it Digital MAGAZINE

Nº 29 · JULIO 2025

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

ZERO TRUST: CUANDO LA DESCONFIANZA ES LA CLAVE DE LA PROTECCIÓN

APOSTANDO POR UNA ESTRATEGIA DE DATOS INTELIGENTE

TENDENCIAS DE CIBERSEGURIDAD EN EL CANAL MAYORISTA

DEFINIENDO LA SEGURIDAD EN 2025

NUTANIX CONGREGA AL CANAL CLOUD EN SU MSP DAY

#CONTENIDOS

ZERO TRUST: CUANDO LA DESCONFIANZA ES LA CLAVE DE LA PROTECCIÓN

DEBATE IT

Tendencias de ciberseguridad en el canal mayorista

Definiendo la seguridad en 2025

ÍNDICE DE ANUNCIANTES

it Digital MAGAZINE

Nº 29 · JULIO 2025

ACTUALIDAD

REVISTA DIGITAL

NO SOLO IT

PUESTO de trabajo SEGURO

esprinet

¿Qué incluye la solución completa que te ofrecemos si eres agente digitalizador?

Esprinet y Microsoft te proporcionan **"materiales de marketing"** para que lances la campaña de Puesto de Trabajo Seguro del Kit Digital a tus clientes.

Configuración inicial

Protección de dispositivos

Justificación
1ª fase

Antivirus, formación
y soporte 24×7

Justificación
2ª fase

Acompañamiento
auditorias

Línea Exclusiva Kit Digital: 976 97 15 05 | kitdigital@esprinet.com

Financiado por la Unión Europea NextGenerationEU

DES 2025 IMPULSA LA TRANSFORMACIÓN INTELIGENTE DE LAS EMPRESAS Y EL SECTOR PÚBLICO

La inteligencia artificial, la computación cuántica, la ciberseguridad y la transformación digital de sectores como las Administraciones Públicas o el Retail han sido los puntos clave de la pasada edición del Digital Enterprise Show 2025. Este congreso, que ha vuelto a superar el éxito del año anterior, ha ido ganando relevancia hasta convertirse en uno de los principales eventos tecnológicos del país, y en un importante motor de digitalización para las empresas de la región.

RICARDO GÓMEZ (MÁLAGA)

Entre los días 10 y 12 de junio se celebró en Málaga el Digital Enterprise Show 2025 es, un evento en el que se dieron cita numerosas empresas y profesionales relacionados con la tecnología para compartir conocimientos y experiencias, y seguir incentivando la transformación digital del ecosistema empresarial español. Bajo el lema 'El éxito empresarial impulsado por IA', la organización ha ofrecido un

amplio abanico de contenidos enfocados a impulsar la transformación de las empresas y el sector público a través de las nuevas tecnologías.

Esta fórmula ha sentado las bases para cosechar un éxito mayor que en las tres ediciones anteriores celebradas en Málaga, logrando convocar a 17.639 directivos de compañías de 36 países y generando un impacto económico de más de 30 millones de euros para la ciudad. Además, la organización señalaba especialmente que han participado 612 expertos en el Digital Business Congress y que en estos tres días se han presentado 681 innovaciones de la mano de 408 empresas tecnológicas. Francisco de la Torre, alcalde de Málaga, ha destacado en el acto de clausura la importancia de la colaboración público-privada para seguir desarrollando el DES, y señaló que este tipo de foros "nos ponen en el mapa y nos ayudan a tejer alianzas entre mercados como el europeo con Asia o Estados Unidos, con una competitividad sana en materia tecnológica".

TRANSFORMACIÓN A TRAVÉS DE LA TECNOLOGÍA

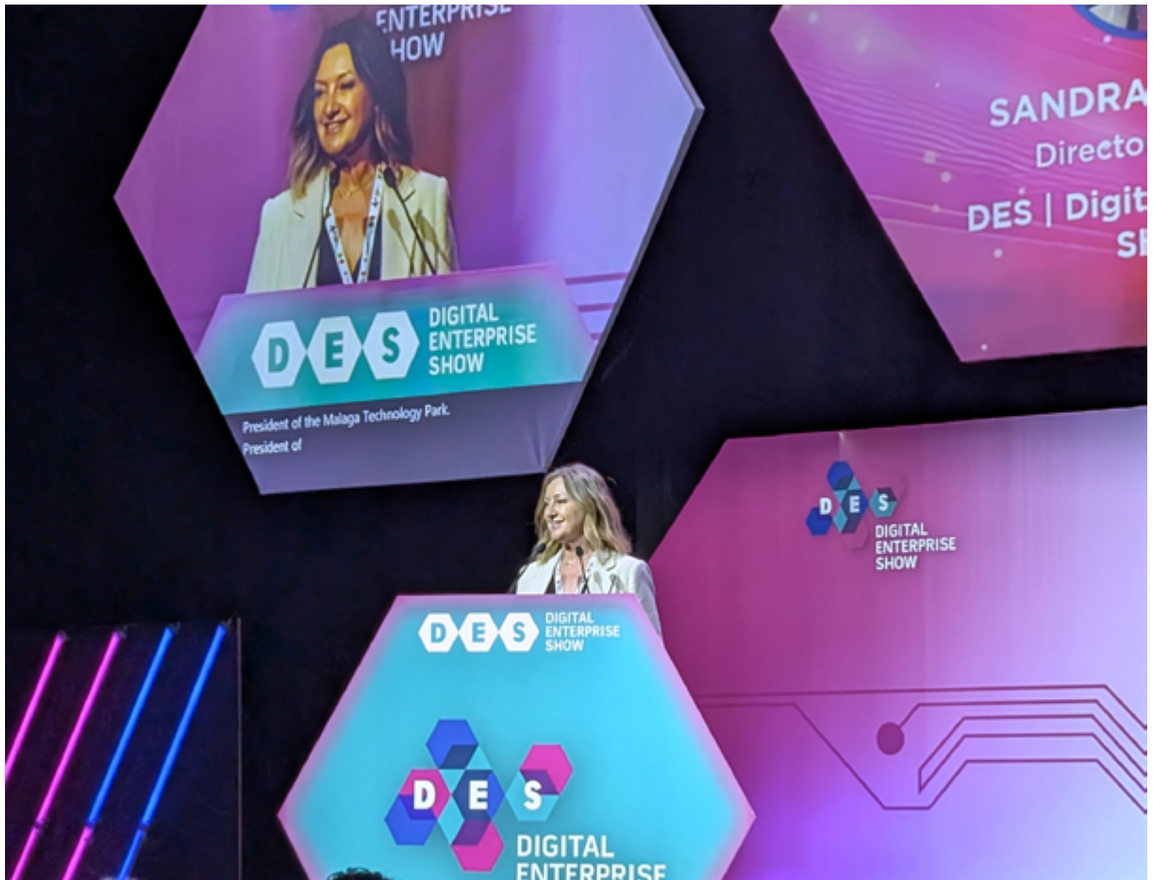
El programa del DES 2025 ha contado con numerosas conferencias, charlas, debates y talleres, distribuidos por áreas temáticas, en las que se han dado cita gran cantidad de profesionales de la industria para compartir su visión y su experiencia sobre temas como las nuevas tecnologías basadas en la inteligencia artificial, la computación cuántica, la ciberseguridad y la transformación digital de las Administraciones Públicas, y de sectores como el Retail.

En una entrevista realizada durante el segundo día del evento, Sandra Infante, directora del DES, nos comentaba que "todos los participantes nos están trasladando buenas sensaciones, se sienten satisfechos con el perfil de los asistentes y el contenido del congreso y consideran que les está aportando muchísimo valor". Señalaba que "para nosotros esto es lo más importante, que los participantes puedan interconectarse para generar nuevas oportunidades de negocio, de conexión para nuevos proyectos, que es al final lo que queremos ofrecer en el DES".

> "LO MÁS IMPORTANTE EN DES ES QUE LOS PARTICIPANTES PUEDAN INTERCONECTARSE PARA GENERAR NUEVAS OPORTUNIDADES DE NEGOCIO"
>
> **SANDRA INFANTE,** directora del **DES**

LA IA COMO MOTOR DE MODERNIZACIÓN

La inteligencia artificial tiene un gran potencial transformador para las empresas y ha tenido un papel clave en DES 2025, estando presente en muchas de las conferencias y debates como factor clave para mejorar los procesos en las organizaciones. Como explicaba Sandra Infante, "la inteligencia artificial es tema recurrente en los últimos años, y el reto está en entender cómo podemos cada uno de nosotros, en nuestra organización, en nuestra industria, utilizar esta tecnología". Destacaba, además, que "la gran ventaja del DES es que, a través de nuestro programa de conferencias, somos capaces de explicar las diferentes



formas en que se puede aplicar la inteligencia artificial" y cómo poco a poco está ampliando sus capacidades y su alcance.

A lo largo del DES se ha hablado mucho de las distintas variantes de IA y de su rápido desarrollo y, según Sandra Infante, "hemos de entender que esto viene para quedarse y que el reto es cómo integrarlo en las organizaciones para no perder palancas de competitividad y cómo usamos esta IA a nivel personal". Destacaba "cómo la administración pública también ha de hacerse cargo de esos desarrollos de tecnología para transformar los procesos de atención a la ciudadanía y también el ecosistema empresarial", y que en DES 2025 las organizaciones han acudido precisamente para contar cuáles son sus necesidades, qué están haciendo en el ámbito digital, en qué casos de uso están aplicando la tecnología y cuáles son los principales retos a los que se enfrentan en esta transformación.

USO RESPONSABLE DE LA TECNOLOGÍA

Otro de los temas clave que se han tratado en el DES 2025, totalmente transversal en cuanto a la digitalización, es la necesidad de hacer un uso responsable de la tecnología para beneficiar tanto a las industrias como a la sociedad en su conjunto, apoyándose en valores fundamentales como la transparencia o la ética. En este sentido, Margaret Mitchell, fundadora del departamento de Ética de Google, ahora directora de ética de Hugging Face, comentó que "en el contexto empresarial, necesitamos aplicar una normativa que defina los valores que nos ayudarán a tomar decisiones", pero que hay que tener cuidado a la hora de determinar quién aporta estos valores.

Clica en la imagen para ver la galería completa

Por ello, muchos expertos abogan por construir un marco regulatorio que guíe la evolución de la IA y proteja los derechos de las personas sin minar el avance digital. Ceyhun Necati, counsel del despacho de abogados internacional Linklaters, recalcó el liderazgo de la Unión Europea como "pionera en la regulación y perspectivas legales de la IA", y aconsejó seguir las pautas de estas legislaciones a la hora de abordar los proyectos de inteligencia artificial.

TRANSFORMACIÓN DEL SECTOR PÚBLICO

Otro de los temas clave del DES 2025 es la digitalización del sector público, que ocupó un lugar especial el tercer día del congreso, a través del Foro Modernización de las Administraciones Públicas, en el que participaron representantes de diferentes Comunidades Autónomas, diputaciones y ayuntamientos para

DES 2025, EN CIFRAS

>> **17.639** directivos de **36** países asistieron al evento
>> **612** expertos participaron en el congreso
>> Se presentaron **681** innovaciones de **408** empresas
>> Impacto económico de más de **30** millones de euros

tratar de impulsar la modernización del sector. Por ejemplo, Aleida Alcaide, directora general de IA del Ministerio de Transformación Digital y de la Función Pública, quien destacó cómo el anteproyecto de ley nacional pretende adaptar a la legislación española el Reglamento Europeo de IA, centrando su enfoque en la prevención, la transparencia y el acompañamiento a empresas y ciudadanos.

Por su parte, Óscar López, ministro para la Transformación Digital y de la Función Pública, anunció en la sesión inaugural una inversión de 16.000 millones de euros en la Sociedad Española para la Transformación Tecnológica (SETT), que se destinarán a "operaciones tecnológicas pioneras y palpables"; la adjudicación del diseño para el nuevo centro de investigación y producción de semiconductores que se construirá en Málaga, bajo el sello de IMEC; la aprobación del Plan de Impulso de Espacios de Datos Sectoriales, que contará con más de 500 millones de euros para apoyar al sector privado y las Administraciones Públicas; y el lanzamiento después del verano del kit Espacios de Datos, enfocado a impulsar la digitalización de las pymes. ■

MÁS INFO +

» DES 2025 consolida su éxito en la ciudad de Málaga

» DES 2025 pone el foco en el futuro de la IA

COMPARTIR EN REDES SOCIALES

AVANCES EN COMPUTACIÓN CUÁNTICA

Uno de los temas clave en DES 2025 ha sido el creciente interés por la computación cuántica, algo que se ha dejado sentir en numerosas presentaciones y charlas, cuyos protagonistas han coincidido en la necesidad de reforzar la colaboración público-privada para acelerar el desarrollo de este nuevo paradigma de la informática, enfocándolo en aportar beneficios a la sociedad y la economía. Por ejemplo, Andrés Gómez, administrador de aplicaciones y proyectos de Galicia Supercomputing Center, quien señaló en su intervención durante el congreso que "la administración debe explorar qué problemas tiene y si la computación cuántica puede ser la solución para problemáticas como los fraudes o la planificación del tráfico". O José Luis Bezares, subdirector general de Ciberseguridad de la Secretaría de Estado de Digitalización e Inteligencia Artificial, para quien "las tecnologías cuánticas y las sinergias que se puedan crear no son solo una cuestión del futuro, sino una oportunidad del mercado y una innovación comercial para hoy".

NUTANIX CONGREGA A LOS LÍDERES DEL CANAL CLOUD EN SU MSP DAY

En un encuentro en Madrid, la compañía ha presentado Nutanix Elevate Service Provider Program, su programa para Proveedores de Servicios Gestionados, detallando su funcionalidad en diferentes casos de uso y explicando la propuesta de valor de la plataforma de nube híbrida de Nutanix.

RAFA CLAUDÍN (MADRID)

Nutanix logró reunir a decenas de líderes del canal cloud en su MSP Day, una jornada en la que la compañía detalló su estrategia para Proveedores de Servicios Gestionados (MSP), un segmento en el que espera un amplio crecimiento, gracias a la capacidad de su plataforma para la nube híbrida y la fortaleza de sus alianzas, entre las que destacaron las de OVHcloud, Acronis, Cohesity, Commvault, Lenovo, Veeam y Virtual Cable.

Jorge Vázquez, director general de Nutanix para España y Portugal, abrió el evento explicando que el segmento MSP se ha convertido en una línea estratégica para Nutanix. “Los negocios ven la nube como un acelerador de crecimiento. El 78% de los CxO ven la nube como una capacidad de acelerar su go-to-market. Un 87% ve que cuando sacan algún servicio apoyado en la nube mitiga mucho los riesgos. Además, el mundo híbrido tiene que seguir funcionando. El 75% de las empresas grandes y medianas mueven en alguna medida sus cargas al cloud; el 81% no eligen una sola nube, sino que buscan tener una infraestructura distribuida en diferentes nubes”.

NUTANIX ELEVATE SERVICE PROVIDER

La estrategia MSP de Nutanix está liderada por Álvaro Jerez, recientemente incorporado a la compañía como MSP manager Iberia. El directivo explicó el modo en que Nutanix lleva las ventajas de la nube pública a la privada, entre las que destacó la escalabilidad horizontal; la hiperconvergencia; la automatización y la orquestación; la resiliencia y la tolerancia a fallos; el modelo basado en software; el pago por uso; la agilidad; y la experiencia similar a la nube pública.

Álvaro Jerez partió de una cita de Rajiv Ramaswami, CEO de Nutanix, quien comentó en una reciente entrevista que los servicios representaban menos del 10% de su revenue, para explicar la “apuesta por relanzar este negocio: invertimos en programas de canal, en tecnología, en licenciamiento y comercialización”. Un fortalecimiento de su estructura de apoyo a partners, con un incremento de los recursos dedicados en el terreno y centralizados para MSP y con la adaptación de su plataforma para entornos multi-tenant.

Nutanix Elevate Service Provider es el programa que estructura la propuesta de la compañía para los Proveedores de Servicios Gestionados. Las claves del programa son el licenciamiento flexible, con consumo por OPEX, mensual y con posibilidad de escalabilidad, los servicios gestionados desde una sola plataforma multicliente, la unificación de on-prem y nube pública en la plataforma de nube híbrida de Nutanix y el enfoque multi-tenant, todo ello respondiendo a las necesidades reales de los clientes.

> “HAY QUE ENCONTRAR EL BALANCE DE RENDIMIENTO, SEGURIDAD, COMPLIANCE Y COSTE”
>
> **JORGE VÁZQUEZ**
> director general de **Nutanix** para España y Portugal

UNA ALTERNATIVA REAL A VMWARE

Una cuestión que sobrevoló toda la jornada fue la oportunidad surgida tras los cambios en VMware. Como es sabido, tras la adquisición por parte de Broadcom, sus políticas de precios han sufrido ciertos vaivenes. Nutanix se propone como una alternativa real a VMware, hasta el punto de que lanzó el programa Surge para recompensar a las organizaciones que apostaran por la migración a su plataforma.

De hecho, Sean Torres, senior systems engineer de Nutanix, dedicó una parte de su exposición a explicar cómo se lleva a cabo en la práctica la migración desde VMware a la plataforma de la compañía. El experto detalló el modelo de operación simplificado que propone Nutanix, teniendo en cuenta que “cuanto más sencillo sea el sistema, es más escalable y predecible”.

A lo largo de la jornada se fueron desgranando los diferentes casos de uso con los que trabaja Nutanix, desde la Infraestructura como Servicio (IaaS) y la Plataforma como Servicio (PaaS) hasta el Backup como Servicio (BaaS), Recuperación ante Desastres como Servicio (DRaaS) o las Bases de Datos como Servicio (DBaaS). Pero fue OVHcloud quien explicó en primer plano cómo trabaja con Nutanix.

LAS ESTRECHAS ALIANZAS SECTORIALES

Fernando Ramos, presales engineer de la francesa OVHcloud, detalló cómo su compañía, el primer hiperescalar europeo, ofrece servicios con Nutanix. Y lo hace en dos sabores, con un servicio que incluye el paquete completo o con un modo BYOL (Bring Your Own Licence). La propuesta combina las licencias de software de Nutanix Cloud Platform con la infraestructura de nube privada de OVHcloud certificada por Nutanix.

La jornada se cerró con dos mesas redondas, moderadas por Arancha Asenjo, periodista tecnológica de ITDM Group. La primera se centró en la confianza digital y la protección de los entornos híbridos, y contó con Fernando Feliu, executive

managing director en Virtual Cable, Santiago Sánchez Taboada, senior sales engineer en Cohesity, y Marta San Millán, partner business manager en Commvault.

En la segunda, Alexandre Bento, general manager Iberia ISG de Lenovo, Ángel Martinez, regional alliance sales manager en Veeam, y Aitor González, business development specialist en Acronis, se centraron en la búsqueda de eficiencias, la virtualización y las infraestructuras convergentes. La sencillez de despliegue y de operación y el alto nivel de integración han convertido a Nutanix en un partner crítico para todos ellos. ■

Álvaro Jerez, MSP manager Iberia de Nutanix.

Sean Torres, senior systems engineer de Nutanix.

Fernando Ramos, presales engineer de OVHcloud.

MÁS INFO +

- Nutanix Elevate Service Provider
- Nutanix presenta en .NEXT 2025 su estrategia en entornos híbridos multicloud e IA empresarial

COMPARTIR EN REDES SOCIALES

Arancha Asenjo (ITDM Group), Santiago Sánchez Taboada (Cohesity), Marta San Millán (Commvault) y Fernando Feliu (Virtual Cable).

Arancha Asenjo (ITDM Group), Alexandre Bento (Lenovo), Ángel Martinez (Veeam) y Aitor González (Acronis).

BITDEFENDER REDEFINE LA SEGURIDAD DEL ENDPOINT CON GRAVITYZONE PHASR

Bitdefender ha anunciado el lanzamiento de GravityZone PHASR (Proactive Hardening and Attack Surface Reduction), una nueva solución de seguridad para endpoints que representa un cambio significativo en la forma en que se reduce la superficie de ataque en entornos corporativos, según nos ha explicado Luis Fisas, regional director South Europe de la compañía.

MIGUEL ÁNGEL GÓMEZ

Bitdefender GravityZone PHASR introduce un enfoque dinámico y personalizado, ajustando continuamente las configuraciones de seguridad en función del comportamiento y los privilegios de cada usuario.

UN PROBLEMA CRÍTICO DE CIBERSEGURIDAD

El producto aborda un problema crítico en ciberseguridad: más del 70% de los incidentes graves incluyen el uso de herramientas legítimas y técnicas LOTL (Living-Off-the-Land), que permiten a los atacantes operar sin desplegar malware. PHASR está diseñado específicamente para frenar este tipo de ataques al controlar con precisión el acceso a utilidades como PowerShell y WMIC, deteniéndolos en sus fases iniciales.

GravityZone PHASR analiza el comportamiento de cada usuario —incluyendo cómo usan aplicaciones, acceden a recursos y qué privilegios tienen— y restringe dinámicamente el acceso a herramientas o capacidades que no estén alineadas con su perfil habitual. Este análisis se apoya en técnicas de inteligencia artificial y aprendizaje automático, integradas en la plataforma GravityZone XDR, per-

"ES ESENCIAL EN CIBERSEGURIDAD REDUCIR LA SUPERFICIE DE ATAQUE", LUIS FISAS, BITDEFENDER

mitiendo una evaluación profunda de vulnerabilidades y vectores de ataque.

Según Andrei Florescu, presidente del área empresarial de Bitdefender, “esta innovación resuelve problemas reales sin añadir complejidad, al aplicar controles personalizados que refuerzan la seguridad sin afectar la productividad”.

PRINCIPALES BENEFICIOS DE GRAVITYZONE PHASR

Los principales beneficios de GravityZone PHASR incluyen:

- Adapta dinámicamente la seguridad a cada usuario, según su comportamiento y privilegios.
- Reducción continua de la superficie de ataque al ajustar automáticamente políticas de seguridad conforme evolucionan amenazas y roles.
- Detección y bloqueo proactivo de ataques LOTL, responsables del 70% de los incidentes, mediante la restricción de herramientas legítimas como PowerShell y WMIC.
- Defensas personalizadas por sistema, lo que evita la reutilización de técnicas de ataque entre entornos.
- Control de seguridad granular, permitiendo bloquear acciones específicas de riesgo sin afectar aplicaciones necesarias.
- Integración sencilla y gestión eficiente en GravityZone, con autopiloto y agrupación inteligente.

REDUCIENDO LA SUPERFICIE DE ATAQUE

Uno de los principales beneficios de PHASR es la reducción drástica de la superficie de ataque. Al correlacionar las acciones de los usuarios con vectores de amenaza, determina una configuración de seguridad óptima para cada uno, lo que permite a las organizaciones mantener su eficiencia operativa sin exponer sistemas innecesariamente.

Además, PHASR detiene de forma proactiva el uso de binarios conocidos como LOLBins antes de que puedan ser explotados, ayudando a reducir filtraciones de datos, exceso de alertas y costes operativos.

La solución también evita que los atacantes apliquen las mismas técnicas en distintos entornos al adaptar dinámicamente las defensas, haciendo que cada sistema responda de manera distinta a intentos similares de intrusión.

INCREMENTANDO LA AUTOMATIZACIÓN DE TAREAS DE CIBERSEGURIDAD

Gartner prevé que, para 2030, el 60% de las tareas de gestión de exposición y remediación estarán automatizadas, frente al 10% actual. Según la consultora, la reducción de la superficie de ataque es esencial porque no depende de la detección para proteger. En este contexto, PHASR se alinea perfectamente con las proyecciones del sector, al priorizar la mitigación preventiva del riesgo y una arquitectura de seguridad que actúe antes de que se materialicen los ataques.

GravityZone PHASR está disponible como una extensión de la plataforma GravityZone, permitiendo una integración fluida con las capacidades existentes de seguridad unificada y análisis de riesgos de Bitdefender. ■

MÁS INFO +

» Entrevista a Luis Fisas

» GravityZone PHASR

COMPARTIR EN REDES SOCIALES

DMI Computer

KIOXIA

Ready for the Next Adventure

EXCERIA HIGH ENDURANCE

EXCERIA PLUS

EXCERIA G2

RAFA CLAUDÍN

NO TE FÍES NI DE TU CEO:

CUANDO LA CIBERSEGURIDAD ES CUESTIÓN DE DESCONFIANZA

El añejo y resistente perímetro de seguridad de las organizaciones se ha ido diluyendo poco a poco hasta casi desaparecer. O peor, hasta convertirse en una ilusión. Y probablemente lo único peor que no tener un sistema de ciberseguridad sólido es la ilusión de tenerlo. Las propuestas Zero Trust asumen la realidad de un nuevo perímetro de la seguridad: la identidad, planteando un marco tecnológico y estratégico para la ciberseguridad corporativa.

Sí, no te fíes ni de tu CEO. A lo mejor un poco más del CISO, pero tampoco. Puede parecer un planteamiento un poco exagerado, pero cualquiera que haya sufrido un intento del fraude del CEO sabe de lo que hablamos. Es una vieja táctica de ingeniería social básica, usada preferentemente contra un nuevo fichaje del departamento financiero, en la que el estafador se hace pasar por el CEO para empujarle a realizar de forma urgente una cuantiosa transferencia.

Un intento de fraude que todavía hoy se produce. Incluso, mucho más hoy, gracias a los deepfake de la IA generativa que han dado a una estafa de las de toda la vida un cierto aire de refinamiento. Ahora el que se hace pasar por tu CEO tiene su voz e incluso su cara. Aunque llamativo, solo es un ejemplo del modo en que ha cambiado la ciberseguridad en el entorno corporativo. Durante décadas, se basó en lo que solía llamarse modelo bastión: una fortaleza con una muralla protectora en la que se confiaba en todo el que hubiese pasado el filtro de entrada.

Este modelo hace tiempo que no es viable. Para explicar la situación actual, Sergio Martínez, de SonicWall, suele cambiar la imagen del bastión por la de un aeropuerto. Decenas de entradas y salidas y miles de personas moviéndose de un sitio a otro. Una imagen bastante acertada: no puedes establecer un perímetro corporativo cerrado para proteger la empresa, sino crear el perímetro para cada entidad, humana o máquina, que entre en ella.

UN SEGMENTO DE LA CIBERSEGURIDAD EN AUGE

El concepto de Zero Trust viene a resolver esa situación. Se trata de un nicho de la ciberseguridad del que todo el mundo dice estará destinado a ser un estándar básico. Según los datos de Fortune Business Insights, el mercado Zero Trust global tuvo un valor de más de 36.000 millones de dólares en 2024, superará los 42.000 millones este año y llegará a 124.500 millones en el 2032. Nada menos que una tasa de crecimiento interanual compuesta estimada en el 16,7%.

La razón de ese crecimiento está en la necesidad de un paradigma como el que plantea, en el que de entrada no puedes confiar en ninguna de las conexiones a los sistemas corporativos. Un cambio considerable que no está exento de retos. Javier González, director técnico de Virtual Cable, explica que “uno de los principales desafíos es el cambio cultural y operativo que implica abandonar el modelo tradicional de confianza implícita dentro del perímetro corporativo. Zero

> “LA TENDENCIA ES CONTAR CON PLATAFORMAS CONVERGENTES QUE INTEGREN ACCESO SEGURO, PROTECCIÓN DE DATOS, VISIBILIDAD Y ANÁLISIS EN TIEMPO REAL DESDE LA NUBE”
>
> **IGNACIO FRANZONI,** director de ingeniería de soluciones en **Netskope**

Trust exige validar constantemente la identidad de usuarios y dispositivos, segmentar los accesos y aplicar controles de manera granular. Esto requiere una revisión profunda de los sistemas existentes, una integración entre soluciones de identidad, red y aplicaciones, y una gestión precisa de los permisos".

Ignacio Franzoni, director de ingeniería de soluciones en Netskope, coincide en que "implementar un modelo Zero Trust implica cambiar la perspectiva de seguridad en las organizaciones. El principal desafío es la visibilidad: una política adecuada requiere saber quién accede, desde dónde y a qué recursos. También se necesita revisar procesos heredados, integraciones entre plataformas y gestionar identidades, dispositivos y datos. Esto implica coordinar equipos de red, seguridad y TI, romper silos y aplicar controles en tiempo real sin fricción".

LA RESISTENCIA A LA CONFIANZA CERO

Todo ello sin olvidar el factor clave en los desarrollos tecnológicos de alto impacto: el factor humano. Sergio Martínez, country manager de SonicWall para Iberia, recuerda que "son varios desafíos los que se plantean ante un despliegue Zero-Trust. Además de la integración con los sistemas heredados y la complejidad técnica, diría que la parte humana (resistencia al cambio) es posiblemente la más importante, además de definir claramente quién y a qué se puede acceder, el mapa de los usuarios, recursos y aplicaciones de la organización. Cambiar procesos y a las personas siempre es más complejo que la tecnología".

La resistencia al cambio forma parte de nuestra idiosincrasia como seres humanos. La resistencia es más fuerte si, además, el cambio supone que el usuario tenga que autenticarse demasiadas veces. O no demasiadas, simplemente más de las que estaba acostumbrado. Por ello los proveedores de ciberseguridad trabajan para minimizar el impacto que pueda tener sobre la operativa o la usabilidad, manteniendo al mismo tiempo los principios de Zero Trust.

Ignacio Franzoni, de Netskope, considera que "uno de los errores más comunes es asumir que Zero

> "LA IA Y EL MACHINE LEARNING SE INTEGRARÁN DE FORMA MÁS PROFUNDA EN LOS SOC, LO QUE CONLLEVA UNA MAYOR RESPONSABILIDAD"

SERGIO MARTÍNEZ,
country manager de **SonicWall** para Iberia

Trust implica fricción constante. Sin embargo, cuando se basa en una combinación adecuada de identidad, contexto y análisis de comportamiento, las políticas de Zero Trust pueden aplicarse prácticamente de manera imperceptible para el usuario. Por ejemplo, si un empleado accede a una aplicación corporativa desde su ordenador habitual, en una red confiable y con autenticación robusta, el sistema puede permitir el acceso sin interrupciones. Solo al detectar una anomalía, como un nuevo dispositivo, ubicación o patrón de uso, se refuerzan los controles".

BENEFICIOS DE ZERO TRUST

Incluso a pesar de que pueda producirse cierto punto de fricción, las ventajas superan con creces a los inconvenientes. Marcos Jimena, director técnico de Zscaler en Iberia, resume que "Zero Trust reduce drásticamente la superficie de ataque, ya que elimina la confianza implícita, segmenta los accesos a nivel de aplicación y oculta los recursos a usuarios no autorizados, haciendo a las empresas prácticamente invisibles ante amenazas externas. En segundo lugar, permite prevenir eficazmente los movimientos laterales en caso de una brecha, ya que cada intento de conexión se evalúa y se controla individualmente. Además, al incorporar capacidades avanzadas como la inspección de tráfico cifrado, la prevención de pérdida de datos (DLP) y la inteligencia artificial (IA) para la detección de amenazas, se mejora significativamente la capacidad de respuesta ante incidentes".

Sergio Martínez, de SonicWall, destaca entre otras ventajas de Zero Trust la "verificación de la identidad de usuarios y dispositivos, con una estricta verificación de ZTNA que se basa en las credenciales del usuario, el tiempo de acceso y la conformidad del dispositivo para permitir un acceso rápido y sencillo a las aplicaciones y datos de la organización; las políticas de privilegios de mínimo acceso, en las que los usuarios solo pueden acceder a lo necesario para realizar su trabajo, y nada más, no se permiten usuarios con privilegios excesivos; y la microsegmentación para definir límites de confianza internos y controlar de forma granular el flujo de tráfico y de acceso a los recursos para proteger los datos y evitar que las amenazas se propaguen lateralmente".

LAS PROPUESTAS TECNOLÓGICAS

Hemos querido saber cuál es la propuesta Zero Trust concreta de las empresas que han colaborado en este artículo. Javier González, de Virtual Cable, explica que su propuesta "se basa en la autenticación centralizada y segura, con soporte para MFA y SSO; la asignación dinámica de escritorios y aplicaciones según perfil de usuario; el aislamiento total entre sesiones y segmentación de recursos; la no persistencia de datos locales, evitando exposición de información confidencial; y el registro y auditoría completa de sesiones para trazabilidad. Con UDS Enterprise, las organizaciones pueden aplicar una arquitectura Zero Trust desde el acceso al entorno de trabajo, construyendo una capa segura, flexible y adaptable a cualquier estrategia de seguridad corporativa".

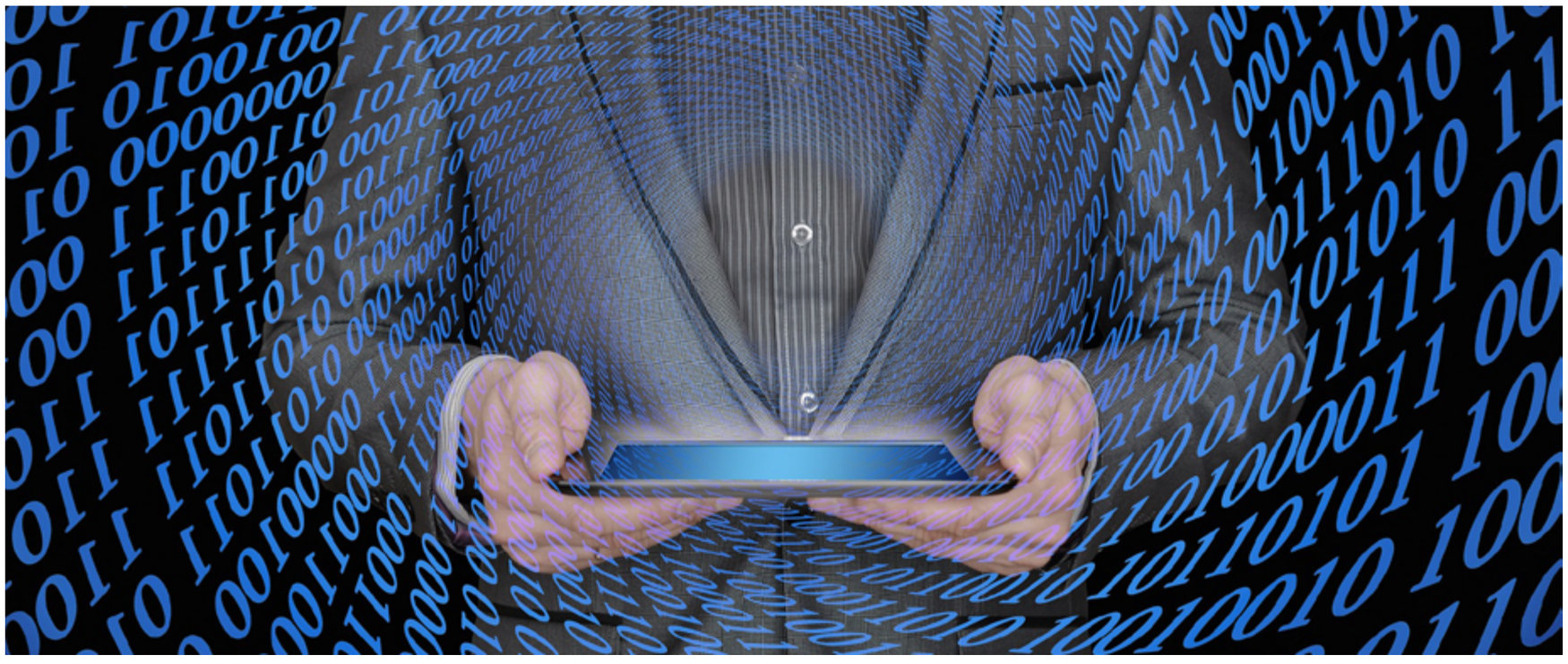
Ignacio Franzoni, director de ingeniería de soluciones en Netskope, detalla que la compañía "permite políticas basadas en identidad, ubicación, dispositivo, nivel de riesgo y contenido específico. Por ejemplo, se puede permitir acceso a Microsoft OneDrive corporativo y bloquear acceso a uno personal, o permitir

> "EL DIGITAL WORKPLACE SERÁ UNO DE LOS VECTORES CLAVE PARA APLICAR POLÍTICAS ZERO TRUST DE FORMA EFECTIVA, SIN SACRIFICAR PRODUCTIVIDAD NI FLEXIBILIDAD"
>
> **JAVIER GONZÁLEZ,** director técnico de **Virtual Cable**

ver un documento confidencial sin autorizar su descarga. Esto es posible gracias a nuestra arquitectura en la nube y la red New Edge, que inspecciona el tráfico en tiempo real sin afectar el rendimiento. No solo permitimos o denegamos accesos, aplicamos controles dinámicos según el contexto. Así, ayudamos a implementar una estrategia Zero Trust efectiva sin comprometer la experiencia del usuario ni la eficiencia operativa".

Marcos Jimena, de Zscaler, explica que, partiendo de su plataforma Zero Trust Exchange, "el proceso se basa en cuatro pasos clave: verificar de forma estricta la identidad del usuario y del dispositivo, determinar a qué aplicación se quiere acceder, evaluar el contexto y el riesgo de la sesión, y aplicar una política de acceso granular en tiempo real. Todo ello sin exponer direcciones IP, sin dar acceso a la red y sin depender de dispositivos físicos. Nuestro enfoque cubre múltiples casos de uso: acceso seguro a aplicaciones privadas sin VPN, protección de aplicaciones SaaS, seguridad para entornos OT e IoT, control de accesos de terceros, y protección de cargas de trabajo en la nube. Además, todo se gestiona desde una consola centralizada, lo que facilita la visibilidad, la automatización y la gobernanza".

Por su parte, Sergio Martínez, country manager de SonicWall para Iberia, comenta que "la propuesta de Zero Trust de SonicWall consiste básicamente en ofrecer un sistema de seguridad que aplica control continuo sobre usuarios, dispositivos, aplicaciones y datos, tanto dentro como fuera de la red corporativa. Es



> "EL FUTURO DE LA CIBERSEGURIDAD SERÁ CADA VEZ MÁS DINÁMICO, DISTRIBUIDO Y CENTRADO EN EL CONTEXTO. Y ZERO TRUST SERÁ SU PIEDRA ANGULAR"
>
> **MARCOS JIMENA,** director técnico de **Zscaler** en Iberia

un acceso remoto ZTNA moderno que sustituye a las VPN tradicionales de una forma sencilla, pero tremendamente potente a nivel de prestaciones y seguridad".

UN FUTURO DE CONFIANZA CERO

Ya se sabe que cuando se pierde la confianza es muy difícil recuperarla. En este caso, se trata del escenario tecnológico general. Cuando las nuevas tecnologías han mostrado una forma más eficiente de trabajar y los procesos se han transformado, es imposible volver atrás. Estar en la nube, apostar por la IA, tener miles de dispositivos conectados, es imprescindible para ser competitivo. Y en ese panorama la gestión de la identidad y los accesos, la microsegmentación de las redes y la autenticación reforzada son la opción principal de protección.

Así, Javier González, director técnico de Virtual Cable, considera que "Zero Trust dejará de ser una tendencia para convertirse en un estándar. Su adopción se acelerará conforme las organizaciones enfrenten entornos más híbridos, movilidad permanente y amenazas avanzadas. A medida que maduren las herramientas de automatización, inteligencia artificial y análisis de comportamiento, las arquitecturas Zero Trust serán más dinámicas y proactivas".

Para Marcos Jimena, director técnico de Zscaler en Iberia, "veremos una adopción masiva de arquitecturas Zero Trust en todos los sectores, impulsada por la necesidad de proteger entornos híbridos, aplicaciones distribuidas, dispositivos móviles y usuarios remotos. Además, estamos asistiendo a una convergencia natural entre redes y seguridad con SASE (Secure Access Service Edge) y SSE (Security Service Edge) [...] La IA jugará un papel central en la automatización de decisiones de acceso, en la detección de amenazas avanzadas y en la optimización de la experiencia del usuario. Y con el auge del IoT, el edge computing y los entornos OT, Zero Trust será clave para asegurar no solo los datos, sino también las operaciones críticas". ■

ZERO TRUST, UN NOMBRE ACERTADO PARA UN CONCEPTO CLAVE

Simple, con gancho y perfectamente ajustado al concepto que define. El nombre de Zero Trust se lo debemos a John Kindervag, analista sénior de Forrester Research cuando fijó el concepto en 2009. Poner nombres que se acaban perpetuando es una especie de superpoder de las consultoras. Como explicó Mary Pratt en TechTarget, en realidad el concepto tiene un antecedente importante de 2004, en una presentación del miembro del Jericho Forum Paul Simmonds. Pero él lo llamó "deperimeterization". Bastante claro, pero con Zero Punch.

Aunque llegó más tarde a las nomenclaturas Zero Trust, Gartner también es responsable de algunos de los nombres clave de todo el planteamiento de la confianza cero. Suyos son nada menos que Zero Trust Network Access (ZTNA), los productos que ofrecen acceso Zero Trust a las redes, y Secure Access Service Edge (SASE), un modelo de seguridad en la nube que protege los elementos corporativos, físicos o en la nube, en cualquier lugar.

MÁS INFO +

- La adopción de zero trust podría haber reducido las pérdidas económicas globales en un 31%
- Solo el 35% de las iniciativas zero trust logran implementarse con éxito

COMPARTIR EN REDES SOCIALES

Strategy₿

Inteligencia potenciada por IA.

ENCUENTROS **ITDM GROUP**

APOSTANDO POR UNA ESTRATEGIA DE DATOS INTELIGENTE

ORGANIZA

PATROCINADORES GOLD

PATROCINADORES SILVER

ENCUENTROS ITDM GROUP: APOSTANDO POR UNA ESTRATEGIA DE DATOS INTELIGENTE

Los datos se han convertido en un activo clave para las organizaciones, que pueden aprovecharlos para optimizar sus operaciones, ser más eficientes y competitivas, evolucionando hacia modelos data-driven. En estos Encuentros ITDM Group analizamos cómo las empresas están transformando sus estrategias de datos para lograr una gestión más inteligente que apoye la toma de decisiones e impulse el negocio, con la colaboración de Making Science, Schneider Electric, Crayon, PUEDATA, QNAP y SonicWall.

#ENCUENTROSITDMGROUP

El volumen de datos que manejan las organizaciones es cada vez mayor y también lo es su potencial para modernizar el negocio, impulsar la eficiencia, la innovación digital y la competitividad. Para sacar partido de estas ventajas, las empresas necesitan cambiar hacia un modelo data-driven basado en mejorar la gestión y el aprovechamiento de los datos a todos los niveles, y en adoptar tecnologías clave como la inteligencia artificial, la automatización, Internet de las Cosas (IoT) o los servicios en la nube. Este cambio hacia arquitecturas de datos modernas e inteligentes promete grandes beneficios, pero también conlleva importantes desafíos, tanto desde el punto de vista tecnológico como humano, que se deben tener en cuenta para alcanzar el éxito.

A lo largo de los Encuentros ITDM Group: Apostando por una estrategia de datos inteligente abordamos cómo están enfocando las empresas españolas la necesaria evolución hacia modelos de negocio apoyados por datos, a qué retos se enfrentan y qué tecnologías son clave para lograrlo, con expertos de Making Science, Schneider Electric, Crayon, PUEDATA, QNAP y SonicWall.

MAXIMIZANDO EL VALOR DEL DATO: ESTRATEGIAS Y ARQUITECTURAS INTELIGENTES EN LA ERA DATA-DRIVEN

El plato principal de estos Encuentros ITDM Group es un evento de la Comunidad IT, apoyado por Making Science y Schneider Electric, en el que reunimos a representantes de ACCIONA, AEDAS Homes, Banco Sabadell, Caixabank Payments & Consumer, CEU Educational Group, Grupo ASV, Sincrolab, Urbaser y Vithas para hablar sobre las nuevas arquitecturas tecnológicas y estrategias en torno al dato. Junto a ellos, han participado César Ramos, business intelligence area manager de Making Science; y Víctor Manuel Gago, datacenter and C&SP sales manager de Schneider Electric.

ENTREVISTA >> Noelia González, de la Universidad Alfonso X el Sabio, nos habla sobre buenas prácticas en la gestión y el gobierno de los datos, y sobre tendencias y tecnologías relacionadas con el dato.

EVENTO >> En este debate reunimos a líderes de TI de empresas de diferentes sectores con portavoces de Making Science y Schneider Electric, para hablar sobre estrategias y arquitecturas de datos inteligentes.

APOSTANDO POR UNA ESTRATEGIA DE DATOS INTELIGENTE

A continuación, celebramos una mesa redonda centrada en cómo las empresas están avanzando hacia estrategias de datos inteligentes apoyándose en tecnologías como la IA, y en los desafíos que están surgiendo en el ámbito de la ciberseguridad. Para ello, contamos con Álvaro Montoya, data and IA sales executive de Crayon; Sergio Rodríguez, CTO de PUEDATA; Guillermo Alcover, regional sales specialist de QNAP; y Sergio Martínez, country manager de SonicWall.

OTROS CONTENIDOS PARA LA COMUNIDAD IT

Además de estas dos mesas redondas, para tener una visión más amplia sobre la importancia de los datos para el negocio y sobre la evolución de las estrategias de datos entrevistamos a Noelia González, data & AI expert, Universidad Alfonso X el Sabio (UAX), que nos habla sobre buenas prácticas y tendencias en la gestión del dato; y a Jorge Valero, director de aplicaciones y data, AEDAS Homes, para conocer cómo aplican las nuevas tecnologías en su empresa para extraer valor de los datos. ■

MÁS INFO +

» Encuentros ITDM Group: Apostando por una estrategia de datos inteligente

MESA REDONDA >> Debatimos con expertos de Crayon, PUEDATA, QNAP y SonicWall, sobre cómo las empresas están redefiniendo sus estrategias de datos para avanzar hacia un modelo data-driven.

ENTREVISTA >> Jorge Valero, de AEDAS Homes, explica cómo el sólido trabajo previo con los datos de la compañía les ha servido para desplegar una eficaz estrategia de inteligencia artificial agéntica.

Muchas organizaciones quieren sacar partido de los datos para impulsar su toma de decisiones y ser más eficientes y competitivas, convirtiéndose en una organización data-driven. Pero esto requiere un alto grado de madurez, no solo tecnológica, sino también a nivel de estrategia y cultura corporativa, para lo que es fundamental tener claros tanto los objetivos como los riesgos, y diseñar un plan de transformación que contemple la gestión del dato de una forma holística, basada en información de calidad, fiable y segura.

EL CAMINO HACIA UNA EMPRESA DATA-DRIVEN

La transformación hacia modelos de negocio basados en el dato se presenta como el camino a seguir para cualquier organización, pero este cambio tiene muchas implicaciones y requiere un plan claramente definido, que abarque las diferentes dimensiones de los datos dentro de una empresa. Uno de los temas clave a tener en cuenta es el crecimiento constante de información que proviene de múltiples canales, un activo que las empresas necesitan capturar, almacenar y gestionar adecuadamente antes de poder aplicar técnicas de analítica y procesamiento que aporten verdadero valor a la toma de decisiones.

Como explica José A. Rodríguez-Serrano, director académico MSc en business analytics de ESADE en un artículo publicado a comienzos de 2025, "la toma de decisiones basada en datos se ha convertido en una estrategia indispensable para las empresas que buscan optimizar sus operaciones y mantenerse competitivas". Explica que, para alcanzar la ansiada toma de decisiones guiada por datos se requieren datos cuantitativos, en lugar de basarse en intuiciones o experiencias pasadas, un proceso que "implica recolectar, analizar e interpretar datos para hacer elecciones informadas que minimicen riesgos y maximicen oportunidades".

En este camino surgen muchos retos y también nuevas tecnologías que las organizaciones deben saber aplicar para obtener datos relevantes y de calidad, que puedan ser procesados para obtener información realmente valiosa para el negocio. Y, como indica este experto, permita "identificar patrones, prever tendencias y tomar decisiones estratégicas fundamentadas en evidencias concretas". Como especialista en inteligencia de negocio, define una serie de pasos que las organizaciones deben dar para transformar los datos que recogen en información aprovechable para impulsar la toma de decisiones.

UNA BUENA PREPARACIÓN

El primer paso que debe dar una organización para lograr estos objetivos es diseñar una estrategia y una arquitectura de datos que de soporte no solo a las necesidades actuales, sino también a las del futuro, apostando por un modelo de gestión capaz de soportar el crecimiento de los datos y su aplicación a nuevas áreas del negocio. José A. Rodríguez-Serrano afirma que lo primero es "definir claramente los objetivos empresariales", que "deben ser específicos, medibles, alcanzables, relevantes y limitados en el tiempo".

OBTENCIÓN DE DATOS

A continuación, la organización debe trabajar en el modelo de obtención de datos que más conviene para alcanzar estos objetivos, comenzando por identificar las fuentes de información existentes y las que puedan añadirse en el futuro. Esto abarca tanto los datos internos de la compañía, provenientes de áreas como ventas o finanzas, como externos, incluyendo informes de mercado, información de la cadena de suministro, de los clientes y de otras fuentes relevantes.

Lo siguiente es diseñar la forma en que toda esta información se recopilará, almacenará y estructurará, poniendo especial cuidado en la selección y curación de los datos, obviando la información irrelevante, dudosa o contradictoria, y definiendo claramente cuál es la "única fuente de verdad" que servirá a los objetivos del negocio. Desde ESADE, destacan

que “es fundamental implementar procedimientos que garanticen la integridad y la calidad de los datos recolectados, ya que datos inexactos o incompletos pueden conducir a conclusiones erróneas y, en última instancia, a decisiones empresariales equivocadas”. Para evitarlo, apunta, se deben establecer protocolos de calidad de los datos.

ANÁLISIS PARA OBTENER CONOCIMIENTO

Una vez que ya está definida la forma en que se recopilan y estructuran los datos, quedándose solo con la información relevante, es el momento de platearse cómo transformarla en insight útiles. Como explica José A. Rodríguez-Serrano, existen multitud de herramientas y técnicas de análisis y visualización de datos, comenzando por las dedicadas al análisis estadístico que, en sus palabras, “permiten a los analistas aplicar métodos cuantitativos para desentrañar patrones y tendencias ocultas en los datos”. En este ámbito, existen tres técnicas principales de análisis: descriptivo, para entender los datos históricos; predictivo, para obtener generalizaciones en base a muestras de datos de grupos específicos de clientes... y prescriptivo, para ofrecer sugerencias concretas basadas en los resultados predictivos.

Además, destaca la importancia de contar con herramientas de visualización de los datos y los resultados de los procesos de análisis, que ofrezcan una representación visual, con gráficos, mapas y diagramas que faciliten la interpretación de la información. Y añade que “la visualización de datos no solo ayuda a identificar patrones y tendencias rápidamente, sino que también facilita la comunicación de hallazgos complejos a audiencias no técnicas”.

APLICACIÓN A LA TOMA DE DECISIONES

El último paso en este camino hacia un modelo operativo guiado por datos es aplicar esos insights obtenidos en los pasos anteriores a la toma de decisiones de negocio que, en opinión de este experto, “deben basarse en una interpretación objetiva y cuidadosa de la información, considerando tanto los beneficios como los posibles riesgos asociados”. También considera vital comunicar claramente las decisiones que se toman en base a los datos, lo que “implica presentar los hallazgos y las conclusiones de manera comprensible para todos los stakeholders involucrados”.

Pero el proceso no acaba aquí, sino que es muy importante evaluar los resultados de estas decisiones, para lo que es necesario definir métricas y KPI que permitan medir el impacto en el negocio y llevar a cabo un seguimiento continuo. Solo así se puede determinar si se está siguiendo el camino correcto, o si es necesario reevaluar la estrategia para ajustarse a los objetivos de la organización.

En todo este proceso de análisis de información, toma de decisiones en base a datos y evaluación de resultados es fundamental apostar por tecnologías asociadas al big data, como machine learning e inteligencia artificial, que ayudan a contextualizar los datos seleccionados y extraer información relevante para el negocio.

A lo largo de estos Encuentros ITDM Group analizamos estas y otras cuestiones relacionadas con la evolución de las empresas hacia modelos data-driven, con la ayuda de expertos en la materia de diferentes sectores, incluyendo a representantes de la industria tecnológica. ■

> “LA TOMA DE DECISIONES BASADA EN DATOS SE HA CONVERTIDO EN UNA ESTRATEGIA INDISPENSABLE PARA LAS EMPRESAS”
>
> **JOSÉ A. RODRÍGUEZ-SERRANO,** director académico MSc en business analytics de **ESADE**

MÁS INFO +

» Encuentros ITDM Group: Apostando por una estrategia de datos inteligente

COMPARTIR EN REDES SOCIALES

making science

Google Cloud

DEMOCRATIZA EL ACCESO

« A DATOS CON IA Y ACELERA TU TOMA DE DECISIONES »

makingscience.es

Contáctanos

NOELIA GONZÁLEZ, DATA & AI EXPERT DE LA UNIVERSIDAD ALFONSO X EL SABIO

“La IA generativa ha ayudado a que las iniciativas de datos cobren la importancia que merecían”

Abrimos este Encuentro ITDM Group con esta entrevista a Noelia González, data & AI expert de la Universidad Alfonso X el Sabio. Con un amplio historial docente en diferentes universidades, ha trabajado también en las áreas de datos e inteligencia artificial en empresas de perfiles muy diferentes, desde Minsait hasta Electronic Arts.

BUENAS PRÁCTICAS EN TORNO AL DATO

La experta explica que “las buenas prácticas deben partir de un propósito. Para qué queremos los datos. Qué decisiones o procesos de negocio vamos a mejorar con ellos. A partir de ahí, hay que utilizar los criterios habituales en la gestión de datos: que la calidad en el origen sea buena, que no se hagan cambios posteriores y definir los roles

ENTREVISTA >> Noelia González, de la Universidad Alfonso X el Sabio, explica las buenas prácticas aprendidas en la gestión y el gobierno de los datos, junto a las tendencias que emergen del cruce con las tecnologías basadas en datos.

claros de la responsabilidad sobre el dato". La adaptación a la realidad del negocio define incluso el marco de gobierno de datos que se escoja, desde DAMA, hasta CMDC o aplicaciones Data Mesh.

Entre otras cosas, recomienda trabajar con arquitecturas flexibles para adaptarse al negocio y a los cambios, así como medir el impacto de las iniciativas para que se vea su valor. Además, es necesario ampliar la cultura data de las organizaciones, basada en la confianza. "Hay una serie de herramientas que nos ayudan, pero hay que tener una estrategia muy clara y unas personas muy alineadas en este proceso".

EL DESPERTADOR DE LA IA GENERATIVA

La inteligencia artificial generativa ha sido "un despertador brutal", llamando la atención tanto en la vida personal como en la laboral e impulsando numerosas iniciativas dentro de las compañías. Al mismo tiempo, "ha expuesto las debilidades relacionadas con el dato. Muchas empresas se han dado cuenta de que no tenían una base sólida de los datos, bien estructurada y gobernada".

Los proyectos de IA pueden dar malos resultados si los datos de partida no son de calidad, lo que no solo ha servido para mejorar las estrategias de datos, sino que ha añadido nuevas áreas, como "la gobernanza de Prompts, la alineación ética de los modelos, la gestión de los derechos y los contenidos... La IA generativa ha ayudado a que las iniciativas de datos cobren la importancia que merecían".

TENDENCIAS DE DATOS

Aunque los principios básicos de las estrategias de datos son más o menos similares a los de hace unos años, con cuestiones de privacidad, gobernanza, gestión y calidad, lo cierto es que el cruce de área data con las tecnologías basadas en datos ha ido añadiendo capas a esas políticas iniciales. En particular, la IA generativa, que ha supuesto como veíamos la creación de nuevas áreas en el gobierno de los datos.

Además, Noelia González explica que se ha avanzado mucho en cuestiones como la trazabilidad del dato y la IA explicable, entre otras cosas por exigencias regulatorias; la automatización del gobierno del dato; la democratización del acceso a los datos; el enfoque sostenible del dato, midiendo el coste energético y económico de almacenar y procesar todos los datos que se generan. Para la experta, "la clave es no solo tener los datos sino usarlos de una forma eficiente, responsable y ética". ■

> "NO SE PUEDE PLANTEAR UNA CULTURA DATA-DRIVEN SI LAS PERSONAS NO ENTIENDEN EL LENGUAJE DEL DATO"
>
> **NOELIA GONZÁLEZ,**
> data & AI expert de la
> **Universidad Alfonso X el Sabio**

MÁS INFO +

» Noelia González, UAX

COMPARTIR EN REDES SOCIALES

Liquid Cooling más fácil

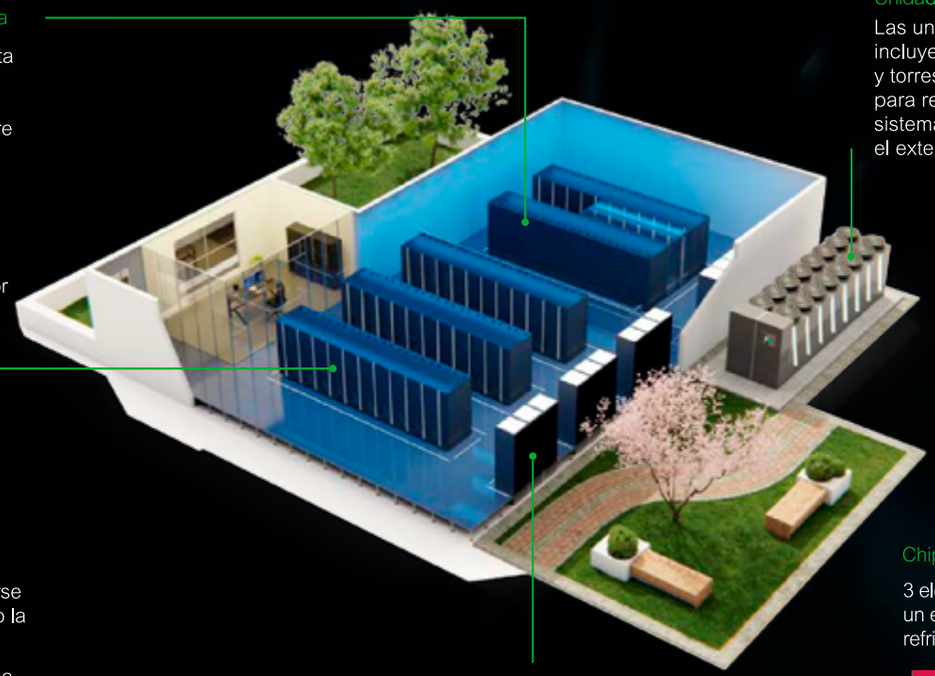
La refrigeración líquida se ha vuelto esencial para la computación acelerada de alto rendimiento. La refrigeración por aire era práctica cuando las densidades de los chips eran más bajas. Sin embargo, estas densidades se han disparado, ejerciendo más presión sobre la refrigeración por aire tradicional hasta hacerla cada vez más inmanejable. Así pues, se necesitan nuevos enfoques para la eliminación del calor con el fin de evitar el riesgo de puntos calientes que provocan fallos en los equipos y tiempos de inactividad.

La refrigeración líquida directa no es un producto, sino una arquitectura respaldada por sistemas críticos que incluyen unidades de distribución de refrigerante. Sin embargo, la refrigeración líquida directa es algo más de lo que su nombre indica, ya que incluye la refrigeración por aire y las unidades de rechazo de calor (por ejemplo, enfriadores) que ya conoces y que prevalecen en los centros de datos actuales.

Refrigeración por aire complementaria

La refrigeración por aire complementa a la refrigeración líquida y es necesaria para rechazar el calor de los componentes refrigerados por aire en el espacio informático.

Esto incluye, entre otros, el aire acondicionado de la sala de ordenadores y el climatizador, la pared de ventiladores, el perímetro tradicional, InRow y el intercambiador de calor de la puerta trasera



Unidades de rechazo de calor

Las unidades de rechazo de calor, que incluyen enfriadoras, enfriadores secos y torres de refrigeración, se utilizan para rechazar el calor en el bucle del sistema de refrigeración técnica hacia el exterior.

Servidores con refrigeración líquida

Direct-to-chip es el método preferido hoy en día, en el que el refrigerante líquido se bombea a través de una placa fría fijada directamente al chip. Las placas frías también pueden fijarse a otros componentes calientes, como la memoria.

La inmersión es otro método en el que los componentes se sumergen total o parcialmente en refrigerante líquido.

Navega por la refrigeración líquida

Unidad de distribución de refrigerante (CDU)

La CDU aísla el bucle del sistema de refrigeración técnica del resto del sistema de refrigeración y controla la temperatura, el caudal, la presión, el tratamiento de fluidos y el intercambio de calor.

Las CDU varían en cuanto al tipo de intercambio de calor, la capacidad y el factor de forma (montaje en bastidor o en el suelo).

Chip-to-Chiller

3 elementos principales de un ecosistema de refrigeración líquida

Captación de calor en el servidor

Intercambio de calor en el centro de datos

Método para expulsar el calor al exterior

Life Is On Schneider Electric

MAXIMIZANDO EL VALOR DEL DATO: ESTRATEGIAS Y ARQUITECTURAS INTELIGENTES EN LA ERA DATA-DRIVEN

En medio del terremoto provocado por la inteligencia artificial, que está dando ya sus primeros pasos en el terreno de la agéntica, las empresas modulan sus estrategias de datos para mantener el equilibrio entre las necesidades de negocio, los requisitos de cumplimiento, control y seguridad de los datos y el ritmo acelerado que marca la evolución tecnológica.

ENCUENTRO COMUNIDAD IT >> Hablamos sobre los progresos en el uso de los datos y el modo en que se combinan con otras tecnologías con representantes de **ACCIONA, AEDAS Homes, Banco Sabadell, Caixabank Payments & Consumer, CEU Educational Group, Grupo ASV, Sincrolab, Urbaser** y **Vithas**, en una mesa redonda que ha contado con el patrocinio de **Making Science** y **Schneider Electric**.

> PARA LA INTELIGENCIA ARTIFICIAL GENERATIVA, LA CLAVE NO RESIDE TANTO EN LOS DATOS EN SÍ, SINO EN LA RIQUEZA DEL CONTEXTO QUE LOS ENVUELVE

RAFAEL SOCORRO
Head of data & analytics,
ACCIONA Construcción

> CUANDO ESTÁS EN LA NUBE, NO SOLO DEBES TENER EN CUENTA LOS COSTES DEL ALMACENAMIENTO O LA COMPUTACIÓN, SINO TAMBIÉN LOS DE TRANSFERENCIAS DE DATOS

JORGE VALERO
Director de aplicaciones y data,
AEDAS Homes

Clica en la imagen para ver la galería completa

Clica en la imagen para ver la galería completa

Al Hamlet tecnológico se le acumulan las incógnitas. ¿On-prem o en la nube? ¿Barra libre a la innovación o control férreo? ¿IA tradicional o generativa? ¿Generativa asistencial o agéntica? Entre tantas incógnitas que va generando la cada vez más acelerada evolución tecnológica, hay una certeza absoluta: los datos. Sin calidad ni privacidad de los datos, sin gestión ni gobierno, no habrá inteligencia artificial de ningún tipo, ni proyecto de digitalización que tenga visos de lograr el éxito.

Los datos, además, cada vez crecen más en volumen y en complejidad; con el despliegue de la nube, si no por otros motivos, impulsado por la IA; con la propia inteligencia artificial removiendo los cimientos corporativos por las expectativas puestas en su desarrollo; con la proliferación de dispositivos IoT, especialmente en entornos industriales; con la automatización... El futuro verá el 2025 como un año en que ya estamos más que inmersos en la era data-driven.

Un momento idóneo que comprobar cómo se están enfrentando compañías de los más diferentes perfiles a esta realidad. Para ello hemos tenido el placer de compartir una mesa redonda con representantes de **ACCIONA, AEDAS Homes, Banco Sabadell, Caixabank Payments & Consumer, CEU Educational Group, Grupo ASV, Sincrolab, Urbaser** y **Vithas**, con el patrocinio especial de **Making Science** y **Schneider Electric**.

LA REALIDAD DE LOS MODELOS HÍBRIDOS

Salvo excepciones, la primera pregunta que nos hacíamos, ¿on-prem o en la nube?, tiene una respuesta bastante clara: ambas. La realidad ha confirmado una de las tendencias que indicaba Gartner para este año: la adopción de la nube híbrida. Los motivos para mantener una

> PARA EL TRATAMIENTO DE DATOS MÁS ANALÍTICOS, PRINCIPALMENTE, UTILIZAMOS LA NUBE, MIENTRAS QUE EN EL CASO DE DATOS CORE Y REGULATORIOS, NOS CENTRAMOS EN ON-PREMISE

ALESANDER GÓMEZ
Director de IT data & MLOPS, unidad de data, analytics e IA, **Banco Sabadell**

> CLASIFICAMOS LOS DATOS EN FUNCIÓN DE SU VALOR Y DE INFINIDAD DE VARIABLES, LO QUE PERMITIRÁ, POR EJEMPLO, POTENCIAR LA CALIDAD EN LOS MÁS VALIOSOS

ÍÑIGO DE JAIME
Director de gobierno del dato, **Caixabank Payments & Consumer**

Clica en la imagen para ver la galería completa

infraestructura on-premise varían entre la necesidad de controlar los datos por cuestiones normativas o por ser considerados el core del negocio... Y la de controlar los costes.

Depende también de las infraestructuras heredadas que pueda tener una organización y de cuál sea el sector en el que opera. La sensación generalizada es que, en mayor o menor medida, la adopción de la nube es imprescindible para poder acceder a la innovación que representan tecnologías como las IA generativa. Pese a que hay empresas que incluso han empezado a bajar cosas que tenían en la nube, es imposible olvidarse de ella. Lo que sí se puede hacer, y se debe, es controlar los costes que supone.

David Castaños, head of data & automation en Urbaser, explica que "nuestra estrategia de arquitectura de datos se basa en un modelo híbrido. Por un lado, tenemos una estructura organizativa on-prem con todas las bases de datos que tenemos; y por otro lado aprovechamos de la nube todas las ventajas que nos da en temas de IoT o de sensórica. La parte on-prem tiene más que ver con la estrategia de costes. La escalabilidad que te da la nube es infinita, pero hay que tener un control inmediato, sobre todo en el movimiento del dato, para no tener sorpresas en el coste".

La persistencia del data center la certifica la fortaleza de empresas como Schneider Electric. Víctor Manuel Gago, datacenter and C&SP sales manager de la compañía, explica que su "propuesta de valor es integral. Somos el único fabricante en infraestructuras que podemos dar desde la alta tensión hasta el último interruptor que te encuentres en un

> EN UN PROYECTO EN EL QUE PARTES CON ARQUITECTURA ON-PREM DEBES RENTABILIZARLA, Y DARLE CONTINUIDAD, PERO EN EL MEDIO-LARGO PLAZO, TODO ESTARÁ EN LA NUBE

ÓSCAR VIÑAS
Management information & business intelligence director, **CEU Educational Group**

Clica en la imagen para ver la galería completa

> LA FIGURA DEL ANALISTA DE DATOS ESPECIALIZADO EN CADA ÁREA DE NEGOCIO ES FUNDAMENTAL PARA APALANCAR EL AUTOCONSUMO DE LOS DATOS

MARCO ANTONIO MARTÍNEZ
Responsable de BI, data y reporting, **Grupo ASV**

Clica en la imagen para ver la galería completa

data center. Gestionamos la energía desde la red hasta el chip, tenemos sistemas de refrigeración, de control y de servicios. Y tenemos la sostenibilidad por bandera: cuando trabajamos con un cliente en un proyecto intentamos reducir al máximo el coste de todo el ciclo de vida".

FinOps, el control de los gastos de la nube, sin duda es una tendencia que se mantendrá en el tiempo. Hay que tener en cuenta no solo un temor lógico al vendor lock-in, sino que el consumo de la nube se ha disparado con la llegada de la inteligencia artificial generativa. Otro difícil equilibrio muy de Hamlet: ¿cómo dar rienda suelta a la querencia de innovación impulsada por IA de las empresas sin que se desmadre el presupuesto tecnológico? De ahí la importancia creciente de la eficiencia operativa y el control de costes.

LOS DATOS SIN CONTROL NO SIRVEN DE NADA

Volvemos a la tesis de partida. O, más que la tesis, la realidad de partida. Los datos no gobernados, sin una calidad que se mantenga y se revise, no pueden ser útiles para los proyectos de digitalización. Las estrategias y políticas de adopción de los datos, nuevamente, varían entre las empresas, particularmente de si son más veteranas o nativas digitales. Pero también de otros "pequeños detalles", como las exigencias normativas que afronten o la apuesta de la alta dirección por lanzarse de lleno a la era data-driven. Datos, datos, datos... Pero con control.

Alesander Gómez, director de IT data & MLOPS en la unidad de data, analytics e IA del Banco Sabadell, señala que intentan "ser más rigurosos con la información que almacenamos. En muchos casos, almacenarlo todo no tiene sentido, debemos hacer una

> TRABAJAMOS CON LA IDEA DE QUE LA IA GENERATIVA TE PUEDA OFRECER UN PRE-DIAGNÓSTICO QUE LUEGO SIEMPRE TENDRÍA QUE CORROBORAR UN TERAPEUTA

ÍÑIGO LÓPEZ
Chief Data Officer, **Sincrolab**

> EN EL DEPARTAMENTO DE DATA, ESTAMOS UTILIZANDO LA IA GENERATIVA PARA EL RECONOCIMIENTO DE PATRONES, DETECCIÓN DE ERRORES O INCONSISTENCIAS, PERO TODAVÍA HAY QUE GUIARLA

DAVID CASTAÑOS
Head of data & automation, **Urbaser**

Clica en la imagen para ver la galería completa

selección de datos. Además, nuestra normativa de seguridad nos exige refrescar la información utilizada periódicamente, con lo que vamos eliminando ciertos datos a medida que va pasando el tiempo. También tenemos un control mucho más férreo de toda la información que los usuarios suben a las plataformas. Con el avance de las nuevas tecnologías de autoservicio, los usuarios son más independientes para utilizar datos y generar informes, pero es necesario controlar qué información se sube y para qué se utiliza. En nuestro caso, contamos con un flujo de gestión de peticiones que involucra al CDO, al DPO y al CISO".

Por su parte, Íñigo de Jaime, director de gobierno del dato en Caixabank Payments & Consumer, explica que han "centrado los esfuerzos en que el dato que tienen en negocio esté gobernado. Y está gobernado: independientemente de cómo hagan los informes o cómo hagan las consultas, el dato que va a salir está gobernado, es el mismo. Ahora estamos en un momento de cambio de cultura en la empresa. Estamos pasando a que, en lugar de que se saquen los datos y los consulten, se los damos nosotros. Les damos un informe ya gobernado, con su calidad, con todas las variables que hay que tener en cuenta".

En una empresa muy joven como Sincrolab, el dato es la base del negocio. Íñigo López, su chief data officer, comenta que "los datos que manejamos tienen que ser muy confiables: deben tener una validación clínica y pasar muchos controles. Nuestros datos son la propia terapia digital a la que nos dedicamos. Tenemos una aplicación para niños con TDAH en la que les ajustamos las terapias utilizando inteligencia arti-

ficial. No IA generativa, sino Machine Learning: en función de su rendimiento, les damos unos parámetros para cada juego, de modo que los niños ni se frustren ni se aburran".

POR EL CAMINO DE LA INTELIGENCIA ARTIFICIAL

La inteligencia artificial generativa está apuntalando la necesidad de trabajar adecuadamente los datos. La IA tradicional ya lo exigía: la diferencia con GenAI es que todo el mundo la quiere. Puede que te resistas a cambiar tus hábitos para algo tan misterioso como el Machine Learning o el Deep Learning, pero ¿quién no quiere un ChatGPT o un Copilot en el trabajo? Bienvenida sea una política estricta de datos con ese fin.

César Ramos, business intelligence area manager de Making Science, recuerda que "todo el mundo está utilizando cuatro cajas negras, cuatro modelos de IA. Lo único que podemos controlar es el contexto y el contexto lo controlamos a través de nuestros datos. Cuanto más gobernados y más controlados tengas esos datos, mayor éxito puedes tener en este tipo de proyectos. Hay dos principios clave: la agilidad y la gobernanza y el etiquetado del dato. Tanto la IA tradicional como la generativa no van a funcionar si no tienes los datos bien gobernados y etiquetados".

> "LA IA NOS OBLIGA A PASAR DE UNA OLIGARQUÍA DEL DATO EN LA QUE UNOS POCOS LO GOBERNAMOS Y CONTROLAMOS TODO A UNA DEMOCRATIZACIÓN REAL DEL DATO"
>
> **HÉCTOR VÍCTOR**
> Director de data analytics, **Vithas**

El viaje hacia la inteligencia artificial, como cualquier cambio que tiene implicaciones a muchos niveles de las organizaciones, se suele dar un poco a base de nadar y guardar la ropa. Incluso los más dispuestos a abrazar la nueva IA tienen hábitos de los que cuesta desprenderse. Llámalo hábito o llámalo Excel. O Power BI. Así y todo, es una transformación que está siendo mucho más acelerada que las anteriores.

Clica en la imagen para ver la galería completa

Óscar Viñas, management information & business intelligence director en CEU Educational Group, considera que, "a futuro, los cuadros de mando como tal van a desaparecer. No creo que en 10 años se desarrolle un solo cuadro de mando, sino que van a ser todos agentes de IA de datos, que al final están atacando una capa semántica. Nos vamos a dedicar a tener un modelo de datos bien organizado, bien gobernado, bien etiquetado, con una capa semántica de un conjunto de agentes. Pero a día de hoy nos toca convivir con un modelo híbrido donde vas a tener que hacer cuadros de mando mientras avanzas en la IA. Lo importante es basarse en un dato certificado".

Antes que desaparecer, las herramientas de BI se adaptan a marchas forzadas. Marco Antonio Martínez, responsable de BI, data y reporting en Grupo ASV, comenta que "tenemos el rol de experto que permite realizar esa serie de reportes y de análisis y que además lo va a distribuir a la gente que tiene a su cargo o a quien corresponda. Además, las herramientas de Business Intelligence son bastante potentes y cada vez van evolucionando más. Te permiten que puedas interpretar con IA generativa ciertas estructuras de tu modelo, además de poder crear los dashboard de forma bastante más ágil y más sencilla que hace unos años".

CUANDO LA NUEVA IA YA ES UNA REALIDAD

Por su parte, Rafael Socorro, head of data & analytics de ACCIONA Construcción, distinguió entre el valor inmediato y la transformación profunda

CÉSAR RAMOS, MAKING SCIENCE

“El principio que seguimos es build for change: asume que todo lo que construyas va a cambiar dentro de poco”

César Ramos, business intelligence area manager en Making Science, detalla cómo las empresas presentes en la mesa redonda apuestan en gran medida por los entornos multicloud, lo que les permite cierta agilidad en el momento de tener que escoger por una nube u otra cuando surjan nuevas funcionalidades. También destaca de la mesa la necesidad de disponer de plataformas de datos, gobernados y centralizados, que estén listas para aplicar los modelos de IA.

Desde la compañía ofrecen una gestión integral del ciclo de vida del dato, desde Infrastrucuture as a Code o ciberseguridad hasta Data Ops, GenAI Ops o el contexto inteligente para que los modelos de IA funcionen bien. Para Ramos, “el gran reto que tienen las empresas es cómo construyes algo sólido y que resista este cambio. Vemos las plataformas de datos como edificios antisísmicos: son flexibles, absorben el cambio, no son reticentes a él.

> “LA INNOVACIÓN, LA INTELIGENCIA ARTIFICIAL Y LAS PLATAFORMAS DE DATOS TIENEN QUE SER ÁGILES Y TIENEN QUE ESTAR PREPARADAS PARA EL CAMBIO”

CÉSAR RAMOS
Business intelligence area manager, **Making Science**

Clica en la imagen para ver la galería completa

que ofrece la IA: “Si bien la utilidad de los agentes de IA para la consulta de datos es un punto de partida claro y aceptado por todos, el verdadero potencial transformador reside en que estos agentes modifiquen la forma en que opera la compañía en su núcleo. Y ahí es donde el desafío es mayor. Un proyecto que facilita el autoservicio tiene una acogida excelente, pero la verdadera evolución llega cuando se rediseñan procedimientos y flujos de trabajo para introducir automatización de alto impacto.

Es aquí donde puede surgir una lógica resistencia al cambio. Esto nos obliga a elevar la conversación más allá de la tecnología: exige un planteamiento estratégico de alto nivel sobre qué modelo de compañía queremos construir para el futuro”.

La inteligencia artificial es una realidad ante la que no puedes ponerte antiojeras. Lo que no significa que su

RESPONDIENDO A LOS RETOS DEL SECTOR

VÍCTOR MANUEL GAGO, SCHNEIDER ELECTRIC

“Queda mucho por hacer, desde añadir más controles y segmentar servicios a controlar los accesos dentro de las redes industriales”

Víctor Manuel Gago, datacenter and C&SP sales manager de Schneider Electric, destaca que los ponentes de la sesión tenían muy claros los beneficios y los inconvenientes de los diferentes modelos de arquitectura de datos, apostando la mayor parte de ellos por arquitecturas híbridas. Aunque los retos a los que se enfrentan las organizaciones son similares, en la mesa llamó la atención algún ejemplo más avanzado de uso de la IA agéntica, entre otras cosas para suplir el reporting tradicional.

Gago explica que en Schneider Electric, “como lideres en sostenibilidad y gestión de la energía y la automatización, somos un partner tecnológico que puede ayudar a las empresas en sus retos de arquitectura de datos. Tanto si están pensando en poner sus datos en la nube como si lo tienen que complementar con infraestructura on-premise o edge. Podemos ayudarles en todo el diseño y el mantenimiento de sus infraestructuras críticas, desde la red hasta el chip, la refrigeración y el control”.

«

> “INCORPORAMOS LA FIGURA DEL DATA BUSINESS PARTNER, QUE REPORTA JERÁRQUICAMENTE A DATA, PERO FUNCIONALMENTE A CADA UNO DE LOS NEGOCIOS”

VÍCTOR MANUEL GAGO
Datacenter and C&SP sales manager, **Schneider Electric**

adopción no pueda ser prudente. Héctor Víctor, director de data analytics en Vithas, recuerda que “la llegada de la IA ha distorsionado el escenario que teníamos. Han surgido muchas iniciativas, algunas de negocio; unas tienen que ver con la IA generativa, otras con la IA más tradicional, con temas de machine learning y deep learning. Este hecho implica que tienes que mover datos a otras unidades de negocio y en cierta medida puedes perder el control de los datos y su trazabilidad. Por eso, tendemos a modelos híbridos, en entornos multicloud donde podamos utilizar y aprovechar las ventajas que nos proporcionan cada una de las tecnologías, estableciendo un modelo estricto de gobierno del dato y creando estructuras regulatorias orientadas al gobierno de la IA, creando para ello un comité en el que se deciden y evalúan qué proyectos se van a realizar”.

Hemos dejado para el final el que quizá fue el caso más maduro de adopción de la inteligencia artificial

»

que estuvo sobre la mesa. Jorge Valero, director de aplicaciones y data de AEDAS Homes, explica que “la nube nos ha dado ventajas adicionales, sobre todo en el campo de la IA. Estamos cambiando las herramientas de BI por agentes de IA. Los empleados tienen acceso a IA agéntica, que les permite hacer tareas, consultar directamente el data warehouse. Hemos dedicado mucho tiempo y esfuerzo a que la capa semántica sea hecha, bastionada y gobernada por la gente de negocio, no por tecnología. Ellos son los encargados de darle calidad no solamente al dato, sino a la semántica, porque ven que tiene un sentido cuando van a hacer consultas directamente a los informes. Hemos pasado de dos informes por persona a 80 para 300 empleados. 200 de ellos utilizan a diario nuestros agentes de data. La nube está dando unos beneficios espectaculares desde punto de vista de eficiencia operativa”.

Datos, nube, IA, tradicional y generativa, IoT, automatización... Y datos otra vez. En los últimos años ha habido una enorme evolución en la cuestión crucial del gobierno de los datos. No hace mucho eran proyectos muy interesantes, pero más o menos modestos, a los que les costaba sacar un compromiso claro de la alta dirección y también un pedacito de los presupuestos. En estos momentos se ve una mayor madurez. Por supuesto, con margen de mejora, pero con planteamientos muy bien encaminados. ■

#ENCUENTROSITDMGROUP

Clica en la imagen para ver la galería completa

MÁS INFO +

» Encuentros ITDM Group: Apostando por una estrategia de datos inteligente

» Making Science

» Descubre la refrigeración líquida

» Self-service BI: Del mito a la realidad con Agentes Conversacionales

» Schneider Electric presenta su nueva línea de soluciones para centros de datos

COMPARTIR EN REDES SOCIALES

Crayon

Descubre el poder de la IA generativa y convierte los nuevos retos de tu negocio en oportunidades.

En esta guía descubrirás:

- Cómo identificar los casos de uso y evitar los problemas de principiantes.
- Las claves para una IA responsable, ética y alineada con la normativa.
- Ejemplos de casos reales en diferentes sectores como sanidad, finanzas, sector público, educación, etc.

Accede al eBook

APOSTANDO POR UNA ESTRATEGIA DE DATOS INTELIGENTE

Para avanzar hacia modelos data-driven las empresas necesitan replantear la estrategia en torno al dato y la propia arquitectura de TI, para facilitar la captura de información relevante y su posterior uso. Pero este cambio también tiene otras derivadas en el campo de la ciberseguridad, el cumplimiento normativo y la gestión del talento tecnológico.

MESA REDONDA >> Debatimos, junto a expertos de Crayon, PUEDATA, QNAP y SonicWall, cómo las empresas están redefiniendo sus estrategias de datos para sacar partido de la inteligencia artificial en su transición hacia un modelo data-driven, y sobre los desafíos que encuentran.

El volumen de datos que manejan las organizaciones es cada vez mayor y también lo es su potencial para modernizar el negocio, impulsar la eficiencia, la innovación digital y la competitividad. Para sacar partido de estas ventajas, las empresas necesitan evolucionar hacia modelos data-driven, un cambio al que acompañan importantes desafíos que trascienden la dimensión tecnológica. De estas y otras cuestiones hablamos en esta mesa redonda, enmarcada en los 'Encuentros ITDM Group: 'Apostando por una estrategia de datos inteligente', en la que han participado Álvaro Montoya, data and IA sales executive de Crayon; Sergio Rodríguez, CTO de PUEDATA; Guillermo Alcover, regional sales specialist de QNAP; y Sergio Martínez, country manager de SonicWall.

DESAFÍOS EN TORNO AL DATO

Tradicionalmente, las organizaciones han tratado la información de forma desorganizada, desde su recopilación inicial hasta su uso final, pasando por todas las etapas de gestión, pero para avanzar hacia un modelo data-driven es necesaria una gestión del dato más holística e inteligente. Para Álvaro Monto-

ya, data and IA sales executive de Crayon, “el reto está no solo en la captación del dato primario, ya que, si queremos conseguir una visión radiográfica del cliente, de nuestro proveedor, no nos podemos quedar en esa capa”. Opina que “tenemos que llevar eso un paso más allá, y llevar una ordenación del dato, contextualizarlo para poder explotarlo con técnicas de inteligencia artificial y, más concretamente, analítica avanzada”.

Sergio Rodríguez, CTO de PUEDATA, explica que en la empresa moderna el dato se encuentra en muchos lugares, y el primer reto es “recolectar toda esa información proveniente de arquitecturas centralizadas o distribuidas”, para lo que es necesario “definir como parte de la estrategia un ciclo de vida de los datos”. Explica que, “no se trata solamente de disponer de la información, sino de qué va a suceder con ella dentro de dos años, cómo se va a seguir siendo viva”.

A esto, Sergio Martínez, country manager de SonicWall, añade “la responsabilidad de tener según qué datos y de qué forma se protegen” para garantizar el cumplimiento con normativas como NIS2, DORA o

Clica en la imagen para ver la galería completa

GDPR, algo que en su opinión pasa por securizar mejor las infraestructuras tanto en la empresa como en la cadena de suministro, y definir claramente la responsabilidad del dato.

Por su parte, Guillermo Alcover, regional sales specialist de QNAP, opina que “hay que tener en cuenta el gran crecimiento de datos a la hora de diseñar la estrategia de datos y la infraestructura subyacente”. Señala varios problemas en este sentido, como la necesidad de hacer una correcta selección de los datos para valorar cuáles son importantes y cuáles no, así como definir el plazo de tiempo durante el cual se deben mantener y proteger. Esto implica una mayor complejidad y mayores riesgos relacionados con la responsabilidad corporativa.

UNA NUEVA FORMA DE ENTENDER LA GESTIÓN

Para todos los portavoces queda claro que en el camino a seguir para lograr una estrategia de datos más inteligente y productiva, las organizaciones necesitan replantear completamente la gestión de datos y apoyarse en la inteligencia artificial para diferentes etapas del ciclo de vida de la información. Sergio Rodríguez, de PUEDATA, identifica la IA generativa como una de las tecnologías más importantes en este campo, pero matiza que antes es imperativo asegurar la calidad de los datos porque “si no tienes la información controlada con responsabilidad, con seguridad, con la calidad requerida, al final se produce el denominado trash-in trash-out”, según el cual, si la información no es buena, el resultado de procesarla tampoco lo será.

Álvaro Montoya, de Crayon, se muestra de acuerdo y pone énfasis en la importancia de asentar las premisas de los proyectos de IA. Considera que se debe tener “una arquitectura del dato que te permita, a través de plataformas analíticas del dato, saber dónde tienes todo centralizado, cubrir todo su ciclo de vida”, abarcando desde la

> A PARTIR DE 2026 IREMOS HACIA UNA INDUSTRIALIZACIÓN DE LOS CASOS DE USO Y LAS PRUEBAS DE CONCEPTO DE IA

ÁLVARO MONTOYA
data and IA sales executive de **Crayon**

> ES CASI IMPOSIBLE PROCESAR O ENTENDER LA CANTIDAD DE DATOS QUE SE GENERAN HOY EN DÍA SIN LA IA

SERGIO RODRÍGUEZ
CTO de **PUEDATA**

captura, la ingesta, el almacenamiento, la federación del dato en espacios de datos, la virtualización, y el gobierno".

LAS EMPRESAS NECESITAN ADOPTAR LA IA

Otro punto en el que coinciden estos expertos es que España la adopción de la inteligencia artificial está por detrás de otras economías desarrolladas, y abogan por impulsar esta modernización, pero de la forma correcta. Así lo cree Guillermo Alcover, de QNAP, para quien "muchas empresas han dado un salto muy grande directamente, sin

Clica en la imagen para ver la galería completa

hacer el recorrido habitual, o el paso a paso", acelerando la adopción de la IA sin diseñar una estrategia adecuada y "eso ha llevado a problemas de implementación y a una utilización incorrecta" que ha conducido a muchas a dar un paso atrás.

Lo mismo percibe Álvaro Montoya, de Crayon, quien añade que "desde la irrupción de la IA generativa ha habido una fase de exploratoria", donde muchas empresas han evaluado qué podía aportar esta tecnología, pero "en 2025, estamos entrando en una fase de madurez inicial, donde se empiezan ya a ver proyectos piloto, pruebas de concepto, de esos asistentes virtuales, con un cometido claro". Y, opina, "a partir de 2026 iremos hacia una industrialización de los casos de uso y las pruebas de concepto de IA que se han identificado".

Sergio Rodríguez, de PUEDATA, opina que entre 2024 y 2025 ha habido una enorme evolución en el campo de la IA generativa, y que "es casi imposible procesar o entender la cantidad de datos que se generan hoy en día

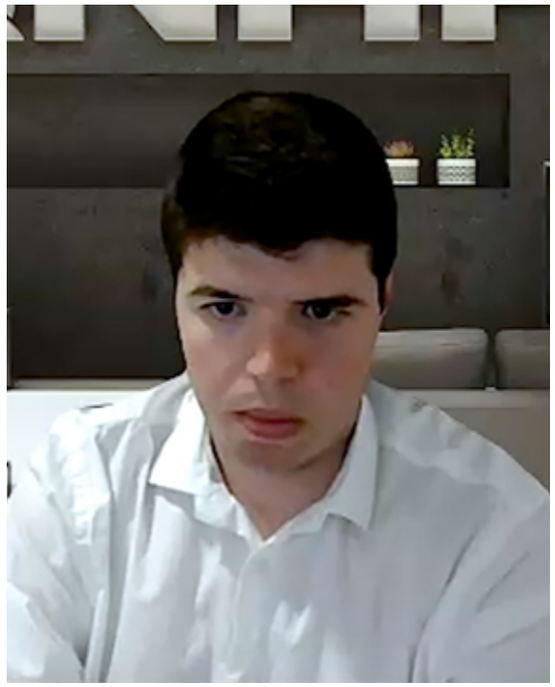
Clica en la imagen para ver la galería completa

sin la ayuda de la inteligencia artificial". Actualmente, dice, solo se utiliza entre un 30% y un 40% de la información que se produce y cree que es precisa una mayor madurez tecnológica, algo que se alcanzará gracias a la IA agéntica a partir de 2026.

Coincide con esta percepción Sergio Martínez, de SonicWall, para quien se ha logrado un gran avance

> HAY QUE TENER EN CUENTA EL CRECIMIENTO DE DATOS A LA HORA DE DISEÑAR LA ESTRATEGIA Y LA INFRAESTRUCTURA

GUILLERMO ALCOVER
regional sales specialist de **QNAP**



> HAY QUE APLICAR ESTRATEGIAS ZTNA Y CONSTRUIR EL ACCESO A LOS RECURSOS Y A LOS DATOS BASÁNDOSE EN CONFIANZA CERO

SERGIO MARTÍNEZ
country manager en
SonicWall España

desde el machine learning tradicional, por ejemplo en el ámbito de la ciberseguridad, a las nuevas formas de IA, que "son sistemas especializados, entrenados con tus propios datos y circunscritos a un tipo de actuaciones concretas", pudiendo aportar mucho valor a las organizaciones.

INTELIGENCIA APLICADA A LA CIBERSEGURIDAD

No se puede hablar de inteligencia artificial y datos sin tener muy presente la ciberseguridad, ya que la IA se utiliza tanto para atacar como para defender, somo señala Sergio Martínez, de SonicWall. Recalca que las empresas siempre van por detrás de "los malos", que aplican la inteligencia artificial para revitalizar "viejos tipos de ataques", principalmente para descubrir sistemas vulnerables o no parcheados, encadenar tipos de ataque sofisticados y ofuscar los ataques que ya han tenido éxito, para tener más tiempo de explotarlos.

Clica en la imagen para ver la galería completa

Destaca cómo "el cibercrimen se ha convertido en una industria muy fructífera, en la que hay auténticas empresas que sacan partido económico de esto". Frente a esto, recomienda construir una defensa por capas, "aplicando estrategias ZTNA para construir el acceso a los recursos y los datos basándose en confianza cero".

En QNAP, como comenta Guillermo Alcover, están notando un incremento de número de ataques, por lo que están "intentando concienciar más a las empresas y a las personas de la necesidad de tener copias de seguridad para proteger sus datos". Y recomienda "tanto prevenir, a nivel de seguridad activa, para evitar que estos ataques entren, como aplicar las medidas de protección que hay detrás, para permitir recuperar esos datos".

Clica en la imagen para ver la galería completa

Sergio Rodríguez, de PUEDATA, coincide en la mayor sofisticación de los ataques y en el uso creciente de la IA para potenciarlos y personalizarlos, basándose en el engaño. Por ello, apunta, "no queda otra que un tema de concienciación y de educación, y de training dentro de las empresas a la hora de fomentar todo esto, pero luego también proteger la informa-

Clica en la imagen para ver la galería completa

ción que se expone hacia el exterior", teniendo toda la superficie de ataque absolutamente controlada.

PROPUESTAS DE LA INDUSTRIA EN TORNO AL DATO

Los cuatro portavoces nos detallan cuáles son sus propuestas y novedades en torno al dato de cara al resto de 2025. Guillermo Alcover (QNAP), comenta que "en nuestros sistemas de almacenamiento, aplicaremos inteligencia artificial a las herramientas de búsqueda", trabajando con LLM de empresas externas, "y también estamos trabajando en uno propio para facilitar la búsqueda del dato interno y poder conversar de alguna manera con todos los datos que tenemos dentro de equipos QNAP". Y, en cuanto a la ciberseguridad, seguirán centrándose en la inmutabilidad del dato para "conseguir que todas las empresas y las personas puedan tener sus datos protegidos dentro de un equipo".

Álvaro Montoya (Crayon), dice que se centrarán en cuatro áreas principales de su propuesta a valor. La primera, "muy orientada a modelos generativos por vertical, por sector de actividad, que sean integrables con las principales arquitecturas de datos de los principales hiperescalares". También apostarán por el uso de agentes de IA basados en el análisis de documentación interna, por "un gobierno del dato orientado a espacios de datos, para espacios de datos de sectores como Turismo, Sanidad y Agroalimentario" y, por último, "FinOPs y DataOps para optimizar tanto la infraestructura del dato como el consumo de ese dato".

En PUEDATA, como comenta Sergio Rodríguez, se están volcando en el uso de IA generativa y agéntica para "una vez que toda la infraestructura que hay por debajo está ordenada, clasificada, bien preparada y optimizada, poder utilizar IA generativa para poder conversar con tus datos, estén donde estén". Y, añade, "es fundamental que la parte de analítica esté apoyada por IA generativa" para "sacar valor de la información que tienes".

Finalmente, Sergio Martínez (SonicWall), explica que tienen novedades en sus tres líneas de producto actuales: en el área de firewalls, en el segundo semestre lanzarán nuevos dispositivos a los que incorporarán la generación 8, añadiendo prompts a su plataforma de gestión para poder hacer preguntas sobre el estado de la infraestructura y presentarán novedades para endpoints y seguridad de la red. En el área de negocio de servicios gestionados, añade, "seguiremos incorporando nuevos entornos para nuestro SOC as a service, para los partners", "impulsando todo tipo de sistemas, incorporando nuevas marcas y soporte para nuevas marcas". Por último, "en la línea de Cloud Secure Edge, que es pago por uso, sacamos una versión nueva y seguiremos potenciándolo" para proteger el acceso a datos basándose en ZTNA. ■

MÁS INFO +

» Encuentros ITDM Group: Apostando por una estrategia de datos inteligente

COMPARTIR EN REDES SOCIALES

SONICWALL®

2025 Informe de Ciberamenazas de SonicWall

LA NECESIDAD DE RAPIDEZ Y DE ALIADOS FUERTES PARA SUPERAR EL CAMPO DE BATALLA DE LA CIBERSEGURIDAD

El panorama de las amenazas sigue evolucionando a un ritmo sin precedentes, sin dejar inmune a ninguna organización.

Muchos de los ataques destacados en este informe pueden prevenirse con una higiene de ciberseguridad sólida. Tomar medidas proactivas puede mejorar en gran medida su postura de seguridad. Descubra cuáles son en el Informe de Ciberamenazas 2025 de SonicWall.

DESCARGUE EL INFORME COMPLETO

JORGE VALERO, DIRECTOR DE APLICACIONES Y DATA EN AEDAS HOMES

“Incluimos IA generativa en los procesos donde tuviera sentido, con un ROI claramente positivo”

ENTREVISTA >> Jorge Valero, de AEDAS Homes, explica cómo el sólido trabajo previo con los datos de la compañía les ha servido para desplegar una eficaz estrategia de inteligencia artificial agéntica.

Cerramos este Encuentro ITDM Group con esta entrevista a Jorge Valero, director de aplicaciones y data en AEDAS Homes. Esta promotora inmobiliaria de obra nueva, con más de 5.200 viviendas entregadas en el último ejercicio, nació en 2016 y tiene entre sus principios rectores la sostenibilidad y la innovación, tanto en lo que se refiere a los métodos modernos de construcción como a la digitalización interna, con un excelente trabajo realizado tanto en el ámbito de los datos como en el de la inteligencia artificial.

EL DATO, UN ACTIVO MÁS DE LA COMPAÑÍA

El proceso de digitalización en el que está inmersa la compañía arrancó hace cinco años, cuando dieron

el paso de construir su primer Data Warehouse para que los datos se convirtieran en activos útiles para diferentes áreas de AEDAS Homes, desde las unidades de negocio hasta la financiera o la propia de tecnología. Gracias a ese trabajo inicial, pudieron añadir una capa de Business Intelligence, desplegada para toda la organización. Un planteamiento, además, que resultó fundamental para la siguiente ola tecnológica, la inteligencia artificial generativa.

Como explica Valero, "con la explosión de la IA generativa nos hemos dado cuenta de que era un trabajo que tenía aún más sentido, porque ahora nos permite activar el dato para proyectos de innovación, para poder generar agentes IA en cuestión de semanas". Los dos factores que más han favorecido el exitoso despliegue de la IA generativa que está realizando la compañía son esa base previa de trabajo que había hecho sobre los datos y el apoyo de la alta dirección, que ha adoptado la IA como parte de la estrategia corporativa.

EL EQUIPO IA EN ACCIÓN

En esta estrategia, "lo primero que hemos hecho es formar un equipo de IA, precisamente para poder entender, desde un nuevo prisma, cómo son los nuevos retos que tenemos como organización". Un equipo del que formaba parte el Comité de Dirección de la empresa; es más, cada uno de los miembros del CODIR patrocinaba un proyecto de IA, transmitiendo el mensaje de que este proceso tan transformador no era un capricho de TI, sino una estrategia corporativa de pleno derecho.

De ese equipo surgieron más de 180 ideas, con las que se definió una estrategia a largo plazo en diferentes etapas, "con unas luces cortas, medias y largas. Las cortas eran muy sencillas: incluir tecnología de IA generativa en todos los procesos, allá donde tuviera un sentido, con un ROI claramente positivo". Identificaron casos de uso y la inteligencia artificial se fue incorporando en procesos como la atención al cliente, la captura de datos o la conversión de datos no estructurados en estructurados.

MAX, EL AGENTE DE IA PARA LOS EMPLEADOS

Otro de los ejemplos más llamativos es la creación de Max, un agente de IA que presta su servicio a los empleados de la compañía. Entre otras funcionalidades, Max es el primer punto de contacto del soporte técnico interno. Valero explica que "cuando tienen un problema en una aplicación, hablan con MAX, que tiene por detrás a muchos agentes IA que hacen tareas. Hay un agente de soporte que identifica el problema y busca dentro de todos los manuales una posible solución. Si no es el caso, sin preguntar, crea el ticket automáticamente y al equipo de soporte le da toda la información de contexto (manuales, guías, capturas de pantalla) para que puedan resolver el problema en menos tiempo".

Más allá de la sencillez de la interacción por voz, la solución supone considerables ahorros de tiempo para los empleados. "Esos ahorros de tiempo, esa eficiencia operativa es donde vemos que hay un potencial aún enorme en todas las compañías, para que veamos cambios en la forma de hacer los cientos de procesos que todavía tenemos que gobernar. Ya no solo introducir tecnología, sino volver a pensar el proceso desde el inicio y ver todo lo que podemos hacer para simplificarlo". ■

> "TODAS LAS SEMANAS HACEMOS FORMACIÓN DE IA PARA EMPLEADOS PARA QUE VAYAN ADQUIRIENDO NUEVOS CONOCIMIENTOS"
>
> **JORGE VALERO,** director de aplicaciones y data en **AEDAS Homes**

MÁS INFO +

» Jorge Valero, AEDAS Homes

COMPARTIR EN REDES SOCIALES

PRINCIPALES TENDENCIAS EN TORNO A LA CIBERSEGURIDAD EN 2025. LA VISIÓN DEL MAYORISTA

La ciberseguridad se ha convertido en una prioridad para las organizaciones, tanto por el aumento de las amenazas y su peligrosidad como por las nuevas regulaciones europeas en esta materia. En este contexto, necesitan apoyarse en socios que garanticen la protección de sus sistemas y el cumplimiento normativo, y el canal se presenta como actor clave para brindar todo esto al cliente final. En el Debate IT Reseller 'Principales tendencias en torno a la ciberseguridad en 2025' hablamos de todas estas cuestiones en un completo programa compuesto por dos mesas redondas y varias entrevistas. Comenzamos con un debate centrado en la visión del mayorista, en el que contamos con Víctor Orive, CEO de ADM Cloud & Services; Ángel García, networking & security business unit manager de Arrow Enterprise Computing Solutions; Javier Jurado, director de desarrollo de negocio de Exclusive Networks; Martín Trullás, director de advanced solutions de

DEBATE IT >> Debatimos junto a representantes de ADM Cloud & Services, Arrow Enterprise Computing Solutions, Exclusive Networks, Ingram Micro, TD SYNNEX y V-Valley sobre el desarrollo del mercado de ciberseguridad en España y las principales tendencias en este segmento dentro del canal, como el avance hacia la prestación de servicios gestionados.

Clica en la imagen para ver la galería

Ingram Micro; Alejandro Benito Sánchez, director de seguridad y networking de TD SYNNEX; y David Gasca, head of marketing & operations cybersecurity de V-Valley.

DESARROLLO DEL MERCADO

Según las últimas cifras, el mercado español de ciberseguridad creció en 2024 un 14,2%, lo que representa un aumento del 70% con respecto a 2020, y todo parece indicar que esta tendencia se mantendrá en 2025. Para David Gasca, de V-Valley, la digitalización está siendo un motor del mercado cyber, ya que cada vez hay más sistemas a proteger y más mercado que cubrir, a lo que se suma una mayor concienciación por parte de las empresas. Opina que el mercado seguirá creciendo al ritmo previsto, y que se avanza hacia una mayor profesionalización en este segmento.

Alejandro Benito, de TD SYNNEX, confirma el crecimiento en la primera mitad de 2025 y, aunque espera un ritmo más tranquilo en el segundo semestre, prevé que en 2026 se alcanzará de nuevo el doble dígito. A esto añade que el crecimiento se está notando especialmente en el canal, y que el mayorista está adoptando un rol cada vez más importante en el segmento de ciberseguridad, gracias a su apuesta por la especialización y su mayor colaboración con los partners.

Desde Ingram Micro, Martín Trullás señala que sus cifras en este segmento han superado el 10%, y señala cómo las empresas están invirtiendo más para hacer frente a las amenazas cada vez más sofisticadas. Y para ello demandan que los partners les ofrezcan servicios gestionados de ciberseguridad, especialmente las pymes, que no cuentan con recursos propios para protegerse adecuadamente, y cada vez son más consciente de ello.

Como explica Javier Jurado, en Exclusive Networks han registrado cifras superiores a la media registrada por Context el año pasado, y señala que “el secreto está en la disrupción tecnológica” que permite hacer más cosas y disponer de nuevas soluciones para proteger una superficie de ataque cada vez mayor. Sus previ-

TRANSFORMA TU NEGOCIO CON LA TECNOLOGÍA DEL FUTURO

ADM Cloud & Services

Infraestructura Cloud · Ciberseguridad · Servicios Gestionados

Soluciones digitales seguras, escalables y personalizadas.
Gana agilidad, eficiencia y protección real.

La nube es el presente. Nosotros somos tu futuro.

> LA ÚNICA MANERA DE DAR UNA COBERTURA INTEGRAL A LAS PYMES ES MEDIANTE LA ASOCIACIÓN Y COLABORACIÓN ENTRE PARTNERS

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

> CRECE LA INVERSIÓN EN CIBERSEGURIDAD, PERO TAMBIÉN CRECE EL PORCENTAJE DE INVERSIÓN DE LOS CIBERDELINCUENTES

ÁNGEL GARCÍA,
networking & security business unit manager de **Arrow Enterprise Computing Solutions**

Clica en la imagen para ver la galería

siones para el segundo trimestre del año son buenas y prevé un aumento de cara a la segunda mitad del año.

Ángel García, de Arrow Enterprise Computing Solutions, se muestra de acuerdo en el gran potencial del mercado y sus perspectivas para este año son muy buenas. Explica que "hemos crecido a lo largo de los años y el mercado espera tener un impacto positivo gracias a las inversiones en sector público, especialmente en Defensa". Y, puntualiza que "crece la inversión en ciberseguridad, pero también el porcentaje de inversión de los ciberdelincuentes", por lo que es necesario seguir apostando por la seguridad.

Coincide con esta perspectiva Víctor Orive, de ADM Cloud & Services, quien destaca el crecimiento tradicional a doble dígito en el segmento de ciberseguridad, también en su compañía. Explica que, al estar muy focalizados en los servicios gestionados, perciben cómo la digitalización está impulsando el gasto de las empresas en ciberseguridad, ya que ven la inversión en este campo como una necesidad para protegerse ante las nuevas amenazas digitales.

CONCIENCIACIÓN SOBRE SEGURIDAD

Los participantes en este debate perciben en general que la concienciación sobre la importancia de la ciberseguridad es cada vez mayor entre las empresas españolas, desde las grandes hasta las pymes, que tienen cada vez más claro el peligro de las ciberamenazas. Víctor Orive destaca que "el empresario o el gerente se preocupa mucho más de ver hasta qué punto su empresa es vulnerable a ese tipo de riesgos".

Coincide Javier Jurado, de Exclusive Networks, pero añade que, "aunque aumenta la concienciación, todavía tenemos por delante un camino hacia la madurez", ya que todavía hay muchas que creen estar a salvo porque no se consideran

> PARTE DE LA LABOR DE LOS MAYORISTAS Y DEL CANAL, DE LOS PARTNERS, ES AYUDAR A CONCIENCIAR

JAVIER JURADO,
director de desarrollo de negocio de **Exclusive Networks**

> LOS MAYORISTAS SOMOS PIEZA CLAVE PARA EL DESARROLLO DE ESAS NUEVAS SOLUCIONES MSSP

MARTÍN TRULLÁS,
director de advanced solutions de **Ingram Micro**

Clica en la imagen para ver la galería

un objetivo. Opina que el peligro no está solamente en las ciberamenazas, sino también en la falta de cumplimiento normativo, y afirma que “parte de la labor de los mayoristas y del canal, de los partners, es ayudar a entender que el perímetro de la ciberseguridad va mucho más allá de poner una primera barrera de firewalls”.

“La labor de los CISO y CSO es en parte hablar con el director financiero y el CEO de que la ciberseguridad no un gasto, es una inversión”, en palabras de Martín Trullás, de Ingram Micro. Opina que no todos lo han entendido, y para muchos este conocimiento llega tras un ataque, y se dan cuenta de que deberían haber invertido más en protegerse.

Ángel García, de Arrow Enterprise Computing Solutions, opina que las nuevas regulaciones están ayudando a cambiar el enfoque de reactivo a proactivo, impulsando la concienciación, algo que comenzó en las grandes compañías y ha ido extendiéndose a las pymes. Aunque afirma que “es bueno seguir concienciando y nuestra labor y la de los partners es transmitir la idea de que nadie está libre de esto”.

Clica en la imagen para ver la galería

El mercado y las empresas han alcanzado más madurez, opina David Gasca, de V-Valley, porque “ya hay soluciones que permiten hacer un análisis de la exposición de riesgos, ver dónde están los puntos débiles y dónde afrontar las siguientes inversiones”. Y apunta que los clientes apuestan cada vez más por eso, y por el cumplimiento normativo en ciberseguridad, así como por un enfoque más proactivo.

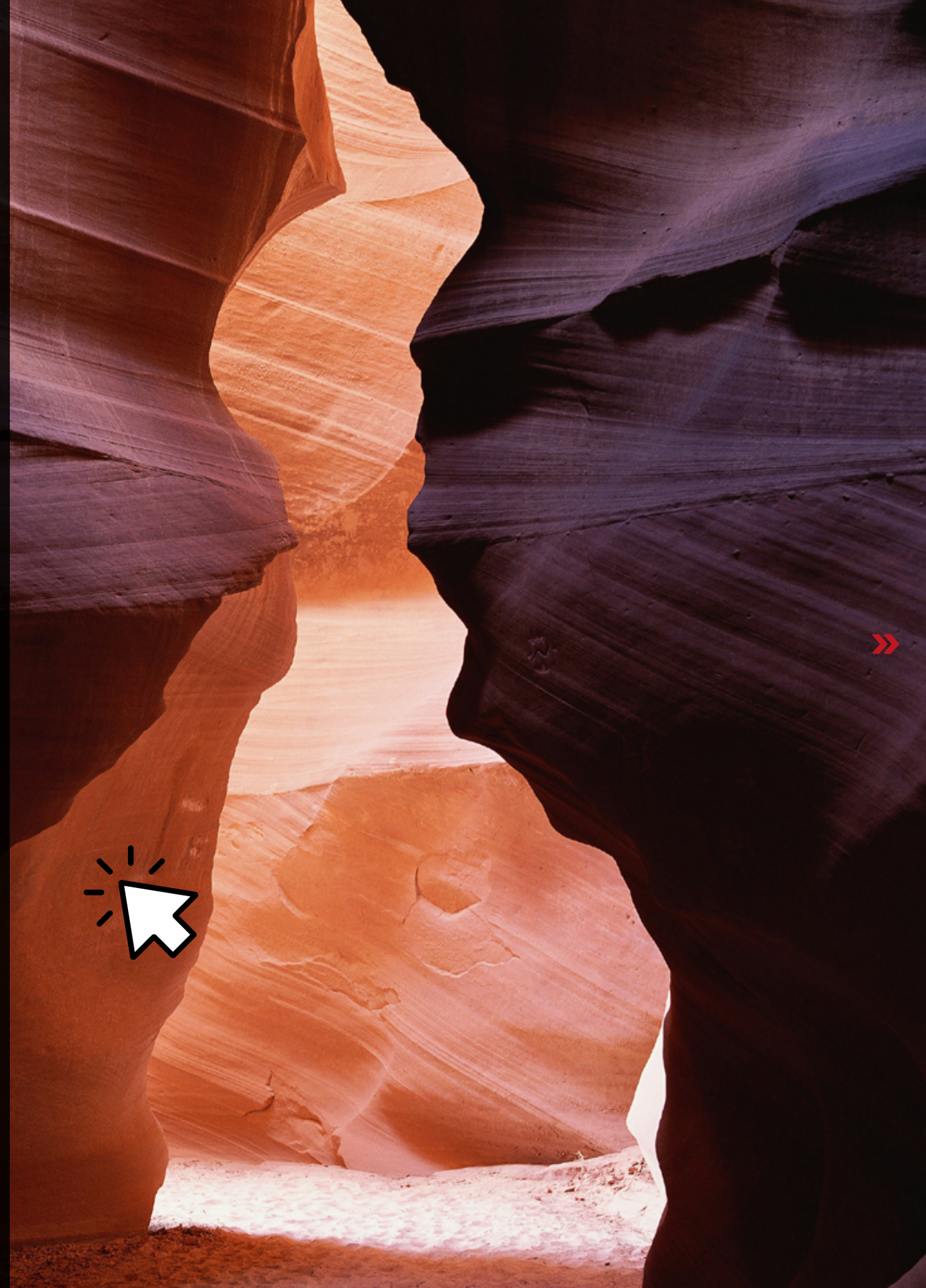
Se muestra de acuerdo Alejandro Benito, de TD SYNNEX, en que “el mercado y las personas dentro de las empresas han madurado en la cultura de la ciberseguridad”. Pero también opina que falta mucho por crecer, y que desde los mayoristas pueden ayudar a seguir concienciando sobre los peligros de no protegerse adecuadamente, “porque nos

Añada una capa inteligente a la seguridad

Nuestros expertos le pueden ayudar a proporcionar inteligencia a las operaciones de sus clientes, para **una respuesta ante amenazas más rápida y coordinada**.

arrow.com/globalecs/es

ARROW



están atacando a todos las continuamente".

IA EN CIBERSEGURIDAD

La inteligencia artificial está encontrando diferentes aplicaciones en ciberseguridad, tanto desde la parte de los atacantes como de los proveedores de seguridad. Alejandro Benito, de TD SYNNEX, aclara que, según datos de IDC, el 80% de las empresas relacionadas con TI ya están haciendo pruebas de concepto con inteligencia artificial, pero solo el 25% lo está intentando llevar a producción", y solo un 1%-2% están usando datos propios. Opina que "tenemos mucho que hacer alrededor de la IA y nos va a ayudar mucho en el área de ciberseguridad".

"La inteligencia artificial hace que los ataques sean más sofisticados, más difíciles de detectar", comenta Ángel García, aunque "por otro lado, los fabricantes ya están implementando esa IA para poder detectarlos de una forma proactiva", y considera que esta tecnología "ha venido para quedarse, para ayudar en muchos procesos básicos", permitiendo que las empresas se enfoquen en otras cosas. Lo mismo opina Martín Trullás, de Ingram Micro, para quien

Clica en la imagen para ver la galería

"ni nosotros, como mayoristas, ni los fabricantes, ni los propios que están ahora haciendo POC, saben hasta dónde va a llegar el nivel de automatización en las empresas". Pero pone sobre la mesa la falta de profesionales cualificados en esta materia, particularmente en el área de ciberseguridad. Por ello, cree que "los mayoristas tenemos que

> "TENEMOS MUCHO QUE HACER ALREDEDOR DE LA IA Y NOS VA A AYUDAR MUCHO EN EL ÁREA DE CIBERSEGURIDAD"
>
> **ALEJANDRO BENITO SÁNCHEZ,** director de seguridad y networking de **TD SYNNEX**

trabajar en la parte de formación y concienciación".

Javier Jurado, de Exclusive Networks, ensalza la labor de los fabricantes, que llevan muchos años trabajando con modelos de machine learning y deep learning, por lo que no son novatos en el campo de la inteligencia artificial. Y alerta de los peligros de fuga de datos al alimentar estos modelos con información sensible de las organizaciones, y de que "sí falta gente cualificada y tenemos un reto como canal para formar y habilitarlos".

Para David Gasca, "la IA generativa viene a ser la revolución industrial del mundo digital", y está avanzando gracias a herramientas que permiten industrializar la tecnología. Considera que, aunque genera riesgos en cuanto a la destrucción de puestos de trabajo tradicionales, "permitirá también la creación y llegada de nuevos tipos de profesiones o especializaciones", también en el área de ciberseguridad.

EVOLUCIÓN DEL CANAL

El segmento de ciberseguridad en el canal también está evolucionando hacia los servicios gestionados y una cierta consolidación. Ángel García, de Arrow Enterprise Computing Solutions, opina que "hay muy pocas empresas o muy pocos partners capaces de cubrir todas las necesidades del cliente", lo que fomenta la especialización y la colaboración entre socios del canal, pero también una cierta consolidación. En este contexto, comenta, "la figura de MSSP cobra una relevancia muy importante, porque va a ser su socio de la parte de ciberseguridad". Por ello, desde la plataforma Arrowsphere están ampliando la lista de fabricantes para brindar a los partners la posibilidad de ofrecer a sus clientes ciberseguridad en modalidad de pago por uso.

Desde Ingram Micro, Martín Trullás percibe que ahora “se está viendo una consolidación de los integradores, los partners”, con “empresas muy especializadas, muy de nicho, que están siendo incorporadas a grandes empresas”. Y afirma que “el mercado, los fabricantes, nos están empujando a desarrollar soluciones MSSP” y que, “al final, los mayoristas somos pieza clave para el desarrollo de esas nuevas soluciones”.

Javier Jurado, de Exclusive Networks, recalca que “en España seguimos siendo un país de pymes, tanto de cliente final como de partners, y que, como mayoristas tenemos un rol muy relevante para facilitar esa colaboración entre partners que no se conocen, y que dominan determinada tecnología”. Por ello, señala, en su compañía se enfocan en ampliar la lista de partners con los que trabajan porque creen que hay una gran oportunidad para acercar a las pymes las tecnologías que tradicionalmente solo llegaban a las grandes empresas.

Por su parte, Víctor Orive opina que la consolidación se está produciendo a todos los niveles, desde el fabricante, al mayorista y los partners, y cree que “la única manera de

Clica en la imagen para ver la galería

poder dar una cobertura integral a las pequeñas empresas es mediante la asociación y colaboración entre partners”, algo que apoyan desde ADM Cloud & Services a través de su plataforma, ayudándolos a que “puedan abordar proyectos integrales para pymes”.

Desde V-Valley, como comenta David Gasca, reconocen la necesidad del canal de ofrecer servicios gestionados, y precisamente la adquisición que hicieron de Lidera hace dos años estaba enfocada a “habilitar a los partners que quieren ser MSP, pero que todavía no quieren o no pueden invertir en las herramientas necesarias”. Y afirma que “el trabajo que tenemos para los próximos años es ayudar en la transición de los partners hacia un modelo de servicios gestionados”.

> “EL TRABAJO QUE TENEMOS PARA LOS PRÓXIMOS AÑOS ES AYUDAR EN LA TRANSICIÓN DE LOS PARTNERS HACIA UN MODELO MSP”

DAVID GASCA,
head of marketing & operations cybersecurity de **V-Valley**

En el caso de TD SYNNEX, como aclara Alejandro Benito, con la compra de Ajoomal buscaban incrementar el nivel de servicio de los fabricantes con los que ya trabajaban, ofrecer una oferta diferente a los MSP a través de una plataforma y fomentar la colaboración en el canal. Considera que el rol actual de mayorista es el de “orquestador entre todos estos tipos de partners”, porque “estamos en un ecosistema en que los roles son múltiples y cambian muy rápidamente”.

PROPUESTAS DEL CANAL EN CIBERSEGURIDAD

Los seis portavoces nos han adelantado cuáles son sus propuestas y novedades en ciberseguridad para lo que resta de año, comenzando por Víctor Orive, quien nos explica que en ADM Cloud & Services se están centrando “en cumplimiento normativo, NIS2, DORA, CIS, ISO, ISO 26001”, y también “en todo lo relacionado con la privacidad”.

Ángel García, de Arrow Enterprise Computing Solutions, comenta dos puntos importantes: “seguir manteniendo los fabricantes líderes en el mercado dentro de nuestro porfolio, incorporando nuevos fabricantes”. Por otro lado, en la división comercial, “trabajar con partners, regionales o muy grandes, focalizados específicamente en alguno de los

EXCLUSIVE NETWORKS

Soluciones integrales. Soporte global. Siempre cerca.

Conectando experiencia y capacidad para proteger tu negocio, estés donde estés.

XGS
Exclusive Global Solutions

- +1.800 profesionales técnicos, incluyendo 600 ingenieros y 1.200 especialistas en ventas técnicas certificados
- Presencia local en más de 150 países
- Enfoque equilibrado: 1 técnico por cada 2 comerciales
- Red global de más de 10.000 ingenieros de confianza
- Centros logísticos en puntos estratégicos
- Formación en las principales tecnologías de ciberseguridad de nuestro portfolio

¡Descubre todo sobre nuestras formaciones!

productos de nicho que sean muy importantes para ellos, crecer con ellos y acompañarlos".

En exclusive Networks, Javier Jurado destaca que están apostando fuerte por las plataformas de los principales fabricantes para los grandes proyectos, y esperan obtener los frutos de estos esfuerzos en el segundo semestre. Por otro lado, a través de nuevos vendors que han incorporado a su catálogo, esperan un mayor acercamiento al mid-market con plataformas más sencillas y asequibles, y también brindar "soluciones tecnológicamente disruptivas, como la de microsegmentación automatizada, sin agentes".

En Ingram Micro, explica Martín Trullás, la estrategia seguirá girando en torno a su plataforma Xvantage, basada en el concepto de gemelo digital, donde continuarán incorporando más soluciones, entre ellas de ciberseguridad, para que el cliente pueda acceder a ellas a través de modalidades de pago por uso. Y aumentar la automatización para facilitar a los partners el acceso a los productos y soluciones de su catálogo. En el ámbito concreto de la ciberseguridad, comenta, seguirán ampliando su catálogo "con soluciones diferentes, disruptivas", "buscando complementar tipos de soluciones con más microsegmentación, mucho más de nicho".

Alejandro Benito apunta también a un enfoque de plataforma en TD SYNNEX, en su caso StreamOne, que seguirán desarrollando y mejorando. Además, explica, "hemos multiplicado por tres la inversión en recursos de ciberseguridad". En este sentido, durante el primer semestre han completado con éxito la integración de los equipos de trabajo de Ajoomal, y su objetivo para el resto de 2025 es "expandir todos los servicios y la formación", de una forma integrada, para dar cobertura a todos los partners y proveedores con los que trabajamos habitualmente".

Por último, David Gasca, de V-Valley, pone en valor su apuesta en los últimos 7 años por "tener el mejor equipo humano posible". Seguirán apostando por estos valores ya que considera que "es lo que te permite dar un mejor servicio a los partners con los que trabajamos, y es lo que está haciendo que los clientes y los fabricantes sigan queriendo trabajar con nosotros". Además, dice, seguirán "potenciando los servicios profesionales para apoyar al canal" y que "el partner pueda seguir evolucionando en su trayectoria, llegar a los canales donde vea más rentabilidad, y darle una cobertura en los servicios profesionales. ■

Clica en la imagen para ver la galería

MÁS INFO +

» Principales tendencias en torno a la ciberseguridad en 2025 - La visión del mayorista

COMPARTIR EN REDES SOCIALES

INGRAM MICRO®

Impulsando el futuro de la distribución

SIMPOSIUM

«JUEVES | 02-10-2025

Fira Barcelona »

Fira Barcelona Gran Vía

MÁS INFORMACIÓN

#IngramMicroSimposium

Víctor Orive, CEO de ADM Cloud & Services

"EN SEPTIEMBRE REFORZAREMOS NUESTRA OFERTA CON CUATRO NUEVOS PROVEEDORES"

Aprovechando su participación en este debate entrevistamos a Víctor Orive, CEO de ADM Cloud & Services, para hablar sobre las tendencias que están protagonizando el mercado de la ciberseguridad en 2025. En su opinión, "las amenazas que detectamos van básicamente desde el ransomware, con ataques cada vez más sofisticados, hasta el phishing y la suplantación de identidad. Los ataques de día cero, aprovechándose de las vulnerabilidades no conocidas, son otro de los vectores importantes de ataque que estamos detectando dentro de ADM Cloud & Services".

Para poder hacerles frente y "poder mitigar todas esas ciberamenazas, estamos abogando por sistemas Zero Trust que, por defecto, hacen que nada sea confiable, además de sistemas de doble factor de autenticación y segmentaciones de redes para evitar desplazamientos laterales".

Cerrada ya la primera mitad del año, "para el segundo semestre de este año 2025, apostamos por reforzar todas las soluciones que tenemos de ciberseguridad, sobre todo para hacer frente a la sofisticación de las amenazas. Nos estamos enfocando también en soluciones de ciberseguridad de cara a cumplimiento de normativas como NIS2, DORA, ISO 27001… y también en la privacidad".

"En el mes de septiembre", continúa, "vamos a lanzar al mercado dos fabricantes nuevos. Uno es DataGuard, un proveedor alemán principalmente orientado al negocio de ciberseguridad, cumplimiento y privacidad, y otro, en este caso holandés, Lupasafe, que se sitúa en la misma categoría de soluciones, pero con un foco más claro en la pequeña y media empresa. También vamos a incorporar a un fabricante muy conocido del mercado, Nord Security, especializado en VPN y en gestión de contraseñas. Y, por último, vamos a añadir a la oferta una solución de automatización de TI, Pulseway, un fabricante de origen indio que tiene su sede central en Estados Unidos".

Tal y como señala, "con este incremento del catálogo vamos a poder apoyar a nuestros partners para que cuenten con un abanico mayor de soluciones para defenderse de las amenazas del mercado".

TD SYNNEX

¿Listos para liderar el futuro de la ciberseguridad?

El momento es ahora.

Las soluciones y servicios gestionados de ciberseguridad no son una opción, son el pilar de cualquier estrategia y tu cliente los necesita. Descubre cómo te podemos ayudar en esta nueva realidad.

Contacta con TD SYNNEX y te ayudamos a liderar el futuro.

Security_ES@tdsynnex.com

David Gasca, head of marketing & operations cybersecurity de V-Valley

"QUEREMOS AYUDAR A LOS PARTNERS A SER MÁS RENTABLES"

Aprovechando su participación en este debate entrevistamos a David Gasca, head of marketing & operations cybersecurity de V-Valley, para hablar sobre las tendencias que están protagonizando el mercado de la ciberseguridad en 2025. En palabras de este responsable, "la mayoría de los ataques que estamos viendo son de ransomware, pero los ataques de disponibilidad de las páginas web o ataques de denegación de servicio son unos de los estamos viendo que se están incrementando en el mercado. Por tanto, proteger los activos digitales de las compañías es una de las prioridades que vemos ahora mismo".

Pero no son los únicos, y, como añade, "también los ataques dirigidos o de gran profesionalidad en las empresas son uno de los mayores peligros que podemos ver porque, con una gran cantidad de tiempo de ejecución consiguen grandes retornos y por eso siguen funcionando".

"Es muy importante", continúa, "encontrar empresas que tengan soluciones de ciberseguridad maduras para poder darse cuenta de cuándo les han entrado, intentar evitarlo y cambiar el enfoque proactivo. Porque el enfoque reactivo de las soluciones debe ir evolucionando a uno proactivo incrementando, además, la complejidad de las soluciones. Esto, que no es fácil, es lo que permite que podamos ir un pasito por delante y protegernos de una manera más inteligente".

Para David Gasca, "la prioridad de V-Valley, como los últimos 7 años, es invertir en un equipo más profesional y experto. Al final ha sido lo que ha garantizado nuestro éxito durante este tiempo, tener mejores personas, comerciales y técnicos, que es lo que nos está permitiendo ir al mercado cada vez con más éxito. Nuestro equipo comercial tiene una gran experiencia, y los equipos de servicios profesionales y el personal técnico, están haciendo que nuestra estrategia siga avanzando. Cada vez más fabricantes se acercan a nosotros para poder utilizar este equipo para incrementar su capacidad de llegada al mercado. También está la parte de servicios profesionales donde lo que queremos hacer, desde la adquisición de Lidera, que hicimos hace un par de años, es incrementar el apoyo que podemos dar a los partners con soluciones que ellos quieren dar y que todavía no se sienten cómodos para ofrecer".

En conclusión, "queremos ser ese partner de confianza, un aliado para complementar su negocio y permitirles acceder a negocios más rentables".

PRINCIPALES TENDENCIAS EN TORNO A LA CIBERSEGURIDAD EN 2025. LA VISIÓN DEL FABRICANTE

En la segunda mesa redonda del debate de IT Reseller titulado 'Principales tendencias en torno a la ciberseguridad en 2025', nos centramos en la visión de los mayoristas sobre el desarrollo del mercado, las últimas tendencias en ciberprotección para las empresas y la evolución de las propuestas de la industria y el canal en el segmento de ciberseguridad. Para ello contamos con Francisco Machuca, senior channel sales manager de Netskope; Carlos Castañeda, responsable de preventa y desarrollo de negocio de Serval Networks; Sergio Martínez, country manager de SonicWall; y Borja Pérez, country manager de Stormshield.

DEBATE IT >> Debatimos con portavoces de Netskope, Serval Networks, SonicWall y Stormshield sobre cómo está progresando el mercado de ciberseguridad en España, la evolución tecnológica y regulatoria y la transformación del canal en este segmento, hacia la consolidación y el modelo MSSP.

PROGRESO DEL MERCADO

El valor del mercado de ciberseguridad español, incluyendo hardware, software y servicios, alcanzó los 2.500 millones de euros en 2024, un 13% más que en 2023 y un 70% más que en 2020. Francisco Machuca, de

netskope

Seguridad moderna o rendimiento de la red. Sin concesiones.

Netskope es líder en seguridad moderna, redes y análisis. La arquitectura única de su plataforma Netskope One permite la seguridad en tiempo real basada en el contexto para personas, dispositivos y datos dondequiera que vayan, y optimiza el rendimiento de la red, sin concesiones ni sacrificios.

Miles de clientes y partners, entre ellos más de 30 de las 100 empresas de Fortune, confían en la plataforma Netskope One, su motor patentado Zero Trust Engine y su potente red NewEdge a fin de reducir riesgos, simplificar la infraestructura convergente y proporcionar visibilidad y control totales sobre la actividad de la nube, la IA, SaaS, la Web y las aplicaciones privadas.

Seguridad y redes reimaginadas

Visite netskope.com/es

Netskope, corrobora estos datos y recalca que la ciberseguridad se ha convertido “en un acelerador para la transformación digital, tanto de grandes empresas como de pymes”, ligada a la migración a la nube.

Carlos Castañeda, de Serval Networks, añade a esto el papel que están jugando las nuevas regulaciones en el impulso de la ciberseguridad, que están obligando a las empresas a incorporar nuevas soluciones de ciberseguridad para garantizar no solo su protección, sino el cumplimiento.

Desde el punto de vista de SonicWall, Sergio Martínez confirma un crecimiento interanual en 2024 similar a las cifras generales, y también con respecto a 2020. Desde entonces, dice, su mensaje ha sido muy similar: “apuesta por la defensa por capas, la visibilidad, el acceso remoto seguro, el detectar lo desconocido y que las pymes puedan acceder” a las tecnologías de ciberseguridad.

Borja Pérez, de Stormshield, coincide en que los factores clave para este crecimiento están en la transformación digital y en las nuevas normativas sobre protección del datos y ciberseguridad. Y destaca que esta obligatoriedad “también le ha dado una herramienta a los CISO para justificar las inversiones”

Clica en la imagen para ver la galería

PERCEPCIÓN DEL RIESGO EN LAS EMPRESAS

Como consecuencia de esta misma imposición normativa, y con el papel de los CISO como comunicadores de la importancia de la seguridad y el cumplimiento con NIS2, DORA o GDPR, Borja Pérez opina que se está incrementando la concienciación entre la dirección de las empresas. Por otro lado, destaca que estas regulaciones están impulsando mejores tiempos de respuesta y de comunicación de incidentes, haciendo que también las propias compañías sean más conscientes de la importancia de la ciberseguridad.

Sergio Martínez, de SonicWall, sí cree que en materia de concienciación todavía hay una brecha entre la dirección de las compañías y los departamentos de TI y ciberseguridad, por lo que en muchos casos está costando que cale la idea de que la ciberseguridad es una inversión y no un gasto. Por ello, recalca que se ven forzados a hablar de las consecuencias económicas y reputacionales de un ciberataque, en lugar de sobre las ventajas competitivas que proporciona una buena seguridad.

Para Carlos Castañeda, de Serval Networks, “a fuerza de hablar con el CISO, y el CISO con la dirección, se termina entendiendo en ciberseguridad, pero no se logra que se perciba como una inversión, un tema de gestión reputacional”. Y cree que se debe pensar en la ciberseguridad “no solamente como tecnología, sino incluyendo también a las personas, los procesos, la resiliencia y la continuidad de negocio”. Y ve especial problemática en las pymes, que no cuentan con un departamento de ciberseguridad con su propio responsable, sino que un trabajador se encarga de muchos otros temas, y le es difícil impulsar esa concienciación y obtener los recursos para proteger a la empresa.

En Netskope, como comenta Francisco Machuca, coinciden en general con la problemática del tejido em-

> ESPAÑA TIENE UN BUEN NIVEL DE CONCIENCIACIÓN EN LAS EMPRESAS Y TENEMOS UN MERCADO DE CIBERSEGURIDAD MUY MADURO

FRANCISCO MACHUCA,
senior channel sales manager de **Netskope**

> LAS NUEVAS REGULACIONES ESTÁN OBLIGANDO A LAS EMPRESAS A INCORPORAR NUEVAS SOLUCIONES DE CIBERSEGURIDAD

CARLOS CASTAÑEDA,
responsable de preventa y desarrollo de negocio de **Serval Networks**

Clica en la imagen para ver la galería

presarial español, compuesto principalmente por pymes, pero asegura que “España tiene un buen nivel de concienciación en las empresas y tenemos un mercado de ciberseguridad muy maduro”. Y opina que la importancia de la ciberseguridad ha calado no solo en las empresas, sino también entre todos los actores del canal. Pero, coincidiendo con Carlos Castañeda, cree que la pyme adolece de esa falta de figuras especializadas en ciberseguridad, y aboga por un modelo de servicios gestionados a través de un partner.

IMPOSICIÓN NORMATIVA COMO IMPULSOR

Como han comentado los cuatro portavoces, el cambio normativo que se viene produciendo en Europa en los últimos años está actuando como impulsor del mercado de ciberseguridad. Borja Pérez (Stormshield) destaca cómo esto está ayudando al CISO a “definir un marco de prioridades, de arquitecturas, de procesos y sistemas”. Aunque en el otro extremo está la obligatoriedad de reportar en tiempo y forma los incidentes, que genera problemas a las empresas.

Sergio Martínez (SonicWall), ve positivamente que “las regulaciones te obligan, pero a la vez te acompañan”, proporcionando pautas que ofrecen más seguridad y transparencia que si cada empresa lo hiciese a su manera y, en sus palabras, “es un marco normativo que ayuda, si lo interpretas de esa forma, a llegar más lejos”.

En opinión de Carlos Castañeda (Serval Networks), la industria ha construido su mensaje en base al miedo a ser atacados, y “si tengo miedo, me voy a quedar quieto”, lo que se traduce en retrasos en la digitalización, la innovación y la seguridad. Por ello, apuesta por trabajar desde el canal en la concienciación de las empresas, para que entiendan que invertir en ciberseguridad es hacerlo en el negocio, ya que

Con nuestros **Servicios de Ciberseguridad**

ponemos ojos en
la oscuridad del Ciberespacio

serval NETWORKS

www.servalnetworks.com

sienta las bases para poder desarrollarse en muchas áreas.

Por parte de Netskope, Francisco Machuca destaca la importancia de relacionar la ciberseguridad con la continuidad del negocio, para que las empresas entiendan que invertir en este campo sirve para mejorar. Y termina diciendo que “nosotros, como vendors, y con la tecnología que tenemos, debemos implementarla o facilitarla al canal y al mercado, y ser herramientas útiles” desde la fase consultiva, para entender lo que realmente necesitan y quieren los clientes en cuanto a sus activos de datos.

IA COMO ALIADO

La inteligencia artificial tiene una doble vertiente en el ámbito de la ciberseguridad: para atacar y para defender. Carlos Castañeda piensa que se debe abandonar la idea de que a la inteligencia artificial se le ha dado la capacidad de pensar, ya que simplemente es una herramienta que ya se usaba de una manera, y ahora se hace de otra. Afirma que “no debemos tenerle miedo, es algo que tenemos que asumir”, pero opina que “hay que ponerle reglas de juego claras para que todos seamos capaces de utilizarla” de la manera adecuada.

Clica en la imagen para ver la galería

Coincide Sergio Martínez, de SonicWall, en los fallos que puede tener la IA en cuanto a inventarse información para responder al usuario, aunque destaca que en su compañía llevan muchos años utilizando machine learning y el deep learning para la inteligencia de amenazas y, ahora, “hemos sacado un prompt para poder interrogar sobre la infraestructura”.

> “VAMOS CASI DOBLANDO MES A MES EL NÚMERO DE PARTNERS QUE TRABAJAN CON NUESTRO SOC”

SERGIO MARTÍNEZ,
country manager de **SonicWall**

Pero alerta de que los ciberdelincuentes están mucho más avanzados en el uso de la IA para, principalmente “descubrir sistemas vulnerables”, “enlazar tipos de ataque y hacerlos más sofisticados”, y “hacer ataques mucho más evasivos y difíciles de detectar”.

Borja Pérez, de Stormshield, también pone el foco en la doble vertiente de la IA en ciberseguridad, y en que “los malos” la utilizan más intensamente que en la parte de protección. Pero rompe una lanza en favor de sistemas que no se basan completamente en la IA, y apuesta porque “utilicemos la inteligencia artificial bien, y no absolutamente para todo”.

PRINCIPALES AMENAZAS

En 2025 se siguen detectando muchas de las amenazas clásicas, y según el informe Cyber Threat Report de SonicWall, como comenta Sergio Martínez, “los ataques de ransomware siguen creciendo, quizás ya no a los ritmos de otros años, pero ahora son mucho más letales y mucho más dirigidos y focalizados”. También destaca el crecimiento de los ataques dirigidos a IoT y las amenazas que utilizan los canales encriptados, que se han duplicado. Y alerta sobre que “el 60% de las brechas se producen en las primeras 48 horas de un ataque”, y que “el 90% de los ataques tienen que ver con un error humano”.

A esto, Francisco Machuca, de Netskope, añade las vulnerabilidades relacionadas con los hiperescalares o aplicaciones cloud, que considera vectores importantes a tener en cuenta. Por ello, apuesta por monitorizar y proteger el tráfico en tiempo real para minimizar este riesgo, precisamente a donde enfocan sus soluciones. Y, en cuanto a la IA, destaca cómo la están aplicando en sus laboratorios para que los operadores y los administradores puedan automatizar procesos y ayudarles en la detección de amenazas.

Desde Serval Networks, como señala Carlos Castañeda, perciben claramente el aumento de ciberataques. Por ello, se enfocan en “crear todo un esquema de servicios gestionados que se centren en la anticipación”, para poder actuar antes de que se produzca un problema. En su caso destacan las amenazas vinculadas a los DNS que, en sus palabras, “se han convertido en un vector de ataque”. Y, por otro lado, afirma, el SOC tradicional, el SIEM, ya no es tan efectivo como era, y precisamente el SIEM se ha vuelto un motor de acumulación de datos que no se usan correctamente.

Borja Pérez, de Stormshield, destaca los datos de un informe de la Agencia Nacional de Sistemas de Seguridad de la Información de Francia (ANSI), según el cual “la mitad de los incidentes graves reportados venían por vulnerabilidades de fabricantes de seguridad”. Ante esto, dice, “tenemos que ser muy conscientes de que, como fabricantes de ciberseguridad, somos el objetivo número uno de los criminales”, algo que abordan a través de sus programas de desarrollo, de seguridad, haciendo que los procesos sean independientes unos de otros y auditando el código fuente a través de terceros.

> “COMO FABRICANTES DE CIBERSEGURIDAD, SOMOS EL OBJETIVO NÚMERO UNO DE LOS CRIMINALES”
>
> **BORJA PÉREZ,** country manager de **Stormshield**

Clica en la imagen para ver la galería

HACIA LOS SERVICIOS GESTIONADOS

Desde el punto de vista de los fabricantes, no solo se percibe la tendencia hacia la prestación de servicios gestionados de ciberseguridad, sino que son de los principales impulsores del modelo MSSP. Aunque Borja Pérez (Stormshield) señala que el canal está haciendo su parte, con ciertos actores, incluso locales, que llevan tiempo ofreciendo servicios en modalidad de pago por uso para atender las necesidades de las pymes. Y, en su opinión, “la manera más sencilla para una pyme de contratar estos servicios de seguridad es tener un servicio gestionado y pagar una mensualidad”.

En SonicWall, como explica Sergio Martínez, hace un año que lazaron su SOC as-a-Service, no con la intención de sustituir nada que haga el canal, sino para ayudarle y que sea más fácil proporcionar servicios avanzados al cliente final, apoyando el modelo MSSP. Desde entonces, afirma, “vamos casi doblando mes a mes el número de partners que trabajan con nuestro SOC”, lo que considera una evolución mu positiva de este movimiento.

Para Carlos Castañeda, “el éxito del canal es el éxito de los fabricantes” y apuesta por una conjunción entre estos y los integradores. Recientemente han anunciado acuerdos con fabricantes en el ámbito MSP, para “construir un modelo más grande para que el integrador, que en este caso somo nosotros, podamos entregar un servicio”, atendiendo a la necesidad de muchas empresas de contar con soluciones llave en mano con unas condiciones claras de valor. Añade que “otra parte fundamental dentro de la propuesta del servicio gestionado es entregar valor en términos de toma de decisiones”.

Francisco Machuca, de Netskope, coincide con el resto de los portavoces en la importancia de impulsar los servicios gestionados para permitir a los clientes finales consumir lo que necesitan mediante pago por uso y, señala que su política de canal está dirigida a potenciar la integra-

SAMSUNG

Seguridad total para tu negocio

Galaxy S25 Ultra para tu negocio

Galaxy AI ✨

Imagen simulada. Para ciertas funcionalidades de Samsung AI, puede ser necesario iniciar sesión en la Cuenta Samsung. La disponibilidad de las funcionalidades de Galaxy AI puede variar según el modelo. La UI/UX real puede diferir. La disponibilidad de Samsung Knox Vault puede variar según el modelo, incluyendo, pero no limitado a, la serie Galaxy A, Galaxy Tab y otros. Samsung Knox ha cumplido con éxito los rigurosos requisitos de seguridad establecidos por gobiernos y grandes empresas a nivel mundial, proporcionando a los usuarios empresariales una solución de seguridad móvil robusta. https://www.samsungknox.com/en/knox-plataform/know-certifications

ción de los partners adecuados, que ofrezcan ciberseguridad con su tecnología, para ofrecer a los clientes "una solución enriquecida". Y, para impulsar esta integración, optan por la plataformización para "tener más módulos, más servicios", dando más relevancia al partner, que es quien se está formando constantemente para estar al día de toda la oferta disponible, de forma que pueda diseñar la propuesta con lo que necesite el cliente. En este sentido, apuesta también por la integración vía API.

Clica en la imagen para ver la galería

PROPUESTAS DE LA INDUSTRIA

El mercado de ciberseguridad avanza constantemente y los cuatro portavoces nos adelantan cuáles son las novedades que traerán de cara a los próximos meses. Comienza Sergio Martínez, de SonicWall, destacando que "en el H2 lanzaremos más firewalls con la nueva generación que hemos lanzado ahora en mes de junio, implementaremos una nueva generación de nuestro entorno de gestión en la nube para todos los dispositivos y avanzaremos más en el mundo de los servicios gestionados y del acceso remoto seguro ZTNA".

En Stormshield, como comenta Borja Pérez, "ya habíamos anunciado los algoritmos poscuánticos para las comunicaciones cifradas entre firewalls, y también alternativas a las VPN, otro tipo de conectividad sin necesidad de concentradores, que creo que va a ser bastante potente", con "una mayor potencia de cifrado y mayor capacidad de intermallado sin necesidad de concentradores". También anticipa que van hacia el modelo de plataforma, como la mayoría de los fabricantes, y a "tener unas plataformas de gestión únicas y modulares, de manera que el cliente o el partner pueda activar o desactivar servicios en función de lo que necesite su cliente".

Carlos Castañeda, de Serval Networks, comenta que su intención es "consolidarnos en la parte de SOC Serv, proveer una capa de inspección en la dark web a través de otros integradores, y en el aislamiento dinámico", donde trabajarán con Netskope para poder aislar rápidamente los sistemas ante cualquier mal funcionamiento o posible ataque de ransomware.

Finalmente, Francisco Machuca destaca el DSPM que han lanzado, proveniente de una adquisición, y que están comercializando desde este nuevo año fiscal, y también la parte de Enterprise Browser, proveniente también de una adquisición de una empresa española. Se trata de un navegador que "te permite aislar sin el cliente de Netskope y ejercer el mismo control que tienes con el cliente, sin necesidad del cliente", enfocado a "contractor y consultores que vayan a tu empresa o tengan que acceder a tus sistemas". Además, van a lanzar nuevos módulos enfocados a SASE single-vendor, un objetivo prioritario de la compañía, con el que hacen converger la parte SSE con SD-WAN. ■

MÁS INFO +

» Principales tendencias en torno a la ciberseguridad en 2025, a debate

COMPARTIR EN REDES SOCIALES

ENRIQUE MARTÍN, RESPONSABLE DE GRANDES CUENTAS Y ADMINISTRACIONES PÚBLICAS DE SAMSUNG

"La ciberseguridad es un eje estratégico para las organizaciones"

Como parte del Debate IT Principales tendencias en torno a la ciberseguridad en 2025, hablamos con Enrique Martín, responsable de grandes cuentas y administraciones públicas de Samsung, sobre el panorama actual de la ciberseguridad, marcado por el crecimiento de las amenazas, la profesionalización del cibercrimen y la necesidad urgente de concienciación y respuesta automatizada.

La ciberseguridad ha pasado de ser una preocupación técnica a convertirse en un eje estratégico para las organizaciones. Así lo afirma Enrique Martín, que añade que el mercado español de ciberseguridad ha crecido más del 14% en el último año. Un crecimiento que refleja la creciente conciencia en las empresas, aunque aún es des-

ENTREVISTA >> Hablamos con Enrique Martín sobre el panorama actual de la ciberseguridad en España.

igual: “en las grandes cuentas la preocupación ya es palpable, pero en las pymes todavía queda mucho por hacer”.

DESAFÍOS PARA LOS RESPONSABLES DE SEGURIDAD

Uno de los grandes desafíos, señala, es que muchas empresas siguen sin ser conscientes de lo que ocurre en su infraestructura digital. “Saber lo que está pasando y poder reaccionar de forma automatizada son hoy los dos grandes retos”, explica. Y más aún cuando las normativas, como NIS 2, trasladan la responsabilidad de la ciberseguridad directamente a los CEO.

“La seguridad ya no es un asunto solo del CISO. El CEO tendrá que rendir cuentas si hay una brecha”, sin olvidar que, al sufrir un ciberataque grave, “el 70% termina cerrando en menos de cuatro años”, advierte Martín.

EL VALOR QUE APORTA DE LA IA… Y EL PELIGRO QUE SUPONE

En este contexto, la IA se convierte en una herramienta clave para anticiparse a las amenazas. Samsung está integrándola en sus dispositivos para identificar comportamientos anómalos, como un uso inusual de CPU o conexiones sospechosas en horarios extraños. “La IA nos ayuda a detectar patrones de ataque y activar respuestas automáticas. La usamos tanto en seguridad como en la mejora del rendimiento del dispositivo”, apunta Martín.

Sin embargo, el potencial de la IA es una espada de doble filo: los atacantes también la están utilizando para perfeccionar sus ofensivas. “Los correos de phishing ya no son tan burdos. Ahora están más personalizados, con más información y más capacidad de engaño”, reconoce. Por eso, Samsung refuerza tanto la defensa tecnológica como la formación del usuario, que sigue siendo el eslabón más débil. “La mayoría de los ataques tienen raíz humana. La formación es clave”, subraya.

Martín también destaca el papel del canal en esta transformación. Las soluciones de seguridad ya no se venden como productos, sino como servicios. “El canal debe integrar herramientas de distintos fabricantes en soluciones coherentes. Nosotros ofrecemos una plataforma para facilitar la gestión masiva y automatizada de la seguridad a nuestros partners”, señala.

Samsung trabaja, además, en ofrecer datos de sus dispositivos a herramientas como los SIEM y XDR, permitiendo a las empresas tener una visión integrada de su seguridad. “No tiene sentido proteger con una caja fuerte de 100.000 euros algo que vale 1.000. Hay que aplicar sentido común. Pero toda empresa, grande o pequeña, tiene información sensible que proteger”, dice.

Y esa protección, apunta Martín, debe extenderse a todos los dispositivos conectados, no solo a PC o móviles: “todos forman parte del ecosistema y todos deben estar securizados”. La compañía aplica su plataforma Knox de seguridad por hardware a todos los dispositivos, no solo los de TI, creando una “cadena de seguridad” que alerta si uno de ellos presenta comportamientos anómalos. ■

> “LA CIBERSEGURIDAD NO ES UNA MODA, ES UN IMPERATIVO ESTRUCTURAL”
>
> **ENRIQUE MARTÍN,** responsable de grandes cuentas y administraciones públicas de **Samsung**

MÁS INFO +

» Entrevista Enrique Martín, Samsung

COMPARTIR EN REDES SOCIALES

STORMSHIELD

Stormshield, ciberseguridad industrial de confianza con la certificación IEC 62443

Protección de sistemas operacionales

Stormshield ofrece a las empresas de todo el mundo una alternativa europea de confianza para la protección de infraestructuras críticas, datos sensibles y entornos operativos.

www.stormshield.com

JORGE DÍAZ-CARDIEL
socio director general de Advice Strategic Consultants

SECTOR TIC DIGITAL, MOTOR DEL PIB ESPAÑOL EN 2025 POR LA DIGITALIZACIÓN

LORENZO MARTÍNEZ RODRÍGUEZ
experto en ciberseguridad

CONÓCETE A TI MISMO

JOSÉ MANUEL NAVARRO
experto en marketing

UCX EN EL PUENTE DONDE HABITAN LAS MARIPOSAS

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.

SECTOR TIC DIGITAL, MOTOR DEL PIB ESPAÑOL EN 2025 POR LA DIGITALIZACIÓN

El impulso de la Digitalización en España corre a cargo de 3 actores en 2025: la gran empresa española; el sector tecnológico digital y el Plan de Recuperación y Resiliencia (Fondos NEXTGEN, Plan España Digital 2025 y administración electrónica).

Las grandes empresas, adoptando las tecnologías de la Digitalización, tienen un “efecto arrastre” de 1 millón de pymes y 33% del empleo total en España, en 2025. Y contribuyen a la construcción de un modelo más sostenible: la Sostenibilidad es una de las grandes beneficiadas de la Transformación Digital.

España ocupa el séptimo lugar (7º puesto) en Digitalización en la Europa de los 27 (Índice DESI, UE27) y lidera en Conectividad. El impacto de la Digitalización en el crecimiento económico se cuantifica en una aportación al Producto Interior Bruto (PIB) entre 2024 y 2025 entre el 21 y el 28%, según la metodología de análisis utilizada. Advice Strategic Consultants ha optado por usar las dos metodologías más serias y reconocidas por todos (Eurostat, Banco Mundial, OCDE, FMI y WEF): investigación de mercado basada en encuesta cuantitativa en el universo de empresas españolas y análisis de meta data y fuentes de información secundaria, conforme a los criterios estadísticos rigurosos del

Instituto Nacional de Estadística (INE) y el Banco de España. En 2024 y 2025, 24% del PIB tiene que ver con actividades digitales.

Tres "hallazgos" destacan en 2025: la mayor Digitalización de la economía y la empresa han conseguido que España se posicione en primer lugar en la UE27 en tres parámetros: Sostenibilidad, Servicios Públicos y Conectividad. La comparativa con los mismos parámetros estadísticos que utilizan el INE y Eurostat con los aplicados por Advice en la encuesta actual permiten afirmar que la Digitalización económica y empresarial del último lustro ha dado como resultado el liderazgo de España en Sostenibilidad, administración electrónica y Conectividad de banda ancha y fibra en todo el territorio nacional. Los Indicadores DESI que comparan el estado de la Digitalización entre los países de la Europa de los 27 ofrecen conclusiones similares.

BRECHA DIGITAL DE PYMES Y AUTÓNOMOS

En 2025 la digitalización empresarial avanza en España, pero hay desigualdades entre grandes empresas y pymes. Los objetivos de la estrategia nacional "España Digital 2025" aún no se han cumplido: que 25% de empresas usen inteligencia artificial (IA) y Big Data, y el comercio electrónico represente el 25% del volumen de negocio de las pymes.

Según el último estudio de Eurostat, "sólo el 27% de las empresas españolas empezaron 2025 con "buena salud digital". El 37% tiene una "salud digital media" y "36% una mala salud digital".

Las grandes empresas españolas lideran la digitalización, con un 34% en buena salud digital, frente al 26% de las medianas y el 21% de las pymes y microempresas. El 61% de las pymes alcanzaron un nivel de digitalización básico en 2024, superando el promedio europeo del 58%.

LA CIFRA DE NEGOCIOS DEL SECTOR TIC SUPERA LOS 124.316 MILLONES DE EUROS, Y SU VALOR AÑADIDO ES DE 45.619 MILLONES DE EUROS, SEGÚN EL INE

ADOPCIÓN DE TECNOLOGÍAS DE LA DIGITALIZACIÓN EN 2025

La realidad objetiva de la implantación de las tecnologías de la digitalización en la empresa española en 2025, es que solo el 11% de empresas españolas usan Inteligencia Artificial (IA), y en su inmensa mayoría son grandes empresas. El Banco de España, adicionalmente, ha detectado en su Encuesta de Actividades Empresariales (EBAE, mayo 2025) que las grandes empresas usan sobre todo Inteligencia Artificial predictiva (bancos y seguros, telecomunicaciones y TIC, Comercio, Distribución, retail y gran consumo...), versus las pymes, que si usan IA es, habitualmente, inteligencia Artificial generativa en sus versiones gratuitas.

Big Data es usado por el 31% de empresas españolas y el 38% realiza análisis de datos.

Sobre el comercio electrónico (pymes), el total de ventas electrónicas por parte de las pymes, como porcentaje de su facturación total sobre el volumen de negocios, fue del 9,6% en España en 2024, versus el 12,4% en la UE27. El objetivo de la agenda digital España 2025 es del 25%

En España, 54,6% de empresas tienen paquetes de software de planificación de recursos empresariales (ERP) para compartir información entre las distintas áreas funcionales. En la Europa de los 27 el porcentaje de empresas es 43,3%.

IMPACTO ECONÓMICO DE LA DIGITALIZACIÓN

Según los datos:

- En 2024, el 24% del PIB español ya provenía de actividades digitales, reflejando el peso creciente de la economía digital.
- La digitalización es vista como clave para el crecimiento, la productividad y la transición hacia una economía más sostenible y basada en datos.

España ha logrado avances significativos en la digitalización de sus empresas en 2025, especialmente en la adopción de análisis de datos y el crecimiento del comercio electrónico. Sin embargo, el uso de tecnologías avanzadas como la inteligencia artificial sigue por debajo de los objetivos y las pymes siguen teniendo más dificultades que las grandes empresas.

El impulso de la digitalización en España corre a cargo de 3 actores: la gran empresa española; el sector tecnológico digital y el Plan de Recuperación y Resiliencia (Fondos NEXTGEN, Plan España Digital 2025 y Administración electrónica).

EL PAPEL DE LA GRAN EMPRESA ESPAÑOLA EN LA TRANSFORMACIÓN DIGITAL DE ESPAÑA

De la gran empresa española destacan CaixaBank, El Corte Inglés, Telefónica, Inditex, Mercadona, Cellnex Telecom, Santander, Iberdrola, Meliá e Indra, que lideran la digitalización empresarial de España, entre las 500 más grandes

empresas de España por facturación. Ejercen “efecto tractor” sobre las pymes y, de hecho, 64.000 pymes de media, dependen de cada una de esas grandes empresas.

Por su parte, Fundación “La Caixa” lidera la labor de cerrar la brecha digital en España de pymes, microempresas, autónomos y población general con formación y educación digital.

Las grandes empresas españolas son las que más han adquirido e implementado las tecnologías de la Digitalización: Cloud, Internet de las Cosas (IoT), Inteligencia Artificial, Big Data, Ciberseguridad y Conectividad 5G, entre otras. Es una de las principales conclusiones del Estudio de la consultora económica y empresarial Advice Strategic Consultants, ha realizado el informe más extenso y profundo sobre el estado de la digitalización económica y empresarial de España en 2025.

EL SECTOR TIC DIGITAL Y EL EMPUJE DEL PIB CON LAS TECNOLOGÍAS DE LA DIGITALIZACIÓN

En España, hay más de 75.000 empresas en el sector de las tecnologías de la información y la comunicación (TIC), y este sector contribuye significativamente al Producto Interno Bruto (PIB), representando aproximadamente el 24,2% en 2023 (directo + indirecto e inducido), según datos de Ametic, patronal de las empresas tecnológicas junto con DigitalES.

> **LA APORTACIÓN DIRECTA DEL SECTOR TECNOLÓGICO DIGITAL A LA ECONOMÍA ESPAÑOLA ES DEL 5,9%, TOMANDO COMO REFERENCIA ÚNICA EL VALOR AÑADIDO DE LAS EMPRESAS TECNOLÓGICAS AL PIB**

La cifra de negocios del sector TIC supera los 124.316 millones de euros, y su valor añadido es de 45.619 millones de euros, según el INE. La aportación directa del sector tecnológico digital es del 5,9%, tomando como referencia única el valor añadido de las empresas tecnológicas al PIB. La permeabilidad de actividades digitales en la actividad económica y empresarial representa 24% del PIB e incluye el comercio electrónico, los aumentos de productividad y competitividad empresarial fruto de la digitalización, los servicios digitales de la Administración Pública, digitalización en educación y formación...

En el sector tecnológico destacan por su contribución a la digitalización económica y empresarial de España, las Top-150:

Operadoras de Telecomunicaciones: Telefónica, MásOrange, Vodafone, Digi, Avatel Telecom.

Gestión de Infraestructuras de Telecomunicaciones: Cellnex Telecom, American Tower.

Equipos de Telecomunicaciones y Redes: Ericsson, Nokia, Huawei.

Ciberseguridad: Esprinet, Symantec, FireEye, Proofpoint, Fortinet, McAfee, Rapid7, Synack, Trend Micro, Telefónica Tech, WatchGuard.

Software: Microsoft, Oracle, Kyndryl, Salesforce, SAP, SAS, Sage, MicroStrategy.

Computación: HP, IBM, Dell Technologies, Lenovo, Apple, Acer, Asus, Sony.

Electrónica: Samsung, Apple, Sharp, Sony.

Smartphones: Samsung, Apple, Xiaomi, Huawei y Oppo.

Tabletas y ordenadores: Apple, Samsung, Sony.

Televisores y pantallas: LG, Sony, Loewe y Panasonic.

Cámaras digitales: Panasonic, Canon.

Integradores: Telefónica Tech, Accenture, Cap Gemini, Ingram Micro, Inetum, Deloitte, Atos, Minsait (Grupo INDRA), T-Systems.

Cloud: Amazon Web Services (AWS), Microsoft Azure, Google Cloud, Salesforce, Oracle Cloud.

Comercio Electrónico: Amazon, El Corte Inglés, Alibaba, Shein, Temu.

Networking: Cisco Systems, HPE, Avaya Networking, Juniper Networks, Ericsson, Nokia, Huawei.

Periféricos: HP, Lexmark, Brother, Oki, Ricoh, Epson, Toshiba.

Redes Sociales: Meta (Facebook, Instagram, WhatsApp); YouTube (Google); X (antigua Twitter), TikTok (ByteDance).

Procesadores: Nvidia, AMD, Intel, Qualcomm, TSMC, Micron, Mediatek, ASML. ■

MÁS INFO +

» Sector TIC Digital, motor del PIB español en 2025 por la Digitalización

» La digitalización ya supone el 24% del PIB en España

FORMACIÓN HACKING ÉTICO 2025

PENTESTING

ESCALAR PRIVILEGIOS

VULNERABILIDAD

ATAQUES

MALWARE

APRENDE A PENSAR COMO UN ATACANTE...
PARA CONVERTIRTE EN DEFENSOR

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

CONÓCETE A TI MISMO

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.

Estoy seguro de que el lector habrá visto esta motivadora frase decenas de veces: en un fondo que parece un verde paisaje, la inmensidad del océano, un busto de Sócrates o en un tatuaje realizado en alguna extremidad de alguien. Sin embargo, el significado profesional que tiene para un responsable IT o de seguridad de una empresa no es precisamente motivador, sino que es el primer e imprescindible paso para inventariar los potenciales puntos que, por su abuso o explotación, puedan derivar en un incidente de seguridad.

Por una parte, el *conócete a ti mismo* aplicado al mundo IT conlleva ser consciente de las tecnologías utilizadas por la organización, tanto internamente como con exposición directa a Internet (aunque bien está conocer si además hay exposición externa, para otorgarle un plus de peligrosidad mayor), así como en cualquier servicio de hosting o nube que tenga contratada la organización.

En redes complejas, con mucha actividad de servicios que se exponen y se ocultan, así como en organizaciones de sistemas coadministrados, puede suceder que uno crea que tiene expuesto un número determinado y mínimo de servicios, y que realmente, por un error involuntario o por una negligencia, haya servicios expuestos de manera no controlada. De hecho, muchas veces este tipo de servicios suelen ser temporales, como por ejemplo entornos de testing o de desarrollo, que no cumplen con ninguna medida de seguridad, puesto que todo el mundo cree que no están expuestos y que son únicamente de uso interno.

Por eso, el "Conócete a ti mismo" (o su equivalente anglosajón Know yourself), orientado a IT, nos indica claramente que no podemos confiar en lo que creemos que hay expuesto, tanto en número de servicios como en la seguridad de las versiones y configuración implementadas en los mismos, sino que debemos comprobarlo para quedarnos tranquilos.

Llevar a cabo esta verificación de manera periódica es equivalente a lo que hacemos en otras facetas de nuestra vida, como llevar nuestro vehículo al mecánico para que haga una inspección —tanto visual como con herramientas especializadas— o que, por ejemplo, un médico nos pida un análisis de sangre anual completo para verificar que los diferentes valores e indicadores están dentro de los niveles que tienen que estar.

Es importante también que quien lleve a cabo esta verificación lo haga de una forma objetiva y completamente realista. Si se hace desde una sede externa, distinta a la principal (siempre y cuando la organización tenga más de una sede), es posible que los resultados obtenidos vengan alterados porque haya algún servicio que tenga que ser visible desde dicha sede. La interpretación de este resultado puede llevarnos a pensar que, dado que se ha hecho desde un sitio desde el cual ese determinado servicio es visible, es algo normal. La única manera de obtener resultados fiables es hacer el análisis desde una ubicación que nada tenga que ver con la organización y, si además quien lleva a cabo esta labor es una empresa especializada en auditorías, será miel sobre hojuelas. Quien se dedica a esto a diario siempre podrá aportar un valor adicional al riesgo de la exposición sobre los servicios identificados como expuestos, mediante la realización de pruebas específicas de explotación.

EL "CONÓCETE A TI MISMO" ORIENTADO A IT NOS INDICA CLARAMENTE QUE NO PODEMOS CONFIAR EN LO QUE CREEMOS QUE HAY EXPUESTO, TANTO EN NÚMERO DE SERVICIOS COMO EN LA SEGURIDAD DE LAS VERSIONES Y CONFIGURACIÓN IMPLEMENTADAS

Constatar que lo que se tiene expuesto es lo que se espera tener es el primer paso. El segundo es dedicarle tiempo a la mejora de la seguridad recomendada en el informe de los resultados obtenidos. A veces, la solución puede ser la actualización de la versión del software provisto para un determinado servicio; otras, la correcta configuración del mismo. En ocasiones quizá merezca la pena acotar el acceso a determinadas direcciones IP públicas únicamente, hacer accesible el servicio mediante una conexión VPN previa, exigir un certificado digital de cliente en un navegador para acceder al contenido o, incluso, como solución más drástica, si no es posible eliminar o mitigar el riesgo con las medidas anteriores, retirar la exposición del servicio de manera urgente hasta identificar cómo poder proveerlo de manera segura.

Como proveedor de este tipo de servicios de auditoría y hacking ético, muchas veces experimento sentimientos encontrados respecto a mis clientes. Casi siempre nos limitamos a la entrega de un informe de resultados en el que detallamos cómo es posible acceder a los sistemas, ejecutar comandos en ellos, exfiltrar información sensible, etc., y les facilitamos medidas de mitigación y solución. Sin embargo, ahí termina nuestro trabajo.

Se da el caso de que nos solicitan llevar a cabo un nuevo análisis, a veces un año después o, a veces, incluso pasa más tiempo. Me resulta increíble ver cómo siguen existiendo algunas de las mismas vulnerabilidades reportadas anteriormente. No se ha protegido nada, no se ha cambiado nada. Todo sigue igual, todo sigue mal.

Y no lo entiendo. Cuando el médico me receta un tratamiento, me tomo la medicación a rajatabla. Él sabe mejor que yo qué tengo que hacer para curarme. Es más, para eso le pago: para que me diga qué me pasa, me ponga por escrito qué tengo que hacer y me explique los riesgos que supone para mi vida no hacerlo.

Nosotros, como el médico, hacemos lo mismo recetando el tratamiento que consideramos más adecuado a quienes nos contratan una auditoría de ciberseguridad. Sin embargo, muchas veces tengo la sensación de que la motivación para ello proviene de una normativa, un estándar o una política que requiere un informe anual de auditoría. Pero ¿qué sentido tiene ignorarlo y guardarlo en un cajón?

Conócete a ti mismo, o pide que te ayuden a conocerte, pero, por favor ¡tómate la medicación! ■

MÁS INFO +

» Una de cada cuatro empresas experimentó filtraciones de datos en entornos cloud o SaaS

¡Descubre las **estrategias de digitalización** que han llevado al éxito a las grandes empresas de nuestro país!

DESCARGAR

itResearch

ADVICE
STRATEGIC CONSULTANTS

UCX EN EL PUENTE DONDE HABITAN LAS MARIPOSAS

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”.

COMPARTIR EN REDES SOCIALES

Cuando afrontaba el contenido de este artículo, el título que había elegido era “UCX: cuando la mente del cliente es el territorio donde se desarrolla la estrategia empresarial”, pero coincidió su redacción con la lectura del libro El puente donde habitan las mariposas de la neurocientífica Nazareth Castellanos. Entonces surgieron algunas ideas para afrontar la experiencia de cliente desde la perspectiva de la neurociencia, la tecnología y, sobre todo, la gestión del propósito del usuario para diseñar acciones que se traduzcan en vínculos estables y duraderos. Ya pueden entender el cambio de título; aún más si se animan a leerlo.

La doctora Castellanos es una neurocientífica destacada, reconocida por su habilidad para desmitificar conceptos científicos complejos, haciéndolos accesibles a una audiencia más amplia. Su trabajo integra de manera única la filosofía, la neurociencia y profundas reflexiones personales. En su obra, subraya que la comunicación y la interacción social no dependen únicamente del lenguaje hablado, sino que están profundamente entrelazadas con nuestra biología subyacente. Así, postula que la respuesta fisiológica del cuerpo a la emoción precede a la percepción consciente, afirmando que “el cuerpo sabe lo que la mente aún no se ha dado cuenta” y antes de que el individuo tome una decisión. Este concepto se alinea directamente con la “hipótesis del marcador somático” de A. Damasio, enfatizando la influencia inconsciente de los estados corporales en nuestras decisiones y sentimientos.

Si reparamos en los principios de la doctora Castellanos en relación con la denominada Experiencia Unificada de Cliente (UCX), observaremos una perspectiva enriquecedora para diseñar experiencias que tengan una implicación a un nivel más profundo ya

que se orientarán a estimular la **atención**, al fortalecer la **memorización** de las propuestas, a activar la regulación **emocional** y a potenciar la **intención** de tomar una decisión coherente (aquí la intención involucra a voluntad conscientemente fortalecida a través de mecanismos de motivación intrínseca y extrínseca). Esta posición recuerda al postulado de K, Christoff que defiende que la conexión, el puente, entre el "yo esencial" y el "yo narrativo" es el lugar donde habitan la percepción, la cognición, la emoción y la acción. Crucemos ese puente...

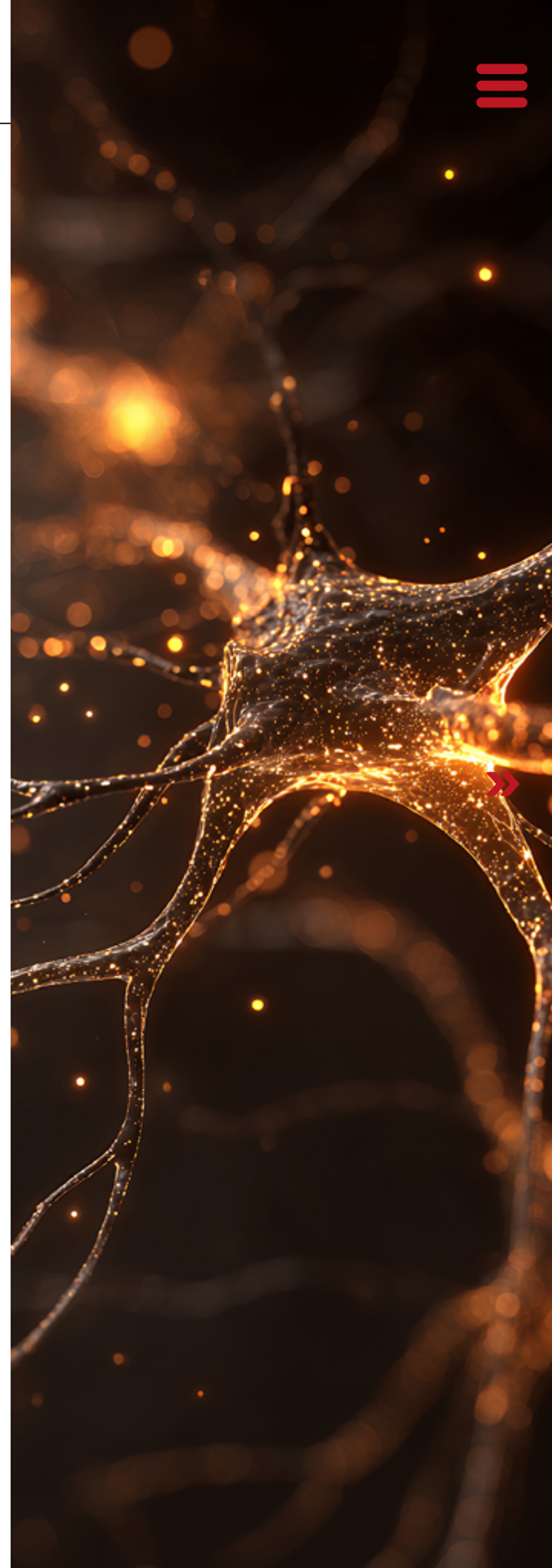
En un entorno de consumo fragmentado y altamente competitivo, donde las marcas se disputan la atención fugaz del consumidor, la experiencia del cliente (CX) dejó de ser un diferenciador para convertirse en una exigencia estratégica. Pero la evolución del mercado y de la tecnología nos ha conducido hacia la UCX, que ha emergido como una respuesta integral al reto de ofrecer recorridos coherentes, fluidos y emocionalmente significativos. Más allá de optimizar interacciones individuales, la UCX busca construir un relato continuo y orquestado a lo largo de todo el ciclo de vida del cliente. Su objetivo no es solo reducir la fricción, sino activar emociones, reforzar vínculos y consolidar una percepción de marca unificada, independientemente del canal o momento de contacto. Esta visión trasciende la lógica multicanal y omnicanal para convertirse en una filosofía holística de diseño de relaciones.

Este cambio de paradigma exige que las organizaciones abandonen la visión funcional y fragmentada de la experiencia del cliente y adopten una arquitectura centrada en el flujo emocional y cognitivo del usuario. La marca deja de ser una suma de departamentos para convertirse en una identidad coherente y reconocible que acompaña al cliente en cada paso. Para ello, hemos de ayudarnos de la neurociencia.

Desde la perspectiva de esta ciencia, el cerebro interpreta continuamente la postura y el estado físico de nuestro cuerpo, lo cual es fundamental para comprender nuestro estado general. Nuestra capacidad de atención voluntaria es inherentemente limitada, pero puede mejorarse significativamente a través de prácticas como la atención plena, lo que conduce a un mayor bienestar y una mayor capacidad para estar y sentir el presente (aquí, el lóbulo frontal desempeña un papel crítico en la atención focalizada). La comunicación no verbal, que incluye la postura corporal, los gestos faciales y el contacto visual, influye profundamente en las interacciones, a menudo a un nivel inconsciente. Además, la "reciprocidad fisiológica" (la alineación inconsciente de los patrones de ondas cerebrales y la adaptación a los estados emocionales y atencionales de los demás) ocurre durante la interacción humana y también en la que se produce con máquinas humanizadas.

¿Cómo podemos hacer una aplicación estratégica de los disparadores de la **atención** en un modelo de UCX avanzado? Desde mi punto de vista, podremos considerar, entre otras, tres variables:

- Diseñar pensando en la cognición corporal mediante el reconocimiento de que el estado físico del cliente (si está relajado o estresado) influye directamente en su capacidad de atención. El diseño UCX debe minimizar las molestias físicas o las posibles distracciones, por ejemplo, mejorando la usabilidad de las aplicaciones móviles para que los usuarios no encuentren puntos de fricción y, por ejemplo, para que puedan navegar fácilmente con una mano cuando están haciendo alguna actividad que les impide usar las dos.



➤ Aprovechar las señales no verbales en los puntos de contacto, como en los interfaces digitales tipo chatbots, en los que se podrá utilizar un lenguaje y patrones de respuesta que transmitan o inviten a mantener una “postura” tranquila o útil. En entornos minoristas físicos o durante videollamadas, es oportuno capacitar al personal de atención al cliente sobre la importancia de una posición abierta, un contacto visual apropiado y expresiones faciales genuinas para fomentar una reciprocidad fisiológica positiva y captar y mantener la atención de manera efectiva. Una actitud tranquila y enfocada por parte de un agente de servicio, real o virtual, puede ayudar a pacificar el estado emocional agitado de un cliente y generar un ambiente de confianza estable.

Dada la capacidad limitada del cerebro para la atención voluntaria sostenida, la UCX debe desglosar tareas engorrosas o información compleja en pasos más pequeños, digeribles y manejables con independencia del canal en el que se interactúe. Es recomendable emplear un lenguaje claro y conciso y jerarquías visuales intuitivas para guiar la atención de manera efectiva, evitando la sobrecarga de información que puede conducir a la fatiga cognitiva.

EN UN ENTORNO DE CONSUMO FRAGMENTADO Y ALTAMENTE COMPETITIVO, DONDE LAS MARCAS SE DISPUTAN LA ATENCIÓN FUGAZ DEL CONSUMIDOR, LA EXPERIENCIA DEL CLIENTE (CX) DEJÓ DE SER UN DIFERENCIADOR PARA CONVERTIRSE EN UNA EXIGENCIA ESTRATÉGICA

Con estos tres ejemplos sencillos podremos obtener un mayor compromiso del cliente, reduciendo las tasas de abandono y generando un procesamiento de información más eficiente gracias a experiencias diseñadas en armonía con los límites atencionales naturales de las personas. Como expone Castellanos, nuestros cerebros se adaptan inconscientemente a los estados emocionales y atencionales de aquellos con quienes interactuamos. Esto implica una dinámica profunda, a menudo pasada por alto, en el servicio al cliente. Si un agente comercial es percibido como estresado o desinteresado, o su interacción denota cierta urgencia, ese estado atencional puede “infectar” inconscientemente al cliente, lo que lleva a su frustración, una comprensión reducida o una interrupción en la comunicación. Por ello, la capacitación de una experiencia de usuario adecuada para roles de atención o apoyo al cliente (tanto humanos como virtuales) debe ir más allá de los meros guiones y protocolos de venta para incorporar principios de inteligencia emocional e “higiene atencional”.

En segundo lugar, ¿qué estrategias hemos de usar para crear experiencias unificadas memorables? La activación de los procesos de **memorización** y los de recuperación de recuerdos, la interpretación de eventos pasados y la anticipación de escenarios futuros son componentes integrales del proceso de toma de decisiones humano. El hipocampo está específicamente relacionado con la formación y recuperación de la memoria a largo y corto plazo, y está ubicado en el centro del sistema límbico donde también se halla el sistema de recompensa del cerebro, el núcleo accumbens, que se activa con estímulos positivos, asociando así la marca con el placer y fortaleciendo significativamente la memoria de marca.

Además, una narración convincente activa las mismas regiones cerebrales que se activan cuando experimentamos eventos reales, fomentando la empatía, mejorando la memoria y profundizando la participación. La anticipación de una recompensa, en lugar de solo su obtención, activa la dopamina, crucial para mantener el compromiso y la motivación. Lo más interesante, es que estas áreas median entre el sistema de percepción y el área prefrontal encargada de racionalizar la toma de decisiones. Por ello, es importante considerar cómo funcionan los procesos de memorización y recuerdo para ayudar a accionar las respuestas alineadas con la estrategia de marca. Así, se puede:

➤ Implementar bucles de retroalimentación positiva (o rutas de recompensa) a lo largo de todo el viaje de la UCX. Esto puede manifestarse como confirmaciones inmediatas, pequeños premios inesperados (por ejemplo, un mensaje de agradecimiento personali-

zado, un descuento sorpresa...) o elementos gamificados cuidadosamente integrados que desencadenan la liberación de dopamina. Estas asociaciones positivas refuerzan la memoria y construyen la afinidad con la marca.

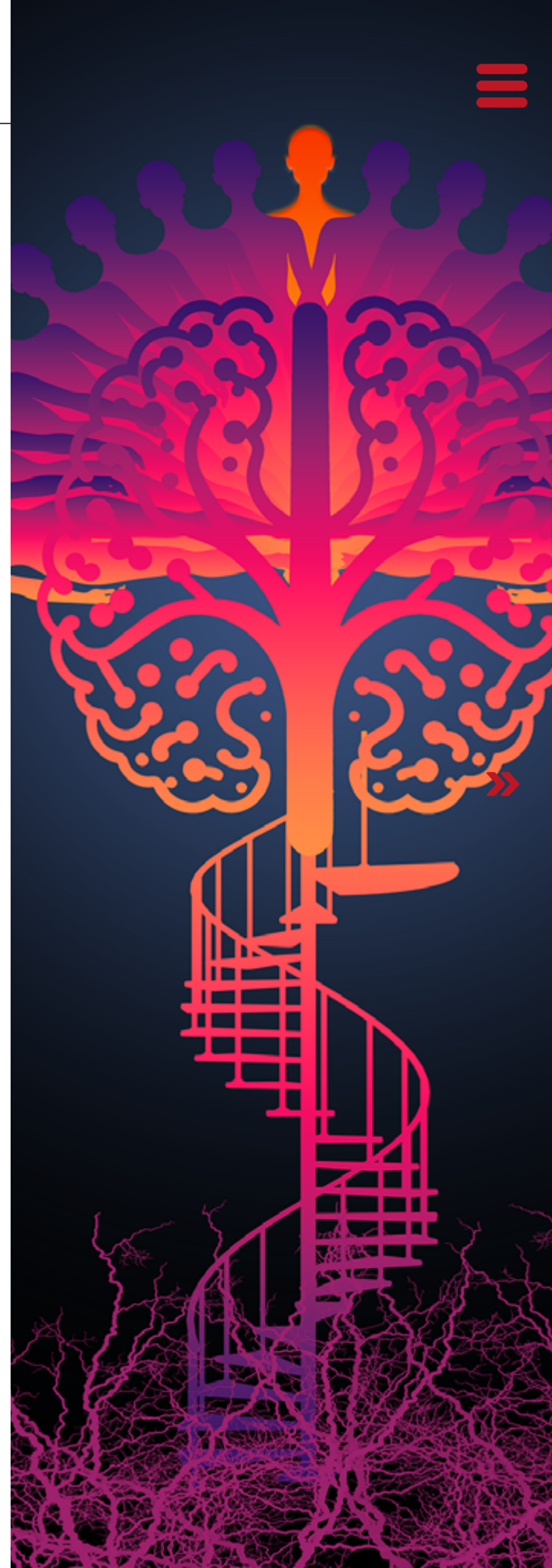
➤ Elaborar "viajes narrativos" en lugar de presentar a los clientes una serie de interacciones desconectadas, enmarcar toda la UCX como una historia coherente y atractiva donde el cliente es el protagonista central. Utilizar una voz de marca, una identidad visual y elementos temáticos consistentes para construir una narrativa continua que sea inherentemente más fácil de recordar y conectar emocionalmente para el cerebro.

➤ Aprovechar la "Regla del pico final" (Peak-End Rule) para centrarse estratégicamente en hacer que los momentos más intensos (pico) y los momentos finales de cualquier interacción con el cliente sean excepcionalmente positivos y memorables. Investigaciones de Kahneman y colaboradores muestran que estos puntos específicos influyen desproporcionadamente en la memoria y la percepción general de toda la experiencia.

Estas sencillas muestras ayudarán a obtener un mayor recuerdo de la marca, establecer vínculos emocionales más fuertes, una mayor retención de clientes y una mayor defensa frente a la competencia, ya que las experiencias positivas y memorables tienen más probabilidades de ser compartidas y repetidas. La activación del sistema de recompensa mediante la narración de historias activa áreas cerebrales como si se vivieran eventos reales. Esto sugiere que la formación de la memoria no se trata simplemente de almacenar información fáctica; está profundamente influenciada por el contexto emocional o la "etiqueta" asociada a esos hechos. Una etiqueta emocional positiva para un modelo UCX consistente hace que los procesos de memorización sean más prominentes, más fácil de recuperar las vivencias positivas y significativamente más propenso a influir positivamente en el comportamiento futuro y la percepción de la marca. Por lo tanto, la UCX debe diseñarse intencionalmente para crear experiencias emocionales positivas en los puntos de contacto críticos, particularmente aquellos que son novedosos, sorprendentes o que resuelven eficazmente un punto de dolor del cliente. Estas memorias "etiquetadas emocionalmente" serán las que impulsen la repetición de momentos de compra, fomenten la lealtad a la marca y se establezca una poderosa memoria de "marca como experiencia positiva" en primera línea de la mente del cliente ("top of mind").

Las **emociones** son procesos fisiológicos inconscientes que se generan a partir de estímulos internos (modulados por el sistema interoceptivo) o externos (percibidos por el sistema sensorial) que provocan cambios corporales cuya toma de conciencia se traduce en sentimientos. Este fenómeno es central para la hipótesis del marcador somático, de manera la respuesta organizada a determinados estímulos será siempre la misma para acelerar la reacción sin necesidad de hacer intervenir a las áreas responsables de la toma de decisión racional. Este mecanismo evolutivo está preparado para garantizar la supervivencia mediante respuestas rápidas a contextos de riesgo. Pero también ha servido para establecer vínculos afectivos entre miembros de una comunidad, modulando las relaciones en base a experiencias positivas previas.

En las relaciones comerciales, una interacción unificada, sin fricciones y personalizada tiene el poder de activar el sistema límbico, generando sentimientos de placer, recono-



cimiento y pertenencia. La UCX, por lo tanto, debe ir más allá de la mera eficiencia para lograr una profunda repercusión emocional que prepare la toma de decisiones, casi de manera automática, a favor de la propuesta de venta. El neuromarketing ha perfeccionado la técnica para identificar específicamente qué estímulos son más efectivos para generar respuestas emocionales positivas o negativas, ayudando a las marcas a posicionarse en función del perfil de su mercado objetivo y de la oferta específica de sus productos o servicios. ¿Cómo nos puede ayudar en el marco de una UCX exitosa?

➤ Orientando la estrategia creativa para generar un "priming emocional inconsciente", centrándose estratégicamente en las señales sutiles que preparan estados emocionales positivos incluso antes de que el cliente se involucre en el procesamiento consciente. Esto incluye garantizar un diseño intuitivo, tiempos de carga rápidos para las interfaces digitales, una marca visual consistente y atractiva, y transiciones fluidas entre los diferentes canales.

➤ Capacitando a los agentes de atención al cliente para que estén muy atentos a las señales no verbales (como la postura, el movimiento de los ojos o la tensión facial) que indican el estado emocional subyacente de un cliente. Abordar proactivamente estas señales corporales puede prevenir eficazmente las emociones negativas o amplificar las positivas, a menudo antes de que el cliente las articule conscientemente.

LA EVOLUCIÓN DEL MERCADO Y DE LA TECNOLOGÍA NOS HA CONDUCIDO HACIA LA UCX, QUE HA EMERGIDO COMO UNA RESPUESTA INTEGRAL AL RETO DE OFRECER RECORRIDOS COHERENTES, FLUIDOS Y EMOCIONALMENTE SIGNIFICATIVOS

➤ Evitando cualquier forma de fricción, como exigir a los clientes que repitan información, navegar por procesos excesivamente complejos o encontrar datos inconsistentes, que genere marcadores emocionales negativos (por ejemplo, frustración, ansiedad) que pueden hacer descarrilar el "customer journey". El énfasis central de la UCX en la fluidez mitiga directamente estos desencadenantes emocionales negativos.

El profundo énfasis de Castellanos en las respuestas emocionales preconscientes del cuerpo y el concepto de "reciprocidad fisiológica" va más allá de simplemente generar emociones positivas. Esto nos ayuda a entender que una UCX bien diseñada puede regular activamente el estado emocional del cliente a lo largo de los puntos de contacto y de la relación en su conjunto con la marca. Si un cliente inicia una interacción sintiéndose frustrado, una interacción de UCX diseñada sin problemas (por ejemplo, un chatbot tranquilo y empático, un agente humano bien informado con acceso inmediato a datos unificados del cliente) puede ayudar a cambiar su estado fisiológico y emocional hacia la tranquilidad, la comprensión o la satisfacción. La marca, en esencia, se convierte entonces en un estabilizador emocional para el cliente.

En este sentido, las estrategias de UCX deben evolucionar para incorporar la regulación emocional como un objetivo central, no solo la conexión emocional puntual. Esto implica identificar proactivamente los posibles desencadenantes emocionales del cliente y diseñar intervenciones específicas (ya sean dirigidas por humanos o automatizadas) que guíen al cliente hacia un estado emocional más positivo, productivo y, en última instancia, satisfactorio.

Por último, contemplemos cómo guiar la **intención** consciente del cliente hacia la acción y, finalmente, la lealtad. La intención consciente de actuar está intrínsecamente influenciada por la actividad cerebral subyacente previa (como exploró Libet). Críticamente, la intención voluntaria y un claro sentido de propósito están modulados por la corteza cingulada que funciona como un "interruptor de encendido/apagado" crucial que facilita la transición de la información de las áreas que regulan los procesos inconscientes (desde el sistema reptiliano al límbico) a las que generan la conciencia (áreas corticales, especialmente la prefrontal). El delicado equilibrio entre las respuestas emocionales y el procesamiento cognitivo es donde se conforman la intención de compra consciente y la lealtad duradera a la marca. Las experiencias

UCX excepcionales están diseñadas para minimizar posibles disonancias posteriores a la emoción, reforzando así poderosamente el camino elegido por el cliente. Veamos algunos ejemplos de cómo fortalecer los procesos de intención hacía la dirección que conduce a la decisión de compra.

➤ Después de una activación emocional inicial, la UCX debe proporcionar información clara, consistente y fácilmente accesible que empodere al cerebro racional del cliente para justificar lógicamente su preferencia impulsada por la emoción. Este refuerzo estratégico genera una profunda confianza y reduce significativamente cualquier posible disonancia o arrepentimiento posterior a la compra.

➤ Diseñar rutas de UCX que se sientan genuinamente como una guía de apoyo, en lugar de que se puedan percibir como manipuladoras. Para ello, hay que otorgar a los clientes un fuerte sentido de control a lo largo del proceso de compra. Las llamadas a la acción claras y convincentes, los procesos transparentes y la navegación intuitiva son elementos cruciales que empoderan la intención consciente de proceder con una compra o establecer un compromiso a medio y largo plazo.

➤ Conviene esforzarse por comprender el propósito más genuino y subyacente del cliente para interactuar con la marca, yendo más allá de una mera compra de producto. Si la experiencia UCX se alinea con este propósito personal más profundo, la intención voluntaria del cliente de interactuar y permanecer leal será significativamente más fuerte y resistente.

Podremos obtener mejores tasas de conversión, mayor retención de clientes, una defensa de la marca más sólida y el cultivo de una base de clientes profundamente leal impulsada mediante un pequeño empujón (nudge) de la intención, cuidando la motivación intrínseca, y un sentido del propósito compartido. Cuando el propósito personal de un cliente (por ejemplo, autoexpresión, salud, conexión comunitaria, sentido solidario...) se alinea genuinamente con el propósito de la marca, su intención de interactuar se vuelve íntimamente motivada, altamente resistente y significativa.

La acción de compra, cuando va precedida de una UCX impecable, se transforma de una mera transacción en una reafirmación y un ritual de confianza que consolida la relación cliente-empresa, haciendo que ésta, en última instancia, sea duradera e inquebrantable. Esto requiere una comprensión del motivo que respalda su compromiso y del diseño del "customer journey" más pertinente para reforzar constantemente ese propósito compartido, transformando así a los clientes en defensores apasionados que sienten una conexión genuina y orientada a un propósito con la marca.

El uso de las nuevas tecnologías (como la inteligencia artificial, el machine learning, las plataformas de datos de clientes, la realidad aumentada, los sistemas biométricos de autenticación o la securización transaccional) es una condición necesaria, pero no suficiente. La UCX exige una cultura interna transformadora, donde cada colaborador entienda su rol en la construcción de la experiencia. Esto implica romper silos organizativos, fomentar la colaboración interdepartamental y establecer una visión compartida de lo que significa una experiencia coherente. Las marcas que triunfan con la UCX son aquellas donde el mensaje, los valores y la actitud del equipo están alineados en todos los frentes. Todos los elementos de la organización dejan de ser ejecutores de tareas para convertirse en agentes emocionales de la marca. Esta alineación interna convierte cada interacción en una manifestación tangible del propósito de la organización.

En "El puente donde habitan las mariposas" encontraremos algunas claves esenciales para comprender cómo cuerpo y mente interactúan en la experiencia del cliente. Su enfoque, basado en la integración de neurociencia, filosofía y contemplación, si lo trasladamos al mundo empresarial nos brinda una mirada profunda a los procesos no conscientes que determinan nuestras emociones, decisiones y vínculos y cómo el diseño de experiencias memorables debe considerar no solo lo cognitivo, sino también lo somático y sensorial mediante la integración de tecnología, cultura, ciencia y narrativa para construir relaciones sólidas, coherentes y emocionalmente inteligentes. ■

MÁS INFO +

» El puente donde habitan las mariposas

» Nazareth Castellanos

» Teorema de Thaler

La documentación TIC, a un solo clic

SASE: Conectividad y acceso seguro

Descubre en este documento qué es SASE y sus beneficios, y cómo Ikusi ha construido, con tecnología Cisco, un servicio integral que combina capacidades de SD-WAN con funciones integrales de red y ciberseguridad para respaldar las necesidades dinámicas de acceso seguro de las empresas en el entorno digital.

Mapa de soluciones NIS2

¿Cómo cumplir con NIS2? ¿Qué soluciones tecnológicas dan respuesta a las exigencias de esta normativa? Consulta este mapa de soluciones, proporcionado por Kaspersky, y conoce no solo los aspectos clave de la norma, sino cómo cubrir los requisitos técnicos para darle cumplimiento.

Éxito Empresarial y Digitalización en España

Advice Strategic Consultants ha publicado una nueva ola de su informe "Éxito empresarial y Digitalización", sobre el estado de la Digitalización económica y empresarial de España en 2025.

En su estudio, para el que la consultora económica y empresarial ha entrevistado a empresas de toda índole y líderes de opinión, se refleja el estado de la Digitalización en nuestro país, así como el avance en el uso de tecnologías como Cloud, Ciberseguridad, Big Data, Conectividad, IoT e IA.

Beneficios clave de una red Wi-Fi 7

Wi-Fi 7 es la última generación de tecnología inalámbrica, diseñada para ofrecer velocidades más rápidas, mayor capacidad y menor latencia en comparación con Wi-Fi 6 y versiones anteriores. Su llegada abre un mundo de posibilidades para las empresas que buscan una conectividad más rápida, segura y eficiente. Descarga este documento y prepárate para transformar tu experiencia de conectividad.