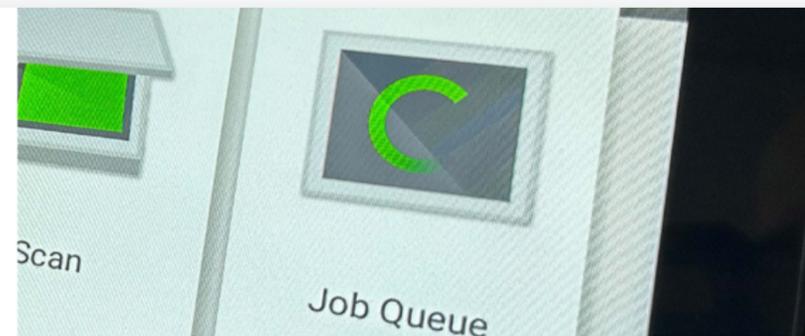
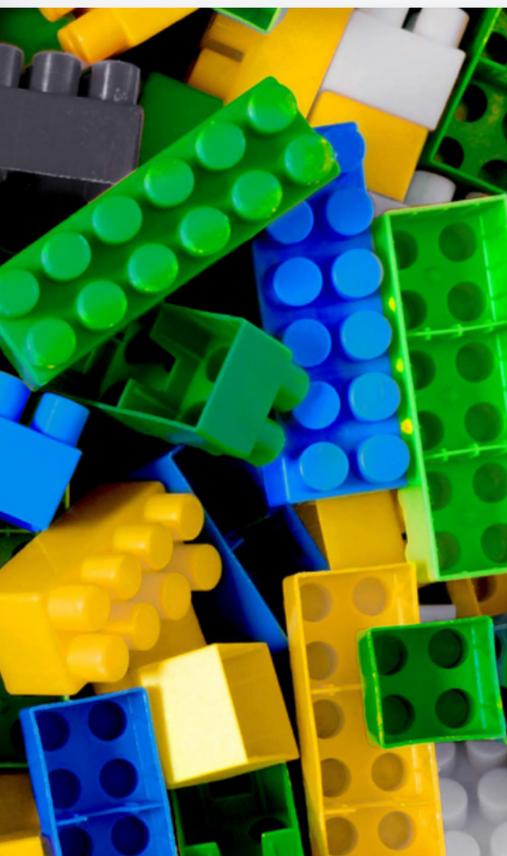


# El estado actual del Turismo 4.0 en España

Las empresas ante el reto de protegerse

Cómo luchar contra ataques impulsados por IA

**COMPARATIVA**  
soluciones de gestión de procesos empresariales (BMP)



## Nuevas impresoras A3 Serie-9 de Lexmark

### **Versátil**

Consiga una solución avanzada de impresión y digitalización para su empresa.

### **Sencilla**

Impresión de calidad sin complicaciones. Fácil navegación, durabilidad y una gran variedad de sofisticadas herramientas de seguridad.

### **Sostenible**

Impresión eficiente y sostenible. Hecha con un 56-73% de plástico reciclado. Diseño compacto que reduce el impacto medioambiental. Diseñada para durar más de siete años.

- 4 **Carta del Director**
- 5 **Actualidad**
- 16 **Webinars y encuentros BYTE TI**
- 31 **Comparativa** Soluciones de gestión de procesos empresariales (BPM)
- 39 **El estado actual del Turismo 4.0 en España**
- 49 **Legalidad TIC**
- 51 **Mujeres TIC** María Eugenia Carbonell
- 53 **Un CIO en 20 líneas** Pablo Giancarli
- 55 **Aplicación práctica**
- 58 **Tendencias**
- 62 **Entrevista** Antonio García Romero
- 64 **Cibercotizante**



N.º 328 | ÉPOCA IV  
 Edita: Publicaciones Informáticas MKM  
 Julio - Agosto 2024.

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

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

**Redacción**  
 Vanesa García (vgarcia@revistabyte.es)

**Coordinador Técnico**  
 Regina de Miguel

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

**Fotógrafos**  
 P. Varela, E. Fidalgo

**Diseño de portada**  
 Juan Medina

**Diseño y maquetación**  
 Juan Medina www.juanmade.com

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

**DEPARTAMENTO COMERCIAL**  
 Directora comercial: Isabel Gallego (igallego@mkm-pi.com)  
 Account Manager: Laura Sierra (lsierra@mkm-pi.com)  
 Tel.: 91 632 38 27

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

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

**Revista mensual de informática**  
 iSSN: 1135-0407

**Depósito legal:** B-6875/95

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

## Carta del Director



**Manuel Navarro Ruiz**  
Director de BYTE TI

# La importante relación CIO-CISO

Hace no tantos años, la figura del CISO era prácticamente inexistente en la gran mayoría de las empresas españolas. Su labor era realizada por el departamento de TI que dirigía el CIO. Hoy, sin embargo, no se entiende ninguna gran compañía que no tenga un departamento enfocado exclusivamente a la ciberseguridad.

Los ataques han aumentado en número y son cada vez más sofisticados por lo que las organizaciones llevan años realizando inversiones que protejan sus activos. Y aquí, la labor del CISO es esencial.

El problema viene cuando no hay un entendimiento entre el departamento de TI y el de tecnología. Al principio, cuando las empresas empezaban a incorporar la figura del CISO a sus plantillas y comenzaron a crear los departamentos de ciberseguridad, los CIOs se mostraban recelosos. Era una actitud más que comprensible. Muchos de ellos se preguntaban por qué su empresa estaban creando ese departamento cuando las funciones de ciberseguridad las estaban realizando ellos. ¿Acaso estaban haciendo mal su trabajo? ¿La empresa les había retirado la confianza?

Con el paso de los meses, vieron que esas dudas eran infundadas: no sólo las empresas confiaban en su trabajo, sino que la irrupción del

departamento de seguridad suponía un mayor apoyo para el departamento que dirigían.

Y así llegamos al día de hoy, en el que ambos departamentos trabajan de forma conjunta para fortalecer el negocio de la compañía. Sin embargo se producen tiranteces. En ocasiones, las estrategias del CIO y del CISO no están alineadas y, en ese momento, se puede producir un problema importante que afectará a la compañía entera.

Esto es lo que puede haber pasado en El Corte Inglés, donde su CIO, Roberto Solbes, acaba de ser despedido, por problemas con la CISO de la compañía, Catalina Polán [según informan desde El Confidencial](#). Solbes fue fichado desde el Banco Sabadell hace poco más de un año, así que es de suponer, que el motivo del despido, es que el trabajo de ambos departamentos iba por diferentes caminos.

Es importante que CIO y CISO trabajen de forma conjunta. Lo pusieron muy claro los responsables de Sanitas hace unos meses en un [evento organizado por Byte TI](#). Sólo así puede mejorar el negocio de la empresa.

## Actualidad

# El CISO de AWS insta a implementar la cultura de la ciberseguridad

Cultura. A esa palabra tan simple, pero a la vez tan profunda debería reducirse la ciberseguridad. Esas tres sílabas son fundamentales para la estrategia de cualquier empresa. Al menos, así parece entenderlo el CISO de AWS, Chris Betz, tal y como mostró durante la inauguración de re:Inforce, el evento de la multinacional dedicado exclusivamente a la ciberseguridad.

**MANUEL NAVARRO**  
Filadelfia (EE.UU.)

El directivo hizo hincapié en la importancia de que la ciberseguridad impregne todos los escalafones de una empresa. Y para ello, puso como ejemplo a su propia compañía. Tal y como expresó “después de haber sido cliente de AWS durante muchos años, pensaba que entendía la seguridad de AWS. Sin embargo, no comprendía realmente la profundidad de la inversión en seguridad y las capacidades que tiene esta compañía”.



Betz se incorporó a AWS en Agosto del año pasado y ese cambio le ha permitido apreciar mejor la cultura de seguridad que impregna AWS. Tal y como explicó, “como cliente, cuando se elige un proveedor de la nube, se establece una relación a largo plazo. Se necesita un socio que esté profundamente comprometido con la seguridad. Un socio que mantenga a salvo sus activos más valiosos. Porque no todas las nubes están construidas de la misma manera, especialmente cuando se trata de seguridad. En AWS, hemos desarrollado una cultura de seguridad realmente sólida durante un largo periodo de tiempo. Construir y mantener esa cultura requiere un enfoque de inversión

constante. Esto es importante. Una cultura de seguridad no se construye de la noche a la mañana y puede perderse si no hay un esfuerzo y una inversión constantes”.

Para mostrar cómo esa cultura abarca toda la empresa aseguró que “facultamos a nuestros equipos de servicio para que se apropien profundamente de la seguridad de nuestros productos. Cada equipo tiene un conocimiento profundo de sus productos y servicios, lo que les permite tomar decisiones tempranas e inteligentes sobre cómo construir estos servicios de forma más segura. Los líderes de nuestros equipos de servicio se responsabilizan de la seguridad de sus servicios, y nosotros, como líderes de AWS, también les responsabilizamos a ellos. Para hacerlo mejor, necesitamos apoyar a nuestros equipos de servicio y ayudar a escalar las mejores prácticas de seguridad. Por eso hemos creado el Consejo de Audiencia de AWS. Los guardianes son ingenieros integrados en nuestros equipos de servicio que desarrollan una profunda experiencia en seguridad y ayudan a escalar las prácticas de seguridad en AWS. Como parte de los equipos de servicio, los guardianes están presentes en cada paso del ciclo de desarrollo, desde la planificación dividida hasta las reuniones de destacar y las revisiones

## Actualidad

de seguridad, para dar voz a las decisiones de seguridad y ayudar a crear software más seguro”.

Al final, el objetivo, como el de cualquier empresa, es vender sus soluciones y productos y para ello se necesitan argumentos. El de AWS es un argumento sólido: la seguridad. Como explicó Betz, “cuando se trata de seguridad, tenemos que actuar como un equipo unificado, y en AWS lo hacemos. En AWS, cada asunto relacionado con la seguridad se eleva rápidamente a un equipo de seguridad que asume la propiedad. Por esta cultura de la seguridad, los productos y soluciones de AWS siempre han sido seguro por diseño, definiendo prácticas, tecnologías y controles que están profundamente integrados en todas las capas, desde los centros de datos físicos hasta el diseño de la red y las arquitecturas de superficie”.

El máximo responsable de la ciberseguridad de Amazon Web Services hizo un repaso de una buena parte de las soluciones en las que la seguridad está embebida desde el inicio, desde Graviton 4, su chip que cifra por completo todas las interfaces físicas de hardware de alta velocidad, incluida la DRAM o AWS Nitro Enclaves, una capacidad de EC2 que permite entornos de ejecución aislados que protegen y aseguran aún más el procesamiento de datos altamente confidenciales.

## El CISO de AWS insta a implementar la cultura de la ciberseguridad

### TAMBIÉN LOS SERVICIOS

AWS es consciente de que los clientes están cada vez más preocupados por su ciberseguridad. Y esa cultura también la traslada a los servicios, uno de los mayores negocios de la multinacional. “Tenemos un enfoque muy claro en proporcionar servicios resistentes, seguros y duraderos. Esto significa que no tenemos ningún miedo en desarrollar nuevas herramientas o incluso reescribir el código existente, si vemos que puede ser más seguros. Por ejemplo, el año pasado, sin ir más lejos, más del 98% de los paquetes en producción en Amazon se escribieron utilizando lenguajes seguros para la memoria”.

Asimismo, en esa cultura de ciberseguridad, las pruebas y el testing es muy importante para la organización. Tal y como expuso el CISO de la multinacional, “las pruebas son un concepto importante para garantizar que el sistema se comporta de la forma esperada. Hacemos tanto pruebas positivas como negativas, en las que probamos el sistema con entradas no válidas”.

Las pruebas se pueden hacer de forma manual o de manera automatizada. Esta última opción es una apuesta firme de la compañía, porque ambas categorías de pruebas están limitadas por los tipos y la gama de entradas. Betz se preguntó “¿qué ocurriría si se pudieran probar todas las entradas posibles? El razonamiento automatizado considera infinitas entradas posibles para



sistemas, algoritmos y configuraciones de formas que no son seguras. Su gran ventaja es que nos permite ver de qué comportamientos es capaz el sistema y, a continuación, identificar incluso los comportamientos que hay que corregir. En el caso de los sistemas complejos, las posibles entradas a considerar son muy grandes o incluso infinitas. Podemos hacerlo mejor. Las técnicas de razonamiento automatizado utilizan la lógica formal para explorar ese espacio infinito en sólo unos segundos, y lo hacen de forma sistemática y exhaustiva. En materia de seguridad, lo utilizamos para verificar la corrección de los protocolos criptográficos, la lógica de autorización y la coherencia de los sistemas de almacenamiento. También para que los clientes puedan demostrar que no hay accesos no deseados mediante el razonamiento sobre políticas y controles de red”.



## Actualidad

# ServiceNow digitaliza y automatiza los servicios IT de Abanca

ServiceNow ha anunciado que Abanca ha seleccionado su plataforma Now Platform para optimizar y mejorar sus Operaciones de Servicios (ServiceOps), logrando mayor resiliencia, trazabilidad y eficiencia.

Con tres millones de clientes, Abanca está implementando soluciones que aumenten la automatización y permitan resolver proactivamente problemas e incidencias en las operaciones y servicios. En este sentido Rebeca Cores, Directora de Operaciones e Infraestructura de la entidad asegura que, "la plataforma de ServiceNow nos permitirá gestionar los servicios de TI de manera más robusta, automatizada, trazable y alineada



con las mejores prácticas, mejorando así la satisfacción, la eficiencia operativa y promoviendo la mejora continua de los procesos operativos, lo que es imperativo para abordar DORA con garantías".

Por su parte, Álvaro Guardado, director de ventas de ServiceNow Iberia explica que, "Abanca sitúa la innovación y la mejora continua de sus procesos internos en el centro de su estrategia empresarial. Por eso, con su apuesta por ServiceNow, Abanca podrá lograr la máxima eficiencia y eficacia en sus operaciones y procesos de negocio".

Para gestionar de manera integrada los Servicios y Operaciones de TI, siguiendo las mejores prácticas de ITIL y aprovechando el poder de la inteligencia artificial, Abanca utilizará la Now Platform de ServiceNow. Esta implementación permitirá a los departamentos de TI de la entidad trabajar en una plataforma de última generación, apoyándose en las soluciones de ServiceOps de ServiceNow.

Esto facilitará la colaboración proactiva y fluida, gracias a la inteligencia artificial y el machine learning, previniendo incidencias, resolviendo problemas rápidamente y evitando cuellos de botella en los procesos de TI.

FERNANDO JOFRE



## Pólizas ciber y coberturas de la IA

En nuestro número anterior en la sección de Tendencias se abordaban los riesgos de la IA en materia de ciberseguridad. Un texto muy interesante, al que creo que le faltaba una visión complementaria: la de los seguros ciber. Según el [Estudio sobre Ciberseguridad y Gestión del Riesgo Ciber en España 2024](#) publicado por AON, resulta que en las pólizas que cubren riesgos de ciberseguridad no se suele establecer (de momento) cualquier referencia expresa a un incidente ocasionado o derivado del uso de la IA. Menos mal que tampoco aparecen exclusiones específicas.

Nos recomiendan acertadamente que estemos atentos a la hora de cumplimentar solicitudes de seguro. Si bien las aseguradoras no están haciendo preguntas específicas sobre el uso de la IA en la organización, conforme su incorporación siga creciendo, sin duda los cuestionarios podrían cambiar. Afortunadamente las primas de seguro se están reduciendo gracias a la entrada de nuevas aseguradoras en España, en un mercado cuyo volumen de negocio ha crecido en 2023 nada menos que un 25%, alcanzando ya los 170 M€. El informe nos indica que las empresas por debajo de los 250 m€ todavía no contratan. ¿Es este mi caso?

## Actualidad

MANUEL LOPEZ



## Elegir la Pastilla Roja

Hace 25 años, en 1999, "The Matrix" nos presentó una metáfora poderosa: la elección entre la pastilla roja y la pastilla azul. Esta metáfora es hoy más relevante que nunca en el contexto de la IA.

Elegir la pastilla roja significa comprometerse a entender, cuestionar y moldear cómo la IA influye en nuestras vidas. La pastilla azul, representa la comodidad de la ignorancia, la indiferencia y la aceptación pasiva de sus impactos.

Hoy, más que nunca, es imperativo que elijamos conscientemente cómo interactuamos con la IA. La adopción de la IA trae consigo la disrupción y el cambio. Elegir la pastilla roja significa abrazar la innovación como motor del progreso, pero debe ser equilibrada con una comprensión crítica de sus impactos. Debemos priorizar la transparencia, la innovación ética y el empoderamiento individual.

La elección de la pastilla es una necesidad práctica para abordar el complejo mundo digital en el que vivimos y asegurarnos de que la IA se desarrolle y utilice de manera que beneficie a la humanidad en su conjunto, en lugar de permitir que nos controle sin nuestra plena comprensión y consentimiento. La elección es nuestra, y sus implicaciones son profundas y duraderas.

En este momento crucial, optemos por la pastilla roja.

## Microsoft inaugura su primera región cloud en España para IA

Microsoft acaba de anunciar la apertura de su primera región cloud en España, ubicada en varias localizaciones dentro de la Comunidad de Madrid. Esta nueva infraestructura permitirá a la compañía ofrecer servicios y soluciones de Inteligencia Artificial y cloud a empresas y entidades públicas tanto de España como del resto de Europa.

Con la denominación Spain Central, esta región cloud garantizará fiabilidad, seguridad, privacidad y residencia de datos, acelerando la digitalización de las organizaciones españolas y potenciando el desarrollo de la Economía de la IA en el país, así como el crecimiento de la industria tecnológica local.

Alberto Granados, presidente de Microsoft España, destaca que "Estamos comprometidos con España, mediante inversiones, el impulso de alianzas, y la creación de programas que garanticen un amplio acceso a la nube, así como a los servicios de IA que permitan a las organizaciones y a las personas desarrollar y utilizar la tecnología de manera que sirva al bien público".



Esta iniciativa es parte de un compromiso de inversión de Microsoft en España, que alcanzará los 2.100 millones de dólares entre 2024 y 2025. La expansión de la nube de Microsoft en España responde a la creciente demanda de soluciones de IA y cloud, y según IDC, podría agregar más de 10.700 millones de dólares al PIB nacional y generar cerca de 77.000 empleos entre 2024 y 2030.

Spain Central ofrecerá los servicios más avanzados de productividad, análisis de datos, ciberseguridad, computación y almacenamiento, incluyendo Azure, Microsoft 365, Dynamics 365 y Power Platform. También contará con servicios de Inteligencia Artificial generativa, posicionándose entre las regiones cloud más avanzadas de Europa. La nueva región garantizará alta disponibilidad, escalabilidad y seguridad en los servicios en la nube, con la opción de residencia de datos en el país para las organizaciones españolas.

## Actualidad

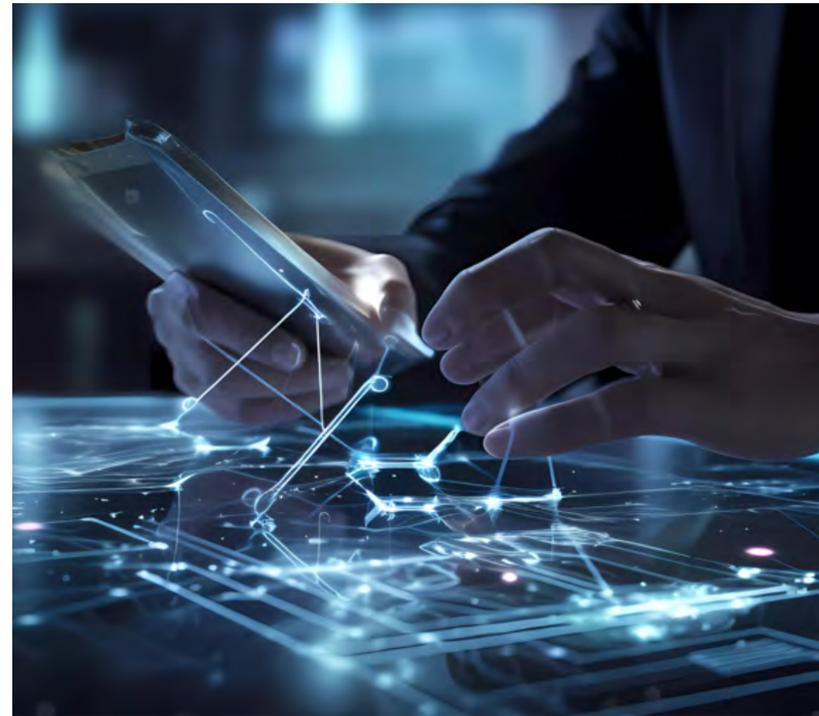
# España se sitúa a la cola en la adopción de la IA

La introducción de nuevas herramientas de IA ha generado una transformación significativa en diversos sectores. Según el informe sobre esta tecnología de InfoJobs, uno de cada cuatro empleados ha utilizado IA en su trabajo, lo que representa un incremento de 5 puntos porcentuales respecto a marzo de 2023, cuando solo el 18% reportó su uso tras cuatro meses desde su lanzamiento inicial. Además, la familiaridad con estas herramientas ha aumentado en 10 puntos porcentuales;

A pesar de este crecimiento, el estudio Decoding Global Talent 2024, llevado a cabo por Boston Consulting Group (BCG) junto con InfoJobs en España como socio exclusivo de The Network, indica que España está rezagada en la adopción de la inteligencia artificial. El informe revela que solo el 26% de los encuestados en España utilizan la IA semanal o mensualmente, situando al país por detrás de potencias internacionales como EE.UU. (39%) y de otros países europeos como Portugal (33%), Alemania (32%), Polonia (31%) y Francia (29%). España supera a naciones como Jordania (25%), Rumanía (23%), Hungría (22%) e Italia (21%).

### Adopción de la IA en España

Solo el 27% de los españoles usa la inteligencia



artificial (IA) regularmente, frente al 39% a nivel mundial. De estos, el 10% la utiliza semanalmente y el 17% mensualmente. Un 61% no utiliza la IA, comparado con el 48% global; el 40% la conoce pero no la usa, y el 21% ni la conoce ni la utiliza. Además, un 13% la ha usado una o dos veces.

Para uso profesional, los españoles emplean la IA principalmente en tareas de escritura (40%), estudio y búsqueda (36%), y tareas administrativas (34%). Los usos menos comunes son la detección de fraude (4%), atención al cliente (11%) y programación (17%). En el ámbito personal, el desarrollo de competencias (44%), conocimiento

general (43%) y traducción (41%) son los usos más frecuentes. La amistad virtual y apoyo emocional son los menos utilizados (4%).

Los sectores con mayor uso de IA en España son IT (66%), marketing y medios (63%), e ingeniería y técnicos (40%). Los desafíos principales para la adopción de la IA incluyen la dificultad de escribir indicaciones (30%), la lentitud (28%) y la falta de datos disponibles (26%).

En cuanto a la percepción de la IA, el 25% de los españoles cree que no afectará al empleo, el 44% piensa que afectará algunas tareas específicas, y el 26% considera que traerá una gran transformación. Un 6% opina que algunos trabajos desaparecerán. España es el país europeo con mayor percepción del impacto de la IA en los próximos cinco años.

Sobre el reskilling, el 61% de los españoles está dispuesto a someterse a este proceso, mientras que el 33% lo haría solo si es necesario y el 5% no está dispuesto. La mitad de los encuestados considera que se necesitan mejores programas de aprendizaje, más tiempo (39%) y mayor apoyo del empleador (34%) para el reskilling.

## Actualidad

# Cisco invertirá 1.000 millones en desarrollar soluciones de IA

Cisco Investments ha lanzado un fondo de 1.000 millones de dólares dedicado a la inteligencia artificial (IA) con el objetivo de fortalecer el ecosistema de startups y fomentar el desarrollo de soluciones de IA seguras y confiables. Como parte de este nuevo fondo, la compañía está realizando inversiones estratégicas en empresas como Cohere, Mistral AI y Scale AI, entre otras.

Y es que, la IA está transformando el mundo a una velocidad sin precedentes, resaltando la creciente importancia de la tecnología en las interacciones globales de las empresas. Según datos recientes de IDC, se prevé que el mercado mundial de IA se duplique, superando los 500.000 millones de dólares en los próximos tres años. Ahora, las empresas tienen la oportunidad de aprovechar el potencial de la IA generativa (Gen AI) para mejorar sus productos y servicios y brindar un mejor servicio a sus clientes y usuarios finales.

Durante más de 30 años, Cisco Investments ha invertido y se ha asociado con cientos de empresas para impulsar la innovación tanto en el marco de las principales arquitecturas de Cisco como en nuevas áreas estratégicas”, afirma Mark Patterson, Director de Estrategia en Cisco. “Estamos bien posicionados para convertirnos en el mejor socio estratégico de los clientes que

buscan construir, proteger y potenciar la IA. Además, Cisco se compromete a invertir en el ecosistema de IA más amplio para satisfacer aún mejor las necesidades de nuestros clientes”.

### Cisco con la IA

En los últimos años, Cisco ha llevado a cabo más de 20 adquisiciones e inversiones enfocadas en inteligencia artificial (IA), potenciando sus capacidades en GenAI y Machine Learning, así como la integración de IA en toda su gama de productos. Además de estas inversiones, Cisco colaborará con empresas de IA para co-innovar y reforzar su posición como proveedor neutral. Entre las inversiones comprometidas con el nuevo fondo de IA se encuentran:

- **Cohere:** Ubicada en Toronto y San Francisco, Cohere ofrece modelos de lenguaje grande (LLM) enfocados en la seguridad y capacidades líderes en la industria de generación aumentada de recuperación (RAG, Retrieval-Augmented Generation) diseñadas para satisfacer las necesidades empresariales.
- **Mistral AI:** Esta empresa global con sede en París se especializa en IA generativa para empresas, combinando excelencia científica, un enfoque abierto y una visión responsable de la tecnología.
- **Scale AI:** Con sede en Estados Unidos, proporciona una plataforma integral centrada en datos que ofrece capacitación y validación para aplicaciones de IA. Cisco participó recientemente en la financiación Serie F de Scale AI como el mayor inversor estratégico de la ronda.



## Actualidad

# El camino de Acer hacia la digitalización sostenible

VANESA GARCÍA  
Lugano. (Suiza)

Acer acogió en sus oficinas de Lugano, Suiza, una rueda de prensa internacional con los principales directivos de la empresa en Europa donde se destacaron aspectos clave en cuanto a la atención al cliente, la estrategia de canal y el compromiso con la sostenibilidad además de presentar nuevos dispositivos. Tal y como se puso de manifiesto Acer se compromete a apoyar la transformación digital en la educación mediante una gama de productos especializados, una red de socios y relaciones con actores clave del sector educativo:

Programa de Socios para la Educación: Este programa, con más de 10 años de existencia, ayuda a las escuelas a adoptar tecnologías adaptadas a sus necesidades. Acer colabora con European Schoolnet y la Coalición Mundial por

la Educación de la UNESCO para impulsar la innovación en la enseñanza.

Prácticas de aprendizaje avanzadas: Acer ofrece tecnologías como Esports in Education y SpatialLabs para fomentar el desarrollo de habilidades y estudios STEM.

Soluciones de IA: Acer utiliza IA para mejorar la productividad y creatividad de los educadores, ofreciendo portátiles TravelMate con hardware especializado en IA que incluye procesadores Intel AI Boost o AMD Ryzen AI, y soluciones como Acer PurifiedView y Acer PurifiedVoice.

"Nos hemos centrado en crear un ecosistema de socios para impulsar la transformación digital del mercado educativo", comentó Cristina Pez, directora Comercial de EMEA. "La colaboración diaria con las partes interesadas del sector educativo permitió a Acer desarrollar productos especializados que respondían a las necesidades de educadores y estudiantes".

## Nuevos equipos

Acer ha presentado dos nuevos portátiles Acer Chromebook Plus Enterprise: el Acer Chromebook Plus Enterprise 515 y el Acer Chromebook Plus Enterprise Spin 514. Diseñados con tecnología avanzada y capacidades de IA de Google,

estos dispositivos están orientados a mejorar la eficiencia y seguridad en el trabajo en la nube. Equipados con ChromeOS Enterprise, ofrecen seguridad de primer nivel, gestión sencilla y soporte administrativo mejorado.

"Los nuevos modelos Acer Chromebook Plus Enterprise llevan lo mejor de la IA en ChromeOS a las organizaciones para impulsar la eficiencia y la colaboración entre su fuerza de trabajo", dijo Massimiliano Rossi, VP Product Business Unit, Acer EMEA. "Organizaciones de todo tipo, desde oficinas corporativas a pequeñas empresas, minoristas y sanitarias necesitan dispositivos fiables y habilitados para IA para impulsar su carga de trabajo, y estos nuevos portátiles Acer Chromebook Plus Enterprise ofrecen todo eso y más".

La compañía también ha lanzado nuevos modelos de la serie TravelMate con IA. Estos portátiles, equipados con procesadores de última generación con NPU integradas, ofrecen un rendimiento superior, mayor productividad, movilidad avanzada, y mejores funciones de seguridad y conectividad. La IA está revolucionando los negocios al aumentar la productividad, personalización y eficiencia energética, beneficiando tanto a proveedores como a socios del mercado de PC.



Actualidad - Te interesa

# Roomba Combo j9+: La revolución de la limpieza inteligente

Si estás pensando en comprar un robot aspirador 2 en 1 de alto rendimiento, te proponemos el último modelo que el fabricante iRobot ha puesto en el mercado, Roomba Combo j9+. Un robot aspirador y fregasuelos que se vacía automáticamente y repone el líquido de fregado, además de saber determinar qué áreas de la casa están más sucias para priorizar su limpieza. Un conjunto de inteligencia y tecnología que te llevará a ver la limpieza del hogar de manera muy diferente a como lo has visto hasta ahora. Una innovación destacada del Roomba Combo j9+ es la incorporación de la estación de vaciado y rellenado automático Clean Base, que se encarga de vaciar automáticamente la suciedad y reponer el agua del robot. Esto garantiza una limpieza continua sin interrupciones y reduce en gran medida la intervención humana.

El robot de limpieza cuenta, además, con el sistema operativo iRobot OS, que presenta funciones clave que lo hacen más inteligente, como Dirt Detective y SmartScrub. El primero permite al robot determinar las áreas más sucias de la casa y priorizar su limpieza en función de este análisis, mientras que SmartScrub ofrece una limpieza más profunda y precisa en zonas

específicas, ejerciendo una presión constante para eliminar la suciedad resistente. El sistema operativo también ofrece la limpieza habitación por habitación, permitiendo a los usuarios tener un control absoluto sobre la limpieza de su hogar. A través de la aplicación iRobot Home, los usuarios pueden personalizar la limpieza y ajustar los parámetros según sus necesidades y preferencias individuales.

iRobot ha centrado sus esfuerzos en áreas clave de preocupación para los usuarios, como la eficacia, la fiabilidad y el control automático de la limpieza. Mediante pruebas exhaustivas, se ha logrado abordar problemas recurrentes como el mal funcionamiento en la detección de obstáculos, problemas en los paños de fregado y la incapacidad para aprender de experiencias anteriores. Estos avances tecnológicos aseguran una experiencia de limpieza superior y eficiente. Roomba Combo j9+ también destaca por su diseño elegante y funcional, que se integra fácilmente en cualquier hogar. Su sistema de limpieza en 4 fases y cepillos de goma dobles le permiten recoger eficientemente desde polvo fino hasta suciedad persistente, incluyendo pelos de mascotas. Además, su exclusivo sistema D.R.I.



(Dry Rug Intelligence) evita mojar las alfombras elevando automáticamente el paño de fregado al detectarlas. Por último, la confidencialidad y seguridad de los datos es una prioridad para iRobot, que utiliza los más altos estándares de encriptación de datos y asegura que los datos de los clientes están protegidos. Los datos de los clientes pueden utilizarse para mejorar su experiencia de limpieza.

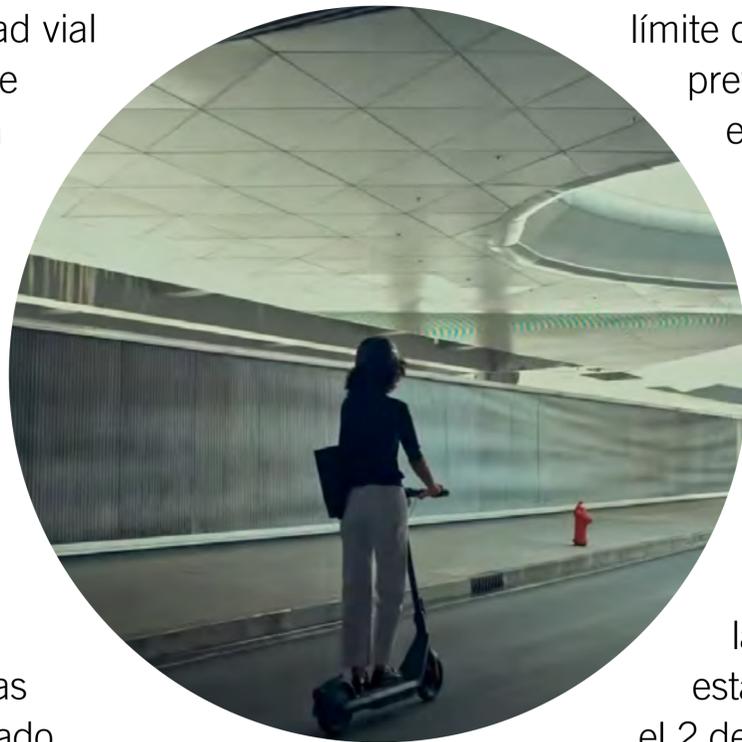
En resumen, Roomba Combo j9+ de iRobot presenta innovaciones técnicas significativas con su estación de vaciado y rellenado automático, el sistema operativo iRobot OS proporciona funciones como Dirt Detective y SmartScrub, que se engloba en un diseño eficiente y seguro. Estas mejoras aseguran una limpieza eficiente y personalizada.

## Actualidad - Te interesa

# Verano seguro en patinete eléctrico: lo que debes saber

Llega el verano y con él, la creciente popularidad de los patinetes eléctricos como una opción de movilidad urbana rápida y eficiente. Ante este aumento en su uso, Segway-Ninebot resalta la necesidad de fomentar una serie de buenas prácticas de seguridad vial entre los usuarios. La reciente actualización de la normativa en España hace que sea más importante que nunca que los usuarios estén bien informados para garantizar una circulación segura y evitar sanciones.

¿Qué se debe tener en cuenta? Es esencial elegir patinetes homologados: desde enero de 2024, todas las marcas y modelos en el mercado deben estar homologados de acuerdo con la nueva normativa publicada por la Dirección General de Tráfico (DGT). Los fabricantes deben mostrar una certificación de fábrica mediante una placa informativa visible, con información sobre el vehículo como serie, número de certificado, marca, modelo y año de fabricación. Los vehículos de movilidad personal que se comercializan desde el 22 de enero de 2024 deben ser certificados y aparecer en la lista de la DGT.



Mientras tanto, hay algunos consejos esenciales que deben tenerse en cuenta. Por ejemplo, el uso del casco es altamente recomendable para protegerse en caso de caída o colisión; mantener una velocidad segura y respetar el límite de 25 km/h es crucial para prevenir accidentes; ser visible es una medida de seguridad vital, especialmente de noche, utilizando luces y dispositivos reflectantes.

Asimismo, hace poco se ha presentado un proyecto de ley que hará obligatorio contratar un seguro de responsabilidad civil. Aunque la medida no será inmediata, está previsto que entre en vigor el 2 de enero de 2026.

## Patinetes eléctricos homologados y eficientes

En Segway-Ninebot ofrecemos tres gamas de patinetes eléctricos homologados según la normativa actual. El MAX G2 es ideal para una conducción superior, con un motor de 900W, capacidad para pendientes de hasta un 22% y una autonomía de hasta 70 km. Además, cuenta con suspensión hidráulica delantera y trasera de doble muelle, un manillar más ancho

con intermitentes integrados, alarma antirrobo, sistema de control de tracción (TCS) y la función Buscar de Apple para localizarlo.

Por su parte, la serie F2, que incluye los modelos F2, F2 Plus y F2 Pro, está diseñada para usuarios exigentes que buscan estabilidad y seguridad, con un manillar ancho, intermitentes integrados, neumáticos de 10 pulgadas autorreparables, tracción trasera, freno de disco delantero, freno electrónico trasero y control de tracción. El modelo F2 Pro añade suspensión delantera y la función Buscar de Apple.

La serie E2, con los modelos E2 y E2 Plus, es una solución asequible para la movilidad urbana, con un estilo surf, salpicadero ampliado, neumáticos sin cámara de aire duraderos, sistema de doble freno y un motor potente para desplazamientos cortos. El E2 Pro E combina potencia y autonomía con tecnología RideyLong, ofreciendo hasta 35 km de recorrido, un motor de 750 W y tracción trasera, además de un sistema de control de tracción (TCS), neumáticos tubeless de 10 pulgadas y frenado dual. Este modelo es compatible con la app Buscar de Apple y la app Segway-Ninebot 6.0 para monitoreo y personalización, convirtiéndolo en una opción inteligente y segura para la conducción urbana.

Actualidad - Te interesa

# Cómo levantar con éxito la última barrera de protección de la ciberseguridad

Ante el incremento en número y complejidad de las amenazas a la seguridad de los entornos IT, salvaguardar los datos de negocio se ha convertido en la última y más definitiva barrera para garantizar la continuidad de las organizaciones. Hoy en día, ninguna organización, independientemente de su presupuesto o tamaño, está exenta de sufrir un incidente en sus sistemas, lo que pone de manifiesto la importancia de contar con una estrategia de ciberseguridad bien diseñada y encaminada a la continuidad del negocio. La combinación de backup y plan de recuperación frente a desastres (DRP, por sus siglas en inglés) es la mejor medida de seguridad pasiva que pueden adoptar las empresas para garantizar su transformación digital.

Y para conseguirlo, una de las formas más efectivas para que así sea es seguir la regla 3-2-1 del backup: tres copias de los datos, dos en soportes distintos y una externalizada y localizada en un lugar físico diferente al principal. Y ahí, por su seguridad y disponibilidad, la nube se ha convertido en la mejor opción para almacenar esas copias de seguridad, externalizando tanto las complejidades derivadas de la gestión del almacenamiento como las garantías de recuperación de sus datos. Sin embargo, debido a la complejidad de los entornos con los que trabajan actualmente los equipos técnicos, no resulta fácil elegir una solución que garantice la integridad de la información y facilite la completa recuperación de los sistemas desde la nube ante los incidentes más graves.



Como pionero en soluciones de infraestructura cloud para empresas, Arsys responde a estas necesidades de los profesionales IT diseñando unas soluciones a medida de copia de seguridad y recuperación completa, que combinan la fiabilidad y facilidad de uso del reconocido fabricante Veeam Software y el rendimiento, soporte técnico y la seguridad que ofrece la nube de la compañía.

La relación comercial entre ambas compañías está tan consolidada que Arsys es el único proveedor español que cuenta con la certificación Platinum en su Programa Cloud & Service Provider, el máximo nivel para los proveedores de infraestructura IT que facilitan soluciones de Veeam al cliente empresarial.

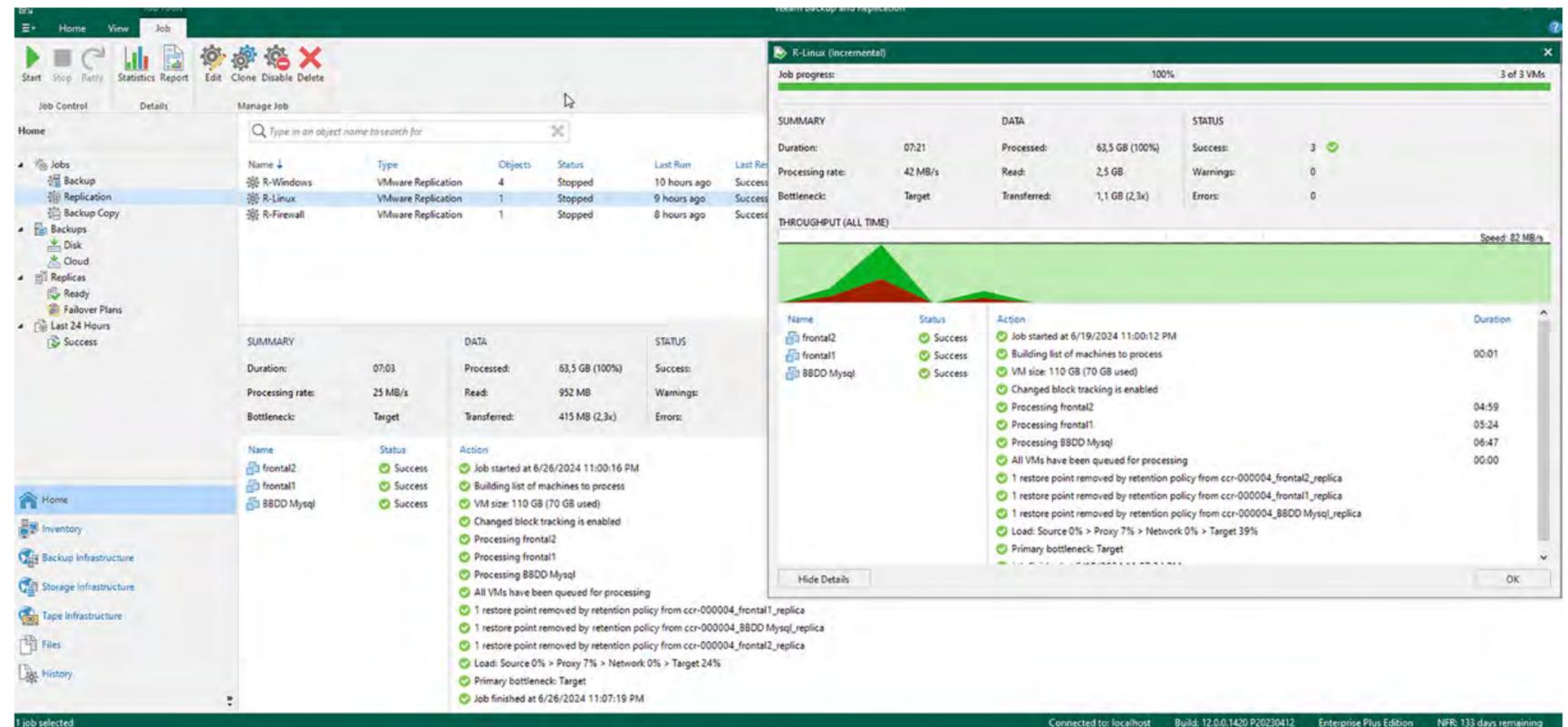
## Actualidad - Te interesa

## Cómo levantar con éxito la última barrera de protección de la ciberseguridad

### SOLUCIONES A MEDIDA

Gracias a esta combinación software-proveedor, Arsys desarrolla soluciones integrales de seguridad pasiva a medida de cada empresa y proyecto, abordando desde el análisis y la toma de requerimientos de las estrategias de ciberseguridad hasta la implantación y, si es necesario, la gestión de este tipo de entornos para backup y recuperación con un equipo de especialistas formados y con experiencia.

Una solución llave en mano, y que permite salvaguardar todo tipo de sistemas, por muy complejos que sean, como los datos de la plataforma de productividad Microsoft Office 365 o los servicios de Kubernetes que se utilizan actualmente en los entornos de desarrollo, por poner sólo dos ejemplos de su versatilidad. Además, las soluciones de seguridad pasiva de Arsys están disponibles en una versión para mayoristas y resellers que, con una consola a



su medida, podrán gestionar más fácilmente y de manera personalizada todos los recursos de backup y continuidad de sus propios clientes.

Con características tan demandadas como el repositorio inmutable para protegerse del ransomware o la aceleración WAN para acelerar la recuperación de los sistemas, las soluciones de backup y contingencia de Arsys facilitan el cumplimiento de las normativas europeas de protección de datos y la soberanía del dato de punto a punto.

Además, están alojadas en los centros de datos de la compañía en España, avalados por

la certificación TIER III con sus plataformas cumplen con las más exigentes certificaciones del sector en calidad, seguridad y sostenibilidad: la categoría Alta del Esquema Nacional de Seguridad, ISO 9001 (calidad), ISO 27001 (seguridad), ISO 50001 (eficiencia energética), ISO 14001 (gestión medioambiental), ISO 27018 (privacidad en la nube), etc. Y cuentan con el cualificado servicio de Soporte Técnico 24/7 de Arsys, localizado en España y con uno de los más elevados niveles de satisfacción del sector entre los clientes empresariales.

Más información en:  
[arsys.es/managed-services/seguridad-pasiva](https://arsys.es/managed-services/seguridad-pasiva)



## Webinars BYTE TI

# Gestión de identidades para salvaguardar la empresa

La gestión de accesos e identidades es esencial en cualquier organización. Para hablar sobre ello, Byte TI, junto con Ping Identity, organizó un encuentro que contó con la participación de Hugo Lavrador Rodrigues, subdirector de ciberseguridad, transacciones y operaciones de Mapfre; Carlos Scott, Sales Engineer de Ping Identity; Javier Santos, director de seguridad global de Santa Lucía Seguros; Jesús Salvador, CDO director program management office de Guardia Civil; Miguel Fontalvo, account executive de Ping Identity; Marian Blanque, responsable de seguridad de la información de Abertis Infraestructuras; Manuel Fernández, CISO de Inversis; Guillermo Arias, account executive de Ping Identity y Eva Otero, Jefe de área de ciberseguridad de Madrid Digital.

El encuentro comenzó tratando el cambio de nomenclatura de ForgeRock. Esta multinacional se ha fusionado con Ping Identity, manteniendo esta nueva marca. Bajo ese nombre, ofrecen la nueva Ping Identity ofrece ventajas únicas, entre las que se cuentan capacidades innovadoras



en CIAM y de identidad del personal, como la protección contra fraudes y riesgos, la verificación de identidad, la identidad descentralizada, la autorización detallada, la gestión del ciclo de vida y la gobernanza y administración de identidades (IGA). Tal y como explicó Guillermo Arias, account executive de Ping Identity, “con esta fusión ganan los clientes porque tanto la plataforma

de ForgeRock como la de Ping Identity van a convivir”. La simbiosis entre ambas es perfecta ya que como detalló Carlos Scott, Sales engineer de Ping Identity “por separado, ambas plataformas lideraban el mercado americano y europeo. Ahora liderarán ambos y los clientes se van a beneficiar de tener acceso a una mayor cartera de productos y servicios”.

## Webinars BYTE TI

### Como abordar la gestión de identidades y accesos

A partir de aquí se abordó cómo están gestionando las organizaciones el control de accesos e identidades. Eva Otero, Jefe de área de ciberseguridad de Madrid Digital, explicó que “en la Comunidad de Madrid, gestionamos todos los usuarios salvo los sanitarios. Ahora estamos solicitando una consultoría para ver el estado en el que nos encontramos a nivel de procesos y tecnologías. Una vez que tengamos los resultados vamos a ver ese gap que nos muestre las debilidades que tenemos y si es posible llegar a ese gobierno de la identidades”.

Por su parte, Hugo Lavrador Rodrigues, subdirector de ciberseguridad, transacciones y operaciones de Mapfre afirmó que “en el área de gestión de identidades de la compañía construimos todas las directrices para todas las entidades de todos los países. Tenemos que pensar por tanto en todo el sistema tecnológico de todo el mundo. También tenemos empresas que trabajan con nosotros además de los clientes, así que desde 2016 se decidió gestionar todo de forma global para lo que creamos un programa que nos permite tener varios proyectos de gestión de identidades. Ahora nos centramos en las fuentes autoritativas con el objetivo de centralizar toda la parte de los empleados. En el resto, área de agentes y proveedores, es más complicados, así que



**Guillermo Arias**  
Account executive  
de Ping Identity

hemos creados unos conectores que nos permite centralizar las peticiones”.

La diferencia en la gestión de identidades es diferente según el organismo u empresa de la que se hable. Por ejemplo, Jesús Salvador, CDO director program management office de Guardia Civil, aseguró que “el enfoque tradicional de la Guardia Civil es que tenemos normas antes de implementar los productos. El single sign on es el punto principal desde el que partimos desde hace años. Uno de los problemas que tenemos es ir al ritmo de la transformación digital que va muy rápido. En el momento en que empezamos a teletrabajar se nos rompieron los esquemas. Tuvimos la suerte de montar un SOC y han aterrizado productos en la nube que no teníamos antes. Ahora tenemos aplicaciones propias, aplicaciones para movilidad,... Los accesos, las altas o las bajas o el cambio de

## Gestión de identidades para salvaguardar la empresa



**Carlos Scott**  
Sales Engineer  
de Ping Identity

destino lo gestionamos de forma muy personal. En este caso no se automatiza en exceso”.

Por su parte, Marian Blaque, responsable de seguridad de la información de Abertis Infraestructuras explicó que “nosotros venimos de unas empresas que eran muy cerradas y al final como estás tan regulado la mentalidad era la de tener todo gestionado de forma interna. Nosotros en AB Infraestructuras, damos servicio a las unidades de negocio que tienen sus propios sistemas y sus propias identidades. Lo que hacemos es duplicar la identidad en nuestro sistema. Con esto en nuestro sistema de altas y bajas de usuario lo tenemos controlado, pero en paralelo estamos haciendo una consultoría para ver los gaps que tenemos. Las bajas cuando es un empleado o un proveedor bien definido no suelen ser un problema.



**Eva Otero**  
Jefe de área de  
ciberseguridad de  
Madrid Digital

## Webinars BYTE TI



**Hugo Lavrador Rodrigues**

Subdirector de ciberseguridad, transacciones y operaciones de Mapfre



**Jesús Salvador**

CDO director program management office de Guardia Civil



**Marian Blaque**

Responsable de seguridad de la información de Abertis Infraestructuras

El mayor de ellos son los usuarios privilegiados, porque en estos casos una baja hay que hacerla de forma muy manual”.

### Facilitar el negocio

Aunar negocio y tecnología suele ser uno de los retos de cualquier departamento de tecnología. En este sentido, Javier Santos, director de seguridad global de Santa Lucía Seguros, afirmó que “una cosa es la visión que tienes como responsable de seguridad y otra cómo eres como facilitador de negocio. El problema principal es como introduces cultura de gestión de riesgo en diferentes culturas, en diferentes divisiones, ... La casuística es muy diferente en cada una de ellas. No es una cuestión técnica sino de un problema de cultura, de cómo haces las cosas. El

modelo de gobierno de identidad es no generar pequeñas islas , que pueden hacer que la gestión y el modelo de gobierno sea un problema. Es una batalla que come muchos recursos”

Por su parte, Manuel Fernández, CISO de Inversis, cree que “hay ámbitos que, quizá por el enfoque empresarial, puede resultar más fácil implantar unas medidas, pero luego la realidad es otra. Sabes que te vas a encontrar muchos problemas pero no te queda más remedio que trabajar en esa realidad. Si a eso le añades otros factores que parecen menos importante la gobernanza se complica más todavía. En nuestro caso sucede que tenemos una plataforma que da uso a cliente final y a cliente interno y aunar una usabilidad para ambos es compleja”. La

## Gestión de identidades para salvaguardar la empresa

diferencia es cómo puede aplicar la gestión.

Para Guillermo Arias de Ping Identity, “el efecto de la seguridad sobre el negocio es muy importante. Los clientes se mueven por reducir costes, aumentar los ingresos o asegurar las infraestructura y los datos. Se trata de aplicar las políticas de seguridad de forma que no saturamos al usuario con una política que la haga inoperante. Si la seguridad impacta negativamente en el negocio, entonces hay un problema. En este sentido, la IA va a ser importante para saber cuál es el nivel de seguridad de cualquier transacción”.

Jesús Salvador considera que “dependiendo del contexto habrá que apostar por una solución u otra. En nuestro caso la heterogeneidad de las aplicaciones y los servicios también es un problema. Normalmente los departamentos de negocio quieren un producto de negocio y la autenticación puede suponer un problema para negocio. En nuestro caso la mayoría de las aplicaciones necesita una contraseña y cada aplicación tare su propia gestión de identidades, lo que nos lleva a que se pierda mucho tiempo en logearse”.

A todo ello, Manuel Fernández aseguró que “mantener todo ello además supone mucho esfuerzo. Necesitas tener distintos niveles de soporte porque la complejidad es alta y requiere

## Encuentros BYTE TI

una cantidad de recursos muy elevada, lo que dificulta la gestión. Y es difícil hacer ver a la organización que necesita todos esos recursos”. Marian Blanque incidió en que “se trata de procesos transversales en lo que tienes que presentar al comité de dirección no sólo las ventajas, sino también las pérdidas. Los CISOS siempre eramos los que poníamos pegas a todo y creo que hay que dar la vuelta a la tortilla presentando los riesgos de negocio si no se adoptan ciertas medidas. Además es importante el cambio de mentalidad de los empleados. Tu tienes muchos empleado con gente muy digital con gente que no se adapta. Ese cambio es importante haciendo ver al empleado que él aplica ciertas medidas de seguridad en su vida personal y que, por tanto, también es necesario que las adopte en su vida laboral. Además creo que es importante la simplificación de procesos con la integración de las aplicaciones”.

### Que le piden

Con ese marco los responsables de TI y de ciberseguridad piden a una solución de control de identidades, “una gestión centralizada donde poder tener un sitio unificado que sea escalable, que se integre con todo, que tenga una autenticación robusta, que incluya doble factor... Se trata de tener una herramienta que sea fácil de implementar y mantener, algo que sea asequible para todo. Se trata de acabar con el caos. La biometría está bien, pero luego



**Javier Santos**

Director de seguridad global de Santa Lucía Seguros.

en ese apartado te metes en el apartado de protección de datos”, afirmó Eva Otero.

La biometría podría ser una solución, pero como afirmó Jesús Salvador, “a nivel técnico es muy buena, pero el problema de fondo es cumplir con la legalidad. Por ejemplo, para implantar un reconocimiento facial hay que saltar la resistencia del usuario que tiene temor a que vayas a utilizar la foto para otra cosa”.

En este sentido el portavoz de Mapfre afirmó que “se trata de un problema cultural. En una entidad se trata de que los dispositivos y portátiles puedan implementarla pero esto tiene mucho coste. Nosotros estamos implementando devops para disminuir el tiempo de identificación y además identificar que alguien que nos llama

## Gestión de identidades para salvaguardar la empresa



**Manuel Fernández**

CISO de Inversis

es quien dice ser. Vamos a trabajar en un piloto para devops y no hay duda de que el factor biométrico da más seguridad”.

Finalmente, Javier Santos explicó que “si ya cuesta tener un factor de identidad culturalmente, con la biometría ese problema se acrecienta. Generalmente, la persona cuando se enfrenta a algo que no conoce siente rechazo, por eso un doble factor de autenticidad les supone un problema. Yo creo que a medida de las noticias que están apareciendo de ciberataques está provocando que el rechazo inicial se esté mitigando”.



**Miguel Fontalvo**

Account executive de Ping Identity



## Encuentros BYTE TI

# El reto del CIO y el CISO en la ciberseguridad

La ciberseguridad es uno de los pilares sobre los que se sustenta la digitalización de las empresas. Para hablar sobre cuáles son los principales retos a los que se enfrentan los CIOs y los CISOs, Byte TI, junto a Sophos y Kyocera, organizó un encuentro que contó con la participación de Javier Paniagua, CIO y director de sistemas de Risi; Carolina Oro, CIO de AXA; Álvaro Fernández, Sales Manager Iberia de Sophos; Daniel Damas, Head of IT Assurance de Nationale Nederlanden; Joan Barceló, CIO y director de sistemas de W2M; José Manuel Casillas, CIO y director de sistemas de LLYC; Javier Torres, CISO de Allfunds Bank; Manuel Serrano, CISO de Atresmedia; José Aznar Laguna, Business Development Manager de Kyocera y Óscar Monrío, director de tecnología y transformación digital de CHC Energía.



El encuentro comenzó analizando las acciones que han realizado en el último año los departamentos de ciberseguridad para mejorar su protección. En este sentido, Joan Barceló, CIO y director de sistemas de W2M, aseguró que en su caso se han centrado “en hacer un ejercicio de evangelización en materia de seguridad de la información porque muchas veces nos quedamos solo en la parte ciber, pero realmente, dentro de las grandes

organizaciones hay muchos procesos que no son únicamente ciber, sino que también son de seguridad de información. En esta parte de evangelización nos hemos centrado sobre todo en el personal interno de la compañía y también hemos realizado un trabajo importante con los diferentes partners y proveedores para asegurar que siguen las líneas que nosotros estamos marcando”.

Por su parte, Manuel Serrano, CISO de Atresmedia, se centró en la idiosincrasia de la compañía para explicar cuál es la estrategia de ciberseguridad: “Nosotros no somos una empresa al uso como las presentes. Somos un medio de comunicación y por tanto, hablar de ciberseguridad en Atresmedia, un grupo que opera en televisión, prensa, radio, cine, incluso hasta en una funeraria, supone dar una cobertura total y diferente a todas esas patas.

## Encuentros BYTE TI



**Joan Barceló**

CIO y director de sistemas de W2M

Así que, primero, nos hemos centrado en crear conciencia, porque a nosotros nos afecta todo y estamos muy expuestos: tenemos que proteger a un reportero que cubre una guerra o defendernos de una posible intrusión, por ejemplo. Nos hemos tenido que adaptar no solamente a lo que se adapta cualquier empresa como protección, ciberataque, concienciación o formación, sino nos hemos tenido que adaptar a que toda la producción tiene que estar orientada en torno a la seguridad. Tenemos una estrategia de ciberseguridad, muy extensa, complicada y atípica”.

Javier Paniagua. CIO y director de sistemas de RISI, explicó que además de sus funciones como CIO, presta especial importancia al apartado de la seguridad: “Es un tema que me preocupa mucho. Afortunadamente, la dirección de la compañía está muy concienciada con este tema y esto es algo que ayuda mucho porque, muchas



**Manuel Serrano**

CISO de Atresmedia



**Javier Paniagua**

CIO y director de sistemas de Risi

veces cuesta conseguir fondos para ciertas cosas, porque la cúpula directiva no entiendo de qué se les está hablando y no consiguen comprender el beneficio de una determinada inversión. Esto, en mi caso no ocurre. Nosotros estamos haciendo muchas cosas. Tenemos un plan director que revisamos cada dos años y aunque no tenemos el nivel de madurez que a mí me gustaría, creo que hemos alcanzado un punto bastante razonable para el tamaño y dimensión de compañía que somos. Creo que lo importante en cualquier estrategia de ciberseguridad es tener las capacidades de inversión acotadas al tipo de compañía que se tiene y hacer todo lo que se pueda hacer sabiendo que no eres indemne a sufrir un ciberataque”.

Carolina de Oro, CIO de AXA detalló que en su compañía “tenemos equipos de ciberseguridad amplios y además estructurados entre lo que es una segunda línea de defensa que nos ayuda



**Carolina Oro**

CIO de AXA

## El reto del CIO y el CISO en la ciberseguridad

a garantizar el assurance y lo que estamos haciendo desde la operativa del día a día de la ciberseguridad, que se realiza desde los equipos de tecnología. Y luego, además, estamos en un entorno internacional en el que tenemos todo el equipo de estrategia de ciberseguridad, el SOC y muchas otras herramientas globales para asegurar que tenemos unos estándares altos en todo el grupo”.

Por su parte, Daniel Damas, Head of IT Assurance de Nationale Nederlanden, cree que “en ciberseguridad siempre se habla de términos muy mediáticos como security by design que son teoría, pero ¿cómo se llevan a la práctica? Hace cuatro años, nosotros arrancamos con el proyecto de cambiar nuestra forma de trabajar a agile y somos una compañía que vendemos pólizas. Así que en este caso, ¿qué es más prioritario? ¿Sacar productos rápido o tener una seguridad al 100%? Nosotros hemos cogido a la gente que diseña los pipeline, al personal de QA que tiene mucha relación con la parte de calidad y a las personas de seguridad y hemos hecho un solo departamento para hacer sinergia entre esos tres grupos. Con ello, hemos conseguido que sin entorpecer a nadie, los developers se autosirvan de infraestructura que ya viene security by design. Con ello, hemos logrado una velocidad enorme en el tema de despliegue, donde nosotros nos metemos ya si vemos que algo se desvía”.

## Encuentros BYTE TI

### Los retos de las empresas

Lo que quedó claro es que cada empresa tiene definida una estrategia propia en la que dependiendo en el sector en el que operen se enfrentan a unos riesgos o a otros. Para Álvaro Fernández, Sales Manager Iberia de Sophos, “la realidad es que el número de ciberataques está en aumento y la superficie a proteger también es mayor. Ante todo esto, yo creo que hay tres problemas importantes. Uno de ellos es el de la escasez de personas especialistas en ciberseguridad. Hay estudios que aseguran que a nivel mundial faltan 3,4 millones de especialistas. En España, la cifra se sitúa entre las 50.000 y las 80.000. El segundo reto son los tiempos de respuesta que las organizaciones pueden dar a las amenazas. Según Gartner, la media se sitúa en las 16 horas que es un tiempo muy alto para lo rápidos y certeros que son los atacantes. Y el tercer reto es el nivel de alertas. Cada vez hay más y esto provoca que para los equipos de seguridad sea cada vez más complejo saber dónde tienen que investigar, qué es lo que tienen que investigar o cómo tienen que investigar”.

### Inteligencia Artificial

La inteligencia artificial va a impactar directamente en las estrategias de ciberseguridad. ¿Qué ventajas se pueden obtener de ella? Para José Manuel Casillas, CIO y director de sistemas de LLYC, “el tener una



**Daniel Damas**

Head of IT Assurance de Nationale Nederlanden

capacidad de analizar una cantidad ingente de datos es fundamental. Seguramente las herramientas de IA van a acelerar los incidentes que puedan producirse. Nosotros estamos mucho en el mundo de la IA. Al final creo que el principal objetivo va a ser el de convencer a la cúpula directiva de que usar esta tecnología es bueno para la ciberseguridad. Creo que es una herramienta muy potente para ayudar en este camino y también veo que la formación va por detrás de los avances”.

Por su parte, Óscar Monrío, director de tecnología y transformación digital de CHC Energía, considera que “lo que estamos viendo en estos momentos es algo más relacionado con el marketing. La Inteligencia Artificial lleva bastante tiempo existiendo, el Machine Learning existe desde hace unos ocho años y la inteligencia artificial para la seguridad



**Álvaro Fernández**

Sales Manager Iberia de Sophos

## El reto del CIO y el CISO en la ciberseguridad



**José Manuel Casillas**

CIO y director de sistemas de LLYC

también se está trabajando desde hace tiempo. Luego está la parte de formación que es muy importante en este caso. La empresa que sea capaz de entender que procesos hace una persona y que en base a eso sea capaz de hacer pruebas que exponga el nivel de riesgo que tiene una persona con respecto a un proceso tendrá mucho ganado. Al final se pone mucho foco en la seguridad y tenemos el problema de las redes cuando lo importante es entender la criticidad de los procesos”.

Por su parte, Javier Torres, CISO de Allfunds, afirmó que “nosotros hemos desarrollado servicios de ciberinteligencia. Desde el primer minuto pensamos que era un tema que había que hacer. Tenemos 15-16 personas a los que se nos monitoriza todo lo que hacemos en RRSS, todos los movimientos que puedo llegar a hacer, incluso en mi correo personal. La única

## Encuentros BYTE TI



**Óscar Monrío**

Director de tecnología y transformación digital de CHC Energía



**Javier Torres**

CISO de Allfunds Bank



**José Aznar Laguna**

Business Development Manager de Kyocera

forma de evitar la desinformación es tener unos buenos servicios de ciberinteligencia. Por ejemplo al CEO nosotros le obligamos a que tenga su firma comercial y su firma personal para que nosotros sepamos cuándo una cosa es personal y otra profesional. En los últimos tres años hemos detectado webs fraudulentas, la web colgada en diferentes dominios... y todo ello gracias a ese servicio de ciberinteligencia”.

**Lo importante en cualquier estrategia de ciberseguridad es tener las capacidades de inversión acotadas al tipo de compañía**

### La nube en la estrategia de ciberseguridad

Finalmente, se trató el apartado de la seguridad en los entornos cloud. Para Carolina de Oro, “la nube no es más ni menos segura per se. Nosotros tenemos muchas cargas en diferentes nubes y de diferentes maneras y hemos hecho un movimiento muy importante hacia allí. La nube te da muchas herramientas, pero en si misma puede ser un facilitador si tu tienes una estrategia previa de seguridad. Luego están los entornos híbridos con los que también hay que tener cuidado. Y además, está la estrategia de reversibilidad a medio largo plazo, algo que no ocurría con el on-premise. En definitiva, con la nube aparecen otros aspectos que hay que tener en cuenta. Evidentemente, ir a la nube sí que te da una serie de mecanismos que te facilitan la seguridad, pero también trae consigo otra serie de riesgos que tienes que tener en cuenta”.

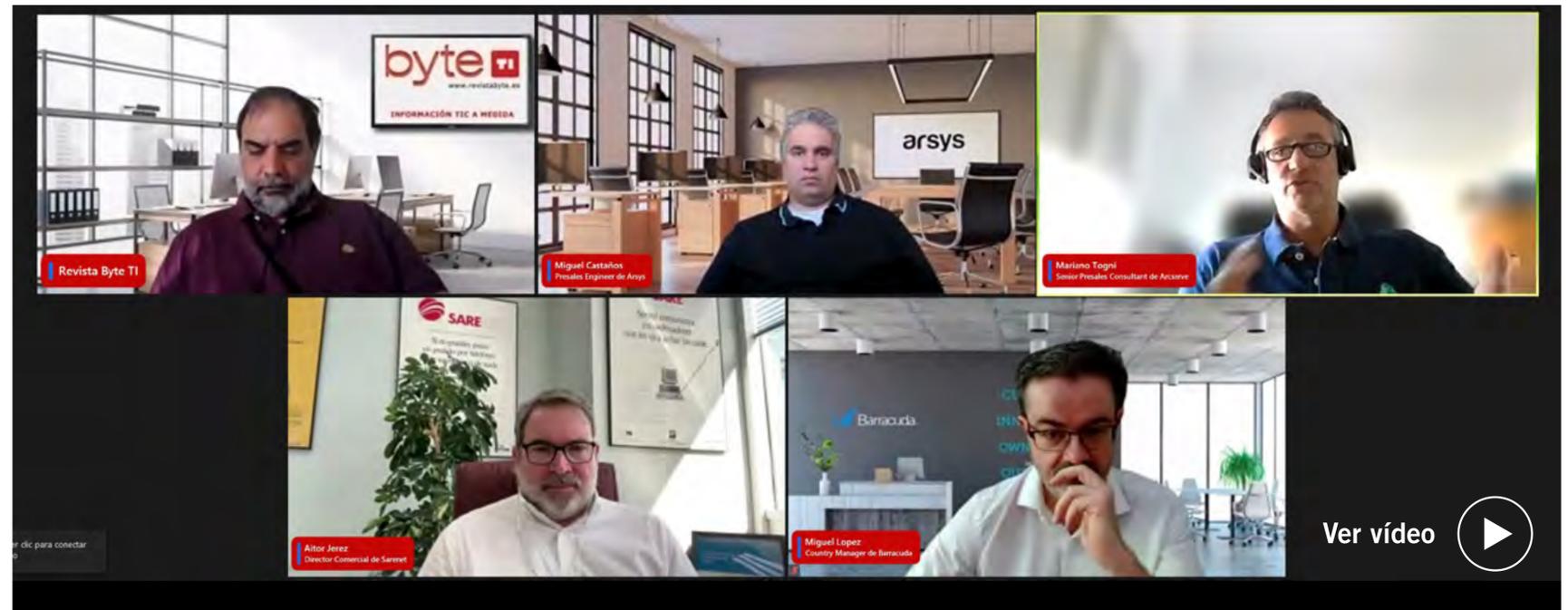
Por último, José Aznar Laguna, Business Development Manager de Kyocera, afirmó que “la venta de productos/soluciones sin un servicio robusto aparejado va a tender a minimizarse”. Esta multinacional nipona cuenta en la actualidad con una amplia gama de servicios alrededor de tres áreas como son la automatización de procesos, el desarrollo y la continuidad de negocio. En todas estas áreas el enfoque de seguridad es clave. Tal y como expuso Aznar Laguna, “para los servicios actuales la nube es un elemento clave a la hora de diseñar estrategias, y tiene cada vez más sentido desde un punto de vista de escalabilidad y seguridad”.



## Webinars BYTE TI

# Backup y Recuperación de Datos

Los datos son uno de los activos más valiosos de las empresas y, por tanto, es imprescindible garantizar su seguridad y disponibilidad en todo momento. Entre las medidas más importantes de protección, figura el backup y la recuperación de los datos, ya que permite proteger la información corporativa contra pérdidas, borrados accidentales o bloqueo del acceso a la información en el caso de haber sufrido un tipo de ataque.



En esta línea, para analizar qué políticas de recuperación de datos están llevando a cabo las empresas y cómo pueden mejorarlas, así como los errores que se cometen de forma habitual, contamos en este webinar con Aitor Jerez, Director Comercial de Sarenet; Miguel Castaños, Presales Engineer de Arsys; Miguel López, Country Manager de Barracuda; Mariano Togni, Senior Presales Consultant de Arcserve.

## La importancia del backup

En un mundo cada vez más digitalizado, la importancia del respaldo y la recuperación de datos no puede ser subestimada. Las

empresas que aún utilizan métodos obsoletos de recuperación se enfrentan a riesgos significativos. Garantizar la integridad de los datos y adaptar las estrategias de respaldo y recuperación es esencial.

Siguiendo este punto, Aitor Jerez, Director Comercial de Sarenet incide en que hoy en día, nos preocupamos mucho por el ransomware y olvidamos que los discos duros también fallan, “los backups no solo resuelven problemas de ciberseguridad, sino también accidentes imprevistos. Es crucial tener un plan de continuidad de negocio y recuperación para

restablecer la normalidad tras un ataque. Además, cumplir con normativas como la directiva europea NIS 2, que afectará a muchas pymes, es esencial. Por eso, disponer de un plan de seguridad sin incluir copias de seguridad es una ilusión; debemos tenerlo siempre en mente”.

De acuerdo con su compañero, Miguel Castaños, Presales Engineer de Arsys resalta que ahora somos más conscientes de las obligaciones legales y del cumplimiento normativo, y somos responsables de ello, “no debemos olvidar el coste reputacional: en la era de internet, todo el mundo se entera cuando algo sale mal.

## Webinars BYTE TI

La protección de la información, considerada el oro de las empresas, requiere cada vez más presupuesto y recursos, por razones evidentes”.

Por su parte, y en línea con lo anterior, Miguel López, Country Manager de Barracuda propone un ejercicio práctico para aquellos que piensan que los ataques no les afectarán, “imaginen que durante 24, 48, o 72 horas sus servidores de bases de datos y aplicaciones dejan de funcionar. Consideren el impacto en su negocio, en su personal...Reflexionen sobre cómo se recuperarían de una pérdida de datos y reconozcan la importancia crítica de los datos y, por ende, de tener políticas de backup y seguridad adecuadas”.

Y es que, a menudo nos enfocamos tanto en la importancia del backup que olvidamos que la finalidad de los backups es la restauración. “Es crucial definir claramente las políticas de protección de datos y de recuperación después de incidentes. La planificación de backups debe incluir estrategias de disaster recovery y considerar los puntos de recuperación (RPO) y los objetivos de tiempo de recuperación (RTO)”, concluye Mariano Togni, Senior Presales Consultant de Arcserve.

### Métodos de recuperación

Muchas empresas aún dependen de métodos obsoletos de recuperación, lo que las deja



**Aitor Jerez**  
Director Comercial  
de Sarenet



**Miguel Castaños**  
Presales Engineer  
de Arsys



**Miguel López**  
Country Manager  
de Barracuda



**Mariano Togni**  
Senior Presales  
Consultant de Arcserve

vulnerables a pérdidas de datos y tiempos de inactividad prolongados. Además, la creciente tendencia de adoptar soluciones en la nube está siendo la mejor opción para las organizaciones modernas. Pero, ¿deberían las empresas invertir en la nube para sus necesidades de respaldo y recuperación, o existen alternativas más efectivas?.

En opinión de Togni algunos clientes aún utilizan estrategias de backup muy básicas, como cintas o discos en el mismo centro de datos que los servidores de producción, lo que se traduce educar a los clientes sobre la regla 3-2-1, que incluye tener una copia fuera del sitio. “En cuanto al equilibrio entre soluciones on-premise y en la nube, no hay una solución única; depende de cada cliente. Aunque el cloud es útil, especialmente para copias off-site, es importante considerar los tiempos de

## Backup y Recuperación de Datos

restauración. Las pequeñas empresas aún necesitan madurar en este aspecto, pero tanto las soluciones on-premise como en la nube son válidas, dependiendo del balance entre inversión y beneficios”, resume.

Queda claro que lo que funcionaba hace décadas ya no es adecuado debido al crecimiento exponencial de los datos y a los cambios en los entornos de producción, que ahora requieren respuestas mucho más rápidas. Para López no se trata solo de adoptar tecnologías modernas como la nube, sino de desarrollar una estrategia completa y actualizada que combine backup en la nube y local, “es esencial integrar la estrategia de backup dentro de la estrategia global de seguridad y colaborar estrechamente con expertos y canales de integración para gestionar los datos de manera óptima y segura”.

## Webinars BYTE TI

### Garantizar la integridad de los datos

Teniendo esta información, las empresas se preguntan que estrategia deberían incorporar ahora mismo para garantizar la integridad de los datos. Sobre esto, el Director Comercial de Sarnet establece que para abordar la gestión de backups, las empresas deben realizar un análisis de riesgos detallado para identificar los datos críticos y establecer una política de backup acorde. Automatizar y centralizar el proceso es clave, utilizando herramientas que permitan verificar la integridad de las copias. Es fundamental que las empresas no se limiten a confiar únicamente en las herramientas del fabricante, sino que adopten un rol activo en la supervisión y verificación de los backups".

El Presales Engineer de Arsys enfatiza la importancia de ir más allá de los objetivos, destacando la necesidad de clasificar y proteger adecuadamente la información sensible con capas de encriptación y recursos adicionales, "para ellos contamos con unas tecnologías que nos ayudan: almacenamientos inmutables, efectivamente, análisis previos de vulnerabilidades. Nosotros contamos en una SIS con herramientas para que lo que tú guardes esté limpio, por ejemplo, sin virus. También es importante el tema de las copias en la nube. Sí, es una opción más, pero ojo, que también tiene sus consideraciones legales y no puedes subirlo a cualquier nube de cualquier manera".

Por su parte, el Country Manager de Barracuda explica que, independientemente de que las soluciones, las propuestas tecnológicas nos aseguren que los datos se han realizado de forma correcta y demás, hay que realizar pruebas no solo para verificar que la tecnología funciona correctamente, sino también para verificar que los procesos que hemos establecido funcionan, y los procesos incluyen personas, "es importante que tengamos establecido cuáles son los procesos, los pasos que hay que dar para recuperar la información. Ya no solamente que la tecnología sea capaz de hacerlo, sino que nuestros equipos y los procesos que hemos establecido son capaces de hacerlo".

Todo ello lo resume el Senior Presales Consultant de Arcserve en dos puntos clave, garantizar tener un backup consistente, y garantizar que ese backup sea recuperable, "es importantísimo, aparte de tener los backup, distintos medios, en distintos lugares y todo eso, las pruebas, y no solo de restauración de un fichero, sino también pruebas de restauración de desastre, recuperar un servidor completo, hacer una prueba de que el servicio de la base de datos funcione, en fin, una prueba realmente real de disaster recovery, periódicamente hay que hacerla"

### El backup en los entornos de trabajo remoto

Con el trabajo remoto, adaptar estrategias efectivas de backup se vuelve crucial para la seguridad y

## Backup y Recuperación de Datos

continuidad de las operaciones empresariales. Cada vez más, se están utilizando soluciones en la nube como OneDrive y SharePoint para almacenar datos, lo que simplifica la gestión pero también plantea nuevos retos de seguridad. "Es crucial contar con aplicaciones diseñadas para proteger estos datos en la nube, dado que se han vuelto una parte significativa de la información del cliente. Con la creciente deslocalización de los equipos de trabajo, la protección de datos en la nube, que incluye aplicaciones como Salesforce y otros CRM, se vuelve cada vez más vital. Es importante recordar que si bien las aplicaciones cloud garantizan el servicio, no se responsabilizan de la seguridad de los datos almacenados", señala Togni.

En los últimos cuatro o cinco años, el entorno de trabajo remoto ha experimentado una evolución notable, impulsada especialmente por la pandemia que aceleró su adopción. Como menciona López, para usuarios remotos con datos críticos que requieren un nivel más sofisticado y seguro de backup, como la capacidad de recuperación local, podemos implementar dispositivos de backup incluso en oficinas pequeñas, "Estos dispositivos se escalan fácilmente y se gestionan de manera centralizada, lo que alivia a los usuarios de la preocupación por el mantenimiento técnico".



## EMPRESAS PARTICIPANTES

### Barracuda

Actualmente el ransomware representa una amenaza significativa para las empresas de todos los tamaños. Una estrategia de backup efectiva es esencial para mitigar los riesgos asociados con este tipo de ataques. Barracuda ofrece soluciones de backup seguras y a prueba de ransomware que permiten a las empresas proteger sus datos críticos estén donde estén. Al implementar backups automáticos y seguros, las empresas pueden recuperar rápidamente su información en caso de un ataque de ransomware, minimizando así el tiempo de inactividad, los daños reputacionales y las pérdidas económicas. Además, Barracuda proporciona características complementarias de protección capaces de evitar la entrada del Ransomware en la organización así como de detectarlo, realizar un análisis forense en tiempo real del ataque y tomar medidas para detenerlo o paliarlo. Adicionalmente también cuenta con medidas de monitorización, control y asistencia como puede ser el servicio gestionado de XDR (eXtended Detection and Remediation) que permiten una rápida detección y reacción en caso de ataque (incluso interoperando con soluciones de terceros que no sean Barracuda).

### Arcserve

Desde Arcserve, queremos resaltar hoy mas que nunca la necesidad de políticas de protección de datos y continuidad de negocio, no solo para proteger los datos de las empresas sino también para cumplir con las nuevas normativas que entran en vigor este año. Para asegurar los datos de nuestros clientes Arcserve ofrece una solución completa tanto Hardware, Software y SaaS para la integridad de los datos en la empresa, y cumpliendo todos los requisitos de las actuales normativas.

### Sarenet

Nuestro servicio de copias de seguridad y recuperación ante desastres destaca por su valor añadido. Contamos con un equipo humano excepcional, actuando como una extensión de los departamentos TIC de nuestros clientes. Ofrecemos una solución completa que incluye además de las tradicionales, copias inmutables, copias de SaaS como O365, réplicas de entornos virtuales y planes de recuperación, utilizando la tecnología de Veeam. Nuestra solución abarca entornos virtuales y físicos, on-premise y en la nube, con mecanismos para verificar la integridad de las copias asegurándose que no guardas ni restauras copias infectadas. Contamos con CPDs propios en territorio nacional y bajo legislación europea, garantizando la soberanía del dato. Tarifas claras y servicio impecable. Os animo a probarlo sin compromiso.

### Arsys

Actualmente, la complejidad de los datos y la convivencia de sistemas y nubes requiere soluciones de backup personalizadas, adaptadas y flexibles, capaces de entender la diferencia entre un entorno de servidores físicos, otro de Kubernetes o una plataforma de Office. Y, además del software, es imprescindible contar con un equipo de profesionales con experiencia, que te asesore e integre sus funcionalidades en la estrategia de ciberseguridad, y ayude a planificar y gestionar el backup y su recuperación, auditando la salud e integridad de las copias para que realmente resulten útiles cuando tengamos que utilizarlas.

## Webinars BYTE TI

# Los cuatro nodos de la confianza digital

La digitalización empresarial está avanzando a de forma muy rápida, de tal forma que elaborar una estrategia para desarrollar esa transformación digital debe estar muy bien fundamentada para que sea exitosa. Esa planificación debe centrarse en cuatro pilares esenciales: personas, procesos, tecnología y organización. Las organizaciones pueden contribuir a reducir la brecha de talento, a impulsar una adaptación ágil a las tecnologías emergentes (IA, Computación cuántica, machine learning, etc), a afrontar los retos y las oportunidades de la ciberseguridad y a fomentar una cultura empresarial que favorezca la innovación. Todo ello, fue tratado en un webinar que Byte TI organizó el pasado 30 de mayo junto con ISACA en el que se trataron los principales retos y los nodos de cómo establecer la confianza digital.



El webinar contó con la participación de Rosa Ortuño, CEO de Optimum TIC; Ramsés Gallego, Hall of Fame de ISACA y Robert Maxwell, director del grado en gestión de ciberseguridad de la Universidad Francisco de Vitoria (UFV) que explicaron cómo las cuatro variables fundamentales de personas, procesos, tecnología y orientación, resultan pilares críticos para la sociedad que debemos y queremos ser.

Fue Rosa Ortuño, CEO de Optimum TIC la encargada de comenzar el encuentro. Nos

encontramos ante una ingeniera informática especializada en compliance y ciberseguridad donde acumula una experiencia de más de veinte años. Su experiencia ejemplifica el tema principal del webinar ya que hace 15 años creó la empresa Optimum TIC, especializada en la optimización de procesos de sistemas, personas y tecnología. Tal y como explicó, la compañía que dirige “tuvo unos inicios complicados porque en aquel entonces no todo el mundo entendía la importancia de tener un buen gobierno de ciberseguridad”.

Robert Maxwell, por su parte, es el director del grado en gestión de ciberseguridad de la Universidad Francisco de Vitoria (UFV). Su ejemplo es el opuesto al de Rosa ya que el inicio de su trayectoria comenzó con temas financieros para después, hace unos 12 años, “enfocarme en temas de investigación criminal y fraudes complejos” Es a partir de un determinado momento cuando la investigación empezó a solaparse con temas de ciberseguridad, hasta que la UFV creó un grado de gestión de la ciberseguridad “enfocado a atraer a jóvenes

## Webinars BYTE TI

con un perfil distinto, hacerles “techies” a base de programación, ética, criptografía, etc.” El año pasado salió la primera promoción donde todos los integrantes del grado ya tenían una colocación nada más terminarlo. Para este especialista uno de los aspectos fundamentales en la ciberseguridad son las personas, porque “somos como médicos, hay que ir formándose cada día del año y porque esto va a ir cada vez a más y mucho más rápido”.

El tercer ponente, Ramsés Gallego del Hall of Fame de ISACA, no necesita mucha presentación. Es uno de los principales especialistas en ciberseguridad de nuestro país. Pertenece al salón de la fama de la compañía, un título que muestra por todo el mundo en la innumerable cantidad de viajes que realiza alrededor del Globo. En su opinión, “es muy importante el nuevo marco de confianza digital que acaba de lanzar la asociación, que me parece brillante”.

### Equilibrar las dimensiones tecnológicas

¿Cuál es la importancia de comprender y equilibrar las dimensiones tecnológicas en la estrategia empresarial para alcanzar el éxito en esta era digital, que es la que estamos? Tal y como expuso Rosa Ortuño, “la tecnología es un elemento totalmente intrínseco a la forma en que todo ocurre en el mundo actual. Ninguna empresa puede ser ajena a ello. Pero se trata



**Rosa Ortuño**  
CEO  
de Optimum TIC

no solo de hacer que la tecnología nos ayude para buscar eficiencias, sino para ayudarnos a hacernos absolutamente todo mejor y más deprisa. Ahora que la transformación digital es un hecho, las empresas han de integrar absolutamente toda esta dimensión tecnológica con los pilares de personas, procesos, tecnología y organización”. Para Ortuño, “las empresas han de entender que el nivel de penetración actual de la tecnología permite, no solo mejorar las cosas, sino fundamentalmente hacer todas las cosas de forma distinta a como lo hemos estado haciendo. La empresa que no tenga alineada tecnología con negocio, no va a subsistir”.

Para Ramsés Gallego, la clave se puede encontrar en un verbo: catapultar. “Ahora que estamos constantemente hablando de machine learning, de inteligencia artificial, de seguridad,... vemos que todas estas tecnologías



**Ramsés Gallego**  
Hall of Fame  
de ISACA



**Robert Maxwell**  
Director del grado en gestión de  
ciberseguridad de la Universidad  
Francisco de Vitoria (UFV)

## Los cuatro nodos de la confianza digital

catapultan los resultados empresariales o la detección de patrones de compra, por ejemplo”.

### La crisis de talento

Sin embargo, uno de los problemas a los que se enfrentan las empresas es la falta de perfiles adecuados. En ciberseguridad, esa carencia es todavía más importante. Tal y como expuso Robert Maxwell, director del grado en gestión de ciberseguridad de la Universidad Francisco de Vitoria (UFV), “hay una falta muy importante de personal especializado en ciberseguridad en España, en Europa, y a nivel mundial. Y estamos hablando de cientos de miles de puestos. Y es un problema muy importante porque la ciberseguridad ya no es un silo dentro del departamento de ciberseguridad de la empresa, sino que se ha convertido en algo transversal. En España además hay una importante falta de cultura de ciberseguridad. Se puede ver en

## Webinars BYTE TI

los usuarios o en casos como en los que una empresa sufre un ciberataque y no lo comunica. Por eso es importante la labor de ISACA, porque es muy importante explicar y evangelizar, porque los riesgos son enormes y las empresas no están preparadas”.

### Reducir la brecha de talento

Empresas, universidades y asociaciones como ISACA están contribuyendo a reducir esa brecha de talento. En el caso de esta última y tal y como comentó Ramsés Gallego, “ISACA contribuye entendiendo el signo de los tiempos, con certificaciones de ciberseguridad, de privacidad, de ciberinteligencia,... Y también haciendo entender lo básico: lo esencial de blockchain, de inteligencia artificial, de la nube y de todo lo que implica la tecnología. Contribuimos de forma continua, con aristas de multiculturalidad y de multidimensión. ISACA contribuye en el viaje de privacidad, ciberseguridad, auditoría, monitorización, control, privacidad, gobierno de la empresa digital y todo ello con certificación CISM, que son las grandes, las muy reconocidas, pero también con otras muchas. Por eso estamos atrayendo todo tipo de jóvenes perfiles que no sólo quieren y necesitan entender la técnica, sino también lo que supone DORA, por ejemplo”.

### ¿Dejar de ser techie?

Una de las claves es que la tecnología sea atractiva. Con ello se favorecerá la atracción de

talento. Ortuño cree que “a la tecnología se la ha visto como algo muy techi cuando la realidad es que no sólo se necesitan ingenieros informáticos o de telecomunicaciones. En Optimum TIC tenemos personas que vienen de otras profesiones y que ven que la tecnología les resulta muy atractiva. Eso es lo que hay que conseguir. Porque, por ejemplo, la gente joven no tiene un concepto de la privacidad, no tiene un concepto de la seguridad y en cambio tenemos mucha normativa, mucha regulación, y vamos a remolque”.

Robert Maxwell se mostró de acuerdo y añadió: “Un problema es que en España la ciberseguridad se considera un coste y no una inversión. Nuestro reto principal pasa por que pensar en upskilling, es decir, coger gente que quiere cambiar y ayudarles. Porque además, en España tenemos talento”.

### Integrar personas, procesos, tecnología y organización

ISACA ha desarrollado el Digital Trust Ecosystem Framework (DTEF) un marco de trabajo del ecosistema de la confianza digital valora la experiencia en la integración de prácticas de confianza digital en todas las organizaciones, guiando estrategias de productos centradas en la confianza y mejorando la competitividad y la reputación. El objetivo, tal y como explicó Gallego es que las empresas “puedan desarrollar un ecosistema a través de un marco de

## Los cuatro nodos de la confianza digital

confianza digital, que tiene que ver con que las transacciones sean seguras, inequívocas e íntegras y que las relaciones sean proporcionales y ajustadas a derecho”. Para Gallego es importante crear “un ecosistema sistemático que implique procesos, procedimientos, control, monitorización y observabilidad. Me parece maravilloso que un ecosistema nos permita ser sistemáticos. Y además tiene que ser sistémico quiere decir que pertenece a un todo. El DTEF de ISACA, articula todo eso y además bebe de las fuentes de otro marco de trabajo de ISACA también, que se llama COBIT y que habla de retención del talento, cultura, formación de las personas...”.

### Aumento de ciberataques

Finalmente, se trató el tema de por qué no somos capaces de paliar los ciberataques. Para la CEO de Optimum TIC “es importante entender los factores de procesos, sistemas y personas. Todo tiene un claro margen de mejora. Para mí, el primer elemento es el factor humano. La persona, la perspectiva personal debe formar parte de una cultura digital. Estamos hablando de transformación digital continuamente, pero no hay cultura digital, no hay cultura de la privacidad, no hay cultura a nivel de los riesgos. La gente no tiene un concepto de riesgo”.



## Comparativa

# 5 soluciones de gestión de procesos empresariales (o BPM)

Cada vez es más habitual que las compañías adquieran programas de gestión de procesos empresariales, conocidos también por las siglas BPM (del inglés Business Process Management) y provistos de tecnologías de automatización. Así lo recogen diferentes informes como la investigación ‘Automation with intelligence’ de la consultora Deloitte que indica que el 73% de las organizaciones a nivel mundial apuesta por este tipo de soluciones. En cuanto a los sectores donde se emplean, su utilización abarca diferentes ámbitos: desde entidades gubernamentales a empresas del sector sanitario, pasando por servicios financieros y compañías minoristas y manufactureras, entre otras.

Los programas de este tipo se caracterizan por englobar un conjunto de sistemas, metodologías, herramientas, dinámicas y tecnologías que permiten a las organizaciones gestionar y optimizar sus procesos de negocio de manera eficaz: el propósito es que alcancen los objetivos que previamente se han marcado mejorando así su rendimiento y eficiencia. Integran para ello un motor de flujo de trabajo que se encarga de automatizar la ejecución de todos esos procesos definidos.



## Comparativa

### Consideraciones principales

Las soluciones BPM comparten, en líneas generales, una serie de características comunes como, por ejemplo, la automatización de procesos y tareas mediante el empleo de tecnologías de automatización robótica de procesos (RPA): a través del uso de bots, las empresas automatizan tareas que son repetitivas, de modo que los trabajadores pueden destinar su tiempo a labores que verdaderamente aporten más valor al negocio y a la vez supriman la dependencia con respecto a los procesos manuales. Asimismo, esta automatización de procesos está impulsada por la inteligencia artificial y el aprendizaje automático, ayudando así a reducir posibles errores.

También destaca la presencia de las llamadas herramientas de modelado a través de funciones como los diagramas de flujo de trabajo. Su empleo facilita a los empleados no solo diseñar, también visualizar y acreditar, los procesos de negocio de una manera sencilla y organizada. Estos programas brindan, por sus características, otras funcionalidades de interés como, por ejemplo, simular diferentes escenarios y variaciones dentro de un proceso en particular para determinar cuáles serían sus posibles consecuencias y efectos; o identificar aquellas áreas de mejora y cuellos de botella dentro de la compañía al efectuar un análisis

## 5 soluciones de gestión de procesos empresariales (o BPM)



desde el punto de vista del rendimiento; rendimiento que se mide y se monitorea por medio de instrumentos específicas. Asimismo, las soluciones BPM proporcionan un marco que garantiza a las empresas que los procesos que llevan a cabo cumplen con las políticas y normativas establecidas.

### Los beneficios

Como cualquier otra solución empresarial que se precie, la gestión de procesos empresariales y su automatización ofrece a las compañías una serie de ventajas que deben valorarse y estudiar. Una de las más importantes es la mejora de la productividad y la eficiencia operativa, pero existen otras de interés como una reducción en el tiempo de ejecución de

los procesos y la posibilidad de adaptarse a las nuevas necesidades cambiantes del mercado. El hecho de que los procesos se automaticen minimiza, por otro lado, los errores humanos y proporcionan resultados más predecibles.

Las soluciones de gestión de procesos empresariales reducen también los costos operativos; brindan un mayor control y visibilidad de los procesos; minimizan las microgestiones al automatizar flujos de trabajo perfectamente definidos; y mejoran la capacidad de la toma de decisiones.

## Comparativa

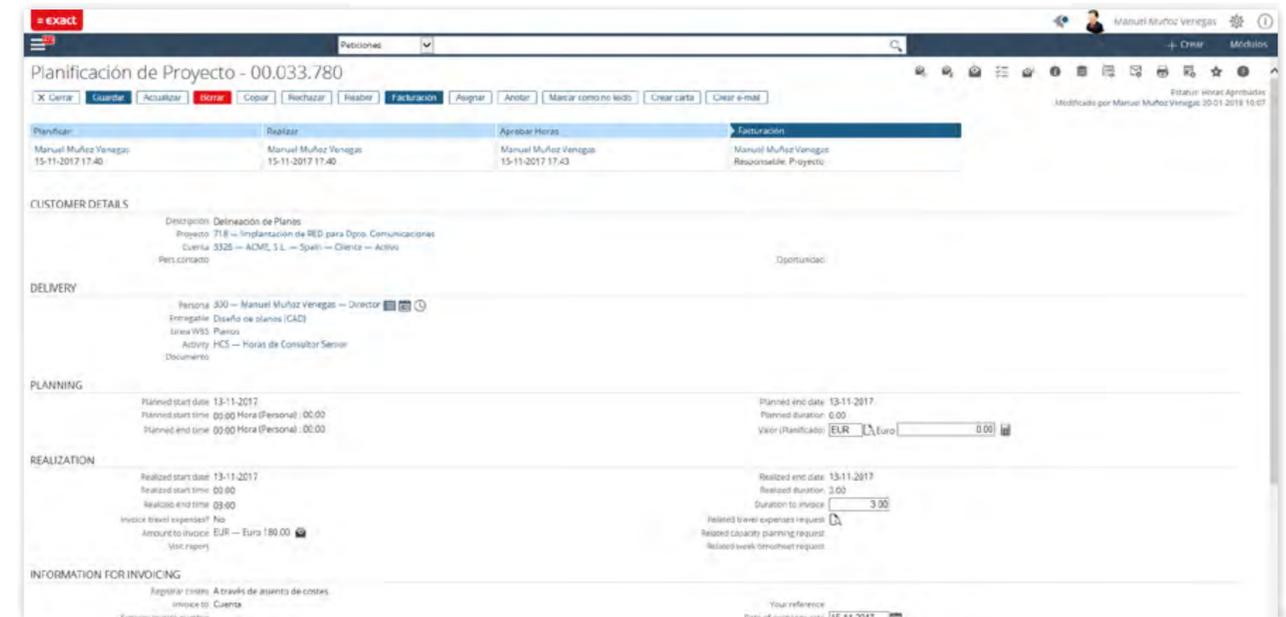
# Exact BPM

Este software, que integra en un único sistema todos los procesos de negocio de una organización, se presenta como una solución que ayuda a optimizar procesos y a dirigir a las empresas hacia la automatización y la digitalización total. Simplifica, para ello, aquellos procesos que resultan complejos y ofrece a los empleados la información necesaria para una toma de decisiones inteligente, independientemente del sector industrial en el que operen y sin la necesidad de disponer de múltiples aplicaciones. Dentro de este escenario, la base sobre la que se sostiene son los productos Exact Globe (software de gestión empresarial) y Exact Synergy (plataforma low code colaborativa, multi idioma y accesible online 24x7 que brinda a los negocios un gestor de procesos y gestión documental)

Entrando en detalle, Exact BPM optimiza y automatiza, a través de flujos de trabajo colaborativos, los procesos que resultan transversales a los distintos departamentos de la compañía: finanzas, clientes, proyectos, documentos, empleados, proveedores, etc. Así, estos flujos garantizan que todos los participantes en una tarea o una actividad específica estén en sintonía porque el trabajo se transfiere automáticamente a la siguiente persona responsable dentro de dicho proceso.

La propuesta de Exact garantiza, por otro lado, que los trabajadores siempre tienen acceso a la información que necesitan tanto para llevar a cabo sus actividades como para tomar las decisiones oportunas; a este respecto, la conectividad con otros sistemas es absoluta y además es posible conectarse 24x7 desde aplicaciones móviles, lo que garantiza una visión general en tiempo real con independencia del lugar en el que se encuentre el usuario. Junto a los análisis dinámicos y los informes integrados, tienen cabida asimismo las alertas que informan a los trabajadores acerca de las cuestiones importantes que deben conocer.

## 5 soluciones de gestión de procesos empresariales (o BPM)

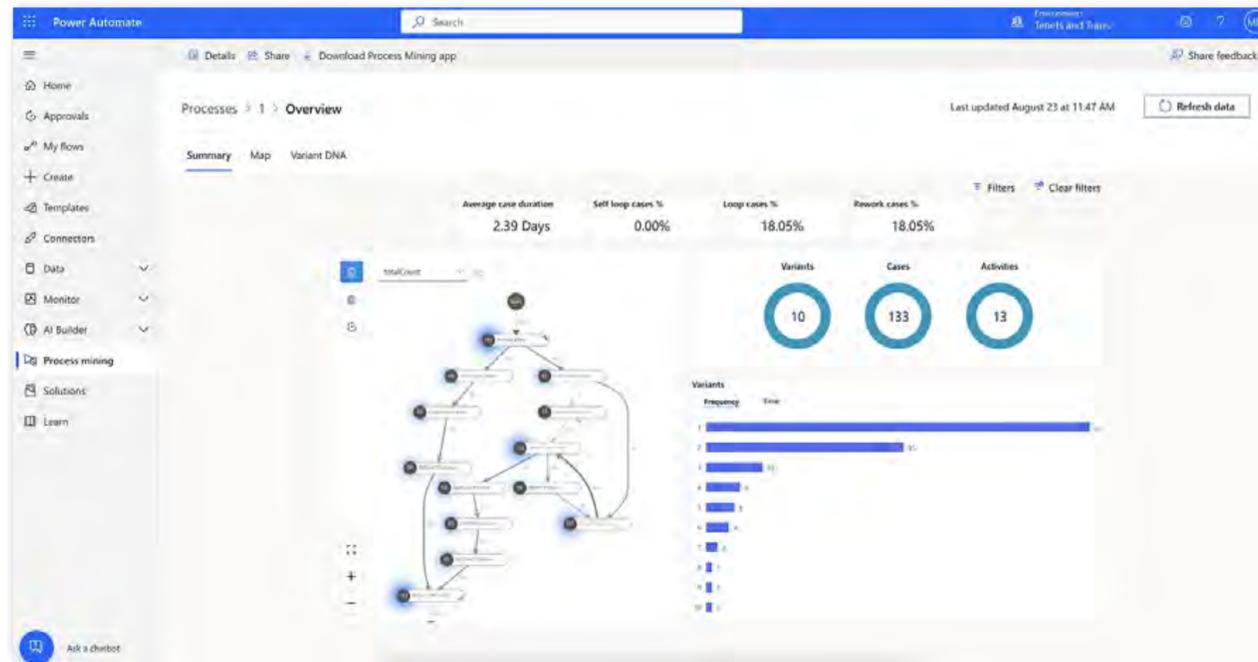


Destacan, en otro orden de cosas, los workspaces (configurables con recursos como vídeos cronogramas o resúmenes, entre otros) que son espacios de trabajo que estructuran la información y recopilan el conjunto de la comunicación, la documentación y la información sobre un proyecto o un proceso en concreto, y la incorporación de plantillas para una rápida implantación. Con varias opciones de implementación (la nube, la instalación local y las soluciones híbridas para adaptarse a diferentes necesidades), los puntos fuertes de la solución de este fabricante incluyen también: incremento de la productividad y eficiencia, seguridad en los procesos, eliminación de las tareas duplicadas y reducción de la microgestión.

Finalmente, hay que añadir que Exact proporciona un soporte integral desde el análisis y asesoramiento de los procesos a optimizar hasta su implementación, así como la capacitación del equipo interno y un soporte continuo para maximizar el retorno de la inversión que efectúan las organizaciones.

## Comparativa

# IBM Concert



La solución del gigante de Redmond para esta comparativa es una plataforma de pago por uso basada en la nube y sin compromiso de permanencia que permite crear flujos de trabajo automatizados y que se integra de manera nativa con otros productos de la compañía como Microsoft 365, Azure y Dynamics 365: esta suite, que se caracteriza por eliminar los silos tradicionales entre departamentos, añade valor a cada una de las capas de análisis de datos, automatiza tareas específicas y mejora las actividades relacionadas, entre otros beneficios; además, puede incorporarse a una amplia variedad de servicios externos. Dentro de este escenario, Power Automate es parte de Microsoft Power Platform, plataforma que destaca porque los profesionales no necesariamente técnicos pueden crear aplicaciones empresariales y automatizar tareas sin necesidad de escribir código convencional o conocer lenguajes de programación concretos (low-code).

Desde la gestión de aprobaciones y notificaciones hasta la integración de sistemas complejos y la sincronización de datos, estas son algunas

## 5 soluciones de gestión de procesos empresariales (o BPM)

de las tareas de producción repetitivas que lleva a cabo la solución de manera automática. Precisamente, esta automatización se potencia con la Inteligencia Artificial de Microsoft que reduce el tiempo que se destina a estas tareas para que los trabajadores se centren en las labores que aportan más valor. En este caso, los empleados pueden crear, editar y ampliar la automatización de procesos utilizando con Copilot lenguaje natural. O convertir datos que están sin procesar en contenido que resulte interesante gracias a la compatibilidad integrada con GPT.

Microsoft Power Automate –que automatiza procesos en casi todos los sistemas, aplicaciones de escritorio y sitios web– emplea, por otra parte, la automatización robótica de procesos (RPA) para automatizar los sistemas heredados con acciones de interfaz de usuario precompiladas o personalizadas. Incluso existe la opción de administrar picos y optimizar los recursos con una infraestructura hospedada que escala y equilibra dinámicamente las cargas de forma automática; la implementación de bots con IA también se contempla.

Los usuarios pueden, en otro orden de cosas, recurrir a la automatización de procesos digitales (DPA) tanto para automatizar aplicaciones como servicios y datos que se ejecutan en la nube o en el entorno local. Es posible, asimismo, escoger entre más de 1.000 conectores de API o que las empresas creen el suyo personalizado para conectar sistemas e intercambiar información.

Para garantizar una implementación segura, es posible utilizar entornos administrados y aplicar una política de prevención de pérdida de datos, entre otras medidas.

## Comparativa

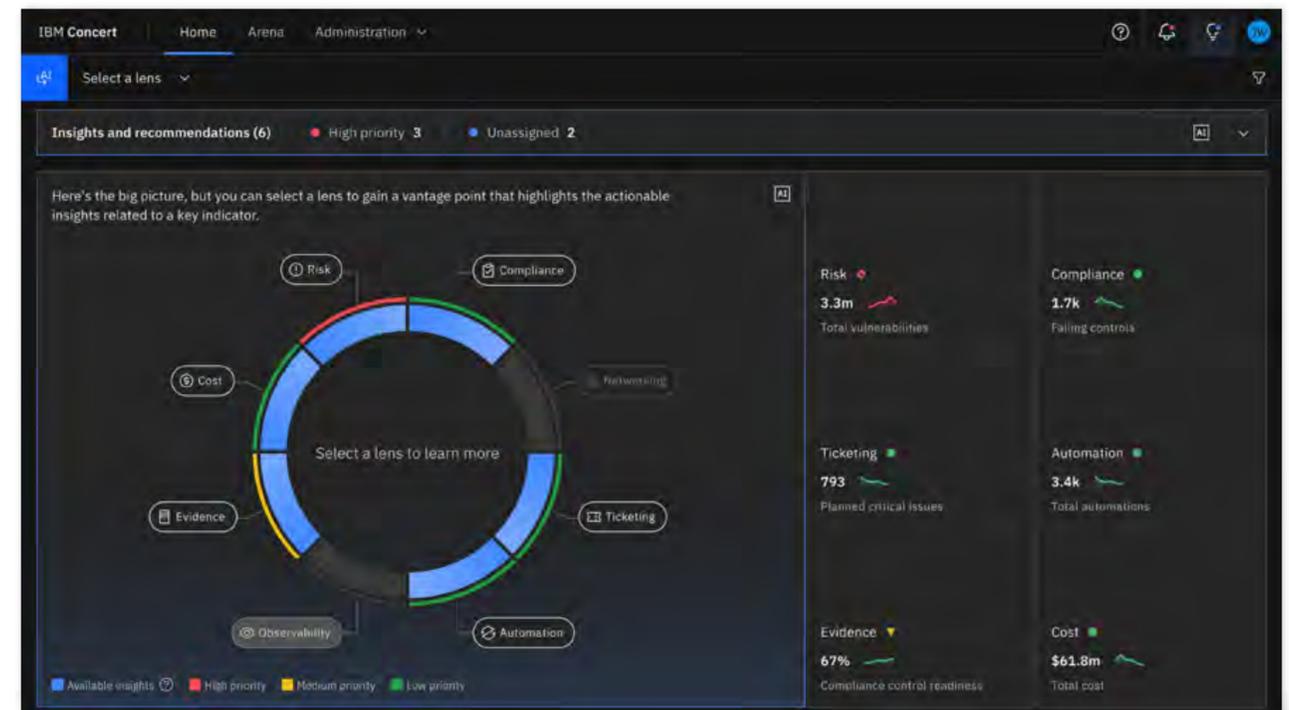
# Microsoft Power Automate

La solución del gigante de Redmond para esta comparativa es una plataforma de pago por uso basada en la nube y sin compromiso de permanencia que permite crear flujos de trabajo automatizados y que se integra de manera nativa con otros productos de la compañía como Microsoft 365, Azure y Dynamics 365: esta suite, que se caracteriza por eliminar los silos tradicionales entre departamentos, añade valor a cada una de las capas de análisis de datos, automatiza tareas específicas y mejora las actividades relacionadas, entre otros beneficios; además, puede incorporarse a una amplia variedad de servicios externos. Dentro de este escenario, Power Automate es parte de Microsoft Power Platform, plataforma que destaca porque los profesionales no necesariamente técnicos pueden crear aplicaciones empresariales y automatizar tareas sin necesidad de escribir código convencional o conocer lenguajes de programación concretos (low-code).

Desde la gestión de aprobaciones y notificaciones hasta la integración de sistemas complejos y la sincronización de datos, estas son algunas de las tareas de producción repetitivas que lleva a cabo la solución de manera automática. Precisamente, esta automatización se potencia con la Inteligencia Artificial de Microsoft que reduce el tiempo que se destina a estas tareas para que los trabajadores se centren en las labores que aportan más valor. En este caso, los empleados pueden crear, editar y ampliar la automatización de procesos utilizando con Copilot lenguaje natural. O convertir datos que están sin procesar en contenido que resulte interesante gracias a la compatibilidad integrada con GPT.

Microsoft Power Automate –que automatiza procesos en casi todos los sistemas, aplicaciones de escritorio y sitios web– emplea, por otra parte, la automatización robótica de procesos (RPA) para automatizar los sistemas heredados con acciones de interfaz de usuario precompiladas o personalizadas. Incluso existe la opción de administrar picos y optimizar

## 5 soluciones de gestión de procesos empresariales (o BPM)

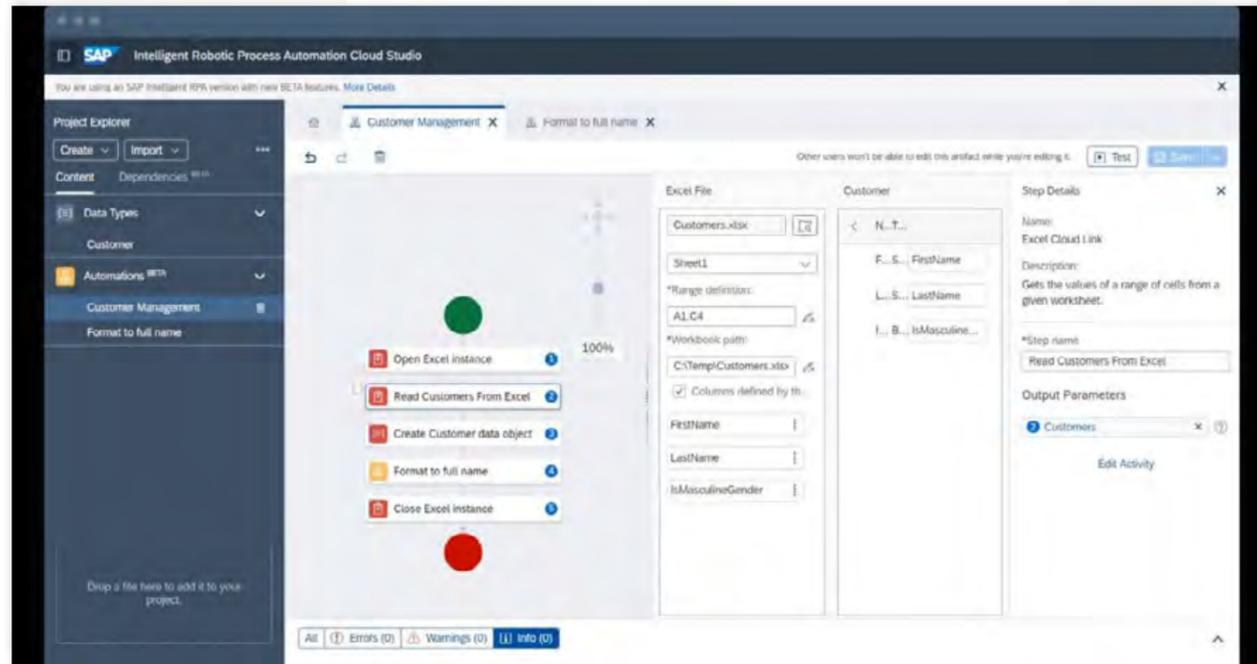


los recursos con una infraestructura hospedada que escala y equilibra dinámicamente las cargas de forma automática; la implementación de bots con IA también se contempla. Los usuarios pueden, en otro orden de cosas, recurrir a la automatización de procesos digitales (DPA) tanto para automatizar aplicaciones como servicios y datos que se ejecutan en la nube o en el entorno local. Es posible, asimismo, escoger entre más de 1.000 conectores de API o que las empresas creen el suyo personalizado para conectar sistemas e intercambiar información.

Para garantizar una implementación segura, es posible utilizar entornos administrados y aplicar una política de prevención de pérdida de datos, entre otras medidas.

## Comparativa

# SAP Build Process Automation



Forma parte de la solución SAP Build de la multinacional alemana y engloba un conjunto de herramientas de bajo código (y también sin código) dirigidas a crear flujos de trabajo y automatizar tareas. De manera más pormenorizada, Build Process Automation -que se integra de forma nativa con las soluciones del fabricante y ofrece la posibilidad de conexión con aplicaciones de otros proveedores, combina la gestión de flujos de trabajo, automatización robótica de procesos (ARP) y funcionalidades de IA incorporadas.

Provisto de un conjunto de plantillas, facilita precisamente que la gestión de los flujos de trabajo y la automatización de las tareas sean más simples y rápidas al incluir contenido específico de sector ya desarrollado y casos prácticos que facilitan el inicio de proyectos por parte de las compañías. Además, apostar por herramientas sin código (antes citadas) que son intuitivas permiten a los trabajadores no solo mejorar sus procesos empresariales, sino crear flujos de trabajo y automatizar tareas mediante funciones visuales para las que no es necesario tener conocimientos de programación.

## 5 soluciones de gestión de procesos empresariales (o BPM)

Partiendo de la idea de que un flujo de trabajo es una secuencia de actividades o tareas conectadas que se realizan para lograr un resultado concreto, las funcionalidades de gestión de flujos de trabajo de SAP Build Process Automation ayudan a los empleados a digitalizarlos y organizarlos. Es posible, asimismo, ampliar procesos estructurados adaptados a las necesidades de la empresa y a usar reglas para automatizar y adaptar de manera flexible la lógica de las decisiones. Mientras, en el caso de las funcionalidades ARP integradas a las que antes se han hecho referencia, concretar que ayudan a mejorar los flujos de procesos utilizando la automatización de tareas mediante bots de ARP; los usuarios tienen la opción de elegir entre una amplia gama de bots de mejores prácticas preconfigurados para varias líneas de negocio. Estos bots, listos para su implementación, ayudan a generar resultados de manera rápida a partir de las funcionalidades de ARP liberando a los trabajadores de las tareas repetitivas.

¿Qué supone para una compañía que SAP Build Process Automation incorpore el valor de la Inteligencia Artificial a la automatización de procesos empresariales? Principalmente, ofrecer funcionalidades unificadas de IA en el ámbito corporativo que ayudan al trabajador a crear procesos de negocio inteligentes; mientras, los expertos en procesos pueden utilizar funcionalidades de IA y aprendizaje automático para dar soporte al procesamiento inteligente de documentos empresariales. A este respecto, la solución cuenta con una función de extracción de información de documentos que ayuda a aumentar la productividad al automatizar el proceso manual de extracción de datos de documentos escaneados o digitales, además de procesar grandes cantidades de documentos empresariales.

Comparativa

# Software AG ARIS

ARIS es una suite de productos que se perfila como una solución de software de análisis y gestión de procesos empresariales dirigida a las compañías que buscan la transformación digital de su negocio con independencia de su tamaño o la actividad a la que se dedique. Se articula en torno a cuatro puntos principales: análisis de procesos de negocio, automatización de procesos, process mining, y gestión del riesgo y cumplimiento.

Con relación al primero de ellos, ARIS ayuda a las organizaciones a diseñar procesos que resulten más eficientes para responder lo antes posible a los cambios en los requisitos comerciales o del mercado. La solución de análisis de procesos de negocio que integra la propuesta de Software AG (ARIS Transformation Suite) provee, en este sentido, de una visibilidad en sus operaciones y de un seguimiento cercano del negocio.

En referencia al segundo punto, la automatización de procesos, el objetivo es que las empresas ganen en productividad y eficacia. Para ello, disponen de bots que están habilitados para RPA (transformación robótica de procesos). Además, es posible sincronizar los objetivos comerciales operativos y la estrategia corporativa de la compañía con las necesidades de TI.

Por su parte, process mining hace referencia a la minería de procesos, es decir, al análisis en profundidad, el descubrimiento, el seguimiento y la mejora de los procesos existentes de una organización. ARIS Process Mining pone de manifiesto, a este respecto, las deficiencias que requieren

## 5 soluciones de gestión de procesos empresariales (o BPM)

ajustes en el diseño, los sistemas de soporte o las necesidades de formación para los empleados. Asimismo, permite disponer de información crítica que ayuda a comprender cómo funciona la compañía y los cambios que son necesarios aplicar para que los procesos se lleven a la práctica según los planes previstos; aquí, la simulación y el análisis de escenarios de optimización de procesos resultan útiles. Incluso es posible analizar los indicadores clave de desempeño de los procesos e identificar los patrones que influyen en ellos a través de la Inteligencia Artificial.

Por último, se encuentra la gestión del riesgo y cumplimiento, En este punto, ARIS Risk & Compliance Management ayuda a identificar y documentar riesgos, así como cumplir las regulaciones básicas; por ejemplo, se garantiza el cumplimiento del Reglamento General de Protección de Datos y el establecimiento de controles internos asignando requisitos normativos a procesos comerciales y definiendo controles relevantes para sus riesgos de cumplimiento. Destacan, por otro lado, la gestión de incidencias y pérdidas (efectuando su seguimiento); el establecimiento de controles internos; la realización de auditorías empresariales; y la confirmación de nuevos procedimientos: esto implica la administración de los procesos de confirmación para asegurar que los trabajadores los han leído y que los nuevos procedimientos, políticas y pautas se comprenden.



Comparativa

5 soluciones de gestión de procesos empresariales (o BPM)

# Conclusiones

En esta comparativa se han incluido cinco soluciones de las principales firmas que copan este nicho de mercado. Todas son una opción interesante para cualquier compañía que, lógicamente, tiene que evaluar sus necesidades a la hora de escoger una u otra. Sin embargo, en nuestra opinión, hay dos opciones que destacan sobre el resto y que por lo tanto son mejores. Hablamos de SAP Build Process Automation y Software AG IRIS. La primera, que puede no solo integrarse de manera nativa con las soluciones del fabricante alemán (brinda asimismo la posibilidad de conexión con aplicaciones procedentes de otros proveedores), destaca porque al integrar

herramientas sin código no es necesario disponer de conocimientos de programación. Se articula sobre tres puntos clave: la gestión de flujos de trabajo, funcionalidades de IA y automatización robótica de procesos (ARP). Por su parte, Software AG ARIS se presenta como una suite de gestión y procesos en la que se distinguen cuatro módulos que son análisis de procesos de negocio; automatización de procesos (con cabida para proyectos de Internet de las cosas); la minería de proyecto (opción de analizar los indicadores clave de rendimiento de dichos procesos); y gestión del riesgo y el cumplimiento (entre sus opciones, ayuda a realizar auditorías empresariales).

Respecto al resto de propuestas, comentar que Exact BPM cuenta con características de interés como los espacios de trabajo que estructuran la información (workspaces), los informes integrados y el soporte especializado. Por su parte, IBM Concert es una solución ‘dos en uno’ dirigida a aquellas empresas que, además de apostar de manera importante por la IA, buscan una herramienta que fomente la colaboración de los equipos de trabajo. Finalmente, Microsoft Power Automate tiene el aliciente de integrarse de manera nativa con otros productos del gigante azul como Azure y Dynamics 365.

## ASPECTOS DESTACADOS

Fabricante Nombre de la solución	Exact Exact para BPM	IBM Concert	Microsoft Power Automate	SAP Build Process Automation	Software AG ARIS
Valoración	★★★★	★★★★	★★★★	★★★★★	★★★★★
Características clave	<ul style="list-style-type: none"> <li>• Colaboración a través de flujos de trabajo</li> <li>• Alertas que informan de manera proactiva</li> <li>• Soporte integral: análisis, asesoramiento, implementación, capacitación del equipo interno...</li> <li>• Plantillas para una rápida implementación</li> <li>• Despliegue: la nube, la instalación local o soluciones híbridas</li> </ul>	<ul style="list-style-type: none"> <li>• Combina las funciones de plataforma de automatización tecnológica y herramienta de colaboración</li> <li>• Uso de IBM watsonx, plataforma de IA</li> <li>• Generación de análisis y recomendaciones</li> <li>• Registros acerca del estado del sistema</li> <li>• Ingeniería de fiabilidad del sitio</li> </ul>	<ul style="list-style-type: none"> <li>• Forma parte de Microsoft Power Platform</li> <li>• Se integra de manera nativa con productos de Microsoft como 365, Dynamics 365 y Azure</li> <li>• Empleo lenguaje natural con Copilot</li> <li>• Automatización de procesos digitales (DPA)</li> <li>• Supervisión completa</li> </ul>	<ul style="list-style-type: none"> <li>• Forma parte de la solución SAP Build</li> <li>• Proporciona herramientas sin código</li> <li>• Integración nativa con otros productos de SAP</li> <li>• Funcionalidades unificadas de IA</li> <li>• Opción de conexión con aplicaciones de otros proveedores</li> </ul>	<ul style="list-style-type: none"> <li>• La suite integra análisis de procesos de negocio</li> <li>• Bots habilitados para RPA</li> <li>• Vista de 360º de la cadena de suministro, servicio al cliente...</li> <li>• Garantiza el cumplimiento del RGPD</li> <li>• Tres versiones: básica, avanzada y empresa</li> </ul>

# El estado actual del Turismo 4.0 en España

El turismo desempeña un papel crucial en la economía, la sociedad y la cultura a nivel global, impulsando el movimiento anual de millones de personas. En 2019, el sector turístico contribuyó con el 10,3 % del PIB mundial y creó uno de cada diez empleos. Para 2023, según el Consejo Mundial de Viajes y Turismo (WTTC), el turismo representaba el 9,1 % del PIB mundial, proporcionando más de 348 millones de empleos.



## Portada

En el contexto de inflacionario actual, las empresas del sector turístico, al igual que muchas otras, deben recortar gastos y aumentar su rentabilidad, todo mientras continúan con sus procesos de digitalización y mantienen un enfoque en la satisfacción del cliente. Sobre esto, las compañías turísticas tienen la ventaja de haber comprendido hace tiempo la importancia de la tecnología para lograr sus metas comerciales y promover un turismo de mayor calidad.

Como bien indica Francisca Campins, Vice-President Consulting Services de CGI, esto incluye “los costes laborales debido a la escasez de talento, lo que las ha llevado a subir los precios. Además de progresar en su digitalización, están explorando el potencial de tecnologías como la Inteligencia Artificial (IA) Generativa”.

Y ya no solo eso, estas empresas están cambiando y avanzando hacia una era de hiper-digitalización, enfocándose en tecnologías que mejoran la experiencia del cliente y del empleado, “también están utilizando Big Data, AI y aprendizaje automático para gestionar grandes cantidades de datos, centralizando la información, realizando análisis en tiempo real y asegurando la seguridad de los datos. Estas estrategias mejoran la toma de decisiones, la personalización de servicios y la eficiencia

operativa”, añade Ricardo Carvalho de Oliveira, director del negocio de Hospitality en Oracle Iberia.

Tecnologías novedosas como las del metaverso y la realidad extendida, que podrían, en palabras del presidente de la Comisión Smart Cities de AMETIC, “revolucionar la forma en que los clientes experimentan y planifican sus viajes, permitiéndoles explorar destinos y servicios de manera virtual en la etapa previa al viaje”.

Pero no solo la inversión en herramientas es fundamental, para Carlos de la Horra, Optical Solution Director en Huawei Empresas España, hay que tener en cuenta también la infraestructura, “no puedes pasar de no ser digital a implantar inteligencia artificial (IA) generativa. Antes hay que establecer los fundamentos de cómo vas a ir adoptando y rentabilizando esos avances”.

Empresas como Microsoft mantienen un firme compromiso con el objetivo de ayudar a todos los sectores, incluido el turístico, a alcanzar mayores logros. Su labor se centra en garantizar que las organizaciones de esta industria puedan mantener su competitividad y responder de manera eficaz a las demandas cambiantes del mercado, “recientemente firmamos un acuerdo de colaboración con Ávoris Corporación Empresarial, empresa líder

## El estado actual del Turismo 4.0 en España



del sector turístico en España perteneciente al Grupo Barceló, para impulsar su transformación digital. La integración de soluciones en la nube y de IA en Ávoris no solo impulsa su innovación y ciberseguridad, sino que también fomenta la sostenibilidad y la creación de modelos de negocio innovadores”, destaca Juan Chinchilla, director de la Unidad de Negocio de Business Applications de Microsoft España.

## Portada

### Retos en la digitalización

El reto fundamental para las empresas turísticas, en opinión del Vice-President Consulting Services de CGI es maximizar el ROI mediante estrategias basadas en el dato como facilitador, “bajo esta máxima, entre los principales desafíos que afrontan las empresas turísticas se encuentran la modernización de los sistemas heredados, la mejora de la eficiencia, la reducción de los costes mediante la automatización de procesos y la



toma de decisiones inteligentes y, por supuesto, la personalización de la oferta y mejora de la experiencia del cliente”.

Las pymes tampoco se libran. Para el presidente de la Comisión Smart Cities de AMETIC, las pequeñas y medianas empresas del sector turístico suelen tener pocos medios para digitalizarse por falta de personal especializado y falta de financiación, “existen algunos programas estatales para resolver el problema pero sigue faltando cultura digital en la pequeña empresa, lo que impide que desde los mandos se concencie la empresa en adoptar soluciones digitales que no se ven como soluciones a la gestión diaria y que acarrear un consumo de tiempo por parte de la dirección. Este problema se ve acrecentado en las Micro pymes”.

El miedo a la inversión, a perder tiempo con tecnologías ineficaces y a perder el toque humano son otras tres barreras significativas para avanzar. Es aquí donde entra, en palabras del Optical Solution Director de Huawei Empresas España, la aplicación de la IA, “y es que, es una evolución natural, derivada de

## El estado actual del Turismo 4.0 en España

los procesos de digitalización y computación en la nube que muchas empresas ya han adoptado. Además, las empresas deben adaptar su infraestructura de comunicaciones y redes para manejar el gran volumen de información, asegurando un ancho de banda adecuado que permita un funcionamiento perfecto en tiempo real y con numerosos usuarios conectados. Es esencial implementar tecnología con una infraestructura capaz de soportar las demandas de tráfico y servicios de red”.

Desde Oracle, aportan la siguiente lista a modo de resumen, de lo que para ellos son los principales retos en la digitalización de las empresas:

- Seguridad de los datos.
- Integración de sistemas.
- Capacitación y contratación de personal.
- Equilibrio entre inversión y control de costes.
- Adaptación al cambio tecnológico.
- Personalización sin invasión de privacidad.
- Adaptación de sus infraestructuras tecnológicas a la nube.
- Gestión de la experiencia del cliente.
- Sostenibilidad.



**El miedo a la inversión, a perder tiempo con tecnologías ineficaces y a perder el toque humano son otras tres barreras significativas para avanzar.**

## La IA y los Algoritmos

La inteligencia artificial y los algoritmos están revolucionando el sector del turístico 4.0, transformando la personalización de la experiencia del cliente, la optimización operativa y la sostenibilidad. Estas tecnologías permiten a las empresas anticipar preferencias, gestionar precios y planificar rutas de manera más eficiente, haciendo los viajes más adaptados y accesibles.

“La inteligencia artificial puede analizar grandes cantidades de datos para ofrecer recomendaciones más precisas y relevantes, mejorando la eficiencia en la atención al cliente mediante chatbots y asistentes virtuales. También facilita la personalización del marketing, incrementando la base y retención de clientes al crear relaciones más sólidas y duraderas. Además, permite la automatización de tareas repetitivas, liberando tiempo para que los empleados se concentren en actividades estratégicas y de alto valor añadido”, recalca Diego Viudes, Sales Leader manager de aggity.

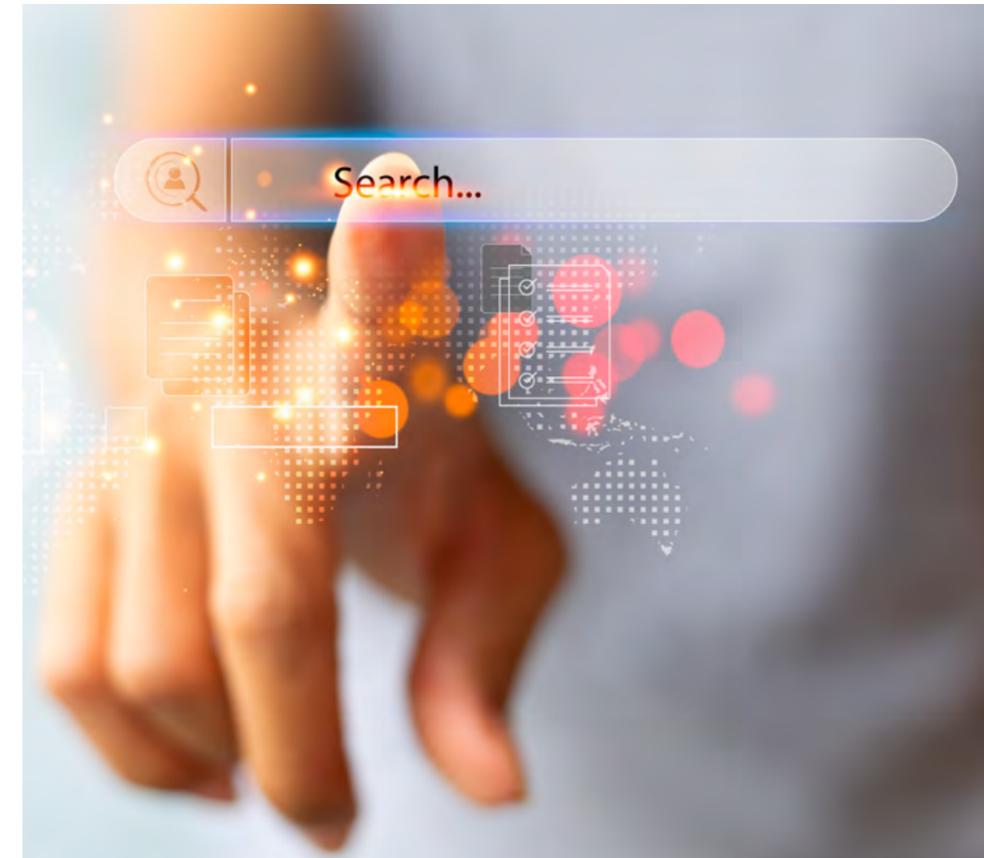
Y es que, aunque presente desde hace ya bastantes años, se manifiesta de manera más abierta en herramientas como los chatbots y asistentes virtuales, algoritmos de recomendación..., “así como en comparadores, experiencias personalizadas en destino, precios

dinámicos, servicios de atención al cliente con alta disponibilidad y eficiencia y análisis predictivo para la planificación de viajes. Muchas áreas de la oferta turística que plantean una gran oportunidad”, añade Francisco Cantón, Head of Sales SAP Services en AYESA.

Sobre uno de estos últimos puntos, la personalización de la experiencia del cliente permite la adopción de una perspectiva integral de 360° del cliente, lo que es esencial para comprender completamente sus necesidades y comportamientos. También, la personalización impulsada por IA fomenta la lealtad del cliente a largo plazo.

Y es que, “cuando los clientes sienten que sus necesidades y preferencias son comprendidas y atendidas, tienden a desarrollar una mayor afinidad con la marca. La capacidad de la IA para personalizar las interacciones en todos los puntos de contacto fortalece esta relación, promoviendo la fidelidad y la retención de clientes”, anota el director de la Unidad de Negocio de Business Applications de Microsoft España.

Pues, llegados a este punto, para el Optical Solution Director de Huawei Empresas España, se busca la hiperpersonalización, “porque el cliente ya no quiere ser uno más quiere ese trato único y personalizado”.



Por la parte del marketing, las ventajas que ofrece el uso de IA para la personalización de la experiencia del cliente están siendo orientadas a segmentar mejor a sus audiencias y a crear campañas de marketing más “quirúrgicas”, efectivas y dirigidas, “se empiezan a ver acciones encaminadas a anticipar las necesidades y deseos de los clientes antes de que ellos mismos los identifiquen. Esto será fundamental para ofrecer experiencias ultra-personalizadas y seguir aumentando las estrategias de fidelización del cliente y venta directa”, subraya el presidente de la Comisión Smart Cities de AMETIC.

## Portada

### La seguridad de los datos

Es evidente que las empresas del sector turístico son un blanco frecuente para los ciberdelincuentes, como lo demuestran varios incidentes recientes. Sin embargo, estas compañías han incrementado su conciencia y formación en seguridad, reforzando las medidas para proteger la privacidad y confidencialidad de los datos de sus clientes y asegurar sus operaciones.

Al igual que en otros sectores, especialmente en infraestructuras críticas, las empresas turísticas se comprometen a ser ciber-resilientes. Han desarrollado estrategias preventivas contra ataques y han implementado sistemas para mejorar la visibilidad, el control y la auditoría de la ciberseguridad. En los últimos años, el modelo de seguridad Zero Trust, que se centra en prevenir y combatir ciberataques mediante un enfoque basado en la desconfianza constante, ha cobrado mayor importancia en el sector.

Además, y como indica Campins, anteriormente las aplicaciones y datos estaban protegidos por un perímetro definido, pero ahora se requiere una ciberdefensa extendida, “el modelo Zero Trust no confía en ninguna conexión a la red, verificando dispositivos, máquinas y usuarios en tiempo real mediante identidad y comportamiento. La seguridad es un ciclo de mejora continua, ya que



las empresas, incluyendo las del sector turismo, deben innovar y actualizar sus estrategias y soluciones para contrarrestar los métodos cada vez más sofisticados de los ciberdelincuentes”.

En palabras de Mario de Felipe, director general de Syntax Iberia asegurar la calidad de los datos, así como la precisión para ayudar a tomar decisiones informadas, y colaborar en una mayor resiliencia corporativa al evitar fraudes y ciberataques, es fundamental, “en los proyectos desarrollados para nuestros clientes del sector, tales como Barceló, Tui, Port Aventura, Playa Hotels and Resorts, etc. priorizamos el establecimiento de conexiones seguras y privadas entre las organizaciones y sus datos, optando por proveedores con

## El estado actual del Turismo 4.0 en España

los más altos estándares de seguridad que favorecen la confianza en las transacciones y el almacenamiento de los datos”.

En resumen, para mitigar estos riesgos, se están implementando diversas estrategias, como la encriptación de datos, el uso de protocolos de seguridad robustos, la formación en ciberseguridad para empleados, y la adopción de tecnologías avanzadas de detección y respuesta ante amenazas. “Además, se están siguiendo las regulaciones y normativas internacionales de protección de datos, como el GDPR, para garantizar la privacidad y seguridad de la información del cliente. Algunas grandes compañías están ya en el desarrollo y la implementación de tecnologías de ciberseguridad basadas en IA, capaces de identificar y responder a amenazas en tiempo real”, concluye el presidente de la Comisión Smart Cities de AMETIC.

Estrategias fiables que empresas como Microsoft introducen en sus productos, “la seguridad es una de nuestras máximas prioridades. Por ello, recientemente pusimos a disposición nuestra herramienta de IA generativa diseñada específicamente para la seguridad, Copilot for Security, que permite realizar análisis de grandes volúmenes de datos y ayuda a cerrar las brechas de seguridad más rápidamente y con mayor precisión”, explica Chinchilla.

## Portada

## El estado actual del Turismo 4.0 en España

### Análisis de datos en la toma de decisiones

Los ERP de las empresas del sector turismo y viajes ya empiezan a manejar datos en abundancia, con históricos considerables. Esto redundará en la mejora de la toma de decisiones al proporcionar información precisa y alertar sobre aspectos relevantes sobre el comportamiento del cliente, los movimientos de los mercados y el rendimiento empresarial de los productos y servicios ofrecidos.

Se están haciendo esfuerzos por identificar oportunidades de mejora en la cadena de valor del turismo lo que implica compartir datos y experiencia entre empresas. Además, desde AMETIC inciden en que el análisis de datos está facilitando la toma de decisiones desde predicciones, “en un futuro muy próximo veremos el uso de análisis predictivo avanzado y modelos de aprendizaje automático para prever con mayor precisión esas tendencias del mercado para poder adaptarse rápidamente a los cambios”.

El análisis de datos en las empresas turísticas permite a los gerentes y directivos contar con información precisa y actualizada sobre el comportamiento de los clientes, las tendencias del mercado, la competencia, entre otros aspectos relevantes para la toma de decisiones. “La veracidad, recopilación, análisis y visualización avanzada de los datos son garantía de una toma de decisiones acertada, tanto en análisis descriptivos con información del pasado como en análisis predictivos para optimizar decisiones futuras”, Campins.

Para Viudes, algunas de las formas en que el análisis de datos mejora la toma de decisiones en las empresas turísticas son, “la identificación de patrones y tendencias; Segmentación de mercado; Personalización de la experiencia del cliente; Optimización de la gestión de inventario y precios, y Evaluación del rendimiento de las estrategias de marketing”.



“**Se están haciendo esfuerzos por identificar oportunidades de mejora en la cadena de valor del turismo lo que implica compartir datos y experiencia entre empresas.**”

## Portada

### Cloud computing e IoT

En el momento presente, la nube se ha convertido en la clave para que las empresas del sector turismo dispongan de una infraestructura optimizada al máximo gracias a su flexibilidad y escalabilidad, que les permite ajustar sus recursos en función de la demanda, algo realmente decisivo en un sector con una elevada variabilidad estacional.

Asimismo, para el director general de Syntax Iberia, el hecho de migrar a cloud reduce la necesidad de contar con una infraestructura física propia, “ y los costes derivados del mantenimiento de la misma y con un mejor acceso a las innovaciones de los proveedores y a sus elevados estándares de seguridad”.

¿Pero cómo es este cloud?, el Optical Solution Director de Huawei Empresas España lo enfoca en una tendencia clara hacia la nube híbrida, pública privada, e incluso una nube local, “que te permita interactuar mucho más eficientemente con los datos propios de los dispositivos y aprender comportamiento y anticipar las necesidades”.

Otra de las ventajas que ofrece el cloud computing en la infraestructura tecnológica del turismo es que permite eliminar mucho hardware y por tanto reducir los costes de mantenimiento

de propiedad, “Además, se adapta a las necesidades de cada momento en capacidad de cálculo y almacenamiento, lo que redundará en ahorros notables de costes al pagar lo realmente usado en cada momento para la gestión del negocio”, resalta el presidente de la Comisión Smart Cities de AMETIC.

Por otro lado, el Internet de las Cosas (IoT) está cambiando la gestión de los servicios turísticos al permitir la conexión y comunicación entre los diferentes dispositivos y sistemas utilizados en el sector. Por ejemplo, en opinión de Viudes, los hoteles pueden implementar sensores en las habitaciones para controlar la temperatura,

## El estado actual del Turismo 4.0 en España

la iluminación y otros servicios, lo que permite una gestión más eficiente y personalizada para los huéspedes, “sin duda, la tecnología IoT está revolucionando la manera en que se gestionan y ofrecen los servicios turísticos, permitiendo una mayor eficiencia, personalización y satisfacción para los usuarios”.

Siguiendo este punto, Campins resalta los múltiples ámbitos de aplicación de esta tecnología, “desde la interacción, conexión y comunicación con los clientes hasta la optimización de los costes mediante la gestión de activos, recursos y consumo de energía como, por ejemplo, la electricidad”.



Portada

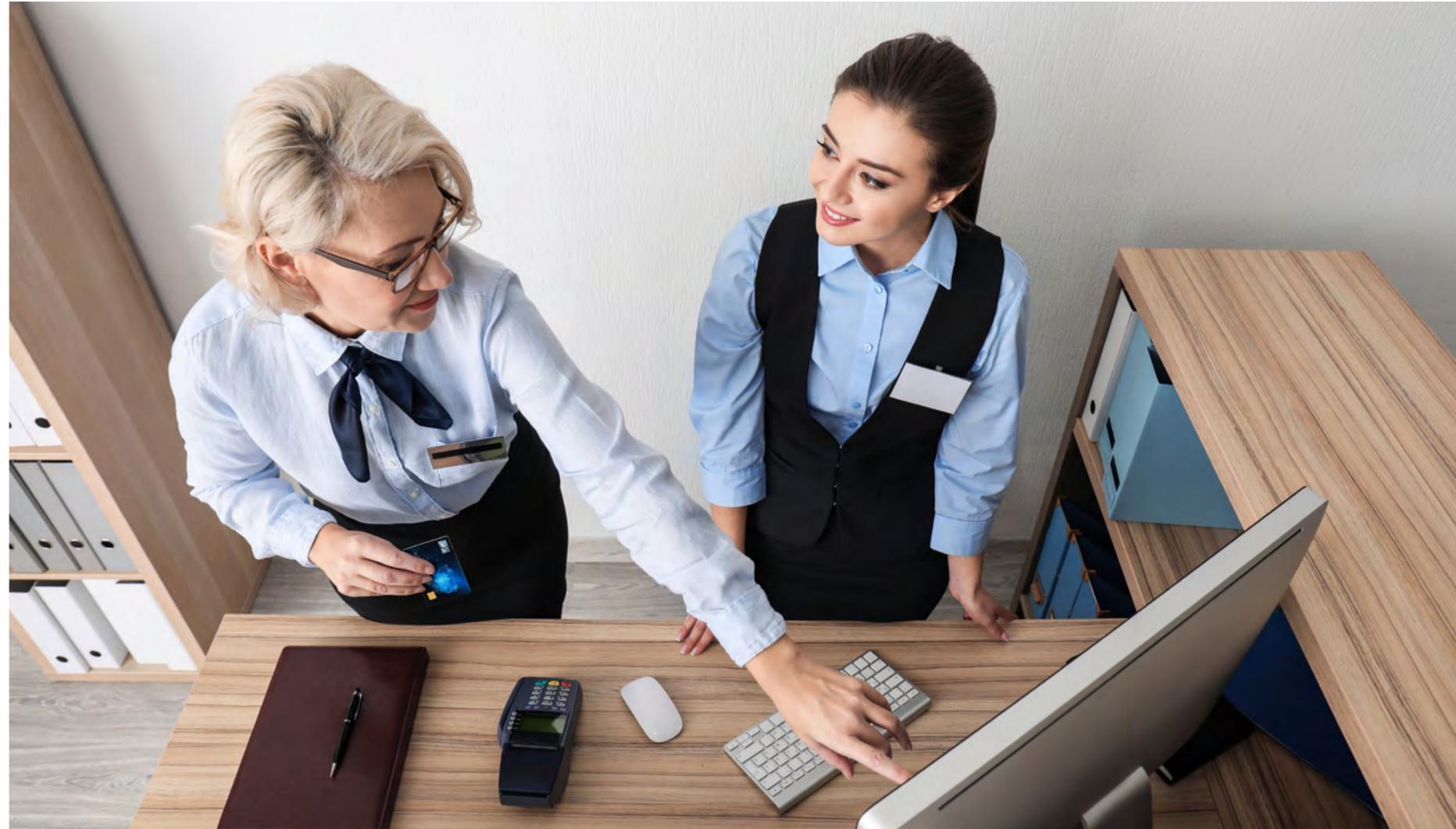
El estado actual del Turismo 4.0 en España

Agenda 2030

Por exigencias legales, las empresas turísticas deben alinear sus objetivos con la Agenda 2030 de sostenibilidad. Para lograrlo, pueden adoptar diversas prácticas sostenibles, como reducir el uso de plásticos, fomentar energías renovables, implementar sistemas de tratamiento de aguas residuales y promover la conservación de la biodiversidad en sus destinos.

Ampliando estas prácticas, desde aggity añaden otras como concienciar a los clientes sobre la importancia de viajar de forma responsable y respetuosa con el medio, “a través de campañas de sensibilización y educación, así como medir y reportar de forma transparente su impacto ambiental y social, para poder identificar áreas de mejora y establecer objetivos concretos para reducir su huella medioambiental y social”.

Siguiendo esta línea, el director de la Unidad de Negocio de Business Applications de Microsoft España señala la migración a plataformas cloud como una estrategia fundamental. “Según un estudio, para 2025, el 95% de las nuevas cargas de trabajo digitales se implementarán en estas plataformas. La nube permite a las empresas turísticas acelerar su digitalización, lo que a su vez optimiza el uso de recursos y mejora la eficiencia de los procesos industriales y de gestión. Esta optimización ayuda a



minimizar el impacto ambiental y reduce el consumo energético”.

Desde AMETIC lo resume en las siguientes ideas:

- Aumentar el nivel de reciclamiento de sus consumos, empezando por la parte de restauración.
- Instalar sistemas de control energético de sus instalaciones para hacer eficiencia energética.

- Concienciar a los empleados con programas de incentivos.
- Fomentar el turismo regenerativo entre sus clientes.
- Electrificando su movilidad.

Portada

 La opinión del CIO | Joan Barceló - **El estado actual del Turismo 4.0 en España**

# Joan Barceló

**CIO de World2Meet y director académico del Global MBA de OBS Business School**



## **Cómo están cambiando las empresas del sector turístico? ¿Cómo han avanzado en sus procesos de digitalización?**

Las empresas del sector han tenido que revisar su estrategia para adaptarse a las nuevas necesidades de los viajeros, a la competencia y a un entorno cambiante, en el que son tan importantes la innovación como la personalización en un marco de sostenibilidad. Los viajeros están evolucionando, de cada vez están más conectados, mejor informados y desean más flexibilidad para disfrutar experiencias únicas y personalizadas.

En este contexto, la digitalización en sí misma no es suficiente, tiene que ser una digitalización con propósito, y se está abordando desde dos ejes, el primero muy orientado al cliente para poder personalizar la oferta, y el segundo más orientado a la mejora de la gestión interna.

El proyecto de World2Meet lo iniciamos en 2020 y somos nativos digitales, por lo que hemos podido adoptar desde el primer momento las nuevas tendencias tecnológicas, y además tenemos la ventaja de contar con un equipo con amplia experiencia en el sector.

## **¿Qué tendencias tecnológicas son las que están impactando más en la digitalización de las empresas del sector turístico?**

En el informe de “tendencias tecnológicas aplicadas al ciclo de vida del viaje” de OBS Business School hemos analizado la evolución de los viajeros y cómo impactan las nuevas tendencias tecnológicas en el ciclo de vida del viaje.

Actualmente, la IA generativa es la tecnología emergente con más impacto y abre un abanico de infinitas posibilidades en todo el ciclo de vida del viaje, tanto desde la perspectiva del viajero como de los profesionales del sector. En este escenario el dato vuelve a ser el protagonista, y el intercambio de información entre todos los partners de la cadena de suministro proporciona una oportunidad única de generar experiencias inolvidables, en un marco colaborativo de hiperconectividad.

## Portada

## La opinión del CIO | Joan Barceló - **El estado actual del Turismo 4.0 en España**

Por tanto, tecnologías como Internet of Things (IoT), 5G, Wireless o SuperApps son también necesarias para que la IA Generativa pueda desplegar su máxima potencia, y las soluciones Fintech, Martech e Insurtech son imprescindibles para obtener mayor flexibilidad.

### **¿Cómo están transformando la inteligencia artificial y los algoritmos el sector turístico?**

Es indudable que el principal objetivo de la transformación es la personalización, desde la inspiración y planificación al disfrute de la experiencia.

No obstante, el ámbito de aplicación es muy amplio, por ejemplo, la IA generativa combinada con automatización puede ser una tecnología clave para mejorar eficiencia y productividad de los profesionales del sector, ayudando también a enfrentarse al reto de la creciente falta de personal. En World 2 Meet estamos introduciendo, progresivamente, smart readers, smart dispatchers y smart decision makers en procesos internos, con excelentes resultados hasta la fecha.

### **¿Es la seguridad de los datos uno de los principales problemas de las empresas del sector? ¿Qué estrategias se están implementando en su empresa?**

La seguridad del dato es un reto en todos los sectores, no solo el turístico. En nuestro caso, la protección del mismo abarca todo el ciclo



**La protección del dato abarca todo el ciclo de vida del viaje, desde la inspiración, hasta el momento del recuerdo, por lo que se extiende más allá de la estricta prestación del servicio**

de vida del viaje, desde la inspiración, hasta el momento del recuerdo, por lo que se extiende más allá de la estricta prestación del servicio.

La estrategia en W2M se ha fundamentado en desarrollar un proyecto formal de Seguridad de la Información y Privacidad con la incorporación de un CISO y la creación de un equipo profesional de protección de datos, GRC, ciberseguridad y prevención del fraude, para poder defender de forma proactiva nuestra información, la de los clientes y la de nuestros partners y proveedores en toda la cadena de suministro. La concienciación y formación son clave en este proceso.

### **¿De qué manera el análisis de datos mejora la toma de decisiones en las empresas turísticas?**

El análisis de datos en el sector turístico es esencial para una toma de decisiones objetiva. No solo facilita la personalización de la experiencia del cliente, adaptando servicios

y ofertas a comportamiento y preferencias, también permite anticipar tendencias y demandas futuras, a la vez que impulsa la innovación en productos y servicios para cubrir nuevas necesidades, así como la sostenibilidad.

Por otra parte, es clave para la optimización de la eficiencia operativa y la estrategia de precios, fortaleciendo la posición competitiva y ayudando a combatir el fraude y riesgos detectando patrones anómalos.

Sin embargo, para que el análisis de datos sea efectivo, los datos deben tener la calidad adecuada. Para ello deben ser precisos, completos, actualizados y consistentes, en estricto cumplimiento de privacidad y seguridad.



## Legalidad TIC

# Estafas en redes sociales y criptomonedas

JAVIER LÓPEZ

Socio de Écija Abogados

Las redes sociales han supuesto un gran avance en muchos sentidos: como mecanismo de comunicación y conexión entre personas, canal para transmitir información y conocimientos, foro donde compartir experiencias y emociones, así como otras muchas más utilidades de gran valor, llegando incluso a ser un instrumento muy eficaz para cumplir objetivos solidarios, como operaciones de crowdfunding para conseguir fondos para causas sociales, o campañas de concienciación de valores como el cambio climático o contra las guerras que asolan nuestro planeta.

Pero como todo espacio donde interactúa el ser humano, también es susceptible de que se realicen actuaciones perniciosas e, incluso, delictivas, o que infrinjan la ley, como la difusión de fake news, incitación al odio, violaciones de derechos de propiedad intelectual e industrial, agresiones contra la libertad sexual, ataques contra la privacidad, extorsiones, etc. Dentro de estas acciones ilícitas, uno de los delitos más peligrosos es el de las estafas cometidas a través y/o haciendo uso de las redes sociales.

Las modalidades usadas por los ciberdelincuentes para ello son muy

variadas. Una de las más conocidas es la llamada “romance scam” (estafa del amor), normalmente perpetrada por organizaciones criminales internacionales, que se aprovechan de la especial vulnerabilidad que provoca en algunas personas sus carencias afectivas, así como del supuesto anonimato que confiere el ciberespacio, para convencer a sus víctimas de que les entreguen su dinero voluntariamente.

En enero de 2024 fue famoso el caso de las hermanas de Morata de Tajuña, que se arruinaron tras entregar importantes cantidades a dos fingidos militares, con los que creían mantener una relación amorosa a distancia, y que acabo con un triple homicidio de estas mujeres y su anciano hermano, presuntamente por un ajuste de cuentas del prestamista a quien se vieron obligadas a pedir dinero para atender las solicitudes económicas de sus pretendidos cibernovios.

Pero este no es el único gancho usado por los ciberdelincuentes. En efecto, uno de los que más se está usando últimamente es el de las criptomonedas, que, tras el boom inicial que tuvieron, han ido perdiendo fuelle a media que se han ido conociendo diversos escándalos que han hecho que se vea mermada la confianza de



los usuarios en la criptoconomía debido a la naturaleza volátil de los activos digitales. En este sentido, sonada fue en noviembre de 2022 la quiebra de FTX, que afectó a más de un millón de clientes y que dejó un pasivo de más de 3.000 millones de dólares.

## Legalidad TIC

Aquí en España, también en noviembre de 2022, generó una gran conmoción la muerte de Javier Biosca, que se precipitó desde la quinta planta de un edificio de Estepona (Málaga), apenas tres semanas después de haber quedado en libertad provisional tras pagar una fianza de un millón de euros. Biosca estaba siendo investigado por la Audiencia Nacional en un procedimiento penal seguido por la comisión de una presunta estafa de 250 millones en criptomonedas realizada a través de la sociedad Algorithmics Group, que carecía de las pertinentes autorizaciones de la Comisión Nacional del Mercado de Valores (CNMV) ni de otros organismos supervisores.

Y es que las sospechas sobre la legalidad de determinadas actuaciones relacionadas con las criptomonedas son crecientes. En este sentido, en marzo de 2024, la Agencia Española de Protección de Datos (AEPD) acordó el cese inmediato de la recogida y tratamiento de datos personales –y el bloqueo de los datos ya recopilados– que estaba realizando en febrero de 2024 en un stand de un centro comercial de A Coruña, la entidad Tools for Humanity Corporation en el seno de su proyecto “Worldcoin”, consistente en la recogida del iris de los ojos de personas (incluidos menores) a cambio de unas criptomonedas, sin información suficiente y sin posibilidad de retirar el consentimiento.

Esto ha provocado que se usen todo tipo de estrategias comerciales para vender criptomonedas, algunas de ellas incumpliendo claramente la legalidad, ya sea vía spam mediante el envío masivo de mails; o mediante mensajes con señuelos en redes sociales, como los realizados usando la imagen de Carlos Sobera, David Broncano o Cristina Pedroche, acompañados de llamativos titulares falsos para provocar que el usuario pinche en ellos y acceda al link que le redirija a una web.

Estas actuaciones implicarían la comisión de diversas infracciones contra quienes sean víctimas de fraudes, como el delito de estafa, vulneración de la normativa sobre protección de Datos Personales, delito de apoderamiento y tráfico ilegal de Datos Personales –en el más que probable supuesto de que estos datos personales se incorporen a bases de datos con las que se comercializa de forma ilegal en la Dark web–, así como vulneración de la normativa sobre publicidad engañosa y protección de los Consumidores, entre otras.

En cuanto a las infracciones legales cometidas contra los personajes famosos cuya imagen se haya usado sin su consentimiento, relacionándoles además con afirmaciones difamatorias, supondría, al menos, la comisión del delito de suplantación de identidad, vulneración del derecho a la propia imagen,

## Estafas en redes sociales y criptomonedas

delito de calumnias o vulneración del derecho al honor, al atribuir hechos falsos que afectan al buen nombre y prestigio, en función de la gravedad de lo que se les impute.

Dicho esto, aunque, en teoría, las redes sociales deben identificar a los usuarios que crean perfiles, en muchas ocasiones existen cuentas fake, ya que no existe un control efectivo sobre los datos de identificación, lo que viene evidenciado por el hecho de que las propias plataformas disponen de espacios para denunciar estas cuestiones. Esto hace que sea muy difícil identificar a los responsables, máxime si están en países donde existen menos controles (Rusia, China, etc.), tratándose en muchas ocasiones de perfiles controlados por bots que generan sus contenidos con inteligencia artificial.

Ello no significa que las redes sociales puedan zafarse de sus obligaciones de control ni eludir las responsabilidades que les corresponden, ya que los artículos 16 y siguientes de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI) establecen la responsabilidad de los prestadores de servicio (en este caso, las redes sociales) en el supuesto de que no retiren contenidos ilícitos tras tener conocimiento efectivo de los mismos.

## Mujeres TIC

# María Eugenia Carbonell

## Responsable de Partner Sales para AWS en el Sur de Europa



### ¿Cómo llegó al mundo TIC?

Llegué por casualidad, me encanta mejorar procesos y siempre para hacerlo usaba la tecnología, por ello se abrió una vacante de Directora de Tecnología en Sanitas Mayores y me ofrecieron participar en el proceso. Resulté ser la elegida. Siempre dejé claro que no venía de un mundo tecnológico, más bien de organización, rediseño de procesos y calidad, donde la tecnología juega un papel fundamental.

### ¿Qué es lo que más valora de su trabajo?

En este sector hay que estar al día y formarse continuamente, porque la tecnología avanza a un nivel vertiginoso y tienes que estudiar, asistir a eventos para estar al día, hablar con muchas personas y leer mucho para siempre estar informada. Eso es algo que me apasiona. También la capacidad de transformar procesos gracias a la tecnología.

### En su opinión ¿qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?

Yo creo que hemos mejorado y que ahora hay más referentes, pero nos toca ayudar a niñas a concienciarlas que es una carrera apasionante. Creo que hay una creencia de que es más fácil otro tipo de carreras, pero creo que hay que quitar esa creencia.

### ¿Cree que existe el “techo de cristal” en las empresas TIC?

No sé si llamarlo techo de cristal, pero sí que cuesta encontrar mujeres en puestos de responsabilidad. Ha cambiado, pero debe seguir mejorando.

### ¿Cuál debería ser la solución?

Creo que es de vital importancia que la legislación siga apoyando este aspecto porque ayuda a conseguir mejores cuotas, ayuda a concienciar a las empresas de la necesidad de incluir mujeres en puestos de responsabilidad. Sé que no es fácil porque creo que es un tema de talento, pero sí creo que ayuda.

## Mujeres TIC

### ¿Una política de cuotas puede resolver el problema?

Sin lugar a dudas, las cuotas ayudan a que no vayamos a lo fácil y haya concienciación en que debemos tener igualdad. Además, es bueno por que creo que el liderazgo de hombres y mujeres es diferente.

### ¿Qué dificultades se encontró usted para llegar a la posición que tiene actualmente?

Tuve muchas. Algunas de ellas: primero que mis compañeros en comités de dirección era hombres, cuyas vidas y gestión con sus hijos estaban cubiertas por sus mujeres, lo cual conllevó que empezaran a pensar que en mi caso no era así. En mi caso, el 50% de las tareas era distribuido con mi marido y mi organización y disponibilidad era diferente. En lo que respecta a la conciliación, había reuniones que acaban a las 20 o 21h, tenía ayuda en casa, pero en muchas ocasiones no podía ver a mi hijo por que llegaba muy tarde. Finalmente, al no venir del sector tecnológico, hubo muchos perfiles que no me vieron de igual a igual. Fue un reto.

### ¿Qué es lo que más valora de su empresa con respecto a la integración de la mujer?

Cantabria Labs cuenta con mujeres maravillosas, en puestos de dirección y en otras posiciones. Por ejemplo, nuestra CEO, Susana Rodríguez. Además tenemos varias directoras generales de negocio que son mujeres, grandes compañeras

## María Eugenia Carbonell, Responsable de Partner Sales para AWS en el Sur de Europa

algo que me ha aportado mucho por que son mujeres fuertes, que me ayudan a crecer cada día y a las cuales admiro.

### ¿Qué cree que hay que mejorar para que se pueda compatibilizar mejor la vida privada o personal?

Creo que es un tema de uno mismo. El teletrabajo ayuda a que si te quedas en casa el tiempo que gastas en desplazamientos lo puedas dedicar a otras cosas, como en mi caso a estar más sana y a hacer deporte. También creo que es necesario poner límites y bloquear tiempo para diferentes aspectos relevantes de tu vida y compaginarlo con tu vida laboral.

### ¿Es un problema de las empresas, de las relaciones de pareja o de uno mismo??

Creo que de uno mismo. El teletrabajo ayuda a que si te quedas en casa el tiempo que gastas en desplazamientos lo puedas dedicar a otras cosas. También creo que es necesario poner límites y bloquear tiempo para diferentes aspectos relevantes de tu vida y compaginarlo con tu vida laboral.

### ¿Le han servido los estudios que hizo para realizar su labor actual?

Sí en muchas cosas. Creo que las carreras técnicas nos aportan un nivel de pensamiento, una forma especial de resolver problemas y de ir más allá. Yo volvería a hacerlo.

### Solucione el problema de la educación en España...

Te diría que hacen falta recursos, dar otro enfoque a la educación actual. Está cómo hace años y debe ser más personalizada. Te pongo un caso. Tengo un hijo disléxico que es un trastorno del aprendizaje que si no se trata puede llevar a los niños a un fracaso escolar. Los profesores si no lo detectan pueden hacer brillar a un niño o destruirlo. Por ello, considero que faltan medios, educadores y tratar de personalizar la enseñanza y creo que la tecnología jugará un papel fundamental en este aspecto.

### ¿Hacia dónde cree que va el sector TIC?

Hacia un mundo que me asusta con la AI. Ahora todo el mundo cree que sabe por qué busca en ChatGPT, pero no sabe de dónde viene esa información. Por ello, más que nunca, el pensamiento crítico y la ética jugaran un papel fundamental en lo que viene.

### En su opinión, ¿cuáles van a ser las tendencias que realmente van a transformar la sociedad?

Sin duda la Inteligencia Artificial transformará cómo vivimos en la actualidad y cómo mejoramos nuestro día a día, también el Cloud y la rapidez en tener infraestructuras para acometer nuestros proyectos.

## Un CIO en 20 líneas

# "La IA va a tener un gran impacto en el sector logístico"

## Pablo Giancarli

*Regional IT Manager IBERIA (CIO) – Rhenus Air & Ocean*

### ¿A qué se dedica la parte principal del presupuesto de TI de la empresa?

Una parte de nuestro presupuesto TI se dedica a mantener y optimizar los sistemas centrales de gestión. Por otra parte importante está dedicada a la transformación digital integral, incluyendo la implementación de soluciones como Microsoft Dynamics 365 y herramientas para un entorno de trabajo digital.

### ¿En qué área se está invirtiendo más este año?

Este año estamos invirtiendo fuertemente en transformación digital, automatización y digital workplace.

### ¿Qué proyecto es del que está más satisfecho?

El proyecto del que me siento más orgulloso fue la de ser parte del equipo de transición en la fundación y creación de la compañía Axion Energy, hacer nacer, crecer y desarrollar una organización desde sus cimientos es algo especial y motivador tanto en lo profesional como personal.

### Si le pusieran todos los beneficios de la empresa a cargo del depto de TI, ¿qué implementaría?

Si tuviera total control del presupuesto, impulsaría un programa de transformación digital integral, incorporando inteligencia artificial para la optimización de cargas y despachos, previsión de demanda, asistentes virtuales; así como robotización de procesos administrativos para mayor eficiencia



**Fecha de nacimiento:** 26/08/1971

**Estado Civil:** Casado

**Hijos:** 2 hijas / 1 hijo.

**Hobbies:** Deporte (golf, running, canicross), cocina, viajes y cine

**Estudios:** Licenciado en Sistemas de Información en USAL  
especialización en TICs.

**Personas a su cargo:** Dirijo un equipo de 15 profesionales de TI

**Trabajos anteriores:** Pan American Energy (2018-2021),  
Axion Energy (2011-2018), Chemo Group (2008-2011).

## Un CIO en 20 líneas

### ¿Qué retos tiene un sector como el de la logística?

Algunos de los mayores retos son la optimización de las cadenas de suministro, gestión de la complejidad operativa, control de costos, satisfacción del cliente y agilidad para adaptarse a cambios de demanda. La transformación digital es clave para abordar estos desafíos.

### ¿Cuál va a ser el impacto de la IA en este sector?

La inteligencia artificial tendrá un impacto tremendamente disruptivo en logística. Algunas aplicaciones clave serán: predicción de demanda, optimización dinámica de rutas, asignación inteligente de recursos, mantenimiento predictivo, visión artificial para clasificar inventario, chatbots para atención al cliente, etc.

### ¿Cuáles cree que van a ser las principales tendencias tecnológicas de impacto?

Las principales tendencias que veo en el horizonte son: Internet de las Cosas, inteligencia artificial, robótica y automatización, analítica avanzada, blockchain aplicado a trazabilidad de la cadena de suministro, realidad aumentada/virtual y computación en la nube.

### ¿Qué tendencias observa en el mundo TIC?

Algunas de las grandes tendencias en TIC son: aceleración de la transformación digital, auge del teletrabajo e imperativos de ciberseguridad, consolidación del modelo de "todo como servicio",

## Pablo Giancarli, Regional IT Manager IBERIA (CIO) – Rhenus Air & Ocean

hiperconvergencia, redes 5G, tecnologías cuánticas emergentes, etc.

### ¿Cuál es la herramienta que le cambió la vida?

La herramienta que verdaderamente me cambió la vida fue la adopción de una solución de Business Intelligence que nos permite tomar decisiones basadas en datos en tiempo real, en lugar de trabajar con reportes estáticos desactualizados. Fue un cambio de paradigma. El negocio feliz!

### ¿Extraer valor del dato supondrá la evolución de empresas como la suya?

Sin duda alguna. En logística, la habilidad de aprovechar el enorme caudal de datos que generamos y aplicar analítica avanzada para extraer insights accionables será un factor clave para nuestra ventaja competitiva y evolución como empresa en el futuro cercano.

### ¿Transformación digital: slogan o necesidad?

La transformación digital definitivamente no es un slogan de moda, sino una necesidad estratégica imperiosa para lograr eficiencias, agilidad, reducción de costos y mantenerse competitivo y relevante en un entorno empresarial que avanza rápidamente. Una maravilla!

### ¿Lo del I+D+i es una leyenda urbana?

Para nada. En nuestro sector la innovación, tanto en procesos como en desarrollo e

implementación de nuevas tecnologías, es un pilar fundamental para destacar y mantenerse a la vanguardia. De otra manera, quedamos rezagados en pos de la competencia.

### ¿En la nube u on-premise?

Nuestra estrategia es una combinación híbrida de mantener ciertos sistemas críticos on-premise por temas de cumplimiento y seguridad; pero estamos abrazando la nube para aplicaciones más livianas y de nueva adquisición por su agilidad, escalabilidad y reducción de costos operativos. A futuro... 90% en la nube.

### ¿Falta de conocimientos de ciberseguridad de usuarios es el principal reto?

Es ciertamente uno de los mayores retos que enfrentamos. Por más mecanismos tecnológicos de seguridad sofisticados que implementemos, la superficie de riesgo siempre incluye el factor humano. La concientización y capacitación constante a todos los usuarios es muy importante.

### ¿Ve realistas los vehículos autónomos a corto plazo?

Los vehículos totalmente autónomos para aplicaciones comerciales masivas aún veo un horizonte de 5-10 años probablemente. Sin embargo a nivel grupo, ya estamos probando funcionalidades semi-autónomas.

## Aplicación Práctica

# Briolf Group pone en marcha su plan estratégico de seguridad TI con fibratel

Briolf Group, grupo industrial con sede en Gerona con más de 20 filiales propias en el mundo, está implementando una estrategia integral de seguridad para las siete sociedades que tiene la multinacional. Este es un proyecto para el que confiado en fsafe, la unidad de ciberseguridad de fibratel.

Este grupo empresarial de origen familiar, que cuenta con más de 1.000 empleados en el mundo, ha crecido mucho orgánica e inorgánicamente, incorporando a nuevas compañías hasta llegar a siete sociedades productivas y posicionándose como referente en tres segmentos de mercado: fabricación de productos para recubrimientos, aerosoles y soluciones para fijación.

Como explica Miquel Calvo, director de Sistemas de Información de Briolf, “el principal reto al que nos enfrentábamos, venía muy condicionado por el crecimiento de los últimos años. Al adquirir nuevas compañías, con sedes de producción en diferentes países, cada una de ellas empleaba diferentes tecnologías, lo que configuraba un escenario muy heterogéneo, difícil de gestionar, de controlar y de saber cuáles eran los comportamientos que estamos teniendo en nuestro entorno tecnológico”.



Eso podía implicar riesgos para sus activos de TI, lo que hizo que la compañía se planteara diseñar e implantar un plan de seguridad, con diferentes proyectos que se fuesen ejecutando en el plazo de tres años, e incrementar así sus niveles de seguridad a partir de un roadmap definido. En él se identificaron las diferentes tecnologías de seguridad aplicables priorizando la securización de los procesos, de los diferentes entornos de producción y la protección de los usuarios.

## Aplicación Práctica

### La consultoría, clave en este plan

En este proyecto desempeñó un papel muy importante la consultoría, eje de los servicios gestionados AllDefense de la unidad de ciberseguridad de fibratel, para, en la fase preliminar, identificar las principales amenazas para el negocio, descubrir aquellas frente a las que no está protegido y priorizar la inversión. “Antes de plantear soluciones, fue muy importante escuchar a nuestro cliente y entender su negocio. Así pudimos adaptar la tecnología a los objetivos definidos por Briolf, realizando pruebas de concepto y proponiendo las mejores soluciones, alineadas con el reto que quería solucionar y aportarle una mejora para su negocio en el área de seguridad”, subraya Carlos Castillo, director de negocio de fibratel.

Al respecto, el CIO de Briolf añade que “valoramos muy positivamente la experiencia de colaboración con fsafe porque, fundamentalmente, nos ha llevado a no cometer el error de invertir en tecnología porque sí, sino buscar cuál es la mejor opción y priorizar aquellas iniciativas que nos iban a aportar más valor y seguir un orden lo más razonable posible en el desarrollo de este plan que estamos trabajando a tres años vista”.

### Beneficios que ya se perciben

Tras el desarrollo de los primeros proyectos, Briolf Group ha obtenido control sobre lo que

## Briolf Group pone en marcha su plan estratégico de seguridad TI con fibratel



está sucediendo en sus activos tecnológicos y en su red. “Al desplegar soluciones EDR en los primeros proyectos, conocemos el comportamiento de nuestros usuarios o los comportamientos malintencionados sobre nuestros equipos, lo que nos permite actuar sobre ellos y tomar decisiones muy rápidas, con un servicio que actúa las 24 horas al día”, explica Miquel Calvo.

Asimismo, ha mejorado el control sobre lo que ocurre en su plataforma de email, uno de los

principales puntos de entrada de los intentos de ataque, al poder inspeccionar el correo.

En definitiva, Briolf está consiguiendo minimizar el riesgo de recibir cualquier tipo de ataque de ciberseguridad.



# ¿Necesitas almacenamiento para sistemas NAS colaborativos?

**WD Red® es para ti**

**Western Digital**



Western Digital, el diseño de Western Digital, el logotipo de Western Digital, OptiNAND, WD Red, WD Red Plus y WD Red Pro son marcas comerciales registradas o marcas comerciales de Western Digital Corporation o sus filiales en EE. UU. u otros países. La marca NVMe es una marca comercial de NVM Express, Inc. Todas las demás marcas comerciales son propiedad de sus respectivos propietarios. Las especificaciones del producto están sujetas a cambios sin previo aviso. Las imágenes mostradas pueden diferir de los productos reales. © 2024 Western Digital Corporation o sus filiales. Todos los derechos reservados.

## Tendencias

# Cómo realizar una correcta migración SaaS

ENRIQUE O'CONNOR, Director general de Vaultinum para Iberia y Latam

KRISTIN AVON, Asesora legal de Vaultinum

Con una tasa de crecimiento anual prevista de alrededor del 18,4%, el mercado mundial de Software-as-a-Service (SaaS) pasará de unos 320.000 millones de dólares en 2024 a cerca de 1,23 billones en 2032[1]. Esta expansión está impulsada por la creciente preferencia por los modelos basados en suscripciones en todos los sectores, desde el entretenimiento hasta el software empresarial, lo que posiciona a este modelo de negocio como un enfoque altamente rentable y sostenible para las empresas de software.

Estas son las principales consideraciones para las empresas que se plantean un cambio a SaaS y cuáles son las posibles razones en contra de hacer esta transición.

### Eficiencia de costes

Uno de los principales impulsores de la adopción de SaaS es su rentabilidad, pues elimina la necesidad de que las organizaciones adquieran, instalen, actualicen y mantengan sistemas de hardware y software. En su lugar, el proveedor de software como servicio gestiona todos los posibles problemas técnicos, y el cliente paga una cuota de suscripción que normalmente incluye soporte, mantenimiento y actualizaciones periódicas.

Este cambio de un modelo de gastos de capital (CapEx) a un modelo de gastos operativos (OpEx) permite a las empresas asignar recursos de forma más flexible y predecible.

### Escalabilidad y accesibilidad

Otra ventaja de SaaS es su escalabilidad inherente, que permite a las empresas ampliar o reducir fácilmente su uso en función de sus necesidades sin tener que realizar cambios significativos en su infraestructura de TI. Además, las aplicaciones bajo este modelo son accesibles desde cualquier lugar, lo que resulta especialmente beneficioso en los entornos de trabajo actuales, cada vez más remotos y distribuidos. Esta accesibilidad mejora la colaboración entre equipos dispersos geográficamente y contribuye a aumentar los niveles de productividad.

### Despliegue rápido e innovación

Las aplicaciones SaaS suelen estar disponibles para su uso casi inmediatamente después de iniciar la suscripción, lo que reduce drásticamente el tiempo y el esfuerzo necesarios para su implantación en comparación con el software tradicional. Además, los proveedores de software como



servicio actualizan con frecuencia sus ofertas para incluir nuevas funciones y mejoras, garantizando que todos los usuarios se beneficien de las últimas funcionalidades sin costes adicionales de actualización ni tiempos de inactividad. Este ciclo de innovación continua anima a las empresas a seguir siendo ágiles y competitivas.

## Tendencias

### LOS RETOS

Aunque las ventajas de esta propuesta son numerosas, existen razones válidas por las que una empresa de software puede optar por retrasar o evitar la migración desde un modelo on-premise:

- **Altas necesidades de personalización de los clientes actuales:** Si la base de clientes tiene amplias necesidades de personalización que están profundamente integradas en sus operaciones, el enfoque estandarizado de SaaS



puede no satisfacer todas las necesidades de los clientes, lo que puede conducir a la insatisfacción del cliente y la rotación.

- **Inversión sustancial en la infraestructura existente:** Las empresas que han realizado recientemente grandes inversiones en su propia infraestructura pueden descubrir que pasar a un modelo de software como servicio no es rentable a corto plazo. Los costes irre recuperables del hardware y el software existentes pueden retrasar el retorno de la inversión de la transición a SaaS.
- **Problemas normativos y de residencia de datos:** Algunos sectores están sujetos a estrictos requisitos normativos que pueden imponer la residencia de los datos, lo que hace que la naturaleza descentralizada de SaaS resulte problemática. En estos casos, puede ser necesario mantener una solución on-premise para cumplir los requisitos legales.
- **Fiabilidad y control:** Dependiendo de un proveedor externo para las operaciones críticas de la empresa puede introducir riesgos relacionados con el tiempo de inactividad y la pérdida de control sobre el rendimiento y las normas de seguridad. Las empresas pueden preferir mantener el control sobre su entorno informático para garantizar la fiabilidad y la seguridad de acuerdo con sus normas.

## Cómo realizar una correcta migración SaaS

### CONCLUSIÓN

La transición de on-premise a software como servicio es un viaje transformador que ofrece a las empresas de software la oportunidad de alinearse más estrechamente con las expectativas de los clientes modernos y las tendencias del mercado. Aunque las ventajas del SaaS son evidentes, como los ingresos recurrentes, la mayor escalabilidad y la mejora del compromiso de los clientes, la decisión de migrar debe planificarse estratégicamente.

Las empresas deben evaluar cuidadosamente su infraestructura actual, su base de clientes y la dinámica del mercado. También deben tener en cuenta los posibles retos, como la necesidad de una inversión inicial sustancial, los cambios en los requisitos de asistencia al cliente y la garantía de la seguridad de los datos y el cumplimiento de la normativa.

En última instancia, el éxito de la migración a SaaS no solo depende de la ejecución técnica y estratégica, sino también de mantener una línea clara de comunicación con los clientes para gestionar las expectativas y proporcionar valor de forma coherente. Con una planificación y ejecución cuidadosas, el cambio a este modelo de software puede abrir nuevas vías de crecimiento.

## Tendencias

# Los servicios que más atraen al CIO en la nube pública

DIONISIO GARCÍA,  
Value Added Services en Avvale

La nube pública se ha convertido en una ayuda para el CIO a que le permite, no sólo la adopción rápida de prácticas para impulsar el crecimiento de la organización, sino también adaptar los procesos a los requerimientos de negocio o mejorar la sostenibilidad de la empresa. Es cierto que los proveedores proporcionan infinidad de servicios pero hay algunos que son más importantes para el CIO que otros y que, posiblemente sean los que van a experimentar un mayor crecimiento de todos los que se pueden encontrar en la nube pública fundamentalmente por los beneficios que presentan, tanto en términos de optimización de eficiencia operativa, como de reducción de costes.

La migración de cargas de trabajo de un entorno on-premise, ya sea con capacidades reducidas o sobredimensionadas, conlleva costes significativos, que incluyen gastos de comunicaciones y eléctricos. Esto nos lleva a considerar cada vez más la migración Cloud, ya sea de todo nuestro landscape de sistemas, aplicativos o para el uso de servicios en modalidad pago por uso, con la intención de reducir tanto nuestros costes de CAPEX (gastos de capital) como de OPEX (gastos operativos).

Está claro que los servicios que ofrece la nube pública reportan importantes beneficios de optimización de eficiencia operativa y reducción de costes, además de ofrecer soluciones innovadoras para impulsar el crecimiento empresarial. A continuación, presentaremos los servicios que más demanda tendrán en los próximos años.



### SERVICIOS DE NUBE PÚBLICA MÁS DEMANDADOS

**Instancias bajo demanda.** ¿Está considerando la implementación de una nueva base de datos en su servidor local? Ponga a prueba paciencia, porque es probable que se encuentre con una espera considerable. Sin embargo, si está dispuesto a explorar la posibilidad de una máquina virtual (VM) en sus instalaciones en lugar de un servidor físico y su empresa utiliza VMware o tecnologías similares, su espera puede minimizarse. Por otro lado, si está pensando en crear una instancia de servidor en Public Cloud, ésta se puede aprovisionar y ejecutar en aproximadamente 15 minutos. Además, tendrá la flexibilidad de adaptarla a sus necesidades y apagarla cuando no esté en uso.

**Servicios sin servidor.** El término "sin servidor" implica que un servicio o un fragmento de código se ejecutará bajo demanda durante un breve período de tiempo, generalmente en respuesta a un evento, sin la necesidad de una máquina virtual dedicada para su ejecución. Cuando un servicio opera sin servidor, por lo general, no es necesario preocuparse por el servidor subyacente; los recursos se asignan desde un grupo gestionado por el proveedor de la nube. Los servicios sin servidor, actualmente disponibles

## Tendencias

en todas las principales nubes públicas, suelen incluir escalado automático, alta disponibilidad integrada y un modelo de facturación de pago por valor. Si busca una aplicación sin servidor sin estar vinculado a una nube pública específica, puede optar por un marco sin servidor independiente del proveedor, como Kubeless, que solo requiere un clúster de Kubernetes disponible como servicio en la nube

**Contenedores bajo demanda.** Los contenedores bajo demanda son una forma eficiente y flexible de empaquetar, distribuir y ejecutar aplicaciones. En esencia, un contenedor es una unidad de software liviana que encapsula el código de una aplicación y todas sus dependencias, lo que permite que se ejecute de manera uniforme en cualquier entorno, desde un entorno de desarrollo local hasta uno de producción en la nube. La ejecución de contenedores bajo demanda ofrece todas las ventajas asociadas con las máquinas virtuales bajo demanda, con el añadido de requerir menos recursos y costar menos. Esta característica los convierte en una opción altamente favorable para diversas aplicaciones, al combinar eficiencia y economía en su implementación

**Imágenes de contenedores preconstruidas.** Se trata de plantillas prediseñadas que contienen todo lo necesario para ejecutar una aplicación dentro de un contenedor. Estas imágenes están configuradas con el sistema operativo, las bibliotecas y las

dependencias necesarias para que la aplicación funcione de manera eficiente en cualquier entorno de contenedor. Suelen estar configuradas con las mejores prácticas de seguridad. Son una herramienta poderosa para simplificar y acelerar el desarrollo y despliegue de aplicaciones, al tiempo que promueven la consistencia y la confiabilidad en los entornos de contenedor

**Servidores de escalado automático.** Son una solución en Public Cloud que permite ajustar dinámicamente la capacidad de procesamiento y almacenamiento de un sistema según la demanda en tiempo real de forma automática, sin necesidad de intervención manual. La mayoría de las nubes públicas permiten escalar automáticamente el tamaño de las máquinas virtuales y los servicios según la demanda, ya sea aumentando o disminuyendo el número de instancias o modificando el tamaño de las mismas. Esto se realiza en respuesta al uso en tiempo real, permitiendo una escalabilidad fluida hacia arriba o hacia abajo según sea necesario. Los beneficios de esta tecnología incluyen una mejor capacidad de respuesta del sistema, optimización de recursos, reducción de costes operativos al evitar la sobre provisión de recursos innecesarios, y una mayor disponibilidad y confiabilidad del servicio para los usuarios finales

**Bases de datos.** Las principales plataformas de nube pública, junto con diversos proveedores de

## Los servicios que más atraen al CIO en la nube pública

bases de datos, han implementado sistemas de bases de datos distribuidas con interconexiones redundantes y algoritmos de consenso distribuidos. Estos avances les permiten operar de manera eficiente y garantizar una confiabilidad excepcional, con un tiempo de actividad que alcanza hasta cinco nueves (99.999%)

**Servicios híbridos.** Las empresas con grandes inversiones en centros de datos a menudo desean extender sus aplicaciones y servicios existentes a la nube en lugar de reemplazarlos con servicios en la nube. Todos los principales proveedores de nube ahora ofrecen formas de lograrlo, tanto mediante el uso de servicios híbridos específicos, por ejemplo, bases de datos que pueden abarcar centros de datos y nubes, como servidores locales y recursos de nube perimetral que se conectan a la nube pública, a menudo llamada nube híbrida

**Continuidad de negocio.** El entrenamiento de modelos de aprendizaje profundo que requieren grandes conjuntos de datos puede extenderse por más de una semana cuando se ejecuta en grupos de CPU. La utilización de GPU, TPU y FPGA puede reducir considerablemente este tiempo y su disponibilidad en la nube simplifica su utilización según sea necesario.



## Entrevista

## Antonio García Romero, CEO de Teldat



# “No podemos tolerar accesos de comunicaciones que no sean seguros”

Teldat está en fase de expansión. La firma quiere consolidar su presencia en España y Latinoamérica a la par que incrementa sus operaciones en Asia-Pacífico. Centrada en la seguridad de la red, la compañía apuesta por la IA para prevenir ataques. Hablamos con Antonio García Romero, CEO de Teldat sobre los retos de la organización.

MANUEL NAVARRO

### ¿Cuáles son los retos que se ha marcado Teldat para este año?

El año 2024 será crucial para nuestra empresa, ya que nos enfrentamos a dos desafíos de gran envergadura. En el ámbito empresarial, estamos decididos a consolidar nuestra presencia en Europa y Latinoamérica, al mismo tiempo que buscamos expandir nuestras operaciones en Medio Oriente y Asia Pacífico. Desde una perspectiva estratégica, estamos comprometidos con tres apuestas fundamentales en el campo de la Inteligencia Artificial. Primero, gracias a nuestra alianza con Google, dotaremos a las nuevas generaciones de equipamiento con las más avanzadas capacidades de Aprendizaje Automático. Además, integraremos las últimas innovaciones en Configuraciones Reactivas de Red en nuestras soluciones de networking y ciberseguridad. Por último, nos enfocaremos en desarrollar un sistema inteligente de generación de amenazas y ataques ZeroDay mediante Inteligencia Artificial Generativa. Estas iniciativas nos permitirán mantenernos a la vanguardia en un mercado en constante evolución y ofrecer soluciones innovadoras a nuestros clientes en todo el mundo.

## Entrevista

### **Su negocio tradicional está en las comunicaciones, sin embargo, en los últimos tiempos están apostando claramente por la seguridad, ¿por qué?**

Ha habido varios factores. En primer lugar, hemos identificado una demanda creciente en el mercado en lo que respecta a soluciones de seguridad. Esta tendencia nos ha llevado a adaptar y diversificar nuestra oferta para satisfacer las necesidades emergentes de nuestros clientes. Además, hemos reconocido la importancia de integrar y generar sinergias entre nuestras capacidades en el ámbito de las telecomunicaciones y la protección de datos. Esta integración nos permite ofrecer soluciones más completas y robustas, que aborden de manera integral tanto las necesidades de comunicación como las de seguridad de nuestros clientes.

A su vez, la evolución del mercado hacia una mayor adopción de redes residenciales para uso corporativo ha generado la necesidad de ofrecer soluciones avanzadas de red, como SD-WAN. Sin embargo, hemos observado que estas soluciones no siempre cubren adecuadamente las exigencias en materia de ciberseguridad para proteger los accesos a estas redes. Así como no concebimos el consumo de agua no potable en nuestros hogares, tampoco podemos tolerar accesos de comunicaciones que no sean seguros. Finalmente, el cambio hacia un entorno laboral más remoto y la desaparición progresiva de

las oficinas físicas plantean nuevos desafíos en términos de conectividad y seguridad. Los empleados que trabajan desde dispositivos móviles o computadoras corporativas necesitan acceder de manera remota a aplicaciones internas de la empresa, así como a servicios en la nube para llevar a cabo sus tareas diarias. En este contexto, es fundamental garantizar que estos trabajadores remotos dispongan de las mismas capacidades de conectividad y ciberseguridad que tendrían si estuvieran físicamente presentes en las oficinas de la empresa.

### **Uno de los sectores que más apuestan por sus soluciones es el industrial, ¿qué necesidades observan en este sector?**

Por un lado, el sector industrial demanda la aplicación de tecnologías de vanguardia que puedan integrarse de manera efectiva en sus procesos. Esto incluye soluciones como SD-WAN, inteligencia artificial y ciberseguridad, con un enfoque en la convergencia entre tecnologías de la información (IT) y operativas (OT). Por eso, es fundamental desarrollar productos y soluciones capaces de comprender los protocolos industriales, adaptándose a la complejidad y especificidades de los entornos de producción. Además, es necesario garantizar que estos productos funcionen de manera fiable en entornos industriales complejos, donde pueden surgir condiciones adversas o variables inesperadas.

## Antonio García Romero, CEO de Teldat

### **¿Qué futuro tiene Teldat? ¿Cuáles son las tendencias que más van a incidir en su negocio?**

El futuro de Teldat se proyecta en mantenerse a la vanguardia de las telecomunicaciones, manteniendo nuestro compromiso con la calidad y el servicio que ofrecemos a todos nuestros clientes. En este sentido, identificamos tres tendencias principales que incidirán significativamente en nuestro negocio. Para comenzar, la virtualización de las redes mediante tecnologías como SDN jugará un papel crucial. Esta tendencia nos llevará a apostar por el control e inteligencia de la red en todas las infraestructuras corporativas, proporcionando soluciones avanzadas para la gestión eficiente y flexible de los recursos de red. Otra tendencia dominante será la evolución hacia nuevos accesos de comunicación impulsados por la tecnología 5G y las capacidades de Open Gateway. Por último, la emergencia de la nueva generación de "ciudades inteligentes" representará una oportunidad importante para nuestro negocio. Estas ciudades estarán equipadas con nodos IoT (Internet of Things) y soluciones de automatización, lo que permitirá una gestión más eficiente y controlada de los servicios urbanos. En este contexto, Teldat se posicionará como un proveedor clave de infraestructura de comunicaciones para impulsar la conectividad y la eficiencia en estas ciudades del futuro.

Cibercotizante



**José Joaquín Flechoso**  
 Presidente de Cibercotizante

## La IA y los servicios públicos protagonistas del DES 2024

Málaga, una vez más se encuentra en el epicentro de la digitalización con la celebración del DES Digital Enterprise Show 2024. Paralelamente al evento, se celebró también el Digital Business World Congress, el mayor foro sobre digitalización que reunió a más de 550 expertos internacionales, que compartieron conocimientos en más de 375 sesiones. Este congreso trató de forma prioritaria el impacto de la IA generativa destacando por su importancia la parte dedicada al informe AI4Humanity, que es la base del informe que verá la luz en noviembre próximo en el seno de Naciones Unidas, con el fin de tener una modelo a seguir, más allá de las regulaciones legales pertinentes. Una vez más quedó plasmada la necesidad de apostar por el humanismo en la IA con un llamamiento de derive hacia un gran pacto mundial en busca del consenso sobre un uso razonable de esta tecnología.

Al respecto de este informe, una experta como Carme Artigas y Zondwa Mandela, nieto de Nelson Mandela ahondaron en algunos de los problemas capitales del uso de la IA para evitar que se convierta en arma de exclusión social. El informe evidencia que hay que evitar “el colonialismo de datos” que según Mandela es

la tónica generalizada, con el fin de contribuir y facilitar que África pueda tener acceso a los datos, las tecnologías y las soluciones digitales de IA, “en lugar de darles soluciones de forma paternalista” tal y como aludía.

La tecnología debe tener un coste adecuado para que los habitantes puedan acceder a ella sin discriminación alguna, pues en países como Sudáfrica, la tasa de desempleo es del 40%, una de las más altas del mundo y por tanto con una población escasa de recursos. La Mandela Legacy Foundation que lucha por la igualdad y los derechos humanos, vela para que la IA sirva como agente de transformación en el continente africano y se integre de modo global evitando las desigualdades. Es evidente que hay generar una tecnología equitativa e inclusiva para el bienestar social donde los datos de las economías del norte y del sur sean considerados por igual. Es necesario mitigar este sesgo, ver la tecnología como algo inclusivo.

Es primordial tener más regulación y atención a los objetivos finales del desarrollo tecnológico, evitando que puedan acrecentar las desigualdades.





# Furia<sup>3</sup> ROLLER

**60W**  
POTENCIA

 **IPX7**  
RESISTENTE AL AGUA

**1+1**  
  
TRUE WIRELESS

**BT**  
BLUETOOTH

*Freedom*  
**addicts**



Código QR para RA

Escanea este código QR con tu teléfono móvil para ver este producto en tu dispositivo y observarlo en tu entorno.

