La supervisión humana también resulta imprescindible cuando la IA interviene en procesos productivos con consecuencias relevantes" puntualizó.

Nebrera señaló que las plataformas con mecanismos de control o guardrails permiten desarrollar soluciones con rapidez y seguridad. También advirtió de que la IA agrava un problema conocido por las empresas: el shadow IT, es decir, el uso de tecnologías fuera del control de los equipos responsables. Disponer de herramientas gobernadas y procesos orquestados ayuda a reducir tiempos y mantener una visión común de las iniciativas.

Blasco añadió que las capacidades de los usuarios han crecido de manera extraordinaria, por lo que las empresas necesitan mecanismos de control ágiles. No se trata solo de proteger los datos, sino también de evitar que distintos equipos desarrollen aplicaciones que resuelvan los mismos problemas sin coordinarse.

El consenso fue que no se debe frenar la experimentación, sino establecer un marco que permita desarrollarla con garantías. Cuando una solución pasa a producción, TI debe asumir el control necesario para asegurar su protección, mantenimiento y aprovechamiento transversal.

Los datos, la base para conectar procesos

La orquestación de los datos fue otro de los asuntos centrales del almuerzo. La fragmentación de la información y la existencia de sistemas aislados siguen dificultando la implantación de soluciones que necesitan acceder a datos procedentes de distintas áreas.

Miranda aseguró que FCC ha avanzado en la eliminación de silos, aunque se trata de un proceso continuo que exige combinar tecnología y gobierno. A su juicio, la IA ha contribuido a que esta necesidad llegue a los consejos de dirección y administración. La expectativa de aprovechar sus capacidades ha impulsado la toma de conciencia sobre la importancia de organizar la información.

Blasco señaló que, en organizaciones complejas como Acciona, cada proyecto puede requerir distintas formas de visualizar y consumir los datos. Por eso, las soluciones deben adaptarse a la realidad de cada proceso.

Interoperabilidad y coordinación de agentes

Desde Appian, Gómez explicó que la plataforma de la compañía permite conectar fuentes de datos sin obligar necesariamente a trasladarlas a un nuevo repositorio. La propuesta consiste en mantener la información donde se encuentra y facilitar su lectura y escritura desde los procesos que necesitan utilizarla. Así, las empresas pueden combinar fuentes y construir soluciones sin afrontar siempre una migración previa.

Gómez también destacó la posibilidad de crear aplicaciones para gestionar y normalizar los datos, una necesidad habitual cuando la información se ha generado durante años en sistemas diferentes. Gozalo explicó que trabajan en la clasificación y normalización de documentos y ficheros con nomenclaturas distintas para datos equivalentes. El objetivo es facilitar su explotación y mejorar la eficiencia mediante procesos centralizados.

Comida BYTE TI

Cómo escalar la IA conectando datos, procesos y tecnología

Para Gozalo, el dato constituye el núcleo de cualquier estrategia de IA. Identificar la información disponible, determinar cuál resulta útil y establecer cómo explotarla de forma automatizada son pasos imprescindibles, siempre dentro de los límites de seguridad y cumplimiento.

La evolución hacia modelos agénticos añade una nueva dimensión al desafío. Gómez señaló que Appian trabaja en la orquestación de agentes y en su comunicación con otras plataformas, en un escenario en el que deberán convivir soluciones de distintos fabricantes. La interoperabilidad será relevante para coordinar las capacidades de los agentes y conseguir que la automatización funcione de extremo a extremo.

Aunque la IA puede asumir una parte creciente del desarrollo y de tareas como la clasificación documental, Gozalo recordó que el conocimiento humano sigue siendo necesario para supervisar los resultados y evitar riesgos. La velocidad de generación no debe confundirse con la ausencia de controles.

Escalabilidad y costes: medir el valor de la IA

La última parte del debate abordó una cuestión decisiva para pasar de las pruebas a la producción: cuánto cuesta utilizar la IA y cómo garantizar que la inversión responde a una necesidad real.

Gozalo identificó el control del consumo como un asunto estratégico. Los cambios de versión de los modelos de lenguaje pueden mejorar los resultados, pero también incrementar notablemente el coste de los tokens. Por ello, las empresas deben evaluar las prestaciones y el impacto económico antes de decidir si una actualización justifica el gasto.

Amérigo destacó las diferencias entre los modelos de suscripción y el pago por uso, y apuntó que este último podría ganar peso en los próximos años. En ese escenario, TI deberá comprobar que las soluciones utilizan los recursos de forma eficiente. La disponibilidad de una capacidad no implica que deba implantarse en todos los procesos: cada decisión debe responder a una aportación de valor concreta.

Nebrera explicó que Appian presta atención tanto al valor generado como al consumo de cada caso de uso, con el objetivo de construir un business case sólido. Gómez añadió la importancia de ofrecer las capacidades de IA de forma controlada, con previsiones de consumo y límites que permitan anticipar las necesidades del servicio.

Para terminar el almuerzo, los asistentes fueron preguntados por qué le pedirían a Appian si dispusieran de presupuesto ilimitado, a lo que Gozalo reclamó una plataforma capaz de trabajar con cualquier modelo de IA, medir el consumo, integrar las capacidades en los procesos automatizados y gestionar los datos sin necesidad de migrarlos. La flexibilidad tecnológica y el acceso a la información son, desde su perspectiva, condiciones esenciales para obtener buenos resultados.

Amérigo, por su parte, pidió mejorar la eficiencia de los agentes y abordar la escalabilidad desde una perspectiva de cartera de proyectos, en lugar de estudiar cada iniciativa de forma aislada. Gestionar los casos como un conjunto permitiría reutilizar capacidades y aprovechar sinergias.

El almuerzo dejó diversos mensajes de gran calado: el futuro de la IA empresarial no dependerá únicamente de la potencia de los modelos, sino de la capacidad de conectarlos con los datos y los procesos, gobernar su utilización y demostrar su impacto. Para las organizaciones, el verdadero salto consiste en convertir las experiencias aisladas en soluciones seguras, escalables y sostenibles. En ese camino, la colaboración entre negocio y tecnología, la calidad de la información y el control de los costes serán tan importantes como la propia inteligencia artificial y el socio tecnológico que se elija para recorrer el camino.

Comida BYTE TI

Automatizar procesos: del ahorro de costes a la transformación del negocio

Alfonso Casas

Automatizar ya no consiste solo en acelerar tareas o reducir costes, sino en transformar procesos completos sin perder el control, la gobernabilidad, la seguridad y el conocimiento de las personas



La automatización de procesos ha dejado de ser una iniciativa exclusivamente tecnológica para convertirse en una herramienta estratégica con la que las organizaciones buscan mejorar su eficiencia, reducir errores y ganar agilidad. La incorporación de la inteligencia artificial, además, está ampliando las posibilidades de actuación, desde la ejecución de tareas repetitivas hasta la coordinación de flujos de trabajo que implican a diferentes departamentos, aplicaciones y equipos humanos. Sin embargo, esta evolución también plantea nuevos desafíos: cómo elegir qué automatizar, justificar las inversiones, garantizar la calidad del dato y escalar las iniciativas sin perder el control.

Estas cuestiones centraron el almuerzo organizado por la revista Byte TI en colaboración con Appian y Entelgy, en el que nueve expertos de Airbus, Atrevia, Iberpay, Ferrovial, IE University, Merck Group y Unicaja compartieron sus experiencias y debatieron sobre los principales retos de esta transformación. Una de las conclusiones fue que automatizar no consiste simplemente en incorporar herramientas, sino en revisar cómo trabaja la organización y qué valor espera obtener de cada iniciativa.

David Gómez, Broad Markets Account Executive de Appian, destacó la importancia de escuchar las necesidades reales de las compañías para abordar esta transformación. Por su parte, David Escribano, líder técnico de RPA en Entelgy, recordó que la automatización lleva años evolucionando desde la automatización robótica de procesos (RPA) hasta la inteligencia artificial. "Pese a que tenemos mucha experiencia, aprendemos todos los días", señaló, poniendo de relieve la necesidad de conocer las

Comida BYTE TI

Automatizar procesos: del ahorro de costes a la transformación del negocio



Carlos Garriga,
CIO en IE University



David Escribano,
Líder técnico de RPA en Entelgy



David Gómez,
Broad Markets Account Executive en Appian



Javier Valero,
Responsable de monitorización y automatización en Iberpay

preocupaciones actuales de las empresas antes de plantear soluciones.

Eficiencia, valor y resiliencia: qué automatizar primero

El primer desafío consiste en identificar los procesos que pueden beneficiarse de la automatización y establecer prioridades. Aunque el ahorro de costes sigue siendo un factor relevante, las organizaciones participantes coincidieron en que no debe ser el único criterio para decidir dónde invertir.

Luis Miguel del Sanz, Digital Project Leader en Airbus, explicó que la compañía persigue tres objetivos fundamentales: "la eficiencia en el coste, hacer las cosas más rápido y siempre de forma segura". En una organización con numerosas áreas y actividades, su experiencia apunta a que resulta más sencillo automatizar aquellos procesos que dependen de una única organización, mientras que las iniciativas que requieren coordinar a diferentes entidades presentan mayores dificultades. Por ello, Airbus está priorizando los procesos internos.

Mario Robledo, director de Infraestructuras y Proyectos de Global IT en Atrevia, resumió su planteamiento con una idea: "Intentamos automatizar todo aquello que pueda dar valor a los puestos". El objetivo, por tanto, no es incorporar tecnología por sí misma, sino liberar recursos y facilitar el trabajo de los profesionales.

En IE University, la prioridad es eliminar fricciones para mejorar la experiencia de alumnos y profesores. Carlos Garriga, CIO de la institución, explicó que la automatización permite reducir tareas repetitivas y dedicar más tiempo a actividades de valor añadido. Para seleccionar los proyectos, la universidad tiene en cuenta tres variables: el impacto, la viabilidad y la posibilidad de extender la solución al conjunto de la organización. "Que sea algo que escale y que se pueda extender a toda la organización y que no se quede en algo de nicho", precisó.

La perspectiva cambia en sectores donde la continuidad operativa resulta crítica. Javier Valero, responsable de monitorización y automatización en Iberpay, situó la resiliencia por delante de otros criterios: "Para nosotros es lo más importante, antes de buscar casos de negocio". La compañía debe garantizar el funcionamiento de los sistemas que sustentan los pagos, por lo que prevenir interrupciones y reducir los riesgos operacionales constituye una prioridad.

Comida BYTE TI

Automatizar procesos: del ahorro de costes a la transformación del negocio



Luis Miguel del Sanz,
Digital Project Leader. IPT RFE DDMSn en Airbus



Maica Aguilar,
IT Security IT & Innovation en Ferrovial



Mario Robledo,
Director de Infraestructuras y Proyectos Global IT en Atrevia



Raquel García, IT Head Global Pharma Manufacturing & Country Head Spain en Merck Group

En la industria farmacéutica, la automatización también está ligada a la calidad y al servicio al paciente. Raquel García, IT Head Global Pharma Manufacturing & Country Head Spain de Merck Group, destacó la necesidad de reducir el tiempo de llegada al mercado, mantener la calidad del producto y mejorar la eficiencia de las plantas. "Todo lo que sea automatizar también permite reducir el coste final del producto", afirmó. A ello se suma la posibilidad de controlar mejor los procesos y disponer de información que ayude a optimizar las operaciones.

Maica Aguilar, responsable de IT Security, IT e Innovation en Ferrovial, coincidió en la importancia de reducir tiempos y errores, y señaló que la compañía ya tiene procesos de facturación automatizados con Appian. Su experiencia refleja cómo la automatización se está extendiendo desde tareas concretas hacia diferentes ámbitos de la actividad empresarial.

El retorno no siempre se mide en euros

Una vez identificadas las oportunidades, la siguiente cuestión es cómo justificar la inversión. El ahorro económico sigue siendo importante, pero los participantes advirtieron de que algunos proyectos ofrecen beneficios difíciles de cuantificar a corto plazo.

García explicó que hay iniciativas cuya rentabilidad directa no resulta sencilla de demostrar, pero que proporcionan una base para mejorar la eficiencia de las plantas y analizar mejor la información. Por ello, la evaluación debe considerar tanto los resultados económicos como el valor estratégico de disponer de mejores herramientas y procesos.

Escribano defendió una aproximación similar desde Entelgy. "Para algunos proyectos y procesos que no superan el umbral de recuperación, entramos a valorar otros costes cualitativos", explicó. Entre ellos figuran la mejora de la información disponible, el impacto en los usuarios y la conservación del conocimiento dentro de la organización. Este último aspecto cobra especial relevancia cuando los procesos cambian y parte de la experiencia acumulada puede perderse.

En Iberpay, Valero señaló que la decisión también depende de la evaluación de los riesgos operacionales y reputacionales. Cuando los indicadores muestran una exposición elevada, la reducción del riesgo puede prevalecer sobre el beneficio económico inmediato.

El criterio, por tanto, debe combinar el retorno

Comida BYTE TI

Automatizar procesos: del ahorro de costes a la transformación del negocio

financiero con la continuidad del negocio, la calidad, la seguridad y la capacidad de mejorar las operaciones. Una automatización puede no ofrecer un ahorro inmediato significativo y, sin embargo, resultar necesaria para evitar interrupciones o preparar a la empresa para futuras transformaciones.

El dato y los procesos, la base de la IA

La expansión de la IA está poniendo de manifiesto una dificultad que las organizaciones arrastran desde hace años: disponer de datos suficientes no garantiza que estos tengan la calidad ni la estructura necesarias para mejorar las decisiones. Además, antes de automatizar es imprescindible comprender cómo se ejecuta realmente cada proceso.

Robledo insistió en la importancia de la calidad de la información y de establecer un buen sistema de gobierno del dato. García, desde IE University, apuntó que, en su experiencia, "tenemos mejor calidad del dato que la calidad de los procesos". A su juicio, estos últimos suelen ser más difusos de lo que las organizaciones creen, lo que dificulta su automatización.

En Merck Group, la acumulación histórica de información también plantea problemas. "Con big data lo hemos ido acumulando, pero de forma que no está pensado para generar una aportación clave", explicó García. La compañía necesita identificar los procesos completos y no limitarse a automatizar tareas aisladas. En el ámbito farmacéutico, además, el uso de IA introduce exigencias adicionales de validación, debido a la naturaleza de los productos y a los requisitos que deben cumplir los procesos.

La gobernabilidad también plantea una cuestión organizativa: quién debe decidir qué se automatiza y cómo se supervisa. Merck combina la iniciativa de negocio con la supervisión tecnológica, mientras que IE University mantiene un modelo descentralizado en el que las áreas identifican sus necesidades. La institución, sin embargo, centraliza la identificación de sinergias y oportunidades que puedan aprovecharse en diferentes departamentos.

Para Gómez, la relación entre procesos, datos e IA resulta inseparable. "Sin datos no hay un buen resultado de IA", advirtió. Y añadió que, sin procesos bien definidos, la tecnología puede no generar las eficiencias esperadas. La propuesta de Appian pasa por coordinar los flujos de trabajo y conectar las tareas humanas, las robóticas y las ejecutadas mediante inteligencia artificial, con mecanismos de supervisión y gobernabilidad.

Escribano coincidió en que el primer paso debe ser normalizar y definir el proceso completo. Solo entonces es posible decidir qué actividades conviene resolver mediante RPA, cuáles pueden beneficiarse de la IA y en qué puntos debe intervenir una persona para validar el resultado. Su visión apunta a un entorno de trabajo en el que los profesionales coordinen diferentes agentes tecnológicos para completar un flujo de principio a fin.

Garriga considera que este enfoque representa una evolución relevante: "El siguiente salto es el proceso como contexto. El proceso como contexto va a ser clave para que la IA trabaje mejor y sea más eficiente".

Orquestar para transformar, no para añadir más herramientas

La complejidad aumenta cuando un proceso atraviesa múltiples aplicaciones y departamentos. En estos escenarios, las organizaciones pueden acabar recurriendo a hojas de cálculo, correos electrónicos y tareas manuales para cubrir las carencias de integración entre sistemas.

Del Sanz advirtió de que parte del conocimiento especializado sobre los procesos se está perdiendo. Cuando las herramientas corporativas no permiten ejecutar las operaciones de la manera esperada, los profesionales recurren a soluciones improvisadas y al método de prueba y error. El reto consiste en utilizar la IA para simplificar los

Comida BYTE TI

Automatizar procesos: del ahorro de costes a la transformación del negocio

procedimientos sin sacrificar su robustez.

Gómez señaló que la creciente fragmentación de los procesos entre aplicaciones hace necesario recuperar la visión de conjunto. La minería de procesos puede ayudar a diagnosticar cómo trabaja una organización, pero el análisis por sí solo no transforma la operativa. Desde Appian, la alternativa consiste en incorporar una capa que permita coordinar los sistemas existentes y ejecutar los procesos de forma unificada.

Como ejemplo, expuso el caso de una empresa que tardaba seis meses en abrir una nueva tienda. El problema no residía únicamente en las tareas más complejas, sino también en actividades básicas y en la comunicación entre departamentos, que se gestionaba mediante correos electrónicos difíciles de seguir. Al coordinar el proceso, la compañía consiguió reducir en dos meses el tiempo necesario para abrir nuevos establecimientos. La experiencia ilustra que una parte importante de las ineficiencias no procede de la ausencia de aplicaciones, sino de la falta de coordinación entre ellas.

Elegir proveedor y escalar sin perder el control

La elección de un proveedor debe responder a las necesidades reales del negocio y a las características del proceso que se pretende transformar. Para Del Sanz, de Airbus, los criterios principales son "la efectividad en el proceso de innovación" y, a continuación, la seguridad y la calidad. Valero volvió a situar la resiliencia como un requisito prioritario, especialmente en actividades donde una interrupción puede afectar a servicios esenciales.

Desde Merck, García destacó la importancia del conocimiento sectorial. La experiencia previa del proveedor en la industria farmacéutica y su capacidad para proponer nuevas formas de trabajar son elementos relevantes a la hora de evaluar una solución.

También resulta fundamental determinar cómo extender los proyectos a otras áreas sin perder la gobernabilidad. Escribano señaló que el conocimiento humano debe mantenerse para supervisar los procesos, mientras que García defendió la existencia de un órgano de decisión que recoja las opiniones de los equipos implicados y controle que las iniciativas mantengan su finalidad.

La recomendación es avanzar con objetivos claros y demostrar el valor antes de ampliar el despliegue. Gómez relató el caso de una empresa presente en siete países que quería acelerar el cierre contable. En lugar de sustituir sus sistemas SAP, la iniciativa comenzó en uno de los países, optimizando la forma en que los empleados introducían datos y ejecutaban tareas manuales. Los resultados permitieron conseguir el respaldo necesario para extender la solución al resto de las geografías.

"Si hay valor se esponsoriza, de lo contrario, no se esponsoriza", resumió Gómez. La experiencia muestra que una prueba de concepto puede servir para validar una transformación concreta y generar apoyo interno. García puntualizó que, en su organización, estas pruebas se realizan sobre el proceso que se quiere automatizar, no únicamente sobre la tecnología.

No obstante, escalar no significa reproducir indiscriminadamente una solución. Cada organización debe identificar qué elementos pueden compartirse y cuáles necesitan adaptarse a sus circunstancias, manteniendo la supervisión y la responsabilidad sobre los resultados.

La gestión del cambio, una responsabilidad de toda la organización

La tecnología puede funcionar correctamente y, aun así, no alcanzar los resultados previstos si los empleados no entienden el propósito de la transformación o no cuentan con las capacidades necesarias para adoptarla. Por ello, la gestión del cambio fue uno de los asuntos que generó mayor consenso durante el encuentro.

"La gestión del cambio es lo realmente difícil",

Comida BYTE TI

Automatizar procesos: del ahorro de costes a la transformación del negocio

reconoció Valero, quien destacó la importancia de implicar a la dirección y preparar a las personas para trabajar con nuevas herramientas. Aguilar añadió que la resistencia depende en gran medida de que los profesionales comprendan las ventajas de la tecnología y dispongan de mecanismos de supervisión humana.

García advirtió de que las empresas deben abordar este aspecto desde el inicio. La comunicación, el respaldo de los responsables y la formación son elementos esenciales, especialmente cuando la automatización modifica funciones o transforma tareas manuales en actividades de supervisión. "No debemos perder el conocimiento del proceso", subrayó, porque los trabajadores siguen siendo necesarios para detectar ineficiencias, comprender las operaciones y contribuir a mejorarlas.

Escribano alertó de un error habitual: delegar en exceso la gestión del cambio en el proveedor tecnológico. Este puede ayudar con la formación, pero la responsabilidad de preparar a los equipos y gestionar la transformación debe permanecer en la propia organización.

La experiencia de Appian en la automatización de procesos complejos también apunta a la importancia del patrocinio interno. Gómez explicó que, en una empresa del sector energético, la actualización de precios de carburantes se gestionaba mediante hojas de cálculo y requería un equipo numeroso, sometido a una elevada presión para evitar errores. La incorporación de reglas de negocio y herramientas de automatización permitió reducir hasta un 80% la carga de trabajo del personal y las bajas por estrés.

El cambio no consistió solo en acelerar una tarea, sino en modificar la forma de trabajar. Para Gómez, mejorar la experiencia de los usuarios y contar con el respaldo de la dirección son condiciones fundamentales para superar las resistencias.

Seguridad y gobernabilidad para una IA responsable

La incorporación de la IA abre nuevas posibilidades, pero también introduce riesgos que deben evaluarse antes de extender su uso. Del Sanz advirtió de que esta tecnología plantea desafíos de seguridad e implantación que no se presentaban de la misma forma con los procesos tradicionales. A ello se suma el riesgo de que la sobreinformación dificulte la identificación de los asuntos realmente relevantes.

En Iberpay, Valero considera la IA una herramienta que puede aportar una perspectiva diferente, pero insiste en que la decisión final debe seguir correspondiendo a una persona. Esta supervisión resulta especialmente importante cuando las operaciones afectan al funcionamiento de servicios financieros esenciales.

Gómez defendió la necesidad de asumir una responsabilidad tanto individual como corporativa ante la expansión de estas tecnologías. "Se está impulsando IA por IA en titulares, pero con responsabilidad corporativa e individual", afirmó. La adopción debe responder a objetivos concretos y ajustarse a las buenas prácticas de cada organización.

Escribano fue tajante respecto al orden de actuación: "Es muy importante poner un gobierno de la IA antes de meter iniciativa de la IA". Establecer reglas, responsabilidades y mecanismos de control permite definir qué usos están permitidos, cómo se supervisan los resultados y cuándo debe intervenir una persona.

Desde Merck, García recordó que el área de IT también debe ayudar a decidir para qué se necesita la IA y cómo se gestionará su utilización entre departamentos y profesionales. En un entorno donde las soluciones pueden actuar sobre procesos cada vez más complejos, la gobernabilidad deja de ser un requisito posterior y pasa a formar parte del diseño inicial.

Comida BYTE TI

La IA pasa de ser experimental a convertirse en estrategia empresarial

Alfonso Casas

La inteligencia artificial ha dejado de ser una tecnología asociada exclusivamente a la innovación para convertirse en uno de los principales ejes de transformación empresarial. Esta es una de las principales conclusiones de la mesa organizada por Byte TI, en colaboración con las empresas VISEO Iberia y Asus que actuaron de patrocinadoras del almuerzo.



Al encuentro asistieron directivos de compañías de sectores tan diversos como educación, energía, banca, seguros, telecomunicaciones, medios de comunicación, construcción, industria y servicios profesionales. Participaron: Carlos Garriga, CIO en IE University; Miguel Ángel Melero, director de personas, procesos y tecnología en Metrovacesa; José Manuel Medina, CTO en Labormatters Abogados; Toni Campos, Sales Channel Manager en ASUS; Alfredo Delgado, director de Transformación y Tecnología en UMAS; Andrés López, Director IT / CIO en Grupo Indigo; Sergio Merchán, CIO de Iberdrola; Mariano Roque, adjunto a la Dirección de Tecnología en Iberpay; Federico Rousaud, Director de la Unidad de Negocio Cloud Apps & Data en VISEO Iberia; Laura Baus, CISO en Vodafone; Elena García, directora de Digital en Vodafone; Julio Muñoz, CTO en El Confidencial; y Carlos Miranda, Head of AI Program en Ferrovial. La mesa estuvo moderada por Manuel Navarro, director editorial de la revista Byte TI.

El debate puso de manifiesto que las empresas se encuentran en una etapa de transición. Tras una primera fase marcada por la experimentación y la proliferación de pilotos, el objetivo comienza a ser mucho más concreto: conseguir que la IA genere impacto medible en el negocio.

Comida BYTE TI

La IA pasa de ser experimental a convertirse en estrategia empresarial



Alfredo Delgado, director de Transformación y Tecnología en UMAS



Andrés López, Director IT CIO en Grupo Indigo



Carlos Garriga, CIO en IE University



Carlos Miranda, Head of AI Program en Ferrovial

Federico Rousaud, director de la Unidad de Negocio Cloud Apps & Data de VISEO Iberia, resumió este cambio de orientación al explicar que la demanda de los clientes está evolucionando. "La foto ha cambiado. Ahora lo que nos piden es poder capturar valor", señaló. En su opinión, la conversación ya no gira solo alrededor de la tecnología, sino en la capacidad de obtener un rendimiento económico, incrementar la productividad y mejorar la rentabilidad.

De hecho, Rousaud considera que el principal reto actual no es tecnológico. "Todo el mundo tiene la IA, pero la clave es cómo pasar de una amplia gama de pilotos de IA a algo que me permita crecer como compañía", planteó. Para conseguirlo, las organizaciones tienen que abordar cuestiones relacionadas con la gestión del cambio, el liderazgo y la definición de aquello que realmente se quiere mejorar. "Si no podemos medirlo, difícilmente podrás cambiarlo", añadió.

De la experimentación a la estrategia

El debate dejó claro que prácticamente ninguna organización puede permitirse permanecer al margen. Sergio Merchán, CIO de Iberdrola, destacó que la IA supone un cambio de paradigma frente a anteriores procesos de transformación tecnológica. Automatización, digitalización o RPA fueron incorporando cambios graduales, mientras que la IA está afectando de manera transversal a la forma en la que las compañías operan.

En Iberdrola, explicó, la IA se ha convertido en el principal pilar estratégico y tecnológico, con tres grandes líneas de actuación: herramientas para los empleados, aplicaciones específicas para los negocios de la compañía e integración de la IA dentro de la propia función tecnológica, bajo el concepto de "Agentic IT".

Una visión similar apareció en otras organizaciones. En Grupo Indigo se ha incorporado un "driver" de IA a los proyectos incluidos en su plan hasta 2030, mientras que en Iberpay la inteligencia artificial y la resiliencia constituyen dos de los pilares fundamentales de su estrategia. La compañía está trabajando en una arquitectura que permita desarrollar, desplegar y operar capacidades de IA de manera escalable y reutilizable.

También en El Confidencial, según explicó su CTO, Julio Muñoz, "ahora no hay estrategia que no sea de IA". La compañía comenzó identificando casos de uso destinados a acelerar tareas y

Comida BYTE TI

La IA pasa de ser experimental a convertirse en estrategia empresarial



Elena García, directora de Digital en Vodafone



Federico Rousaud, Director de la Unidad de Negocio Cloud Apps & Data en VISEO Iberia



José Manuel Medina, CTO en Labormatters Abogados



Julio Muñoz, CTO en El Confidencial



Laura Baus, CISO en Vodafone

eliminar burocracia —desde investigación hasta búsqueda de noticias o fotografías de archivo— para posteriormente avanzar hacia una estrategia de transformación más profunda.

En educación, el impacto adquiere incluso una dimensión estructural. Carlos Garriga, CIO de IE University, explicó que la IA se está desplegando simultáneamente entre el personal administrativo, los equipos y los alumnos. En su opinión, el sector educativo afronta una revolución que afecta a la esencia del modelo, ya que tareas que anteriormente no podían escalar ahora sí pueden hacerlo mediante herramientas de IA.

Elegir la tecnología y demostrar el ROI

Pero la adopción también plantea una dificultad evidente: qué herramientas utilizar, dónde aplicarlas y cómo justificar la inversión.

Toni Campos, Sales Channel Manager de ASUS, puso el foco precisamente en este punto. Desde la perspectiva de los clientes, aseguró que uno de los principales problemas es decidir qué herramienta utilizar en un mercado en el que las versiones y capacidades evolucionan constantemente. Una vez tomada esa decisión aparece una segunda cuestión: "Dónde la enfocan, qué departamento la usa y dónde sacar el ROI".

Campos introdujo además un elemento que adquiere especial relevancia en la estrategia tecnológica: el dispositivo. La llegada de las NPU y de las capacidades de procesamiento de IA en local está modificando la tradicional división entre equipos de usuario y servicios cloud.

"Venimos de la idea de mismos dispositivos para todos los empleados y todo a la nube. Ahora, al meter la NPU en local en el equipo, ponemos al portátil como un punto de decisión clave", explicó.

La cuestión no es únicamente de rendimiento. También afecta a la privacidad, la seguridad y al propio plan de renovación del parque tecnológico. Para ASUS, la elección de la herramienta de IA debe ir acompañada de una reflexión sobre qué capacidades deben ejecutarse en local y cuáles pueden permanecer en la nube.

Además, Campos apuntó a otro factor que empieza a ganar importancia: el coste asociado al consumo de modelos. "El precio por token también está siendo un elemento de elección", señaló.

Una reflexión compartida por otras compañías. Alfredo Delgado, director de Transformación y Tecnología de UMAS, explicó que la organización

Comida BYTE TI

La IA pasa de ser experimental a convertirse en estrategia empresarial



Mariano Roque, adjunto a la Dirección de Tecnología en Iberpay



Miguel Ángel Melero, director de personas, procesos y tecnología en Metrovacesa



Sergio Merchán, CIO de Iberdrola



Toni Campos, Sales Channel Manager en ASUS

está estudiando modelos de procesamiento local que permitan reducir el consumo y hacer más eficiente el uso de tokens. En El Confidencial, Julio Muñoz también situó la optimización del consumo de los LLM como uno de los siguientes pasos de su estrategia tecnológica.

Gobernanza: controlar sin frenar

La aceleración de la IA lleva aparejado otro reto: garantizar que su utilización se produzca dentro de unos límites seguros. La gobernanza se convierte así en una condición necesaria para escalar.

Miguel Ángel Melero, director de Personas, Procesos y Tecnología de Metrovacesa, explicó que la compañía comenzó estableciendo una política de uso y un marco para la adopción de herramientas, teniendo especialmente en cuenta los datos y la confidencialidad. La estrategia se ha basado en identificar casos de uso, analizar las herramientas disponibles y realizar un despliegue ordenado, acompañado de capacitación.

En Grupo Indigo, Andrés López incidió en que la ausencia de gobernanza no supone únicamente un problema económico. También implica no saber si la IA se está utilizando de forma segura, qué datos se están moviendo o si los empleados recurren a licencias y herramientas particulares fuera del control corporativo.

Desde Vodafone, Laura Baus, CISO de la compañía, resumió el desafío como la necesidad de habilitar al negocio manteniendo la velocidad de adopción y, al mismo tiempo, asegurando el control. La compañía ha creado un sistema de gobernanza de IA integrado con sus políticas para garantizar una utilización controlada.

La seguridad, además, adquiere una nueva dimensión. La propia IA amplía la superficie de riesgo y obliga a reforzar las capacidades de ciberseguridad. Pero los participantes coincidieron en que seguridad y negocio no pueden avanzar por caminos separados.

Los datos como elemento diferencial

La calidad de los datos aparece como otra de las piezas fundamentales para que la IA genere resultados diferenciales. Carlos Miranda, Head of AI Program de Ferrovial, puso sobre la mesa una idea especialmente relevante: una IA genérica puede servir para obtener eficiencia, pero difícilmente permitirá construir una ventaja competitiva sostenible. "Sin el entrenamiento con datos propios, la IA será semejante en multitud de empresas", señaló. En su caso, la apuesta pasa por combinar herramientas generales con

Comida BYTE TI

La IA pasa de ser experimental a convertirse en estrategia empresarial

desarrollos propios, hasta alcanzar un equilibrio en el que aproximadamente el 60% corresponda a desarrollo propio.

La misma reflexión apareció desde Vodafone. Elena García, directora de Digital de la compañía, apuntó que, si todas las empresas de un mismo sector utilizan las mismas herramientas, los resultados tenderán a parecerse. La diferencia estará en cómo cada organización utiliza la IA para generar valor específico y mejorar la experiencia de sus clientes.

Sergio Merchán puso como ejemplo el contexto que puede proporcionarse a la IA en áreas como el call center o el CRM. "Es precisamente ahí donde una tecnología disponible para todos puede convertirse en una herramienta diferencial para una compañía concreta", afirmó.

El factor humano gana peso

Quizá la conclusión más transversal de la mesa fue que la IA no elimina la importancia del factor humano, sino que modifica su valor.

Julio Muñoz lo expresó de forma clara: "El humano pasa a ser la ventaja competitiva de la empresa". La tecnología permite ganar eficiencia, pero será la capacidad de las personas para interpretar, cuestionar y utilizar correctamente sus resultados la que determine el valor obtenido.

Toni Campos coincidió en que "la ventaja del equipo humano va a ser determinante en la toma de decisiones". Para él, las organizaciones necesitan personas capaces de observar, aplicar criterio crítico y revisar el resultado generado por las herramientas. En el ámbito del desarrollo, por ejemplo, el profesional puede dejar de dedicar tanto tiempo a escribir código, pero deberá comprobar que aquello que produce la IA es correcto.

Esta transformación afecta especialmente a la formación. Sergio Merchán destacó la importancia de "identificar las capacidades de cada empleado y desarrollar programas que permitan evolucionarlas, incluso mediante una IA Academy. En mi opinión, la falta de capacitación podría dejar fuera a profesionales que no sepan utilizar adecuadamente estas nuevas herramientas".

En Vodafone, Elena García apuntó hacia perfiles cada vez más híbridos, capaces de combinar conocimiento tecnológico con comprensión del negocio. "Vuelve a coger fuerza la inteligencia del negocio", explicó, defendiendo una formación que vaya más allá de aprender a desarrollar una página web o construir un cuadro de mando y permita entender por qué se hacen las cosas.

Para Federico Rousaud, sin embargo, aquí aparece uno de los grandes retos de los próximos años: la velocidad del cambio puede ser superior a la capacidad de adaptación de una parte de los trabajadores. "El problema es la velocidad a la que se viene todo. Hay un gap", afirmó. A su juicio, existe un salto entre la inteligencia del negocio y el valor que las personas pueden aportar a las organizaciones, pero una parte importante de los empleados todavía no estará preparada para asumirlo. "Habrá un problema de gestión social", advirtió.

Los empleos con mayor riesgo por la IA

El debate sobre las capacidades conduce inevitablemente a la otra gran cuestión: qué puestos de trabajo pueden verse afectados por el impacto de la IA. Miguel Ángel Melero explicó que cada vez se habla más de perfiles que de tecnología y puso el foco en las tareas repetitivas, especialmente en áreas como reporting y administración. Son actividades con procesos definidos y poca interacción humana que presentan un mayor riesgo de automatización.

Sin embargo, la cuestión no debería limitarse a la desaparición de puestos. La verdadera pregunta para las empresas será qué hacer con la productividad adicional generada por la IA: convertirla en mayores beneficios o utilizarla para ofrecer productos y servicios más competitivos.

Webinar BYTE TI

Cómo aplicar una estrategia Zero Trust de forma efectiva

En un encuentro virtual organizado por Byte TI, Sergio Martínez, Iberia & Italia Regional Manager en SonicWall, y José Antonio Bayona, Operations Excellence Director en Viseo, analizaron la implementación de estrategias Zero Trust. Ambos expertos debatieron sobre los errores habituales al adoptar este modelo, la gestión de infraestructuras "legacy" y el impacto de la inteligencia artificial, destacando que la identidad se ha convertido en el nuevo perímetro organizativo y exigiendo una gobernanza continua del riesgo.



Por Manuel Navarro

El punto de inicio del debate se centró en que la protección de datos, activos y aplicaciones esenciales se ha transformado en la máxima prioridad estratégica para las organizaciones modernas. En este contexto, el despliegue de un modelo Zero Trust se ha consolidado como un pilar imprescindible para proteger los datos y activos de las organizaciones ante un entorno de ciberamenazas cada vez más complejo. Sin embargo, en el camino hacia su adopción, las empresas cometen equivocaciones estructurales.

Al analizar los errores más extendidos, José Antonio Bayona, Operations Excellence Director en Viseo, señala que el más habitual es "confundir realmente pues que la implantación de determinadas tecnologías al final es equivalente a esa adopción de un modelo Zero Trust". Según explicó Bayona, muchas organizaciones asumen erróneamente que cuentan con una estrategia completa solo por haber instalado un segundo factor de autenticación (MFA), una red privada virtual o por haber realizado una segmentación de red. Para el directivo, la ciberseguridad debe evolucionar desde la confianza implícita hacia una verificación rigurosa, afirmando taxativamente: "no hay que confiar por defecto, sino que hay que convertir cada acceso que se requiera pues realmente en una decisión, una decisión que tiene que ser dinámica, que tiene que valorar el contexto y que tiene que ser gobernada". Además, advirtió contra la falsa idea de considerar Zero Trust como un proyecto cerrado con fecha de fin, recordando que se trata de un proceso dinámico de gobernanza continua en el que se deben revisar de forma constante los privilegios, las políticas y las excepciones ante las variaciones del negocio.

Por su parte, Sergio Martínez, Iberia & Italia Regional Manager en SonicWall, coincide en la necesidad de replantear las bases defensivas de las empresas y advierte sobre los peligros del desconocimiento interno. Martínez sostiene

Webinar BYTE TI

Cómo aplicar una estrategia Zero Trust de forma efectiva

que "el perímetro de verdad es la identidad, la identidad es la que nos da acceso a los recursos". Desde su perspectiva, el fallo más grave al abordar este modelo es el desconocimiento que las organizaciones tienen sobre su propia infraestructura y el Shadow IT, o como resumió de forma gráfica, "desconocer en qué barril estás sentado". Martínez subrayó el riesgo que representa el parque heredado de conexiones SSL VPN desplegado masivamente durante la pandemia, declarando categóricamente que "SSL VPN es un protocolo vulnerable por diseño y hay que ir retirando lo más rápidamente posible de todas las compañías". Según el regional manager de SonicWall, este tipo de accesos se han convertido en la principal puerta de entrada para los ciberdelincuentes, al conceder un acceso indiscriminado a la red una vez superada la autenticación inicial.

A la hora de trazar la estrategia adecuada sin detener la actividad empresarial, los expertos coinciden en que no es necesario contar con un presupuesto astronómico para dar los primeros pasos. Sergio sintetizó el punto de partida fundamental al aseverar que "el primer paso es un ejercicio interno que hay que hacer: un mapeo de qué usuarios, qué tipos de usuarios hay, qué recursos internos y externos hay que acceder". Este inventario debe clasificar los perfiles de usuario, identificar las aplicaciones, el tráfico de internet e identificar con precisión cuáles son las credenciales privilegiadas y quién custodia a los administradores. Complementando este planteamiento, el responsable de Viseo recomienda priorizar los procesos esenciales del negocio y realizar un análisis de impacto antes de invertir. En sus propias palabras, José Antonio aconseja: "partamos primero de conocer qué es lo que hay, veamos realmente dónde tenemos las deficiencias y a partir de ahí definamos el qué". Bayona insistió en evitar la precipitación de adquirir herramientas por moda, remarcando que "no se trata de hacer el ejercicio inverso que muchas empresas han hecho de cojo esta solución que es la que me están ofreciendo como óptima en el mercado y la implemento". El enfoque debe basarse en identificar las brechas existentes, aprovechar la infraestructura actual y añadir soluciones específicas únicamente donde existan deficiencias.

> **A la hora de desarrollar una estrategia hay que identificar las brechas existentes, aprovechar la infraestructura actual y añadir soluciones específicas**



José Antonio Bayona,
Operations Excellence
Director en Viseo

Integración en entornos legacy

La convivencia del modelo Zero Trust con las infraestructuras heredadas (legacy) y operativas (OT) representa un reto técnico mayúsculo, dado que estos sistemas no admiten agentes de seguridad modernos. Para superar esta traba, Martínez explicó que la solución pasa por securizar el entorno periférico de estas aplicaciones e integrarlas mediante arquitecturas basadas en la nube como Cloud Secure Edge. Esta aproximación permite verificar la postura del dispositivo y la ubicación del usuario antes de conceder acceso, protegiendo tanto los sistemas antiguos como los accesos temporales de proveedores externos sin asumir riesgos inasumibles. Asimismo, enfatizó que la ciberdefensa debe estructurarse por capas y centralizar todas las alertas en repositorios de datos capaces de interpretar patrones anómalos. La inmediatez en la detección resulta vital si

Webinar BYTE TI

Cómo aplicar una estrategia Zero Trust de forma efectiva

se tiene en cuenta la pauta temporal de los ciberdelincuentes, sobre la cual Sergio Martínez aportó un dato revelador: "más del 70%, casi el ochenta, de los ataques se producen un viernes sobre las cuatro de la madrugada". Martínez alertó de que los atacantes suelen llevar semanas dentro de la red preparando el terreno antes de ejecutar el secuestro de datos, demostrando que "al final la gente cierra la puerta pero deja la ventana abierta".

En relación con el tipo de amenazas, el directivo de SonicWall compartió cifras contundentes sobre la vulnerabilidad corporativa: el 48% de las filtraciones se inician mediante credenciales comprometidas en redes VPN y el 75% de las alertas de seguridad responden al robo de claves. Además, desmitificó la creencia de que las pymes están a salvo, recordando que representan el 43% de los objetivos y que el 60% de las pequeñas empresas vulneradas terminan cerrando en un plazo de seis meses. Ante este panorama, el ejecutivo fue categórico al describir la tendencia actual: "siempre empiezo todas las entrevistas diciendo: todo va a peor".

Vencer la resistencia cultural

Para vencer la resistencia cultural que a menudo frena las medidas de seguridad, Bayona sostuvo que la concienciación resulta más efectiva que los discursos técnicos. Al referirse a cómo convencer a los empleados y a la alta dirección, el Operations Excellence Director de Viseo afirmó que "el objetivo es no hablar de tecnología". En su lugar, aboga por realizar pedagogía mediante campañas que expliquen los riesgos en términos de negocio y las consecuencias reales que un incidente tendría sobre la continuidad de la empresa y los puestos de trabajo. Del mismo modo, en lo referente a la neutralización de ataques como el ransomware, Bayona aclaró la verdadera dimensión de Zero Trust al manifestar que "en ningún caso vamos a poder evitar el ataque... de lo que se trata es de estar preparados ante cualquier ataque para poder minimizar el impacto".

Finalmente, el debate abordó la irrupción de la inteligencia artificial y su doble filo en la ciberseguridad. Si bien la IA potencia la capacidad de análisis y agiliza el diagnóstico de vulnerabilidades, Bayona advirtió sobre la tentación de delegar la gestión del riesgo de forma ciega, subrayando que "lo que no debemos dejar en manos de la IA es después la toma de decisiones". Asimismo, alertó del riesgo del "Shadow AI", causado por empleados que suben información confidencial a modelos públicos sin control corporativo. Por su parte, Martínez cuestionó la idoneidad de desplegar grandes modelos generalistas para tareas cotidianas cuando se pueden utilizar soluciones agénticas o locales más acotadas, reflexionando de manera irónica: "¿Para qué necesitas un doctor de Stanford sentado en una silla al lado si lo que necesitas es un becario?". Ambos ponentes concluyeron que el futuro exige un uso gobernado de la IA y un control estricto de las identidades para salvaguardar el negocio.

> **El 48% de las filtraciones se inician con credenciales comprometidas en redes VPN y el 75% de las alertas responden al robo de claves.**



Sergio Martínez,
Iberia & Italia Regional Manager en SonicWall

Comparativa

5 soluciones de gestión de identidades y accesos

La gestión de identidades y accesos se está convirtiendo en una prioridad para las organizaciones que deben (y necesitan) controlar quién accede a sus sistemas, aplicaciones y datos, y con qué permisos. Y dentro de este contexto, la evolución de las amenazas está impulsando el interés por estas soluciones. Según un estudio de Delinea sobre seguridad de identidades publicado el año pasado, el 78 % de los responsables de tecnología y seguridad encuestados confiaba aumentar su inversión próximamente.

Las previsiones apuntan a que esta tendencia continuará. En su informe 'Identity & Access Management Market: 2026-2031', la consultora Juniper Research estima que el número de empresas que emplean servicios de gestión de identidades y accesos (IAM) pasará de 67,6 millones en 2026 a más de 88 millones en 2031. Esto supondría que más de un 26% de las organizaciones de todo el mundo los adoptaría. Entre los factores que impulsarían esta evolución se encuentra la necesidad de gestionar las identidades no humanas, como las asociadas a aplicaciones, máquinas y agentes de inteligencia artificial, y de garantizar que cada una disponga únicamente de los permisos que necesita.

Definición y características clave

¿En qué consisten estas soluciones y qué elementos las caracterizan? Las herramientas de gestión de identidades y accesos permiten que las organizaciones empresariales administren sus cuentas digitales y regulen el acceso a sus aplicaciones, datos y sistemas. Para ello, disponen de funciones como la autenticación de usuarios, la asignación de permisos y la gestión de las cuentas durante todo su ciclo de vida.

Así, una de sus características es la capacidad de automatizar tareas relacionadas con las altas, los cambios de puesto y las bajas de los empleados. También pueden incorporar



Comparativa

5 soluciones de gestión de identidades y accesos

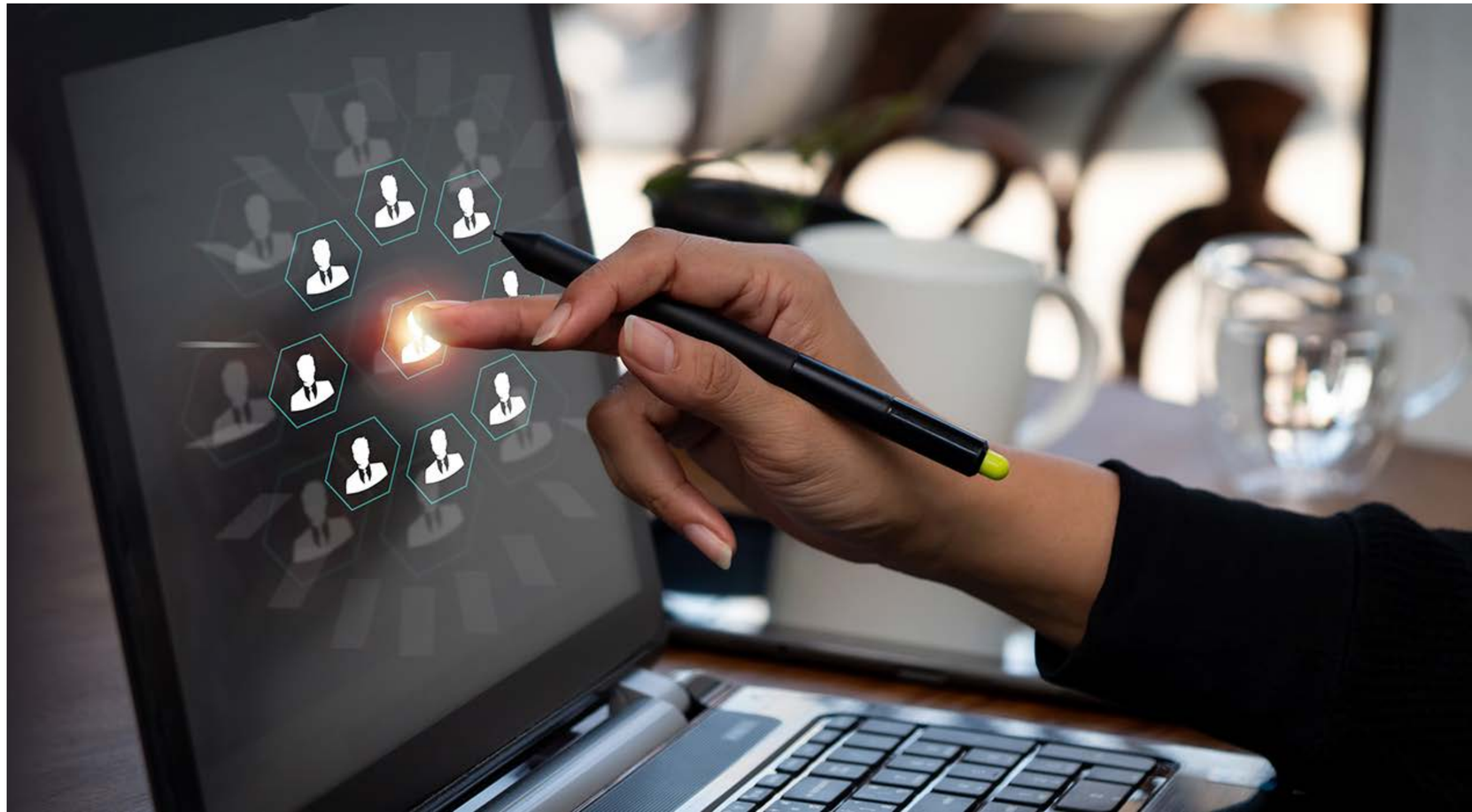
autenticación multifactor, que exige comprobar la identidad mediante dos o más factores diferentes, e inicio de sesión único (SSO) para acceder a varias aplicaciones compatibles tras una única autenticación.

Estas soluciones ayudan, por otro lado, a establecer permisos según el puesto, las responsabilidades o determinadas condiciones de acceso. Algunas incluyen para ello herramientas para revisar autorizaciones, registrar la actividad y generar informes sobre los accesos. En este ámbito se aplica el principio de mínimo privilegio, que establece que cada identidad debe disponer exclusivamente de los permisos imprescindibles para realizar sus tareas.

Ahora bien, hay que tener en cuenta que no todas brindan las mismas funciones. Mientras que, por ejemplo, las plataformas de gobierno y administración de identidades (IGA) se centran en la revisión y supervisión de permisos, las de gestión de accesos privilegiados (PAM) lo hacen en las cuentas con autorizaciones elevadas. En el caso de las de gestión de identidades de clientes (CIAM), en los usuarios de servicios digitales.

En conclusión, al elegir una solución IAM, las organizaciones deben tener en cuenta su infraestructura tecnológica, el número y tipo de identidades que necesitan gestionar y los requisitos de seguridad y cumplimiento normativo. También es importante que la herramienta pueda integrarse con los sistemas existentes y adaptarse a nuevas necesidades, especialmente a medida que aumenta el uso de servicios en la nube y procesos automatizados.

Al elegir una solución IAM, hay que tener en cuenta la infraestructura tecnológica, el número y tipo de identidades a gestionar y los requisitos de seguridad



Comparativa

5 soluciones de gestión de identidades y accesos

AWS Identity and Access Management (IAM)

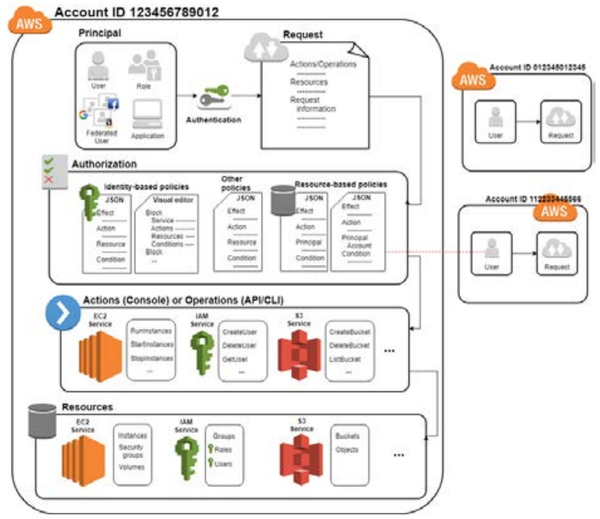
Se trata de un servicio web que permite controlar el acceso a los recursos de Amazon Web Services (AWS). Así, gracias a este, las empresas controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizarlos. En concreto, una de las características que incluye es un analizador de acceso: el objetivo de esta herramienta es conceder únicamente las autorizaciones necesarias para realizar cada tarea, de modo que las organizaciones revisan y ajustan permisos a medida que cambian sus necesidades.

Otra de sus características es el Identity Center, un servicio que les ayuda a gestionar de forma centralizada quién entra o tiene acceso a las aplicaciones de AWS. Por su parte, con AWS Identity and Access Management Roles Anywhere, las organizaciones empresariales obtienen credenciales de seguridad temporales para las siguientes cargas de trabajo: locales, híbridas y multinube. En concreto, su integración con la infraestructura de clave pública empresarial existente en ellas facilita que las cargas de trabajo que se ejecutan fuera de AWS utilicen las mismas políticas y roles de IAM que las que se ejecutan en AWS, sin necesidad de gestionar credenciales a largo plazo.

También destacan el control de acceso granular de IAM y la administración de roles. La primera de estas opciones es útil para establecer permisos que determinen quién puede acceder a qué recursos de AWS y bajo qué condiciones. Por su parte, la segunda hace referencia a entidades que crea el usuario y a las que asigna permisos específicos para que las identidades de confianza (como las identidades de los empleados y las aplicaciones) puedan realizar acciones en AWS. La sexta, y última característica, es la autenticación multifactor, que requiere un segundo factor de autenticación además de las credenciales de inicio de sesión con nombre de usuario y su contraseña.

Los beneficios que brinda esta solución de gestión de identidades son varios. Por ejemplo, es posible emplear conjuntos de permisos y credenciales de seguridad temporales para que los trabajadores accedan a sus recursos de AWS. O analizar el acceso y la validación de las políticas de IAM a medida que se avanza hacia un nivel de privilegios mínimos.

Referente a los casos de uso, la propuesta de AWS permite aplicar permisos específicos y escalar con un control de acceso basado en atributos. Esto quiere decir que es posible crear permisos detallados en función de los atributos



del usuario, como el departamento, el cargo y el nombre del equipo. Otro de los casos de uso es que las empresas tienen la opción de administrar identidades por cuenta con IAM o utilizar el centro de identidades de AWS IAM para proporcionar acceso a varias cuentas y asignaciones de aplicaciones en todo AWS. Asimismo, es posible determinar barreras de protección preventivas y para toda la organización en AWS. Es decir, emplear las políticas de control de servicios con el propósito de establecer barreras de protección de permisos para los roles y usuarios de IAM e implementar un perímetro de datos alrededor de las cuentas en AWS Organizations.

Amazon Web Services

aws.amazon.com/es/contact-us

aws.amazon.com/es/iam

a consultar

Comparativa

5 soluciones de gestión de identidades y accesos

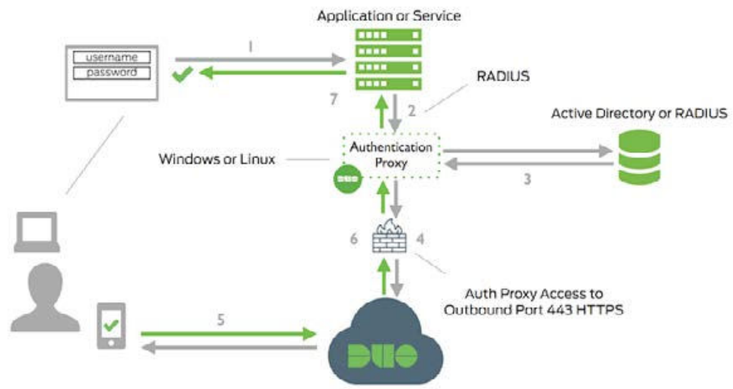
Cisco Duo IAM

Cisco Duo Identity and Access Management (IAM) es una solución integral de seguridad que transforma la manera en que las organizaciones protegen las identidades frente a las amenazas potenciadas por la inteligencia artificial. Basada en una tecnología de autenticación multi-factor (MFA), ofrece protección contra el phishing y otros ataques de ingeniería social, mejorando a su vez la experiencia de usuario y simplificando la administración TI.

Dado que la identidad es en estos instantes uno de los principales objetivos de los ciberdelincuentes, Duo IAM responde a esta vulnerabilidad con un enfoque de zero trust que incorpora la seguridad por defecto, por lo que permite a las empresas prevenir accesos no autorizados sin sacrificar la productividad. Entre sus funcionalidades destaca un nuevo Directorio de Usuarios que facilita el almacenamiento centralizado de credenciales y roles, y simplifica la gestión de accesos. Además, la solución de Cisco garantiza una autenticación multifactor e inicio de sesión único avanzado (SSO) al combinar seguridad y facilidad de uso, con acceso simple a cientos de aplicaciones desde un único portal.

Por otro lado, Cisco Duo IAM 'promete' una integración flexible gracias a la presencia de un nuevo motor de enrutamiento, Duo IAM, que conecta con sistemas de identidad de terceros, actuando como proveedor secundario o intermediario. Mientras, para hacer frente a las técnicas de fraude que intentan suplantar identidad, las organizaciones van a disponer de tres soluciones que refuerzan la protección frente al robo de credenciales y sesiones. La primera es Complete Passwordless que ayuda a verificar la identidad de los usuarios sin necesidad de introducir contraseñas. Por su parte, Proximity Verification asegura que los dispositivos móviles y de autenticación estén físicamente próximos. Por último, se encuentra Session Theft Protection: elimina la dependencia de cookies del navegador y protege frente al secuestro de sesiones. La otra funcionalidad clave de Duo IAM es la presencia de un asistente de inteligencia artificial de Cisco que acompaña a las empresas en la implementación y administración diaria.

Inteligencia de identidad unificada. La infraestructura de identidad suele estar fragmentada y esto deriva en puntos ciegos en la seguridad. Para hace frente a esta problemática, se integra con Cisco Identity Intelligence, una solución de seguridad basada en inteligencia artificial, conectando datos de identidad y acceso en toda la plataforma de ciberseguridad Cisco Security Cloud. De este modo, las organizaciones obtienen una visibilidad integral y continua sobre el riesgo de identidad; análisis de comportamiento



con IA para detectar anomalías; y respuestas adaptativas y automatizadas como poner en cuarentena una identidad, forzar cierres de sesión activos o aislar redes comprometidas.

¿Y los beneficios? El primero es una seguridad reforzada, con protección frente a ataques de phishing, robo de credenciales y secuestro de sesiones. El segundo es una experiencia de usuario sin fricción: acceso fluido con MFA, SSO y autenticación passwordless. Por otro lado, se encuentra la eficiencia operativa con una reducción de los costes de gestión mediante un directorio centralizado e integración con sistemas de terceros. Su escalabilidad y flexibilidad la convierten en una solución adaptable a organizaciones de todos los tamaños y sectores.

Cisco

www.cisco.es

www.cisco.com/c/es_es/about/contact-cisco.html

a consultar

Comparativa

5 soluciones de gestión de identidades y accesos

Microsoft Entra ID

En un entorno donde las organizaciones afrontan un incremento constante de las amenazas basadas en la identidad y la necesidad de facilitar el acceso seguro a sus aplicaciones y recursos desde cualquier lugar, la gestión de identidades y accesos se ha convertido en un elemento fundamental de la estrategia de ciberseguridad. El Gigante de Redmond responde a este desafío con Microsoft Entra ID, anteriormente conocida como Azure Active Directory, una solución de administración de identidades y accesos basada en la nube que ayuda a proteger a trabajadores, aplicaciones y recursos empresariales.

Por sus características, permite que las compañías implementen un acceso adaptativo seguro, protegiendo las identidades frente a posibles amenazas mediante una autenticación sólida y directivas de acceso condicional basadas en riesgos. Estas capacidades ayudan a prevenir ataques dirigidos a las credenciales y se integran de forma nativa con las soluciones de seguridad de Microsoft dentro de un enfoque de confianza cero o Zero Trust.

Para simplificar la experiencia de usuario sin comprometer la seguridad, la plataforma incorpora funcionalidades como autenticación multifactor, inicio de sesión único, autenticación sin contraseña y herramientas de autoservicio que ayudan a que los empleados accedan de forma rápida y segura a las aplicaciones que necesitan para desarrollar su trabajo; mecanismos que contribuyen igualmente a reducir la fricción en el acceso mientras fortalecen su protección frente a amenazas como el phishing.

Asimismo, la solución ofrece una administración centralizada de identidades y accesos, permitiendo gestionar usuarios, permisos y aplicaciones desde una única plataforma, tanto en entornos locales como en la nube. Esta visión unificada facilita a los equipos de TI mejorar la visibilidad, reforzar el control de acceso y aplicar políticas de seguridad coherentes en toda la organización. En referencia a la administración de aplicaciones, cabe explicar que cuando una aplicación está registrada en una entidad de Microsoft Entra, los usuarios que ya están asignados a la aplicación pueden acceder de forma segura. Entre sus funciones se encuentran la administración del acceso mediante inicio de sesión único, la asignación de recursos y el aprovisionamiento automatizado; la configuración de los requisitos de inicio de sesión y las propiedades de cada aplicación; y la protección mediante permisos, autenticación multifactor, acceso condicional, tokens y certificados. También facilita la gobernanza y la supervisión de la actividad, así como la retirada de los permisos



y la eliminación de las aplicaciones que dejan de utilizarse para mantener el entorno de identidad organizado y bajo control. Como la gestión de identidades también abarca los dispositivos desde los que los empleados acceden a los recursos corporativos, Entra ID registra e identifica equipos y dispositivos móviles.

La integración de IA representa otro de los avances más relevantes de la plataforma. A través de Security Copilot en Microsoft Entra, los equipos de identidad pueden utilizar el lenguaje natural para investigar usuarios de riesgo, detectar anomalías en los procesos de autenticación, supervisar cambios en los accesos e identificar posibles brechas en las políticas de seguridad. Esta combinación de identidad e IA ayuda a responder con mayor rapidez y eficacia ante las amenazas.

Microsoft | 91 391 90 00 | A consultar

www.microsoft.com/es-es/security/business/identity-access/microsoft-entra-id

Comparativa

5 soluciones de gestión de identidades y accesos

Ping Identity

Garantizar que las personas e identidades adecuadas accedan a los recursos precisos en el momento oportuno. Bajo esta filosofía, Ping Identity propone una solución de gestión de identidades y de accesos articulada alrededor de cuatro puntos principales.

El primero de ellos está relacionado con Customer Identity and Access Management (CIAM), una solución que nace con el propósito de transformar la seguridad en una ventaja competitiva. Lo hace ofreciendo procesos de registro e inicio de sesión que sean ágiles y sin fricciones, reforzando a la marca (u organización) y deteniendo el fraude antes de que se produzca. Por su parte, con Workforce Identity lo que se persigue es proteger a los empleados con independencia del lugar en el que se encuentren y sin que su productividad se vea afectada o interrumpida: para ello, Ping Identity ofrece una arquitectura Zero Trust, inicio de sesión único y autenticación multifactor.

El tercer elemento clave es B2B & Third-Party Access. Con esta solución, las compañías pueden simplificar su ecosistema mediante una administración delegada. También garantizar que socios, proveedores y clientes dispongan únicamente del acceso necesario para su operativa. Por último, se encuentra Agentic AI & Identity Orchestration. Se trata de un enfoque que engloba un conjunto de acciones para proporcionar a los agentes de IA identidades de confianza, autorización en tiempo real y supervisión humana para que actúen con propósito y no con riesgo; con este planteamiento va más de las reglas estáticas al integrar señales avanzadas de IA para anticipar amenazas, automatizar el cumplimiento normativo y optimizar la seguridad en tiempo real.

La gestión de las identidades digitales también plantea retos cuando se trata de acreditar información de personas y organizaciones de forma segura. En este ámbito entran en juego las credenciales verificables, certificaciones digitales emitida por una fuente de confianza (como un permiso de conducir, un documento de identidad o un título académico) y almacenadas en un monedero digital (Identity Wallet). Así, el usuario mantiene el control total de sus credenciales de identidad y puede presentarlas de forma cifrada. La propuesta de Ping, en este contexto, se alinea plenamente con el marco europeo eIDAS 2.0, lo que permite conciliar la soberanía digital, la protección de la privacidad y la confianza en los intercambios. ¿Cómo emitir y verificar estas credenciales con Ping?

La respuesta se encuentra en las siguientes soluciones: PingOne Verify, PingOne Credentials y PingOne DaVinci. La primera verifica la



identidad real de la persona mediante controles biométricos y documentales, acreditándola de forma sencilla y segura durante el restablecimiento de cuentas, cambios de contraseña... Por su parte, la segunda de estas soluciones emite y gestiona las credenciales verificables en los wallets digitales conforme a estándares abiertos. PingOne Credentials proporciona total interoperabilidad con la plataforma Ping Identity y otros ecosistemas de proveedores de identidad abiertos.

Finalmente se encuentra PingOne DaVinci. Se trata de un estudio de orquestación No-Code que permite diseñar e integrar flujos de usuario a medida arrastrando y soltando elementos. Su interfaz abierta cuenta con integraciones y conexiones a través de múltiples aplicaciones y ecosistemas de identidad.

Ping Identity
sales@pingidentity.com
www.pingidentity.com/es
A consultar

Comparativa

5 soluciones de gestión de identidades y accesos

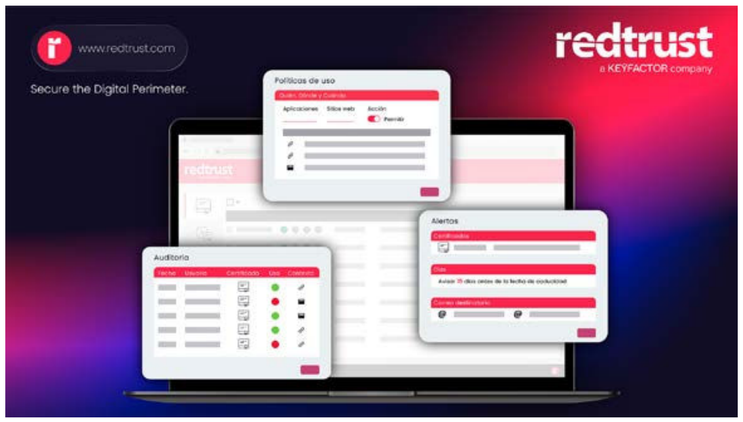
Redtrust – Gestor de certificados digitales

Proteger la identidad digital corporativa. Este es el propósito de Redtrust, firma integrada en el Grupo Keyfactor y con más de 15 años de trayectoria en el mercado español. Actualmente se encuentra en una fase de expansión en Latinoamérica que comenzó en Brasil en 2023, y su cartera reúne a más de 1.700 clientes de sectores tan diversos como bancas y financieras, retail, industria, energía, construcción, transporte y logística, administración pública, y farmacia y salud. Para ayudar al mundo empresarial a blindar, gobernar y automatizar esta identidad digital, se apoya en cinco pilares: gestión centralizada de certificados digitales, firma digital centralizada, autenticación basada en certificados, cifrado centralizado de la información y gobernanza de identidad de agentes de inteligencia artificial.

Participa en esta comparativa con una solución que ha sido diseñada para que las empresas gestionen su identidad digital de forma segura y mantengan el control sobre sus certificados digitales. Así, mediante la centralización y la custodia en un repositorio que es único y cifrado, las organizaciones pueden controlar, proteger y auditar el uso de todos sus certificados.

De igual forma, se pueden configurar políticas de uso con un alto nivel de detalle, supervisar todas las operaciones en tiempo real y gestionar el ciclo de vida de cada certificado, garantizando para ello los siguientes principios clave: seguridad, trazabilidad y cumplimiento normativo. Incluso en el caso de posibles incidentes, los certificados y sus claves permanecen protegidos y no se ven expuestos, evitando aquellos accesos que no son o que no están autorizados, ya que no se instalan en los equipos de los empleados. En su lugar, se custodian en un servidor seguro. Para utilizarlos de forma transparente y sin romper la cadena de confianza, basta con desplegar un agente que actúa como conector entre el equipo y dicho servidor.

Asimismo, con Redtrust las empresas cuentan con una visibilidad total sobre los usos de los certificados, con una auditoría detallada de quién ha utilizado cada uno de ellos, en qué momento y con qué finalidad. Otro de sus puntos fundamentales está relacionado con una implantación rápida y onboarding personalizado: esto incluye una distribución automática de los certificados y el acceso instantáneo a la consola de administración, lo que reduce la carga de trabajo de los equipos de TI. Se trata de una solución escalable, disponible tanto en modalidades cloud como on-premise, y que garantiza su integración con los sistemas corporativos mediante API.



Para una gestión y control de extremo a extremo, es posible definir con precisión las condiciones de uso de los certificados digitales; obtener una trazabilidad completa de todas las acciones realizadas con estos; autenticación y firma digital desde cualquier lugar garantizando una continuidad operativa; y una configuración de alertas de caducidad para evitar los riesgos asociados a los certificados que ya han caducado.

En otro orden de cosas, Redtrust integra Signtrust, un módulo que permite firmar documentos online utilizando los certificados digitales centralizados en su plataforma desde cualquier dispositivo y navegador, y sin necesidad de instalar el agente.

Redtrust
91 905 11 58
redtrust.com
a consultar

Comparativa

5 soluciones de gestión de identidades y accesos

Conclusiones

La elección de una solución de gestión de identidades y accesos depende de las características de cada organización, sus sistemas y las necesidades de protección que tienen. Así, las propuestas seleccionadas responden a distintos escenarios, desde el control de permisos en entornos cloud hasta la protección de las identidades de clientes, empleados y agentes de inteligencia artificial... Sin embargo, dos de ellas destacan ligeramente sobre las demás: son Ping Identity y Redtrust.

La primera lo hace por abordar diferentes tipos de identidad en una misma estrategia: empleados, clientes, socios y proveedores, además de agentes de IA. A ello suma la orquestación de flujos mediante herramientas no-code y la gestión de credenciales verificables. Redtrust, por su parte, centra su valor en la protección de los certificados digitales corporativos. La custodia centralizada, el control detallado de los usos, la trazabilidad y la firma digital desde distintos dispositivos permiten a las empresas mantengan el control en todo momento. El resto de las soluciones son igualmente válidas e interesante.

Amazon Web Services IAM ofrece un control granular de los permisos y herramientas para gestionar accesos a recursos de AWS, incluidas cargas de trabajo externas. Cisco Duo IAM combina autenticación multifactor, acceso sin contraseñas y protección frente al phishing y el secuestro de sesiones, con el apoyo de la inteligencia artificial. Finalmente, Microsoft Entra ID sobresale por administrar usuarios, permisos y aplicaciones desde una plataforma centralizada, aplicar políticas de acceso condicional basadas en riesgos e integrar sus funciones con las soluciones de seguridad de Microsoft.

Aspectos Destacados

Nombre de la solución	AWS Identity and Access Management	Cisco Duo Identity and Access Management	Microsoft Entra ID	Ping Identity	Redtrust-– Gestor de certificados digitales
Valoración	★★★★	★★★★	★★★★	★★★★★	★★★★★
Características clave	* Analizador de accesos de IAM. * Los empleados acceden a una experiencia uniforme y optimizada en todas las aplicaciones de AWS. * Obtención de credenciales de seguridad temporales para cargas de trabajo locales, híbridas y multinube. * Roles de AWS Identity and Access Management. * Auntenticación multifactor.	* Nuevo Directorio de Usuarios: facilita el almacenamiento centralizado de credenciales y roles, y simplifica la gestión de accesos. * Resistencia frente al phishing: innovaciones como Complete Passwordless, Proximity Verification y Session Theft Protection refuerzan la protección frente al robo de credenciales y sesiones. * MFA y SSO avanzados. * IA aplicada a la gestión. * Se conecta con sistemas de identidad de terceros, actuando como proveedor secundario o intermediario.	* Enfoque de Confianza Cero (Zero Trust). * Herramientas de autoservicio. * Administración centralizada de identidades y accesos. * Autenticación sin contraseña. * Security Copilot : uso del lenguaje natural para investigar usuarios de riesgo, detectar anomalías en los procesos de autenticación, supervisar cambios en los accesos e identificar posibles brechas en las políticas de seguridad.	* PingOne Verify: verifica la identidad real de la persona mediante controles biométricos y documentales. * PingOne Credentials: emite y gestiona las credenciales verificables en los wallets digitales conforme a estándares abiertos. * PingOne DaVinci: estudio de orquestación No-Code que permite diseñar e integrar flujos de usuario a medida arrastrando y soltando elementos. * Agentic AI & Identity Orchestration para anticipar amenazas. * B2B & Third-Party Access que simplifica el ecosistema mediante la administración delegada.	* Visibilidad total sobre el uso de los certificados con una auditoría detallada de quién los ha utilizado, cuándo y con qué finalidad. * Los certificados y las claves permanecen custodiados en un servidor cifrado. * Integración con los sistemas corporativos mediante API. * Distribución automática de los certificados y acceso inmediato a la consola de gestión. * Gestión integral, segura y centralizada de los certificados digitales.



Las empresas avanzan hacia entornos digitales más conectados, seguros e inteligentes donde la automatización, los datos y la inteligencia artificial empoderan al empleado y a la organización

Por Alfonso Casas

Trabajo colaborativo.
La nueva experiencia del empleado

Portada

Trabajo colaborativo. La nueva experiencia del empleado

La nueva ola de innovación tecnológica abre la puerta a una forma de trabajar más ágil, en la que la inteligencia artificial, los agentes autónomos y la automatización permiten reducir tareas repetitivas y liberar tiempo para abordar actividades de mayor calado. El reto no consiste únicamente en incorporar herramientas, sino en integrarlas en los procesos de negocio y transformar las mejoras individuales en resultados para toda la organización.

"Las organizaciones que más partido sacan de la IA no son las que más invierten, sino las que empiezan por procesos concretos donde esta tecnología libera tiempo", señala Antonio Torregrosa, Technical PR & Phone de ASUS. Para lograrlo, considera necesario ordenar los datos, identificar qué tareas pueden delegarse y mantener la supervisión humana en las decisiones críticas. Patricia Núñez, PCSD Leader de Lenovo, coincide en la importancia de reducir la fricción operativa y automatizar actividades repetitivas para que los profesionales puedan dedicar más tiempo al trabajo creativo y estratégico.

La evolución hacia un modelo de trabajo más inteligente también pasa por combinar el procesamiento local de los dispositivos con las capacidades de la nube. Esta aproximación híbrida aporta flexibilidad y permite proteger la información sensible, aunque su éxito depende igualmente de la formación de los empleados y de un cambio cultural que facilite la adopción de las nuevas herramientas.

La IA ya está ampliando las posibilidades de los profesionales. "Hemos pasado de una IA que responde a una IA que ejecuta", afirma Antonio Cruz Cruz-Conde, director de AI Workplace de Microsoft España. Según los datos de un estudio recogidos por Microsoft, destaca que el 45,1% de la población española en edad de trabajar utiliza herramientas de IA generativa y el 60% de los profesionales asegura que esta tecnología le permite realizar tareas que hace un año estaban fuera de su alcance. El desafío ahora es extender estas capacidades al conjunto de la empresa: solo el 22% considera que su organización dispone de una estrategia clara y sostenida en torno a la IA.

Este cambio también transforma la colaboración. Enrique Mazón, Regional Vice President Commerce, Revenue Cloud & Slack Iberia de Salesforce, destaca que el trabajo ya no se desarrolla exclusivamente entre personas, sino que incorpora agentes capaces de buscar información, ejecutar tareas y coordinar acciones. Las plataformas colaborativas aspiran así a conectar empleados, aplicaciones, datos y agentes en un entorno común, con asistentes como Slackbot que facilitan el acceso al conocimiento y al contexto de la organización.

> **"La inteligencia artificial debe integrarse en los dispositivos y procesos de trabajo para mejorar la productividad sin comprometer la seguridad ni la privacidad"**
>
> **ANTONIO TORREGROSA, TECHNICAL PR & PHONE DE ASUS**

Tecnologías clave para obtener un mayor impacto

¿Qué tecnologías podrían resultar clave para obtener un mayor impacto?. Para que la innovación transforme realmente el trabajo colaborativo, es necesario conectar dispositivos, redes, plataformas, datos e inteligencia artificial. En lugar de incorporar herramientas de forma aislada, las empresas necesitan construir un ecosistema integrado, seguro y adaptado a las necesidades de los empleados.

Una parte importante de esta evolución comienza en el propio dispositivo. "Los PC con IA integrada se están convirtiendo en la nueva base del puesto de trabajo, ya que permiten ejecutar modelos avanzados en local", destaca Torregrosa. En esta misma línea, Núñez subraya el papel de los equipos equipados con unidades

de procesamiento neuronal (NPU), que aceleran las tareas de IA, y de funciones como los modos inteligentes para reuniones y la cancelación de ruido. La conectividad entre dispositivos y la asistencia técnica remota completan, a su juicio, los elementos necesarios para ofrecer una experiencia más fluida.

Pero el hardware necesita de una infraestructura que garantice la conectividad, la seguridad y la continuidad del servicio. Michel Rodríguez, director de Colaboración en Cisco España, defiende la combinación de "una infraestructura de red segura y resiliente" con plataformas capaces de integrar personas, agentes y aplicaciones, además de herramientas de seguridad y observabilidad. La interoperabilidad también resulta esencial para utilizar diferentes plataformas de reuniones sin perder coherencia en los entornos híbridos.

Sobre esta base tecnológica se construyen las nuevas capacidades de IA. Cruz-Conde identifica tres elementos fundamentales: asistentes para los empleados, agentes especializados en procesos concretos y datos enriquecidos con contexto empresarial. Este último componente resulta decisivo para conectar los sistemas inteligentes con documentos, comunicaciones y procesos de negocio, siempre respetando los permisos y las políticas de gobernanza de cada organización.

Disponer de modelos de lenguaje, plataformas de datos y mecanismos de seguridad, sin embargo, no garantiza por sí solo el aprovechamiento de la IA. Mazón considera necesario incorporar también el contexto de las conversaciones, donde se comparte información y se toman decisiones, y una interfaz colaborativa que facilite la interacción en lenguaje natural entre empleados y agentes. La clave está en acercar la inteligencia artificial al lugar donde se desarrolla el trabajo, en lugar de obligar a los profesionales a cambiar constantemente de herramienta.

> **"La frontera entre la experiencia física y la digital será cada vez menos relevante: personas y agentes colaborarán en los mismos espacios de trabajo"**
>
> **MICHEL RODRÍGUEZ, DIRECTOR DE COLABORACIÓN EN CISCO ESPAÑA**



Portada

Trabajo colaborativo. La nueva experiencia del empleado



La capacidad de comprender ese contexto y convertirlo en acciones es, precisamente, una de las posibilidades que destaca Jorge Hurtado, Sales Manager de Zoom España. Soluciones como ZoomMate permiten preparar documentos y presentaciones, recoger los acuerdos alcanzados en las reuniones y transformarlos en próximos pasos. El objetivo es que «lo decidido deje de quedarse en unas simples notas y pase a ser trabajo hecho».

Seguridad y cumplimiento desde el diseño

La expansión de la inteligencia artificial y de los agentes autónomos en el entorno laboral obliga a reforzar la seguridad, la gobernanza del dato y el cumplimiento normativo. Las empresas deben garantizar que tanto las personas como los sistemas inteligentes accedan únicamente a la información necesaria, mediante controles que permitan supervisar su actividad y prevenir posibles fugas.

Torregrosa defiende la aplicación de principios de confianza cero "Zero Trust", autenticación robusta, cifrado y políticas claras de uso de la IA, acompañados de formación continua. La elección del proveedor tecnológico también resulta estratégica. En este sentido, los equipos ExpertBook de ASUS incorporan mecanismos como BIOS autorrecuperable, chip TPM 2.0 y autenticación biométrica,

> **"El éxito del workplace del futuro no se medirá por la cantidad de IA incorporada, sino por su capacidad para amplificar el talento humano"**
>
> **PATRICIA NÚÑEZ, PCSD LEADER DE LENOVO**

además de capacidad de procesamiento local para evitar que determinados datos tengan que enviarse a la nube.

Para Rodríguez, la seguridad y la gobernanza deben incorporarse desde el diseño de las soluciones. Esto exige conocer qué herramientas y agentes utiliza la organización, qué información manejan y qué acciones pueden ejecutar. "Hay que aplicar controles de identidad y acceso también a los agentes, no solo a las personas", subraya. A medida que estos sistemas adquieren autonomía, resulta imprescindible monitorizar su comportamiento, detectar intentos de manipulación y mantener la capacidad de intervenir durante su ejecución. Estas medidas deben acompañarse de evaluaciones de riesgos, responsabilidades documentadas y supervisión humana proporcional a cada caso de uso.

La gestión de identidades también debe evolucionar para incluir a los sistemas digitales que actúan en nombre de la organización. Cruz-Conde considera esenciales la observabilidad, la auditoría y la supervisión de los agentes. Además, advierte del riesgo de Shadow IT: cuando los empleados no disponen de herramientas corporativas adecuadas, pueden recurrir a aplicaciones de IA de consumo y exponer información empresarial. Facilitar soluciones controladas, establecer políticas claras y formar a los usuarios es, por tanto, fundamental.

Hurtado, por su parte, plantea la seguridad como un elemento que genera confianza y no como un mero requisito normativo. Las organizaciones deben conocer qué datos manejan, dónde se almacenan y quién puede acceder a ellos, además de elegir proveedores comprometidos con la privacidad y la transparencia y cuyos controles estén alineados con la normativa europea.

Convertir el dato en activo estratégico

Para extraer valor de la inteligencia artificial, las organizaciones deben superar la dispersión de la información, garantizar su calidad y facilitar que empleados y agentes puedan utilizarla en el contexto adecuado. La gobernanza del dato se convierte así en una condición indispensable para mejorar la toma de decisiones.

Rodríguez señala que el acceso a información de calidad y la complejidad de prepararla siguen siendo barreras para la adopción de la IA. Conectar datos procedentes de conversaciones, aplicaciones y sistemas operativos permite obtener una visión más completa de la actividad. Así, herramientas como Workplace Insights relacionan la ocupación real de las oficinas con las reservas para mejorar la planificación, mientras que la correlación de datos de redes, dispositivos y aplicaciones ayuda a detectar incidencias y evaluar su impacto en la experiencia del empleado.

El reto, según Mazón, no consiste únicamente en disponer de datos, sino en garantizar que las personas y los agentes accedan a la información correcta con el contexto necesario. Para ello, Salesforce Data 360 unifica la información empresarial, mientras que Slack incorpora el conocimiento generado en las conversaciones de trabajo. "Con Slackbot, ese conocimiento puede combinarse con los datos de Salesforce y con

> **"Las organizaciones pasarán de gestionar aplicaciones a gestionar objetivos"**
>
> **ANTONIO CRUZ CRUZ-CONDE, DIRECTOR DE AI WORKPLACE DE MICROSOFT ESPAÑA**



agentes especializados para pasar de buscar información a utilizarla directamente para tomar decisiones y ejecutar acciones", explica.

Esta integración permite convertir el conocimiento acumulado en resultados operativos. Como ejemplo, Mazón destaca que el agente de TI de Salesforce integrado en Slack redujo un 35% el tiempo medio de gestión de casos en la organización. El caso ilustra cómo la combinación de datos, contexto conversacional y automatización puede trasladar la IA desde la búsqueda de información hasta la resolución de tareas concretas.

Claves de una buena estrategia DEX

Una estrategia de experiencia digital del empleado (DEX) debe conseguir que la tecnología facilite el trabajo, en lugar de convertirse en una fuente de fricciones. Para ello, las organizaciones necesitan combinar rendimiento, facilidad de uso, seguridad, soporte proactivo y formación, con el objetivo de mejorar tanto la productividad como el bienestar digital.

Desde Cisco, Rodríguez considera imprescindible disponer de una visión integral de la experiencia tecnológica, que abarque desde el dispositivo y la conexión WiFi hasta la red corporativa, Internet y las aplicaciones en la nube. La telemetría y la IA permiten detectar incidencias antes de que afecten a los usuarios. A ello se suma la necesidad de integrar los entornos físicos y digitales, garantizar la interoperabilidad de las plataformas de colaboración y coordinar a los equipos de infraestructura, instalaciones y soporte para eliminar obstáculos cotidianos.

El rendimiento del hardware y su adaptación al usuario constituyen otro pilar. Núñez defiende una estrategia que combine dispositivos potentes y portátiles, conectividad y software adaptativo. Funcionalidades como los Smart Modes de

> **La IA dejará de hacer más inteligente al individuo para contribuir a hacer más inteligente a toda la organización**
>
> **ANTONIO TORREGROSA, TECHNICAL PR & PHONE DE ASUS**



los equipos Aura Edition permiten ajustar el dispositivo a diferentes situaciones, desde reuniones y espacios públicos hasta tareas que requieren concentración. Un soporte preventivo capaz de resolver problemas antes de que interrumpan la actividad completa esta propuesta.

Sin embargo, disponer de las herramientas adecuadas no garantiza que se aprovechen. Cruz-Conde propone evaluar la DEX a partir de una pregunta: "¿Cuánta fricción estamos eliminando del día a día de las personas?". El objetivo es reducir el tiempo dedicado a buscar información, coordinar tareas y realizar trabajos repetitivos. Por eso, la formación y la adopción deben formar parte de la estrategia desde el principio.

La experiencia también mejora cuando la IA deja de funcionar de forma aislada y se integra en la dinámica de los equipos. Mazón defiende avanzar hacia una inteligencia artificial compartida: cuando los agentes trabajan en los mismos espacios que las personas, el conocimiento deja de quedar aislado en conversaciones privadas y puede aprovecharse de manera colectiva.

El workplace del futuro

El puesto de trabajo evolucionará hacia un modelo más integrado, flexible y personalizado, en el que las personas y los agentes de inteligencia artificial colaborarán de forma natural. La tecnología dejará de organizarse en aplicaciones aisladas para ofrecer experiencias conectadas que simplifiquen las tareas cotidianas y ayuden a los empleados a centrarse en los resultados. odríguez considera que la frontera entre la experiencia física y la digital será cada vez menos relevante. Personas y agentes compartirán espacios de trabajo, mientras que las salas, las redes y las aplicaciones intercambiarán información para ofrecer una experiencia coherente. Esta visión se

> **"Las herramientas digitales estarán cada vez más integradas, evitando tener que utilizar tantas aplicaciones diferentes como tareas existan"**
>
> **JORGE HURTADO, SALES MANAGER DE ZOOM ESPAÑA**



Portada

Trabajo colaborativo. La nueva experiencia del empleado

refleja en las Intelligent Workplace Experiences de Cisco, que integran redes seguras, dispositivos de colaboración, experiencia digital y espacios físicos en una arquitectura común.

En Lenovo, Núñez anticipa un entorno más adaptativo, contextual y personalizado gracias a la IA, con dispositivos de nuevos formatos que combinarán movilidad y productividad. Los agentes asumirán funciones más activas, desde preparar reuniones y organizar información hasta anticipar tareas o adaptar las herramientas al proyecto en curso. No obstante, advierte de que el éxito no dependerá de la cantidad de IA incorporada, sino de su capacidad para potenciar el talento humano y liberar tiempo para la creatividad, el pensamiento crítico y la toma de decisiones.

Esta evolución también modificará la manera de relacionarse con la tecnología. Cruz-Conde apunta a las denominadas Frontier Firms, organizaciones que no se limitan a añadir IA a sus procesos, sino que rediseñan su modelo operativo en torno a ella. "Pasaremos, en cierto modo, de gestionar aplicaciones a gestionar objetivos", explica. A medida que se deleguen más tareas en los agentes, las personas tendrán que reforzar sus capacidades de pensamiento crítico, creatividad y supervisión, con el foco puesto en los resultados que deben alcanzar.

Mazón coincide en que el trabajo tenderá a concentrarse en un entorno común que reúna personas, datos, aplicaciones y agentes. La IA pasará de ayudar a cada empleado de forma individual a colaborar en espacios compartidos, donde los equipos puedan revisar, corregir y reutilizar los resultados. De este modo, su valor no se limitará a mejorar el rendimiento individual, sino que contribuirá a ampliar la inteligencia colectiva de la organización.

El desafío será construir un workplace conectado e inteligente en el que la tecnología simplifique el trabajo y la IA amplifique las capacidades colectivas, sin sustituir el criterio humano. El verdadero valor de la nueva experiencia del empleado reside en conectar la tecnología con los procesos de negocio, reducir el trabajo manual y conseguir que las ideas y decisiones se traduzcan en resultados concretos. La tecnología, por sí sola, no transforma la forma de trabajar: necesita objetivos claros, datos de calidad, seguridad y una estrategia de adopción que sitúe a las personas en el centro.

Las organizaciones tendrán que preparar a sus equipos para trabajar con agentes, definir nuevas formas de colaboración y decidir qué tareas pueden delegarse en la IA y cuáles requieren criterio humano. La oportunidad está en construir una fuerza laboral híbrida en la que personas y agentes trabajen como colaboradores, combinando automatización y capacidades humanas para mejorar la productividad, la creatividad y la toma de decisiones.



Mujeres TIC

Maica Aguilar

Gerente de Ciberseguridad en Ferrovial y Miembro de la Junta de Women4Cyber Spain



Hijos: Dos adolescentes maravillosos
Hobbies: Pintar, disfrutar de la naturaleza y de las pequeñas cosas del día a día.
Estudios: Ingeniería Informática
Fecha de nacimiento: 30/12/1973

¿Cómo llegó al mundo TIC?
Quería estudiar una Ingeniería. La verdad es que me gustaban las matemáticas y la física, resolver problemas para mí era un reto divertido.

A la hora de elegir finalmente me decante por Informática. Tuve la suerte de elegir carrera en un momento en el que la Informática estaba desarrollándose y me pareció una opción muy interesante. Nunca me ha decepcionado y no me planteo salir del mundo apasionante de la Tecnología. Me siento afortunada de haber sido testigo y parte activa de esta revolución tecnológica y seguir viviendo la transformación social y empresarial que supone.

Comencé por la Ingeniería Técnica en Informática de Gestión porque quería compaginar estudios y trabajo y, ya incorporada al mundo laboral, continue la Superior de Ingeniería Informática. Fueron unos años intenso. No es sencillo compaginar la dedicación laboral y sus horarios con los estudios. Si te has visto en esta situación, seguro que sabes muy bien de que estoy hablando.

Recuerdo esta época con cariño, pero también siendo consciente del sacrificio por la dedicación y esfuerzo, la inversión de tiempo y la renuncia voluntaria a tu tiempo libre. Me viene a la cabeza esas sesiones de cine en que a la media hora de película me quedaba dormida, mi cuerpo decía "aprovechemos para descansar".

¿Qué es lo que más valora de su trabajo?
La diversidad de proyectos, funciones y actividades en las que he participado. Me gusta mucho ese dinamismo, no es nada monótono. También es importante para mí la parte de interacción con distintas empresas y equipos de personas, esta heterogeneidad siempre te enriquece y aprendes formas de hacer diferentes.

En su opinión ¿qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?
Necesitamos generar y visibilizar rol-model que ayude a normalizar la presencia de mujeres en determinadas carreras y se vea

como una opción realista y accesible para las nuevas generaciones.

Tus elecciones, cuando no partes de una vocación clara, se basan en el conocimiento y cercanía. Hay que ayudar a que estas profesiones, que quizá son más desconocidas, se acerquen a la sociedad y rompamos con los estereotipos preconcebidos.

Por otro lado, está claro que hay una diferencia condicionada por el género, eso no es malo, somos distintos y por regla general, nos motivan aspectos diferentes. Tenemos que buscar la igualdad aprovechando y poniendo en valor esas diferencias y la importancia de la diversidad.

Para nosotras es importante percibir una utilidad social en lo que hacemos, el contacto humano y ayudar a los demás. Ese enfoque de cómo desde las carreras STEM se puede mejorar la vida de los demás y fomentar el cuidado y seguridad de la sociedad en general es un aspecto que puede facilitarnos llegar a más mujeres y que vean en la tecnología un propósito que merece la pena.

Tenemos entre todos que "vender" la tecnología mejor, en la sociedad, en los colegios, institutos, etc., tenemos que darle el espacio que realmente tiene a día de hoy.

> **Tenemos que facilitar que cada uno elija y llegue donde quiera llegar, pero desde el conocimiento y la igualdad de oportunidades.**

¿Cree que existe el "techo de cristal" en las empresas TIC? ¿Cuál debería ser la solución?
Creo que se ha avanzado en las últimas décadas, la incorporación de la mujer al mundo laboral de forma masiva ha permitido que se incrementen las mujeres en posiciones directivas en todo tipo de empresas pero es verdad que si en el mundo tecnológico estamos por debajo del 30%, en las posiciones de dirección todavía los porcentajes son muy bajos.

Hay que seguir trabajando entre todos, para que esta tendencia siga incrementándose y no haya retrocesos.

¿Una política de cuotas puede resolver el problema?
Lo ideal sería que llegue un momento en que no tengamos que aplicar medidas para acelerar los procesos. Actualmente esta política de cuotas es una forma de poder reducir los tiempos para contar con un equilibrio necesario y representativo acorde al que tenemos en nuestra sociedad.

Las mujeres en España somos el 51% de la población, no somos minoría, la situación en la que nos encontramos es mejor que la de hace 30 años, pero todavía nos queda mucho recorrido para tener las mismas oportunidades, ocupar determinadas posiciones y romper las barreras y sesgos que todos tenemos y que hacen que las cosas sean hoy como son.

Creo que tenemos que facilitar que cada uno elija y llegue donde quiera llegar, pero desde el conocimiento y la igualdad de oportunidades.

¿Qué dificultades se encontró usted para llegar a la posición que tiene actualmente?
Uno de los hándicaps que tenemos como sociedad es la conciliación de la vida profesional con la personal, no siempre es sencillo cuadrar todas las responsabilidades en la agenda.

Tengo la suerte de haber podido contar con políticas de conciliación y flexibilidad laboral que lo han hecho más fácil y me han permitido adaptarme a las distintas etapas vitales a lo largo de los años.

Por otro lado, podríamos reseñar que en la tecnología, y en mi caso en la ciberseguridad,

se requiere estar permanentemente actualizado, formándote y evolucionando. No es dificultad, es más un desarrollo de capacidades, evolución y adaptación que forma parte inherente de tu profesión, no puedes quedarte estático.

Este tipo de flexibilidad y adecuación permanente ya no es sólo algo de la tecnología, es necesario para todas las funciones empresariales. La IA ha acelerado la transformación y estamos viviendo ese ajuste de funciones en el que las personas tenemos que aportar valor desde una posición más estratégica aprovechando las herramientas que tenemos a nuestra disposición para automatizar, eficientar y reducir determinados procesos. Es un cambio de foco.

¿Qué es lo que más valora de su empresa con respecto a la integración de la mujer?
Mi empresa dentro de las acciones de diversidad lleva años trabajando desde distintos frentes los temas de diversidad de género fomentando y desarrollando distintas iniciativas para atraer, potenciar y visibiliza el talento femenino tanto interna como externamente.

Considero que independientemente del punto de partida en el que se encuentre una empresa lo importante es que tengas en el radar que tienes que actuar para mejorar la situación y te ocupes de ello. Habrá empresas que sean más rápidas y otras más lentas puesto que hay muchos condicionantes, el sector, presupuesto, regulación, países de actividad, etc. Para mí lo más importante es que haya evolución.

> **Una de las decisiones más importantes y que más pueden condicionar la carrera profesional de una mujer es la pareja que elija.**

¿Cómo compatibiliza su vida laboral con la personal? ¿Tiene su empresa planes para poder compatibilizar ambas?
Sí, mi empresa cuenta con medidas variadas para poder fomentar esa conciliación. Algunas más comunes como puede ser flexibilidad horaria o reducción de jornada y otras más vinculadas al bienestar y salud de los empleados desde un plano físico y emocional. También muy necesario puesto que al final la persona es la misma en los dos ámbitos. Algunas que me vienen a la cabeza son la posibilidad de realizar distintas actividades en el ámbito laboral como gimnasio, yoga, pilates, club de montaña, club de runners, servicio de fisioterapia, talleres de salud, etc. Me gusta como mi empresa ha abordado estos aspectos en los últimos años.

¿Qué cree que hay que mejorar en general para que se pueda compatibilizar mejor la vida privada o personal? ¿Es un problema de las empresas, de las relaciones de pareja o de uno mismo?
Considero que es una responsabilidad de todos, de la sociedad, de las empresas y de cada uno de nosotros como integrante de nuestras familias. Hace años asistí a una ponencia de Mercedes Wullich y dijo algo muy interesante que me hizo reflexionar y no es algo a lo que prestemos mucha importancia, la verdad.

Ella comentaba que una de las decisiones más importantes y que más pueden condicionar la carrera profesional de una mujer es la pareja que elija. Contar con una pareja que te permita vivir desde la corresponsabilidad es muy importante.

Mi percepción es que las nuevas generaciones están llevando la conciliación al día día de una forma práctica y más natural que mi generación. Quizá es que ellos hayan vivido la ausencia de sus padres y no quieran repetir determinadas conductas de desequilibrio entre esos dos mundos.

La sociedad se va transformando y confío en que sea para bien.

Mujeres TIC

Maica Aguilar, Gerente de Ciberseguridad en Ferrovial

Un 35% de alumnos no logra ni acabar el bachillerato ni la FP equivalente, ¿está en la educación el problema de la falta de perfiles especializados?
Creo que es más el desajuste de la oferta de perfiles con demanda desde una perspectiva económica. La globalización hace que el talento tenga muchas opciones para buscar ofertas interesantes.

También es verdad que se han fomentado en los últimos años formación académica a todos los niveles tanto universitaria como no univesitaria para ajustar la oferta y demanda pero siempre se requiere un tiempo para encontrar ese equilibrio.

Por otro lado la rapidez en la evolución de la tecnología hace que los perfiles se tengan que adaptar constantemente, pero bueno esta parte son gajes del oficio y no se prevé que vaya a ralentizarse, sino al contrario.

¿Le han servido los estudios que hizo para realizar su labor actual?
Por supuesto que hay una base formativa que viene de los estudios de base pero es importante la formación continua y el desarrollo no solo de esos "hard skills", esos conocimientos especializados sino también de las competencias "Soft", esas habilidades de comunicación, de trabajo en equipo, adaptabilidad, inteligencia emocional, etc.

> **El tener un propósito hace que las vallas y barreras se sobrepasen de forma mucho más fácil**

Solucione el problema de la educación en España...
Creo que se necesita un pacto de estado para definir estrategias de educación a largo plazo que permitan contar en X años con personas con un nivel educativo adecuado para los retos que se aproximan. No me parece que cambiando los planes educativos cada pocos años vayamos a ver resultados significativos. Estamos focalizados en el corto plazo y hay veces que tienes que mirar a lo lejos para establecer la ruta que tienes que seguir.

Si tuviera que aconsejar a una joven qué estudiar de cara a obtener un futuro laboral estable, ¿por dónde le orientaría?
No hay una respuesta mágica para esta compleja pregunta. Es imposible predecir donde vamos a estar en 15 años. Yo le preguntaría al joven que le gusta, en que es bueno y donde se siente él que puede aportar más. El tener un propósito hace que las vallas y barreras se sobrepasen de forma mucho más fácil y puedas superar cualquier obstáculo.

¿Hacia dónde cree que va el sector TIC? En su opinión, ¿cuáles van a ser las tendencias que realmente van a transformar la sociedad?
Considero que estamos viviendo una epoca de inflexión. Hay un antes y un después. El desarrollo y adopción de la Inteligencia Artificial está siendo muy rápido y ha venido para quedarse. Para mí, sin lugar a duda va a transformarnos a todos. Tenemos la oportunidad de tomar un rol activo en vez de espectador y sacar el máximo partido de este momento que nos ha tocado vivir.

IA, automatización, robótica, ¿de verdad cree que el futuro pasa por las personas?
Sí, las personas tienen que estar en ese futuro. No podemos permitirnos otra cosa. La IA, la automatización y la robótica tienen que estar para ayudarnos, tienen que ser herramientas facilitadoras para esta futura humanidad. Si no conseguimos que sea así es que habremos hecho las cosas muy mal.

Un CIO en 20 líneas

"Las personas son clave en el éxito de las empresas, la tecnología por sí sola no cambia los procesos"

Miguel Ángel Melero,
Director de Personas, Procesos y Tecnología en METROVACESA



Por Manuel Navarro

¿A qué se dedica la parte principal de su presupuesto?
Más del 50% del presupuesto ya se dedica a licencias de software, en modo SaaS, PaaS, y mantenimiento, 25% a infraestructuras y seguridad, y otro 25% a proyectos.

¿En qué área se está invirtiendo más este año?
En software de aplicaciones es la mayor inversión/gasto (tomando fuerza la inteligencia artificial), y en cyber, tanto herramientas como servicios de prevención y control.

¿Qué proyecto es del que está más satisfecho?
Claramente los proyectos más rentables actualmente son los que combinan las integraciones con la IA, prácticamente en todos los procesos y departamentos: financiero, marketing y comercial, legal, ...

Un CIO en 20 líneas

Miguel Ángel Melero, Director de Personas, Procesos y Tecnología en METROVACESA

Si le pusieran todo el presupuesto de Metrovacesa a cargo del departamento que dirige, ¿qué le gustaría implementar?
No solo es un problema de presupuesto, también de recursos internos de negocio y de Tecnología. Donde más invertiría sería en agentes de IA en combinación de aplicaciones, que pudieses aligerar los procesos manuales en los ámbitos financiero, compras, gestión de proyectos y comercialización. Hasta ahora estamos implementando mejoras en aplicaciones y flujos de trabajo, estamos usando la IA en múltiples procesos, pero no falta que la IA haga transacciones fiables en nuestras aplicaciones, como SAP, Dynamics, Gestión de Obra, ...

¿Cuáles son los principales retos de su departamento en la actualidad?
Implantar la IA de forma rápida pero ordenada, y conseguir una adopción adecuada y responsable por parte de los empleados y la dirección.

¿Cuál es la herramienta que realmente le cambió la vida?
Primero, Internet y los navegadores universales en las aplicaciones web, después los sistemas de colaboración Skype / Teams, junto con las APPs y movilidad, y ahora la IA.

¿Qué es eso de la importancia de las personas? ¿Slogan o necesidad?
Las personas siempre han sido clave en la evolución y éxito de las organizaciones, la Tecnología por sí sola no cambia los procesos, ni el negocio ni las empresas.

¿Cómo hace para convencer de que es necesario un cambio cultural para afrontar los nuevos retos que afectan a las empresas?
Expongo varias claves: La mentalidad del CEO es CLAVE. En mi caso, además es muy fácil porque me pongo la gorra de RRHH, pero sobre todo y por encima de todo, comunicación e información transparente en todo momento. La estrategia de buscar aliados en negocio siempre funciona, y siempre los encuentras si los buscas.

¿Qué tecnologías emergentes ve con mayor potencial de transformación?
INDUDABLEMENTE LA IMPLANTACIÓN DE LA IA.

¿Qué proyectos están desarrollando actualmente desde su departamento?
Tenemos más de 100 casos de uso de IA por analizar e implantar muchos de ellos, hay muchos proyectos de mejora de procesos comerciales, legales, marketing y financiero.

La ciberseguridad siempre te obliga a estar renovando y protegiendo los flancos de la empresa. Las normativas y exigencias de ESG también nos llevan a adaptar aplicaciones y procesos. Y por último, siempre hay al menos un par de proyectos de upgrade tecnológica en marcha.

¿Cómo ha evolucionado su rol en los últimos años?
Ha ganado mucha relevancia y mayor responsabilidad, pero también mayor riesgo. La automatización, la IA y los riesgos de Ciberseguridad marcan mucho esa evolución.

¿Qué papel juega la inteligencia artificial en su empresa?
En primer lugar, está ya afectando a la tareas diarias y productividad personal de todos los empleados, en segundo lugar, está ya afectando al diseño de muchos procesos, y en un futuro no muy lejano, creo que va a afectar a procesos clave de la actividad, y en consecuencia a la propia organización y funciones, incluyendo a la relación y gestión con proveedores y colaboradores.

¿Cómo está afectando la IA a las personas en Metrovacesa?
La gran mayoría están entusiasmados con lo que están viendo y usando, expectantes y motivados descubriendo nuevos casos de uso, sorprendidos por los resultados que están obteniendo en tan poco tiempo. Y otros pocos, algo más preocupados en sentido negativo, porque pueden ver peligrar sus puestos en el futuro.

Un CIO en 20 líneas

Miguel Ángel Melero, Director de Personas, Procesos y Tecnología en METROVACESA

¿Qué estrategias están aplicando para adaptar a las personas a las tecnologías emergentes?
Como hemos comentado en algún punto anterior, cualquier evolución tecnológica que implique cambio de procesos, lo abordamos con un enfoque triple: 1) consenso del CEO y el comité de dirección, 2) información transparente y comunicación continua, junto con formación; y 3) involucrando al máximo a los usuarios clave, buscando aliados o líderes en los departamentos.

¿Cuál es el principal reto de aplicar el cambio cultural?
En general a las personas les cuesta cambiar su forma de trabajar, pero la mayoría no lo hacen por una mentalidad cerrada o porque no quieran. Las barreras son mucho más sencillas, por ejemplo: Algunos han conseguido procesos muy eficientes que han evolucionado ellos mismos durante mucho tiempo, pero les falta integración, o sea, cada persona es muy eficiente, pero el proceso no lo es en su conjunto. Esto requiere una generosidad profesional, que hay que explicar muy bien, y darles algo a cambio, presente (incentivos) o futuro (beneficios de tiempo/esfuerzo tangibles).

Otra barrera suele ser de disponibilidad, las empresas pretenden cambiar los procesos a la vez que exigen alta productividad y resultados, y las personas no pueden o no quieren dedicar tiempo a su día a día, y sacar tiempo personal extra para cambiar algo que funcionará previsiblemente mejor, pero a medio o largo plazo, y que, en muchos casos, ni siquiera les afectará a ellos. Creo que las empresas deben planificar y compensar esos esfuerzos adicionales y dar mucha visibilidad de las mejoras que van a recibir tras ese esfuerzo extra.

> **La irrupción de la IA es mucho más rápida y agresiva en la forma de trabajar, porque se asemeja mucho más a lo que podemos hacer las personas**

Por último, y en contadas ocasiones, las personas no quieren o no pueden cambiar, y no hay más remedio que cambiarlas a ellas, pero mi experiencia me dice que esto se da en muy pocas ocasiones.

¿Cómo ve el futuro en el medio plazo? ¿Qué cambios cree que se van a producir en la forma de trabajar?
Todas las evoluciones tecnológicas han cambiado los procesos y la forma de trabajar, incluso los perfiles y los puestos de trabajo se han transformado, pero ha sido una evolución lenta, y las organizaciones y personas han tenido tiempo y oportunidades de adaptarse.

La irrupción de la IA es mucho más rápida y agresiva en la forma de trabajar, porque se asemeja mucho más a lo que podemos hacer las personas, y porque el ciclo de adopción y aprendizaje es inmediato.

Esta adopción tan rápida y tan drástica, va a cambiar no solo la forma de trabajar, sino que cambiará rápidamente los procesos, los modelos de negocio (cómo ganar beneficios, y cómo gestionar costes), modelos de organización, tamaños de las mismas, ... algunos puestos desaparecerán cambiarán sus funciones radicalmente, y otros negocios y puestos cobrarán mucho valor.

Debemos estar atentos, y pensar en la implantación de la IA de una forma responsable, que haga empresas sostenibles para los accionistas, pero también para los empleados, los clientes, y la sociedad.

Legalidad TIC

Inteligencia Artificial y derecho: cuando el algoritmo entra en los tribunales

Carlota Parra, Senior Associate de ECIJA

La incorporación de la inteligencia artificial al ámbito jurídico ha dejado de ser una posibilidad futura para convertirse en una realidad que está transformando tanto el ejercicio de la abogacía como el funcionamiento de la Administración de Justicia.

La automatización de tareas, la elaboración de escritos procesales, la investigación jurisprudencial o el análisis de documentación jurídica prometen mejorar la eficiencia y reducir los costes de acceso a la justicia. Sin embargo, esta transformación plantea interrogantes que trascienden la dimensión tecnológica y afectan directamente a principios esenciales del ordenamiento jurídico, como la seguridad jurídica, la buena fe procesal, la tutela judicial efectiva o la responsabilidad profesional.

Desde una perspectiva jurídica, uno de los principales desafíos radica en determinar hasta qué punto puede delegarse en sistemas algorítmicos una actividad que exige interpretación normativa, razonamiento crítico y valoración de circunstancias particulares.

La cuestión adquiere especial relevancia cuando las respuestas generadas por estos sistemas presentan una apariencia de rigor jurídico que no siempre se corresponde con la realidad, trasladando al profesional y, potencialmente, al propio órgano judicial los riesgos derivados de su utilización.

Un ejemplo paradigmático lo encontramos en la reciente sentencia del Tribunal Supremo, Sala Tercera, de lo Contencioso-administrativo, Sección 4ª, Sentencia 803/2026 de 29 Jun. 2026, Rec. 2298/2025. Así, en dicho procedimiento el Alto Tribunal detectó en un escrito procesal referencias jurisprudenciales cuyos pronunciamientos no se correspondían con el contenido real de las resoluciones citadas. El Tribunal constató que los fragmentos entrecomillados no guardaban coincidencia literal ni sustancial con las sentencias invocadas, lo que motivó la remisión del asunto al Consejo General de la Abogacía Española para valorar las eventuales responsabilidades profesionales.

Este supuesto evidencia uno de los riesgos más conocidos de la inteligencia artificial generativa, las denominadas alucinaciones, consistentes en la producción de información



aparentemente coherente y verosímil, pero carente de correspondencia con fuentes reales. En el ámbito jurídico, sus consecuencias resultan especialmente relevantes, pues una referencia jurisprudencial inexistente no constituye simplemente una imprecisión técnica, sino que puede comprometer la fundamentación de una pretensión procesal y alterar las condiciones en las que debe desarrollarse el debate judicial.

Las recientes resoluciones de los tribunales españoles introducen una reflexión particularmente relevante: la disponibilidad de herramientas tecnológicas no reduce el estándar de diligencia exigible al profesional, sino que puede contribuir a concretarlo. El empleo de inteligencia artificial no queda prohibido, pero tampoco permite desplazar hacia el algoritmo la responsabilidad derivada del contenido de los escritos presentados ante los tribunales. La supervisión humana deja así de ser una recomendación de buenas prácticas para configurarse como una exigencia vinculada a los

Legalidad TIC

Inteligencia Artificial y derecho: cuando el algoritmo entra en los tribunales

deberes deontológicos y al principio de buena fe procesal.

La transformación tecnológica del sector jurídico también está ofreciendo resultados que cuestionan los modelos tradicionales de prestación de servicios legales. En Reino Unido, la plataforma Garfield AI, autorizada por el regulador profesional competente, consiguió preparar la documentación necesaria para una reclamación judicial de aproximadamente 7.000 libras, con un coste cercano a 400 libras para la demandante. El procedimiento terminó con una resolución favorable, aunque la representación en juicio la llevo un abogado de carne y hueso.

Así, a la luz de lo anterior, debemos plantearnos las siguientes cuestiones: ¿cuándo una herramienta de información jurídica pasa a prestar verdadero asesoramiento legal? ¿Quién responde por los perjuicios derivados de sus recomendaciones? ¿Y hasta dónde alcanza la responsabilidad del desarrollador cuando el usuario emplea el sistema para adoptar decisiones procesales?

Estas preguntas conectan con un problema más amplio de atribución de responsabilidad en ecosistemas tecnológicos complejos, donde intervienen desarrolladores, proveedores, profesionales y usuarios finales. La intervención de múltiples actores puede dificultar la identificación de quién controla efectivamente el riesgo, especialmente cuando los sistemas generan resultados probabilísticos y sus procesos internos no resultan plenamente transparentes. Por otra parte, la digitalización del entorno jurídico y empresarial también está redefiniendo los límites de la privacidad y la utilización de información obtenida mediante herramientas tecnológicas.

Hay que poner de manifiesto la normativa del Reglamento General de Protección de Datos, las exigencias de confidencialidad profesional y el marco europeo de regulación de la inteligencia artificial, ya que todo ello adquiere una importancia creciente. La utilización de sistemas algorítmicos en entornos jurídicos exige valorar no solo su eficacia, sino también la licitud del tratamiento de la información, las finalidades perseguidas, la proporcionalidad de las operaciones realizadas y las garantías de supervisión humana. Además, determinadas aplicaciones de inteligencia artificial vinculadas a la Administración de Justicia pueden quedar sometidas a obligaciones reforzadas por su consideración regulatoria como sistemas de alto riesgo.

La cuestión de fondo no consiste, por tanto, en determinar si la inteligencia artificial debe incorporarse al Derecho, sino en establecer en qué condiciones puede hacerlo sin debilitar las garantías que justifican la propia existencia del sistema jurídico. La automatización puede contribuir a democratizar el acceso a determinados servicios, mejorar la gestión documental y liberar recursos profesionales para tareas de mayor complejidad, pero su utilidad no elimina la necesidad de preservar la veracidad de las fuentes, la independencia del criterio jurídico y la posibilidad de exigir responsabilidades.

En definitiva, los recientes pronunciamientos judiciales muestran que la inteligencia artificial está dejando de ser únicamente una herramienta auxiliar para convertirse en un factor que condiciona la forma de ejercer, interpretar y aplicar el Derecho. Su integración exige evolucionar desde una confianza basada en la eficiencia tecnológica hacia un modelo de gobernanza sustentado en la verificabilidad, la transparencia, la seguridad y la responsabilidad profesional.

Porque, en última instancia, el verdadero desafío no es conseguir que una máquina sea capaz de elaborar un argumento jurídico convincente, sino garantizar que ese argumento sea correcto, verificable y compatible con los derechos de las personas. La justicia puede apoyarse en algoritmos, pero no puede delegar en ellos las garantías que la definen.

Aplicación Práctica

EMASESA impulsa su digitalización de la mano de IaaS365

EMASESA, Empresa Metropolitana de Abastecimiento y Saneamiento de Aguas de Sevilla S.A., es la entidad que gestiona y administra el ciclo integral del agua en Sevilla capital y once municipios de su área metropolitana. Su objetivo es ofrecer un servicio público de calidad, con un compromiso de transparencia e información permanente a la ciudadanía.

A nivel tecnológico, EMASESA dispone de dos centros de datos, ubicados en la capital andaluza comunicados entre sí mediante red propia, lo que le permite desplegar servicios en uno u otro indistintamente y, en caso de desastre, usar uno de ellos para seguir funcionando sin perjuicio por el que quedase inoperativo. Además, en ellos, alojan importantes equipos y entornos de conmutación que constituyen, en su conjunto, un sistema de misión crítica para la infraestructura de comunicaciones y servicios telemáticos de la entidad.

"La transformación digital de EMASESA exige disponer de una infraestructura tecnológica resiliente, segura y preparada para responder a los desafíos actuales y futuros. Nuestro objetivo no era únicamente renovar tecnología, sino construir una plataforma que sirva de base para la digitalización de procesos, la explotación avanzada de los datos, la automatización de operaciones y la incorporación progresiva de nuevos servicios digitales para la organización", comenta Rafael



Manuel Martínez Torres, Jefe del Departamento de Infraestructuras TIC de EMASESA.

"La situación de partida que teníamos era, por un lado, que ambos CPDs estaban basados en un esquema de tres capas, en el cual los recursos de cómputo, almacenamiento y conectividad teníamos que administrarlos separadamente y donde convivían tecnologías muy diversas, de distintos fabricantes, que nos provocaban una operación compleja y nos dificultaban la gestión técnica y administrativa. A esto se unía, por otro lado, la criticidad de los servicios que estábamos prestando y se prestan desde dichos centros tecnológicos, lo que hacía imprescindible mejorar el plan de continuidad de negocio adaptándolo a las necesidades actuales", añade Rafael.

Dotar de resiliencia a EMASESA

En este contexto, el organismo confió en IaaS365 para llevar a cabo un proyecto para dotarles de resiliencia con dos objetivos. Primero, evolucionar la infraestructura existente adoptando un nuevo modelo innovador, eficiente, seguro y holístico que permita simplificar la administración de los sistemas y el despliegue de nuevos servicios tanto en la plataforma TI local como en la nube. Y, segundo, contar con un servicio de copias de seguridad de los datos y del software que conforman dicha arquitectura tecnológica, que les permita restaurar la situación ante cualquier tipo de problema físico o lógico en los sistemas.

"Desde IaaS365 se trabajó de forma alineada con las exigencias actuales de EMASESA para plantear una solución resolutiva para el presente y también de cara a su evolución futura. El proyecto ha incluido dos retos muy interesantes. Se ha llevado a cabo la prestación de los

Aplicación práctica

EMASESA impulsa su digitalización de la mano de IaaS365

servicios de suministro, instalación y puesta en servicio de una infraestructura hiperconvergente (HCI) que sustituirá a toda la arquitectura x86 actual del organismo. Con este cambio, la entidad va a poder simplificar la gestión de sus centros de proceso de datos, mejorar su seguridad, centralizar la gestión y les permitirá además el crecimiento lineal de la plataforma TI. Y el segundo reto ha sido dotarles de un sistema de copias de seguridad escalable, que les permita el crecimiento en capacidad de cómputo y almacenamiento, sin necesidad de desechar ningún componente ya existente", comenta Rosalía Lima, Regional Account Manager para la zona de Andalucía de IaaS365.

Por su parte, la arquitectura hiperconvergente propuesta cumple con requisitos muy importantes para el correcto funcionamiento de EMASESA. Así, cuenta con un módulo que permite, mediante software, definir firewalls para el control y filtrado granular de las comunicaciones entre máquinas virtuales y aplicaciones. Es compatible con su solución existente de copias de seguridad y con el refuerzo que se ha hecho de la misma. Está preparada para la orquestación de contenedores basada en Kubernetes. Y mejora el sistema de monitorización mediante la automatización de muchas de las tareas TI.

Y, en cuanto a la nueva solución de copias de seguridad, el proyecto les va a dotar de una plataforma distribuida, escalable y de alta disponibilidad que no permita el acceso indebido a los datos salvaguardados y que cuenta con almacenamiento interno. Van a contar además, con inmutabilidad de los datos ante ataques de tipo Ransomware. Les va a proveer de alertas en caso de mal funcionamiento de la solución del tipo que no se estén guardando los datos de forma adecuada, problemas hardware, problemas de rendimiento, etc. Y, también, van a recibir informes sobre el funcionamiento de dicha plataforma, lo que les va a permitir ser proactivos y tomar mejores decisiones.

Para IaaS365, este proyecto es una solución que ejemplifica a la perfección la habilitación de la transformación digital y adopción de nuevas tecnologías para adaptarse a la realidad actual TI. Con la modernización de EMASESA en ambos entornos, la entidad se coloca a la cabeza en innovación institucional volcada a la mejora de los servicios al ciudadano consiguiendo sus objetivos de simplificar la gestión de sus Data Centers, automatizarlos, prepararlos para necesidades y crecimiento futuro y dotarles de mayor seguridad e inmutabilidad.

Con esta iniciativa, IaaS365 consolida su papel como partner tecnológico de referencia, acompañando a EMASESA en todo el proyecto de principio a fin. A los servicios de suministro, instalación y puesta en marcha de ambos retos, se han unido también el de formación al personal del organismo para el correcto uso de las tecnologías implantadas, así como el de mantenimiento y servicio de atención al usuario para contar con un soporte experto personalizado de cara a resolver posibles dudas o incidencias.

EMASESA está encauzando la gestión de sus servicios TI a un modelo de procesos que garanticen la disponibilidad y la mejora continua y con este proceso de digitalización marca un punto de inflexión innovador que la prepara para afrontar el entorno TI tan cambiante.

Al contar con IaaS365 como socio tecnológico para este proyecto, EMASESA consolida una arquitectura tecnológica moderna, segura y preparada para afrontar los futuros retos de una gestión cada vez más digitalizada del ciclo integral del agua. La modernización de sus centros de datos y el fortalecimiento de sus capacidades de continuidad y protección del dato constituyen un paso fundamental dentro de una estrategia más amplia orientada a convertir la tecnología en un elemento impulsor de la eficiencia operativa, la sostenibilidad, la innovación y la mejora continua de los servicios prestados a la ciudadanía.

Tendencias

Como preparar la red empresarial para la IA: la arquitectura es el factor diferenciador

Por David López,
Director de Ventas en España, GTT Communications

Durante la última década, las redes empresariales se han transformado mucho debido a la expansión de la Nube, el trabajo híbrido y la proliferación de dispositivos conectados en el Edge. Actualmente, la inteligencia artificial está acelerando todas estas transformaciones y cambiando de forma radical lo que la red debe ser capaz de hacer. Sin embargo, la mayoría de las redes empresariales no fueron diseñadas para poder afrontar las nuevas dinámicas de la IA.

Las cargas de trabajo de IA generan patrones de tráfico mucho más dinámicos y voluminosos que los previstos en las redes tradicionales. Los datos se desplazan continuamente entre el Edge, la nube y los centros de datos corporativos. A medida que los proyectos pasan de la experimentación a producción, el tráfico se vuelve impredecible y, cuando la WAN no puede absorber esa variabilidad, el rendimiento disminuye y las aplicaciones se ralentizan. Las redes de muchas organizaciones ya muestran signos de presión. Si la capa de red no está preparada para la IA, las estrategias empresariales basadas en ella tendrán dificultades para alcanzar el éxito.

Satisfacer las exigencias de red de las cargas de trabajo de IA requiere un cambio fundamental en el diseño de las redes empresariales: no como canalizaciones estáticas optimizadas para un tráfico predecible, sino como sistemas adaptativos capaces de responder a cambios que aún no se han previsto por completo.

¿Por qué la planificación tradicional ya no funciona?

Hasta ahora la planificación de una red tradicional se centraba en la capacidad: ancho de banda, número de conexiones y rendimiento. Ese enfoque era válido cuando la demanda era relativamente predecible. Sin embargo, el éxito de la IA depende no solo de la potencia de cálculo de GPUs y CPUs sino también de la capacidad de mover datos de forma eficiente a través de la red.

Sectores como la industria, el retail o las finanzas están llevando la IA al Edge para habilitar inteligencia en tiempo real y de baja latencia, operaciones más inteligentes y herramientas innovadoras como la visión artificial, el mantenimiento predictivo, la personalización en tienda o detección de fraude en tiempo real. Como estos sistemas procesan datos localmente y refinan los modelos de forma centralizada, necesitan una infraestructura Edge-to-Core robusta capaz de transportar grandes volúmenes de datos sin crear cuellos de botella.

Por ello, las organizaciones deben dejar de pensar únicamente en capacidad y empezar a planificar capacidades y adaptabilidad. Deben preguntarse si la red puede mover datos eficientemente entre el Edge y los recursos centralizados, soportar grandes volúmenes de



Tendencias

Como preparar la red empresarial para la IA: la arquitectura es el factor diferenciador

tráfico este-oeste, adaptarse a nuevas cargas de trabajo y autenticar de forma segura a un número creciente de usuarios, dispositivos y agentes autónomos.

Diseño de una arquitectura de IA multinivel

Una implantación exitosa requiere una arquitectura multinivel diseñada específicamente para flujos dinámicos de datos entre el Edge, nodos regionales y la nube. El Edge procesa inferencias en tiempo real y captura datos cerca de su origen, pero cada entorno tiene necesidades diferentes: los vehículos autónomos requieren latencia ultrabaja, mientras que los sensores industriales priorizan comunicaciones deterministas y alta fiabilidad.

Los nodos regionales agregan datos antes de enviarlos a la nube o de vuelta al Edge. El equilibrio dinámico de carga, la optimización de protocolos y el enrutamiento adaptativo permiten gestionar mejor los flujos de IA de gran volumen. Las plataformas Cloud de hiperescala soportan el entrenamiento centralizado de modelos y la inferencia a gran escala. Las arquitecturas de IA deben integrarse de forma transparente con estrategias híbridas y multicloud.

Las infraestructuras definidas por software aportan flexibilidad y escalabilidad, pero las WAN



tradicionales no fueron concebidas para gestionar tráfico dinámico entre entornos tan diversos. Las iniciativas de IA requieren SD-WAN, modelos Zero Trust, detección de amenazas en tiempo real y cifrado extremo a extremo.

La flexibilidad no es una característica: es una estrategia

Cuando los requisitos evolucionan tan deprisa, la flexibilidad se convierte en una ventaja competitiva. Los ecosistemas cerrados de un único fabricante pueden ofrecer buen rendimiento, pero dificultan la incorporación de nuevas tecnologías y la interoperabilidad.

Las arquitecturas abiertas y agnósticas permiten integrar nuevas soluciones y evolucionar la red con el tiempo. La pregunta estratégica ya no es qué fabricante ofrece el mejor valor, sino qué arquitectura proporciona la flexibilidad necesaria para conectar, escalar e innovar conforme evolucionan los requisitos de la IA.

Construir la red para la era de la IA

Las organizaciones que triunfen serán aquellas que consideren la red como una plataforma estratégica y no como un activo fijo. Las arquitecturas abiertas, flexibles e interoperables estarán mejor preparadas para integrar nuevas tecnologías y ampliar las iniciativas de IA.

La verdadera ventaja será la agilidad. Las cargas de trabajo, los modelos, los métodos de entrenamiento, los requisitos de inferencia y las necesidades de seguridad seguirán evolucionando. Las redes que se desplieguen hoy deberán ser capaces de soportar cargas de trabajo que todavía no existen.

Las decisiones de infraestructura que se tomen ahora determinarán si la IA se convierte en una ventaja competitiva sostenible o en una costosa limitación operativa. Elegir arquitecturas y proveedores que permitan crecer, adaptarse e integrar nuevas capacidades será esencial para innovar al ritmo que exige la inteligencia artificial.

Tendencias

Sandbox: entre innovación y mercado

Por Olga Rivera,
Project Manager European Funds

El sandbox regulatorio, o espacio controlado de prueba, es un marco estructurado que permite experimentar con tecnologías, productos, servicios o modelos innovadores en condiciones reales o próximas a la realidad, durante un periodo y ámbito delimitados, bajo supervisión regulatoria y con las garantías adecuadas. En los últimos años, este concepto ha adquirido una relevancia creciente en sectores donde la velocidad de la innovación está generando nuevos desafíos regulatorios, como la inteligencia artificial, las tecnologías energéticas, la economía circular, la movilidad autónoma o nuevos modelos industriales.

¿Qué aporta frente a los instrumentos existentes?

Su principal valor es que permite reducir los riesgos asociados al proceso de innovación, facilitando que empresas, administraciones y organismos reguladores generen conocimiento conjuntamente antes de que una solución llegue al mercado. Pero ¿qué aporta realmente frente a los mecanismos de experimentación que ya existían? Un sandbox no tiene como objetivo principal comprobar únicamente si una tecnología funciona. Para eso ya existen herramientas como los laboratorios, que permiten validar tecnologías en condiciones muy controladas; las plantas piloto, que evalúan su funcionamiento a mayor escala; los testbeds, orientados a analizar prestaciones, interoperabilidad o escalabilidad; o los living labs, donde usuarios y otros actores participan en procesos de experimentación.

Todos estos instrumentos responden principalmente a una pregunta: ¿funciona la tecnología? El sandbox introduce otra cuestión: ¿puede esta tecnología funcionar dentro del marco administrativo, operativo y regulatorio existente? ¿Existen barreras regulatorias? ¿Es necesario interpretar determinados requisitos? ¿Debe adaptarse algún procedimiento para permitir la aplicación segura de una nueva tecnología? Esta es la principal diferencia entre un sandbox regulatorio y otros espacios de experimentación: la existencia de una cuestión regulatoria concreta y la participación de una autoridad competente que supervise el proceso. Por ello, un sandbox no es simplemente un piloto tecnológico en un entorno real. Para que exista una experimentación regulatoria debe identificarse una incertidumbre o barrera normativa, definir qué se quiere analizar desde el punto de vista regulatorio y establecer un marco de colaboración entre innovadores y reguladores.

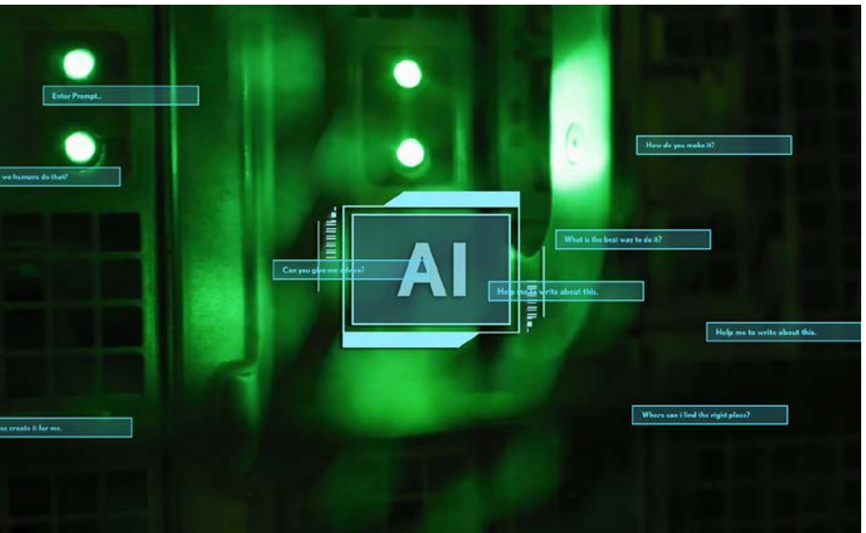


Un entorno controlado: reglas, límites y garantías

En la práctica, se establecen unos requisitos para garantizar que la experimentación sea controlada: la solución no debe encontrarse en fase comercial, la actuación debe ser reversible y, si requiere la instalación de dispositivos o equipos, estos deben poder retirarse al finalizar la prueba dejando el entorno en su estado inicial. Además, la participación en un sandbox no implica una obligación de compra por parte de la Administración y los costes asociados suelen ser asumidos por la empresa promotora. Estas condiciones son fundamentales

para separar la experimentación de la contratación pública, ya que participar en un sandbox no significa vender una solución a una Administración ni garantiza una futura adquisición. El objetivo principal es generar conocimiento y evidencias que permitan determinar si una solución puede desplegarse posteriormente y bajo qué condiciones. Para ello, el proceso debe contar con un plan de pruebas (sandbox plan) que defina objetivos, metodología, indicadores, responsabilidades, mecanismos de seguimiento y criterios de salida, manteniendo siempre las salvaguardas necesarias en ámbitos como la seguridad, la protección de datos, el medio ambiente, los consumidores o los derechos fundamentales.

Incluso cuando una prueba no alcanza el resultado esperado, el aprendizaje generado es valioso. Identificar limitaciones técnicas, dificultades operativas o barreras regulatorias permite mejorar la solución y anticipar problemas antes de una implantación a gran escala. Este



aprendizaje compartido es precisamente uno de los elementos diferenciales del sandbox: el denominado regulatory learning, que permite tanto al innovador como al regulador comprender cómo funciona una tecnología en condiciones reales y cómo debería evolucionar el marco normativo.

Europa impulsa los sandboxes

Este enfoque está adquiriendo una importancia creciente a nivel europeo. La propuesta de Recomendación del Consejo presentada por la Comisión Europea el 9 de septiembre de 2026 (COM(2026) 568 final) establece principios comunes para el desarrollo de regulatory sandboxes en la Unión Europea, con el objetivo de reducir la fragmentación entre Estados miembros y facilitar un marco más coherente para este tipo de experimentación. La propuesta destaca que los sandboxes no buscan desregular, sino crear espacios seguros donde innovación y regulación puedan evolucionar conjuntamente.

Un ejemplo representativo es el AI Act europeo, que incorpora el concepto de AI regulatory sandbox, donde los proveedores de sistemas de IA pueden desarrollar, entrenar, validar y probar soluciones innovadoras bajo la supervisión de las autoridades competentes durante un periodo limitado. En este caso, el objetivo no es únicamente comprobar que el sistema funciona técnicamente,

> **Un sandbox no sustituye a los pilotos, los living labs o los testbeds. Los complementa incorporando una dimensión que antes aparecía más tarde**

sino analizar aspectos regulatorios clave como la gobernanza de datos, la documentación técnica, la transparencia, la supervisión humana, la gestión de riesgos o la futura evaluación de conformidad.

Por tanto, un sandbox no sustituye a los pilotos, los living labs o los testbeds. Los complementa incorporando una dimensión que tradicionalmente aparecía más tarde en el proceso de innovación: la interacción entre la tecnología y el entorno regulatorio y administrativo en el que deberá operar. En un contexto europeo que busca acelerar la llegada al mercado de nuevas tecnologías sin reducir los niveles de seguridad, protección ambiental o derechos de los ciudadanos, los sandboxes pueden convertirse en una herramienta clave para cerrar la brecha entre innovación, demostración y despliegue.

Entrevista

Ramón Valiente,
director de banca y seguros de DXC

"La principal necesidad de los bancos es ganar agilidad sin perder solidez"



Manuel Navarro

El sector bancario afronta un punto de inflexión donde la prioridad es ganar agilidad sin perder solidez. Para responder a las exigencias regulatorias, la IA y los nuevos ecosistemas digitales, DXC Technology ha lanzado DXC CoreIgnite. Esta plataforma de orquestación nativa en la nube permite a las entidades conectar su core bancario tradicional con servicios de terceros y fintechs, reduciendo la complejidad operativa e impulsando la innovación de forma segura. Hablamos sobre ella con Ramón Valiente, Director de Banca y Seguros de la compañía.

¿Cómo calificaría la situación de las TI del sector bancario en la actualidad?
La banca se encuentra en un punto de inflexión tecnológico. Durante los últimos años las entidades han avanzado con éxito en digitalización, automatización y experiencia de cliente, pero ahora el foco se está desplazando hacia la modernización de las plataformas que sostienen el negocio.

Los bancos necesitan responder con rapidez a nuevos modelos de pagos, exigencias regulatorias, ecosistemas de partners y expectativas de clientes cada vez más digitales. Esto obliga a evolucionar arquitecturas que fueron diseñadas

Entrevista

Ramón Valiente, director de banca y seguros de DXC

para priorizar estabilidad y volumen transaccional, pero no necesariamente para integrarse con la velocidad que exige el mercado actual.

En nuestra experiencia, el reto no es tanto sustituir lo que funciona como reducir la complejidad acumulada durante años para ganar agilidad sin comprometer la resiliencia, la seguridad ni la continuidad operativa. Y no hablamos de algo abstracto. DORA ya es una realidad para las entidades financieras, los pagos inmediatos se han convertido en una prioridad regulatoria en Europa y la irrupción de la IA está elevando el valor estratégico de los datos que residen en los sistemas core. Todo ello obliga a evolucionar capacidades tecnológicas mientras una parte importante de los recursos sigue destinada a mantener infraestructuras críticas que soportan el negocio cada día.

¿Cuáles son las principales necesidades que tiene y cuáles son los principales retos que debe afrontar?
Desde mi punto de vista, la principal necesidad de los bancos es ganar agilidad sin perder solidez. El sector opera sobre infraestructuras críticas que exigen máximos niveles de disponibilidad, seguridad y cumplimiento, pero al mismo tiempo debe responder a nuevos competidores, nuevas expectativas de cliente y nuevos modelos de negocio.

El reto está en evolucionar esa tecnología para que sea más abierta, flexible y preparada para

> **Desde mi punto de vista la principal necesidad que tienen los bancos es ganar agilidad sin perder solidez**

trabajar en ecosistemas digitales, sin tener que replantear constantemente sistemas que siguen siendo esenciales para la operativa diaria. La clave no es sustituir lo que existe, sino construir sobre ello capacidades que permitan innovar más rápido, reducir complejidad y aprovechar mejor el valor de los datos y de las inversiones realizadas durante años.

¿Qué representa el lanzamiento de DXC CoreIgnite para el catálogo de soluciones bancarias de DXC Technology y qué necesidad cubre?
CoreIgnite responde a una necesidad que vemos de forma recurrente en el sector, la de acelerar la innovación sin abordar complejos programas de sustitución del core bancario. La plataforma incorpora una capa de orquestación que permite conectar sistemas core con ecosistemas fintech, plataformas de pago, servicios financieros embebidos y nuevas capacidades digitales desde una arquitectura abierta y escalable.

En cuanto a la principal necesidad que cubre CoreIgnite, yo diría que es ayudar a los bancos a cerrar la brecha entre la velocidad a la que evoluciona el mercado y la estabilidad que exige su operativa diaria. Las entidades necesitan incorporar nuevas capacidades digitales, colaborar con terceros y lanzar nuevos servicios con mayor agilidad, pero sin comprometer la seguridad, la fiabilidad y la resiliencia de sus sistemas core. A diferencia de las capas de integración tradicionales, CoreIgnite no pide al banco reemplazar nada ni construir a medida: activa lo que ya tiene. Y no es teoría: los primeros despliegues con partners de BNPL y de activos digitales ya están en marcha, operativos desde la propia app del banco.

¿Implementar CoreIgnite supone reemplazar el lagacy?
No. De hecho, uno de los principios fundamentales de CoreIgnite es precisamente evitar que los bancos tengan que reemplazar sistemas críticos para poder innovar. La realidad del sector es que los sistemas core continúan desempeñando una función esencial y siguen procesando el negocio principal de las entidades. La cuestión no es reemplazarlos necesariamente, sino permitir que convivan con arquitecturas más modernas.

Nuestra visión es que la modernización debe ser progresiva. CoreIgnite actúa como una capa de desacoplamiento que permite introducir nuevas capacidades digitales sin alterar continuamente

Entrevista

Ramón Valiente, director de banca y seguros de DXC

el core bancario. Esto reduce riesgos, protege las inversiones existentes y facilita una evolución tecnológica mucho más sostenible.

¿En qué medida acorta CoreIgnite el time-to-market de un nuevo servicio financiero?
Hoy el mercado exige a los bancos responder con mucha más agilidad que hace unos años. El desafío es que detrás de cada nuevo servicio existen integraciones, pruebas, procesos regulatorios y múltiples equipos trabajando de forma coordinada. Y en banca eso no puede hacerse sacrificando ni la seguridad ni la estabilidad.

Lo que aporta CoreIgnite es una forma mucho más sencilla de incorporar nuevas capacidades sobre la infraestructura existente. Al disponer de una capa común de orquestación, las entidades evitan tener que empezar de cero cada vez que quieren conectar un nuevo servicio o un nuevo partner. En la práctica, esto significa pasar de proyectos que antes duraban meses a lanzamientos en cuestión de semanas. Un ejemplo: un producto de buy now pay later puede llegar a estar operativo en plazos muy reducidos, apoyándose en la infraestructura que el banco ya tiene. Y hay algo más: el cuello de botella no siempre es técnico. Los procesos de riesgos, cumplimiento y aprobación de producto pesan tanto como la integración, y ahí la plataforma también ayuda, al ofrecer controles y marcos reutilizables ya gobernados.

> **Lo que aporta CoreIgnite es una forma mucho más sencilla de incorporar nuevas capacidades sobre la infraestructura existente**

Al final, hablamos de algo muy simple, menos tiempo conectando sistemas y más tiempo lanzando servicios que respondan a las necesidades del mercado y de los clientes. Pero para mí hay algo igual de importante ya que no se trata solo de ir más rápido, sino de innovar con más confianza y con menos riesgo para el negocio.

La plataforma da soporte a servicios basados en activos digitales y stablecoins. ¿Están los bancos españoles y europeos preparados para adoptar esta tecnología de forma masiva o hay barreras regulatorias?
Estamos viendo un interés creciente por parte de las entidades financieras, especialmente a medida que se clarifica el marco regulatorio europeo. Sin embargo, creo que todavía es pronto para hablar de una adopción masiva. En banca, la tecnología por sí sola nunca es suficiente. Tiene que venir acompañada de seguridad jurídica, modelos operativos sólidos y una propuesta de valor clara para el negocio y para el cliente. Y ese marco ya existe: MiCA está plenamente en aplicación, el régimen piloto europeo permite experimentar con la tokenización de instrumentos financieros y el euro digital ya tiene calendario: el BCE prevé un ejercicio piloto a partir de mediados de 2027. La regulación ha dejado de ser una incógnita para convertirse en un terreno de juego definido.

Los bancos europeos están analizando activamente las oportunidades que pueden ofrecer los activos digitales, las stablecoins o la tokenización, pero lo están haciendo con la prudencia que caracteriza a una industria donde la confianza es un activo fundamental. Por eso veremos avances progresivos y vinculados a casos de uso concretos antes que despliegues generalizados.

Desde nuestra perspectiva, el verdadero desafío no está tanto en incorporar estas tecnologías como en integrarlas de forma segura y eficiente dentro de los procesos y plataformas existentes. Las entidades buscarán soluciones que les permitan explorar nuevas capacidades manteniendo los niveles de control, cumplimiento normativo y resiliencia operativa que exige la actividad financiera.

Adoptado Digital



Manuel López

La seguridad que no sabíamos que existía

No hay semana en la que no conozcamos algún nuevo ciberataque. Empresas paralizadas, datos robados, identidades suplantadas, contraseñas comprometidas... Y eso sin contar los intentos que sufrimos personalmente, cada vez más frecuentes y sofisticados. Pero por si no tuviéramos bastante, se aproxima un competidor capaz de cambiar las reglas del juego: la computación cuántica.

Su capacidad para resolver determinados problemas matemáticos podría dejar obsoletos muchos de los mecanismos criptográficos que hoy protegen nuestras comunicaciones, transacciones y datos. No todos, ni de la misma manera, pero sí algunos de los más utilizados. Y aunque todavía no disponemos de ordenadores cuánticos capaces de romperlos a gran escala, la amenaza ya está provocando movimientos importantes. Estados Unidos ha convertido la criptografía poscuántica (PQC) en una prioridad estratégica, estableciendo obligaciones y calendarios de transición. Europa también empieza a ponerse las pilas, con una hoja de ruta que contempla iniciar la migración en 2026 y priorizar los sistemas críticos antes de 2030.

Hasta aquí, podríamos pensar que el problema consiste simplemente en sustituir unos algoritmos criptográficos por otros más seguros. Pero hay una dificultad mucho más sorprendente: muchas empresas ni siquiera saben exactamente qué mecanismos de seguridad están utilizando. Durante años, la criptografía se ha incorporado a aplicaciones, dispositivos, redes, servicios en la nube y sistemas heredados, creando un entramado de protecciones que funciona silenciosamente y que no siempre está documentado. ¿Cómo sustituir algo que ni siquiera sabemos dónde está?

Por eso, antes de implantar PQC, las organizaciones tendrán que realizar un auténtico ejercicio de arqueología digital: descubrir e inventariar sus mecanismos criptográficos, analizar sus vulnerabilidades frente a futuros ataques cuánticos, identificar posibles agujeros de seguridad y establecer prioridades para corregirlos. Afortunadamente, empiezan a existir herramientas capaces de automatizar parte de ese descubrimiento y análisis. Porque la transición poscuántica no comienza comprando nuevas soluciones, sino conociendo los riesgos de las que ya tenemos.

El primer desafío de la seguridad poscuántica no será proteger lo que tenemos, sino descubrir todo lo que estamos protegiendo sin saberlo.

RENDIMIENTO DE ÉLITE PARA CAMPEONES.



SANDISK
OPTIMUS™

SANDISK y el logotipo SANDISK Optimus son marcas registradas o marcas comerciales de Sandisk Corporation o sus filiales en Estados Unidos y/u otros países. El resto de marcas son propiedad de sus respectivos titulares. Las especificaciones de los productos están sujetas a cambios sin previo aviso. Las imágenes mostradas pueden diferir de los productos reales. © 2026 Sandisk Corporation o sus filiales. Todos los derechos reservados.