it Digital MAGAZINE

Nº 38 · MAYO 2026

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

CRIME AS A SERVICE, LA INDUSTRIALIZACIÓN DEL CIBERCRIMEN

MODELOS OPERATIVOS Y HERRAMIENTAS PARA UNA GESTIÓN DEL DATO UNIFICADA, EFICIENTE Y SEGURA

EL ROL DEL PROVEEDOR DE SERVICIOS GESTIONADOS ANTE EL ESTADO DE LA CIBERSEGURIDAD EMPRESARIAL

ENTREVISTA A ATHENA KARP, SVP OF PRODUCT DE WORKDAY

QNAP AFIANZA SU ESTRATEGIA PARA EL MERCADO ENTERPRISE

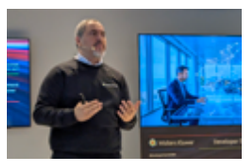
#CONTENIDOS IT

CRIME AS A SERVICE, LA INDUSTRIALIZACIÓN DEL CIBERCRIMEN

NO SOLO IT

ACTUALIDAD

>> QNAP afianza su estrategia para el mercado Enterprise



>> El desarrollo de software con IA protagoniza el Developer Summit 2026 de Wolters Kluwer

>> V-Valley impulsa la ciberseguridad en el canal en el Cybersecurity Summit 2026

ÍNDICE DE ANUNCIANTES

it Digital MAGAZINE

Nº 38 · MAYO 2026

REVISTAS DIGITALES

ENTREVISTA

Athena Karp,
SVP of Product de Workday

Foros Tendencias Tecnológicas @aslan

CIBERSEGURIDAD & IA

20 de mayo

AUTOMATIZACIÓN, EL DATO & IA

24 de junio

PUESTO DE TRABAJO & IA

23 de septiembre

NUBE HÍBRIDA, MULTI-CLOUD & IA

28 de octubre

+ Participa #ForosASLAN **+ www.aslan.es/Foros**

ORGANIZA @aslan *Juntos aceleramos la digitalización*

Creamos espacios de encuentro y divulgación tecnológica gracias al apoyo de más de 200 empresas asociadas. Iniciativas conectadas con:

ASLAN 34 ED 2027 **16, 17 y 18 MARZO** MADRID

QNAP AFIANZA SU ESTRATEGIA PARA EL MERCADO ENTERPRISE

Durante el Media Day 2026, el fabricante QNAP ha expuesto a la prensa su estrategia de negocio para este año, en la que ha reforzado su propuesta para el segmento Enterprise con soluciones completas que abarcan hardware, software y servicios para grandes proyectos y centros de datos. Además, ha adelantado sus próximas novedades, entre ellas nuevas plataformas para ejecutar inteligencia artificial en entornos on-premise.

RICARDO GÓMEZ (MADRID)

El pasado 21 de abril QNAP reunió en la capital a un grupo de periodistas del sector para dar a conocer su estrategia para el mercado de almacenamiento y networking en 2026. Adrián Groba, country manager de QNAP, ha destacado que su facturación creció un 16% en 2025, un año en el que el mercado comenzó moviéndose lentamente, pero que en la última etapa se benefició de “una especie de frenesí” en las compras, a raíz de las subidas iniciales de precios de componentes como los SSD, los discos duros HDD y, especialmente, la memoria RAM. Tras esta eta-

pa, comentaba, QNAP ha registrado un crecimiento del 39% en el Q1 de 2026, una fuerte subida que relaciona con el cambio de enfoque que han venido haciendo durante los últimos tres o cuatro años, hacia el segmento Enterprise, y también por la labor de su equipo local de Iberia.

ENFOQUE EN EL SEGMENTO ENTERPRISE

El esfuerzo estratégico más importante que ha realizado QNAP en este tiempo, explicaba Adrián Groba, es enfocarse en el mercado Enterprise, yendo más allá del B2B para pymes para entrar en grandes proyectos de infraestructura, con servidores, almacenamiento y redes, “porque vemos que es ahí donde está el potencial de crecimiento”. Con esto en perspectiva, tienen intención de duplicar su facturación para finales de este año.

Para lograrlo, están centrándose en la resiliencia del dato y a este nivel ya son capaces de ofrecer “funcionalidades como backup offline o backup inmutable, entre otras, a nivel Enterprise, mediante “una solución completa y flexible”, que abarca hardware, software y servicios, tanto de almacenamiento como de networking.

PROPUESTA BASADA EN SOLUCIONES COMPLETAS

Precisamente, explicaba el responsable de QNAP, la propuesta de la compañía ha pasado de estar basada en productos a centrarse en soluciones, aportando al cliente flexibilidad para escoger si quiere trabajar 100% con sus soluciones o si quiere combinarlas con las de otro proveedor, evitando el vendor lock-in. En este sentido, aunque cuentan con su propia nube, señalaba que “somos compatibles con más de 46 servicios de cloud reconocidos a nivel mundial”.

Aunque su presentación no ha sido de producto, como tal, Adrián Groba ha destacado algunas de sus últimas novedades en almacenamiento y networking, y no solo de hardware, sino también a nivel de funcionalidades de software y servicios pensados para la resiliencia de datos.

Entre ellas, “backup a nivel archivo y a nivel bloque, copia de seguridad de cualquier dispositivo de la nube, inmutabilidad tanto a nivel de backup como de instantánea”, y “unos niveles cada vez mayores de automatización”. También destacó su solución de backup offline y un

INTELIGENCIA ARTIFICIAL ON-PREMISE

QNAP quiere adentrarse en el floreciente mercado de infraestructura pensada para la IA y, para ello, como ha explicado Adrián Groba, están a punto de lanzar soluciones NAS pensadas “para empresas que quieran tener su inteligencia artificial on-premise, sin salir de su LAN”, una primicia que llegará próximamente al mercado. Se trata del NAS QAI h-1290FX, que empleará el sistema QTS Hero y gráficas Nvidia, que pueden ser RTX Pro 6000 o 4500. Explicó que, de momento, permitirán ejecutar hasta cuatro modelos de IA diferentes y que tendrán un precio, sin discos duros, que comenzará en unos 19.000 euros. Añadiendo SSD NVMe, el coste podría estar en torno a 95.000, 96.000 euros.

nivel de monitorización centralizada, donde se ven todos los backups de todas las infraestructuras que estén conectadas a esa aplicación".

Además, subrayó cómo, yendo más allá del concepto cloud first, en QNAP han evolucionado hacia el "Cloud Smart, o Smart Cloud" que, en sus palabras, consiste en "utilizar la nube para aquellos servicios que funcionan y que tienen sentido, en los casos de uso y para los profesionales que tienen sentido", y no utilizarla para todo.

Por otro lado, quiso destacar su enfoque en la continuidad de negocio a través de los servicios y funcionalidades de alta disponibilidad, y cómo han llevado esto al segmento Enterprise. Por ejemplo, con una cabina de doble controladora con redundancia en todos sus componentes, y con la alta disponibilidad en máquinas virtuales, a través de la plataforma Virtualization Station (en fase beta).

En la parte de networking, Adrián Groba explicó que cuentan con una serie de switches con funcionalidad multi-chasis que permite la agregación de puertos entre diferentes equipos. Por último, puso en valor las funcionalidades que QNAP ha ido desarrollando y mejorando en los últimos años, que ofrecen al usuario numerosas posibilidades, especialmente en la seguridad de los datos y la red.

MEJORAS EN EL SERVICIO AL CLIENTE

Otra de las áreas en las que incidió Adrián Groba es en el servicio postventa, donde tienen un nivel básico con reemplazo avanzado Next Business Day y soporte telefónico en horario laboral, y un nivel con reemplazo avanzado Next Business Day con intervención on-site, disponible también para los discos que van en los servidores, y con un servicio de instalación y configuración inicial. Pero lo que el responsable quiso destacar es el próximo lanzamiento de un servicio superior, con soporte "24-7, a nivel de ticket y telefónico, con intervención on-site, con un tiempo de resolución de 4 horas y un tiempo de intervención on-site en máximo 6 horas".

En este encuentro con los medios también estuvieron presentes Pedro Barranquero, business development manager para Iberia de QNAP, Gloria Cuesta, channel account manager para España; y Belén Ruiz Pintos, marketing manager para España y Portugal. ■

MÁS INFO +

- QNAP afianza su estrategia para el mercado Enterprise
- QNAP facilita la migración hacia redes de 100GbE con un nuevo switch gestionable

COMPARTIR EN REDES SOCIALES

Clica en la imagen para ver la galería completa

NOVEDADES PARA 2026

Adrián Groba desgranó las claves del éxito que están teniendo en su estrategia para abordar el mercado Enterprise y detalló las principales novedades de la compañía en productos y servicios

D-Link 40 ANNIVERSARY

Gestión Unificada de Redes Empresariales
100% CLOUD
100% GRATUITA

nuclias unity

¡Pruébalo aquí!

D-Link Nuclias Unity es una **plataforma web de administración de redes alojada en la Nube** para ofrecer **la máxima agilidad,** desde la **configuración inicial** de switches y puntos de acceso Wi-Fi **a la gestión avanzada de redes LAN y WLAN.**

Con **capacidad multi-sede gracias al acceso remoto 100% Cloud**, dispone de funcionalidades como topología de red, panel de color para identificación de puertos, gestión de VLANs, SSIDs, radio frecuencias y canales, portal cautivo, etc. En switches de agregación o core se puede acceder a su propia WebGUI o bien a CLI.

Con herramientas para identificar cuellos de botella en el ancho de banda de cada dispositivo, análisis del budget PoE, estudio de canales, planificador de cobertura sobre planos reales y mucho más...

EL DESARROLLO DE SOFTWARE CON IA PROTAGONIZA EL DEVELOPER SUMMIT 2026 DE WOLTERS KLUWER

La última edición del evento para desarrolladores de Wolters Kluwer Tax & Accounting España se ha centrado en el avance que se está produciendo en el mundo del software con la introducción de la inteligencia artificial. A través de diversas charlas y talleres, la compañía ha mostrado cómo está impactando esta tecnología en todo el ciclo de vida del desarrollo de aplicaciones, aportando ventajas que ya están remodelando la industria.

RICARDO GÓMEZ (BARCELONA)

Wolters Kluwer Tax & Accounting España ha celebrado el pasado 10 de abril en Barcelona la cuarta edición de su Developer Summit, un evento en el que ha reunido a alrededor de 180 desarrolladores de software para exponer las últimas tendencias del sector, que este año han estado protagonizadas por el uso de inteligencia artificial en la programación de aplicaciones, especialmente para el ámbito fiscal, laboral y contable.

En la presentación del evento, Alex González, director de Tecnología de la compañía, explicó que “la IA está transformando la forma en que desarrollamos software”, una irrupción que está causando “un cambio profundo que va mucho más allá de la tecnología y nos obliga a redefinir roles, procesos y herramientas”. Con esta tecnología, opinaba, “estamos evolucionando hacia un modelo de desarrollo en el que la IA amplía y potencia a los equipos de desarrollo, al tiempo que plantea nuevos retos técnicos y organizativos”. Y añadió que “en Wolters Kluwer, apostamos

por una IA orientada a la resolución de problemas, que ayude a los equipos a ser más productivos sin comprometer el rigor técnico, la solidez del software ni las prácticas éticas y responsables".

POTENCIAL DE LA IA EN EL DESARROLLO

El Developer Summit 2026 contó con diferentes presentaciones y sesiones técnicas en las que varios expertos ahondaron en cómo se puede utilizar la inteligencia artificial para mejorar los flujos de trabajo en todas las etapas del desarrollo de software, desde la planificación hasta la validación del código, utilizando herramientas como GitHub Copilot, Claude Code y Cursor, entre otras.

En la primera, titulada "Más allá del vibe coding: La IA aplicada a proyectos reales de desarrollo", Xavier Redó, cofundador y CTO de MarsBased, explicó cómo han transformado la metodología de uso de la inteligencia artificial en su compañía hacia una forma más evolucionada que el vibe coding.

La segunda, titulada "Desarrollo con AI Agents: fundamentos para developers", contó con la visión de Abel Márquez, lead technology product manager en Wolters Kluwer Tax & Accounting España, y Alberto González, Manager, Technology DXG de la compañía, sobre las nuevas posibilidades que ofrecen los agentes autónomos de IA en el campo del desarrollo de aplicaciones.

El siguiente bloque constó de dos sesiones técnicas: "Observabilidad y datadog: trazas, logs y

EL ROL DEL DESARROLLADOR ANTE EL AVANCE DE LA IA

En el marco del Developer Summit 2026 de Wolters Kluwer conversamos con Alex González sobre su visión de hacia dónde se dirige el sector y cómo va a impactar la inteligencia artificial en el rol de los desarrolladores. Lo primero que destacaba es que el programador seguirá necesitando amplios conocimientos técnicos, pero opinaba que "tiene que asumir un rol más hacia la izquierda, más centrado en el trabajo de diseño, en las especificaciones, en entender las soluciones informáticas de forma completa". Y considera que "el rol de codificador se debe elevar", por lo que insta a los profesionales a especializarse en las nuevas capacidades que aporta la IA al desarrollo de aplicaciones, para adaptarse a un futuro en el que esta tecnología será un pilar fundamental del sector.

> ANTE EL AVANCE DE LA IA EL PROGRAMADOR TIENE QUE ASUMIR UN ROL MÁS CENTRADO EN EL DISEÑO Y EN LAS ESPECIFICACIONES, EN ENTENDER LAS SOLUCIONES INFORMÁTICAS DE FORMA COMPLETA

ALEX GONZÁLEZ,
director de Tecnología de
Wolters Kluwer Tax & Accounting España

métricas: un paso más allá", guiada por Rubén Carretero, lead engineer DXG de Wolters Kluwer Tax & Accounting España; y "Spec-Driven Development con IA", una master class a cargo de Facundo Alarcón, staff engineer DXG de la compañía.

PRESENTE Y FUTURO DEL DESARROLLO CON IA

Tras estas dos charlas técnicas, en la que los expertos mostraron importantes avances en el uso de inteligencia artificial para la creación de aplicaciones, Alvaro Moya, founder y CTO de LIDR.co, ofreció la presentación "Presente y futuro del desarrollo con IA", una intervención con alto contenido técnico en la que enseñó a los asistentes cómo utilizar ciertas herramientas basadas en IA para optimizar el trabajo en diversas etapas del desarrollo de software.

Por su parte, Álex González, destacaba que la inteligencia artificial tiene potencial para transformar todo el ciclo de vida del desarrollo de software y, aunque "el foco principal a día de hoy está en la codificación", otras áreas clave están cambiando con la introducción de esta tecnología, "desde la revisión de las contribuciones hasta la gestión de la integración de esas contribuciones en el producto, la parte de observabilidad, la de exploración, de definición de productos, definición de casos de uso, la creación de prototipos...". Y comentaba que "todos los players que están operando en el ciclo de vida del desarrollo, en cualquiera de las fases, están innovando".

Por otro lado, alertaba, "hay que vigilar cómo usas la IA en la exploración y la definición del producto, por el propio comportamiento de la IA, ya que los LLM son modelos que te van a dar, probablemente, la respuesta más correcta para una pregunta o necesidad específica", y "si de repente en el mercado todos le preguntamos a la IA cómo se soluciona ese problema del cliente, la IA estadísticamente nos dará la misma respuesta a todos", lo que dificultará esa diferenciación tan necesaria en el mercado. Por ello, opina que "la definición del producto y la innovación tienen que estar lideradas por las personas, empoderados con la IA". ■

Clica en la imagen para ver la galería completa

MÁS INFO

» Wolters Kluwer Developer Summit 2026

COMPARTIR EN REDES SOCIALES

DEVELOPER SUMMIT 2026

El Developer Summit 2026 de Woltesr Kluwer ofreció a los asistentes diversas presentaciones y sesiones técnicas a cargo de varios expertos de la compañía: Abel Márquez, lead technology product manager; Alberto González, manager, Technology DXG, Rubén Carretero, lead engineer DXG; y Facundo Alarcón, staff engineer DXG. A estas, se sumaron las intervenciones de expertos como Xavier Redó, cofundador y CTO de MarsBased; y Alvaro Moya, founder y CTO de LIDR.co.

V-VALLEY IMPULSA LA CIBERSEGURIDAD EN EL CANAL EN EL CYBERSECURITY SUMMIT 2026

El mayorista V-Valley ha celebrado un año más su evento dedicado a la ciberseguridad, reuniendo a sus principales partners, fabricantes y clientes en el Cybersecurity Summit 2026. En esta edición, han puesto el foco en las principales tendencias del sector y se han centrado especialmente en fomentar el networking entre los más de 200 asistentes para generar nuevas oportunidades de negocio en el canal.

RICARDO GÓMEZ (SEGOVIA)

V-Valley ha escogido de nuevo Segovia para la celebración de su Cybersecurity Summit 2026, que ha tenido lugar entre los días 16 y 17 de abril, una importante cita para el canal donde la compañía ha reunido a sus principales partners, fabricantes y clientes, junto a miembros de la prensa, en torno a la ciberseguridad. Este año, el evento no solo contó con la presencia de más de 200 asistentes, sino que las sesiones celebradas durante el primer día se retransmitieron por streaming a unos 400 partners registrados. Además, en el segundo día se celebraron encuentros

Clica en la imagen para ver la galería completa

1-to-1 entre fabricantes, partners y clientes, con un enfoque pensado en facilitar la puesta en común de necesidades y soluciones, y en fomentar las relaciones entre los miembros del canal y las empresas para generar oportunidades de negocio.

Tras la recepción, David Gasca, responsable de Marketing y Operaciones de Ciberseguridad de la compañía; y Alberto López, country manager Iberia de Ciberseguridad, presentaron esta edición del congreso, destacando especialmente la trayectoria del mayorista en este segmento del mercado, en el que durante los últimos cinco años han ido sumando referencias y partners.

Alberto López ponía en valor, además, varios aspectos clave que les han permitido desarrollar la línea de negocio de ciberseguridad: “la confianza que me dio el Grupo Esprinet hace ocho años para montar este proyecto”, y la capacidad de su equipo de trabajo, que comenzó con doce personas y actualmente cuenta con casi 80 profesionales dedicados a la ciberseguridad.

Tras la presentación inicial, se celebró una serie de tertulias en las que se abordaron algunas de las principales tendencias en torno a la ciberseguridad corporativa en diversos sectores, iniciadas por expertos en cada área, y en las que participaron representantes de diversas compañías del sector de la seguridad, tanto fabricantes como partners.

CYBERSECURITY SUMMIT 2026

Las tertulias celebradas durante el primer día del Cybersecurity Summit 2026, que abordaron diferentes aspectos de la ciberseguridad actual, contaron con las intervenciones de Víctor Sánchez, inspector jefe de la Policía Nacional y miembro de C1b3rwall; Martin Vigo, hacker e investigador; Eduvigis Ortiz, fundadora y presidenta de Women4Cyber Spain; Ramsés Gallego, presidente de ISACA Barcelona Chapter; Alejandro Villar, head of Information Security/ Information Security Manager en TRC; y Noé Villar, CTO & CISO en DQS Consulting

EL ESTADO DE LAS CIBERAMENAZAS: LA RADIOGRAFÍA REAL DEL CIBERCRIMEN EN LA CALLE HOY

Víctor Sánchez, inspector jefe de la Policía Nacional y miembro de C1b3rwall, el proyecto la División de Formación y Perfeccionamiento del Cuerpo, dedicado a las ciberamenazas, abrió la primera sesión hablando sobre la misión de esta unidad. Tras esto, profundizó en el contexto actual de las ciberamenazas, en cómo funcionan las organizaciones cibercriminales hoy en día y en la importancia de proteger a las empresas, desde las más grandes a las pymes, para blindar toda la cadena de suministro.

EL ATAQUE DEFINITIVO: IA OFENSIVA Y NUEVAS FRONTERAS

Martin Vigo, hacker e investigador, habló sobre una tendencia que está cobrando mucha importancia en el ámbito de las ciberamenazas: el prompt injection. Y puso ejemplos de cómo los atacantes están aplicando esta peligrosa práctica, que consiste en la vulneración de modelos de lenguaje (LLM) para alterar las directrices de funcionamiento de la IA y realizar todo tipo de acciones maliciosas.

EL FACTOR HUMANO: RETENCIÓN DE TALENTO, DIVERSIDAD Y LA LUCHA CONTRA LA FATIGA EN LOS EQUIPOS

Eduvigis Ortiz, fundadora y presidenta de Women4Cyber Spain, introdujo el tercer bloque, en el que puso de relieve el problema de la escasez de talento en el sector de la ciberseguridad, y para combatirlo recomendó a las empresas y departamentos de recursos humanos apostar por la formación y la certificación. Además, destacó el papel

cada vez más relevante de las mujeres en el ámbito de la ciberseguridad y cómo su organización se esfuerza por seguir incentivando la presencia femenina en este sector.

EL TSUNAMI REGULATORIO (DORA/NIS2): EL IMPACTO Y LA AUDITORÍA EN LA CADENA DE SUMINISTRO

Presentada por Ramsés Gallego, Chief Technologist, Cybersecurity en DXC Technology y presidente de ISACA Barcelona Chapter, esta charla giró en torno a cómo las nuevas regulaciones relacionadas con la ciberseguridad y la protección del dato tienen un impacto a largo plazo en las organizaciones. Porque, parafraseando a Juan Antonio Bayona, director de la película Lo imposible, “un tsunami no es una ola; son muchas”; y tanto el sector público como el privado deben prepararse para los cambios que imponen estas normativas, que afectan a múltiples niveles en toda la cadena de suministro.

CIBERDEFENSA E INFRAESTRUCTURAS CRÍTICAS: LA PROTECCIÓN DEL ECOSISTEMA OT/IOT Y EL CIBERESPACIO

Esta tertulia comenzó con la intervención de Alejandro Villar, Head of Information Security/Information Security Manager en TRC, quien se centró en las particularidades de la ciberseguridad en entornos de tecnología operativa (OT) e IoT, destacando las profundas diferencias con respecto a la seguridad de entornos TI. Aunque también apuntó que “hay que acabar con la idea de que los entornos industriales y las infraestructuras críticas están aisladas”, ya que normativas como NIS2 han cambiado las reglas de juego también para infraestructuras críticas e industrias, y recomendó centrarse en soluciones creativas que permitan garantizar niveles aceptables de seguridad sin comprometer la continuidad de las operaciones, e involucrar a los responsables de planta en la toma de decisiones de ciberseguridad.

EL ESTADO DEL CANAL: LOS RETOS, SERVICIOS Y NECESIDADES DEL INTEGRADOR ACTUAL

Noé Villar, CTO & CISO en DQS Consulting, comenzó la última sesión hablando sobre el estado del canal, la labor de sus diferentes actores en el ámbito de la ciberseguridad, cómo los partners tienen un papel clave a la hora de entender las necesidades de los clientes de diferentes tamaños, y los grandes esfuerzos que deben hacer para contar con especialistas y fabricantes que cubran las distintas áreas en las que interviene la seguridad cibernética. ■

MÁS INFO

» V-Valley Cybersecurity Summit 2026

» V-Valley convoca al ecosistema TI en su Tech Summit 2026

COMPARTIR EN REDES SOCIALES

#ENTREVISTA

Ofrecemos a nuestros clientes la posibilidad de escalar su innovación en IA a medida que cambian sus necesidades

ATHENA KARP, SVP OF PRODUCT DE WORKDAY

RICARDO GÓMEZ (MADRID)

¿Cómo ha evolucionado su rol en Workday desde que se unió a la empresa, tras la adquisición de HiredScore?

Han pasado casi dos años desde que HiredScore pasó a formar parte de Workday, donde comencé como gerente general de HiredScore, trabajando para nuestro director de producto. Rápidamente, quise hacer aún más en la compañía y vi que tenemos en torno a 11.500 clientes y, probablemente debido a quiénes eligen Workday, suelen ser algu-

nas de las empresas y marcas más innovadoras, que priorizan la transformación y los datos; son visionarias. Para mí, fue la oportunidad de trabajar en un ámbito más amplio y siempre me atrajeron los retos de la adquisición y la gestión del talento. Creo que, como parte de Workday, podemos hacer mucho en el área de RR.HH., en Finanzas y, cada vez más, también en TI y en el ecosistema en general. Este otoño asumí el cargo de vicepresidenta sénior de Estrategia de IA, que abarca toda la IA de Workday, y es a lo que me dedico actualmente.

¿Cómo se está integrando la IA en flujos de trabajo empresariales críticos, como Recursos Humanos y Finanzas?

Creo que RR.HH. probablemente se adelantó a Finanzas en la incorporación de la IA y, de hecho, en algunos de nuestros clientes, Recursos Humanos lideró la implementación en toda la empresa, en parte porque, para ellos, los casos de uso de IA en esta área eran muy claros. Porque con ella los candidatos pueden postularse a 60 empleos en un minuto, con un currículum y una carta de presentación personalizados para el puesto al que quieren optar. Esto es una especie de carrera armamentística desigual, porque ante la proliferación de solicitantes hay que aplicar una contramedida cuanto antes desde las empresas.

Sin embargo, en Finanzas estamos viendo que cada vez más directores financieros, responsables de Finanzas y equipos se interesan por la IA, especialmente en áreas como la planificación, donde tenemos un producto de planificación increíble y nuestro agente está haciendo cosas realmente impresionantes. Por otro lado, estamos viendo un cambio en TI, que ahora se integra con RR.HH. y Finanzas, proponiendo pensar conjuntamente los casos de uso o áreas donde puede ser interesante incorporar la IA, para luego desarrollarla.

> “CON SANA OFRECEMOS UNA NUEVA FORMA DE TRABAJAR PARA LOS EMPLEADOS, LOS GERENTES Y LA EMPRESA”

¿Qué importancia tiene contar con una arquitectura unificada de datos, procesos y contexto para aprovechar al máximo el valor que la IA aporta a las organizaciones?

Quien ha intentado crear agentes sobre sistemas que no tienen un modelo de datos unificado, ni controles de acceso y permisos unificados, sabe la respuesta. Como desarrolladores de IA, siempre decimos: “te acompañaremos hasta donde podamos como cliente”. Sabiendo esto, cuando desarrollaba sobre Workday, siempre podía avanzar mucho más rápido y llegar mucho más lejos porque, en esencia, los datos siempre seguían un mismo modelo. Porque el acceso a los permisos y los controles estaban siempre unificados gracias a la gobernanza y al marco de procesos de negocio.

Creo que la mayoría de nuestros clientes no compraron Workday por su preparación para la IA, pero al comenzar a desarrollar, se dan cuenta de que esos componentes eran fundamentales para esta nueva etapa y ya están integrados, de forma que no necesitan resolver estos temas por sí mismos. Otro aspecto importante es que los agentes que estamos desarrollando, específicamente para cada dominio, ofrecen mecanismos de protección predefinidos para operar en áreas sensibles, como Recursos Humanos y Finanzas.

¿Cómo deberían las empresas definir su estrategia de gobernanza, seguridad y control para la IA, a medida que esta tecnología se integra cada vez más en procesos críticos, como Recursos Humanos y Finanzas?

De hecho, una de las ventajas de Workday es que, en muchos casos,

nuestros clientes ya tuvieron que realizar un trabajo arduo al implementar Workday, reflexionando sobre cómo establecer la gobernanza, la seguridad, los permisos de acceso a los datos. Ahora disfrutan de un sistema sencillo que gestiona una enorme complejidad en cuanto a acceso, visibilidad y capacidad de edición.

Otro problema que vemos deriva de los agentes que se comunican con otros agentes y otros sistemas, volviéndose ingobernables. En este contexto, Workday actúa controlando quién usa cada agente, cuál es su rol y responsabilidad, qué sistemas usa, qué tareas realiza y si es sospechoso. Se han implementado todos estos complejos controles de permisos y acceso a los datos más sensibles, y esa es parte de la razón por la que nuestras grandes inversiones e innovaciones se centran en herramientas de plataforma.

¿Podría comentar algunos de los casos de uso de IA más relevantes para Workday en Recursos Humanos y Finanzas?

Algunos de los agentes que aportan más valor a los clientes son nuestros Agentes de Experiencia del Candidato, que pueden funcionar 24-7. Además, este agente permite contratar rápidamente un gran volumen de personal, logrando una reducción del 40% en el tiempo de contratación. Otro ejemplo es el Agente de Reclutamiento HiredScore. Considerando que los candidatos están usando IA para postularse a empleos, y que el volumen de solicitudes está creciendo, muchas empresas no pueden seguir el ritmo y muchos se quedan fuera del proceso. Pero gracias a este agente ofrecemos un proceso de selección respetuoso, y se tiene en cuenta a las personas para futuras ofertas de trabajo.

Por otro lado, en nuestros clientes vemos que es más difícil facilitar la búsqueda de talento interno que externo, y creemos que aquí la IA puede ser una herramienta útil para mostrar las oportunidades que ofrece la empresa para desarrollo profesional. El último aspecto es el aprendizaje, la formación y el desarrollo, donde nuestros clientes ya utilizan Workday Learning, con tecnología de Sana, para crear contenido personalizado para los empleados, logrando reducir en más del 98% el tiempo necesario para hacerlo.

En cuanto al ámbito financiero, tenemos nuestro agente de planificación, que permite ejecutar escenarios de planificación a empresas que carecen del personal para hacerlo y desarrollar un plan. También vemos más demanda en Financial Audit y Financial Close Agent, nuestra inteligencia documental que permite que un agente lea los contratos, informe sobre su contenido y los vincule con los ingresos y los programas financieros.

¿Cómo ha evolucionado la IA de Workday, y qué aporta Sana al entorno laboral moderno?

Creo que es fundamental que las personas puedan experimentar los sistemas de RR.HH. y Finanzas con una interfaz intuitiva, como la de un chat, y Sana es revolucionario en este sentido. No existen otras plataformas de RR.HH. y Finanzas que no requieran conocimientos técnicos y se les pueda preguntar en lenguaje natural. Y el sistema no solo da respuestas, sino que también te pregunta en el mismo lenguaje cómo quieres proceder. Esta es una nueva forma de trabajar para los empleados, los gerentes y la empresa, y una vez que se integre la experiencia de Sana, la gente se dará cuenta de lo potente que es Workday para gestionar todas estas cosas.

En cuanto a la evolución de la IA de Workday, creo que lo que ha

cambiado para nosotros es la mentalidad abierta de nuestros clientes que, ahora, en lugar de empezar por el proceso y luego pensar en sus necesidades de IA, empiezan por el objetivo de negocio o por el resultado. Y, luego, piensan en cómo debería ser el proceso, cómo podría serlo gracias a la IA y dónde integrar la intervención humana en la toma de decisiones.

A medida que las empresas incrementan el uso de la IA en sus procesos, los costes pueden aumentar, dependiendo del proveedor. ¿Qué modelo aplica Workday para tarificar el consumo de inteligencia artificial? ¿Se incluyen de base todas las capacidades de IA o el coste depende del nivel de uso?
Una de las principales diferenciaciones de Workday en este sentido son nuestros créditos flexibles, que permiten a nuestros clientes consumir la innovación de la forma que necesitan. Porque, al invertir en un contrato de IA fijo de varios años, con licencia, tienes que saber con certeza que vas en la dirección correcta y saber exactamente quién lo va a usar y cómo, algo difícil de saber antes de extenderlo a toda la plantilla. Y la tecnología cambia tan rápido que nadie puede predecir qué pasará con la IA dentro de 12 meses.

Por eso, ofrecemos a nuestros clientes la posibilidad de escalar su innovación en IA con nosotros, tanto hacia arriba como hacia abajo, a medida que cambian sus necesidades, sus prioridades o la disponibilidad de nuestros agentes. Y otro punto importante es que nuestros créditos se pueden usar en todos los diferentes tipos de innovación laboral, lo que te brinda la máxima flexibilidad para explorar qué puede funcionar y cómo funciona, probar y experimentar, pero también para ampliar o reducir la capacidad según sea necesario.

En cualquier caso, controlar el consumo de inteligencia artificial representa un desafío para las empresas. ¿Cómo crees que evolucionará la gestión del coste de la IA en el futuro?
Creo que cada vez más departamentos pensarán como lo hacen hoy los departamentos de TI y de la nube. El trabajo con la IA pasa de ser realizado por humanos a ser realizado por un tándem de humanos y máquinas. Ya no es solo un elemento tecnológico; también contribuye al trabajo y a la productividad. Y creo que este cambio implica comprender que se está pagando por cosas diferentes a las que se han pagado históricamente.

Muchas empresas carecen de los modelos, el vocabulario y los procesos internos necesarios para adoptar la IA. Por lo tanto, creo que habrá mucha más madurez en los próximos meses, y probablemente en uno o dos años, a medida que la industria aprenda a comprender a qué se asemeja esto, cómo lo financiamos, cómo lo presupuestamos y cómo lo comparamos con las licencias SaaS tradicionales que adquirimos en el pasado, algo que todavía no está sucediendo. ■

> “LOS AGENTES QUE ESTAMOS DESARROLLANDO, ESPECÍFICAMENTE OFRECEN MECANISMOS DE PROTECCIÓN PARA OPERAR EN ÁREAS SENSIBLES”
>
> **ATHENA KARP,**
> SVP of product de **Workday**

MÁS INFO +

» Entrevista a Athena Karp, Workday

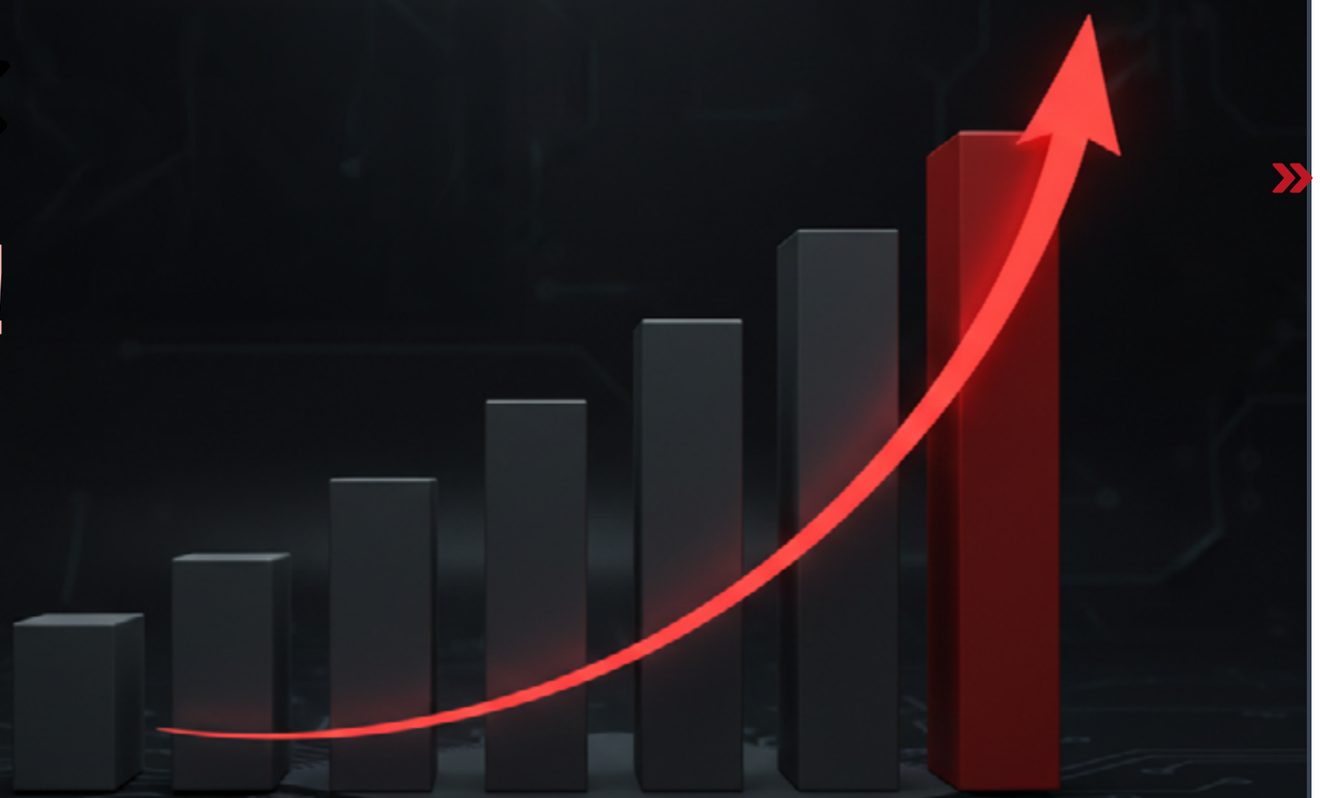
COMPARTIR EN REDES SOCIALES

DESCUBRE POR QUÉ
SOMOS TU SOCIO ESTRATÉGICO

35 AÑOS

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

Tu stock, a un clic de distancia



¡ESCALAMOS TU NEGOCIO!

DMI Computer

CRIME AS A SERVICE, LA INDUSTRIALIZACIÓN DEL CIBERCRIMEN

RAFAEL CLAUDÍN

La industrialización de las ciberamenazas que se ha dado en la última década ha tenido un protagonista destacado: el cibercrimen como servicio. Un cambio en la cadena de suministro de los ciberataques que los ha profesionalizado y multiplicado, antes incluso de la IA agéntica. Nos ayudan a entender mejor el CaaS los expertos Josep Albors, Ignacio Franzoni, Iván Gulina, Simon Marchand, Sergio Martínez y Óscar Vierge.

El concepto de Crime as a Service (CaaS) es al mundo del cibercrimen lo que las metodologías ágiles al desarrollo de software. Una metodología de trabajo capaz de transformar completamente el modo en que se opera. En el caso de los ciberataques, supuso casi un cambio de su propia esencia: ya no son cosa de un puñado de ciberdelincuentes solitarios, sino parte de una industria criminal extraordinariamente provechosa. Tanto, que en la última década ha pasado a convertirse en la tercera economía del mundo.

Han pasado tantas cosas y tan rápido, que el 2015 se nos antoja un año en el que todavía conservábamos parte de la inocencia. El recién nacido INCIBE (empezó su andadura en 2012) registró un incremento del 200% en los ciberataques que gestionaba, acercándose a los 50.000. Este pasado 2025, gestionó más de 122.000. Como todas las estadísticas, hay que ponerla en contexto: significa que se realizan más ciberataques, pero también que hay una mayor capacidad de detección y una mayor confianza en el Instituto Nacional de Ciberseguridad.

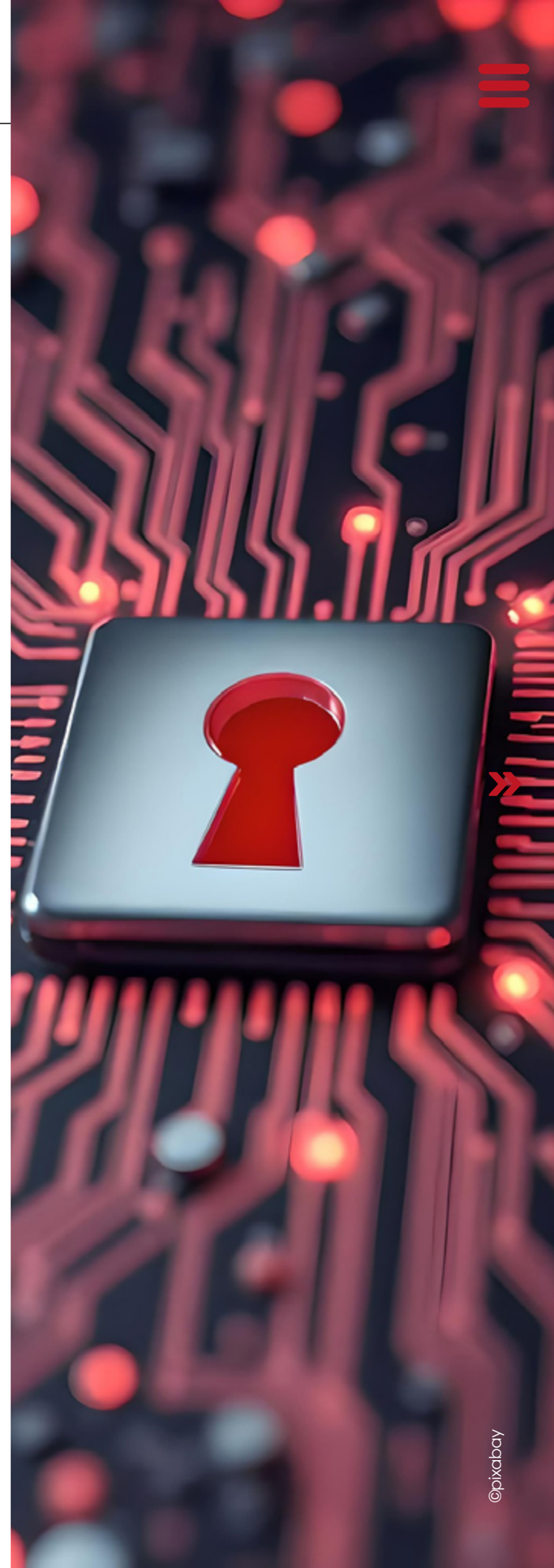
En todo caso, si bien el último impulso al crecimiento de las amenazas se lo podemos imputar a la inteligencia artificial, hace una década ya había comenzado el cambio fundamental del Cibercrimen como Servicio. En el informe de Microsoft "Tendencias de 2016 en ciberseguridad", basado en datos de 2015, se definen los "kits de ataques" como "recopilaciones de ataques agrupados que se venden como software comercial o como un servicio". En ese momento, el "kit típico consta de una colección de páginas web que aprovechan varias vulnerabilidades de exploradores web y complementos de explorador populares".

UNA HISTORIA DE CIBERCRIMEN COMO SERVICIO

Los cibercriminales habían empezado a especializarse y robaron tal cantidad de identidades que, como explica el experto internacional en fraude Simon Marchand, "ante la imposibilidad de monetizar cada una de ellas de forma individual, la reventa masiva se convirtió en una vía no solo para asegurar un flujo constante de ingresos, sino también para reducir riesgos, al evitar la implicación directa en el ataque final".

Marchand amplía que durante la pandemia de 2020 "detectamos una nueva tendencia: los ciberdelincuentes abandonaron la dark web para empezar a utilizar plataformas accesibles al público general. Empezaron a proliferar grupos de ayuda, tutorías, asesoramiento y guías sobre cómo poner en marcha diversos negocios ilícitos. Esto impulsó el fenómeno del cibercrimen como servicio hasta el escenario actual, al que nos enfrentamos hoy: una oferta a medida, barreras de entrada mínimas y redes que resultan prácticamente imposibles de desarticular de forma definitiva".

Sergio Martínez, country manager de SonicWall, coincide en que "el Cibercrimen como Servicio ha experimentado una evolución muy clara en los últimos años, pasando de ser una actividad relativamente fragmentada y artesanal a convertirse en una auténtica industria global. Hoy hablamos de un modelo plenamente profesionalizado, en el que existe especialización, economías de escala y una clara orientación al beneficio. Este enfoque ha permitido que perfiles sin grandes conocimientos técnicos puedan lanzar ataques complejos gracias a herramientas listas para usar, lo que ha democratizado el acceso al cibercrimen. Además, la expansión del entorno digital, impulsada por el


©pixabay

cloud, la movilidad y el trabajo híbrido, ha ampliado enormemente la superficie de ataque, favoreciendo el crecimiento de este modelo".

Por su parte, Iván Gulina, head of Cybersecurity en Veridas, recuerda que, "históricamente, los ciberataques estaban reservados a individuos o grupos reducidos que debían poseer conocimientos técnicos muy profundos. Sin embargo, hoy en día el cibercrimen ha adoptado plenamente la filosofía corporativa del modelo SaaS (Software-as-a-Service). Hemos pasado de atacantes aislados a verdaderas empresas cibercriminales. Actualmente, estas organizaciones operan de forma industrializada: ofrecen suscripciones mensuales, portales de gestión, acuerdos de nivel de servicio (SLA), actualizaciones constantes de software para evadir nuevas defensas e, incluso, servicios de soporte técnico 24/7 alojados en la Dark Web para atender a sus 'clientes'".

LAS EMPRESAS ANTE EL CIBERCRIMEN COMO SERVICIO

La sensación es que todo va tan rápido que a veces cuesta seguirle el ritmo. Y no seguir el ritmo de las ciberamenazas es en sí mismo un alto riesgo. El propio concepto del Cibercrimen como Servicio ha vivido su propia evolución, su transformación desde esos kits de ataques que mencionaba Microsoft hace 10 años. Así lo refleja Óscar Vierge, sales director Strategic Accounts de Serval Networks:

"El principal cambio es que el cibercrimen como servicio ha dejado de girar únicamente en torno al malware para orientarse cada vez más hacia la obtención, compra y explotación de accesos. Hoy es habitual que un ataque no comience con una infección clásica, sino con el uso de credenciales legítimas, cookies robadas o sesiones comprometidas que después son aprovechadas por otros actores para avanzar dentro de la organización. A esto se añade el uso creciente

> "EL CIBERCRIMEN COMO SERVICIO SERÁ AÚN MÁS AUTOMATIZADO, ACCESIBLE Y ESPECIALIZADO, CON UN MAYOR USO DE LA IA PARA GENERAR ATAQUES MÁS PERSONALIZADOS Y RÁPIDOS"

JOSEP ALBORS
director de Investigación y Concienciación, **ESET España**

> "HEMOS PASADO DE UNA CULTURA UNDERGROUND A ALGO QUE SE PUEDE ADQUIRIR CON LA MISMA FACILIDAD CON LA QUE REALIZAMOS CUALQUIER OTRA COMPRA ONLINE"

SIMON MARCHAND
experto internacional en fraude

de la IA, que está permitiendo automatizar tareas como la generación de mensajes de phishing más creíbles, la personalización de señuelos y la escalabilidad de campañas de fraude".

Josep Albors, director de Investigación y Concienciación de ESET España, considera que "la mecánica del Cibercrimen como Servicio se ha vuelto mucho más profesionalizada y modularizada. Hace años, el ciberdelincuente lo hacía casi todo por su cuenta mientras que ahora puede suscribirse o alquilar servicios ya preparados —como kits de phishing, servidores de envío masivo de correos/SMS, ransomware, botnets, alojamiento resistente a bloqueos y soporte técnico—, lo que permite automatizar ataques, escalar campañas y repartir tareas entre distintos actores. En la práctica, el cambio no altera tanto el daño final como la forma de ejecutarlo: hoy hay más especialización, más anonimato, pagos recurrentes y una cadena delictiva más organizada que facilita que más personas puedan lanzar ataques complejos".

Siguiendo el razonamiento de Albors, ¿hasta qué punto es relevante para una empresa el modo en que operan las estructuras del cibercrimen? Quizá el mayor cambio en los sistemas de ciberprotección está en los servicios de inteligencia, que se encargan de detectar el rastro de una empresa en la Dark Web para adelantarse a posibles filtraciones. Pero, al igual que sucede con la inteligencia artificial, el impacto de esta transformación del cibercrimen se deja notar sobre todo en el volumen de las ciberamenazas.

Ignacio Franzoni, director de ingeniería de soluciones en Netskope, explica que "el hecho de que el CaaS democratice el ataque implica que las empresas se enfrentan a un volumen mucho mayor y constante de amenazas. El perímetro de seguridad tradicional ha desaparecido, ya que los ataques suelen provenir de servicios

> "LA IA GENERATIVA ESTÁ EN LOS KITS, LO QUE PERMITE CREAR CAMPAÑAS DE PHISHING HIPER PERSONALIZADAS Y GENERAR CÓDIGO MALICIOSO CAPAZ DE SORTEAR LAS DEFENSAS TRADICIONALES"

IGNACIO FRANZONI
director de ingeniería de soluciones, **Netskope**

> "LA COLABORACIÓN ENTRE DIFERENTES GRUPOS CRIMINALES HA GENERADO UNA RED DE SERVICIOS CADA VEZ MÁS SOFISTICADA Y DIFÍCIL DE RASTREAR"

ÓSCAR VIERGE
sales director Strategic Accounts, **Serval Networks**

legítimos en la nube, lo que hace que las defensas convencionales resulten insuficientes. Los ataques de ingeniería social erosionan la confianza de los usuarios, por lo que las organizaciones deben adoptar modelos de Zero Trust. Por supuesto, el impacto financiero es considerable, ya que el auge del CaaS ha incrementado la eficacia del ransomware y obliga a las compañías a invertir tanto en protección como en ciber resiliencia para poder recuperarse rápidamente".

Iván Gulina, de Veridas, considera que "el impacto es doble. Primero, nos enfrentamos a una inflación del riesgo: el volumen de ataques diarios crece exponencialmente porque la barrera del conocimiento ya no existe. En segundo lugar, esto genera una presión financiera directa sobre las organizaciones. Para neutralizar las amenazas más frecuentes y sofisticadas, las empresas se ven obligadas a invertir en capas de defensa más robustas y avanzadas. En definitiva, la economía de escala del cibercrimen está forzando a las compañías a escalar sus presupuestos de seguridad para no quedar vulnerables".

Donde más se deja sentir el CaaS es, según Simon Marchand, "en el ámbito de la prevención del fraude que en el de la ciberseguridad tradicional. La superficie de ataque se expande constantemente, y el volumen de ofensivas, siempre al alza, hace que sea cada vez más difícil confiar únicamente en herramientas de prevención de fraude obsoletas (legacy). Una de las tendencias más preocupantes que observamos es el uso de herramientas basadas en Inteligencia Artificial (IA) para escalar las operaciones de fraude a niveles industriales. Los grupos criminales están aprendiendo rápidamente a aprovechar la IA generativa y los modelos de lenguaje (LLM) en sus ataques. Este es el gran desafío: ataques totalmente automatizados, sin necesidad de intervención humana, que utilizan identidades y avatares creados con deepfakes para

"VEREMOS UNA MAYOR ORIENTACIÓN HACIA EL ROBO DE IDENTIDAD Y EL ACCESO A SISTEMAS CRÍTICOS, ASÍ COMO MODELOS DE NEGOCIO DELICTIVOS TODAVÍA MÁS ESTRUCTURADOS"

SERGIO MARTÍNEZ
country manager, **SonicWall**

"LAS HERRAMIENTAS 'AS-A-SERVICE' SON LAS RESPONSABLES DIRECTAS DE QUE LOS INTENTOS DE ATAQUE HAYAN CRECIDO ENTRE UN 30% Y UN 40% EN LOS ÚLTIMOS AÑOS"

IVÁN GULINA
head of Cybersecurity, **Veridas**

ejecutar ataques complejos, desde la apertura de cuentas hasta el robo de las mismas".

AMENAZAS BASADAS EN CAAS

Es difícil identificar el porcentaje de todas las ciberamenazas actuales que se corresponden con este modelo. Se trata de una especie de malla de fondo que cada vez se va extendiendo más. Quizá se puedan dejar fuera los ciberataques que se realizan con una motivación política, o incluso el hacktivismo. Pero en el caso de la ciberdelincuencia común la presencia del Cibercrimen como Servicio es cada vez mayor. Josep Albors, de ESET España, explica así esta ausencia de una estadística más o menos oficial:

"No hay un porcentaje único y fiable que mida qué parte del volumen total de ciberamenazas corresponde al Cibercrimen como Servicio, ya que se suele tratar como un modelo de negocio que impulsa muchos tipos de amenazas —phishing, ransomware, robo de credenciales, botnets y accesos iniciales, etc—, pero no como una categoría estadística separada con cuota oficial del total. Lo más correcto sería decir que su peso dentro de la industria del cibercrimen es muy alto y continúa aumentando, porque facilita y multiplica ataques que antes requerían más habilidad técnica, pero las cifras públicas suelen medir incidentes, víctimas o costes, no el porcentaje exacto del Cibercrimen como Servicio sobre todas las amenazas".

Lo que sí está bastante identificado es el tipo de amenazas en las que estas prácticas tienen más calado. Óscar Vierge, de Serval Networks, indica tres áreas en las que predomina, empezando por "el Ransomware-as-a-Service (RaaS): prácticamente el 90% de los incidentes de ransomware actuales son ejecutados por 'afiliados' que alquilan la infraestructura a grupos de élite, permitiendo una cadencia de ataques que antes era imposible. El segundo ámbito es el Phishing-as-a-Service (PhaaS) con IA: la proliferación de kits que automatizan engaños hiperpersonalizados ha disparado el volumen de phishing, siendo responsable de que el 42% de todas las brechas globales en 2026 comiencen con una suplantación de identidad servida 'en bandeja' al atacante. Por último, en la tercera área están los Access Brokers, intermediarios especializados en vender accesos ya comprometidos a redes corporativas".

PRÁCTICAS EMPRESARIALES AL SERVICIO DEL CIBERCRIMEN

Es muy llamativo el hecho de que los grupos de cibercriminales imiten las mismas estructuras que las empresas que operan dentro de la legalidad. Puede que sea el modo en que nosotros interpretamos los cambios que se producen en su espectro, aplicando los conceptos que tenemos. Pero además del propio concepto "como servicio", se sabe que este tipo de grupos tienen sus equipos de marketing y de recursos humanos para atraer talento. Cada vez más parecidos a una empresa de software al uso.

Y eso que apenas hemos tocado de refilón otro elemento que ha contribuido a democratizar la ciberdelincuencia: la inteligencia artificial generativa. El combinado de GenAI y CaaS es bastante explosivo. Pensemos en algo como Mythos utilizado de forma automatizada, industrializada. Y, en el momento en el que se le sume la computación cuántica, "explosivo" se quedará corto.

A medio plazo, Ignacio Franzoni, de Netskope, cree que el CaaS "seguirá transformándose. Estamos viendo ya ataques autónomos con agentes de inteligencia artificial que podrán actuar en tiempo real dentro de las redes de las víctimas sin necesidad de intervención humana. El foco de los ataques se irá desviando del bloqueo de sistemas hacia la exfiltración y la extorsión de datos sensibles, especialmente los alojados en la nube y las aplicaciones de IA generativa. Ante la creciente sofisticación del CaaS, el mercado responderá consolidando el modelo SASE, que integra red y seguridad para garantizar una visibilidad total, con independencia de la ubicación del usuario o del dato". ■

MÁS INFO +

- El sector financiero afrontó amenazas de IA, blockchain y crimen organizado en 2025
- Los responsables antifraude reconocen ir por detrás del cibercrimen
- Google desmantela la red proxy IPIDEA, empleada por más de 550 grupos maliciosos

ENCUENTROS ITDM GROUP

MODELOS OPERATIVOS Y HERRAMIENTAS PARA UNA GESTIÓN DEL DATO UNIFICADA, EFICIENTE Y SEGURA

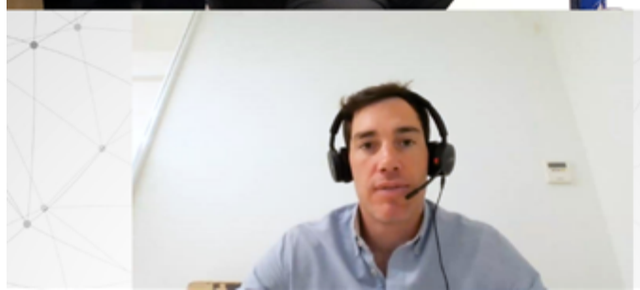
ORGANIZA

PATROCINADORES GOLD

MODELOS OPERATIVOS Y HERRAMIENTAS PARA UNA GESTIÓN DEL DATO UNIFICADA, EFICIENTE Y SEGURA

Las organizaciones están modernizando sus arquitecturas y estrategias de datos para construir modelos operativos que permitan una gestión unificada, eficiente y segura de la información. Centramos esta edición de los Encuentros ITDM Group en cómo las organizaciones se están apoyando en herramientas modernas, basadas en tecnologías como la inteligencia artificial, para transformar su negocio hacia modelos más inteligentes y guiados por los datos. Para ello, contamos con la colaboración de Lutech, ML Code y SonicWall, y con la visión de Penteo.

El volumen de datos que manejan las organizaciones está creciendo exponencialmente, pero en muchos casos se pierde su valor estratégico, ya sea porque la información crucial queda atrapada en silos, o por la dificultad de aplicar estándares de calidad y acceso que permitan identificarlos y aprovecharlos en beneficio del negocio. Todo ello establece barreras que ralentizan los procesos de analítica, introduce riesgos para el cumplimiento normativo y puede inducir errores que afecten gravemente a la toma de decisiones. Por ello, el reto al que se enfrentan las empresas en su camino hacia un modelo guiado por los datos no es tanto capturar suficiente información, como contar con una estrategia y una metodología que los unifique, los haga confiables y valiosos para el negocio.



A lo largo de esta edición de los Encuentros ITDM Group, titulada Modelos operativos y herramientas para una gestión del dato unificada, eficiente y segura, hemos analizado cómo está evolucionando la estrategia, arquitectura e infraestructura de datos en las empresas españolas para desarrollar nuevos modelos operativos y de negocio data-driven.

CLOUD: MAXIMIZANDO LA EFICIENCIA, EL CONTROL Y LA AGILIDAD DE LA INFRAESTRUCTURA TECNOLÓGICA

Como elemento principal de este evento hemos organizado un encuentro de la Comunidad IT, con el apoyo de Lutech, ML Code y SonicWall, en el que debatimos sobre la evolución de las empresas hacia modelos operativos basados en la información, con expertos en datos y analítica de Acciona, Caixabank Payments & Consumer, Cajasiete, Codere, Embou, Exera Energía e Ilunion Hotels. En este debate, además, estuvieron presentes Paolo Mioli, CEO de Lutech; Severino Gala, vicepresidente de ventas de ML Code; y Sergio Martínez, country manager de Sonicwall, quienes aportaron su punto de vista sobre cómo la industria tecnológica puede ayudar a las empresas a modernizar su forma de gestionar y proteger los datos.

OTROS CONTENIDOS PARA LA COMUNIDAD IT

En esta edición de los Encuentros ITDM Group también hemos contado con la visión de otros expertos en la materia sobre la transformación tecnológica que se está produciendo en torno al dato. Para aportar contexto sobre los avances que están llevando a cabo las empresas españolas, Luis Alfaro, asesor de Tecnología y Ciberseguridad en la consultora Penteo, nos ha ofrecido la ponencia “Situación del dato”.

Y, para conocer cómo enfocan la estrategia y arquitectura de datos en la industria financiera, hemos conversado con Jaime Pérez, CDO de Cajasiete, quien ha destacado su avance hacia modelos federados, la importancia que tiene la calidad de la información, especialmente ante el avance inexorable de la inteligencia artificial. ■

MÁS INFO +

» Encuentros ITDM Group: Modelos operativos y herramientas para una gestión del dato unificada, eficiente y segura

PONENCIA >> Luis Alfaro, de Penteo, analiza la situación del dato en la empresa española, destacando la necesidad de mejorar el gobierno y la calidad de la información frente al rápido avance que está experimentando la inteligencia artificial.

EVENTO >> Analizamos la evolución de las empresas hacia modelos más inteligentes y guiados por los datos con expertos de Acciona, Caixabank Payments & Consumer, Cajasiete, Codere, Embou, Exera Energía e Ilunion Hotels.

ENTREVISTA >> Jaime Pérez, Chief Data Officer de Cajasiete, analiza la evolución de la estrategia del dato en la entidad, destacando la transición hacia modelos federados, la calidad de la información y el impacto de la inteligencia artificial.

NUEVOS MODELOS OPERATIVOS PARA EXPLOTAR EL VALOR DE LA IA

La inteligencia artificial ha llegado al mundo empresarial para acelerar la modernización de las organizaciones, prometiendo impulsar la eficiencia y la productividad, y habilitando niveles nunca vistos de automatización e inteligencia de negocio. Pero para aprovechar su potencial debe alimentarse con la información adecuada, lo que obliga a replantear profundamente las arquitecturas tecnológicas y estrategias en torno al dato, una asignatura pendiente para muchas empresas.

Desde el lanzamiento de las primeras herramientas de inteligencia artificial generativa la evolución de la IA se ha acelerado y las grandes tecnológicas involucradas en su desarrollo han logrado integrarla en todo tipo de soluciones empresariales. Al principio se planteaba como una herramienta de productividad para el entorno de trabajo, pero con la llegada de los agentes autónomos su potencial se ha disparado, ofreciendo nuevas capacidades para automatizar procesos y tareas más complejas, y prometiendo generar un impacto positivo y medible para el negocio.

Esto ha llevado a muchas organizaciones a invertir grandes sumas para incorporar la IA en sus operaciones, pero no todas están logrando obtener los resultados deseados. El motivo, en muchos casos, es que no cuentan con la infraestructura ni estrategia de datos necesaria, y esto tiene mucho que ver con el enfoque de sus inversiones en TI.

EN BUSCA DEL RETORNO DE LA IA

Según una investigación reciente de Gartner, las organizaciones con iniciativas de IA exitosas invierten hasta cuatro veces más (de sus ingresos) en áreas fundamentales, como la calidad de los datos, la gobernanza, la formación de sus trabajadores en IA o la gestión del cambio, que aquellas que obtienen malos resultados del uso de inteligencia artificial.

En opinión de Rita Sallam, vicepresidenta analista y directora de Investigación de Gartner, "los líderes de Data & Analysis desempeñan un papel fundamental para obtener el valor esperado de la IA en sus organizaciones". Para lograrlo, comenta, su labor hasta el año 2030 será garantizar las condiciones adecuadas en áreas clave, como "nuevos datos confiables, bases contextuales e inteligencia perceptiva", y considera que "responder a este mandato requerirá cambios en la forma en que el equipo de D&A se organiza, trabaja, desarrolla, escala y crea valor".

TRANSFORMACIÓN DEL ÁREA DE DATOS Y ANALÍTICA

Según la visión de Gartner, hay seis cambios que los líderes de D&A deberían hacer para obtener el valor que se espera de la inteligencia artificial en esta área:

- Centrar las iniciativas de datos y analítica en el aprovechamiento de la IA, para alinearlas con los objetivos de negocio.
- Impulsar la colaboración entre personas y agentes en el área de D&A, con equipos de decisión multidisciplinares apoyados por expertos en IA y agentes enfocados a resultados de negocio.
- Situar el contexto como elemento crítico, optando por agentes de IA

con “acceso contextual y controlado a los datos correctos”.

➤ Apostar por prácticas de ingeniería que conecten datos, IA, contexto e ingeniería de software para impulsar la IA a gran escala en la organización.

➤ Establecer “una gobernanza dinámica que integre contexto automatizado y controles de sesgo, privacidad y cumplimiento en los flujos de trabajo”.

➤ Ir más allá del ROI para generar valor compuesto, creando “un ciclo de valor, en el que las mejoras de eficiencia derivadas de inversiones de alto impacto se reinviertan en crecimiento e innovación”.

MODELOS DE NEGOCIO MÁS AUTOMATIZADOS

El impacto de la IA en las organizaciones es cada vez más transversal, a medida que se incorporan herramientas como los agentes autónomos al software y a los procesos. Según una encuesta realizada por Gartner a 469 altos ejecutivos en todo el mundo, el 80% de ellos afirma que la IA obligará a una profunda transformación de sus capacidades operativas, cambiando el enfoque del negocio digital por el de negocio autónomo. En palabras de Don Scheibenreif, vicepresidente analista de la consultora, “El negocio autónomo es una estrategia en la que agentes de software de autoaprendizaje y clientes automatizados toman decisiones, actúan y crean nuevos tipos de valor para las organizaciones”. Y señala que “mientras que el negocio digital cambia lo que hace la organización, el negocio autónomo cambia cómo lo hace”.

Por el momento, como indica el 45% de los encuestados, la automatización que aplican se limita a tareas específicas, pero solo el 13% espera que esto se mantenga para el año 2028. A su vez, el 32% espera implementar herramientas de IA adaptables y de autoaprendizaje para apoyar la toma de decisiones y un 27% espera que sus organizaciones operarán casi sin intervención humana, llevando a cabo una profunda transformación hacia ecosistemas empresariales autónomos.

Esto podría mejorar enormemente la eficiencia de los procesos, pero también plantea riesgos importantes. Según David Furlonger, vicepresidente analista de Gartner, “los directores ejecutivos se están dando cuenta de que la IA no es simplemente otra capa de automatización”, y un 28% opina que los ingresos transaccionales son los más vulnerables a la IA porque, en sus palabras, “a medida que los agentes de IA automatizan las compras, los precios y las negociaciones, eliminan los pasos adicionales y las ineficiencias que las comisiones por transacción estaban diseñadas para cubrir”, lo que obligará a los directivos a “replantearse sus modelos de negocio y orientarlos hacia los ingresos recurrentes basados en resultados para evitar pérdidas”.

> “LOS LÍDERES DE DATA & ANALYSIS DESEMPEÑAN UN PAPEL FUNDAMENTAL PARA OBTENER EL VALOR ESPERADO DE LA IA EN SUS ORGANIZACIONES”
>
> **RITA SALLAM,** Gartner

GOBERNANZA PARA LA IA AGÉNTICA

Los agentes autónomos de IA se revelan como el camino a seguir en los próximos años para impulsar la automatización de procesos, mejorar las fuentes de información que apoyan la toma de decisiones e incrementar la eficiencia y la productividad. Pero esta tecnología debería operar bajo un marco de gobernanza que proteja los intereses de las organizaciones, algo que todavía está lejos de ser una realidad. Según otra investigación de Gartner, para el año 2028, una empresa promedio de la lista Fortune 500 global contará con más de 150.000 agentes en uso (menos de 15 en 2025), pero solo el 13% de ellas cree tener la gobernanza adecuada para controlar el uso de esta tecnología.

Max Goss, analista sénior de la consultora, afirma que "a medida que los CIO y los líderes de TI observan una explosión de agentes de IA en sus organizaciones, muchos se enfrentan a una proliferación descontrolada de estos agentes que los expone a diversos riesgos, como la desinformación, el intercambio excesivo de información y la pérdida de datos". Por ello, opina que "las organizaciones necesitan encontrar un equilibrio que les permita gestionar los agentes y controlar su proliferación, al tiempo que puedan empoderar a los empleados para innovar con estas herramientas de forma segura". ■

CÓMO CONTROLAR LA PROLIFERACIÓN DE AGENTES

Ante la perspectiva de proliferación de agentes autónomos de IA en las organizaciones, los expertos de Gartner han elaborado una lista con seis pasos recomendados para ayudar a los CIO a controlar el uso de IA agéntica en la organización y evitar muchos de los problemas asociados:

- **Establecer gobernanza y políticas sobre quién, cómo y para qué se crean y usan los agentes de IA.**
- **Crear un inventario centralizado de los agentes, con herramientas de gestión de confianza, riesgo y seguridad de la IA (AI TRiSM).**
- **Definir claramente la identidad, los permisos y el modelo del ciclo de vida de los agentes.**
- **Desarrollar la gobernanza de la información que utiliza la IA.**
- **Monitorizar y corregir a los agentes para detectar anomalías y garantizar que se cumplen las políticas establecidas.**
- **Fomentar una cultura de responsabilidad sobre el uso de la IA.**

MÁS INFO +

- Las organizaciones con iniciativas de IA exitosas invierten más en fundamentos de datos y análisis - Gartner
- La IA obligará a transformar de las capacidades operativas – Gartner
- Seis pasos para gestionar la proliferación de agentes de IA - Gartner

LUTECH

Google Cloud

El 56% de las empresas tiene sus datos atrapados en silos.

Sin datos unificados, tu IA no es inteligencia — es ruido.

En Lutech cerramos la brecha entre el dato fragmentado y la IA que tu negocio necesita.

DESCUBRE CÓMO

LUIS ALFARO, ASESOR DE TECNOLOGÍA Y CIBERSEGURIDAD EN PENTEO

“La inteligencia artificial avanza más rápido que el dato”

Iniciamos esta edición de los Encuentros ITDM Group, titulada Modelos operativos y herramientas para una gestión del dato unificada, eficiente y segura, con una ponencia ofrecida por Luis Alfaro, asesor de Tecnología y Ciberseguridad en Penteo. En su intervención, el experto analiza en detalle la situación actual de los datos en las organizaciones españolas en los primeros meses de 2026. Además, comenta las tendencias de inversión en tecnología relacionada con el dato, los retos en materia de gobierno y calidad de la información y el impacto de la inteligencia artificial en la analítica avanzada y la toma de decisiones.

CRECIMIENTO E INVERSIÓN EN EL DATO

Luis Alfaro comienza señalando que, a finales de 2025, el dato y la

PONENCIA >> Luis Alfaro, de Penteo, analiza la situación del dato en la empresa española, destacando la necesidad de mejorar el gobierno y la calidad de la información frente al avance de la IA.

analítica ocupaban el tercer puesto en prioridades de inversión, solo superados por la inteligencia artificial y la ciberseguridad. En cuanto al presupuesto, se observa un incremento del 8% en el CAPEX respecto al año anterior. Sin embargo, advierte sobre un cambio de tendencia, ya que tras el auge de la digitalización por la pandemia y la migración al cloud, el ritmo de crecimiento se está relajando. Actualmente, las empresas españolas han entrado en una fase de búsqueda de optimización y eficiencia, exigiendo un retorno claro de sus inversiones ante lo que Alfaro define como una cierta fatiga en la transformación digital de las organizaciones.

EL ROL DEL CDO Y LA CULTURA DEL DATO

Respecto a las aplicaciones prácticas, las prioridades de las empresas se centran en el análisis del comportamiento del cliente, el forecasting de demanda y el control de costes internos. Para gestionar estos activos, la presencia de un responsable de datos (CDO) varía según el tamaño de la organización. Mientras que en empresas de más de 3.000 usuarios dos tercios cuentan con esta figura, en las pequeñas apenas alcanza el 13%. Y Luis Alfaro destaca que en la administración pública solo el 20% dispone de un CDO. En cuanto a su función, estos responsables parecen priorizar la IA generativa por encima de la propia estrategia o gobierno del dato, un enfoque que, en su opinión, podría generar desequilibrios si no se acompaña de una sólida cultura del dato entre los empleados.

RETOS EN GOBIERNO Y CALIDAD

El panorama del gobierno del dato en España revela que aún queda mucho camino por recorrer. Un 62% de las organizaciones tiene el gobierno definido, pero no implementado, y apenas un 18% cuenta con un catálogo de datos completo. Alfaro subraya que estos procesos se perciben a menudo como burocracia costosa con resultados a largo plazo, lo que dificulta su adopción real. Y cree que esta falta de estructura se refleja en la calidad de la información, ya que más de la mitad de las empresas admite tener una calidad media o baja, y la mayoría confiesa no realizar auditorías de remediación. A esto, se suma que la tendencia de migrar sistemas legacy sin verificar la corrección de la información está provocando un problema estructural que muchas compañías parecen ignorar.

ANALÍTICA AVANZADA E INTELIGENCIA ARTIFICIAL

Finalmente, Luis Alfaro explica que la analítica en España se debate entre lo descriptivo y lo predictivo, y opina que la la inteligencia artificial no sustituirá a la analítica tradicional, tan necesaria para el reporting y la auditoría, sino que la impulsará hacia un modelo de analítica aumentada. Esta evolución facilitará que usuarios no expertos interactúen con la información mediante lenguaje natural, democratizando el acceso al dato en toda la organización. Y señala que el uso de arquitecturas modernas como Fabric o Mesh será clave para acelerar estas predicciones. Por otro lado, señala el gran reto para las empresas de que su interés en la tecnología no eclipse la necesidad de establecer políticas robustas, que hagan que el dato sea accesible, legal y útil para los objetivos del negocio. ■

> “LA IA NO SUSTITUIRÁ A LA ANALÍTICA, PERO SÍ LA IMPULSARÁ HACIA LO QUE SE HA DENOMINADO ANALÍTICA AVANZADA, O AUMENTADA”

LUIS ALFARO,
asesor de Tecnología y Ciberseguridad en **Penteo**

MÁS INFO +

- Ponencia de Luis Alfaro, Penteo
- Encuentros ITDM Group: Modelos operativos y herramientas para una gestión del dato unificada, eficiente y segura

COMPARTIR EN REDES SOCIALES

MODELOS OPERATIVOS Y HERRAMIENTAS PARA UNA GESTIÓN DEL DATO UNIFICADA, EFICIENTE Y SEGURA

La historia de la transformación digital es la historia de la evolución de los datos en el entorno corporativo. Como elemento central de los desarrollos tecnológicos, clave en el despliegue de la inteligencia artificial, el área de data intenta afianzar el gobierno y la calidad. A los desafíos previos se suma la llegada de la IA agéntica, capaz de poner a prueba las estrategias data… Y de mejorarlas.

ENCUENTRO COMUNIDAD IT >> Hemos hablado del trabajo con los datos con líderes de tecnología, datos y analítica de **Acciona, Caixabank Payments & Consumer, Cajasiete, Codere, Embou, Exera Energía** e **Ilunion Hotels**, en una mesa redonda que ha contado también con representantes de **Lutech, ML Code** y **SonicWall.**

> ANTES DE PENSAR EN EL FUTURO DE LA IA, ESTÁ LA ESTRATEGIA DE LA EMPRESA. A PARTIR DE AHÍ, ¿QUÉ HERRAMIENTAS PUEDEN AYUDARNOS?

RAFAEL SOCORRO
head of Data & Analytics, **Acciona**

> A VECES SE QUIERE PONER INTELIGENCIA ARTIFICIAL CUANDO NO LA HAY NATURAL, LO QUE PROVOCA UNAS EXPECTATIVAS QUE NO SE PUEDEN CUMPLIR

ÍÑIGO DE JAIME
responsable GICD, **Caixabank Payments & Consumer**

El concepto data-driven lleva más de un par de décadas entre nosotros, pero no empezó a sonar con verdadera fuerza hasta la década pasada. Y, todavía, solo vinculado a las empresas más innovadoras, las que eran nativas digitales o tenían la tecnología en el centro de su modelo de negocio. De entonces a esta parte, el panorama corporativo ha dado un salto gigantesco hacia la digitalización. Un proceso que tiene los datos en su misma esencia. Y ser data-driven, o como mínimo digital, ha pasado a ser relevante para un creciente número de empresas.

Clica en la imagen para ver la galería completa

Ha pasado a ser, casi, una cuestión de estado. Al menos, una cuestión relevante para lograr los objetivos de la Década Digital 2030 de la Unión Europea, teniendo en cuenta que la intención es que, como mínimo, el 75% de las empresas realice analítica de datos, tenga servicios cloud o utilice la IA. No se trata de que las compañías cambien su esencia porque lo pide la UE; se trata de que se consideran elementos centrales para que el viejo continente mantenga cierto grado de competitividad.

Pero, ¿cuál es impacto real de los datos en las empresas españolas, cuál el grado de evolución y adopción de la cultura data-driven? Hemos hablado de todo ello con líderes de tecnología, datos y analítica de **Acciona, Caixabank Payments & Consumer, Cajasiete, Codere, Embou, Exera Energía** e **Ilunion Hotels**, en una mesa redonda que ha contado también con representantes de **Lutech**, **ML Code** y **SonicWall**.

Clica en la imagen para ver la galería completa

EN BUSCA DE LA CULTURA DEL DATO

La digitalización acelerada que trajo consigo la pandemia puso un peso extra sobre los equipos de tecnología, no solo por las necesidades

“PUEDES HACER PEQUEÑOS PILOTOS DE IA, PERO SI LOS DATOS NO ESTÁN GOBERNADOS CON LA CALIDAD SUFICIENTE, AL PONER EN PRODUCCIÓN ESOS PILOTOS FRACASARÁN”

JAIME PÉREZ
Chief Data Officer, **Cajasiete**

“NOS APOYAMOS EN NEGOCIO PARA QUE PUEDA ACOMPAÑARNOS EN LA CALIDAD DEL DATO, AYUDÁNDONOS A DEFINIR LOS CONTROLES DE ESA CALIDAD”

JENIFFER CHÁVEZ
data manager, **Codere**

Clica en la imagen para ver la galería completa

puntuales para adaptarse al trabajo remoto, sino porque redujeron a pocos meses una transformación que probablemente habría necesitado años. Desde el 2020, ha habido una impresionante evolución tecnológica; pero incluso con la tecnología “de entonces” la digitalización era posible. Lo que no es tan sencillo es el cambio humano.

Todavía hoy la transformación cultural sigue siendo la principal piedra de toque de la evolución corporativa basada en datos. Replantear el gobierno de los datos... O, mejor dicho, establecer un gobierno de los datos exige replantear (ahora sí) los procesos de trabajo corporativos y los hábitos de todos los empleados, desde la alta dirección hasta los becarios. No se trata, además, de un cambio pequeño ni de un cambio único, sino que viene acompañado de múltiples elementos, como el doble factor de autenticación o el uso de la nube.

Iñigo de Jaime, responsable de Gobierno de la Información y Calidad del Dato en Caixabank Payments & Consumer, destaca que “el reto más importante para transformar una compañía en data-driven es que la principal estrategia en la toma de las decisiones se base en los datos. Si en el momento en que llega la IA todavía no tenemos los datos bien gobernados, ¿en qué se va a basar la IA? La llegada de la inteligencia artificial puede tener el efecto positivo de que se invierta para que el dato esté bien para que sus usos sean buenos. Hay que poner el dato en el centro porque sin él no hay ni IA, ni tecnología, ni decisiones estratégicas. El problema del dato no es tanto técnico como de conocimiento funcional. Hay que identificar a las personas con conocimiento de la organización para ponerle el cascabel al dato”.

Rafael Socorro, head of Data & Advanced Analytics en Acciona, explica que, en su caso, son “una empresa multinacional, convivimos con diferentes sistemas, diferentes legisla-

> “NUESTRO SIGUIENTE RETO ES DEMOCRATIZAR EL USO DE LOS DATOS, HACIENDO LLEGAR HERRAMIENTAS DE EXPLOTACIÓN DE LOS DATOS A LOS CLIENTES”

ALEJANDRO VELILLA,
CTO, **Embou**

> “EL MAYOR RETO AL QUE NOS ENFRENTAMOS ES LOGRAR QUE TODA LA ORGANIZACIÓN, DE ALGUNA MANERA, REME EN LA MISMA DIRECCIÓN Y ESTÉ CONVENCIDA DEL PROYECTO”

CARLOS OLMEDA
head of O&M Data Centers,
Exera Energía

Clica en la imagen para ver la galería completa

ciones y clientes. Un primer reto es unificar a nivel conceptual nuestros modelos de datos. Estamos en una etapa de construcción de este tipo de dominios y, en paralelo, implementado el gobierno del dato, identificando data owners, procesos, etc., para acompañar el crecimiento de la empresa. Hemos trabajado muchísimo en asegurar la calidad del dato para hacer el mapeo de los procesos de la organización, entender quiénes interactúan y qué datos se manejan. Una labor de identificación para intentar dar al negocio una visión de los datos no basada en sistemas. No somos un negocio digital, hay una parte importante en torno al dato que es cultural y el gobierno está directamente relacionado con este desafío”.

Por su parte, Jaime Pérez, Chief Data Officer de Cajasiete, señala que, “a corto plazo, hemos optado por gobernar y centralizar el dato. Una vez esté gobernado, nuestra estrategia es empezar a descentralizarlo, buscando los early adopters o embajadores que ayuden a “vender” internamente el proyecto. Nos enfocarnos, sobre todo, en la parte corporativa, mejorando la eficiencia y la disponibilidad de la información. Hemos optado por hacer un cambio gradual y dar soluciones muy tácticas, que tengan impacto en el negocio y ayuden a gestionar las expectativas. La parte de la plataforma de datos es fundamental de cara a poder escalar y gobernar bien toda la estructura de datos, sobre todo con lo que estamos viendo a día de hoy con la IA. Por otro lado, en cualquier movimiento tecnológico tenemos que contar con la variable normativa. Nos apoyamos en los compañeros que tienen estas competencias, que ayudan a agilizar todo este proceso”.

EL MODELO DE GESTIÓN DEL DATO

Uno de los temas más interesantes que se pusieron sobre la mesa fue, precisamente, el modelo de gestión del dato con el que se está trabajando, distinguiendo entre centralizado, distribuido o híbrido. El consenso generalizado es no decidirse por un modelo específico que vaya a funcionar de forma constante a largo plazo, sino que depende en gran medida del momento en que se encuentre la organización en su evolución hacia los planteamientos data-driven.

Álvaro Avendaño, head of Data & Analytics en Ilunion Hotels, detalla que “un modelo centralizado con un gobierno muy concentrado puede venir bien para sentar unas bases y para generar un proyecto común del que partir. Pero es cierto que es un modelo que al final se tensiona, cuando se empieza a demandar más volumen de datos o más procesos, más cambios. Por contra, el modelo descentralizado reparte las funciones en diferentes áreas, pero puede generar silos. Está más cerca del negocio, pero también se corre el riesgo de tener varios flujos de trabajo que atacan el mismo problema. Nosotros estamos migrando hacia un modelo

> “ESTAMOS EN UN PROCESO DE REMODELACIÓN DE LA ARQUITECTURA DE DATOS PARA INCORPORAR CAPAS DE IA QUE NOS HAGAN MUCHO MÁS EFICIENTES Y EFECTIVOS”

ÁLVARO AVENDAÑO
head of Data & Analytics,
Ilunion Hotels

más híbrido, intentando centralizar lo que consideramos que hay que centralizar, como la seguridad integrada en una arquitectura unificada que nos garantice tener una única fuente de la verdad, una semántica compartida. Y, por otra parte, descentralizar o federar otras funciones más relacionadas con la aportación de valor del dato y la activación de ese valor, más cerca de las funciones que se realizan desde las distintas áreas del negocio”.

Jeniffer Chávez, data manager de Codere, también señala que están

Clica en la imagen para ver la galería completa

“llevando todo nuestro planteamiento de datos a una nueva arquitectura centralizada con un modelo híbrido en el que el ownership está enfocado a los diferentes países o unidades de negocio. Venimos de silos de información y estamos evolucionando hacia un modelo híbrido, además de una evolución tecnológica. Tenemos una plataforma centralizada con la arquitectura, la seguridad, las políticas de gobierno del dato y todo lo que consideramos que debemos centralizar. Pero el ownership lo hacemos descentralizado. Nos apoyamos en todos los países y en la gente local. Tenemos personas a las que llamamos link, vínculos, en cada país para que nos ayuden a llevar toda la estrategia de datos. La parte tecnológica sí es muy importante y costosa, pero lo más relevante es que esté alineada bastante bien con negocio, porque son el sponsor, el que le da sentido al dato”.

LA EXIGENCIA DE LOS AGENTES DE IA

Si los equipos de tecnología, de ciberseguridad y de datos manejaban ya entornos de alta complejidad, la llegada de la inteligencia artificial generativa supuso una nueva revolución interna. Muchas empresas llevaban años trabajando en desarrollos de Deep learning y Machine learning, pero la IA generativa trajo complejidades diferentes. Una de ellas, que por una vez era una tecnología que todo el mundo quería, hasta el punto de que el concepto Shadow IT dio paso en seguida a Shadow AI.

> PARA LA IA, HACEN FALTA PERSONAS CON FANTASÍA, QUE PIENSEN FUERA DE LOS ESQUEMAS; PARA DATA, PERSONAS QUE ASEGUREN LA CALIDAD Y LA SEGURIDAD

PAOLO MIOLI
CEO, **Lutech**

RESPONDIENDO A LOS RETOS DEL SECTOR

PAOLO MIOLI, LUTECH

“Ayudamos a estructurar los datos de una forma lógica, con los metadatos necesarios, que puedan ser utilizados por la inteligencia artificial”

La inteligencia artificial generativa ya removió las aguas corporativas, pero los agentes de IA suponen una escalada que exige una revisión de todo el trabajo realizado con los datos. Si un asistente basado en IA no te da una respuesta del todo cierta, el daño es relativo. Pero un agente al que se le da la capacidad de realizar una tarea de forma completamente autónoma no puede tener esa ineficacia. Así que antes que nada hay que preguntarse si nuestros datos están preparados para la IA agéntica.

Severino Gala, vicepresidente de ventas de ML Code, recuerda que “la compañía nació inicialmente con el objetivo de gestionar las iteraciones que se hacen con el dato pasado por la IA, con el foco puesto en la prevención y el tratamiento de la información personal. Esto es, el gobierno y control de la IA. A partir de ahí, montamos una plataforma de desarrollo agéntico, diseñada

Paolo Mioli, CEO de Lutech, explica que la compañía cuenta con tres años de presencia en España, enfocando su actividad en los ámbitos de SAP e inteligencia artificial. Su objetivo principal es ayudar a las organizaciones a estructurar y catalogar la gran cantidad de datos generados para que la tecnología pueda “producir un resultado positivo”. Según señala, el modelo tradicional de centralización presentaba fallos operativos, provocando la “descentralización de la responsabilidad y del valor del dato”.

Para solucionar esto, la firma propone organizar la información de forma lógica mediante metadatos, tratando “el dato como un verdadero producto”, que sea accesible y útil para diferentes departamentos, como marketing o contabilidad, que a menudo tienen visiones distintas de un mismo concepto. El enfoque actual se desplaza de la cantidad a la calidad y la seguridad. En este sentido, Mioli subraya que “el dato es un activo, un producto que tiene la empresa” con un valor estratégico esencial, ya que “en función del dato se toman decisiones estratégicas” fundamentales para el negocio.

> CON PERSONAS Y MÁQUINAS HABLANDO UN LENGUAJE COMÚN, UN LENGUAJE NATURAL, SE ELIMINAN MUCHAS BARRERAS: LAS POSIBILIDADES QUE ABRE LA IA SON INFINITAS

SEVERINO GALA
vicepresidente de ventas,
ML Code

Clica en la imagen para ver la galería completa

con un punto de vista absolutamente abierto y desde la perspectiva de los microservicios para que los clientes elijan las capacidades que necesitan. Ofrecemos un alto nivel de atomicidad en la construcción de las piezas, con elementos con un recorrido breve antes de la siguiente evolución. Un planteamiento mucho más dinámico".

FLEXIBILIDAD Y CIBERSEGURIDAD

Para Carlos Olmeda, head of O&M Data Centers en Exera Energía, "como organizaciones, tenemos que movernos hacia un modelo con mayor peso preventivo y predictivo. Y, por otro lado, hacia organizaciones mucho más flexibles. Estamos en un ámbito tecnológico, en el que la tecnología habitualmente avanza mucho más rápido de lo que creemos y de lo que somos capaces de asumir o asimilar. Desde arriba

RESPONDIENDO A LOS RETOS DEL SECTOR

SEVERINO GALA, ML CODE

"Dotamos nuestra plataforma de capacidades adicionales para que se pueda desplegar e incorporar la IA en los procesos previos de la compañía"

Para Severino Gala, vicepresidente de ventas de ML Code, se observa un "momento efervescente" en el ámbito empresarial actual, donde las organizaciones buscan aprovechar la inteligencia artificial para "poner el dato en valor". Esta tendencia afecta a todo el espectro corporativo: mientras las grandes empresas con carga administrativa han avanzado primero, la IA también está "calando en las empresas medianas y empresas pequeñas" al identificar sus posibilidades de futuro.

La estrategia de ML Code se centra en "dotar a nuestra plataforma de esas capacidades adicionales" para que las compañías puedan aprovechar las ventajas de la inteligencia artificial incorporándola a sus propios procesos. En la etapa actual, el objetivo principal es la creación de "casos de uso que generen la confianza dentro de las propias compañías". Estos casos actúan como un "catalizador y revulsivo" esencial para fomentar el despliegue continuo de la tecnología y ganar la seguridad necesaria para su adopción integral.

> LOS MALOS USAN LA IA PARA COSAS MUY PROSAICAS: LOCALIZAR VULNERABILIDADES O AUTOMATIZAR ATAQUES, PERO SOBRE TODO PARA HACER PHISHING CONVINCENTE

SERGIO MARTÍNEZ
country manager, **SonicWall**

Clica en la imagen para ver la galería completa

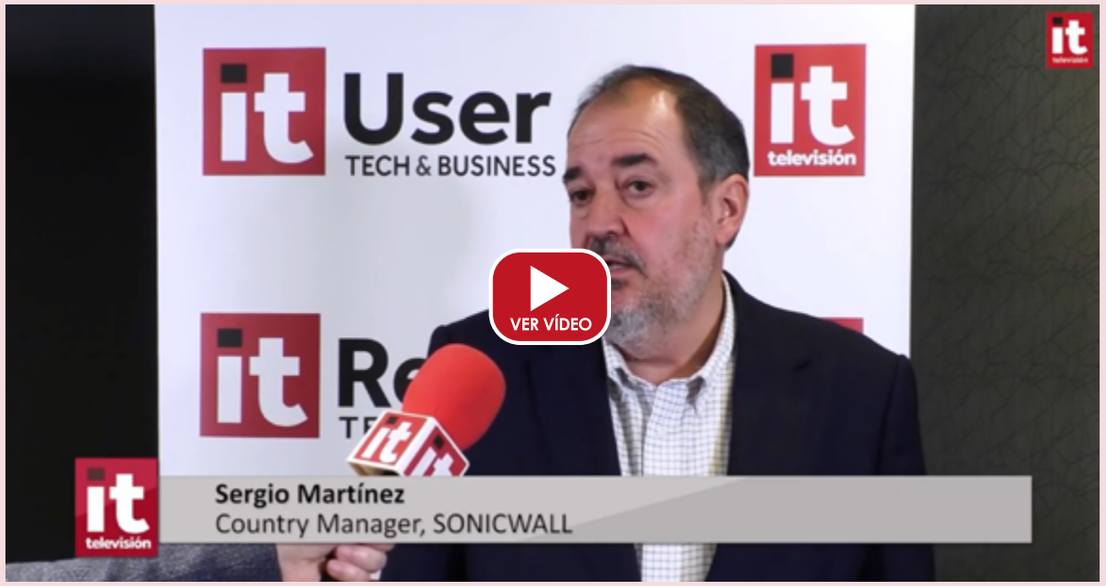
hasta abajo, en cascada, hay que impulsar organizaciones flexibles, porque de lo contrario no te vas a poder adaptar a la actualidad. La IA hay que verla como una herramienta. El dato, además analizado a través de la inteligencia artificial, puede mostrar tendencias y ayudar a la toma de decisiones basadas en esas tendencias que nosotros, como seres humanos, no somos capaces de ver o de anticipar. Y, por tanto, ese tipo de decisiones van a estar mejor informadas y por tanto serán de mayor calidad y más acertadas".

Paolo Mioli, CEO de Lutech, coincide en que "una de las palabras del día es la flexibilidad. Tenemos que adaptarnos a la realidad, a la normativa. Por un lado, debemos ser flexibles para adaptarnos al entorno, a la tecnología. Y, por otro, hay que saber aprovechar las oportunidades que nos brinda la tecnología. En

RESPONDIENDO A LOS RETOS DEL SECTOR

SERGIO MARTÍNEZ, SONICWALL

"Estamos entrando en un nuevo entorno en el que el despliegue de estrategias Zero Trust es imprescindible en todas las organizaciones"



Sergio Martínez, country manager de SonicWall, recuerda el informe de amenazas de la compañía, según el cual las tendencias actuales en ciberseguridad suponen un "retorno a los basics", ya que no se observan grandes sorpresas respecto a años anteriores. El principal problema detectado es que "el robo de identidades constituye el 85% del origen de la mayor parte de las brechas", sumado a que aproximadamente el 75% de estos incidentes proviene de un "deficiente acceso remoto a los sistemas y a los datos". Ante este escenario, Martínez señala que es imperativo el despliegue de estrategias de Zero Trust, "es decir, de máxima desconfianza y mínimo privilegio", junto con la modernización del acceso remoto. El experto advierte además que los atacantes suelen pasar "180 días durmiendo en la organización esperando su momento", dejando pistas que a menudo se ignoran, pues "el 44% de las alertas no se analizan". Por ello, la solución que propone radica en monitorizar y contar con "servicios de seguridad, servicios de SOC, para saber qué es lo que ocurre y poder detectar y responder a tiempo".

nuestro caso, estamos utilizando la IA para completar y mejorar la calidad del dato. Creo que todas las organizaciones, todas, aunque vengamos de sectores distintos, tenemos problemas similares para lograr que la organización se haga responsable del dato, de su calidad; y, al mismo tiempo, que sea capaz de adaptarse a los cambios".

Todos ellos son elementos compartidos, en mayor o menor medida, por todas las empresas. Aunque, como es habitual, las peculiaridades de cada compañía son las que marcan sus propios desafíos. Alejandro Velilla, CTO de Embou, explica que para ellos "el mayor reto ha sido el crecimiento constante. Cada año nos ha llegado una nueva empresa con un partner distinto, un entorno diferente, otra directiva. No se trata solo de la aparición de shadow IT o silos de información, sino de nuevas empresas con su propio legacy. Por supuesto, nuevas empresas que hay que abrazar e integrar de la mejor manera posible... Y en el menor tiempo posible. Tenemos iniciativas transformadoras; por ejemplo, cada área tiene personas clave que están impulsando la inteligencia artificial. También hay otras medidas transversales. Por ejemplo, por ciberseguridad, las VPN con SSL se han quedado obsoletas, están descartadas en la política empresarial".

La ciberseguridad de esta digitalización acelerada es sin duda el común denominador para diferentes tipos de empresa. Sergio Martínez, country manager de SonicWall, explica que "el cibercrimen está utilizando cada vez más lo de siempre. El 85% de todos los incidentes y las brechas de seguridad parten de un compromiso de identidad. Más allá de la protección del dato está quién accede al dato, que es uno de los temas clave. La identidad es la clave para garantizar que quien accede a los datos es quien tiene que acceder. En la pandemia explotó el acceso remoto a través de VPN, sobre todo con protocolos tipo SSL, con un diseño vulnerable. El 70% de los incidentes de ciberseguridad ahora mismo están vinculados al acceso a través de una VPN insegura. Si no haces un profiling de los usuarios y metes una capa de tecnología para identificarlos bien, corres un gran riesgo. El camino pasa por desplegar los múltiples factores de identificación, hacer un profilling de usuarios y luego monitorizar y saber qué es lo que pasa en las redes corporativas".

La ciberseguridad, la protección y la privacidad de los datos son el telón de fondo de las estrategias data-driven. Los datos, por supuesto, son la materia prima que alimenta la digitalización y el elemento sin el que todo lo demás pierde el sentido. Un "todo lo demás" que incluye ese otro factor que puede transformar radicalmente las compañías: la inteligencia artificial. Más vale hacer bien los deberes del dato para que la IA tenga sentido. Como se dijo en la mesa, si la alimentas con basura, lo que sale es basura. ■

#ENCUENTROSITDMGROUP

MÁS INFO +

- Encuentros ITDM Group: Modelos operativos y herramientas para una gestión del dato unificada, eficiente y segura
- Entrevista Jaime Pérez, CDO de Cajasiete

COMPARTIR EN REDES SOCIALES

SONICWALL®

Nunca solo. Seguridad inquebrantable.

Soluciones de ciberseguridad para

- Red
- Nube
- Endpoint
- Servicios XDR gestionados

Descubra cómo impulsar sus ingresos: visite SonicWall.com o escríbanos a spain@sonicwall.com.

JAIME PÉREZ, CHIEF DATA OFFICER DE CAJASIETE

“Queremos migrar la plataforma hacia un modelo federado que permita el autoconsumo de datos”

Cerramos los Encuentros ITDM Group: Modelos operativos y herramientas para una gestión del dato unificada, eficiente y segura con una entrevista a Jaime Pérez, Chief Data Officer de Cajasiete. Nos explica cómo la entidad financiera canaria ha transformado su arquitectura informacional, pasando de silos aislados a una arquitectura centralizada que continúa evolucionando hacia un modelo federado. Además, identifica los principales retos relacionados con la calidad del dato, la gobernanza necesaria para implementar la IA y señala cómo las normativas europeas actúan como guías estratégicas para el negocio en la industria financiera.

ENTREVISTA >> Jaime Pérez, CDO de Cajasiete, analiza la evolución de la estrategia del dato en la entidad, destacando la transición hacia modelos federados, la calidad de la información y el impacto de la inteligencia artificial.

ESTRATEGIA DE MADUREZ Y CENTRALIZACIÓN

Jaime Pérez explica que el punto de partida en Cajasiete fue un

análisis profundo de madurez que reveló niveles muy heterogéneos, según el área o unidad de la entidad. Aunque existía un alto grado de autoconsumo de información, este carecía de una estrategia de gobierno normalizada y segura. Para solventar inconsistencias y ganar la confianza de los usuarios, la organización optó por una fase inicial de centralización del dato. Este proceso, explica, ha sido un reto técnico y cultural, orientado siempre a aportar valor real al negocio y mejorar el servicio al cliente. Tras estos primeros años de recorrido, el objetivo actual de la compañía es evolucionar hacia un modelo federado que fomente la autonomía de las áreas con capacidades analíticas, especialmente dentro de la particular estructura del Grupo Caja Rural, donde diversas cooperativas independientes comparten sistemas y tecnología.

RESPONSABILIDAD Y CALIDAD DEL DATO

Respecto a la calidad de la información, Jaime Pérez sostiene que la mayor responsabilidad recae en el usuario inicial y en el diseño de los sistemas de origen para evitar errores de entrada. Y comenta cómo identificar deficiencias en las etapas finales del ciclo de vida del dato resulta extremadamente costoso y genera impactos no deseados en la toma de decisiones. Por ello, en Cajasiete la estrategia se centra en automatizar la gobernanza y la auditoría desde las fases más tempranas, mediante plataformas especializadas. Aunque advierte que la perfección en la calidad es inalcanzable, opina que el auge de la inteligencia artificial ha convertido este factor en algo crítico, bajo la premisa de que datos de mala calidad solo producirán resultados erróneos.

GESTIÓN DE EXPECTATIVAS EN INTELIGENCIA ARTIFICIAL

Al abordar proyectos de inteligencia artificial, Jaime Pérez identifica la gestión de las expectativas como el principal desafío, incluso por encima de las limitaciones técnicas. Aunque crear pilotos o pruebas de concepto es hoy más accesible y democratizado, escalar estos modelos en una corporación altamente regulada es complejo, y sin una base de datos bien gobernada y auditada, el paso a producción de la IA puede derivar en fracasos significativos. Por ello, defiende un enfoque de “vísteme despacio que tengo prisa”, señalando que la rapidez tecnológica no debe eclipsar la necesaria madurez cultural de la organización.

SEGURIDAD Y REGULACIÓN COMO GUÍA ESTRATÉGICA

La seguridad del dato en Cajasiete se gestiona como un objetivo estratégico de toda la entidad y no solo como una decisión técnica de arquitectura. Jaime Pérez valora normativas como la AI Act o DORA no como impedimentos al negocio, sino como metodologías que proporcionan una guía clara para escalar y gobernar la tecnología de forma adecuada. En cuanto a la inversión tecnológica, destaca que cada iniciativa debe presentarse como un plan de negocio particular con métricas de retorno claras. Además, destaca que utilizar un lenguaje orientado a la eficiencia y productividad, en lugar de términos puramente técnicos, ha sido fundamental para obtener el respaldo de la alta dirección en la actualización de sus plataformas de información. ■

> “CENTRALIZAMOS EL DATO PARA DARLE NORMALIZACIÓN, GOBIERNO Y CALIDAD, Y SOBRE TODO PARA QUE LOS USUARIOS TENGAN CONFIANZA EN EL MISMO”

JAIME PÉREZ,
Chief Data Officer de **Cajasiete**

MÁS INFO +

- Entrevista a Jaime Pérez, Cajasiete
- Encuentros ITDM Group: Modelos operativos y herramientas para una gestión del dato unificada, eficiente y segura

COMPARTIR EN REDES SOCIALES

MODELOS OPERATIVOS Y HERRAMIENTAS PARA UNA GESTIÓN DEL DATO UNIFICADA, EFICIENTE Y SEGURA

¡VER AHORA!

it Digital MAGAZINE

ENCUENTROS ITDM GROUP

ENCUENTROS IT RESELLER

EL ROL DEL PROVEEDOR DEL SERVICIOS GESTIONADOS ANTE EL ESTADO DE LA CIBERSEGURIDAD EMPRESARIAL

ORGANIZA

it Reseller TECH&CONSULTING

PATROCINADOR

ESET Cybersecurity
Progress. Protected.

LA IA ACELERA LA DISRUPCIÓN DEL MSP Y SITÚA LA CIBERSEGURIDAD EN EL CENTRO DEL NEGOCIO

#ENCUENTROSITRESELLER

La irrupción de la IA está transformando el negocio de los proveedores de servicios gestionados, automatizando tareas clave y obligando a los proveedores a replantear su propuesta de valor. La ciberseguridad emerge como el pilar más estable para sostener ingresos y diferenciarse en un mercado cada vez más competitivo.

El mercado de los proveedores de servicios gestionados (MSP) vive un punto de inflexión. La inteligencia artificial se ha convertido en la variable que más está transformando la operativa, la oferta de servicios y la relación con los clientes. De hecho, el 48% de los MSP identifica la IA y la automatización como la principal necesidad de sus clientes, por encima incluso de la seguridad o el backup.

Pero esta demanda llega en un contexto de presión creciente, con el 71% de los MSP que afirma que captar nuevos clientes es su mayor desafío. El tamaño medio de los contratos se ha reducido drásticamente, pasando del 75% al 41% en acuerdos superiores a 25.000 dólares anuales. La competencia aumenta, los márgenes se estrechan y demostrar valor rápido se ha convertido en una exigencia crítica.

En este escenario, la IA aparece como la palanca para escalar operaciones sin aumentar plantilla. El 53% de los MSP ya utiliza IA para automatizar ticketing, parcheo y monitorización, con mejoras visibles en tiempos de respuesta y eficiencia técnica. Sin embargo, la mayoría apenas ha automatizado una cuarta parte de su carga de trabajo, lo que evidencia que el recorrido es amplio, pero también complejo.

LA AUTOMATIZACIÓN REDEFINE EL VALOR DEL MSP

A pesar del entusiasmo, la realidad es que la IA está generando menos impacto del esperado. Un análisis de Boston Consulting Group (BCG) revela que solo el 5% de las organizaciones obtiene valor real de la IA a escala, mientras que un 60% reconoce que el impacto es escaso o inexistente. La causa no es tecnológica, sino organizativa.

Las empresas están desplegando IA sin preparar los cimientos, tales como la gobernanza del dato, la calidad y accesibilidad de la información, el impacto en los equipos, la definición de métricas de éxito, y la alineación con los procesos reales del negocio. Este vacío entre expectativas y resultados abre una oportunidad clara para que los MSP se conviertan en los actores que traduzcan la IA en impacto tangible.

Históricamente, el negocio MSP se ha sustentado en soporte, mantenimiento, monitorización y gestión de dispositivos. Pero la IA está automatizando gran parte de estas tareas de bajo nivel. Esto implica que el modelo tradicional basado en ho-

LOS MSP DEBEN SITUARSE EN EL CORAZÓN DE LOS PROCESOS DEL CLIENTE. YA NO BASTA CON GESTIONAR INFRAESTRUCTURA, HAY QUE ENTENDER CÓMO SE TRABAJA, DÓNDE SE PRODUCEN LOS CUELLOS DE BOTELLA Y QUÉ CASOS DE USO PUEDEN GENERAR VALOR INMEDIATO

ras, tickets y mantenimiento pierde peso. Facilitar acceso a herramientas es la parte fácil, pero ayudar a lograr resultados tangibles es el verdadero reto, y eso exige un cambio profundo en el rol del MSP.

La oportunidad de negocio no está en vender acceso a IA, sino en traducir la tecnología en impacto real. Los MSP que abracen este rol ayudarán a sus clientes a pasar del interés al impacto, y se posicionarán como actores esenciales en la próxima década de transformación digital.

Para generar impacto real, los MSP deben situarse en el corazón de los procesos del cliente. Ya no basta con gestionar infraestructura, hay que entender cómo se trabaja, dónde se producen los cuellos de botella y qué casos de uso pueden generar valor inmediato.

El nuevo modelo exige mapear workflows críticos y detectar ineficiencias, priorizar casos de uso simples y visibles para demostrar valor rápido; involucrar a COO, responsables de negocio y líderes de procesos, no solo a TI; definir métricas claras de éxito desde el primer día; acompañar al cliente en gobernanza, formación y adopción; y medir y optimizar de forma continua para sostener el impacto. Este enfoque consultivo convierte al MSP en un socio estratégico, no en un proveedor de soporte.

LA CIBERSEGURIDAD COMO PILAR DEL NEGOCIO

Mientras la IA automatiza tareas y redefine el modelo operativo, la ciberseguridad se consolida como el área donde los MSP pueden aportar más valor inmediato y medible. Los datos lo confirman: el 71% de los MSP reporta crecimiento interanual en servicios de ciberseguridad, la cifra más alta de todas las categorías, seguida por continuidad de negocio y recuperación ante desastres.

En un mercado donde demostrar valor rápido es cada vez más difícil, con un 19% de los MSP que reconoce problemas para hacerlo, casi el doble que el año anterior, la seguridad ofrece métricas claras, impacto directo, urgencia real, una narrativa comprensible para el cliente y un retorno inmediato.

La ciberseguridad se convierte así en el refugio del MSP, el área donde los clientes siguen invirtiendo, donde el valor es evidente y donde la competencia es menos sensible al precio. ■

EL ROL DEL PROVEEDOR DE SERVICIOS GESTIONADOS ANTE EL ESTADO DE LA CIBERSEGURIDAD EMPRESARIAL

ASAC, Excelia, Inforges, INSSIDE Ciberseguridad, Minery Report y Secure&IT analizaron en un nuevo Encuentro IT Reseller, apoyado por ESET, cómo está evolucionando la ciberseguridad empresarial y por qué el modelo de servicios gestionados se ha convertido en una pieza clave para proteger a las organizaciones. En un escenario marcado por la presión regulatoria, la escasez de talento y el aumento de amenazas, los proveedores coinciden en que el mercado demanda acompañamiento experto y relaciones de largo plazo.

La ciberseguridad ha dejado de ser una conversación reservada a los departamentos técnicos para instalarse de lleno en los comités de dirección. El incremento de

ENCUENTRO COMUNIDAD IT >> ASAC, Excelia, Inforges, INSSIDE Ciberseguridad, Minery Report y Secure&IT analizaron en un nuevo Encuentro IT Reseller, apoyado por ESET, cómo está evolucionando la ciberseguridad empresarial y por qué el modelo de servicios gestionados se ha convertido en una pieza clave para proteger a las organizaciones.

#ENCUENTROSITRESELLER

Clica en la imagen para ver la galería

amenazas, la presión regulatoria, la escasez de profesionales especializados y la creciente dependencia digital están obligando a las empresas a revisar sus estrategias de protección. En ese nuevo escenario, los modelos de servicios gestionados ganan peso porque ofrecen acceso inmediato a conocimiento experto, capacidad operativa continua y una estructura flexible que muchas organizaciones no pueden desarrollar por sí solas.

Esa fue una de las principales conclusiones del Encuentro IT Reseller, celebrado con el apoyo de ESET España y Ontinet, y en el que participaron directivos de ASAC, Excelia, Inforges, INSSIDE Ciberseguridad, Minery Report y Secure&IT. A lo largo del debate, los asistentes analizaron cómo está evolucionando el panorama de riesgos, qué demandan hoy los clientes y por qué la confianza, más que la tecnología en sí misma, se ha convertido en el verdadero factor diferencial dentro del mercado de la ciberseguridad.

ESTADO DE LA CIBERSEGURIDAD EN ESPAÑA EN LA PRIMAVERA DE 2026

Josep Albors, head of Awareness and Research de ESET España, arrancó el debate explicando que el mercado vive una continuidad de amenazas tradicionales que ahora se ven reforzadas por nuevas capacidades tecnológicas. En su opinión, el phishing sigue siendo el gran protagonista del panorama criminal, ya sea mediante correo electrónico, mensajes SMS, redes sociales o campañas más sofisticadas.

“Vemos no tanto una evolución, sino una continuidad de amenazas clásicas”, señaló. A su juicio, la inteligencia artificial ha permitido además que actores con escasa preparación técnica puedan lanzar ataques con mayor facilidad.

El directivo de ESET también puso el foco en el ransomware y en la posición de España dentro del mapa de riesgo europeo. El dato preocupa especialmente porque una gran parte de los ataques se dirige a compañías medianas y pequeñas, donde la resistencia suele ser menor y la recuperación, más costosa.

EL ESLABÓN MÁS PRESIONADO SIGUE SIENDO LA PYME

La pequeña y mediana empresa ocupó buena parte del debate. El motivo es evidente. Y es que España mantiene un tejido productivo ampliamente apoyado en este segmento y muchas de estas organizaciones operan con recursos limitados, plantillas reducidas y una capacidad tecnológica muy desigual.

Ricardo Martínez, Director de Desarrollo de Negocio de Ciberseguridad de Excelia, defendió que el retraso acumulado en muchas pymes las ha convertido en un objetivo prioritario para los atacantes. “Las pymes no han puesto tanto cuidado y llevan mucho retraso”, afirmó.

Desde la experiencia de Excelia, el esfuerzo criminal necesario para comprometer una pyme suele ser menor que el exigido por una gran

“LA CIBERSEGURIDAD ES CONFIANZA Y TRANQUILIDAD PARA EL CLIENTE”

MARIO CORPAS
consultor TIC en **ASAC**

“AHORA LOS CLIENTES BUSCAN MÁS LO QUE LE VAS A DAR CON EL PRODUCTO QUE LO QUE EL PRODUCTO HACE”

RICARDO MARTÍNEZ
director de Desarrollo de Negocio de Ciberseguridad en **Excelia**

Clica en la imagen para ver la galería completa

corporación, mientras que las probabilidades de monetización son elevadas. Esa ecuación explica por qué el foco de los delincuentes se ha desplazado con tanta claridad hacia este colectivo. “Es un segmento al que deberíamos poner foco dentro de nuestras estrategias de ciberseguridad”, recalcó.

Germán Sánchez, responsable de línea de negocio de Sistemas y Ciberseguridad de Inforges, recordó además que el 90% del tejido empresarial español está formado por pymes, lo que convierte cualquier debilidad estructural en un problema sistémico para la economía. “El problema que tenemos es tratar de que un gerente vea la necesidad y la importancia”, señaló. En muchas pequeñas compañías, explicó, la inversión en seguridad sigue posponiéndose hasta que se produce un incidente real.

También Miguel Ángel Romero, CEO y socio fundador de Minery Report, explicó que están detectando un fuerte incremento de necesidades entre pequeñas empresas industriales, alimentarias y organizaciones que tradicionalmente habían quedado fuera del radar de los grandes integradores. “No encuentran proveedores directamente que sean capaces de ayudarles”, indicó al referirse a compañías que necesitan apoyo tanto en entornos IT como OT. Según explicó, muchas de ellas sí disponen de cierta gestión informática, pero siguen muy perdidas en todo lo relacionado con protección industrial.

Por su parte, Lautaro Fernández, Chief Information Security Officer & Cybersecurity Advisor de INSSIDE Ciberseguridad, apuntó que “las pymes y las startups, que para mí son dos conceptos diferentes, están teniendo un gran problema”. En su opinión, muchas grandes compañías están trasladando exigencias regulatorias a su cadena de suministro sin tener en cuenta la capacidad real de sus proveedo-

> LA CIBERSEGURIDAD YA NO ES UNA CUESTIÓN TÉCNICA, ES UNA CUESTIÓN DE NEGOCIO

GERMÁN SÁNCHEZ,
responsable de línea de negocio de Sistemas y Ciberseguridad en **Inforges**

Clica en la imagen para ver la galería completa

res más pequeños para asumirlas en plazo.

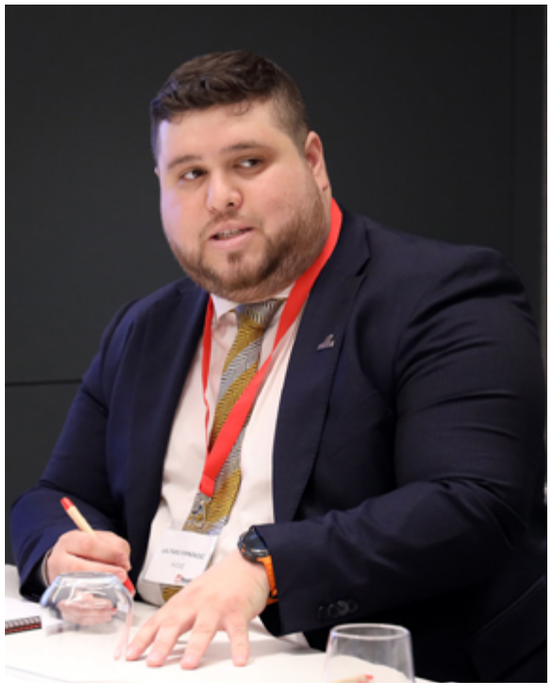
LA CIBERSEGURIDAD ENTRA DE LLENO EN LA AGENDA DEL NEGOCIO

La conversación sobre ciberseguridad ya no pertenece exclusivamente a los departamentos técnicos. Esa fue una de las ideas más compartidas durante el encuentro. Los incidentes afectan a la continuidad operativa, a la reputación, a la capacidad de facturación y, en muchos casos, a la viabilidad misma de una compañía cuando no existe preparación previa.

En esa línea se pronunció Germán Sánchez, de Inforges, quien recordó que la ciberseguridad ya no puede tratarse como una partida aislada. “La ciberseguridad ya no es una cuestión técnica, es una cuestión de negocio”, indicó. Cuando una fábrica se detiene, cuando un ERP queda bloqueado o cuando una operación logística se interrumpe, el problema deja de pertenecer al área tecnológica y pasa a la cuenta de resultados.

> LA CIBERSEGURIDAD NO PUEDE ESTAR EXENTA DE LA MISIÓN Y VISIÓN DE LA COMPAÑÍA

LAUTARO FERNÁNDEZ
Chief Information Security Officer & Cybersecurity Advisor en **INSSIDE Ciberseguridad**



Clica en la imagen para ver la galería completa

También Javier Martí, responsable de seguridad de Secure&IT, insistió en la velocidad a la que evoluciona el riesgo. “Antes cuando salía una vulnerabilidad teníamos semanas para parchearlo y ahora si tienes horas pues has tenido suerte”, afirmó. Esa aceleración obliga a revisar procesos internos, capacidad de respuesta y nivel real de vigilancia.

Desde ASAC, Mario Corpas, consultor TIC, añadió que muchas organizaciones todavía están en fases tempranas de madurez y necesitan orientación para priorizar inversiones. Según explicó, no siempre falta voluntad, sino conocimiento para decidir por dónde empezar y qué controles implantar primero. “El cliente lo que necesita ahora mismo es priorizar”, señaló. Esa necesidad de criterio está elevando el papel de los proveedores especializados como socios de decisión y no solo como suministradores tecnológicos.

> EL PRINCIPAL VALOR QUE APORTAMOS AL CLIENTE ES POSICIONARNOS A SU LADO Y QUITARLE PESO

MIGUEL ÁNGEL ROMERO
CEO y socio fundador en
Minery Report

> UN MSP TE DA LA POSIBILIDAD DE TENER UN EQUIPO MULTIDISCIPLINAR FORMADO EN UN ÁMBITO DE 24X7

JAVIER MARTÍ
responsable de Seguridad en
Secure&IT

REGULACIÓN Y CUMPLIMIENTO ACELERAN LAS DECISIONES

Si durante años muchas organizaciones aplazaron inversiones en protección digital, la llegada de nuevas normativas está actuando como catalizador. NIS2, DORA y otros marcos sectoriales están obligando a revisar procesos, proveedores y niveles reales de madurez.

Mario Corpas, de ASAC, explicó que una parte relevante de su actividad se concentra en administraciones públicas y entidades relacionadas con ellas. En esos entornos, el cumplimiento normativo se ha convertido en prioridad inmediata. “Nos piden acompañamiento para ‘compliance’ e implementar todas las medidas técnicas posibles”, señaló. Según explicó, muchas entidades necesitan apoyo tanto jurídico como operativo, además de un socio que les ayude a traducir la norma en medidas reales.

Clica en la imagen para ver la galería completa

Corpas añadió que, en numerosos casos, las organizaciones deben centrarse en su misión principal y no disponen de estructura suficiente para asumir internamente toda la carga que exige la nueva regulación.

También Miguel Ángel Romero, de Minery Report, confirmó un fuerte incremento de demanda vinculado al cumplimiento. “Este primer trimestre hemos tenido casi un 40% más de trabajo relacionado con la normativa NIS2 o similares”, aseguró.

Romero explicó que muchos responsables de TI ya han entendido que adaptarse no consiste en comprar una herramienta ni en redactar un documento. Requiere revisar procedimientos, medir riesgos, establecer controles y, sobre todo, generar cultura interna.

Clica en la imagen para ver la galería completa

Lautaro Fernández, Chief Information Security Officer & Cybersecurity Advisor de INSSIDE Ciberseguridad, introdujo asimismo una reflexión especialmente relevante. Para él, la seguridad no puede imponerse de forma artificial cuando

“VEMOS NO TANTO UNA EVOLUCIÓN, SINO UNA CONTINUIDAD DE AMENAZAS CLÁSICAS”

JOSEP ALBORS,
head of Awareness and Research en **ESET**

“LOS CLIENTES YA NO QUIEREN SOLO EL PRODUCTO, SINO A ESA PERSONA QUE HAY DETRÁS”

FRAN MOLLÁ
channel account manager en **Ontinet**

« Clica en la imagen para ver la galería completa »

la organización no ha desarrollado antes un nivel básico de orden y madurez. “La ciberseguridad es madurez. No puedes implementar herramientas sobre cosas que no tienen un nivel de madurez”, subrayó.

SOBERANÍA DIGITAL Y REVISIÓN DEL CLOUD

La geopolítica y la dependencia tecnológica también ocuparon una parte relevante del debate. Muchas organizaciones están revisando su relación con los grandes proveedores internacionales y replanteando la ubicación de cargas críticas.

Mario Corpas, de ASAC, aseguró que ciertos clientes públicos ya no solo buscan alternativas a los hiperescalares, sino alojar infraestructuras directamente en España, y Germán Sánchez, de Inforges, confirmó una tendencia de retorno parcial tras años de migraciones intensivas al cloud. Primero llegaron los modelos híbridos, y ahora determinadas cargas críticas vuelven a valorarse en entornos locales.

Javier Martí, de Secure&IT, introdujo una precisión importante, que “la localización del dato no es lo mismo que la soberanía del dato”. En su opinión, no basta con conocer dónde reside la información. También importa quién la gestiona, cómo se comparte y bajo qué legislación queda sometida.

Ricardo Martínez, de Excelia, amplió el foco hacia las propias soluciones de seguridad. Para él, la discusión no debería limitarse al datacenter, sino incluir la procedencia tecnológica de las herramientas utilizadas.

Clica en la imagen para ver la galería completa

EL VALOR CRECIENTE DEL MODELO MSP Y MSSP

Con amenazas al alza, presión regulatoria y escasez de profesionales, el avance de los servicios gestionados aparece como consecuencia natural. Las empresas buscan acceso inmediato a conocimiento especializado sin asumir los costes y dificultades de construirlo desde cero.

Corpas, desde ASAC, defendió que para una pyme resulta muy complejo justificar internamente la inversión necesaria para alcanzar un nivel alto de madurez tecnológica y organizativa. “No le va a compensar ni técnica ni económicamente frente a un proveedor que ya tenga esa madurez”.

El argumento se repitió con distintos matices a lo largo del encuentro. No se trata solo de externalizar tareas, sino de incorporar capacidades que de otro modo serían inaccesibles.

Javier Martí, de Secure&IT, incidió en la capacidad operativa del modelo. “Un MSP te da la posibilidad de tener un equipo multidisciplinar formado en un ámbito de 24x7”.

Sin embargo, para el directivo de Secure&IT, el verdadero diferencial no está únicamente en la vigilancia continua, sino en el conocimiento del negocio protegido. Gestionar alertas sin contexto solo genera ruido, e interpretarlas según el impacto real es lo que aporta valor. “Necesito saber si lo que se ha tocado está conectado a la máquina de café o es una base de datos de la empresa”, explicó con ironía.

Germán Sánchez, desde Inforges, añadió otra ventaja decisiva. La economía de escala permite ofrecer servicios avanzados a precios asumibles para compañías medianas y pequeñas. Compartir especialistas, herramientas y experiencia multiplica la eficiencia del modelo.

DEL PRODUCTO A LA RELACIÓN DE SERVICIO

El mercado tecnológico vive además un cambio profundo en la forma de comprar. Durante años, buena parte de la conversación comercial giró alrededor del producto. Hoy el cliente pregunta cada vez más por resultados, acompañamiento y capacidad de respuesta.

Fran Mollá, Channel Account Manager de Ontinet, explicó que muchos partners ya no buscan solo licencias o funcionalidades. “Ya no quieren solo el producto sino a esa persona que hay detrás”. El ejecutivo de Ontinet/ESET España sostuvo que el cliente valora poder llamar, hablar con alguien que conoce su entorno y resolver incidencias con rapidez. Esa proximidad, unida a personal altamen-

RESPONDIENDO A LOS RETOS DEL SECTOR

JOSEP ALBORS, ESET

“Las amenazas actuales afectan a todo tipo de empresas, pero impactan mucho en la pyme”

Tal y como explicaba Josep Albors, head of Awareness and Research en ESET, la situación actual del mundo de la ciberseguridad en España no está viviendo una gran revolución, sino una evolución e incremento de tendencias que han estado presentes en el mercado.

Para este responsable, “lo que estamos viendo es que se están reutilizando muchas técnicas clásicas pero potenciadas, por una parte, por kits que están vendiendo los delincuentes, y, por otra, por la inteligencia artificial, lo que facilita el acceso de los ciberdelincuentes a todo tipo de estafas, fraudes, ciberamenanzas… incluso algunas medianamente avanzadas. La implosión de este tipo de amenazas y el gran número de ellas repercute, sobre todo, en el sector pyme, que es el principal en España”.

te certificado, sería muy difícil de replicar internamente para muchas organizaciones.

Miguel Ángel Romero, desde Minery Report, fue todavía más explícito. “Nosotros no vendemos producto”. Su enfoque pasa por asesorar desde una posición agnóstica y recomendar aquello que realmente necesita el cliente, no lo que más conviene comercialmente al proveedor.

Ricardo Martínez, de Excelia, coincidió en esa evolución del mercado. “En el pasado –señaló–, se implantaban soluciones que luego nadie sabía explotar correctamente. Hoy el cliente quiere entender qué problema resuelve la inversión y cómo se traduce en mejoras tangibles”.

LA CONFIANZA COMO GRAN FACTOR COMPETITIVO

Cuando el encuentro se adentró en la diferenciación entre proveedores, apareció una palabra repetida de forma casi unánime: confianza.

Mario Corpas, de ASAC, lo resumió con claridad. “La ciberseguridad es confianza”. El cliente necesita dedicar tiempo a su negocio y sentirse respaldado por un socio que responda cuando surge un incidente o una necesidad urgente.

Javier Martí, desde Secure&IT, recordó que la reputación en este sector se construye lentamente y puede perderse muy deprisa. “Yo os puedo engañar a todos una vez, pero si engaño una vez ya estoy muerto”, afirmó. La frase resume una realidad conocida en el canal. Y es que las referencias, el boca a boca y la experiencia compartida pesan más que cualquier campaña publicitaria.

Para Germán Sánchez, de Inforges, esa confianza fortalece vínculos duraderos y convierte al proveedor en una extensión operativa del cliente. Ya no se trata de vender una herramienta, sino de estar disponible cuando hace falta, incluso fuera del horario convencional.

Lautaro Fernández, de INSSIDE Ciberseguridad, prefirió definir ese vínculo “no como un proveedor, sino un aliado estratégico”.

EL RETO MENOS VISIBLE SIGUE SIENDO EL TALENTO

Aunque el mercado ofrece crecimiento y oportunidades, los propios proveedores reconocieron un desafío persistente, en la capta-

RESPONDIENDO A LOS RETOS DEL SECTOR

FRAN MOLLÁ, ONTINET

“Debemos proteger al cliente, que deposita su confianza en nosotros”

Desde la perspectiva de Fran Mollá, channel account manager en Ontinet, “una de las principales ventajas que ofrece el modelo MSSP, tanto para los distribuidores como para los usuarios, es la cercanía, el conocimiento y la relación que se extiende en el tiempo y se adapta a las necesidades de las empresas”.

Para ayudar en este terreno a los reseller, “tenemos un gran abanico de productos y podemos adaptarlos a sus necesidades, entendiéndolos y proporcionándoles un trato muy humano con nuestros equipos de soporte e ingeniería técnica”.

De hecho, “como hemos podido ver en el debate, es muy importante cuidar al cliente que deposita su confianza en nosotros, proporcionándole un servicio llave en mano, totalmente gestionado, para que puedan contar con expertos de primer nivel pero sin la necesidad de incrementar su plantilla ni realizar costosas formaciones entre su personal”.

ción y retención de profesionales especializados.

Corpas explicó que muchas compañías invierten meses en formar perfiles junior que, una vez adquieren experiencia, reciben ofertas difíciles de igualar. “El tema de la rotación de personal es complicado”.

Javier Martí, de Secure&IT, añadió que la velocidad del cambio obliga a un aprendizaje continuo. Nuevas tecnologías, amenazas y normativas exigen estudio permanente. “Es un aprendizaje constante”.

Ricardo Martínez, desde Excelia, recordó además que el modelo solo funciona si es rentable. “Hay que dar servicio y encima ganar dinero”. En esta línea, Miguel Ángel Romero, de Minery Report, defendió la combinación entre ingresos recurrentes y proyectos de mayor especialización como vía para sostener crecimiento, talento e inversión futura.

UN MERCADO MÁS MADURO Y EXIGENTE

La jornada dejó una conclusión compartida. El mercado ha madurado. Las empresas ya no compran únicamente tecnología, ni se dejan seducir con facilidad por catálogos interminables de funcionalidades. Buscan criterio, acompañamiento, honestidad comercial y capacidad real de respuesta.

Josep Albors, de ESET España, reivindicó precisamente ese valor relacional al explicar la larga trayectoria de muchos partners con la compañía. Según señaló, el soporte recibido en momentos difíciles pesa tanto como el propio producto. “El boca a boca funciona y la confianza hace muchísimo”.

Fran Mollá, de Ontinet.com, cerró el encuentro con una idea sencilla y muy reveladora. “La mayor ventaja que ofrecemos a los MSSP es la creación de una relación duradera con los clientes”. En un entorno de amenazas crecientes y decisiones cada vez más complejas, esa relación puede ser la diferencia entre un proveedor más y un socio imprescindible. ■

MÁS INFO +

» El rol del proveedor de servicios gestionados ante el estado de la ciberseguridad empresarial

QUE LA CIBERSEGURIDAD DE TU EMPRESA NO TE QUITE EL SUEÑO

Monitorización, detección y respuesta 24/7 para tu negocio.

SABER MÁS

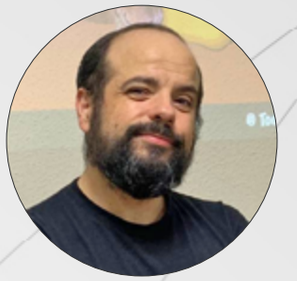
ESET®

Cybersecurity
Progress. Protected.

JORGE DÍAZ-CARDIEL
socio director general de Advice Strategic Consultants

LAS TECNOLOGÍAS DIGITALES MÁS DISRUPTIVAS EN ESPAÑA

LORENZO MARTÍNEZ RODRÍGUEZ
experto en ciberseguridad



EL FIN DE UN CICLO... DE FORMACIÓN

JOSÉ MANUEL NAVARRO
experto en Marketing

LA AUTONOMÍA FINANCIERA EN EUROPA

DANIEL PÉREZ LIMA
CIO & CISO de Genomcore

CÓMO PROTEGER LA EMPRESA EN ENTORNOS HÍBRIDOS (ACCESOS EN LA NUBE / SAAS) – REGISTRO DE DISPOSITIVOS

JORGE DÍAZ-CARDIEL
Socio director general de Advice Strategic Consultants

Economista, sociólogo, abogado, historiador, filósofo y periodista. Autor de más de veinte mil de artículos de economía y relaciones internacionales, ha publicado más de una veintena de libros, cinco sobre Digitalización. Ha sido director de Intel, Ipsos Public Affairs, Porter Novelli International, Brodeur Worldwide y Shandwick Consultants.

LAS TECNOLOGÍAS DIGITALES MÁS DISRUPTIVAS EN ESPAÑA

En España y Europa la disrupción de 2026 no viene de una sola tecnología, sino de la combinación de IA agéntica + confianza digital + automatización física, con computación cuántica y smart glasses, como apuestas estratégicas de siguiente generación.

En abril de 2026, por tanto, las tendencias más disruptivas se concentran, sobre todo, en IA agéntica, robótica, computación cuántica, smart glasses y "digital trust"/verificación de contenidos. También destacan biotecnología aplicada a alimentos y servicios basados en automatización empresarial, ya que están pasando de la fase de prueba a la de despliegue real.

LAS TECNOLOGÍAS DISRUPTIVAS MÁS IMPORTANTES

- **IA agéntica (AgenticAI).** El gran objetivo de 2026 es pasar de "copilotos" a sistemas que planifican, ejecutan y coordinan tareas, casi de extremo a extremo, dentro de las empresas. Distintas fuentes sitúan 2026 como el año en que los agentes pasan de pilotos a producción, con usos en cloud, ciberseguridad, finanzas, atención al cliente y operaciones.
- **Robótica física.** La robótica se está saliendo del entorno industrial puro y entrando en logística, reparto, Retail y asistencia personal. La parte más disruptiva no es solo el robot humanoide, sino la combinación de robots con IA para operar en entornos reales, con productos y

despliegues previstos durante 2026. El Corte Inglés en España y Amazon en EE.UU. ya utilizan este tipo de robótica en el "back-office", en almacén, aumentando la productividad y eficiencia.

- **Computación cuántica.** En 2026, la cuántica ya no se presenta solo como investigación, sino como infraestructura con casos de uso en optimización, materiales, logística y ciberseguridad. La narrativa dominante es que no sustituirá al cómputo clásico, sino que lo complementará en problemas muy específicos y de alto valor. Los grandes bancos españoles llevan tiempo haciéndolo, destacando CaixaBank en el análisis de riesgos de inversiones en el volátil e impredecible negocio de seguros con VidaCaixa, de la mano de D-Wave Computing.
- **Smart glasses y XR.** Las gafas inteligentes están volviendo con fuerza, ahora impulsadas por IA, mejores pantallas y ecosistemas XR. La novedad disruptiva es que pueden convertirse en una interfaz cotidiana para información, asistencia y captura de contenido, compitiendo parcialmente con el móvil en algunos usos.
- **Digital trust y verificación.** Todo lo relacionado con provenance metadata, trazabilidad, autenticidad y etiquetado de contenido generado por IA, gana peso por la regulación europea y por el problema de los deepfakes. Esto está empujando servicios de identidad, firma, autenticación y prueba de origen de contenido.
- **Biotecnología y foodtech.** La fermentación de precisión y las proteínas alternativas están avanzando hacia mayor escala industrial, con foco en coste, consistencia y formulación. Esto puede ser muy disruptivo para alimentación, ingredientes funcionales y cadenas de suministro de proteína.

RANKING DE TECNOLOGÍAS: MAYOR DISRUPCIÓN

De mayor a menor disrupción, las siguientes tecnologías digitales más destacadas en abril de 2026 serían:

- **IA agéntica en empresa:** por velocidad de adopción y por impacto directo en productividad.
- **Robótica con IA en mundo físico:** por efecto en costes, trabajo y logística.
- **Digital trust / verificación:** porque la demanda regulatoria y el fraude digital la convierten en infraestructura crítica.

> **PONIENDO FOCO EN ESPAÑA PRIORIZARÍAMOS TECNOLOGÍAS COMO IA AGÉNTICA, CIBERSEGURIDAD Y DIGITAL TRUST, ROBÓTICA/AUTOMATIZACIÓN, CUÁNTICA, SMART GLASSES/XR Y BIOTECNOLOGÍA APLICADA**

- **Smart glasses:** si el formato cuaja, puede ser el próximo gran cambio de interfaz.
- **Cuántica comercial:** enorme potencial, pero todavía más selectiva y menos generalizada.

Poniendo foco en España priorizaríamos tecnologías como IA agéntica, ciberseguridad y digital trust, robótica/automatización, cuántica, smart glasses/XR y biotecnología aplicada. En España, además, hay señales claras de foco institucional y empresarial en agentes de IA, ciberseguridad, 5G, IA y digitalización industrial. En el ámbito de la gestión de infraestructuras de telecomunicaciones solo Cellnex Telecom ha aunado todas esas tecnologías en 2025 y primer trimestre de 2026.

PRIORIDAD DE TECNOLOGÍAS DIGITALES DISRUPTIVAS, POR SU IMPACTO

- **IA agéntica.** Es la tendencia más inmediata, porque ya se está orientando a uso empresarial real: agentes autónomos con capas de gobierno para operar en entornos de negocio. En España, CaixaBank abrió la caja de pandora con "Agentic AI" en el Barcelona MWC 2026, y su potencial para mejorar sus procesos de negocio y la atención al cliente online en su neobanco Imagin y 22 millones de clientes que usan su app CaixaBankNow.
- **Ciberseguridad y digital trust.** En Europa, la combinación de regulación, deepfakes y automatización está empujando soluciones de autenticación, trazabilidad, identidad y verificación de contenidos. La Comisión Europea sigue usando el marco de la AI Act como referencia de cumplimiento, y en España la agenda digital incluye explícitamente, ciberseguridad como una de sus áreas troncales.
- **Robótica y automatización física.** La robótica vuelve con fuerza por la presión de productividad, falta de mano de obra y mejora de la IA

aplicada al mundo físico. En sectores europeos como industria, logística y retail puede ser especialmente disruptiva porque reduce costes operativos de forma directa, como ha demostrado El Corte Inglés en "primicia y vanguardia", tanto en el front-office, para atender al cliente con su "Catálogo Extendido", como en el back-office, con logística, supply chain y uso del Internet de las Cosas (IoT), 5G y soluciones de Industria 4.0.

- **Computación cuántica.** La cuántica es menos inmediata que la IA, pero muy estratégica para España por su valor en optimización, materiales, química, logística y seguridad. En 2026, la narrativa ya no es "si llegará", sino qué industrias empiezan a monetizar casos concretos. IrsiCaixa y CaixaResearch Institute, dos entidades de investigación médica de última generación, pertenecientes a Fundación La Caixa, usan IA y quantum para el desarrollo de vacunas y curas para enfermedades como el cáncer, el sida y, como pudo verse con eficacia, con COVID. La World Health Organization (WHO) reconoció -aunque tarde- a Fundación La Caixa, por ser la primera entidad del mundo en desarrollar, primero, cuidados paliativos y, después, una vacuna eficaz contra COVID en tiempo récord, gracias la combinación de investigación médica tradicional con el uso de inteligencia artificial, quantum y desarrollo de algoritmos propios.
- **Smart glasses y XR.** Las gafas inteligentes serán la nueva interfaz útil para trabajo de campo, asistencia remota, traducción, navegación y productividad. En España se despegarán primero en entornos profesionales y luego en consumo masivo, por su encaje con logística, mantenimiento, salud y retail.
- **Biotecnología y foodtech.** La fermentación de precisión y las proteínas alternativas pueden alterar la cadena alimentaria española y europea, sobre todo por coste, sostenibilidad y seguridad de suministro. No es el fenómeno más visible, pero sí uno de los más estructurales a medio plazo. ■

MÁS INFO +

» Las tecnologías digitales más disruptivas en España

TECNOLOGÍAS DISRUPTIVAS A VIGILAR EN ABRIL DE 2026

Tecnología	¿Qué está cambiando?	¿Por qué importa?
IA agéntica	Agentes que ejecutan tareas y procesos, no solo responden	Puede reducir costes operativos y acelerar workflows.
Robótica	Robots humanoides y de servicio en más entornos	Puede transformar logística, retail y asistencia.
Cuántica	Más pilotaje comercial y cloud quantum	Afecta a optimización, simulación y seguridad.
Smart glasses	Nuevos dispositivos con IA integrada	Podrían redefinir la interacción con software y contenido.
Digital trust	Trazabilidad y verificación de contenido/datos	Se vuelve una necesidad regulatoria y reputacional.
Foodtech	Fermentación de precisión y proteínas alternativas	Puede alterar la industria alimentaria y de ingredientes.

USO Y AFECTACIÓN DE LAS TECNOLOGÍAS DISRUPTIVAS EN SECTORES DE ACTIVIDAD, ESPAÑA, ABRIL 2026

Sector	Tecnologías que más le afectan	Qué cambia
Banca	IA agéntica, digital trust, ciberseguridad, cuántica	Automatización de riesgos, fraude, cumplimiento y atención al cliente.
Telecom	IA agéntica, smart glasses/XR, cuántica, ciberseguridad	Más demanda de conectividad, edge, identidad y servicios empresariales.
Industria	Robótica, IA agéntica, cuántica, ciberseguridad OT	Más automatización, mantenimiento predictivo y control de operaciones.
Medios	Digital trust, IA agéntica, smart glasses	Verificación de contenido, nuevos formatos y automatización editorial.
Retail	IA agéntica, robótica, smart glasses, digital trust	Mejor atención, más automatización y nuevas experiencias en tienda.
Ciberseguridad	IA agéntica, digital trust, cuántica	Más presión regulatoria, más automatización defensiva y nuevos riesgos

NO ESTÁS SOLO ANTE LA TECNOLOGÍA...

¡Participa en los Encuentros de la Comunidad IT!

Un espacio único y de confianza para debatir los retos y las oportunidades de los despliegues tecnológicos en todo tipo de sectores.

Un lugar en el que los líderes de tecnología pueden:
- Compartir conocimiento
- Analizar el estado de las iniciativas tecnológicas
- Fomentar la relación entre compañeros del sector TIC

Si quieres formar parte de nuestros **Encuentros de Comunidad IT**, ponte en contacto con nosotros en el correo eventos@itdmgroup.es

itEVENTS

#ComunidadIT

EL FIN DE UN CICLO... DE FORMACIÓN

LORENZO MARTÍNEZ RODRÍGUEZ
Experto en ciberseguridad

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

A lo largo de nuestras vidas nos preparamos para ser capaces de superar múltiples retos. Desde el colegio, con el instituto, la universidad, los procesos de selección para una posición laboral, las oposiciones para un puesto público... vivimos estudiando, aprendiendo o practicando para ser capaces de desempeñar determinada actividad o mejorar nuestros conocimientos en una u otra materia.

Me ha tocado (y me toca) vivir este tipo de situaciones en las que decenas o centenas de horas de mi dedicación se ponen a prueba y se juegan a una única carta. Quizá el primero, y más duro, sea el examen de selectividad (tengo ya una edad y desconozco cómo se llama esto ahora); la entrevista final para el puesto de trabajo de tu vida; la ratificación en juicio de un informe pericial; la presentación a un cliente de los resultados de una auditoría de ciberseguridad; o la propuesta de servicios profesionales a un cliente al que te ha costado sangre de unicornio y un pacto con el diablo conseguir la oportunidad de tener su contacto... Son algunos de los casos que se me ocurren en los que no vale un resultado a medias.

Es análogo a cuando un piloto de una línea aérea aterriza un avión. No vale aterrizarlo a medias: o aterriza y todo el mundo sale andando por su propio pie, o ese vuelo, lamentablemente, sale en las noticias.

Sin embargo, a veces me toca estar en el otro lado: aquel en el que son otras personas quienes se han preparado profesionalmente para jugárselo todo a esa única carta y yo soy quien tiene que evaluarles.

Empiezo a escribir este artículo desde un aula del CNTG (el Centro de Novas Tecnoloxías de Galicia), en Santiago de Compostela. Estoy vigilando una convocatoria del examen de certificación IRCP (Incident Response Certified Professional), por el que 20 aguerridos profesionales del mundo de la informática me han sufrido durante cerca de tres intensos meses. En ese tiempo he intentado transmitirles, de la mejor manera

que he sabido, todos los años de experiencia que llevo a mis espaldas en el mundo del peritaje informático forense y en la gestión y respuesta ante incidentes de ciberseguridad.

Han sido más de 90 horas puras de clases y entrenamientos 100% prácticos en los que interiorizar los conocimientos adquiridos, así como la metodología que usamos en mi empresa para la resolución de este tipo de incidentes. Pero han sido más de 90 horas. Quienes he logrado entusiasmar y motivar lo suficiente, además, han hecho ejercicios por su cuenta, me han consultado dudas y han profundizado en una materia tan compleja todo lo que han podido. ¿Para qué? Para dos cosas: ser mejores profesionales, capaces de resolver incidentes de seguridad de una forma más eficiente; y jugarse el todo por el todo esta tarde durante ocho largas horas de examen, en las que han de demostrar que efectivamente son aptos para obtener un certificado que no es sencillo de aprobar.

Ahora estoy en el lado cómodo. Les veo las caras y puedo percibir el estado mental de concentración extrema de cada uno. No se oye ni el vuelo de una mosca; solo los teclados de los ordenadores funcionando a pleno rendimiento. El tiempo es suficiente si encaran el incidente por el camino correcto o, como digo yo siempre, si se abre el melón por el sitio más adecuado.

Para que ellos puedan resolver ese ejercicio en ocho horas, yo tengo que haberlo hecho antes en cuatro. Si yo he podido, ellos tienen que poder.

No obstante, el reto es singular. Cuando se ha consumido la mitad de la jornada, las fuerzas empiezan a flaquear. El cansancio empieza a hacer mella en ellos y la frecuencia del parpadeo aumenta. Según pasa el tiempo, la hora se les echa encima y el grado de profundidad en la investigación que demostraban al principio seguramente bajará. Es probable que se olviden de revisar elementos que, en un momento más inicial de la prueba, seguro que no se les habrían pasado.

Son las normas del juego.

El objetivo es precisamente que vivan el estrés de un incidente de seguridad real, en el cual el tiempo y el cansancio acumulado son los mayores enemigos del analista forense. No solo se trata de medir sus conocimientos técnicos y la metodología empleada, sino también su capacidad de documentarlo de una forma que me permita concluir que el candidato ha entendido el incidente, puesto que sabe explicar de manera precisa qué hechos han sucedido siguiendo un orden cronológico.

Y para esto solo disponen de ocho horas, de manera ininterrumpida y presencial, bajo una vigilancia que me garantice que nadie más que cada alumno hace el examen.

Quedan pocos minutos para terminar y las teclas resuenan con una frecuencia aún mayor que antes. Cuando suene “la campana”, deberán enviarlo a una dirección de correo electrónico genérica y, como decían los latinos, alea iacta est. La suerte estará echada, a la espera de que tres evaluadores independientes corrijamos todos los exámenes, previamente anonimizados por un tercero para que no sepamos a quién corresponde lo que ha escrito cada uno y así garantizar que no existen potenciales favoritismos.

Los candidatos terminan. Están extenuados mentalmente. Conozco la sensación. Es mi día a día en Securízame, y más cuando me toca pelearme con un incidente de seguridad, en el que sé cuándo empiezo, pero no cuándo termino.

El cliente necesita volver a trabajar en su empresa tras haber sufrido una intrusión. Necesita un informe técnico, sí. Pero además necesita saber cuál ha sido el punto de entrada, con la finalidad de cerrar el agujero que ha posibilitado el acceso y, sobre todo, la postexplotación. Hasta dónde ha llegado el atacante, cuántas trampas ha dejado y qué mecanismos de persistencia ha creado en la infraestructura: nuevos usuarios, conexiones inversas, tareas programadas que se ejecutarán dentro de un mes y posibilitarán un nuevo acceso, servicios troyanizados cuyo script de arranque ejecuta algo más que un Apache, etc. Y todo esto, ¡para ya!

De eso se trata.

Los alumnos que superen este ejercicio tengo claro, y puedo avalar, que son capaces de meterle mano a un incidente de seguridad. Y que han sido capaces de demostrarlo haciendo diana con el disparo de una sola flecha, tras una larga y extenuante tarde. ■

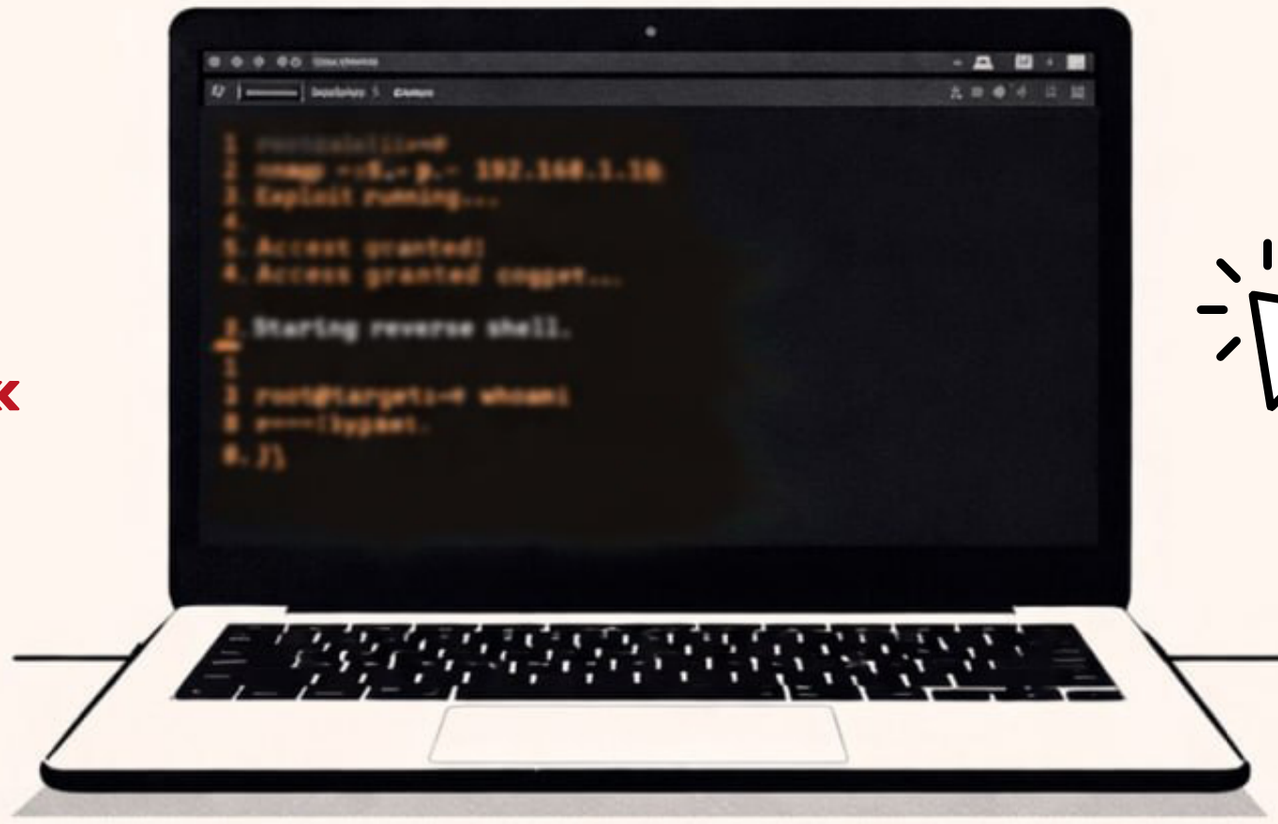
MÁS INFO +

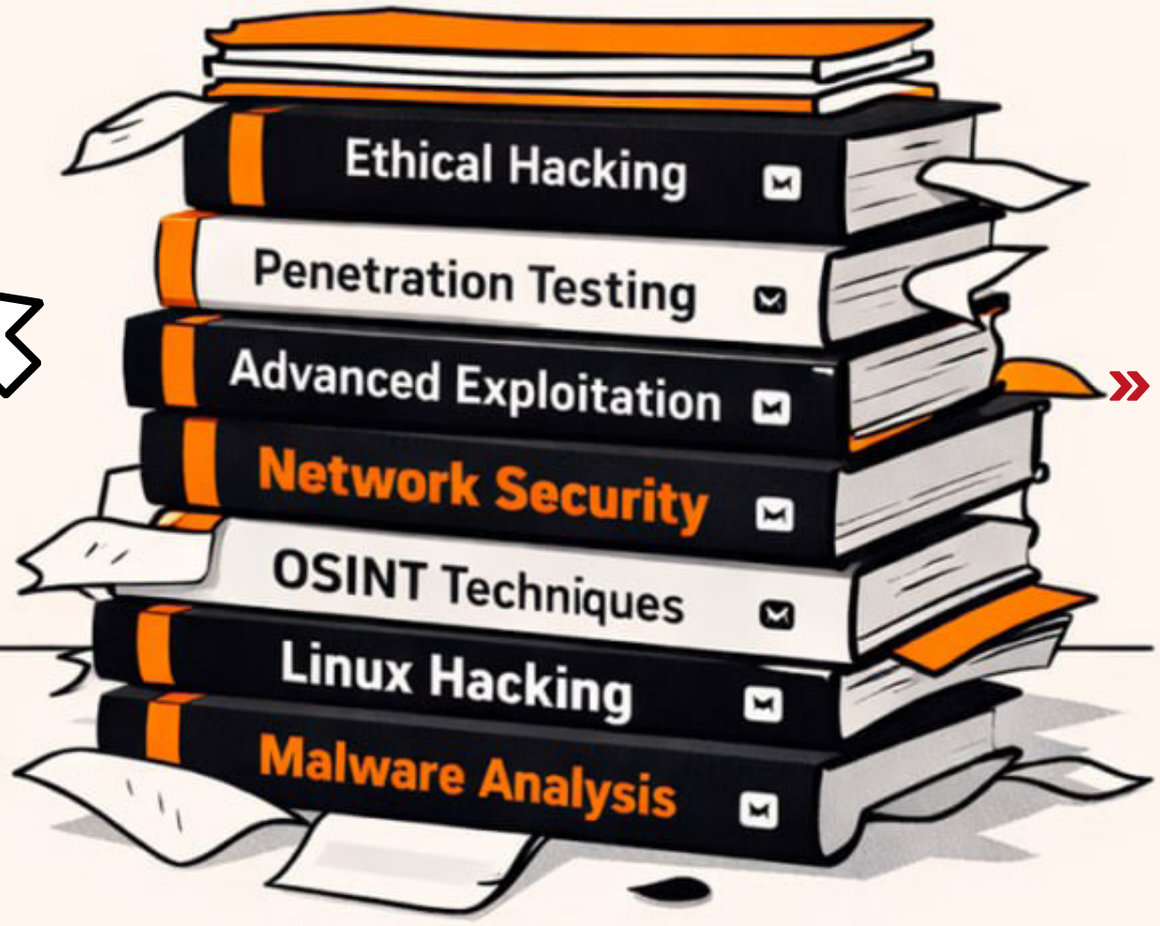
» Hacking ético

SECURIZAME

FORMACIÓN DE HACKING ÉTICO 2026

LO QUE APRENDES AQUÍ LO APLICAS EN EL MUNDO REAL





MÁS PRÁCTICA, MENOS TEORÍA

https://www.securizame.com/hacking-etico

LA AUTONOMÍA FINANCIERA EN EUROPA

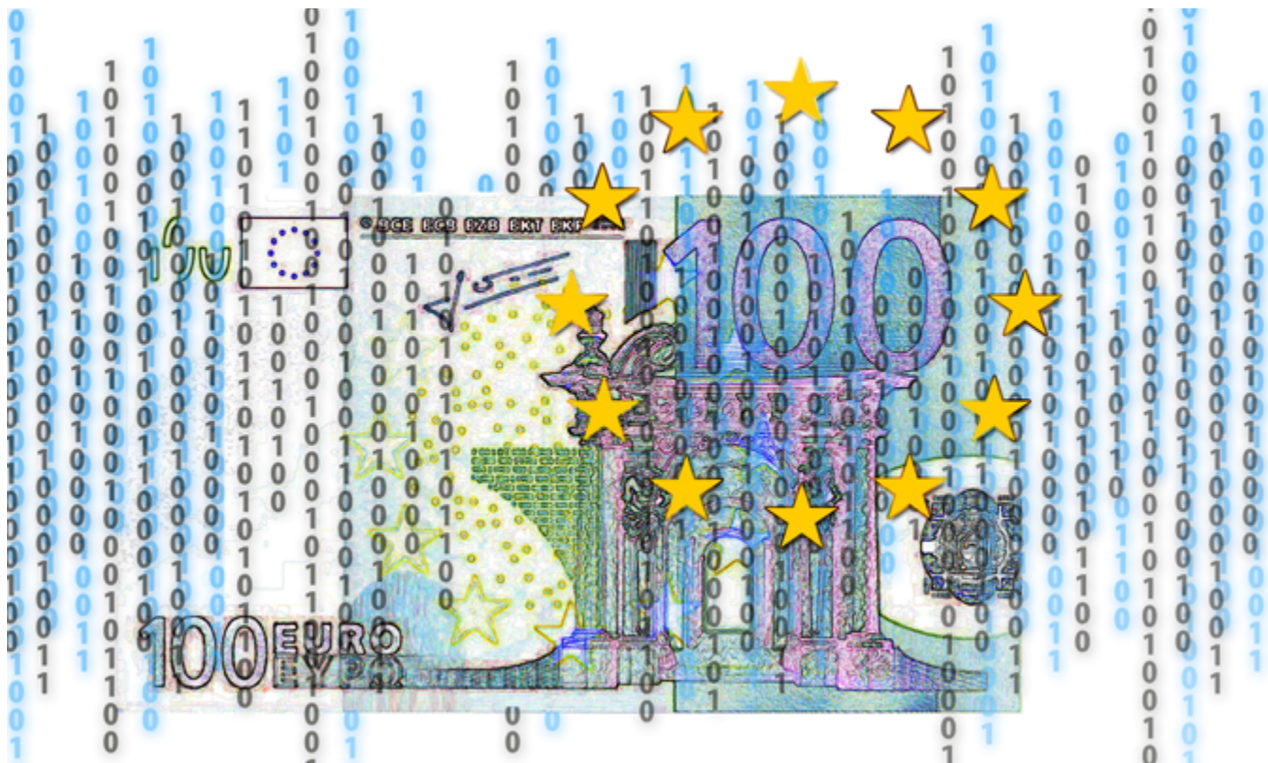
JOSÉ MANUEL NAVARRO
Experto en marketing

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

La situación actual del mercado de pagos en el continente europeo atraviesa un proceso de reconfiguración estructural que va más allá de la simple actualización tecnológica. Nos encontramos en un punto de inflexión donde la geopolítica, la regulación y la innovación tecnológica convergen para intentar devolver al continente una soberanía financiera que se ha visto erosionada durante décadas por la dependencia de infraestructuras externas.

En estos momentos, el panorama se define, más allá de por el volumen transaccional, por quién controla los canales por los que circula el dinero y cómo estos se adaptan a un entorno de inmediatez absoluta y de inteligencia artificial aplicada al consumo. La fragmentación histórica de los sistemas de pago nacionales, que obligaba a los comercios a integrar múltiples soluciones locales para operar de forma transfronteriza, está siendo sustituida, mediante un esfuerzo coordinado, por alternativas paneuropeas capaces de competir con los gigantes globales que actualmente gestionan mayoritariamente el mercado de tarjetas en la eurozona.

Este impulso hacia la soberanía se fundamenta en la necesidad de resiliencia operativa y de adaptación a un mercado que responde con avidez ante nuevas propuestas innovadoras, ágiles y seguras. La excesiva dependencia de proveedores no europeos deja a los usuarios (particulares y empresas) vulnerables ante posibles restricciones motivadas por decisiones políticas ajenas a la Unión Europea. Por ello, las autoridades y el sector privado han alineado sus estrategias para fortalecer una infraestructura compartida, centrada en la interoperabilidad de los pagos inmediatos y el desarrollo de una moneda digital emitida por el Banco Central Europeo. Las expectativas de



los consumidores ya han cambiado en el sentido de que el comercio actual, por ejemplo, no tolera el retraso de varios días para la liquidación de fondos, y demanda experiencias móviles fluidas que funcionen igual de bien en su país de origen como en cualquier otro estado miembro.

La entrada en vigor definitiva del Reglamento de Pagos Instantáneos (IPR) en octubre de 2025 ha perfeccionado la operativa bancaria ya que, lo que comenzó como una opción para transferencias de valor añadido, se ha convertido en la capacidad básica obligatoria para los proveedores de servicios de pago (PSP) en la eurozona. Los pagos instantáneos SEPA (SCT-Inst) permiten liquidar transacciones en menos de diez segundos, ininterrumpidamente, lo que ha transformado la gestión de tesorería empresarial al eliminar la necesidad de mantener grandes colchones de liquidez a corto plazo. La legislación no solo ha forzado la adopción técnica, sino que ha igualado el coste de las transferencias tradicionales, eliminando así las barreras de adopción para el mercado masivo.

Sin embargo, la inmediatez ha traído consigo la necesidad de rediseñar los sistemas de seguridad. En 2025, la verificación del beneficiario (VoP) fue esencial para combatir el fraude de pagos autorizados (APP), obligando a las instituciones a validar la identidad del beneficiario en tiempo real antes de ejecutar el envío. Los bancos han pasado de procesos por lotes a una monitorización continua, donde la inteligencia artificial analiza patrones de comportamiento para detectar anomalías en milisegundos. Esta evolución tecnológica está facilitando que la banca abierta evolucione perfeccionando las finanzas abiertas (Open Finance), permitiendo que los datos financieros se compartan de forma segura para ofrecer servicios hiper-personalizados bajo el marco regulatorio FiDA.

INICIATIVA DE PAGOS EUROPEA

En este contexto de búsqueda de escalabilidad, la Iniciativa de Pagos Europea (EPI) ha consolidado su billetera digital, Wero, como el eje de la interoperabilidad regional. Wero ha superado los 52 millones de usuarios registrados en Francia, Alemania y Bélgica en el primer trimestre de 2026, y se encuentra en pleno proceso de absorción de sistemas nacionales dominantes como iDEAL en los Países Bajos. La firma del memorando de entendimiento en febrero de 2026 entre EPI y la Alianza EuroPA (que integra a Bizum de España, Bancomat de Italia y MB WAY de Portugal) representa un hito sin precedentes, la conexión de 130 millones de usuarios bajo un estándar técnico común. Esta alianza no solo busca facilitar el envío de dinero entre particulares, sino que tiene como objetivo prioritario el comercio electrónico y el punto de venta físico a partir de 2027 (aunque Bizum ya se ha adelantado presentando su modelo de pago instantáneo P2B en comercio físico), utilizando tecnologías como NFC y códigos QR para desafiar la hegemonía de las tarjetas tradicionales.

PROYECTO DEL EURO DIGITAL

En este contexto, el proyecto del euro digital, por su parte, ha superado su fase teórica para entrar en una fase de preparación técnica crítica (ya se ha abierto la convocatoria de manifestaciones de interés para la participación de los PSP en el proyecto piloto del euro digital). El BCE lo ha definido como un complemento digital del efectivo, diseñado para garantizar que el dinero público siga siendo accesible y utilizable en una economía cada vez más digitalizada. A diferencia de las soluciones privadas (criptomonedas), el euro digital gozará de curso legal, lo que garantiza su aceptación

NOS ENCONTRAMOS EN UN PUNTO DE INFLEXIÓN DONDE LA GEOPOLÍTICA, LA REGULACIÓN Y LA INNOVACIÓN TECNOLÓGICA CONVERGEN PARA INTENTAR DEVOLVER AL CONTINENTE UNA SOBERANÍA FINANCIERA QUE SE HA VISTO EROSIONADA DURANTE DÉCADAS POR LA DEPENDENCIA DE INFRAESTRUCTURAS EXTERNAS

universal en toda la eurozona, y se centrará en ofrecer niveles de privacidad equivalentes al efectivo en sus modalidades offline.

La arquitectura del euro digital para 2026 se basa en el "diseño inclusivo", con interfaces adaptadas para personas con discapacidad y ciudadanos con baja alfabetización digital. Uno de los mecanismos más innovadores que se están probando es el denominado "waterfall" que vincula la billetera digital con la cuenta bancaria del usuario para completar pagos incluso si el saldo en euros digitales es insuficiente, evitando así las fricciones de las recargas manuales.

Fase del Proyecto Euro Digital	Objetivos Principales	Cronograma
Conclusión fase de preparación	Definición de infraestructura técnica y selección de proveedores	Octubre 2025
Legislación y estándares	Aprobación del marco legal en el Parlamento Europeo	Durante 2026
Proyecto piloto	Pruebas en entornos reales con comercios y usuarios	Mediados 2027
Emisión potencial	Disponibilidad masiva de la primera versión del euro digital	Durante 2029

A pesar del impulso político, el camino hacia la emisión sigue enfrentando debates sobre los importes límites de tenencia para preservar la estabilidad de los depósitos bancarios. No obstante, el consenso técnico indica que el euro digital actuará como un catalizador para la innovación, permitiendo que las empresas privadas construyan servicios de valor añadido sobre sus estándares abiertos, como pagos condicionales o automatización de suscripciones. La integración de la moneda digital en infraestructuras de registros distribuidos (DLT) a través de iniciativas como "Pontes" reforzará además el papel del dinero de banco central en los mercados financieros mayoristas.

STABLECOINS

Las stablecoins, criptomonedas que han acelerado la decisión de lanzar el euro digital, se han consolidado en 2026 como una infraestructura crítica para los pagos transfronterizos y la gestión de liquidez corporativa. Gracias a la plena aplicación del reglamento MiCA en la Unión Europea, las empresas y bancos cuentan ahora con la claridad jurídica necesaria para emitir y utilizar tokens referenciados al euro. Iniciativas bancarias como Qivalis están permitiendo que la liquidez se mueva en tiempo real, las 24 horas del día, eliminando los costes y retrasos asociados a la banca corresponsal tradicional y los plazos bancarios.

Aunque las stablecoins referenciadas al dólar (como USDT y USDC) siguen dominando el mercado global, el surgimiento de opciones europeas reguladas está empezando a ganar tracción en los corredores B2B. Se estima que, para finales de la década, entre el 10% y el 20% de los pagos internacionales podrían liquidarse mediante estos canales digitales, que ofrecen programabilidad y finalidad inmediata. La integración de estos activos en plataformas de orquestación de pagos permite a los comerciantes optimizar sus flujos financieros de forma adaptativa, seleccionando la vía más eficiente en cada momento.

Una de las predicciones más sólidas para los próximos tres a cinco años es el ascenso del comercio agente. La inteligencia artificial agéntica ha dejado de ser un asistente pasivo para convertirse en un actor autónomo con capacidad de ejecución financiera. Ya estamos viendo la implantación de protocolos como el Agentic Commerce Protocol (ACP) de OpenAI y Stripe, y el Universal Commerce Protocol (UCP)

de Google, que permiten a los agentes de IA buscar, comparar y comprar productos en nombre del usuario sin intervención humana directa.

Esta transformación desplaza el control de la relación con el cliente desde la interfaz de pago hacia la interfaz de búsqueda. Las empresas de pagos ya no compiten solo por ser elegidas en el "checkout", sino por ser el canal preferido por el agente de IA, basándose en criterios de coste, velocidad y riesgo. Para los bancos, esto supone un reto de gobernanza masivo: el concepto tradicional de "conozca a su cliente" (KYC/KYB) debe expandirse al de "conozca a su agente" (KYA), estableciendo límites de delegación acotada para asegurar que los agentes operen dentro de mandatos específicos de gasto y seguridad.

NUEVA OLA DE PRODUCTIVIDAD

La adopción de estas tecnologías generará una nueva ola de productividad en la industria, estimada por McKinsey en hasta 110.000 millones de dólares anuales, gracias a la automatización de operaciones de IT, desarrollo de productos y atención al cliente. Sin embargo, los comerciantes deberán adaptar sus catálogos para que sean legibles por máquinas, priorizando los datos estructurados sobre el marketing visual tradicional para no quedar invisibles en las rutas de compra iniciadas por IA.

Como consecuencia, la industrialización del fraude mediante IA y deepfakes representa el mayor desafío operativo para el ecosistema de pagos en 2026. Las pérdidas por fraude financiero proyectan un crecimiento del 153% para 2030, alcanzando los 58.300 millones de dólares a nivel global. Los delincuentes operan ahora bajo modelos de "Fraude como Servicio" (FaaS), utilizando identidades sintéticas o "Frankenstein" que mezclan datos reales y ficticios para eludir los controles de identidad estáticos.

La respuesta legislativa europea se articula a través de la PSD3 y el Reglamento de Servicios de Pago (PSR), que redefinen la responsabilidad en casos de estafas de suplantación de identidad. A partir de 2026, la carga de la prueba y la responsabilidad financiera se desplazan significativamente hacia los PSP que no implementen controles preventivos robustos, como la concordancia obligatoria entre el nombre del beneficiario e IBAN para todas las transferencias en la UE.

Además, el marco normativo (resumido a continuación) busca fomentar la competitividad permitiendo que instituciones de pago y de dinero electrónico accedan directamente a los sistemas de liquidación, rompiendo el monopolio histórico de las entidades de crédito. Esta apertura, combinada con la transparencia exigida en las comisiones de cambio de divisas y el acceso al efectivo en comercios sin necesidad de compra (cashback), configura un mercado más orientado al usuario y menos dependiente de los márgenes de intermediación tradicionales.

Elemento Clave PSD3/PSR	Impacto en el Mercado de Pagos	Fecha Aplicación Prevista
Armonización vía PSR	Reglas de conducta aplicables en toda la UE	Entrada en vigor Q2 2026
Responsabilidad en fraude	Reembolso obligatorio al cliente en estafas de suplantación	18-24 meses tras su publicación
Acceso a sistemas de pago	PSP y EDE podrán acceder directamente	Plena operatividad en 2028
Mejora de API	Obligatoriedad de interfaces de banca abierta sin fricciones	Supervisión continua desde 2026

ESTE IMPULSO HACIA LA SOBERANÍA SE FUNDAMENTA EN LA NECESIDAD DE RESILIENCIA OPERATIVA Y DE ADAPTACIÓN A UN MERCADO QUE RESPONDE CON AVIDEZ ANTE NUEVAS PROPUESTAS INNOVADORAS, ÁGILES Y SEGURAS

El análisis detallado de las fuerzas que moldean el mercado europeo de pagos permite predecir un escenario de convergencia tecnológica y estratégica en los próximos cinco años. La era en la que la escala genérica y el volumen transaccional eran los únicos motores de rentabilidad ha llegado a su fin. La presión sobre los márgenes y el encarecimiento de los costes de cumplimiento obligan a los actores del mercado a buscar valor en la especialización vertical y en los servicios añadidos integrados en el pago.

En los próximos años se consolidará definitivamente el pago de cuenta a cuenta (A2A) como opción preferente en el comercio electrónico europeo, impulsado por la madurez de Wero y la interoperabilidad de las billeteras nacionales. A medio plazo (tres a cinco años) el mercado evolucionará hacia un entorno más rápido, interoperable y exigente en cumplimiento, donde los pagos instantáneos dejarán de ser un nicho para convertirse en infraestructura base. En este contexto, el euro digital no solo funcionará como instrumento de pago, sino como referencia pública en términos de estabilidad y privacidad, forzando al sector privado a redefinir su propuesta de valor.

Las tarjetas no desaparecerán; seguirán siendo relevantes por hábito, aceptación y cobertura, pero perderán parte de su exclusividad funcional a medida que las transferencias inmediatas y las carteras digitales ganen peso en el uso cotidiano. La transformación no vendrá por la sustitución de un medio por otro, sino por la reducción estructural de la fricción en el proceso de pago. En paralelo, la soberanía de pagos impondrá su carácter estratégico, lo que no implica excluir actores globales, sino evitar la dependencia total en el control de la experiencia de usuario. La clave no reside en una solución única, sino en una arquitectura propia, interoperable y resiliente que combine pagos instantáneos como base operativa y, potencialmente, el euro digital como ancla de soberanía monetaria.

En este nuevo equilibrio, la competencia se desplazará hacia la interfaz del cliente, que tenderá a integrarse en ecosistemas de inteligencia artificial. Las entidades deben posicionarse como infraestructura de confianza para agentes autónomos para ser las que capturen mayor valor en la cadena digital.

El resultado es un modelo de pagos europeo definido por tres vectores: soberanía, inmediatez y autonomía. E inteligencia. ■

MÁS INFO +

- FiDA
- Pontes
- Qivalis
- Universal Commerce Protocol (UCP) de Google

DANIEL PÉREZ LIMA
CIO & CISO de Genomcore

in

CIO y CISO con amplia experiencia práctica, orientado a resultados y en liderar gobernanza de seguridad, gestión de riesgos y operaciones de TI en empresas y multinacionales, especialmente sector industrial y healthcare. Experto en alinear estrategias de TI y ciberseguridad con los objetivos empresariales y marcos de cumplimiento (ISO, ENS, NIST, CMMC, PCI DSS...), asegurando una prestación de servicios de TI resiliente, eficiente y segura. Cuenta con certificaciones CISSP, CISM, CompTIA Security+, COBIT e ITIL, entre otras

Cómo defenderse ante ataques contra la identidad (I)

CÓMO PROTEGER LA EMPRESA EN ENTORNOS HÍBRIDOS (ACCESOS EN LA NUBE / SAAS) – REGISTRO DE DISPOSITIVOS

Tradicionalmente se ha establecido que la red empresarial se puede proteger detrás de unos firewalls perimetrales: confío en lo que está dentro, me protejo de lo que está fuera.

Si bien esta configuración tradicional puede ser válida en muchas empresas, lo que está claro es que ya no es suficiente. El modo de trabajo híbrido actual, donde muchos de los recursos están en la nube y los trabajadores cuentan con mucha movilidad, convierte la identidad en el "nuevo perímetro", frase que cada vez se oye con más fuerza en los foros y eventos de ciberseguridad.

Por un lado, obviamente, tenemos la protección MFA, la cual es totalmente imprescindible hoy en día. Aún tenemos empresas que siguen haciendo excepciones a esta regla por motivos clásicos como resistencia el cambio o problemas de configuración, pero es algo que poco a poco se está consiguiendo revertir para asegurar que el 100% de las cuentas de la empresa estén protegidas por MFA.

Pero, aun con MFA, sigue habiendo peligros que están muy activos y presentes, que pueden sortear MFA sin ningún problema:

- **Fuga de credenciales.** Usuarios que facilitan sus credenciales al caer en phishing o ingeniería social.
- **Phishing avanzado (Adversary-in-the-Middle).** Los atacan-

tes pueden robar credenciales y tokens válidos.

- **Robo de tokens de sesión.** Un token robado permite acceso sin contraseña ni MFA.
- **MFA Fatigue – Abuso de MFA.** Se provoca una aceptación de login por MFA por insistencia o desconocimiento por parte del usuario.
- **Acceso desde dispositivos personales o comprometidos.** Aunque el usuario sea legítimo, el dispositivo puede no serlo.

Eso lleva a pensar en una nueva estrategia de protección: ya no puedo confiar únicamente en lo que tengo “dentro”, y “debo” confiar también en lo que “está fuera”.

¿Cómo lo hago? La seguridad moderna exige verificar quién accede y desde qué dispositivo, y en esta tribuna exploraremos una de las mejores soluciones para mitigar este riesgo: el registro de dispositivos.

¿QUÉ ES EL REGISTRO DE DISPOSITIVOS?

El registro de dispositivos implica establecer políticas de configuración que permitan reconocer un dispositivo como corporate/corporativo, y, de este modo, poder aplicar un acceso condicional basado en si se reconoce el dispositivo como propio o no.

Si es posible reconocer un dispositivo como propio, puedes prohibir el acceso de los recursos corporativos a cualquier otro dispositivo, y, por tanto, establecer una línea de defensa ante los riesgos anteriormente descritos. Gracias al registro de dispositivo podemos:

- Identificarlo de forma única.
- Aplicar políticas condicionales basadas en el dispositivo.
- Verificar su estado de seguridad.
- Aplicar políticas de protección.
- Aplicar políticas de compliance.
- Revocar acceso si se pierde o compromete.

Un dispositivo registrado es un dispositivo bajo control.

ACCESO CONDICIONAL

El acceso condicional son las políticas que permiten establecer reglas para:

- Solo permitir el acceso si el dispositivo está registrado.
- Bloquear el acceso desde navegadores no gestionados.
- Exigir el cumplimiento de políticas de seguridad.
- Denegar el acceso desde dispositivos no corporativos.

Esto significa que aunque un atacante robe credenciales o un token, no podrá acceder sin un dispositivo autorizado. Dicho de otro modo, aunque tengas una fuga de credenciales porque alguien caiga en un phishing, el atacante no podrá hacer login porque proviene de un dispositivo no corporativo/registrado.

No basta con saber quién accede; también importa desde qué dispositivo lo hace.

CONCLUSIÓN

Registrar los dispositivos y aplicar políticas de acceso condicional permite garantizar que solo equipos corporativos, seguros y gestionados puedan acceder a información crítica, incluso si las credenciales han sido comprometidas.

En un escenario donde los ataques a la identidad son inevitables, la verificación del dispositivo es la barrera que marca la diferencia entre un incidente contenido y una brecha grave. Este enfoque reduce drásticamente el riesgo de accesos no autorizados y elimina la posibilidad de que un atacante utilice credenciales robadas desde un dispositivo no confiable.

Registrar dispositivos y aplicar acceso condicional no es solo una buena práctica: es una necesidad estratégica para cualquier organización moderna. ■

MÁS INFO +

» El riesgo de las todopoderosas identidades digitales

La documentación TIC, a un solo clic

Navegue por el “desordenado medio” de la transformación impulsada por IA

Este documento ofrece una visión honesta y basada en datos sobre cómo están afrontando las empresas esta etapa clave de la adopción de la IA. Descubrirás por qué la IA no solo acelera tareas, sino que transforma flujos de trabajo completos, exige nuevas habilidades, etc.

Guía práctica para transformar la gestión de la información en tu empresa

La información es uno de los activos más valiosos de cualquier empresa, y también uno de los más difíciles de gestionar. Documentos dispersos, procesos manuales, riesgos de cumplimiento normativo y falta de visibilidad son desafíos habituales que impactan directamente en la productividad, los costes y la toma de decisiones.

Cómo anticipar los ciberataques del mañana con Inteligencia Contextual de Amenazas

El panorama de amenazas evoluciona a un ritmo que supera la capacidad de respuesta de muchas organizaciones. Los atacantes innovan constantemente, automatizan sus campañas y perfeccionan sus tácticas para evadir las defensas tradicionales. Este whitepaper explica cómo la Inteligencia Contextual de Amenazas permite transformar señales fragmentadas en conocimiento accionable para anticipar ataques antes de que se produzcan.

Perspectivas de inversión en TI y tendencias tecnológicas para 2026

Advice Strategic Consultants ofrece en este informe un análisis del comportamiento del mercado tecnológico y las previsiones de inversión y demandas tecnológicas de las empresas. Descarga ahora este documento y conoce, con una mirada amplia, qué está sucediendo en el mercado tecnológico y qué deparará el próximo año.