



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



it Reseller
TECH · CONSULTING

ESCASEZ DE TALENTO TECNOLÓGICO,
el gran desafío del canal

it User
TECH & BUSINESS

LA NUBE,
¿el nuevo legacy de las empresas?

it Digital Security

CIBERSEGURIDAD,
la gran oportunidad en 2023



ENTREVISTA A RICARDO LABARGA, DELL TECHNOLOGIES



ENTREVISTA A RICARDO MATÉ, SOPHOS

it TRENDS



PRONÓSTICOS TECNOLÓGICOS Y FACTORES QUE INFLUIRÁN EN SU DESPLIEGUE



TENDENCIAS EN CIBERSEGURIDAD PARA 2023 Y LOS RETOS PARA EL CANAL, A DEBATE

Director

Pablo García Reales

pablo.garcia@itdmgroup.es

Redacción y colaboradores

Hilda Gómez, Arantxa Herranz, Reyes Alonso,

Ricardo Gómez, Alberto Varet

Diseño revistas digitales

Eva Herrero

Producción audiovisual

Miss Wallace, Alberto Varet

Fotografía

Fernando Gutiérrez

Director General

Juan Ramón Melara

juanramon.melara@itdmgroup.es

Director de Contenidos

Miguel Ángel Gómez

miguelangel.gomez@itdmgroup.es

Directora IT Events & Lead Gen Programs

Arancha Asenjo

arancha.asenjo@itdmgroup.es

Directora División Web

Bárbara Madariaga

barbara.madariaga@itdmgroup.es

Directora IT Digital Security

Desirée Rodríguez

desiree.rodriguez@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid

Tel. 91 601 52 92

UNA NUEVA ERA

Como cada año por estas fechas toca hacer balance y mirar al futuro trabajando con el ánimo de mejorar aún más nuestras propuestas.

Haciéndonos eco de la evolución que nos está demandando la industria a los medios especializados, en aras de superar estructuras editoriales ya anquilosadas, este mes de enero lanzamos una nueva y renovada revista mensual, bajo el nombre “IT Digital Magazine”, que consolida los contenidos de IT User, IT Reseller y IT Digital Security en una única publicación, dirigiéndose a una audiencia mucho más extensa. Los sitios web, canales sociales, newsletters, es decir, nuestras herramientas más pegadas a la actua-

lidad se mantienen como hasta ahora, con toda su carga de información especializada para el perfil de lector interesado, pero las revistas mensuales, en las que enmarcamos nuestros contenidos de contextualización y análisis en profundidad, se fusionan en esta nueva publicación mensual.

Este año 2023 es ya el octavo en la singladura que iniciamos en IT Digital Media Group allá por 2015. En todos estos años hemos trabajado duro para ocupar un hueco importante en el interés de todos aquellos ITDM (IT Decision Makers) que día a día navegáis por el proceloso mundo de la información en busca de los datos que os ayuden en la toma de decisiones más correcta. En esta aventura

hemos intentado ayudaros incorporando, a lo largo de nuestra existencia, foros de conversación y de debate, y damos un nuevo paso creando nuestros Encuentros ITMD (IT Digital Media Group). Os iremos informando en breve de ésta y otras novedades. De momento seguimos trabajando en un remozado porfolio de productos y servicios en el que estamos poniendo todo el esfuerzo, toda la experiencia y toda la energía que usted, nuestro lector, merece con creces.

De corazón, le deseamos un año repleto de éxitos personales y profesionales y le dejo con el número 1 de IT Digital Magazine. Espero que sea de su agrado. ■

JUAN RAMÓN MELARA, Director General

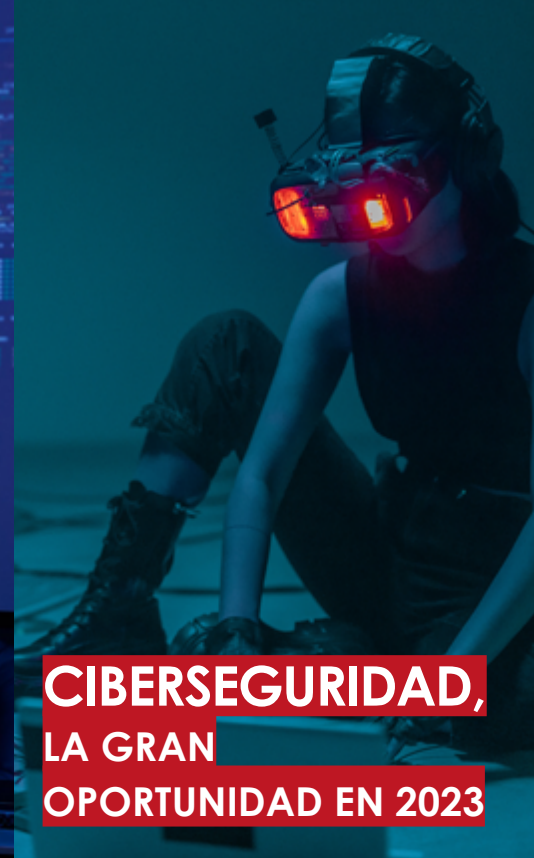




**LA NUBE,
¿EL NUEVO LEGACY
DE LAS EMPRESAS?**



**ESCASEZ DE
TALENTO
TECNOLÓGICO**



**CIBERSEGURIDAD,
LA GRAN
OPORTUNIDAD EN 2023**

ACTUALIDAD

- >> El entorno inflacionista dificultaría la contratación de talento TIC
- >> La intensa actividad legislativa digital en 2022
- >> España: uno de los países más avanzados en la adopción de la e-factura
- >> Schneider y SAP trabajarán en la integración de IT y OT en las fábricas

ENTREVISTAS



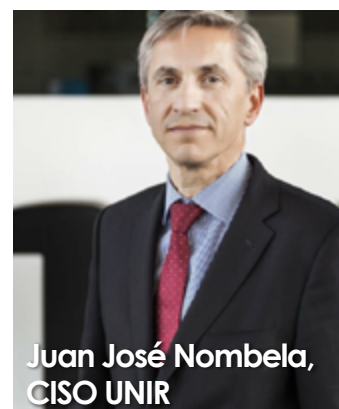
Ricardo Labarga,
Dell Technologies



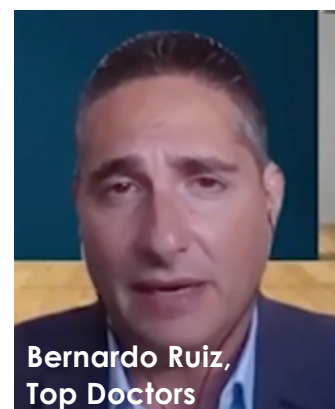
Julia White,
SAP



Ricardo Maté,
Sophos



Juan José Nombela,
CISO UNIR



Bernardo Ruiz,
Top Doctors

NO SOLO IT



WEBINAR

Tendencias tecnológicas 2023 y factores que influirán en su despliegue



DEBATE IT

Tendencias en Ciberseguridad para 2023 y los retos para el canal

TENDENCIAS

- >> España atraerá 5.000 millones de euros en inversiones para datacenters
- >> 2023, ¿un mal año para el Metaverso?
- >> 7 de cada 10 empresas de TI planean realizar fusiones y adquisiciones en 2023
- >> ¿Qué esperar de 2023 en términos de ciberseguridad?

ÍNDICE DE ANUNCIANTES

- >> ISE
- >> ESPRINET
- >> DMI
- >> SONICWALL
- >> HILLSTONE
- >> ARROW
- >> V-VALLEY
- >> IT WHITEPAPERS
- >> INFORME IT TRENDS
- >> TECNOLOGÍA Y EMPRESA

Transform

Business



Spaces



ISE es la feria líder mundial en integración audiovisual profesional. Descubre las tecnologías que crean entornos corporativos de excelencia mundial.

DESCUBRE MÁS!



Obtén tu **ENTRADA GRATUITA!**
Regístrate con el código: itreseller

iseurope.org

EL ENTORNO INFLACIONISTA PODRÍA DIFICULTAR MÁS LA CONTRATACIÓN DE TALENTO TIC

La inflación y la necesidad de contener los costes salariales tensionan la gestión del talento en las organizaciones en un contexto de escasez de conocimientos técnicos. Este es un problema especialmente crítico en el caso de los perfiles de base tecnológica, ya que los profesionales digitales y cualificados representan el 70% de los perfiles demandados en España.

➤ REYES ALONSO

“Las compañías españolas se encuentran en una auténtica encrucijada: atraer y retener el talento necesario para poder cumplir con sus planes de crecimiento en un entorno marcado por el fuerte crecimiento de la inflación y la necesidad de contener los costes salariales”, afirma Amaia Otaola, socia de People & Organisation

en PwC, como conclusión de un informe que acaba de presentar la firma sobre el impacto de la inflación de la gestión del talento, a partir de una encuesta realizada a 53 grandes empresas españolas.

[Según este análisis](#), la inflación tensiona la gestión del talento de las grandes compañías, que están viendo cómo se incrementan sus costes



salariales en un contexto marcado por la escasez de talento y la falta de perfiles de base tecnológica.

SEGUIR SIENDO UNA OPCIÓN ATRACTIVA PARA EL TALENTO

En este contexto, tienen que tomar medidas para seguir siendo atractivas como empleadoras. El estudio revela que las empresas están apostando, por un lado, por aplicar subidas salariales moderadas en 2023 para compensar parte de la pérdida de poder adquisitivo de sus empleados como consecuencia del tirón de la inflación. El 63% de las compañías encuestadas tienen previsto incrementar el salario base de sus profesionales por debajo del 4% (el 40% entre el 3% y el 4%) y sólo el 34% espera aplicar subidas medias por encima de esta cifra. Por otro, están poniendo en marcha un mix de iniciativas que pasan por potenciar las promociones internas (60%), retocar sus paquetes retributivos (57%), mejorar las iniciativas relacionadas con el bienestar y la experiencia de sus empleados en la compañía -el 40% de las empresas encuestadas van a desarrollar, al menos, tres iniciativas en este ámbito-, y reforzar sus planes de formación para impulsar las capacidades de sus empleados en áreas clave (51%).

PROFESIONALES DE BASE TECNOLÓGICA

El estudio muestra que el 70% de los perfiles que se demandan en el mercado laboral español son profesionales digitales y cualificados. Concretamente, el 63% de las compañías entrevistadas está buscando perfiles de base tecnológica y el 51% cualificados para frenar la rotación no deseada de sus plantillas. De hecho, cuando se les pregunta a las empresas de la muestra sobre cuáles son los cuatro grandes desafíos a los que se enfrentan en la actualidad, el 66% asegura que la falta de candidatos externos. Muy por delante de la negociación salarial (31%) o de la poca agilidad en la contratación (26%). De cara a abordar el déficit de capacidades en sus plantillas, el de-

sarrollo interno del talento y su impulso se imponen a la búsqueda en el mercado laboral, según el 66% de los encuestados

El informe también confirma que el tirón de la inflación no sólo está dificultando la gestión del talento, sino que, además, está presionando al alza los costes de personal de las compañías, que están pisando el acelerador de la tecnología para mejorar su productividad y su eficiencia y compensar así el incremento de los precios. El 66% de las empresas encuestadas en el estudio, por ejemplo, prevén incrementar la automatización de los procesos en sus organizaciones y el 26% reasignar a personas y equipos para ganar en eficiencia. Otras medidas de mejora de la productivi-

dad pasan por reforzar la gestión del desempeño (57%) e invertir en nuevas tecnologías (46%).

Finalmente, una inmensa mayoría, cercana al 80% de la muestra, no se plantea tomar ningún tipo de medida de carácter colectivo en un futuro cercano, y las pocas que están estudiando hacerlo se refieren a bajas incentivadas, principalmente.

¿HACIA DÓNDE VA EL PUESTO DE TRABAJO?

Los próximos cinco años marcarán un periodo de cambio evidente tanto en la mecánica como en las actitudes sociales que rodean a las prácticas de trabajo, según IDC. Sus expertos sostienen que los actuales retos económicos, climáticos y empresariales exigen que los trabajadores formen parte de equipos dinámicos y reconfigurables.

El trabajo híbrido, que en su día se pensó que era un algo temporal para permitir a las empresas continuar con sus operaciones comerciales durante la pandemia, se ha convertido en un pilar de nuestro futuro panorama laboral global. Esa es la transición que están llevando a cabo las empresas, si bien, en opinión de sus analistas, el futuro del trabajo está plagado de mu-



chas incógnitas, desde dónde y cómo se hará el trabajo hasta cómo van a impactar las presiones económicas en las oportunidades de trabajo.

En este sentido, la investigación destaca que los retos actuales en materia económica, climática y empresarial exige que los trabajadores formen parte de equipos dinámicos y reconfigurables que puedan adaptarse rápidamente a las necesidades de las organizaciones y a los nuevos requisitos del mercado, en cualquier momento, en cualquier lugar y desde cualquier ubicación física.

ATRAER Y RETENER TALENTO

A partir de estas reflexiones y con la premisa de que el futuro pasa claramente por modelos de trabajo híbridos, que permitirán mejora en la adquisición de talento, la retención de empleados y la satisfacción del cliente, IDC ha esbozado sus predicciones sobre el futuro del trabajo.

La primera es que el 30% de las organizaciones de la lista G2000, que aglutina a las 2.000 mayores compañías privadas del mundo, adoptarán servicios de videoconferencia inmersiva en el metaverso para impulsar políticas de sostenibilidad y de salud de las plantillas.

LOS PRÓXIMOS CINCO AÑOS MARCARÁN UN PERIODO DE CAMBIO EVIDENTE TANTO EN LA MECÁNICA COMO EN LAS ACTITUDES SOCIALES QUE RODEAN A LAS PRÁCTICAS DE TRABAJO, SEGÚN IDC

En segundo lugar cree que, en 2024, el papel del desarrollador será ubicuo, con más del 60% de las empresas formando y apoyando a los usuarios empresariales para que creen sus propias aplicaciones y procesos automatizados utilizando herramientas de bajo código.

Por otro lado, debido a la escasez de personal cualificado, los directores de TI que inviertan en plataformas de adopción digital y tecnologías de aprendizaje automatizado conseguirán un aumento de la productividad del 40% en 2025, lo que permitirá una mayor rapidez en la adquisición de conocimientos especializados.

La cuarta predicción nos traslada de nuevo a 2024, fecha en la que, según IDC, las empresas que hayan desplegado medidas de microvigilancia de los empleados (cámara/teclado) verán una disminución del 20% en la productividad real de los empleados. También en

2024, a las empresas de la lista G2000 que hayan puesto en marcha modelos de trabajo híbridos reactivos y tácticos les advierte que perderán un 20% de sus ingresos del 20% en 2024 debido al desgaste laboral y al bajo rendimiento de los equipos.

POLÍTICAS DE SEGURIDAD HÍBRIDAS

La sexta predicción es que, en 2025, las organizaciones que hayan creado políticas de seguridad híbrida dedicadas y desarrollado una cultura de confianza tendrán tres veces menos probabilidades de sufrir una brecha de seguridad.

Asegura IDC en su séptima predicción que, en 2024, las empresas que ofrezcan a los trabajadores de primera línea un acceso democratizado a la colaboración digital, la automatización de procesos y herramientas similares experimentarán un aumento del 20% en sus ingresos debido a la mejora de la productividad.

También sostiene que la analítica holística e integrada dentro de un ecosistema de espacio de trabajo digital inteligente impulsará un aumento del 70% en los resultados empresariales. Esto lo fecha en 2026.

La penúltima predicción es que, al difuminarse el espacio y el lugar, en 2025 el 65% de las empresas de la lista G2000 considerarán que la presencia online de sus empleados es equiparable a la física.

Finalmente, la firma de análisis señala que, en 2024, el 55% de los equipos directivos de las empresas utilizarán la tecnología de planificación inteligente del espacio y la capacidad para reinventar las ubicaciones de las oficinas para reunirse, colaborar y aprender. ■

MÁS INFO +

» [Impacto de la inflación en la gestión de personas](#)



COMPARTIR EN REDES SOCIALES

LEY DE INTELIGENCIA ARTIFICIAL, DE STARTUPS O LA DE SERVICIOS DIGITALES, LA INTENSA ACTIVIDAD LEGISLATIVA DE 2022

2022 ha tenido una intensa actividad legislativa. Tanto desde la Unión Europea, como desde el Gobierno de España, se han aprobado numerosas leyes que buscan modernizar el tejido empresarial para adaptarlo a la nueva realidad digital. Repasamos cuáles han sido las principales leyes aprobadas en este año recién concluido.

2022 será recordado, además de por acontecimientos como la Guerra de Ucrania, la incertidumbre económica o la compra de Twitter, por la intensa actividad legislativa que se ha llevado a cabo tanto desde la Unión Europea como desde España, con el fin de impulsar el ecosistema digital. Repasamos algunas de las leyes más importantes que se han aprobado en los últimos doce meses.

LEY DE SERVICIOS DIGITALES

Aunque no empezará a aplicarse hasta mayo de 2023, el pasado mes de noviembre entró en vigor la nue-

va Ley de Servicios Digitales, la cual plantea obligaciones a las empresas consideradas como 'gatekeepers' o guardianes de acceso en el entorno digital para que no desarrollen comportamientos que puedan limitar la competencia de compañías de menor tamaño. El reglamento impone una serie de obligaciones para garantizar unos mercados digitales equitativos y abiertos, y no penalizar la innovación de empresas más pequeñas a través de prácticas desleales, como favorecer sus propios servicios o impedir que los usuarios profesionales de sus servicios lleguen a los consumidores.

LEY DE INTELIGENCIA ARTIFICIAL

El pasado mes de abril, la UE propuso oficialmente la Ley de Inteligencia Artificial, en la que se describe la capacidad de supervisar, regular y prohibir los usos de la tecnología de aprendizaje automático. El objetivo, según la UE, es invertir y acelerar el uso de la IA en la Unión, impulsando la economía al tiempo que se garantiza la coherencia, se abordan los desafíos globales y se establece la confianza con los usuarios humanos. La Ley clasifica los casos de uso de la IA en tres niveles: riesgo inaceptable, riesgo alto y riesgo bajo o mínimo,

➤ BÁRBARA MADARIAGA



así como para fomentar su desarrollo y la implantación de la IA, especialmente en las PYMES y las Administraciones públicas.

DIRECTIVAS DE CIBERSEGURIDAD

El Diario Oficial de la Unión Europea (DOUE) publicó, el 27 de diciembre, la nueva normativa sobre resiliencia de las entidades críticas que busca incrementar la protección de aquellas organizaciones que prestan servicios esenciales y que son consideradas cruciales para el mantenimiento de funciones sociales vitales, las actividades económicas, la salud y la seguridad públicas y el medio ambiente. Esta directiva forma parte de un paquete legislativo, junto con otras dos normas que también se publicaron a la par: la Directiva (UE) 2022/2555 (NIS2), que sienta las bases para las medidas de gestión de riesgos de ciberseguridad (los países de la UE tendrán que adoptar estrategias nacionales designar a autoridades competentes de gestión de crisis) y la obligación de notificación en los sectores que cubre (energía, transporte, sanidad e infraestructura digital); y el Reglamento (UE) 2022/2554 (DORA), que establece requisitos uniformes para la seguridad de las redes y siste-

AUNQUE NO EMPEZARÁ A APLICARSE HASTA MAYO DE 2023, LA NUEVA LEY DE SERVICIOS DIGITALES IMPONE UNA SERIE DE OBLIGACIONES PARA GARANTIZAR UNOS MERCADOS DIGITALES EQUITATIVOS Y ABIERTOS

mas de información de las empresas y organizaciones que operan en el sector financiero, así como de terceros esenciales que les presten servicios relacionados con las TIC, como plataformas en la nube o servicios de análisis de datos.

LEY DE CHIPS

La ley europea de chips ve la luz con el objetivo de reforzar la competitividad y la resiliencia de Europa y ayudará a lograr la transición digital y ecológica y, según anunció la Comisión Europea, “traerá un sector de semiconductores próspero desde la investigación hasta la producción y una cadena de suministro resistente. Movilizará más de 43 000 millones de euros de inversiones públicas y privadas y establecerá medidas para prevenir, preparar, anticipar y responder rápidamente a cualquier interrupción futura de las cadenas de suministro, junto con los Estados miembros y nuestros socios interna-

cionales”. Además, también garantizará que la UE disponga de las herramientas, habilidades y capacidades tecnológicas necesarias para convertirse en líder en este campo más allá de la investigación y la tecnología en el diseño, la fabricación y el empaquetado de chips avanzados, para asegurar su suministro de semiconductores y reducir sus dependencias.

LEY DE TELECOMUNICACIONES

La Ley General de Telecomunicaciones (LGTel) fue aprobada el mes de junio en el Congreso de los Diputados. Con ella queda transpuesto al ordenamiento jurídico español el Código Europeo de Comunicaciones Electrónicas, de diciembre de 2018. La normativa tiene como objetivo regular las telecomunicaciones, y comprende “la instalación y explotación de las redes de comunicaciones electrónicas, la prestación de los servicios de comunicaciones electrónicas, sus recursos

y servicios asociados, los equipos radioeléctricos y los equipos terminales de telecomunicación”.

LEY DE STARTUPS

El Congreso de los Diputados aprobó, a principios de diciembre y de forma definitiva, la Ley de Fomento del Ecosistema de Empresas Emergentes, que (más conocida como Ley de Startups), cerrando así el trámite parlamentario que se inició en julio de 2021. Con la Ley de Startups, se pretende estimular la inversión y la atracción de talento, favorecer la colaboración entre pymes, grandes compañías y empresas emergentes, impulsar la I+D+i, también en la Administración, y fomentar la cooperación de las empresas emergentes y los emprendedores con las Universidades y centros de investigación.

PROGRAMA RETECH

Según aseguró en julio, la vicepresidenta primera del Gobierno y ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño, el Gobierno va a destinar 530 millones de euros al programa RETECH entre 2022-2023 para poner en marcha “una red de proyectos estratégicos emblemáticos transformadores

en el área digital propuestos por las Comunidades Autónomas". Con esta inversión se impulsarán, según el Ministerio, proyectos con un alto impacto territorial y económico en ámbitos como el de inteligencia artificial, los gemelos digitales como las soluciones tecnológicas de simulación virtual de objetos y sistemas; tecnologías "verdes por diseño" (GreenTech), ciberseguridad, redes de emprendimiento digital, e iniciativas de digitalización en entornos rurales y despoblados (RuralTech), de la industria de la moda y el textil (FashionTech) y de la Salud Digital.

PERTES

Aunque no son leyes, los PERTES han sido otra de las iniciativas gubernamentales de este 2022. El Gobierno de España aprobó en mayo el PERTE de microelectrónica y semiconductores, con el que movilizará una inversión pública de 12.250 millones de euros hasta 2027. El proyecto tiene como objetivo desarrollar las capacidades de diseño y producción de la industria de la microelectrónica y los semiconductores en España y favorecer la autonomía estratégica nacional y de la UE en este sector, en línea con lo previsto en la Ley Europea

de Chips de la Comisión Europea. Además de este PERTE, el Ejecutivo español también aprobó el PERTE del vehículo eléctrico y conectado, que movilizará una inversión de 11.855 millones de euros a través de 487 proyectos en los que participarán 327 empresas; o el de las industrias agroalimentaria y naval, que está dotado en conjunto con más de 700 millones de euros. ■

MÁS INFO +

- » [NIS2 y DORA, las normativas que refuerzan la ciberseguridad y la resiliencia en la UE](#)
- » [La Ley de Startups](#)
- » [Europa afronta el futuro digital impulsando la industria de semiconductores](#)
- » [Ley de Mercados Digitales de la UE](#)



COMPARTIR EN REDES SOCIALES



ESPAÑA ES UNO DE LOS PAÍSES MÁS AVANZADOS EN LA ADOPCIÓN DE LA E-FACTURA

Una de las principales ventajas de la factura electrónica para las compañías es la reducción de las cargas administrativas, ya que facilita las tareas diarias de los departamentos de administración y contabilidad. En 2025 su uso será de obligado cumplimiento para cualquier tipo de compañía en España, independientemente del tamaño y sector.

La adopción de la factura electrónica avanza a pasos agigantados en Europa. En este contexto, la Unión Europea busca en la facturación electrónica una herramienta que permita a las autoridades controlar la actividad en tiempo real, adoptar medidas sin demora en función del contexto económico y normalizar el tratamiento de las transacciones nacionales y europeas.

En 2019, la UE perdió 134.000 millones de euros en ingresos por IVA, según el informe “Brecha del IVA” de la Comisión Europea del 2022. Entre las principales causas se encuentran las quiebras, insolvencia o los errores de información además del fraude, que en sí mismo cuesta a los países europeos entre 40.000 y 60.000 millones de euros cada año. La e-factura es



vista como una medida eficiente para optimizar el control y seguimiento de la administración, con el fin de mejorar las declaraciones para limitar el fraude fiscal.

En cuanto a las compañías europeas, una de las principales ventajas de la e-factura es la reducción de las cargas administrativas, ya que facilita las tareas diarias de los departamentos de administración y contabilidad. A través de la tecnología, se puede automatizar el envío y recepción de las facturas, conciliar las facturas recibidas con las mercancías recibidas y las órdenes de compra o validar las facturas, de forma rápida, libre de errores humanos y con una mayor eficacia para optimizar, de esta manera, el tiempo.

“Para las empresas, la generalización de la facturación electrónica puede representar un reto importante debido a sus limitaciones técnicas y organizativas. Sin embargo, debe verse sobre todo como una fuente de oportunidades a escala nacional, europea y quizás pronto mundial, dados los numerosos beneficios que aporta a nivel organizativo y administrativo”, apunta Diana Salazar, B2B Integration Sales Manager de Generix Group.

IMPLANTACIÓN POR FASES

La obligación de implementar la factura electrónica se está extendiendo progresivamente a las transacciones B2B. Los Estados miembros de la UE disponen de cierta flexibilidad en cuanto a la implantación de la facturación electrónica tanto con los agentes públicos (B2G) como con los privados (B2B). Por ello, no todos los países se encuentran en la misma fase. En el caso de España, es uno de los países europeos más avanzados en la carrera por implantar la facturación electrónica.

El 29 de septiembre se publicó en el BOE, la Ley 18/2022 de Creación y Crecimiento de Empresas que registra la obligatoriedad de la adopción de la factura electrónica en España, una obligación que se extiende con independencia del sector en el que se desarrolle la actividad. Esta legislación busca mejorar las relaciones entre las empresas y los proveedores para reducir los impagos y el índice de morosidad y que recoge una demanda histórica de los empresarios españoles ya que facilita el emprendimiento y la creación de empresas.

Esta Ley recoge la obligatoriedad de utilizar la facturación electrónica



y que entrará en vigor en dos fases. Por un lado, las empresas y autónomos con una facturación anual superior a 8 millones de euros tendrán la obligación de aplicar esta medida en el plazo máximo de un año desde que se apruebe el desarrollo reglamentario (a partir de mediados de 2023). Por otro lado, el resto de las empresas cuya facturación anual sea inferior a 8 millones de euros tendrán que aplicar esta medida en un plazo de dos años, es decir, en 2025 será de obligado cumplimiento para cualquier tipo de compañía en España, independientemente del tamaño y sector. ■

MÁS INFO +

- » [“La nueva Ley Antifraude incidirá en todos los sistemas informáticos de facturación”: Daniel Cala \(Wolters Kluwer\)](#)
- » [La factura electrónica gana impulso entre las pymes con la Ley Crea y Crece](#)



COMPARTIR EN REDES SOCIALES

SCHNEIDER ELECTRIC Y SAP TRABAJARÁN EN LA INTEGRACIÓN DE IT Y OT EN LAS FÁBRICAS

Ambas compañías han alcanzado una colaboración estratégica con estándares comunes para simplificar la incorporación y la gestión del ciclo de vida de los activos con gemelos digitales y con realidad virtual y aumentada. El resultado son soluciones end-to-end preconfiguradas para reducir los costes y facilitar la implementación y las operaciones.

Schneider Electric y SAP han firmado una colaboración para trabajar conjuntamente en la integración de IT/OT. Ambas buscan encontrar oportunidades de mejora en la innovación de la industria y la transformación digital, impulsar estándares abiertos y fomentar una estrecha integración de las tecnologías ITy OT, lo que supondrá una ventaja para los clientes industriales.

“Nuestra colaboración con Schneider Electric demuestra el apoyo general de SAP al ecosistema de la

Industria 4.0”, explica Peter Maier, presidente de Industrias y Asesoría de Clientes de SAP. “Nuestras empresas están alineadas en la importancia de la colaboración, la innovación y los estándares abiertos, haciendo que las soluciones integradas de información y tecnología operativa sean fáciles de consumir para nuestros clientes conjuntos”.

SOLUCIONES INNOVADORAS

Schneider Electric y SAP quieren validar escenarios con sus ofertas complementarias, para proporcionar así una integración fácil y continua a los clientes industriales en común, además de abordar una futura colaboración en sostenibilidad y gestión de la energía. Tratarán de ofrecer más valor a los clientes a través de soluciones end-to-end preconfiguradas y testeadas para reducir los costes de implementación y de operación, de los procesos de negocio de misión crítica.

Los primeros escenarios serán los de integración simplificada de OT/IT en las fábricas, basada en estándares comunes, onboarding y gestión del ciclo de vida de los activos como gemelos digitales; y gestión inteligente end-to-end de activos y servicios mediante tecnologías de realidad virtual y aumentada.

Por ejemplo, garantizar la conectividad OT/IT end-to-end permite tomar decisiones basada en datos y mejorar las estrategias de rendimiento. Las soluciones que activan automáticamente las órdenes de mantenimiento o servicio en las aplicaciones de SAP pueden cerrar el bucle entre la estrategia de mantenimiento y la ejecución, para un mantenimiento óptimo de los activos. Y la realidad aumentada puede dar a los usuarios la información correcta en el momento y lugar adecuados, para reducir el tiempo y aumentar la precisión a la hora de analizar las causas.

“Muchos de nuestros clientes están buscando formas más fáciles de integrar tecnologías avanzadas en su camino hacia la digitalización”, afirma Bruno Zerbib, EVP, Chief Platform and Technology Officer de Schneider Electric. “Con SAP, estamos comprometidos a abordar los retos del mercado con soluciones digitales innovadoras para ayudar a estos clientes a aprovechar los beneficios de la Industria 4.0”. ■

MÁS INFO +

» [Schneider Electric lanza nuevos productos para partners del sector energético](#)



COMPARTIR EN REDES SOCIALES

TECHMOCRACY

Creemos en la Democracia Tecnológica. Estamos al lado de las empresas para ayudarlas a lograr su transformación digital de una manera más rápida, eficiente, barata, flexible y sostenible.

RENTING DE SOLUCIONES TECNOLÓGICAS
El alquiler de larga duración del parque informático con más servicios y ventajas.



Sin
inmovilizado
de capital



Flexibilidad
del parque
tecnológicos



Tecnología
siempre
actualizada



Reciclaje
según
la Ley



Descubre más en
www.esprinet.com/es/esprinet/
o consulta con tu distribuidor de
confianza

#ENTREVISTA

“La gran debilidad de la economía son aquellas empresas que no se han digitalizado”

RICARDO LABARGA,
DIRECTOR GENERAL DE DELL TECHNOLOGIES EN ESPAÑA

➤ ARANCHA ASENJO

De “riesgo de supervivencia” califica Ricardo Labarga la falta de digitalización de las empresas, si bien, el director general de Dell Technologies en España apunta que hay un cambio de tendencia aupado por la mayor proximidad de los directivos de TI a los comités de dirección y un mejor entendimiento por parte de estos de las consecuencias que no digitalizarse puede acarrear.

ITDM >> Enero 2023



A caba de terminar 2022. ¿Cómo ha sido el resultado de la compañía a nivel mundial y global?

Nuestro cuarto trimestre acaba a finales de enero, por lo tanto, todavía no hay datos. Las cifras de la primera mitad del año fueron muy buenos, tanto en crecimiento como en rentabilidad. En el tercer trimestre, hubo un decrecimiento en la parte de ingresos, pero crecimiento en la parte de beneficio, que proviene de una descompensación o de una cierta paralización en el mercado del puesto de trabajo. Hemos visto caer el número de unidades en puestos de trabajo y, sin embargo, tuvimos un crecimiento excepcional en toda la parte Enterprise: servidores, almacenamiento, networking, servicios de ciberseguridad, que son proyectos de enorme calado en todas las compañías y que aportan un mayor margen. Esperamos en Q4 seguir esa tendencia de Q3.

Veníamos de un tiempo de pandemia donde se reforzaron las compras alrededor del puesto de trabajo. ¿Qué va a pasar ahora con esas políticas? ¿Habrá muchas empresas como Twitter que ya no quieran que sus empleados teletrabajen?

“ EL ACUERDO FIRMADO CON VMWARE CONTEMPLA QUE LA COLABORACIÓN EN I+D Y EL DESARROLLO DE PRODUCTOS CONJUNTOS SE MANTENGA DURANTE AL MENOS CINCO AÑOS. LA RELACIÓN SEGUIRÁ SIENDO EXCELENTE ”

RICARDO LABARGA,
director general de
Dell Technologies en España

El caso de Twitter es una excepción. Es verdad que hay una cierta vuelta a la oficina y todos estamos trabajando allí algunos días. Hemos aprendido a trabajar en un formato híbrido. Todas las empresas están profundizando en el teletrabajo por tres razones. Una es la productividad, no hemos visto reducciones con el teletrabajo. La segunda es la conectividad: necesito estar conectado con la compañía,

estar bien conectado, tener un medio que sea seguro y fiable, estar cómodo. Y hay un tercer punto, que es el de la empatía y es que tenemos que seguir midiendo resultados no por la presencia o telepresencia. Tratamos de mejorar esa relación entre lo que es el mundo del trabajo y el mundo de la vida personal. ¿Qué compañía no quiere que los tres entornos crezcan? La gran mayoría de los miembros de nuestros equipos eso lo perciben como algo positivo. Incluso, las nuevas generaciones perciben lo contrario como algo tan negativo como para dejar de irse o para dejar una compañía y moverse a otra, o directamente para no entrar en la compañía.

Si tuviera que hacer un análisis DAFO (debilidades, amenazas, fortalezas y oportunidades) sobre el estado de la digitalización de las empresas en España, ¿qué destacaría?

La gran debilidad son aquellas empresas que no se han digitalizado o las que no se lo han tomado como una prioridad y no están yendo a la velocidad requerida. Es un riesgo de supervivencia. Según Boston Consulting Group, las empresas que van retrasadas en su digitalización valen significativamente menos que aquellas que

van rápido (0,68 vs 1,5). En ese grupo de las que valen un poco más de la mitad de lo que valían hacía tres años, habrá empresas que puedan tender a desaparecer o que tengan riesgo de desaparición porque no se han adaptado y son menos competitivas en un mercado en el que la digitalización hoy es un valor añadido. En resumen, la digitalización es realmente un elemento de competitividad.

Luego, tenemos una amenaza clarísima, que es la formación y el talento; el talento digital. Falta todavía una adecuación entre la formación universitaria y lo que requieren las empresas. No están saliendo suficientes tecnólogos, personas con conocimientos, con intereses, con las habilidades de tecnología que el mercado requiere. Y el mercado no es solo el de las empresas de tecnología sino cualquier empresa, pues hemos dicho que la tecnología es un elemento diferencial de competitividad.

Desde el punto de vista de oportunidades, la más clara es estar más cerca de los comités de dirección y de los procesos de decisión, bien por la vía de la competitividad o bien por la vía del riesgo, de la parte de los ciberataques y de la ciberseguridad. Es una enorme oportunidad de acer-

carse y hacerse entender por aquellos que anteriormente solo entendían el P&L. Ahora entienden el P&L, entienden el valor de la acción, pero ese valor de la acción y ese profit & loss está también muy dirigido por su capacidad de resistencia ante un ciberataque o por competir como consecuencia de disponer de las herramientas tecnológicas.

Y en cuanto a las fortalezas, el sector tecnológico está muy establecido, con compañías de peso, que tienen una capacidad financiera y una capacidad de resistencia ante el cambio para mantenerse. Y por tanto no es un sector que pueda desaparecer, está en crecimiento. Puede que tenga baches, momentos puntuales como que la demanda de puestos de trabajo durante dos trimestres o durante un año sea menor que la del año anterior porque pasó una circunstancia un poco específica, pero no quiere decir que la tendencia sea así. Es un sector siempre en crecimiento.

¿Y si este mismo análisis se aplicara a la propia Dell Technologies?

No veo grandes debilidades. La debilidad, evidentemente, puede provenir más de las amenazas, no de una debilidad intrínseca. Somos una



ENTREVISTA >> ¿CÓMO PERCIBE DELL TECHNOLOGIES EL AÑO 2023?

compañía que trabaja en los distintos entornos, en la parte de cliente, en la parte de Enterprise, en servidores, almacenamiento, networking... Somos capaces de dar soluciones completas y eso nos da una fortaleza enorme frente al resto de compañías que trabajan más en nichos de mercado. Esa fortaleza nos viene de dos lados. Uno es el cliente, que tiene una percepción nuestra de partner tecnológico. No rehuimos ninguna conversación. Cualquier preocupación o interés de nuestros clientes, al menos tenemos una opinión y tenemos una solución. No quiere decir que vaya a escoger

siempre la nuestra, pero tenemos una opinión y una solución para aportarle y eso es bueno porque tiene a alguien a quien puede preguntar. También quiero destacar nuestro I+D, muy potente, de 2,6 billones de dólares en el último año puramente en la parte de infraestructura. Es un I+D cruzado, que se retroalimenta: lo que he hecho en la parte de servidores, lo aprovecho en la parte de almacenamiento, lo de almacenamiento lo aprovecho en los servidores y también en la parte de networking. Todo este conglomerado de soluciones que atacan todos los entornos tecnológicos, salvo

la impresión, es una enorme fortaleza. La oportunidad, evidentemente, es seguir creciendo apoyándonos en esa fortaleza, más de lo que crece el sector. Es ser el mejor en cada uno de los segmentos en los que operamos, lo que significaría que nuestros clientes confían en nosotros.

En cuanto a las amenazas, tenemos las mismas que la economía mundial, además de las amenazas que ya hemos hablado y el tema de la falta de perfiles que es más de mercado y no específico nuestro.

Vuelve a salir el tema del talento, ¿cómo están abordando esta problemática de captación, pero también de retención de personal?

Somos una compañía muy abierta, que tratamos de predicar con el ejemplo. Recomendamos el trabajo híbrido; un trabajo en el que la gente esté conectada, que exista empatía, que todo esto lleve a la persona a ser más productiva. Así pues, todos en Dell tenemos la capacidad de teletrabajar. No tenemos un número de días en los que tengo que ir a la oficina, ni hora ni cómo. Cada grupo o equipo lo decide con sus líderes. Aquí hay una parte de flexibilidad enorme y es una forma de retener

talento y de atraer también. También tenemos lo que llamamos Referral Program, un programa de referencias en el que alguien con talento dentro de la compañía llama a un amigo suyo que también tiene talento y que puede adaptarse bien a la compañía. Funciona muy bien. Una segunda forma de enganchar al proyecto de Dell, además del mensaje de compañía con capacidad de crecimiento y buenos resultados, es la Responsabilidad Social Corporativa con proyectos muy bonitos. Cada uno de nosotros podemos poner nuestro granito de arena en los ERG (Employee Resource Groups), grupos de empleados que se unen en torno a un tema común, como puede ser el planeta, colectivos, buscar la conexión de las personas o ayuda a la comunidad. Son actividades extraescolares, que nadie te obliga a hacer. En España, cerca del 50% de los empleados pertenece a dos ERG. Y eso une mucho. Ayuda, evidentemente en los objetivos 2030, también a la RSC, pero tú ves que tu propia involucración está ayudando a la mejora de la sociedad. Esos proyectos también están atrayendo y reteniendo a muchos miembros de nuestro equipo, aunque a lo mejor tuvieran una oferta externa

“ PARA CUALQUIER PREOCUPACIÓN O INTERÉS DE NUESTROS CLIENTES, AL MENOS TENEMOS UNA OPINIÓN Y UNA SOLUCIÓN ”

mejor. Pero ven que Dell les aporta otros valores.

Uno de los habilitadores de la digitalización es la nube, con una clara tendencia al multicloud. En este contexto, las alianzas con otros proveedores y la generación de ecosistemas son muy importantes. ¿Cómo está trabajando Dell Technologies en este sentido?

Nosotros llevamos muchos años predicando el mundo del multicloud. Primero lo llamamos cloud híbrida y luego dimos el salto al multicloud. Los clientes ven que cada cloud pública les aporta unas ventajas que las otras no les aporta o que les aportan más una sobre otra. Y, además, esas ventajas no siempre tienen que ser estables en el tiempo: hoy me las aporta una nube y dentro de un año, otra. No me quiero casar sólo con una cloud pú-



blica. Hay que estar bien enterado de qué es lo que está pasando en cada una de las nubes públicas.

Además de eso, quiero saber también cuáles son las cargas de trabajo idóneas para mi cloud privada. Cada vez se está analizando más el coste-beneficio de una cloud privada frente a las públicas. Y cada vez estoy analizando más qué cloud pública es idónea para qué carga de trabajo. El trabajo de decisión de qué dejo en mi cloud privada, cómo hago crecer mi nube privada y qué llevo a la cloud

pública, y a cuál, no es una tarea baladí ni sencilla. Tengo que simplificar. Y ahí es donde estamos trabajando nosotros, en tener acuerdos con todas o con las principales nubes públicas del mercado, para que sea cual sea la decisión que tome el cliente de a qué cloud pública llevo el backup, por ejemplo, ese backup lo pueda seguir haciendo igual que lo hace en su cloud privada si es un cliente de Dell. Eso implica que los proveedores de cloud pública utilizan sistemas de Dell para facilitar a sus clientes que puedan migrar, compartir y facilitarles el trabajo colaborativo entre una cloud y otra, rompiendo los silos. Al principio cuando hablábamos de cloud híbrida era híbrida, sí, pero eran dos mundos separados, no había comunicación entre las dos. Las cargas en cada una de ellas se podían gestionar de diferentes formas. Ahora estamos llegando a acuerdos de colaboración, con VMware, AWS, Microsoft, Google, Red Hat o Wind River, expandiendo así ese ecosistema de multicloud y dando esa capacidad de gestionar mi cloud privada y las públicas donde tengo cargas de la misma forma. Le estoy dando una capa por encima que facilita la administración de una sola forma y no en función de dónde coloco la carga.

Al hilo de esa mención de VMware, en 2023 se aprobará su compra por parte de Broadcom y dejará de ser parte de Dell. ¿Cómo seguirán relacionándose con ellos?

De forma muy positiva. Michael Dell dejó cerrado, cuando era presidente de las dos compañías antes de iniciar la transacción con Broadcom, un acuerdo de colaboración técnico y comercial durante cinco años. En la parte comercial, seguiremos siendo uno de los principales mayoristas, o el principal, de VMware. Y en la parte técnica, si miras las cifras del mercado, somos el número 1 en hiperconvergencia según IDC. Esa posición nos la ha dado un producto desarrollado conjuntamente con VMware, VxRail. El acuerdo firmado contempla que la colaboración en I+D y el desarrollo de productos conjuntos se mantenga durante al menos los próximos cinco años desde que se cierre la transacción. Y eso es muy positivo para ambas compañías. La relación seguirá siendo excelente.

Además del cambio en las relaciones con otros proveedores, también están mutando los modelos de venta. Dell lanzó hace dos años el proyecto APEX, que comercializa la TI en forma de

“SOMOS FLEXIBLES Y CAPACES DE ANALIZAR CUALQUIER PROPUESTA QUE TENGA UN CLIENTE”

servicio. ¿Cómo se está implantando ese modelo en España?

Efectivamente, este modelo se lanzó hace un par de años en Estados Unidos y progresivamente se va incrementando el número de propuestas en APEX, para llegar a un final donde cualquiera de los productos, soluciones o servicios de la compañía se pueda pagar como un servicio, con la capacidad de escalada hacia arriba, pero también de escalada hacia abajo.

En España tenemos una enorme ventaja comparado con algún otro país y frente a nuestros competidores, porque tenemos nuestro propio banco. Dentro de Dell Financial Services está el DBI (Dell Bank International), sucursal en España, con licencia bancaria. Un banco siempre te ayuda a la hora de montar un servicio, especialmente si es en pago por uso: hay que tener unas normas, saber cuáles son los mínimos,

cómo se contrata, cuándo te aumento la facturación...; necesitas herramientas para definir la capacidad del pago por uso, pero también la capacidad financiera y cuanto más cercana la tengas, mejor. Esto facilita las ofertas de APEX, que cada vez están disponibles para más productos comercializados como servicio, desde el puesto de trabajo, al servidor, el almacenamiento, el backup, tanto on-premise como en la nube pública que, aunque lo comercializa el proveedor de nube pública nos está utilizando a nosotros como proveedor de ese servicio... Cada vez estamos llegando con más propuesta de APEX al mercado. Y somos flexibles y capaces de analizar cualquier propuesta que tenga un cliente y encontrar una fórmula intermedia, entre CAPEX y OPEX, según decida la compañía en función de la propia situación en su mercado, con respecto a sus accionistas o su fiscalidad.

Y el canal, ¿cómo ha recibido este modelo de negocio?

Al principio con muchas preguntas sobre si podría quitarles negocio, pues ellos venden servicios, y qué significa para ellos. Rápidamente dimos entrada al canal en el modelo APEX. Nosotros ponemos el banco, ellos una

parte de los servicios, y lo pueden vender como servicio con el respaldo de nuestro banco. Otros partners quieren montar su propio modelo como servicio y nosotros les damos la facilidad. Pero el canal con su servicio tiene cabida en APEX, con sus márgenes y su aportación de valor. Y cuando lo entienden mejor, lo han visto como una oportunidad de llegar a clientes que les decían que no querían invertir, sino que lo quiero como un gasto. Y si antes no tenían una respuesta, ahora sí. Lo están viendo como una oportunidad, más que como una amenaza. ■

MÁS INFO +

» [“Es necesario construir una cultura que trate a las personas como la mayor fuente de innovación”, Ricardo Labarga, Dell Technologies](#)

» [Dell Technologies Forum 2022](#)



COMPARTIR EN REDES SOCIALES

#ENTREVISTA

Cada industria se ha vuelto, en esencia, una industria digital

JULIA WHITE, CHIEF MARKETING AND SOLUTIONS OFFICER AND EXECUTIVE BOARD MEMBER AT SAP

► MIGUEL ÁNGEL GÓMEZ (TEXTO); JOSH LINE (FOTOGRAFÍAS)

“Cada empresa es una compañía tecnológica”. Esta es una frase que repiten los directivos de SAP en sus presentaciones, porque define muy bien el papel que la tecnología ha adquirido en las empresas, independientemente de su sector y su tamaño. Durante la Covid, ha quedado clara la ventaja competitiva que aportan la innovación y la tecnología, pero “queda seguir trabajando y transformar los procesos de negocio, no basta con movernos a la nube”, explica Julia White, Chief Marketing and Solutions Officer and Executive Board Member at SAP.



Recientemente, SAP celebraba en Las Vegas (EE.UU.) una nueva edición de TechEd. Aprovechando la ocasión, IT User tuvo la oportunidad de entrevistar a Julia White, Chief Marketing and Solutions Officer and Executive Board Member at SAP, con quien repasamos algunos temas de actualidad, más allá de los anuncios de este evento.

Tras dos décadas en Microsoft, el pasado año aterrizaba en SAP. ¿Qué ha supuesto un cambio que, desde fuera, parece muy grande, por el perfil de ambas compañías?

Hay muchas cosas que son muy similares y hay algunas que son diferentes, pero sorprende lo mucho que es parecido. Hablamos de dos compañías con varias décadas de historia, si bien en el caso de SAP, es, gran medida, una empresa local que tuvo que transformarse. En ambos casos vemos muchos productos diferentes en la cartera, e, incluso, una estructura organizativa tratando de ejecutar estrategias de una manera profundamente funcional. Así que me sentí muy cómoda con el cambio, pero lo que sí encontré es que SAP tiene una cultura realmente amable. Se preocupa pro-

fundamente por sus clientes, por sus empleados y por ayudar a la sociedad. Es una empresa con valores muy parecidos desde el principio. Además, SAP está increíblemente centrada en el cliente. Reaccionamos cuando un cliente nos necesita, satisfaciendo las necesidades del cliente. Realmente creo que es la mayor diferencia que he visto con el cambio”.

En varios foros, tanto usted como otros directivos de SAP han comentado que cada empresa es una empresa de tecnología. ¿Qué supone esto?

Es así. Pensemos, por ejemplo, en el comercio minorista. ¿Tienen las empresas una página web y capacidad para comprar o gestionar devoluciones en línea? ¿Tiene información y un perfil de cada uno de los clientes a los que se dirigen? Todo esto es tecnología digital. O hablemos del entorno sanitario, con los registros médicos electrónicos de los pacientes. Todos los pasos que se dan acaban en un sistema electrónico. Lo que quiero decir es que cada industria se ha vuelto digital en esencia. Vemos que en todas ellas se está contratando desarrolladores y profesionales a un ritmo que

supera al de tecnológicas como la propia SAP o Microsoft. Cuentan con tanta tecnología que realmente dependen de ella para todo, desde la producción a las finanzas o las relaciones con los bancos. Esto es lo que queremos decir cuando afirmamos que cada empresa se ha convertido en una empresa tecnológica, y ahora tienen que mantenerse al día. Lo vivido durante la Covid fue un ejemplo claro de eso. Las empresas que habían invertido en tecnología tenían capacidades digitales que las hacían estar preparadas y el resto tuvieron que adaptarse rápidamente para estar a la altura, con lo que simplemente se vieron claros el rol y la intensidad que la tecnología ha alcanzado en todos los sectores y en todas las áreas.

Otro gran catalizador de la tecnología es la sostenibilidad. Lo vemos en la industria del automóvil, que necesita mucha tecnología para poder transformarse de los motores de combustión a energías como la eléctrica. O también en las empresas energéticas, que se apoyan en la tecnología para avanzar en la reducción de las emisiones. Son dos ejemplos claros, pero creo que la sostenibilidad es un gran impulsor de la digitalización en todas las empresas.



Hablando de esta sostenibilidad, ¿es algo que ha arraigado en las empresas definitivamente o es solo una corriente temporal?

Veo diferencias. Pero, generalizando, diría que en Europa las empresas se lo toman mucho más en serio que, por ejemplo, las de Estados Unidos. Se trata de una apuesta de más largo plazo, y en Europa la regulación y la preocupación por el Medio Ambiente está más establecida. Siento que las personas han comenzado a posicionarse en torno a esto. Sin embargo, creo que en Estados Unidos las empresas van un poco por detrás.

De todas formas, creo que la presión va a seguir creciendo, aunque no va a ser algo lineal en todas las industrias. Veo un gran avance en las empresas energéticas, porque en ello está su supervivencia. Por eso vemos en este sector proyectos más avanzados en este sentido, porque la presión es mayor y llevan más tiempo trabajando en ello. En cualquier caso, la regulación y la preocupación por el Medio Ambiente van a acelerar las inversiones en sostenibilidad.

Muchas empresas piensan que la Transformación Digital es ir a la nube o permitir a sus equipos trabajar en

“ QUEDA SEGUIR TRABAJANDO Y TRANSFORMAR LOS PROCESOS DE NEGOCIO, NO BASTA CON MOVERNOS A LA NUBE ”

JULIA WHITE,
Chief Marketing and Solutions
Officer and Executive Board
Member at **SAP**

remoto. Pero realmente esta transformación es algo más que eso...

Exactamente. Este es un punto importante. Hay empresas que sacaron sus aplicativos de su centro de datos y los llevaron a la nube, pero los procesos de negocio siguen siendo los mismos. Siguen haciendo todo de la misma manera, mientras su equipo de TI simplemente está administrando el sistema de forma diferente. Nosotros mismos, podemos trabajar en la oficina o en casa, pero, si seguimos haciendo lo mismo, no nos hemos transformado. Simplemente



nos hemos ido a la nube para obtener escalabilidad, eficiencia o capacidades diferentes de gestión. Se trata de un cambio en la infraestructura.

Pero hay clientes que en este tiempo han pasado de vender un producto a vender una suscripción. Necesitan cambiar sus procesos de negocio, cambiar sus sistemas. Han pasado de fijar un precio, empaquetar y vender un producto, a ofrecer una suscripción que tiene un ciclo de vida y unos períodos de renovación, lo que supone un sistema financiero totalmente diferente, lo que implica un cambio en el

proceso y en el modelo de negocio. La clave está en transformar estos procesos de negocio. De ahí la necesidad de talento en las empresas y del apoyo de compañías como SAP, porque el negocio tiene que cambiar, no solo el conocimiento técnico subyacente.

Un ejemplo claro son las cadenas de suministro. En los últimos años, cada una de las empresas con las que trabajábamos en esta área querían concentrarse en pocos proveedores, tan pocos y tan grandes como fuera posible para que fuera la opción más barata. Por eso muchos han reducido

su lista de proveedores a unos pocos de lugares como China. Pero ahora todo está cambiando, y todo el mundo busca nuevos proveedores, nuevas fuentes, nuevos mercados, invertir en diferentes zonas para crear nuevos proveedores regionales, lo que supone un cambio en sus procesos comerciales y en la gestión de la logística y del inventario, lo que implica nuevos procesos de negocio y nuevos sistemas. No se trata de si estamos en la nube o no, sino hacia dónde vamos en términos de transformación.

¿Y en qué punto del camino estamos?

Creo que estamos en el primer cuarto del camino. Las empresas se han dado cuenta de que tienen que mudarse a la nube y dar otros pasos, como permitir el trabajo en remoto, pero los procesos de negocio son los mismos, y como se han topado con la crisis económica, la crisis de la cadena de suministro, la crisis de la inflación... Saben que tienen que cambiar su proceso comercial y abrirlo, con lo que han comenzado con ese plan, pero todavía queda mucho trabajo por delante en términos de una verdadera transformación. Es cierto que algunos lo han hecho, pero creo que la mayoría todavía no.

Algunas industrias, como la Banca o el retail, van por delante frente a otras como la construcción, por ejemplo. ¿Esta diferencia de ritmo se ve también en función del tamaño de los negocios?

Incluso en esas industrias siempre hay diferentes velocidades. Pero, curiosamente, las empresas pequeñas y medianas pueden evolucionar sus procesos de forma más rápida. Es posible que sea porque son procesos menos complejos o porque no cuentan con un legacy que los retenga, pero apoyándose en modelos SaaS, pueden modificar y evolucionar sus aplicaciones de forma más rápida que las grandes compañías, porque, evidentemente, cuesta más girar un barco cuanto más grande es.

Un problema para muchas compañías es la capacitación técnica de su personal, tener los conocimientos necesarios para transformar digitalmente el negocio. ¿Trata el anuncio de SAP Build de ayudarles con este hándicap? ¿Y el resto de novedades de TechEd?

Sí. De hecho, con los anuncios en TechEd creo que podemos ayudarles con la capacitación técnica de los profesionales y la innovación en tres planos diferentes. Dado que se nece-

sitan más profesionales con capacitación técnica, la primera acción pasa por permitir que puedan innovar los profesionales que no son técnicos. No necesitan contratar personas nuevas, porque van a poder innovar con los profesionales con los que cuentan, solo que aportando de otra manera con estas nuevas herramientas, como SAP Build. En segundo lugar, encontramos los desarrolladores profesionales. En este caso, incrementando nuestras inversiones en el plan de aprendizaje de SAP, estamos haciendo que cada vez más profesionales puedan formarse y certificarse en competencias en sistemas SAP de forma gratuita. En tercer lugar, con nuestra alianza con Coursera, podemos ayudar a muchos profesionales a reciclar sus habilidades e incrementar sus capacidades para poder facilitar la innovación en las empresas.

Con SAP Build los profesionales de negocio no necesitan conocimientos técnicos para aportar innovación al negocio. Pero ¿realmente están interesados en hacerlo o prefieren dejarlo en manos de las personas de TI?

Sí, seguro. Las personas que están ingresando en las fuerzas laborales ahora son mucho más expertos téc-

nicamente que sus antecesores. Todos han crecido con un iPhone o con un smartphone Android en el bolsillo. Están acostumbrados a usar aplicaciones y han usado la tecnología desde su nacimiento. Por tanto, la nueva generación de trabajadores ya es más técnica. Pero, además, eso provoca en ellos una mayor frustración en su trabajo por seguir haciendo las cosas de la misma manera y no poder resolverlo técnicamente como están acostumbrados. En definitiva, son empleados muy interesados en ayudar y técnicamente capacitados para ello. ■

MÁS INFO



- » [SAP avanza en su propuesta Low Code con el anuncio de SAP Build en TechEd 2022](#)
- » [SAP se propone formar a 2 millones de personas en competencias TI en tres años](#)



COMPARTIR EN REDES SOCIALES

#ENTREVISTA



“La ciberseguridad es uno de los segmentos más grandes en el sector TIC”

RICARDO MATÉ, REGIONAL VICEPRESIDENT
SOUTH EMEA & EMERGING AT SOPHOS

➤ DESIRÉE RODRÍGUEZ

En algo más de diez años Sophos se ha convertido en una Complete Security Company, y en los últimos ha destacado su crecimiento en la zona Iberia. Nos sentamos con Ricardo Maté, vicepresidente regional para la zona sur de EMEA y países emergentes en Sophos, para analizar la situación que hoy en día viven las empresas, lo que nos deparará este 2023 y cuál es la propuesta de valor de Sophos frente a estas problemáticas.

Ricardo Maté apunta a que la “ciberseguridad se ha convertido en uno de los segmentos más grandes o de mayor crecimiento dentro del sector TIC”. De hecho, Gartner señala que en 2022 se invirtieron en ciberseguridad más de 172 mil millones de dólares y se espera un crecimiento compuesto de un 11 por ciento para los próximos cinco años. En España, IDC prevé un crecimiento de entorno a un 7 por ciento que siga con la tendencia al alza en el sector.

En el último trimestre del año pasado, el mercado de la ciberseguridad ha tenido un crecimiento de un 15,9% interanual ingresando 17.800 millones de dólares. Los ingresos por ciberseguridad en el trimestre en EMEA han alcanzado los 5.200 millones de dólares.

Se nota que existe un cambio en la mentalidad global respecto a la ciberseguridad y las consecuencias derivadas de no estar bien protegido. “Los CEO y los consejos de administración son conscientes de que sus empresas no pueden avanzar en el proceso de transformación digital si sus compañías son vulnerables ante los ciberataques” y eso supone, sin duda, un paso más en lo que

se refiere a ciberseguridad ya que la ciberseguridad está ya en las cúpulas de dirección.

Además, si atendemos a las palabras de nuestro entrevistado, vemos que el mercado de seguridad está en constante evolución y “Sophos ha sido capaz de ir evolucionando su propuesta de valor de forma trepidante” para adaptarse así a la realidad del sector. En parte lo ha hecho gracias a las constantes adquisiciones dentro el sector de la ciberseguridad. La última [SOC.OS](#), una empresa con sede en el Reino Unido, que llega con

el objetivo de resolver el problema de la fatiga de las alertas y la visibilidad limitada tan frecuente en los entornos de seguridad de TI. Esta adquisición “nos está permitiendo posicionarnos como una de las compañías más punteras en la oferta de servicios de detección y respuesta 24/7 con nuestro MDR”.

Así, Sophos cuenta ya con 13.500 clientes bajo servicios de detección y respuesta gestionados, lo que representa un 10% de la facturación y se espera que siga creciendo “tanto a nivel mundial como en Iberia”.

Otro de los secretos del éxito de Sophos es, sin duda, su estrecha relación con el canal y con los grandes integradores. “Seguimos trabajando estrechamente con nuestro canal de distribución”.

SEGURIDAD COMO SERVICIO: LA CLAVE PARA PROTEGERSE ESTE 2023

Si hablamos de los problemas a los que se enfrenta el sector hoy en día, Ricardo Maté lo tiene claro: la complejidad tanto de los ataques como de las soluciones de ciberseguridad y la escasez de talento están en la cima. “La única solución frente a esta tormenta perfecta es la ciberseguridad como servicio”. Por eso, precisamente, Sophos está centrandose su apuesta en ofrecer un servicio gestionado de ciberseguridad 24/7 proporcionado por expertos. El objetivo de Sophos es, en definitiva, “facilitar la adopción de ciberseguridad sin necesidad de tener los conocimientos e independientemente de su nivel de capacitación en ciberseguridad”. Y parece una apuesta segura pues, Gartner apunta a que más de la mitad de las empresas contratarán algún servicio de seguridad gestionada hasta 2025 por lo que la



ENTREVISTA >> “LAS BARRERAS DE ENTRADA A LA CIBERDELINCUENCIA CADA VEZ SON MENORES” Ricardo Maté, Sophos

tendencia es clara hacia este tipo de servicios.

En este sentido, Sophos ofrece tres versiones dependiendo de la capacitación y necesidades del cliente. Sophos MDR se puede personalizar con diferentes niveles de servicio y opciones de respuesta a las amenazas: Sophos Threat Advisor, Sophos MDR y Sophos MDR Complete.

Además, la solución de la compañía es compatible con una lista cada vez mayor de proveedores de telemetría de seguridad, como Amazon Web Services (AWS), Check Point, CrowdStrike, Darktrace, Fortinet, Google, Microsoft, Okta, Palo Alto Networks, Rapid7 y muchos más. La telemetría se consolida, correlaciona y prioriza automáticamente con información exhaustiva de Sophos Adaptive Cybersecurity Ecosystem (ACE) y la unidad de información sobre amenazas Sophos X-Ops.

EN ESPAÑA ESTAMOS MÁS CONCIENCIADOS QUE EN OTROS PAÍSES

Si le preguntamos a Ricardo Maté sobre la singularidad del mercado español respecto al resto de países bajo su cargo, el vicepresidente para el sur de EMEA y países emergentes de

Sophos señala que “España sufre los mismos ataques que el resto, no hay diferencias respecto a otros países, pero nuestro Gobierno y organismos públicos tiene una mayor concienciación”. Sin embargo, parece que queda mucho por hacer pues “prácticamente todas las empresas y organismos públicos han sufrido un incidente grave este año”.

“ EL OBJETIVO DE SOPHOS ES FACILITAR LA ADOPCIÓN DE CIBERSEGURIDAD SIN NECESIDAD DE TENER LOS CONOCIMIENTOS E INDEPENDIENTEMENTE DE SU NIVEL DE CAPACITACIÓN EN CIBERSEGURIDAD ”

RICARDO MATÉ,
Regional Vicepresident South EMEA & Emerging at **Sophos**

Si atendemos a los ataques de este último año parece que los ciberdelincuentes se están profesionalizando. De hecho, en informe anual de Sophos, el ‘Sophos Threat Report 2023’, se dice que los mercados clandestinos de ciberdelincuentes están operando “como negocios convencionales”. Y es que, parece que los cibercriminales ya no solo forman organizaciones u ofrecen los ataques como servicio, sino que además se están especializando como cada uno de nosotros en nuestros respectivos sectores: “están segmentando el conocimiento” asegura Ricardo Maté, que añade que “las barreras de entrada a la ciberdelincuencia cada vez son menores”.

EL CIBERCRIMEN EN 2023: AMENAZAS MÁS DIFÍCILES DE DETECTAR Y A SISTEMAS DIFERENTES

De cara a 2023, el directivo de Sophos pone el foco en los ataques a sistemas que no suelen ser atacados y que, por tanto, tampoco están acostumbrados a esa necesidad de protegerse. Sistemas Linux, Apple o de entornos industriales y, por supuesto, ataques a dispositivos móviles están siendo cada vez más atacados y tienen que empezar, si no lo han hecho ya, a protegerse

porque “vamos a seguir la misma línea en los próximos meses”. Y también advierte de la proliferación de ataques que utilizan herramientas lícitas, herramientas del sistema que “son más difíciles de detectar”.

“Los ciberdelincuentes cada vez están más preparados, son más eficientes”, por eso, apunta el directivo, “las empresas tenemos que hacer los mismo y para ello contar con los proveedores de soluciones de ciberseguridad que permitan esa mayor protección detección y respuesta”. ■

MÁS INFO +

- » [El negocio de la ciberseguridad empresarial sigue creciendo](#)
- » [Sophos](#)
- » [Sophos adquiere SOC.OS](#)
- » [Informe de amenazas de Sophos 2023](#)



COMPARTIR EN REDES SOCIALES

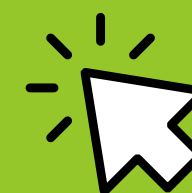
DMI

Computer

Disponible en www.dmi.es

KIOXIA

Comparte tu mundo



TransMemory U365

#ENTREVISTA

“Quiero reforzar la integración entre negocio y el roadmap tecnológico”

BERNARDO RUIZ, CTO DE TOP DOCTORS

➤ ARANCHA ASENJO

Tras un tiempo en la compañía como responsable de desarrollo en el área de movilidad, Bernardo Ruiz ha sido nombrado CTO de Top Doctors, una plataforma de citas médicas on-line presente en ocho países, entre ellos España, y que gestiona más de 275.000.000 visitas y 2.300.000 citas cada año con su cuadro de especialistas. Hablamos con él para conocer, de primera mano, cuál va a ser su función en la compañía tras el nombramiento.

ITDM >> Enero 2023



ENTREVISTA >> “Mi misión va a ser definir e implementar la estrategia tecnológica de la organización”,
Bernardo Ruiz, Top Doctors

Según nos explicaba Bernardo Ruiz, “mi misión va a ser definir e implementar la estrategia tecnológica de la organización. Es decir, orientar y mejorar los productos que tenemos dentro de la compañía para que, en términos de calidad, continuidad y, sobre todo, seguridad, demos un salto cualitativo”. Para conseguir estos objetivos, “lo primero va a

ser incorporar nuevas tecnologías, apoyándonos en varios pilares: los datos, Machine Learning, inteligencia artificial... con un alto grado de observabilidad, porque no se trata solo de incorporar mejoras, sino de ser conscientes de que éstas están funcionando, y, al ser un mundo que está totalmente interconectado, poniendo un énfasis especial en la integración”.

NUEVOS RETOS DESDE SU POSICIÓN EN LA COMPAÑÍA

Desde su nuevo rol en la organización, Bernardo Ruiz asume nuevos retos que, a corto plazo, se traducen en “reforzar el equipo de TI. Necesitamos cubrir roles importantes e implementar medidas para gestionar el talento, algo muy complicado a día de hoy en este sector. Por otro lado, mejorar la calidad y seguridad de nuestros productos, y, para ello, vamos a realizar una fuerte inversión para reforzar los equipos de QAP y DevOps incorporando roles más relacionados con datos. Además, quiero asegurar más el alineamiento entre negocio y el roadmap tecnológico, que no haya saltos entre lo que quiere la gente de negocio y lo que desarrolla el equipo de TI. En este sentido, es fundamental el rol de análisis funcional, para convertir los requisitos de negocio en funciones entendibles para el equipo de desarrollo. Posteriormente, quiero migrar a tecnologías más punteras, agilizar los procesos de negocio, los procesos de desarrollo, la observabilidad, integraciones con todos los jugadores del mercado, es decir, doctores, pacientes, aseguradoras, hospitales, farmacias...”

Con la mirada puesta en el medio plazo, “mis retos pasan por mejorar

los proyectos de datos de la empresa. Tenemos un proyecto concreto, Layer Intelligence, que unifica todas las fuentes de datos de la organización, pero queremos seguir trabajando e introducir algoritmos de Machine Learning y crear nuevos cuadros de mando, por ejemplo, para que se enfoque tanto al área técnica como de negocio. Queremos seguir avanzando en el área de inteligencia artificial, donde actualmente tenemos un proyecto, Chatbot, que sustituye a nuestro sistema de llamadas para

reserva de citas. A día de hoy es un piloto que necesita algunas mejoras, para implementarlo en otros países”.

Y en el largo plazo, “se abre un abanico de posibilidades con tecnologías como Blockchain para los historiales médicos, Metaverso e IoT con dispositivos médicos”.

TECNOLOGÍAS ESENCIALES PARA EL SECTOR DE LA SALUD

Desde la pandemia, hemos asistido a un vuelco total y a la transformación del sector sanitario. Para Bernardo Ruiz, “podemos destacar la inteligencia artificial, que está redefiniendo el sector mejorando la calidad de la atención reduciendo los costes para los hospitales y las aseguradoras. Se están modificando los algoritmos

para más usos, como, por ejemplo, la gestión de los medicamentos, o se están aplicando en la mejora de la atención al paciente que antes se hacía de forma manual y que ahora puede ser un servicio 24x7. Por otra parte, tecnologías como big data o machine learning están muy asentadas para ayudar en la toma de decisiones estratégicas, consiguiendo que el diagnóstico y la gestión de pacientes sean sencillos y manejables. Los datos generados por la industria de la salud están creciendo año a año un 50%, de ahí que sea fundamental tener una buena herramienta de análisis de datos. Otro ejemplo es la telemedicina, que, aunque avanza lentamente, está generando experiencias positivas en los pacientes

“NECESITAMOS CUBRIR ROLES IMPORTANTES E IMPLEMENTAR MEDIDAS PARA GESTIONAR EL TALENTO, ALGO MUY COMPLICADO A DÍA DE HOY EN ESTE SECTOR”

BERNARDO RUIZ,
CTO de **Top Doctors**



atendidos en telesalud. Va a transformar el sector, sobre todo, si lo unimos con los dispositivos médicos de IoT, que permiten monitorización y control del paciente en tiempo real. Tampoco podemos olvidar Blockchain, que puede ser muy importante para securizar las transacciones de datos de los pacientes. Fuera de nuestro ámbito, la nanotecnología está dando pasos importantes, por ejemplo, para los sistemas de administración de medicamentos. Es una tecnología en la que está habiendo grandes inversiones. Por último, el metaverso, que es una realidad por la que apuestan muchas compañías”.

TENDENCIAS Y METODOLOGÍAS DE DESARROLLO EN ESTE SECTOR

Aprovechando la experiencia de Bernardo Ruiz en desarrollo, nos comentaba que “cada día se mueve todo más hacia la computación en la nube, dejando la tecnología on-premise atrás. Destaca también el uso de herramientas de Low-Code y No-Code, apoyadas en IA, para permitir llevar el desarrollo a personas con menores conocimientos de programación. También sigue en aumento el uso de JavaScript, sobre todo para la creación de soluciones innovadoras. Otra

tendencia son los microservicios, y se está convirtiendo en un nuevo estándar para las aplicaciones, al igual que DevOps para mejorar los flujos de trabajo y la eficiencia del desarrollo. Por último, aunque todavía no se ha consolidado, el desarrollo con frameworks multiplataforma, sobre todo para aplicaciones móviles”.

INFRAESTRUCTURA TECNOLÓGICA

Centrándonos en Top Doctors, quisimos saber algunos detalles de su infraestructura tecnológica. En palabras de su nuevo CTO, “nosotros partíamos de una infraestructura monolítica, y hemos cambiado radicalmente. Ahora tenemos una arquitectura hexagonal, con back-end

y front-end separados y organizados por microservicios en contenedores, utilizando clusters de Kubernetes... alojado todo en la nube. En el front-end utilizamos mucho JavaScript y en el back-end tecnologías de vanguardia como Colab. Y todo ello con integración continua y bajo la supervisión de herramientas de observabilidad”.

Pensando en 2023, “nos enfrentamos a uno de los cambios más decisivos de nuestra historia: migrar los diferentes países a esta infraestructura tecnológica que comentaba, algo que solo hemos hecho en 3 de los ocho países en los que operamos. El resto los vamos a migrar antes del verano de 2023, para contar con una única plataforma rejuve-

necida y optimizada, que nos ofrezca un ahorro de costes y escalabilidad, así como la capacidad para centrarnos en nuevos proyectos. Sin olvidar proyectos más concretos como Layer Intelligence, que nos va a permitir contar con una plataforma puntera”.

Uno de los grandes problemas de todas las empresas “con base tecnológica”, apuntaba Bernardo Ruiz, “es el de la gestión del talento. Nosotros estamos avanzando mucho en el diseño de planes de carrera y apostando por la flexibilidad laboral y la deslocalización y el teletrabajo. Asimismo, estamos dando importancia a la promoción interna, y contamos con la ventaja de estar en un segmento atractivo”. ■



MÁS INFO +

- » [Entrevista Bernardo Ruiz, CTO de Top Doctors](#)
- » [Top Doctors](#)



COMPARTIR EN REDES SOCIALES

Proteger una institución del calibre de UNIR no es tarea fácil

JUAN JOSÉ NOMBELA, CISO UNIR

➤ DESIRÉE RODRÍGUEZ

Con más de 30 años de experiencia en TIC y ciberseguridad y siendo autor de los dos primeros libros sobre el sector de España, no es de extrañar que hace 8 meses, la Universidad Internacional de La Rioja (UNIR) nombrase a Juan José Nombela, CISO de la institución.

Desde ese momento, Juan José forma parte de la lista de expertos en ciberseguridad encargados de gestionar la seguridad de su empresa y enfrentarse a los retos, cada vez más numerosos, que afectan al sector. Por eso, hemos querido hablar con él de cómo ha afrontado este nuevo cargo

y cuáles serán los retos a tener en cuenta de cara a los próximos meses.

LOS RETOS DE PROTEGER UNIR

Ser CISO de una institución del calibre de UNIR no es tarea fácil. El mayor reto al que se enfrenta Juan José Nombela desde que llegó al cargo es “sin duda, el nivel de exposición”. Y es que, hay



que tener en cuenta que hablamos de una Universidad online lo que quiere decir que todos los alumnos estudian online, todos los profesores dan clase online y todos los procesos y gestiones se llevan a cabo también de forma digital. “Esto supone una superficie de exposición enorme que hay que proteger”, señala Nombela.

Además, el grupo al que pertenece UNIR cuenta con más de 5.000 empleados en todo el mundo y eso supone un riesgo en sí mismo.

Si hablamos de protegerse en un entorno educativo como el de UNIR teniendo en cuenta la gran superficie de exposición que abarca debemos abordar multitud de aspectos:

► Primero se ha tener en cuenta que, el sector educativo, igual que el sector sanitario, ha sido el blanco de muchos ataques durante la pandemia. Sobre todo, de ataques de ransomware. Ya lo vimos con los ataques dirigidos a la Universidad Autónoma de Barcelona, la de Castilla La Mancha o la de Extremadura si nos alejamos más en el tiempo. “Somos objetivo de las bandas de ciberdelincuentes, no somos un Banco ni una empresa multinacional con unos ingresos como los que pueden tener ellos pero estamos siendo un objetivo claro en los últimos años”, apunta Nombela. Y es por eso que, desde su punto de vista, uno de los principales retos hoy en día es “saber enfocar correctamente estas amenazas con soluciones avanzadas que utilizan inteligencia artificial o machine learning para poder detectar, de una forma eficiente y eficaz, este tipo de intentos de ataques a los que estamos siendo sometidos”.

► La utilización de tecnología de primer nivel, que ayude a detectar y parar amenazas es un must para cualquier empresa y también parece serlo para UNIR. Para entender esta necesidad, hay que tener en cuenta que, aunque la institución ejerza en varios países, su equipo de ciberseguridad

es bastante reducido: “Necesitamos herramientas que utilicen automatización, inteligencia artificial, remediación automática, o sea que tomen acciones o realicen la respuestas de forma autónoma en la medida de lo posible, porque como ocurre en muchas empresas no tenemos equipo suficiente como para estar vigilando todos los eventos de seguridad que se pueden producir a lo largo del día e investigarlos y dar una respuesta inmediata sin ayuda de la tecnología”.

LA SEGURIDAD DESDE EL DISEÑO

No obstante, al contrario que en muchas organizaciones e institucio-

nes del sector, **la seguridad forma parte del ADN de UNIR**: “tenemos un equipo de más de 100 desarrolladores que crean nuestras aplicaciones campus virtuales y todo tipo de plataformas. Por eso tenemos en nuestro ADN la seguridad y la privacidad desde el diseño” asegura Juan José Nombela. “Nuestro objetivo es cumplir con esa privacidad y seguridad no solo en los nuevos productos sino también, e incluso más, en los que ya utilizamos” añade.

Si le preguntamos por ese proceso de creación, Nombela apunta a que “no solo cuenta la calidad del software”. De hecho, lo primero a tener en

cuenta es la conformidad, “**la seguridad va por delante** y nuestro equipo lo tiene que contemplar” sentencia. Y cuando piensa en equipos, este responsable no incluye únicamente a técnicos y programadores. “Cuando hablo de empleados hablo de todos, también de la alta dirección. De hecho, la concienciación de la cúpula directiva es, si cabe, más importante pues son los que deciden en qué invertir cada partida y los que más acceso tienen a los datos esenciales de la empresa. Eso es un reto y un objetivo que deberíamos tener todas las empresas y que en UNIR tenemos desde hace meses”, dictamina.

Para cumplir con esta meta, UNIR cuenta ya con un proyecto cuyo principal objetivo es implantar una cultura de seguridad a todos los niveles. “Queremos que la ciberseguridad sea un pilar, que conlleve un cambio de comportamiento en todos los ámbitos porque la mayor parte de los ataques parten o se aprovechan del usuario. Que el usuario esté concienciado y tenga la formación necesaria para no ser cómplice de los ciberdelincuentes es vital”, nos explica Juan José Nombela.

En este sentido, con el objetivo de seguir mejorando en ciberseguridad,

“ CUANDO HABLO DE EMPLEADOS HABLO DE TODOS, TAMBIÉN DE LA ALTA DIRECCIÓN. DE HECHO, LA CONCIENCIACIÓN DE LA CÚPULA DIRECTIVA ES, SI CABE, MÁS IMPORTANTE PUES SON LOS QUE DECIDEN EN QUÉ INVERTIR CADA PARTIDA Y LOS QUE MÁS ACCESO TIENEN A LOS DATOS ESENCIALES DE LA EMPRESA ”

JUAN JOSÉ NOMBELA, CISO UNIR

UNIR quiere, como uno de los propósitos principales, de cara a este 2023 que acaba de empezar, certificarse en la ISO 27001 con el fin de poder asegurar la protección de todos y cada uno de sus activos de la mejor manera posible. Y, como tantas otras empresas a nivel mundial, UNIR tiene en mente dar el salto a la nube pública en los próximos meses. “Ya utilizamos cloud desde hace tiempo, pero queremos poder utilizar la nube pública de forma segura con lo que hay que tener en cuenta muchos parámetros”.

TALENTO Y ESPECIALIZACIÓN

Alejándonos ahora de la UNIR y los retos de Juan José Nombela como CISO de la entidad, no hemos podido dejar de preguntarle por los obstáculos que cree, tiene el sector a día de hoy. Para él, la principal dificultad a la que se enfrenta la ciberseguridad hoy en día, más allá de los ataques, es la falta de talento. “La falta de profesionales es un gran freno, ya que sin el conocimiento adecuado es difícil hacer frente a unos cibercriminales cada vez más preparados”.

Precisamente para hacer frente a esta falta de talento en UNIR han creado un máster específico en ciberseguridad que está teniendo una

muy buena acogida y del que se espera que salgan los profesionales de ciberseguridad de la próxima generación. “En UNIR -apunta Nombela- creemos que la mejor forma de asegurar el futuro de las empresas parte de tener un buen colchón de talento en ciberseguridad. Por eso el Máster en Ciberseguridad de UNIR, que ya va por su 20ª edición, es el primero oficial con docencia 100% online que te forma en las principales técnicas de protección frente a ataques y amenazas en sistemas operativos, redes, software de aplicación, sistemas web y bases de datos”.

Entre los hitos conseguidos por la institución está formar a 300 alumnos al año, y no solo en España. “Tenemos unos 100 alumnos anuales en España y otros 200 en Latinoamérica” cifra Juan José. Con estas cifras, podríamos pensar que, al menos en UNIR, no tienen problemas a la hora de encontrar talento y, sin embargo, su CISO nos abre los ojos frente a la cruel y triste realidad: **“A pesar de que tenemos esa cantera, cuesta encontrar talento para cubrir las vacantes que tenemos incluso internamente”**. Así, Nombela se une al 60% de los directivos que, según apunta el Informe sobre la brecha de

habilidades en Ciberseguridad 2022 de Fortinet, admite que su organización tiene dificultades para contratar personal o (el 52%) para retenerlo.

También tienen una apuesta decidida por la especialización. “Especialista en ciberseguridad es un término muy amplio ya que implica tener conocimientos en forense, redes, entornos industriales... en UNIR apostamos por una mayor especialización que sirva a esos futuros profesionales para encuadrarse en lo que realmente les guste”.

FUTURO Y CIBERGUERRA VAN DE LA MANO

Si dejamos de lado el talento y preguntamos al CISO de UNIR por el futuro y lo que nos depararán los próximos meses, su topic estrella está claro: **“La ciberguerra va a seguir dando mucho de qué hablar”** sentencia. A lo que añade: “La Guerra entre Rusia y Ucrania es un tema que va a hacerse notar sino a corto, a medio o largo plazo. De momento ya hemos visto ciberataques cuyo objetivo ya no es económico sino dejar sin funcionamiento infraestructuras críticas, bancos u otros servicios esenciales para los ciudadanos de uno u otro país. A esto hay

que unir ataques hacktivistas que intentan hacerse con el control de alguna institución o infraestructura esencial con el objetivo de mostrar su descontento con la situación que se está viviendo. Creo que estos ataques van a seguir sucediéndose e incluso agravándose según avance el conflicto pues los ataques informáticos llevan años ganando importancia mundial y este tipo de conflictos potencian su uso. No olvidemos, además, que Rusia es una de las grandes potencias en ciberseguridad y ya ha colaborado y apoyado la realización de ciberataques en otras ocasiones ya sea por acción propia o simple omisión del delito”. ■

MÁS INFO +

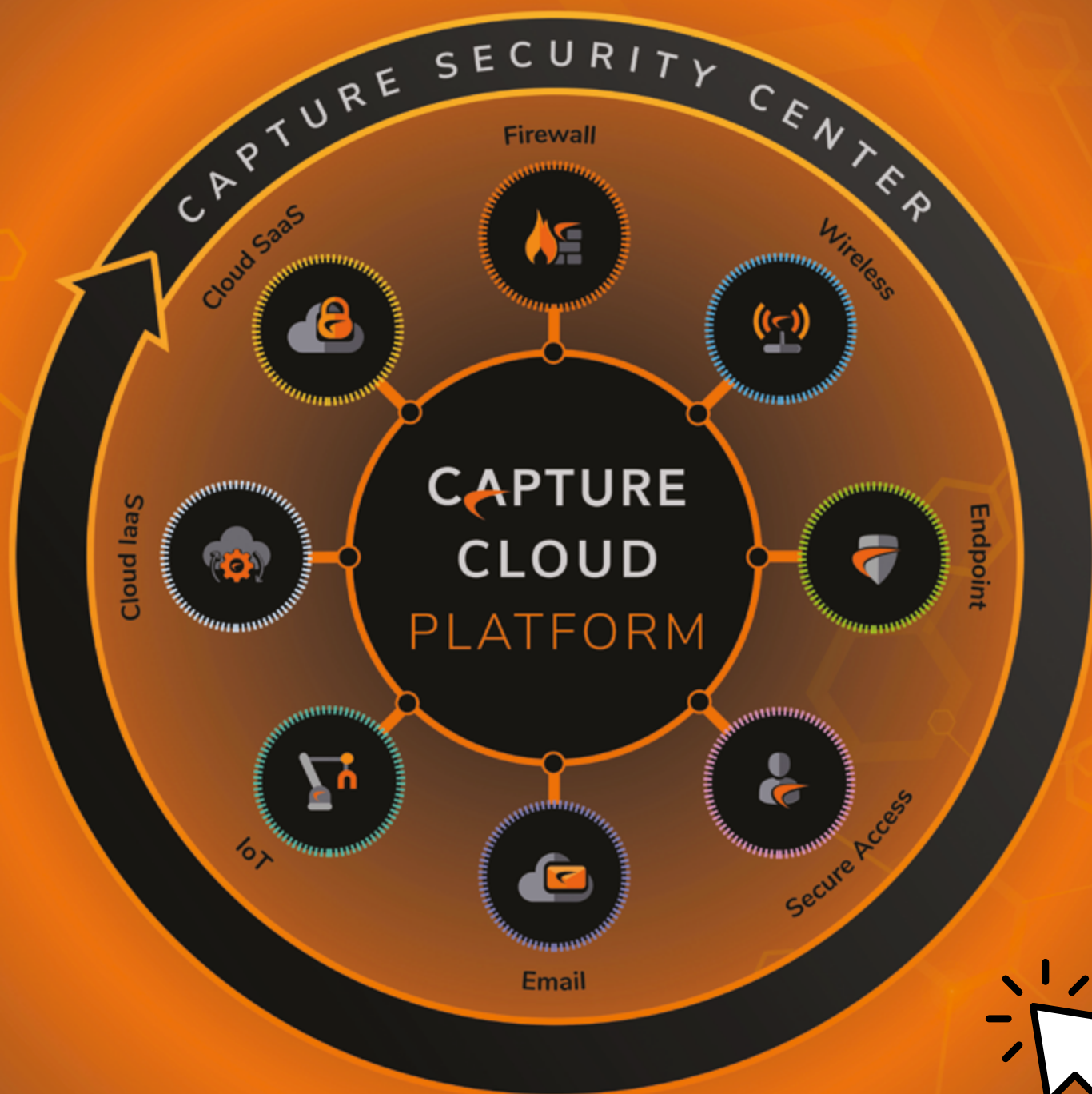
- » [UNIR](#)
- » [Ciencias de la Seguridad](#)
- » [2022 Cybersecurity Skills Gap](#)



COMPARTIR EN REDES SOCIALES

SONICWALL®

BOUNDLESS CYBERSECURITY



Reduzca la brecha de Ciberseguridad

Entre en la era de la ciberseguridad sin límites ni perímetro

- Protección contra puntos de exposición ilimitados con una defensa por capas
- Inteligencia global sobre amenazas para una protección en tiempo real sin fisuras
- Reducción del coste total de propiedad mientras se atiende a trabajadores remotos y móviles



Network Security



Secure Access Service Edge



Simplified Management



Advanced Threat Protection



Secure SD-Wan



Wireless Security



Secure Remote Access



SaaS Security



Endpoint Protection



Email Protection



SonicWall.com/Boundless

ESPAÑA ATRAERÁ 5.000 MILLONES DE EUROS EN INVERSIONES PARA CENTROS DE DATOS

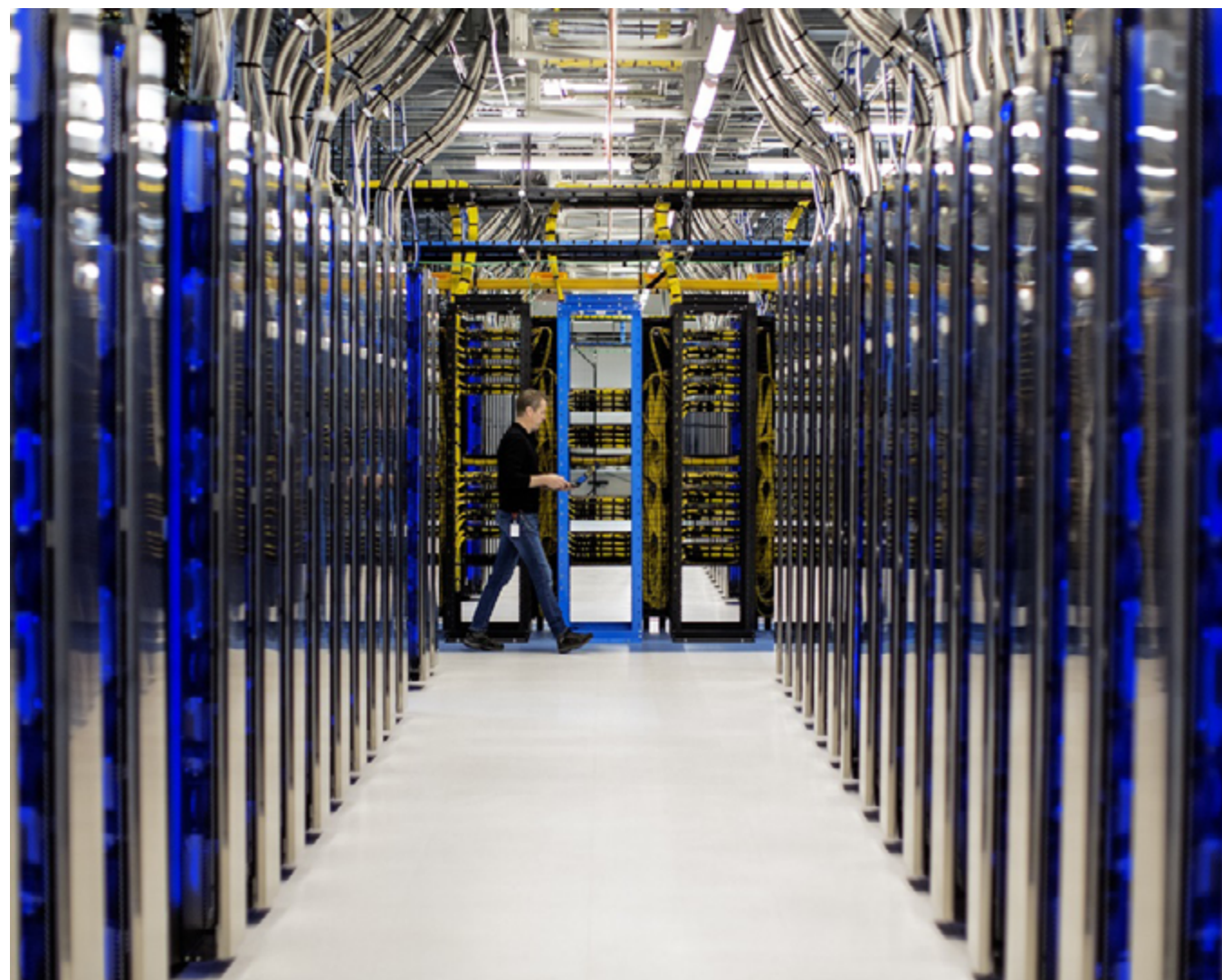
El sector de los data centers ha observado un crecimiento muy notable que continuará en los próximos años. De hecho, SpainDC estima que durante los próximos cinco años España podrá atraer inversiones de unos 5.000 millones de euros en infraestructuras físicas.

“Los centros de datos se han convertido en un factor clave dentro de la economía española, donde las grandes empresas del sector ya invierten grandes sumas monetarias para la construcción de sus infraestructuras. Mantener estas inversiones no solo depende de los beneficios que ofrece

nuestro país para los centros de datos, sino que también hay que saber hacer frente a las nuevas demandas del mercado y afrontar los retos futuros”, declara Ignacio Cereijo, director de desarrollo de negocio de la unidad especializada de Data Center de fibratel, que resalta algunos de los desafíos a los que se enfrenta la industria para el próximo año:

► **Sostenibilidad.** La industria tecnológica es la responsable del 6% de las emisiones de CO2. Por esta razón, los data centers están dirigiendo sus esfuerzos hacia la conversión a un data center sostenible. Para ello,

Mantener las inversiones no solo depende de los beneficios que ofrece nuestro país para los centros de datos, sino que también hay que saber hacer frente a las nuevas demandas del mercado y afrontar los retos futuros, incluido el cuidado del medioambiente, asegurar la disponibilidad del data center, la contratación de más personal y el ahorro energético.



además de estudiar la ubicación de las instalaciones para favorecer el ahorro energético –ya que situar los centros de datos en lugares con climas más suaves, favorecen su refrigeración consiguiendo un ahorro térmico de cerca del 50%–, es importante conocer las alternativas existentes en cuanto a procesadores y refrigeración de la infraestructura. En ese sentido, la refrigeración líquida ganará más adeptos el próximo año. Según estima fibratel, la instauración de este método de refrigeración podría suponer un ahorro de más de 205.000kWh por un rack de ocho servidores con respecto a el enfriamiento por aire. Con respecto a los procesadores, apostar por procesadores de bajo consumo reduce el gasto energético en un 10%.

► **Disponibilidad.** La tendencia en este sentido es dirigirse hacia centros de datos que aseguren una disponibilidad lo más cercana posible al 100%, los conocidos como Tier IV, que garantizan un 99.995%. Estos cuentan con varios sistemas independientes y de mantenimiento concurrente, lo que favorece que no se vea afectado ante un imprevisto o un mantenimiento planificado y sufra una interrupción en el servicio. Se trata de la certificación más robusta que puede recibir un data

center y para 2023 lo expertos de fdata estiman que estas certificaciones aumenten por la transformación de muchos centros de datos y la construcción de otros nuevos.

► **Talento.** El rápido crecimiento de esta industria hace necesaria la contratación de más personal para garantizar un servicio óptimo. Sin embargo, existe cierta complejidad a la hora de atraer talento y retenerlo, lo que hace que muchas empresas no logren cumplir los cupos de demanda.

Por eso, 2023 se presenta como una oportunidad por parte de empresas e instituciones educativas para poner en valor la importancia de la formación en centros de datos, incorporando más conocimientos relacionados con esta temática.

► **Energía.** El ahorro energético, así como el uso de fuentes de energía alternativas son dos de los principales retos del sector para el próximo año. Y es que, la industria de los centros de datos consume en torno

a 205 teravatios hora, que equivale al 1% de toda la energía consumida a nivel global, con previsión de llegar a cerca del 8% de la demanda total de electricidad proyectada. Así, además de adoptar medidas para mejorar la eficiencia energética, como la refrigeración líquida, cuidar la ubicación del centro de datos y el uso de procesadores de bajo consumo, es importante optar por el uso de energías renovables, que puede conseguir unas emisiones de dióxido de carbono casi nulas, lo que favorece la sostenibilidad. ■

EL RÁPIDO CRECIMIENTO DE ESTA INDUSTRIA HACE NECESARIA LA CONTRATACIÓN DE MÁS PERSONAL PARA GARANTIZAR UN SERVICIO ÓPTIMO



MÁS INFO +

- » [La demanda de infraestructura física para centros de datos crece un 11%](#)
- » [Los centros de datos se alzan como garantes de la digitalización y la sostenibilidad](#)



COMPARTIR EN REDES SOCIALES

#TENDENCIAS

2023, ¿UN MAL AÑO PARA EL METAVERSO?

➤ REYES ALONSO

Desde que se presentó en sociedad el concepto de Metaverso se han generado opiniones en todos los sentidos. Inicialmente, Facebook fue el mayor impulsor de la idea, hasta el punto de que la compañía cambió su nombre por Meta, volcando muchos recursos en su desarrollo. Otras em-

presas han entendido que el futuro de Internet y de muchos negocios digitales estará ligado al Metaverso, y se han lanzado a desarrollar sus propias versiones y servicios basados en el Metaverso, o de sumarse a los primeros entornos virtuales generados en base a este concepto. Por otro lado, se ha expandido el escepticismo entre

una gran cantidad de empresas y sectores, que ven una falta de madurez en la idea del Metaverso y en los modelos de negocio basados en él. Las opiniones al respecto son muy dispares, y los resultados económicos de la propia Meta no ofrecen unas buenas perspectivas para el desarrollo del Metaverso el año que viene.

El Metaverso continúa generando opiniones muy dispares, con empresas que se han lanzado de cabeza a este nuevo mundo digital, mientras que otras siguen mostrándose muy escépticas con respecto a su potencial y su futuro.

Las perspectivas para el Metaverso en 2023 no son muy positivas, pero los expertos creen que esto no impedirá que el concepto siga desarrollándose a más largo plazo, y en los próximos años proporcionará a los internautas una nueva forma de interactuar y consumir todo tipo de servicios digitales.

UN MAL AÑO PARA EL METAVERSO, SEGÚN LOS EXPERTOS

Los investigadores de GlobalData se suman a este mal pronóstico y anticipan que 2023 será un mal año para el Metaverso, ya que los consumidores están mostrando un gran desinterés, y las inversiones en estos mundos virtuales no están creciendo como estaba previsto hace un año. William Tyson, analista asociado del equipo de inteligencia temática de esta firma de investigación, destaca cuáles son las principales tendencias sobre el Metaverso para el año que viene y más allá.

La primera es que el Metaverso no va a cumplir con las expectativas el año que viene, ya que arrastra la carga de la inmadurez de tecnologías clave, como la realidad virtual y la inteligencia artificial. Al mismo tiempo, los consumidores están perdiendo el interés y perciben que estos entornos no serán tan accesibles, dado el elevado coste de las tecnologías habilitadoras de una experiencia completa en el Metaverso, como las gafas de realidad virtual. Esto limitará seriamente la adopción del Metaverso en 2023.

En opinión de Tyson, “la ausencia de una visión única para el Metaverso

significa que su futuro es maleable e incierto. Su extraordinario potencial a largo plazo es ampliamente reconocido, razón por la cual las grandes tecnológicas continúan canalizando miles de millones hacia su creación, a pesar de la ausencia de retorno de la inversión a corto plazo”. Pronostica que la tecnología del Metaverso sufrirá un enfriamiento a corto plazo, pero cree que esto también dará tiempo para que se desarrollen las tecnologías subyacentes.

Otra tendencia a destacar es el impulso que experimentará el Metaverso en China, donde las inversiones en las tecnologías habilitadoras están aumentando rápidamente, a pesar de las importantes restricciones impuestas por el gobierno. Este control condicionará mucho el camino que seguirán las empresas chinas para desarrollar el Metaverso, pero su interés en construir las bases de este concepto parece superar al de las empresas occidentales.

En opinión de Tyson, “la planificación central en China ayudará al desarrollo del Metaverso a medida que las empresas buscan socavar las capacidades de Occidente. Las empresas chinas se beneficiarán de políticas preferenciales y subsidios

en sus intentos de innovar”. Esto es algo que no se verá en Occidente, donde los gobiernos y las empresas lo tienen mucho más difícil para justificar la inversión en una tecnología que se encuentra en una etapa tan temprana de desarrollo. Además, la caída de la economía lo pone aún más difícil de cara a 2023, y habrá que esperar varios años para que el Metaverso se consolide como una tecnología de uso común.

¿PREPARADOS PARA EL IMPACTO DEL METAVERSO?

Pero, como decíamos, no todos los expertos son negativos con la evolución del Metaverso, y se estima que tendrá un impacto significativo en nuestra realidad. DXC Technology ha identificado los cinco escenarios principales: la colaboración en el trabajo, los eventos, el ocio, la interrelación con las marcas y los procesos de selección de personal y de onboarding.

► **La colaboración en el lugar de trabajo nunca volverá a ser lo mismo.** En todo el mundo, el Metaverso formará parte del trabajo diario de millones de empleados. En lugar de mirar un conjunto de caras bidimensionales en una pantalla de videoconferencia, los asistentes podrán



elegir su asiento en una mesa virtual, salir de la sala para un descanso e incluso dar un paseo virtual con su jefe. Para acelerar los beneficios, muchas empresas están combinando las videoconferencias tradicionales con tecnologías de colaboración inmersiva. En DXC ya se ha comprobado el impacto positivo de su propio mundo virtual privado, con mayores niveles de productividad, compromiso y creatividad entre sus empleados. “Las experiencias basadas en el Metaverso están ayudando a los empleados a concentrarse mejor y retener más información. Los mundos virtuales pueden ayudarnos a salir de la rutina de las videoconferencias y abrir la puerta a una mayor colaboración e innovación”, afirma Nathalie Vancluysen, responsable de Realidad Extendida de DXC Technology.

► **Los eventos profesionales a gran escala serán virtuales.** El Metaverso es un lugar donde miles de avatares de todo el mundo pueden reunirse para interactuar, conocerse y llegar a acuerdos. Controlados por las personas desde la comodidad del lugar que elijan, los avatares 3D personalizados pueden moverse libremente por un espacio casi infinito y teletransportarse de un lugar a otro

2023 SERÁ UN MAL AÑO PARA EL METAVERSO, YA QUE LOS CONSUMIDORES ESTÁN MOSTRANDO UN GRAN DESINTERÉS, Y LAS INVERSIONES EN ESTOS MUNDOS VIRTUALES NO ESTÁN CRECIENDO COMO ESTABA PREVISTO HACE UN AÑO

de forma instantánea. En el futuro, cada vez más eventos a gran escala, como conferencias, exposiciones y cumbres, se celebrarán en mundos virtuales, lo que permitirá mayores oportunidades de colaboración a escala mundial y reducirá el tiempo, los recursos y la huella de carbono de los desplazamientos.

► **Los grupos de música, los DJ, los clubes deportivos y las citas pasarán al Metaverso.** Cada vez más personas y organizaciones de la industria musical y deportiva animan a los aficionados a unirse a ellos desde asientos virtuales en recintos virtuales, llevando la emoción de los conciertos y partidos al hogar del espectador. Además, algunas aplicaciones de citas como Nevermet y Flirtual ya ofrecen servicios en el Metaverso. En los próximos cinco años, habrá una mayor oferta de actividades interactivas y con una

experiencia “envolvente” a través de avatares digitales.

► **Las marcas se expresarán de nuevas formas.** Las experiencias virtuales de los clientes se convertirán en algo habitual, ya que las marcas buscarán formas nuevas y más impactantes de relacionarse con sus clientes. Grandes marcas como Louis Vuitton, Adidas, Gucci, Coca-Cola y Nike, junto con empresas automovilísticas como Nissan, Toyota y Ferrari, ya están experimentando con entornos virtuales y realidad aumentada. En los próximos cinco años, DXC espera que cada vez más marcas ofrezcan a sus clientes la oportunidad de explorar sus marcas, soluciones y servicios en 3D desde cualquier lugar en el mundo.

► **La contratación y la incorporación sufrirán una metamorfosis.** Reclutar talento es esencial para el éxito de cualquier empresa, y llegar a él es el primer paso. En los próxi-

mos cinco años, las organizaciones recurrirán cada vez más al Metaverso para conectar con los candidatos de forma atractiva y seductora. El Metaverso también puede ser bueno para fomentar la inclusión, ayudando también a facilitar la integración de empleados de perfiles más introvertidos. Celebrar la primera ronda de entrevistas en el Metaverso puede ayudar a los responsables de la contratación a identificar a los candidatos con el perfil de comportamiento adecuado, y no limitarse a los que tienen las credenciales o el aspecto adecuados en su currículum. ■

MÁS INFO +

- » [Ordenando el Metaverso. Claves para no quedarte fuera del ciclo de innovación](#)
- » [Metaverso, el espacio virtual que liderará la nueva revolución digital](#)



COMPARTIR EN REDES SOCIALES

7 DE CADA 10 EMPRESAS DE TI PLANEAN REALIZAR FUSIONES Y ADQUISICIONES EN 2023

rente a la alta inflación, la crisis energética y la caída de la confianza del consumidor, la mayor oportunidad para las empresas de tecnología en 2023 es adoptar una estrategia activa de fusiones y adquisiciones (M&A), según el informe de EY [“Top 10 opportunities for technology companies in 2023”](#). Esto está respaldado por un estudio reciente de EY, que encuentra que el 72% de los CEO de tecnología encuestados planean realizar fusiones y adquisiciones en los próximos 12 meses, en comparación con el 59% de los CEO de todas las industrias.

Según Olivier Wolf, EY Global TMT Strategy and Transactions Leader, “el mercado de acuerdos se ha desacelerado debido a los vientos



Las adquisiciones transformadoras podrían lanzar a las empresas de tecnología a nuevos mercados o verticales adyacentes, y fortalecer sus carteras con tecnologías de vanguardia. El 78% de las empresas de tecnología planean desacoplar la cadena de suministro, mientras aumenta la presión para retener a los mejores talentos.

macro en contra y la volatilidad financiera, pero esto ha mejorado las oportunidades para los compradores corporativos con balances sólidos. A su vez, la competencia por los objetivos debería calentarse nuevamente el próximo año, a medida que cientos de miles de millones de dólares de capital privado lleguen al mercado. Las adquisiciones transformadoras podrían lanzar a las empresas de tecnología a nuevos mercados o verticales adyacentes. como HealthTech, y las adquisiciones crecientes tienen el potencial de fortalecer las carteras con tecnologías de vanguardia. como la inteligencia artificial”.

La lista completa de oportunidades para el sector en 2023 incluye:

- ▶ Acelerar la ejecución de la estrategia de fusiones y adquisiciones para afianzar el crecimiento
- ▶ Experimentar con ecosistemas de plataformas
- ▶ Reducir la localización
- ▶ Priorizar la sostenibilidad ambiental
- ▶ Introducir el pago por uso para atraer fuentes de ingresos complementarias
- ▶ Aprovechar las herramientas de análisis para optimizar los ingresos

- ▶ Invertir en el ecosistema edge para mejorar las operaciones y las experiencias
- ▶ Garantizar la protección de datos
- ▶ Impulsar una estrategia de talento ágil
- ▶ Prepararse para la reforma global del impuesto mínimo

OPORTUNIDADES Y RETOS PARA EL SECTOR TI

Las mejoras en la cadena de suministro en los últimos años se han visto frustradas por un deterioro del clima político, económico y financiero. La tercera gran oportunidad en el ranking de este año es que las empresas tecnológicas reduzcan su dependencia de geografías geopolíticamente inestables duplicando la localización. Y los ejecutivos de tecnología encuestados están de acuerdo, con el 78% planeando desacoplar su cadena de suministro, incluida la relocalización y el nearshoring.

La oportunidad para que las empresas construyan una estrategia de talento ágil se encuentra en la novena posición del ranking. Hasta hace unos meses, el mayor desafío de la fuerza laboral para las empresas tecnológicas era “La Gran

Dimisión”. Impulsado por una reorientación en las prioridades laborales durante la pandemia de la COVID-19, el 56% de los empleados del sector indicaron que estaban considerando dejar su puesto actual en busca de salarios más altos, mejores programas de bienestar y nuevas oportunidades profesionales. Hoy en día, el sector no solo está lidiando con la escasez de talento para impulsar su crecimiento a largo plazo, sino también con congelaciones de contrataciones y rondas de despidos en respuesta a la incertidumbre económica.

El informe predice además que la sostenibilidad ambiental (cuarta posición en el ranking) tendrá un impacto en el sector tecnológico en 2023 más que en años anteriores, a medida que las empresas se adaptan para cumplir con la regulación entrante sobre divulgación de emisiones y riesgos de cambio climático. Y un nuevo participante en la séptima posición es el potencial de que la computación edge alcance la madurez en los próximos 12 meses para aquellas empresas que estén dispuestas a invertir en nuevas arquitecturas de TI. ■

LAS MEJORAS EN LA CADENA DE SUMINISTRO EN LOS ÚLTIMOS AÑOS SE HAN VISTO FRUSTRADAS POR UN DETERIORO DEL CLIMA POLÍTICO, ECONÓMICO Y FINANCIERO

MÁS INFO +

- » [La tasa de inversión en el sector tecnológico en España es de solo el 7%](#)
- » [Los inversores ven la industria de TI como una oportunidad de alto rendimiento](#)
- » [Oportunidades para empresas TI en 2023](#)



COMPARTIR EN REDES SOCIALES

#TENDENCIAS

¿QUÉ ESPERAR DE 2023 EN TÉRMINOS DE CIBERSEGURIDAD?

➤ REYES ALONSO

Faltan en torno a 3,4 millones de profesionales de ciberseguridad en el mundo, lo que es un problema en un contexto de aumento de las ciberamenazas, no solo en 2023, sino en los próximos cinco años.

Para los expertos de DXC Technologies, tanto los ciberdelincuentes como los profesionales de la ciberseguridad utilizarán la inteligencia artificial (IA) en una batalla de ingenio cada vez más sofisticada. En el caso de la defensa de la ciberseguridad, la tecnología se ha utilizado principalmente para identificar patrones de comportamiento sospechoso ya que, debido al volumen de actividad sospechosa y al número de falsos

positivos, el personal de ciberseguridad se ve a menudo desbordado.

CRECIENTE PAPEL DE LA IA

La buena noticia es que, a partir de 2023, deberíamos poder empezar a automatizar los controles de seguridad y los mecanismos de respuesta basados en IA, lo que nos ayudaría a reaccionar con mayor rapidez y precisión ante los ciberataques, reduciendo los posibles tiempos de inactividad y protegiendo



do los datos personales y empresariales críticos.

En una segunda previsión destacan que 2023 va a ser un año importante para el metaverso, con Meta, Microsoft, Virbela y otros apostando por la generalización de los mundos virtuales. Sin embargo, la actividad en el metaverso puede plantear problemas de legitimidad: ¿cómo saber si la persona con la que crees que estás hablando es quien dice ser? “Los certificados digitales basados en blockchain ayudarán a asegurar las transacciones virtuales en el metaverso. Lo que está claro es que a medida que el metaverso se expande, también

lo hacen los riesgos”, explica Mark Hughes, presidente de Security.

ENTORNO COMPLICADO

Por otro lado, subraya DXC que el ataque de Rusia a Ucrania nos ha recordado de la manera más cruda posible, que la guerra es ahora híbrida y que los riesgos de ciberataques por motivos geopolíticos son reales. Como resultado, muchas pólizas de ciberseguros se están actualizando para excluir los actos de ciber guerra, lo que plantea retos para la mitigación del ciber-riesgo.

Con las persistentes tensiones geopolíticas, esta amenaza continuará e irá más allá de 2023. De

hecho, con más de 70 países en los que se celebrarán elecciones legislativas en 2023, será un año difícil para las defensas de ciberseguridad.

En la cuarta predicción alerta de los ataques a las infraestructuras nacionales críticas. En este sentido, cuando se va la luz o se corta el gas, es poco probable que la mayoría de la gente piense que es el resultado de un fallo de ciberseguridad industrial. Sin embargo, la realidad es la tecnología operativa (OT) es un campo de batalla emergente para los ciberataques, ya que los sistemas que controlan y automatizan las fábricas y la infraestructura civil, incluidas las centrales eléctricas y las presas, se están convirtiendo en un objetivo.

Por último, la firma destaca que aumentarán las oportunidades profesionales en ciberseguridad. Se calcula que en el mundo faltan unos 3,4 millones de trabajadores en ciberseguridad. Esta escasez en un escenario de incremento de las amenazas será un problema en los próximos cinco años.

SIETE FACTORES QUE IMPULSAN LA RESILIENCIA EN CIBERSEGURIDAD

Para hacer frente a un panorama de amenazas en constante evolución,

EL 96% DE LOS EJECUTIVOS IDENTIFICAN LA RESILIENCIA EN SEGURIDAD COMO UNA ALTA PRIORIDAD

la ciber-resiliencia se vuelve clave, según un estudio de Cisco, que confirma que es una de las principales prioridades empresariales. De hecho, el 96% de los más de 4.700 directivos encuestados por la compañía en 26 países identifican la resiliencia en seguridad como una alta prioridad.

Entre los participantes, un 62% reconoció haber sufrido un ataque reciente, con consecuencias en sus operaciones internas, la continuidad de las TI, cortes en la cadena de suministro o daños reputacionales. Por tanto, ahora la premisa es prevenir los ciberincidentes y estar preparados para mitigar las pérdidas cuando se producen.

Apoyándose en una metodología para generar una puntuación de resiliencia en seguridad, Cisco ha identificado siete factores que ayudan a una organización a impedir

incidentes, resistir ante ellos y recuperarse lo antes posible:

1 Conseguir el apoyo de la alta dirección: no será posible sin el soporte de los ejecutivos C-Suite es deficiente. Las organizaciones que admiten un escaso apoyo a la seguridad por parte de los directivos obtuvieron, según la metodología de Cisco, han obtenido una puntuación un 39% inferior a la de aquellas con un fuerte soporte ejecutivo.

2 Crear una cultura de seguridad: las compañías que afirman tener una cultura de seguridad excelente han logrado una puntuación media un 46% superior a las que no la tienen.

3 Mantener personal y recursos internos adicionales para responder a los incidentes: estas compañías suman un 15% más de resiliencia.

4 Reducir la complejidad de las migraciones a cloud y la gestión de entornos de nube híbrida: en este punto, merece la pena destacar que las empresas cuyas infraestructuras tecnológicas son mayoritariamente locales o basadas en la nube han obtenido las puntuaciones más altas, y casi idénticas, en materia de resiliencia de seguridad. Sin embargo, las empresas que se encuentran en las fases iniciales de la transición

de un entorno local a uno híbrido en el cloud han visto caer sus puntuaciones entre un 8,5% y un 14%, dependiendo de la dificultad de gestión de los entornos híbridos.

5 Implementar un modelo Zero Trust maduro: si lo hacen, aumentan un 30% su puntuación en resiliencia.

6 Disponer de capacidades avanzadas de detección y respuesta extendida: esto ayuda a incrementar la resiliencia en un 45%.

7 Converger las funcionalidades de red y seguridad en una arquitectura SASE: así aseguran el perímetro de la red y garantizan el acceso seguro, y se produce un aumento del 27%. ■

MÁS INFO +

» [Tendencias de ciberseguridad para blindar a las empresas](#)

» [Security Outcomes Report](#)



COMPARTIR EN REDES SOCIALES

Ciberseguridad 2023: Tendencias

El uso de la Inteligencia Artificial y el Machine Learning ayuda a las empresas a defenderse contra ataques nuevos o desconocidos.



Server Breach Detection System (sBDS)

I-Series



#EN PORTADA

> ARANTXA HERRANZ

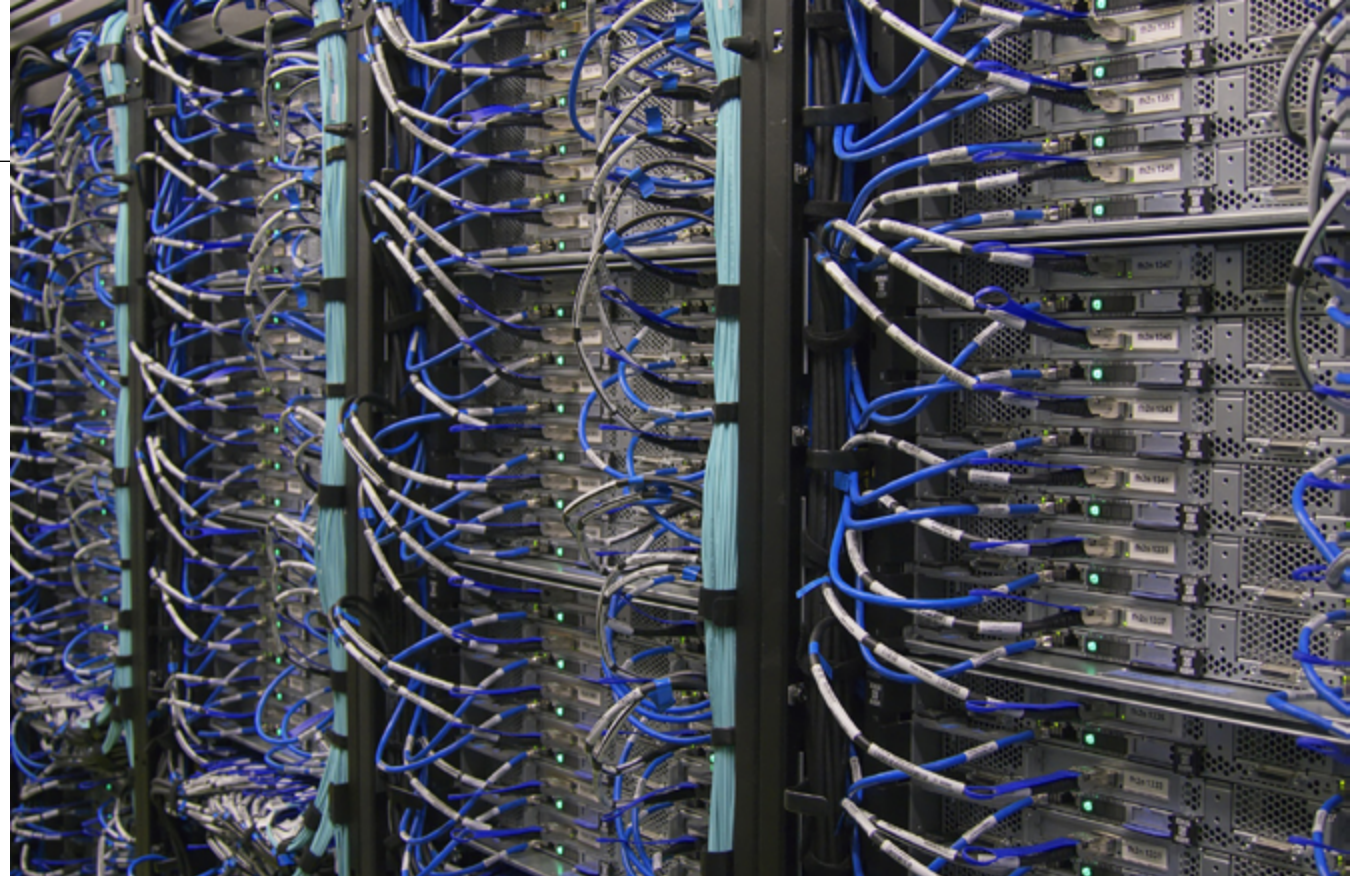
**LA NUBE,
¿el nuevo legacy
de las empresas?**

La tecnología siempre ha sido estratégica para las empresas. Buena parte de su competitividad empresarial ha ido ligada al uso de productos y herramientas TIC. Tradicionalmente, las empresas realizaban unas inversiones estratégicas en determinados productos (tanto hardware como software), desarrollando unos planes a largo plazo en TI. Eran sistemas que debían dar soporte a sus negocios de forma silenciosa y eficaz durante años y años.

Sin embargo, la cada vez mayor aceleración digital ha provocado que muchos de esos planes quedaran obsoletos y que esas estrategias deban ser más cortas en el tiempo. De hecho, para muchas empresas, estas inversiones anteriores pueden llegar a convertirse en costosos quebraderos de cabeza porque este legacy, estos sistemas heredados, son una gran sangría de recursos, especialmente económicos. [Se calcula](#) que tres cuartas partes de los 35 billones de dólares que las empresas se han gastado en tecnología desde 2010 se han destinado al funcionamiento y mantenimiento de los sistemas existentes. Al menos 2,5 billones de

dólares se han gastado en intentar sustituir los sistemas informáticos heredados, de los cuales unos 720.000 millones se han malgastado en esfuerzos de sustitución fallidos.

[Un informe elaborado en el Reino Unido](#) también pone de manifiesto que dos de cada tres (67%) responsables de TI del sector público creen que los problemas de infraestructura heredada están frenando sus esfuerzos de transformación digital. Algo que lleva a firmas como IDC a asegurar que hasta el 65% de las empresas modernizarán agresivamente los sistemas heredados con inversiones en nuevas plataformas tecnológicas como la nube hasta 2023.



QUÉ ES EL LEGACY

Se entiende por legacy, o sistemas heredados, cualquier sistema informático, hardware o software obsoleto que sigue en uso.

Sin embargo, no todos los sistemas heredados son tecnologías obsoletas. La mayoría de los sistemas heredados funcionan aunque estén anticuados, y las empresas suelen seguir utilizando sistemas heredados que son fundamentales para sus funciones diarias y sus necesidades empresariales.

Así pues, las características que hacen que una tecnología pueda considerarse como legacy son:

- ▶ Ya no reciben actualizaciones, soporte o mantenimiento de sus desa-

rolladores o creadores de software.

- ▶ Ya no están disponibles para su compra o dependen de tecnología obsoleta para funcionar y mantenerse.

- ▶ En el caso de hardware como los mainframes, ya no son capaces de soportar el software de una organización.

- ▶ Para su mantenimiento, el sistema requiere profesionales de TI con conocimientos tecnológicos complejos y en gran medida obsoletos, como la programación en Common Business-Oriented Language, o COBOL. Estos profesionales pueden ser difíciles de encontrar y costosos de contratar.

- ▶ Las reparaciones llevan demasiado tiempo en comparación con los sistemas nuevos.

► Los costes de mantenimiento se vuelven demasiado excesivos para continuar.

► Están sobreexpuestos a vulnerabilidades de seguridad y no pueden actualizarse para cumplir las normas modernas de ciberseguridad.

La mayoría de las empresas utilizan aplicaciones y sistemas informáticos heredados que siguen atendiendo necesidades empresariales críticas. Normalmente, el reto consiste en mantener en funcionamiento la aplicación heredada al tiempo que se convierte a un código más nuevo y eficiente que haga uso de la tecnología y los lenguajes de programación actuales.

POR QUÉ PERMANECE EL LEGACY

Las organizaciones siguen utilizando sistemas y aplicaciones heredados por varias razones. En primer lugar, porque siguen funcionando. De hecho, no es solo que muchos sistemas y aplicaciones heredados funcionan, sino que siguen siendo importantes para las funciones diarias de una empresa. Sustituir sistemas y tecnologías que siguen funcionando simplemente porque están anticuados no siempre es necesario.

Además, el coste de sustituir un sistema o aplicación heredados

puede ser elevado. Aunque mantener los sistemas heredados puede costar más dinero a las empresas a largo plazo, algunas organizaciones no disponen de recursos inmediatos para modernizar sus sistemas. La actualización también puede requerir largos periodos de tiempo, el reciclaje del personal o la contratación de personal para aprender e integrar las nuevas tecnologías. Algunas organizaciones también conservan sistemas anticuados porque aún no han recuperado la inversión realizada en ellos.

También hay que tener en cuenta que modernizar los sistemas heredados puede ser una empresa compleja. Algunas organizaciones carecen de los conocimientos necesarios para modernizar sus sistemas

y hacer frente a los retos que pueden surgir al hacerlo. Los retrasos en el servicio, la pérdida de datos y la mala experiencia del usuario también pueden ser consecuencia de las migraciones.

EL SALTO A LA NUBE

Las organizaciones de todo el mundo están reemplazando algunos de sus sistemas locales, especialmente los legacy, por la nube con la esperanza de ver cumplidas las promesas de una potencia informática flexible, escalable y rentable. Desde la reducción de los costes de TI hasta la aceleración de la innovación, hay muchas razones de peso para embarcarse en un viaje de migración a la nube. Sin embargo, hacer la tran-

sición no es fácil sin un plan bien elaborado y experiencia en la nube.

Algunas de las razones principales por las que las organizaciones migran a una plataforma en la nube son la reducción de los costes de TI, el aumento de la agilidad empresarial, mejorar la seguridad, eliminar las preocupaciones sobre el final de la vida útil de la tecnología, llevar a cabo una consolidación de los centros de datos o aprovechar las nuevas tecnologías.

En nuestro país, más del 32% de las empresas españolas compran algún servicio de cloud computing, [según los datos del INE](#) (Instituto Nacional de Estadística), que también pone de manifiesto que, cuantos más empleados tiene el negocio, más se emplea la nube.



EL COSTE DE LA TRANSFORMACIÓN

Al fin y al cabo, cuando las empresas apuestan por la nube siempre se entiende que están fomentando la transformación digital de sus negocios. Sin embargo, y pese a esto cantos de sirena sobre las bondades del cloud computing, la experiencia está mostrando que no todas las promesas se cumplen y que, incluso, los costes del cloud, lejos de ser menores, puede ser incluso mayores.

“Se ha invertido mucho en esta transformación digital y en la nube, pero se perdido el control de lo que se está haciendo”, asegura Ángel Pineda, CEO de Orizon. Tanto que, según sus palabras, “el cloud se ha ido de las manos. No se sabe dónde está y lo que cuesta”, lo que está

conllevando que algunas empresas reconozcan que el presupuesto que tenían para tres años se ha ido en uno. En su opinión, esto se debe a que la nube no es más barata, tal y como se ha defendido siempre. Entre otras razones, porque para poder sacar partido de esta tecnología también se necesitan perfiles nuevos. “Hay muchos costes ocultos”, asegura. Tanto que, después de haber hablado con más de una treintena de directivos de grandes empresas en el último mes, Pineda asegura que muchos de ellos “se plantean si tienen que estar o no” en la nube.

En este caso, seguir con un sistema heredado puede resultar más

barato y menos molesto que pasarse a un servicio en la nube de pago por uso. Algo por lo que las empresas apuestan por esos modelos híbridos en los que parte de la tecnología reside en local y otra parte se ha trasladado a la nube.

Como veíamos antes, cuando una tecnología se vuelve muy costosa de mantener y exige que haya unos profesionales dedicados muy específicos, puede considerarse que estamos ante un legacy. Y son dos parámetros que, como estamos viendo, también se pueden aplicar al cloud computing. Por eso, en opinión de Pineda “el cloud es el nuevo legacy de las empresas”. Es más, considera que

los proveedores de la cloud pública “no han hecho nada que no hicieran en su momento los fabricantes de servidores y mainframe”

CONTROLAR CON FINOPS

Así pues, no es de extrañar que solo el 20% de empresas consideran su migración al cloud como un éxito y que solo el 9% considere que este movimiento ha conllevado efectivamente, el prometido ahorro de costes. De hecho, en ese 80% de empresas para las que el salto a la nube no ha sido un éxito, esta adopción ha conllevado un aumento de los costes de entre un 20 y un 50%.

Parte del problema, a ojos de Óscar Ferrer, responsable del equipo de Goodly en Paradigma Digital, es que no se ha cambiado el modelo. Es decir, que las empresas han trasladado su forma de operar de on-premise a la nube sin tener en cuenta que las reglas del juego no tienen por qué ser las mismas, por lo que las estrategias de “lift and shift” (subir los sistemas a la nube sin más) no son adecuadas. “El problema no es el cloud sino el uso que se hace de la nube”, asegura. Eso sí, este experto reconoce que, como pasa con los sistemas heredados que residen en

SOLO EL 20% DE EMPRESAS CONSIDERAN SU MIGRACIÓN AL CLOUD COMO UN ÉXITO Y SOLO EL 9% EXPERIMENTA UN AHORRO DE COSTES



un mainframe o en un ERP complejo, “salir del cloud no es fácil” por lo que considera que “es momento de aprovechar sus posibilidades”.

En cualquier caso, este aumento de los costes asociados la uso del cloud computing va a conllevar, según Ferrer, que en 2023, se vaya a hablar mucho de FinOps, un marco de trabajo para llevar la educación financiera a todos los departamentos de negocios.

FinOps es una disciplina de gestión de la nube pública que permite a las organizaciones obtener el máximo valor empresarial de la nube ayudando a los equipos de tecnología, finanzas y negocio a colaborar en la toma de decisiones de gasto basadas en datos. Los defensores y profesionales de FinOps subrayan que la suya es una filosofía de gestión financiera de la nube. El elemento central de esta práctica de gestión es la aplicación de controles de costes a los despliegues en la nube, preservando al mismo tiempo el acceso de los desarrolladores a los recursos de la nube.

Sin embargo, los gastos operativos de la nube pueden ser muy variables y descontrolarse rápidamente. Por ejemplo, los individuos o grupos de la

organización pueden adquirir servicios o instancias en la nube independientemente unos de otros, sin una supervisión o coordinación de alto nivel.

Esa desconexión puede llevar a un aprovisionamiento excesivo para un conjunto de cargas de trabajo y a un aprovisionamiento insuficiente para

otro. Cualquiera de estos resultados puede provocar un sobrecoste sustancial, cuando un esfuerzo más coordinado podría haber producido una solución adecuada a un coste menor. Los silos organizativos y la dispersión geográfica pueden agravar aún más la mala gestión de los

recursos en la nube, especialmente en empresas multinacionales y conglomerados.

Para Ferrer, FinOps está compuesto de tres etapas: visibilidad de todos los gastos en la nube en todos los equipos; optimizar todos los mecanismos; operar y predecir los gastos y hacer recomendaciones y predicciones, pero también sistema de atribuciones de cada proceso y unidad de negocio con el retorno de la inversión. ■

CUANDO UNA TECNOLOGÍA SE VUELVE MUY COSTOSA DE MANTENER Y EXIGE QUE HAYA UNOS PROFESIONALES DEDICADOS MUY ESPECÍFICOS, PUEDE CONSIDERARSE QUE ESTAMOS ANTE UN LEGACY



MÁS INFO +

- » [La realidad oculta del legacy en los sistemas TI](#)
- » [Infraestructura heredada, freno a la Transformación Digital](#)
- » [Cloud Computing en la empresa española, según el INE](#)



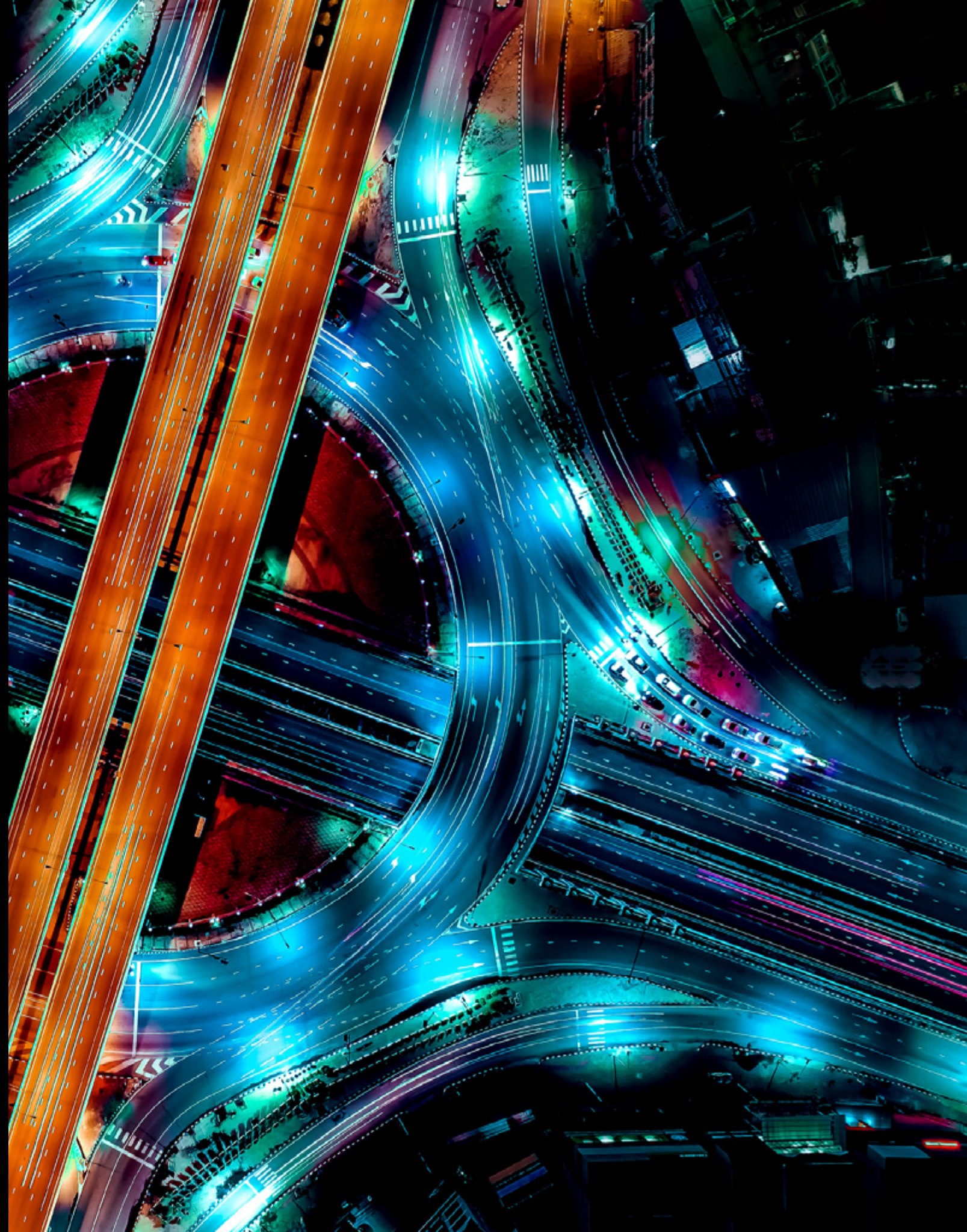
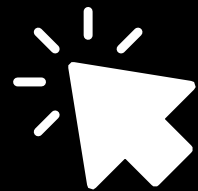
COMPARTIR EN REDES SOCIALES

La distancia más corta entre innovación y realidad

Ayudamos a empresas de todos los tamaños e industrias a desarrollar las soluciones de TI más potentes, prácticas y completas, integrando múltiples proveedores.

ARROW

arrow.com/ecs/es



ESCASEZ DE TALENTO TECNOLÓGICO: EL GRAN DESAFÍO DEL CANAL

➤ HILDA GÓMEZ

Hoy en día, las organizaciones se enfrentan a un problema de oferta y demanda de talento tecnológico, lo que supone un desafío, especialmente a la hora de atraer y retener a los profesionales. Con un enfoque cada vez mayor en la automatización de TI, la seguridad y la IA/ML, los líderes de TI empresariales están legítimamente preocupados por el hecho de que el progreso en estas importantes iniciativas podría estancarse sin las habilidades y el talento adecuados. Lo mismo ocurre entre las empresas que conforman el canal de distribución TI, que deben competir con compañías de otros sectores por captar a los profesionales tech necesarios para ejercer su labor con garantías.

Al igual que el año pasado, las empresas seguirán luchando en 2023 con el talento y las brechas de habilidades. Según la última Encuesta de Población Activa, en nuestro país la tasa de paro se sitúa en un 12,7%. Sin embargo, paradójicamente, 8 de cada 10 empresas tienen dificultades a la hora de reclutar talento para su compañía y un 10% de los puestos de trabajo se quedan sin cubrir. De hecho, según los datos más recientes del Instituto Nacional de Estadística, en 2021 el 47% de las empresas españolas tuvo dificultades para cubrir alguna vacante de especialista en TIC, porcentaje que asciende hasta el 77% en las compañías con más de 250 trabajadores.

BRECHA LABORAL

El sector tecnológico es el que más puestos de trabajo generó el pasado año, representando un 17% de las vacantes de empleo y con perfiles que tienen una tasa de paro del cero al 4%. No es de extrañar teniendo en cuenta que la necesidad de digitalización llega a todos los sectores. De hecho, el “Informe de presupuestos IT 2022 y estimación 2023”, llevado a cabo por LiceoTIC Training, desvela que las empresas esperan aumentar el número

de empleados del sector TI en más de un 6%. Dicho estudio señala que el sector que más va a apostar en 2023 por profesionales TI es distribución y retail (12%).

Según datos de la Comisión Europea, de cara a 2030 los empleos relacionados con la tecnología, entre los que se encuentra el sector digital, crecerán un 11%, con la creación de más de 300.000 puestos de trabajo. Sin embargo, la Asociación de Empresas Tecnológicas DigitalEs afirma que España tiene actualmente más de 120.000 vacantes tecnológicas sin cubrir.

La escasez de perfiles está comportando que las empresas ofrezcan re-

tribuciones más altas y, actualmente, el sueldo medio de un trabajador del sector digital se sitúa en los 38.500 euros anuales, cifra notablemente superior a la media española. Esta situación, teniendo en cuenta la consolidación como hubs tecnológicos de ciudades como Madrid o Barcelona, donde los profesionales tech cobran un 30% más que en el resto de ciudades españolas; y el afianzamiento del teletrabajo, que alcanza un 40% de penetración en las profesiones digitales, deja una gran brecha laboral disponible para todos aquellos profesionales que cuentan con las capacidades digitales más demandadas.

Tampoco hay que olvidar que el sector de las TIC ha experimentado una fuga de hasta 100.000 profesionales desde 2008. Se trata de profesionales que han encontrado mejores oportunidades en países europeos como Alemania, Francia, Inglaterra o Irlanda, donde los sueldos a menudo doblan o triplican los ofrecidos en España. Así pues, la fuga de talento está estrechamente relacionada con las condiciones laborales de los profesionales tech. “En España el talento digital está encontrando oportunidades laborales fuera del país”, denuncia Gary Mullan, director de Prosperity Digital.

A todo lo anterior se suma que los trabajadores de TI están más inclinados a renunciar a sus trabajos que los empleados con otras funciones, con un 10,2% menos de intención de quedarse que los empleados que no son de TI, la más baja de todas las funciones corporativas, según una encuesta de Gartner. A nivel mundial, solo el 29,1% de los trabajadores de TI tiene la intención de permanecer en su empleo actual, mientras que, en Europa, solo el 38,8% tiene la intención de quedarse, lo que exacerba el problema de la captación y retención de talento.

“**VENÍAMOS
ARRASTRANDO UN DÉFICIT
DE PROFESIONALES TI QUE
LA CRISIS DE LA COVID-19
HA ACENTUADO**”

JUAN UZAL,
director de consultoría
estratégica de **CE Consulting**



IMPULSO TECNOLÓGICO

Es evidente que la infraestructura económica española está pisando el acelerador para no quedarse atrás en la incorporación de talento digital, una cuestión imprescindible para adaptar las organizaciones a un contexto marcado por los beneficios que aporta la aplicación de las nuevas tecnologías.

En este sentido, cabe señalar que la Comisión Europea estima que, a corto plazo y con la puesta en marcha del Plan de Recuperación, Transformación y Resiliencia, en España será necesario incorporar 135.000 nuevos especialistas. Así pues, esta demanda laboral aumentará impulsada por la inyección económica que supondrán los Fondos Next Generation, especialmente a través del programa Kit Digital orientado a la digitalización de las pymes, que contempla una inversión de 3.000 millones de euros.

“Los fondos Next Generation quieren acelerar un proceso ya existente, que es el de la digitalización de todos los sectores, lo que ayuda aún más a que el mercado busque desesperadamente perfiles digitales de casi cualquier tipo”, apunta Gary Mullan, de Prosperity Digital. “La incorporación de perfiles digitales impulsa y ayuda a las compañías a realizar su proceso

de transformación digital de un modo más ágil y efectivo”.

En la misma línea, según recoge el estudio ‘Empleabilidad y Talento Digital 2021’ realizado por la Fundación VASS y la Universidad Autónoma de Madrid, las compañías reconocen que podrían crear un 20% más de empleo en áreas vinculadas a la tecnología si hubiera más perfiles aptos y disponibles.

Las empresas de TI no escapan a esta búsqueda de profesionales. Pese a las noticias de despido de empleados en grandes multinacionales tecnológicas como Meta, Twitter y Amazon, los índices de empleabilidad se mantienen elevados. Como señala el último barómetro TIC Monitor, elaborado por VASS y el Centro de Predicción Económica CEPREDE, el 77% de los empresarios del sector de servicios TIC seguirá aumentando sus plantillas a corto plazo.

La evolución en cuanto a la demanda de talento especializado en el sector español de servicios TI se mantiene igualmente robusta, con un incremento interanual del 8,2%. “El sector de servicios digitales en España cuenta ya con 39.000 afiliados más que en diciembre de 2021, y alcanza las 433.000 personas empleadas en todo el país”, afirma Antonio Rueda,



HACIA LA IGUALDAD LABORAL

A la brecha digital existente hay que añadir otra brecha, la de género, que en el sector TI es preocupante. En España solamente un 5,7% de las empresas cuentan con mujeres expertas en tecnología o digitalización. La situación de brecha de género es especialmente grave en áreas como, por ejemplo, programación, en la que solo un 20% de los programadores son mujeres, frente al 80% representado por hombres.

Según datos de Closingap, al ritmo en el que se están incorporando las mujeres en el sector digital, se lograría terminar con la brecha de género en 2058. La necesidad de acelerar la incorporación de las mujeres en las profesiones digitales es crucial, especialmente si se tiene en cuenta la gran demanda que hay de este tipo de perfiles, así como la previsión de aumento de esta demanda.

En muchas ocasiones, a las dificultades de acceso al puesto laboral se suma también una brecha salarial, lo que no es tan frecuente dentro del sector digital. “Las profesiones digitales, así como las startups reconocidas, tienden a remunerar económicamente de forma equitativa a su equipo de trabajo, ya que temas como la diversidad o la igualdad de género están muy presentes dentro de las agendas de estas compañías. Aun así, hay camino todavía por recorrer en el sector digital en general”, recalca Gary Mullan, de Prosperity Digital.

Revertir esta situación es clave y las empresas pueden hacer mucho para fomentar la igualdad salarial, así como la puesta en valor de las figuras femeninas dentro de la empresa, con tal de construir referentes y motivar a otras mujeres a formarse en materia tecnológica y ejercer de ello.

director de VASS Research y responsable de TIC Monitor.

PERFILES MÁS SOLICITADOS

Dentro del sector TIC hay perfiles claramente diferenciados. Aunque algunos de los más demandados corresponden a profesiones con larga trayectoria en el panorama laboral, hay otros puestos generados de manera más reciente al calor de los avances en tecnología de la última década. De cualquier modo, hay posiciones muy demandadas en estos momentos y que el mercado no es capaz de cubrir por falta de la capacitación digital adecuada, estos son algunos de ellos:

► **Desarrolladores.** Es decir, profesionales especializados en el pre-desarrollo y desarrollo de aplicaciones o diferentes tipos de software. Se necesitarían cubrir en estos momentos más de 40.000 puestos en este ámbito, según la Asociación Española para la Digitalización.

► **Especialistas en sistemas, hardware y CPD (Centro de Procesamiento de Datos).** En este caso, según la patronal, hay 25.000 puestos vacantes para profesionales formados en instalación y mantenimiento de este tipo de infraestructuras.

► **Expertos en ciberseguridad.** Se estima que en España son necesarias 25.000 personas formadas en ciberseguridad en estos momentos. Es uno de los puestos imprescindibles para las empresas que están en plena transformación.

► **Especialistas en cloud computing.** El mercado laboral precisa más de 8.000 profesionales de la tecnología en la nube. El éxito del cloud computing o del software que se almacena en un entorno visual es una realidad. Las empresas encuentran mayor flexibilidad y agilidad al operar desde cualquier sitio y momento gracias a la ventaja de la conectivi-

“ LA ESCASEZ DE PERFILES TI ES UNA REALIDAD QUE AFECTA AL SECTOR, Y CADA AÑO PARECE SER MÁS GRANDE ”

JOAN RAMÓN GUILLÉN,
gerente de desarrollo de negocios de **Izertis**

dad. Esto ha generado la necesidad de una gran cantidad de perfiles expertos en esta tecnología.

► **Técnicos de big data.** Su función está en la identificación, procesamiento, análisis y explotación de volúmenes ingentes de datos a través de la tecnología. Es otro de los perfiles con más empleabilidad a presente y futuro porque son necesarios 5.000 profesionales en este ámbito.

De acuerdo con WTW España, los roles tecnológicos más demandados en 2022 entre las compañías de ámbito multisectorial han sido los de desarrolladores de ciberseguridad, data scientists, program managers y

project managers. En el caso de las empresas especializadas en el sector TIC, el perfil de desarrollador de ciberseguridad es también el más demandado, seguido por los de program manager, ingeniero/desarrollador de software y diseñador UX.

Si nos centramos en las capacidades (skills) más requeridas por las compañías de ámbito multisectorial para los perfiles tecnológicos, destacan aquellas relacionadas con Python, SQL, la seguridad de la información y la computación en red. Por su parte, las compañías puramente tecnológicas demandan especialmente skills ligadas a inteligencia artificial, Python, machine learning y la computación en red.

REPERCUSIÓN EN EL CANAL

Pese a los buenos datos de empleabilidad en el sector de servicios TIC, las empresas de consultoría e integradoras no son ajenas a la escasez de especialistas. Preguntados acerca de cómo solventan el problema, Juan Uzal, director de Consultoría estratégica de CE Consulting, reconoce que “veníamos arrastrando un déficit de profesionales TI que la crisis de la COVID-19 ha acentuado, al acelerar los procesos de transformación digital.



ESPAÑA TIENE ACTUALMENTE MÁS DE 120.000 VACANTES TECNOLÓGICAS SIN CUBRIR

Para hacer frente a esta escasez no existen recetas mágicas, pero desde CE Consulting creemos que hay que poner el foco en dos flancos: la captación y la retención”.

Dada la carencia endémica de expertos en nuevas tecnologías, claves para acompañar la transformación digital de los clientes, muchas compañías del sector optan por desarrollar políticas de política de captación, desarrollo y fidelización de talento TIC, sustentadas en la formación continua. Es el caso de Softtek, cuyo director de consultoría, Antonio Gálvez, confirma el desarrollo de “diferentes iniciativas para impulsar los jóvenes talentos en las diferentes ramas de STEM, como universidades, institutos y colegios”.

Gálvez reconoce asimismo que Softtek guarda un gran compromiso con la diversidad en general dentro del mundo laboral. “Por otro lado, para que todos puedan tener oportunidades es importante deslocalizar el talento



existente. Para ello ayudamos a crear las condiciones necesarias a través del territorio español. Así podremos atraer a perfiles TIC y talentos locales que han elegido otro lugar de trabajo o incluso otro trabajo debido al problema de la ubicación de oportunidades”, añade el directivo.

En la misma línea, Manuel Saz, director asociado de Altia, sostiene que “desde Altia impulsamos la formación de jóvenes talentos a través de varios proyectos, como por ejemplo los Altia Tech Day, donde tienen la oportunidad de aprender de forma práctica sobre las tecnologías más disruptivas utilizadas por las compañías que desarrollan proyectos reales. Igualmente, trabajamos para adaptar la formación

a la demanda laboral y animamos a los más jóvenes a formar parte de la transformación digital y a reducir la brecha de género, con nuestros programas GenTech”.

Por último, Joan Ramón Guillén, gerente de Desarrollo de Negocios de Izertis, confirma que “la escasez de perfiles TI es una realidad que afecta al sector, y cada año parece ser más grande. En Izertis hemos encontrado la forma de combatir la falta de especialistas a través del desarrollo de BootCamps especializados en diferentes áreas, en los que se forma a futuros profesionales del sector y donde, además, se les brinda la oportunidad de desarrollar su carrera profesional junto a nosotros”. ■

MÁS INFO +

- » [Se dispara la demanda de perfiles TIC hiperespecializados](#)
- » [Las empresas demandan cada vez más analistas, ingenieros cloud y expertos en IA](#)
- » [El empleo TIC lidera las contrataciones los próximos meses con más del 50% del total](#)
- » [España necesita incorporar 135.000 profesionales tecnológicos a corto plazo](#)
- » [Sólo el 29% de los trabajadores de TI permanecería en su empleo actual](#)
- » [Sólo el 1,6% de las mujeres se dedican al sector de las TI en España](#)



COMPARTIR EN REDES SOCIALES



V-Valley, el punto de referencia para tu negocio

ESPECIALISTAS EN ADVANCED SOLUTIONS

Te acompañamos para ayudarte a potenciar, aún más, tus proyectos de transformación digital dirigidos a clientes finales y Administraciones Públicas. Entra en v-valley.es y accede a la más amplia gama de soluciones y servicios.



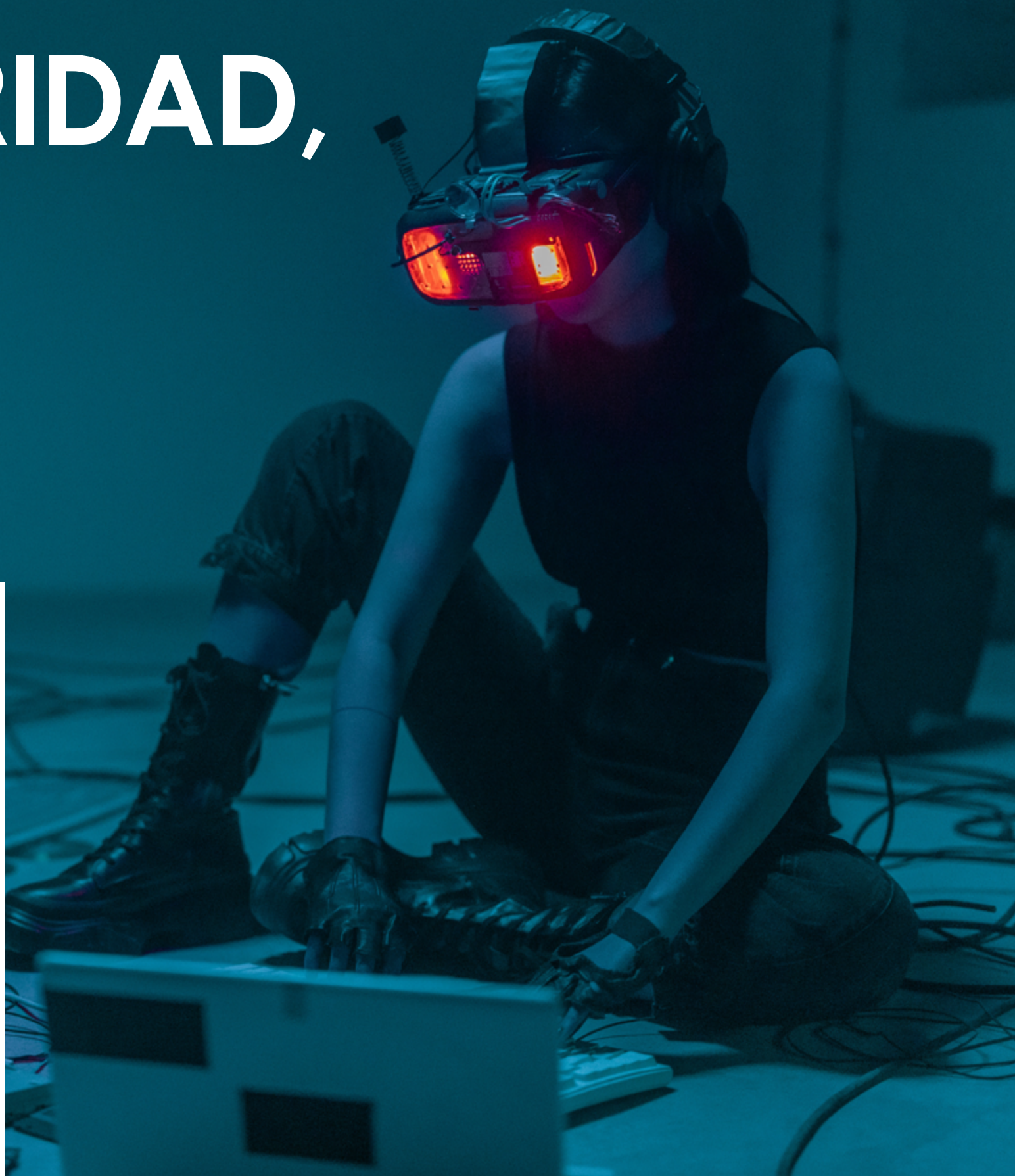
#enhancingyourbusiness

#EN PORTADA

CIBERSEGURIDAD, LA GRAN OPORTUNIDAD EN 2023

➤ DESIRÉE RODRÍGUEZ

“El pueblo que no conoce su historia está condenado a repetirla”. Esta frase, utilizada en innumerables ocasiones por personajes de todo tipo, va a ser la protagonista de este primer reportaje de ciberseguridad de 2023. Y es que, después de leer innumerables listas de predicciones en las que unos y otros parecen haberse hecho con una bola de cristal más típica de la Edad Media que de nuestro tiempo, creo que es necesario dejar de mirar a un futuro cada vez más incierto e intentar aprender del pasado.



Si observamos la historia de los pueblos y la propia humanidad, es fácil concluir que los seres humanos parecemos abocados a repetir constantemente los mismos errores. ¿Por qué no poner el foco, entonces, en aprender del pasado y dejar de lado la bola de cristal? ¿No podría aportarnos mucho más intentar aprender de nuestros errores que imaginar los que cometeremos en los próximos meses?

Sobre todo, si tenemos en cuenta que la realidad, en los últimos años, está demostrando ser mucho más original de lo que cabría esperar. Virus mundiales y guerras cibernéticas han dejado de pertenecer a la esfera cinematográfica para convertirse en nuestra realidad más cruel.

ESTOS SON LOS CIBERATAQUES MÁS IMPORTANTES DE 2022

Acceso remoto, uso seguro de la red, seguridad en las aplicaciones, cadena de suministro... Los aspectos a tener en cuenta cuando hablamos de ciberseguridad se han multiplicado y es por ello por lo que los ciberataques son, cada vez, más numerosos. Para comenzar el año con buen pie queremos aprender del

pasado así que vamos a repasar los ataques más importantes de 2022 y las lecciones que nos han enseñado:

► **La ciber guerra ya no es solo cosa de películas:** La lista de ataques ligados al conflicto entre Rusia y Ucrania es ya inabarcable. Y es que, a los ataques perpetrados por uno u otro país se unen los de hacktivistas que, aprovechando la grave situación, muestran su apoyo a uno u otro bando. En este sentido, Ucrania ha sido objeto de numerosos ataques, que han provocado cortes de energía y propagado malware destructivo. Las instituciones y la infraestructura se han visto afectadas en numerosas ocasiones: WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper... la lista es larga (y se prevé que siga aumentando en los próximos meses.

Por su parte, Rusia también ha sufrido represalias en su entorno. Destacan ataques los ataques de

denegación de servicio y fuga de datos que, entre otras instituciones han afectado a los ferrocarriles locales, RuTube.

► **El cibercrimen paraliza un país:** Un país paralizado, ese fue el resultado de Por primera vez, un país se vio paralizado por culpa del cibercrimen. En abril de este año, Costa Rica tuvo que declarar la emergencia nacional tras sufrir un ciberataque a nivel global que logró paralizar las operaciones financieras de todo un país. No contentos con el resultado, los cibercriminales del grupo Conti, volvieron a actuar en mayo. La víctima en esta ocasión fue la caja de seguridad social nacional.

► **El robo de datos se convierte en un juego de niños:** El 2022 empezó con un ciberataque masivo en el que se vieron envueltos Nvidia, Ubisoft y Samsung. En marzo, la filtración de datos afectaba a Microsoft y en

septiembre, las víctimas eran Uber y Rockstar Games. Detrás del delito se encontraba Lapsus\$, un recién llegado al mundo cibernético, con ganas de llamar la atención. Usan las redes sociales para promocionar su pesca e incluso preguntan por los datos que deberían publicar. Los cabecillas de estas filtraciones eran un joven de 16 años y un adolescente de 17, quienes fueron detenidos junto a otros siete miembros de la organización.

ONG, Hospitales... las infraestructuras médicas son ya una de las dianas favoritas de los cibercriminales:

Lamentablemente, si hablamos de ciberataques a proveedores de atención médica, ONG y hospitales la lista es amplia. En enero, la Cruz Roja Internacional fue víctima de un ciberataque que supuso la interrupción de su servicio afectando a unas 500.000 personas.

Si nos centramos en infraestructuras médicas la lista va desde el Consorci Sanitari Integral (CSI), que incluye varios centros de salud en Barcelona, hasta el hospital de Corbeil-Essonnes en Francia, pasando por Baptist Health System, Resolute Health Hospital, Kaiser Permanente y Yuma Regional Medical Center en EE.UU. e Inglaterra.

EL AÑO 2022 SE VA A CERRAR CON UN INCREMENTO DEL GASTO EN CIBERSEGURIDAD EMPRESARIAL DEL 7,7% HASTA LOS 1.749 MILLONES DE EUROS, Y EL CRECIMIENTO VA A CONTINUAR SIENDO ELEVADO EN LOS PRÓXIMOS EJERCICIOS

Ataques patrocinados por Estados:

Llevamos años diciendo que muchos de los ciberataques que se comenten tienen detrás a países que financian la industria del cibercrimen. En este 2022, los estados-nación han aprovechado su poder para infiltrarse en otros gobiernos y realizar ataques a infraestructuras críticas de “rivales”. Así, la Agencia de Seguridad Cibernética de EE. UU. ha alertado en diversas ocasiones sobre intento de espionaje por parte de China. Por su parte, el país asiático amenaza con reproducir el escenario ucraniano con Taiwán (Beijing no reconoce la independencia de la isla).

Estos son algunos de los principales ataques del pasado 2022, un año que, para muchos expertos ha supuesto un punto de inflexión ya que el auge del cibercrimen ha supuesto un cambio en la forma de ver la seguridad de millones de empresas y usuarios: “Este año ha sido el de la conciencia en ciberseguridad para las empresas, que han sufrido muchos de los problemas que acarrea la falta de seguridad de, por ejemplo, sus dispositivos móviles o del uso de redes domésticas para el trabajo. Aun así, falta mucho por ha-

cer en este campo y hay que tener presente que para ir por delante de las amenazas hay que adoptar un enfoque proactivo en ciberseguridad”, sentencia Mario García, director general de Check Point Software para España y Portugal.

Por su parte, Juan Antonio Rodríguez, jefe del Departamento Contra el Cibercrimen, UCO, asegura que para mejorar la seguridad de empresa y usuarios y minimizar las posibilidades de ser víctima de un ciberataque “hay que desarrollar un sentido común cuando hablamos de ciberseguridad”.

Parece claro que la concienciación con respecto a la importancia de los riesgos digitales ha aumentado, pero todavía queda un largo camino por recorrer para plantar cara a los cibercriminales.

ESTAS SON LAS LECCIONES QUE NOS DEJA 2022 EN MATERIA DE CIBERSEGURIDAD

► **Hay que poner límites a la guerra, también en el terreno cibernético.**

Después de invadir Ucrania en febrero, la relación entre ambos países, ya de por sí bastante belicosa en lo digital, Rusia ha aumentado su presión atacando las instituciones e infraestructuras ucranianas con



SEGÚN DATOS DEL ESTUDIO ESTADO DE LA CIBERSEGURIDAD EN ESPAÑA, DE SECURE&IT, EN UN ESCENARIO DE AMENAZAS EN MÁXIMOS HISTÓRICOS, EL 51,3% DE LAS COMPAÑÍAS TIENE PREVISTO INCREMENTAR SU INVERSIÓN EN 2023

ciberataques. Por su parte, Ucrania ha reaccionado formando un “Ejército de TI” voluntario, que, desde el inicio del conflicto, ha intentado frenar los ataques dirigidos hacia sus infraestructuras. Los ucranianos han recibido, además, ayuda de hacktivistas de todo el mundo dando pie a un gran número de ataques relacionados con este conflicto armado.

Las violaciones de datos e interrupciones del servicio se han dado en ambos bandos y han dejado claro que la batalla va mucho más allá del terreno físico hoy en día y que, al igual que la guerra tradicional, puede ser fatal para millones de personas inocentes. En este sentido, se ha vuelto a abrir el debate sobre la necesidad de actualizar, y convertir en vinculantes, documentos como el manual de Tallin que, patrocinado por el Centro de Excelencia en Defensa Cibernética Cooperativa (CC-

DCOE, por sus siglas en inglés) De la OTAN en 2009, expone las claves sobre el derecho internacional aplicable a la guerra cibernética.

► **Ha llegado el momento de proteger, de verdad, las infraestructuras críticas.** Los ciberdelincuentes saben dónde pueden hacer más daño y lo están demostrando. El cibercrimen puede afectar al mundo físico y, tristemente, lo hemos visto en diversas ocasiones en los últimos meses. Servicios esenciales como industrias, hospitales e instituciones gubernamentales se han visto afectadas por ciberataques y seguirán siendo protagonistas de la lista de víctimas si no ponen la ciberseguridad en el foco de acción lo antes posible.

► **PYMES, grandes empresas... todo vale.** Si algo ha dejado claro 2022 es que los ciberdelincuentes atacan a todo tipo de empresas por lo que estar protegido, sea cual sea tu sector,



es cada vez más vital. Los últimos meses han mostrado la importancia de la autocrítica y los ejercicios de red team. Ya lo decía Carlos Loureiro, criminólogo y organizador de la comunidad Hackmadrid, en el especial sobre tendencias que celebramos como broche del año: “Conocer las debilidades propias es la mejor forma de protegerse”.

Carlos Estrada, director de ciberseguridad de Vestiga Consultores señalaba en una mesa redonda celebrada en julio que, según su experiencia en consultoría, “en consultoría, el 80% de los proyectos de pymes son reactivos, una vez ya hay un problema de que ya hay

un hackeo, y es importante que la empresa identifique de dónde va a venir el problema, de dónde van a venir nuestros atacantes”. Precisamente esa necesidad de conocerse a uno mismo parece la clave de cara al futuro más cercano. Y es que, muchos expertos en ciberseguridad apuntan a que cada empresa es única, pero todas pueden protegerse de los cibercriminales si conocen sus puntos débiles. Así lo asegura Clara Ferreiro, EMEA Business Development Manager de Netscout: “Es importante tener claro cuál es tu negocio, tu superficie de ataque, tus vulnerabilidades. También saber que la ciberseguridad no es un proyecto

que empieza y termina, es un proceso que siempre se tiene que estar revisando”.

CONOCERSE A UNO MISMO, CLAVE EN CIBERSEGURIDAD

¿Hay alguna forma de evitar repetir constantemente los mismos errores? Es evidente que no solo radica en conocer la historia. También debemos saber cómo somos. Cada individuo es único y eso, en ciberseguridad, supone que cada organización e institución tiene necesidades propias. No obstante, parece que hay algo común: la necesidad de invertir en ciberseguridad para mejorar la protección y la necesidad de hacer de los empleados un freno más.

Oriol Solà, CEO de WeFox, asegura que la clave para mejorar la ciberseguridad en cualquier empresa es la educación. Los empleados “tienen que estar preparados. Si queremos que sean nuestros primeros baluartes, tienen que estar bien formados y concienciados. Así, al menos, haremos que el eslabón que es más débil no lo sea tanto”.

INVERSIÓN

En los últimos años hemos visto cómo la ciberseguridad ha pasado

del departamento de TI a la sala de juntas y como el sector ha pasado de ser considerado un gasto a una inversión.

El año 2022 se va a cerrar con un incremento del gasto en ciberseguridad empresarial del 7,7% hasta los 1.749 millones de euros, y el crecimiento va a continuar siendo elevado en los próximos ejercicios, fruto de la necesidad de protegerse entornos de TI más abiertos y digitalizados en un escenario de amenazas complejo. Los cálculos de IDC, que plasma en un estudio realizado con Seidor, son que el mercado de ciberseguridad generará 2.200 millones en 2025, manteniendo ritmos de crecimiento similares cercanos al doble dígito.

Parece que este 2023, la inversión en TI continuará en alza, sobre todo en materia de ciberseguridad, que según los análisis del IDC Research crecerá en un 3,4% en las empresas españolas. En este sentido, según datos del estudio Estado de la ciberseguridad en España, de Secure&IT, en un escenario de amenazas en máximos históricos, el 51,3% de las compañías tiene previsto incrementar su inversión en 2023. Además, de las restantes, el 44% piensa

mantener los mismos niveles que el año pasado; casi un 1% empezará a invertir, y solo un 3,8% ha manifestado su intención de reducirlos. Si quieres conocer cómo evolucionará el sector de la ciberseguridad este año, no te pierdas este estudio en el que revelamos cuál son los ataques que más preocupan, qué tecnologías se están implantando más en las empresas y cómo buscar ayuda en caso de sufrir un incidente. ■

MÁS INFO +

- » [Centro de Excelencia en Defensa Cibernética Cooperativa](#)
- » [Tendencias de Ciberseguridad en 2023](#)
- » [El mercado de ciberseguridad generará 2.200 millones en 2025](#)
- » [Estado de la Ciberseguridad en España](#)



COMPARTIR EN REDES SOCIALES

SI ALGO HA DEJADO CLARO 2022 ES QUE LOS CIBERDELINCIENTES ATACAN A TODO TIPO DE EMPRESAS POR LO QUE ESTAR PROTEGIDO, SEA CUAL SEA TU SECTOR, ES CADA VEZ MÁS VITAL





La documentación TIC, a un solo clic

Plataformas de comunicaciones empresariales en modo suscripción. ¿Por qué?

En un modelo de trabajo flexible, las comunicaciones empresariales han protagonizado gran parte de la revolución tecnológica. Las videollamadas, la mensajería instantánea o la compartición de archivos se ha hecho imprescindible para trabajar en equipo y gestionar la atención al cliente de las empresas.



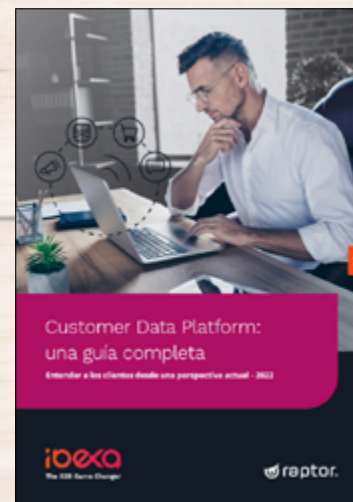
Work from Anywhere: una solución VMware SASE

Para que las empresas puedan ofrecer a los empleados un entorno mejor de trabajo desde cualquier lugar o desde casa, VMware SASE combina VMware SD-WAN y completas opciones de seguridad de SaaS y de nube, para proporcionarles flexibilidad, agilidad, seguridad y escalabilidad, y favorecer la transformación de la WAN y el perímetro.



Customer Data Platform: una guía completa

Una Customer Data Platform (CDP) unifica y activa los datos de los clientes en toda la organización para beneficiar al cliente y su experiencia en todos los canales y plataformas donde interactúen con la marca. Esta guía, creada por Ibexa, permite conocer cómo definir, implementar y aprovechar una CDP, con el objetivo de maximizar los resultados y mejorar la satisfacción de los clientes.



Los CIO estratégicos vinculan la optimización de costes a los resultados del negocio

Una visión estratégica a largo plazo de la gestión de costes, la dinámica empresarial y la situación económica ayudarán a evitar conversaciones reactivas centradas en costes", afirma Gartner en el informe que puedes leer a continuación. Accede y conoce cómo hacer que la optimización de costes sea estratégica y programática y cómo colaborar y promover el apoyo entre los líderes del negocio.



TENDENCIAS TECNOLÓGICAS 2023 Y FACTORES QUE INFLUIRÁN EN SU DESPLIEGUE

Arranca un nuevo año y nos preguntamos qué nos depararán los próximos doce meses en lo que al sector tecnológico se refiere; cómo se van a definir y desarrollar las estrategias digitales de las empresas; cuáles van a ser los retos que van a tener que superar las compañías en sus procesos de transformación de los negocios; será posible encontrar una solución al acuciante problema del talento digital en las organizaciones, tanto nacionales como internacionales...

Éstas son solo algunas de las preguntas que nos hemos hecho y que, de la mano de los principales expertos en cada área, hemos tratado de responder en este [Encuentro IT Trends Tendencias Tecnológicas 2023 y factores que influirán en su despliegue](#).

Para ello, preparamos una agenda con entrevistas, ponencias y mesas redondas en las que participaron profesionales de los diferentes ámbitos del mundo TI.

Y comenzamos hablando de las [tendencias tecnológicas que marcarán el año](#). Adrián López Jareño,

senior digital advisor de Penteo, nos adelantaba alguna de ellas, con el foco puesto en las áreas de inversión y el desarrollo tecnológico en España. Según este responsable, “el avance de las estrategias de digitalización de las empresas en España es positivo. Poco a poco va calando el enfoque que creemos que es el correcto a la hora de abordar los proyectos de transformación digital. Estos deben empezar con una visión clara de hacia dónde queremos ir con esta transformación, para, con ello, movilizar a la organización, las personas, los procesos y, por último, la tecnología”.



**Tendencias TI
2023**
y factores que influirán en su despliegue

VER VIDEO

itTRENDS

#EncuentrosITTrends

WEBINAR >> TENDENCIAS TECNOLÓGICAS 2023 Y FACTORES QUE INFLUIRÁN EN SU DESPLIEGUE

TECNOLOGÍAS Y SEGURIDAD PARA 2023

Para hablar de cuáles serán las tecnologías que acelerarán la gestión digital, celebramos una [mesa redonda](#) en la que participaron Javier Ahedo, country & partner manager de Ibexa; Carolina Henao, business developer de Mendix en Incentro; y Antonio Picazo, sales engineer de Micro Focus.

De igual modo, para repasar cuáles serán las tendencias de ciberseguridad en el año próximo, organizamos una segunda [mesa redonda](#) en la que participaron Miguel Abreu, CEO de B-FY; Luis Enrique Laguna, ingeniero de preventa de Ikusi; Ivan Mateos

Pascual, sales engineer de Sophos; y Ricardo de Ena, area sales manager de WatchGuard.

PREVISIONES PARA LOS PRÓXIMOS DOCE MESES

Para poner negro sobre blanco las previsiones de lo que nos traerá el año nuevo, participó [Jorge Díaz-Cardiel, director general de Advice Strategic Consultants](#), que nos explicaba que hay dos ideas esenciales, “la mayor parte de las empresas del sector han dado beneficios y han incrementado sus ventas, en un año donde se ha puesto foco en la valoración en Bolsa de muchas de ellas. Si vemos

los números, lo que soporta a estas empresas es aumento de ventas y beneficios, con lo que podemos decir que el sector está muy sano. Además, en Occidente hemos visto un avance muy importante en la digitalización, tanto a nivel empresarial como a nivel familiar. Esto se debe a la incorporación de las TIC de manera más natural en la vida de las empresas y de las personas”.

Entre las grandes noticias de este 2022, Jorge Díaz-Cardiel destacaba “la compra de Activision por parte de Microsoft, la compra de Elon Musk de Twitter, por 70.000 y 44.000 millones de dólares, respectivamente. También

la creación del Metaverso, que se está desarrollando como otras tecnologías relacionadas. Ha sido un año de fusiones y adquisiciones importantes”.

NUEVOS AIRES EN CIBERSEGURIDAD

En su participación en este encuentro, [Carlos Loureiro, criminólogo, coordinador en C1b3rwall Academy](#), y organizador de la comunidad Hackmadrid, nos comentaba que “en 2022 hemos visto un gran auge de los ataques de ransomware. Las empresas de todos los tamaños han visto que es una gran amenaza, tanto a nivel ciber como a nivel económico, sin olvidar la pérdida



Adrián López Jareño, Penteo, nos explicó las principales tendencias tecnológicas que marcarán 2023.



Hablamos de tendencias que acelerarán la gestión digital con la participación de Ibexa, Incentro y Micro Focus.



Hablamos de las tendencias que definirán la ciberseguridad en 2023 de la mano de B-FY, Ikusi, Sophos y WatchGuard.

de información, que les obliga a empezar de cero. Este ha sido el gran año de la concienciación del ransomware”. A lo largo del año hemos visto muchos y grandes ataques, “y su presencia en los medios de comunicación ayuda a la concienciación de la población general”.

El sector de la ciberseguridad, a nivel general, “presenta blancos y negros”, nos comentaba Carlos Loureiro, pero en el caso español “tenemos una problemática importante que parece que estamos empezando a resolver. Hemos visto el impulso de una iniciativa como el Escudo Digital, que va a permitir proteger a las empresas,

grandes y pequeñas, en tiempo real de estos ataques”.

EL RETO DE ENCONTRAR Y MANTENER EL TALENTO TI

Tal y como nos indicaba [Mercedes Fernández, directora general de MF-Talent](#), “una de las grandes preocupaciones de las empresas españolas es la capacidad de atracción de talento TI, pero también su posterior retención. Estamos en una situación convulsa que se agrava por la situación global. Por tanto, es esencial que nos adaptemos a nuevos modelos de negocio y a una nueva metodología

para llevar a cabo los procesos de selección”. La búsqueda de talento TI es, para Mercedes Fernández, “un reto importante. Pero el mayor hándicap existe para las empresas que no han sabido adaptarse a los modelos de negocio actuales, porque según un estudio de LinkedIn, un 87% de los candidatos se decantan por factores como movilidad, flexibilidad y un modelo de trabajo remoto. Así que esto, sumado al estilo de liderazgo de los responsables de las empresas, va a marcar mucho la elección de un candidato, que buscan compañías innovadoras, ágiles y adaptables”.

MÁS INFO +

- » [Encuentro IT Trends Tendencias tecnológicas 2023 y factores que influirán en su despliegue](#)
- » [2023, el dominio de la experiencia digital](#)
- » [Digitalización y negocio. Lo que las TI nos depararán en 2023](#)



COMPARTIR EN REDES SOCIALES



Jorge Díaz-Cardiel explicaba las principales tendencias económicas y tecnológicas que marcarán el año 2023.



Carlos Loureiro nos explicó en esta entrevista de qué van a tener que defenderse las empresas en 2023.



Mercedes Fernández analiza en su participación en este encuentro los perfiles que se espera que sean los más demandados en 2023.

#DEBATE IT

TENDENCIAS EN CIBERSEGURIDAD PARA 2023 Y LOS RETOS PARA EL CANAL

¿Qué nos deparará 2023 en el ámbito de la protección de la información? ¿Cómo seguirá evolucionando el canal de distribución al respecto? ¿Qué papel jugará el mayorista? También analizaremos en qué estadio se encuentra el proceso de consolidación del ecosistema tecnológico de la ciberseguridad en España, tanto a nivel de fabricantes como de mayoristas y canales.



MESA REDONDA >> Analizamos las principales tendencias que se van a producir en materia de ciberseguridad el próximo año y sus implicaciones en el ecosistema de canal, de la mano de Arrow ECS, Hillstone Networks, SonicWall, Stormshield y V-Valley.

Debatimos sobre estas y otras cuestiones junto a Ángel García, Manager Enterprise Computer Solutions en Arrow; Alberto Carrillo, Iberia sales engineering manager de Hillstone; Sergio Martínez, Iberia regional manager en SonicWall; Antonio Martínez Algora, responsable técnico de Stormshield Iberia; y David Gasca, business unit coordinator Enterprise Security en V-Valley.

Las tendencias en el área de la ciberseguridad a lo largo de este 2022 fueron el punto de partida del debate, repasando cómo ha evolucionado el

nivel de amenazas y la capacidad de protección de las empresas a lo largo de los últimos doce meses. Asimismo, quisimos adelantarnos al nuevo año, y preguntamos a los participantes en el debate sobre cuál va a ser la evolución de este segmento del negocio en los próximos trimestres, un período en el que destaca la continuidad en cuanto al tipo de amenazas, encabezadas por el ransomware, así como un incremento de la complejidad y personalización de los ataques que se esperan, y el papel que elementos como la concienciación de los usuarios o la formación de estos como barreras a

tener en cuenta para incrementar la protección, más allá de las herramientas tecnológicas con las que pueda contar cada organización.

Más allá de los elementos tecnológicos, en 2023 parece que se mantendrán dos tendencias establecidas en el mercado en los últimos meses: el crecimiento en el negocio de la ciberseguridad será mayor que el que tenga el global del mercado TI, y la falta de expertos con capacidades y conocimientos especializados en seguridad llevará a las empresas a recurrir a partners que puedan ofrecerle la protección como un servicio. ■



DESCARGA
EL DOCUMENTO
COMPLETO

DESCARGAR



ÁNGEL GARCÍA,
Manager Enterprise
Computer Solutions en **Arrow**



ALBERTO CARRILLO,
Iberia sales engineering
manager de **Hillstone**



SERGIO MARTÍNEZ,
Iberia regional manager en
SonicWall



ANTONIO MARTÍNEZ ALGORA,
responsable técnico de
Stormshield Iberia



DAVID GASCA,
business unit coordinator
Enterprise Security en
V-Valley



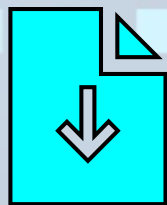
Lo que las TI nos depararán en 2023

Muchas personas, aprovechan el nuevo año para proponerse conseguir nuevos objetivos, personales y profesionales. Las empresas y las economías, también. La diferencia entre está en la intencionalidad para cambiar.

Lo vemos en el ámbito empresarial todos los días, cuando menos en el sector tecnológico norteamericano. Tanto los miles de despidos (Microsoft, Amazon, Intel, HP, Twitter, Meta, Cisco, etc) como los cambios en las cúpulas hechos o anunciados por las firmas tecnológicas estadounidenses, son la antesala de un fuerte cambio empresarial y económico que sucederá en 2023. No fruto del azar, sino de la intencionalidad: "necesidad, obliga", dice el refrán.

Los mimbres que conforman la realidad geopolítica, estratégica e internacional, condicionan (aunque no determinan) la actividad empresarial, especialmente en el sector tecnológico digital, que lo informa todo, lo impregna todo, empuja y transforma todo.

Esos "mimbres", factores, son de todos conocidos, aunque el análisis de sus consecuencias implicaría largas explicaciones y estudios. La guerra entre Rusia y Ucrania; la posible extensión o contagio de ese conflicto a otros países que siempre han tenido mala relación con Rusia, como las naciones que fueron invadidas por los soviéticos al final de la Segunda Guerra



¡Descárgatelo ahora!

INFORME IT TRENDS

Descárgalo ahora y sigue leyendo el informe IT Trends



Lo que las TIC nos depararán en 2023



JORGE DÍAZ-CARDIEL
Socio director general de
Advice Strategic Consultants



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



LO QUE LA DIGITALIZACIÓN NOS DEPARARÁ EN 2023

¿Significa algo tangible cambiar de año? ¿Se transforma la vida del 31 de diciembre al 1 de enero, cada año? No. A no ser que te toque la lotería, tengas un hijo o cambies de trabajo, por ejemplo, la vida de las personas,

las familias, las empresas, las economías y las naciones no cambian -menos aún, radicalmente-, de un día para otro. Más allá de las ilusiones, esperanzas, expectativas y buenos deseos, que todos tenemos y nos deseamos, después de comer

las uvas con las doce campanadas. Muchas personas, aprovechan el nuevo año para proponerse conseguir nuevos objetivos, personales y profesionales. Y las empresas y las economías, también. La diferencia entre esta afirmación y lo dicho en el pá-



COMPARTIR EN REDES SOCIALES

rafo anterior, está en la intencionalidad para cambiar. Arriba, decimos que la vida no cambia sola, a no ser que suceda un acontecimiento de calado. Ahora decimos que, muchos -no todos- se proponen mejorar en el nuevo año. El profesional quiere ascender y se propone adquirir nuevas capacidades profesionales que, en el mundo de los servicios, serán digitales en el 90% de los casos. La empresa quiere aumentar sus ventas o ser más rentable y, los directivos, se encuentran el Plan de Negocio encima de la mesa el 2 de enero: y no tanto para leerlo, sino para cumplirlo. Las economías y las naciones también pueden proponerse cambiar: por eso, se elaboran los presupuestos generales del estado, que son un medio para conseguir objetivos políticos, económicos, sociales o militares y estratégicos.

Todo lo dicho antes es obvio. Pero todos los años nos encontramos con “lo bonito”, que son los buenos deseos para el nuevo año y el duro choque con la realidad que supone, en 2022 y 2023 empezar de verdad, en serio, un nuevo año.

Lo vemos en el ámbito empresarial todos los días, cuando menos en el sector tecnológico norteamericano.

Tanto los miles de despidos (Microsoft, Amazon, Intel, HP, Twitter, Meta, Cisco...) como los cambios en las cúpulas hechos o anunciados por las firmas tecnológicas estadounidenses, son la antesala de un fuerte cambio empresarial y económico que sucederá en 2023. No fruto del azar, sino de la intencionalidad: “necesidad, obliga”, dice el refrán.

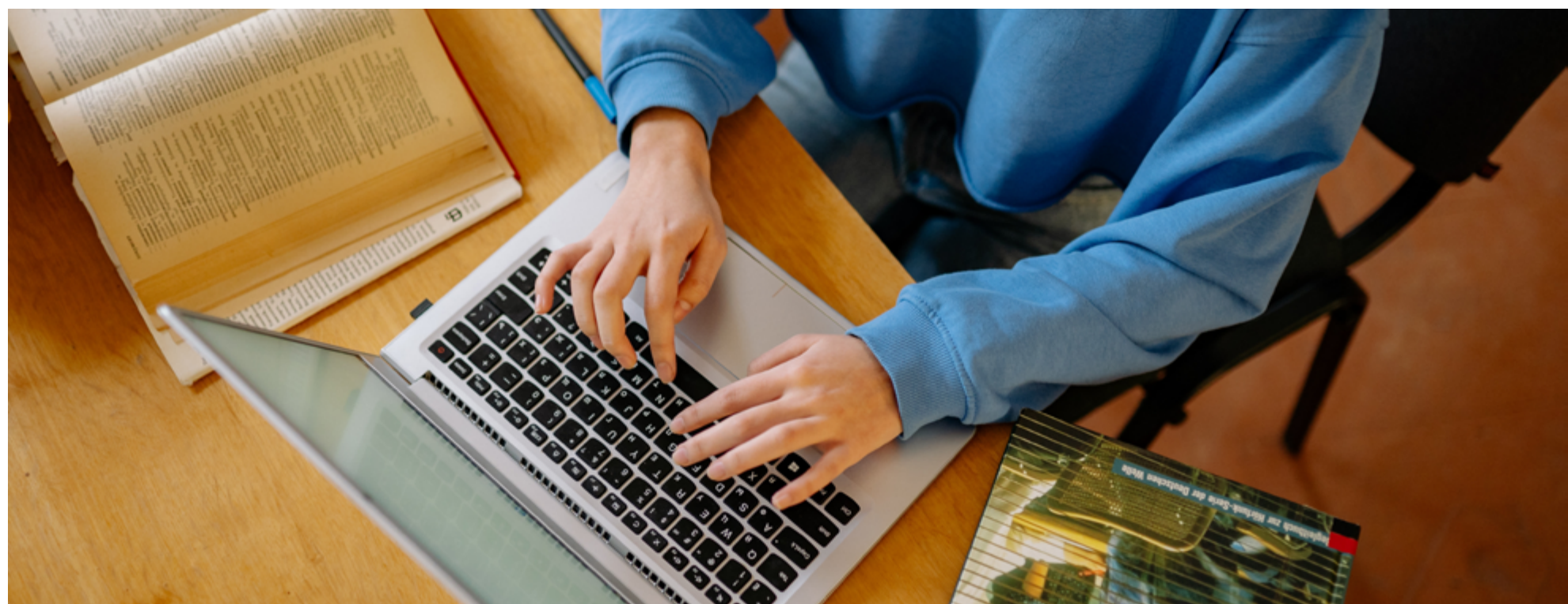
Los mimbres que conforman la realidad geopolítica, estratégica e internacional, condicionan (aunque no determinan) la actividad empresarial, especialmente en el sector tecnológico digital, que lo informa todo, lo impregna todo, empuja y transforma todo. Esos “mimbres”, factores, son de todos conocidos,

aunque el análisis de sus consecuencias implicaría largas explicaciones y estudios. De hecho, esta tribuna es un “aperitivo” de un amplio, extenso y profundo [estudio](#) que explicará en detalle “lo que nos deparará 2023”, y que realizará Advice Strategic Consultants para IT Trends e IT Digital Media Group.

La guerra entre Rusia y Ucrania; la posible extensión o contagio de ese conflicto a otros países que siempre han tenido mala relación con Rusia, como las naciones que fueron invadidas por los soviéticos al final de la Segunda Guerra Mundial y hace 30 años no quieren saber nada de Rusia: Polonia, Rumanía y tantos otros. También, antiguas repúbli-

cas soviéticas que hoy son naciones soberanas como la propia Ucrania y Georgia, entre otras. Los Balcanes, de nuevo, como en 1914, podría ser un hervidero de tensiones con consecuencias **impensables**: las naciones que compusieron la antigua Yugoslavia están “nerviosas”: Serbia, Croacia, Bosnia, Montenegro...

Las relaciones entre Rusia y Estados Unidos (primera potencia del mundo, todavía, con la mayor economía y más potentes fuerzas armadas) son hoy las peores, desde los peores momentos de la Guerra Fría, con la excepción de la Crisis de los Misiles de Cuba. La afectación del conflicto ruso-americano influye en Europa, militarmente en el medio



plazo y en la crisis energética en el futuro (presente) inmediato. Occidente impone sanciones a Rusia, a la exportación de su petróleo y gas y, entre otras, vemos estas consecuencias: Europa sufre la falta de energía y en Alemania la gente corta árboles para encender chimeneas; y franceses e ingleses, “corren, vuelan”, en la construcción de centrales nucleares, para dejar de depender de la energía rusa. El gas licuado que nos llega de Estados Unidos o del Norte de África, resumen, son parches, no son soluciones. Y, además, Rusia se arrima más a China, Pakistán e India (dos países enfrentados desde su fundación), Irán y Arabia Saudí (también enfrentados) y otros países de la OPEC (Venezuela) que aprovechan los altos precios del crudo para recortar la producción, haciendo sufrir a Occidente, como sucedió con los embargos de petróleo de 1973 y 1979. Esos años nos enseñaron lo que significa la “stagflación”: recesión (parón o decrecimiento del PIB) y altos precios en todos los productos.

Y la madre de todas las guerras: China y Estados Unidos. Fabricación, exportaciones, tecnologías de la información, patentes, espionaje,

2023 SERÁ UN AÑO DE INCREÍBLE EXTENSIÓN, IMPLANTACIÓN Y USO DE LAS TECNOLOGÍAS DE LA DIGITALIZACIÓN

ciberseguridad...; son factores que alteran no ya el comercio mundial sino la propia Globalización que durante tres décadas generó lo que los economistas denominamos “La Gran Moderación”, entre 1990 y 2020. **La cadena de suministro vive la mayor crisis de su historia y afecta a todos los sectores de actividad.**

En el sector tecnológico, China está dejando de ser la gran fábrica de Apple, Samsung o Intel. Cientos de empresas tecnológicas se llevan -de nuevo- parte de la producción a Estados Unidos, Corea del Sur y Taiwán (país motivo de conflicto potencialmente muy serio entre EEUU y China) y en Texas y Arizona, Intel, HP, Apple, TSMC y otras construyen fábricas de **chips/semiconductores** para no depender tanto de China, cuyas políticas de “cero COVID” en sus fábricas, ha causado fuerte falta de componentes a la industria de semicon-



ductores, afectando negativamente a NVIDIA, Intel, AMD, Qualcomm, TSMC y Samsung, entre otras. **De los procesadores a la industria tecnológica que lideran Lenovo, HP, Acer, Asus, Samsung, Apple, etc, no hay sino un suspiro** y, la falta de componentes más la falta de demanda por los altos precios consecuencia de la inflación, han reducido las ventas de ordenadores, pc, portátiles, tabletas... un 20% este año. De 2023, aún no decimos nada...

La explosión (negativa) de las plataformas de intercambio de criptomonedas (que anticipamos desde Advice Strategic Consultants con la

quiebra de FTX y Alameda Research) ha tambaleado ese sector con un efecto dominó que afecta, desde FTX a Coinbase, BlockFi, Genesis, Gemini y, en mucha menor medida, a las criptomonedas en sí mismas: Bitcoin y Ethereum aguantaron el tipo y las tecnologías subyacentes, **Blockchain, NFT y Web3 no se han inmutado**, lo que es buena noticia para 2023 porque Blockchain, NFT y Web3 se expandirán en 2023, al igual que el Metaverso donde están y quieren estar todo tipo de empresas de la mano de las firmas de videojuegos que ya ofrecen realidades inmersivas como Epic Games, Xbox, Activision

y Decentraland y otras plataformas, donde hay empresas de todos los sectores deseando hacer negocio: desde McDonald's a Gucci, desde Nike a Inditex, CaixaBank con Imagin e Imagin Café a los bancos de inversión y el sector inmobiliario.

Las redes sociales (las empresas de RRSS) cambian el foco. TikTok, a quien muchos expertos, autoridades, reguladores, legisladores y gobiernos restan credibilidad porque (y cito textualmente al regulador norteamericano) “su algoritmo crea dependencia, es adictivo” y “lo es que es peor (...) ha dado lugar a suicidios niños y adolescentes”. Pero, se habla de “la “economía de TikTok”, porque ya genera más de 100 billones de

dólares en ventas y el 70% de las 500 marcas más importantes, reconocidas y más reputadas del mundo, están presentes en TikTok. Lo que no significa dar por muertas a Facebook, Instagram, Whatsapp (las tres pertenecientes a Meta Platforms o, en otras palabras, Mark Zuckerberg, con 3,5 billones de usuarios), Telegram, Snapchat, Twitter y muchas más. **Las redes sociales no van a desaparecer, sino que, en 2023 cambiarán de modelo de negocio,** como veremos en el informe.

Elon Musk es en sí mismo una tendencia, tanto o más que Jeff Bezos en Amazon o Tim Cook en Apple, Satya Nadela en Microsoft y Sundar Pichai en Alphabet (Google, YouTube)...

Hay tecnologías de la digitalización que están triunfando in crescendo desde hace 5 años y que no van a parar de crecer: Big Data para conocer las necesidades de los clientes incluso antes que estos las sepan; Ciberseguridad (obvio); Inteligencia Artificial / Machine Learning / Deep Learning; Internet de las Cosas / Edge Computing; Conectividad con 5G y 6G; Cloud, cuando la estrategia multicloud está ya más que sellada con cemento y tres grandes proveedores, AWS, Microsoft Azure y Google Cloud. Esas tecnologías, y otras, requieren miles de empresas proveedoras, **lo que pone en extraordinario valor la figura de los integradores de tecnologías de nueva generación como Telefónica Tech,** de las pocas multinacionales tecnológicas españolas que triunfan en el mundo, con 6.000 empleados en 24 mercados internacionales. O, en la imprescindible gestión de redes (infraestructuras de telecomunicaciones inalámbricas), que resalta la otra multinacional española tecnológica, Cellnex Telecom, líder en Europa.

La aplicación -sí o sí- de las tecnologías de la información y digitalización que el Foro Económico Mundial (World Economic Forum)

denomina “Cuarta Revolución Industrial” será una realidad en 2023, tanto en gran empresa como en las pymes, revolucionando, ya sí, el retail / distribución / comercio; la banca, con DEFI; alimentación; Industria 4.0; energía inteligente, etc.

Citando al maestro Torrente, en 2023 pasaremos del “dicho al hecho, porque no es lo mismo ver chirlas que comerlas”: **2023 será un año de increíble extensión, implantación y uso de las tecnologías de la digitalización.**

Pero, como dijimos al inicio, esta tribuna solo incoa la cuestión y, en el [Estudio de Advice Strategic Consultants / IT-Trends](#) veremos en detalle el **despliegue de la transformación digital.** ■

MÁS INFO +

- » [Digitalización y negocio. Lo que las TI nos depararán en 2023](#)
- » [IT Trends: 2023, el dominio de la experiencia digital](#)
- » [Tendencias tecnológicas 2023 y factores que influirán en su despliegue](#)





JOSÉ MANUEL NAVARRO
experto en Marketing



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



COMPARTIR EN REDES SOCIALES

EL PAPEL DE LAS EDE ANTE EL EURO DIGITAL

En el reciente [informe Digital 2022](#), realizado por Hootsuite y We Are Social, se exponen algunos datos que son significativos para vislumbrar cuál puede ser el futuro de la industria financiera en general, y de la de pagos en particular, en base a la utilización por parte de los usuarios a nivel global de las redes sociales y de la adopción de tecnologías móviles, así como las principales tendencias digitales en el

marco de una economía tensionada por diversas y sucesivas crisis.

Del casi 63% de la población mundial que son usuarios de una conexión a internet, el 71,5% manifiestan pagar de manera recurrente por contenidos digitales y casi el 60% compran todas las semanas en diversos comercios electrónicos. Si tenemos en cuenta que en torno al 60% de la población mundial es usuaria de redes sociales y que el tiempo medio de consumo

diario se ha elevado a dos horas y media, las oportunidades que tienen las grandes empresas para llegar con publicidad a sus potenciales clientes se han incrementado exponencialmente, generando un nuevo “mercado social” que requiere de fórmulas seguras y flexibles de pago. A este escenario, se suma el 10% de usuarios de internet que poseen algún tipo de criptomoneda cuyo futuro se está cuestionando en este momen-



to a partir de la deriva de empresas como FTX, y las debilidades que han mostrado estos activos, entre las que destaca su incapacidad para generar flujos de caja, su elevadísima volatilidad y su inadecuación a los sistemas de pago regulados.

La conjunción de los efectos de la pandemia, de la crisis económica cuyo origen está en la política monetaria de los bancos centrales, de la guerra en Ucrania y de la rápida adopción de sistemas y dispositivos digitales por todas las capas sociales, ha provocado cambios culturales en unos casos y consolidación de conductas de relación interpersonal y de uso de los medios electrónicos, en muchos otros, que pronostica un futuro inmediato de grandes retos para los profesionales de marketing de cualquier empresa. La segmentación clásica ya no es válida y la observación de los comportamientos de los usuarios para asignarles un perfil característico deberá tener en cuenta variables, tan imponderables como inciertas, relacionadas con los ajustes emocionales de los ahorradores y de los inversores ante escenarios de incertidumbre y de duda alimentados por la cantidad de información disponi-

ble, y mediatizados por los sesgos cognitivos que cada humano utiliza para tomar decisiones económicas.

En entornos de incertidumbre y duda, también surge el miedo y la inseguridad para realizar todo tipo de operaciones “online” en las que medie una transacción económica, debido a que el fraude de diversa naturaleza (“phishing”, “smishing”, “vishing”, “spoofing”) está creciendo al mismo ritmo que la adopción de dispositivos y monederos digitales, y de los métodos alternativos de pago a través de canales electrónicos, virtuales, sociales y, últimamente, en el “criptomercado”. Este hecho queda reflejado en el [informe Global State of Fraude and Identity](#) de LexisNexis, en el que se apunta que las nuevas fórmulas de pago son igualmente presa del fraude iniciado por humanos y por máquinas. El incremento en el último año fue del 32% en los primeros y del 38% en las segundas, abarcando la estafa desde los pagos sin contacto y con QR hasta la financiación BNPL e, incluso, el robo de criptodivisas y la apertura de cuentas.

Aunque los gobiernos han intervenido con diligencia robusteciendo los requisitos normativos para proteger a

LAS EDE, AL CONTAR CON LICENCIA BANCARIA PARA EMITIR, DISTRIBUIR Y REEMBOLSAR DINERO ELECTRÓNICO, ESTÁN MÁS QUE SUFICIENTEMENTE PREPARADAS TECNOLÓGICAMENTE PARA ADOPTAR EL PAPEL DE GESTORAS DE CBDC

los usuarios y prevenir tanto el fraude como el blanqueo de capitales, los protocolos de seguridad no terminan de ser 100% infalibles por dos cuestiones básicas: (1) el perfeccionamiento de los defraudadores para eludir los procesos de salvaguarda más complejos y (2) la ingenuidad o escaso cuidado de algunos usuarios al acceder o confiar en sitios donde no existen las debidas medidas de autenticación reforzada durante la transacción de identificación y pago.

La entrada de nuevos “player financieros” como neobancos, challenger banks, proveedores de servicios de iniciación de pagos (PISP), proveedores de servicios de información de cuentas (AISP), procesadores de soluciones [embed finance](#) o de agregación de cuentas, al amparo de las directivas europeas sobre servicios de pago (PSD2) y de protección de datos (RGPD), ha supuesto un reto para la banca convencional que ha tenido que



acelerar la adaptación de sus sistemas heredados a un entorno digital más dinámico. También han tenido que cambiar el foco de su actividad en los productos y servicios a situar en el centro de su estrategia a los clientes, quienes demandan soluciones individualizadas que les proporcionen mayor libertad de elección y una tramitación más fluida, segura y transparente.

A la substanciación de estos cambios se le ha llamado [Open Finance](#), modelo en el que se ha avanzado mucho hacia la desintermediación de servicios básicos, aunque la estricta regulación impide llegar al modelo de finanzas descentralizadas ([DeFi](#)) reales a la que muchos ciudadanos aspiran. La muestra de ello es la creación de una economía paralela

dominada por los criptoactivos, en la que la ausencia de regulación parecía estar compensada por la fortaleza de la tecnología y la voluntad de sus usuarios, pero el tiempo ha demostrado que las carencias de la primera (excesivo consumo de energía, debilidades en la protección de las claves personales, ralentización de los procesos de intercambio, inoperatividad en la industria de pagos, etc.) y la elevada volatilidad de sus posiciones debido a la dependencia emocional de los inversores (FUD -miedo, incertidumbre y duda) cuya conducta es una réplica de la que se produce en el

mercado de valores convencional, han construido un ecosistema actualmente cuestionado por las dramáticas caídas de valor de algunas criptomonedas, la quiebra de algunos exchanges y el cuestionamiento de otros.

No obstante, en el tránsito por el “criptoinvierno” aún existe la esperanza de algunos inversores de frenar la estrepitosa caída de los criptoactivos mediante acciones de compra masiva y, más eficaz, de impulso de las funcionalidades más demandadas por los usuarios. Entre éstas hay que destacar los pagos con criptodivisas en comercio electrónico y físico (como los que

intenta promover Coinbase), las transacciones entre empresas para reducir a segundos las transferencias transfronterizas (como las que ofrece Syro), la compra de NFT’s como las que se gestionan en la plataforma de BitPay, los pagos P2P dentro del nuevo ecosistema web3 (como los ofrecidos por DePay), o el pago de remesas (como la pasarela de TripleA).

Siendo conscientes del alcance, riesgos y oportunidades que están poniendo sobre la mesa los defensores de la “criptoeconomía”, los bancos centrales se han puesto de objetivo urgente la emisión de su propia criptodivisa y la inaplazable regulación de las empresas que custodian, intercambian y dan servicio de soporte y procesamiento a las actuales criptomonedas, al menos a las más sólidas. Otra cuestión será la legalización de estas, ya que supondría el reconocimiento de su validez (hasta la fecha frenado por el sector financiero más convencional) y, sobre todo, iniciar ajustes y cambios operativos de elevado riesgo para que sean admitidas en los esquemas y estándares de todos los procesadores actualmente autorizados, además de reforzar los mecanismos de prevención de blanqueo de capitales.

LAS EDE PUEDEN ASUMIR EL PAPEL QUE EL BCE PRECISA QUE REALICEN LAS ENTIDADES FINANCIERAS AL LANZAR SU PROTOTIPO DE CBDC MINORISTA EN EL PRIMER TRIMESTRE DE 2023



En el caso de la Unión Europea, la creación de un marco jurídico a través del [Reglamento MiCA](#), es un primer paso para unificar la definición de un criptoactivo como “una representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante la tecnología de registro descentralizado u otra similar”. También para diferenciar los diferentes tipos que deben quedar regulados: “utility tokens” (necesarios para acceder a un bien o servicio digital), “tokens estables” (ficha referenciada a un activo estable y de curso legal) y “tokens de intercambio” (fichas de dinero electrónico para ser usadas como medio de pago o de intercambio de otros tokens, con un valor estable y referenciado a una moneda fiat de curso legal). Y, por supuesto, para preparar la creación del euro digital que conviva con el dinero físico y el bancario, y que frene la actividad de las criptomonedas actuales.

Frente a los aparentes beneficios que podría aportar el euro digital, como reforzar el crecimiento económico de la eurozona, ampliar las opciones de pago de los ciudadanos, equilibrar la evolución de la moneda respecto de los avances de la tecnología o prevenir posibles ataques contra

la estabilidad financiera si el “cripto-mercado” se consolidara como una alternativa real y seria, es necesario tener en cuenta otras cuestiones que le hacen perder atractivo. Entre éstas hay que considerar la pérdida de privacidad y de anonimato que tendrían sus usuarios, ya que el banco central podría no solo fiscalizar el saldo y las operaciones de cada uno, sino que también podría establecer límites de uso, asignar criterios de fungibilidad o de valoración para estabilizar la inflación o crear métodos de vigilancia de la conducta de consumo.

No son cuestiones baladíes, por lo que el BCE creó un [grupo de investigación](#) para resolver estas cuestiones de cara a evitar posibles consecuencias negativas para el sector y para los ciudadanos, y para limitar la utilización del euro digital como medio de pago, no como alternativa de inversión ni especulación. Adicionalmente, ha puesto en marcha la creación de [un prototipo](#) de moneda digital (CBDC minorista) en el que intervienen [cinco entidades](#) para el desarrollo del modelo de datos, transaccional y de servicios de plataforma, con el que pretende probar su viabilidad como medio de pago (online y offline) y la usabilidad de las aplicaciones que soporten su operatoria.



Por su parte, el Banco de España [ha convocado a las entidades y empresas tecnológicas nacionales](#) para participar en un experimento parecido al iniciado por el BCE, aunque en el marco de una moneda digital mayorista, para evaluar el potencial real que ofrecen estas criptodivisas en base a la tecnología actual y a la esperada evolución para dar respuesta a su funcionalidad como activo de liquidación seguro para la operativa que sucede en los sistemas de compensación y liquidación de alto importe entre entidades, y entre éstas y el banco central.

En la construcción de la estructura que soportará la creación de la CBDC europea por los bancos centrales,

quienes pueden aportar un valor especial son las entidades de dinero electrónico cuya [legislación](#) ya las habilita para ser las mejores candidatas para asumir el rol que ostentan en la actualidad los exchanges centralizados (CEX), pero con las garantías y regulación que les permita gestionar y distribuir CBDC mayoristas y minoristas dentro de esquema bancario europeo.

Las EDE, al contar con licencia bancaria para emitir, distribuir y reembolsar dinero electrónico (además de otras actividades relacionadas con los servicios de custodia y movimiento de fondos entre cuentas, de pagos, de información, de gestión de instrumentos de pago...), están más que suficientemente preparadas tec-

nológicamente para adoptar el papel de gestoras de CBDC ya que muchas de ellas, además, han avanzado en el desarrollo de sus plataformas y procesadores mediante la tecnología blockchain, tokenizando sus transacciones y generando “smart contract” como modelo operativo avanzado. Por otro lado, los procesos de onboarding (identificación y autenticación) de clientes ya los han perfeccionado para hacerlos sin presencia física, la custodia de las claves de usuario también la ostentan como proveedores de monederos electrónicos seguros, ya aplican estrictas medidas de prevención de blanqueo de capitales y financiación del terrorismo, cuentan con servicios de defensa del cliente auditados por los órganos reguladores y, finalmente, garantizan el 100% de los depósitos de cada cliente (a diferencia de la banca convencional, que solo puede garantizar lo estipulado en cada momento por el [Fondo de Garantía de Depósitos](#)).

Las EDE pueden asumir el papel que el BCE precisa que realicen las entidades financieras al lanzar su prototipo de CBDC minorista en el primer trimestre de 2023, garantizando la privacidad de los clientes y el anoni-

mato de las transacciones, proveyendo de coherencia al modelo de gestión del dinero digital dentro del esquema bancario europeo (ya lo hacen para el dinero electrónico), garantizando la inviolabilidad de las operaciones mediante procesos de autenticación reforzada y de registro inalterable, cohesionando los sistemas de la industria de pagos compatibilizando el uso de dinero digital y electrónico mediante billeteras inteligentes... En definitiva, intermediando en la relación de las CBDC con los usuarios sin que haya discrepancias con los sistemas tradicionales. ■

MÁS INFO +

- » [Digital 2022](#)
- » [Global State of Fraude and Identity](#)
- » [Embebed Finance](#)
- » [PSD2](#)
- » [Open Finance](#)
- » [Reglamento MiCA](#)



¿Cuál es la situación de la empresa española en relación con la digitalización?

¿Qué tecnologías son las que están impulsando la transformación digital?

Descubra las últimas tendencias en el **it** Centro de Recursos **User**

»»»»»»
»»»»»»



Tecnología

para tu **Empresa**

««««««
««««««

Con la colaboración de:

brother **FUJIFILM**

Life Is On | **Schneider**
Electric

