

EL VALOR DE AUTOMATIZAR LOS PROCESOS



- GESTIONAR CLOUD
CON CIBERSEGURIDAD
- EL COSTE DE INTEGRACIÓN
EN LA GESTIÓN DE LOS DATOS

COMPARATIVA  Soluciones de seguridad de red

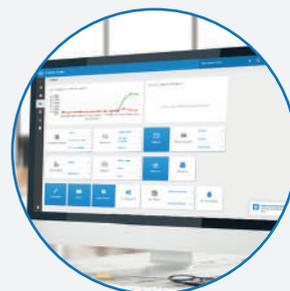


a3innuva ERP

La solución online que simplifica la gestión del negocio de la pyme y del autónomo, integrando la facturación y la contabilidad de forma centralizada y completamente adaptada a tus necesidades.



Gestionar tus **presupuestos**, crear tus **facturas de compra-venta**, o gestionar los **cobros y pagos** nunca había sido tan fácil ni rápido.



Facilita la gestión de la **contabilidad** y **presentación de impuestos** accediendo a toda tu información de manera rápida y eficiente.

La extorsión de Broadcom



Manuel Navarro Ruiz
Director de BYTE TI

Los que preveían que, cuando la compra de VMware por parte de Broadcom fuera efectiva, se iba a producir un espectacular terremoto, parece que tenían razón. Muy pocas adquisiciones han dependido tanto del entorno y de factores externos, pero sí es la única en la que desde el primer momento se iba a saber lo que iba a suceder al día siguiente de la adquisición. Las previsiones, de hecho, se quedaron cortas. A día de hoy, y tan sólo cuatro meses después de la compra, la nueva VMware by Broadcom puede presumir de haber despedido a buena parte de la plantilla y tener en el descontento y la incertidumbre a otra parte; haber liquidado a uno de los mejores canales de distribución del sector TIC; descoyuntar por completo la oferta de producto; aniquilar las páginas webs locales; tener descontentos a los clientes con un cambio de licencias que todavía no llegan a comprender y, de paso, subirles de forma radical los precios... ¿Qué más se puede pedir?

Pues sólo le faltan las demandas. Y éstas pueden estar cercanas. CISPE es la organización de proveedores de servicios cloud europea y ha decidido dar la alerta por las prácticas de Tan Hock, CEO de Broadcom. Este conjunto de empresas acaba de rogar a los reguladores, legisladores y tribunales de toda Europa que examinen de forma rápida la nueva política de Broadcom: no creen que sea legal que Hock pueda cancelar de forma unilateral los términos de las licencias del software de virtualización con el que trabajan.

No les falta razón. Empresas, organismos públicos, pymes o startups llevan años utilizando el software de VMware. Todos ellos firmaron unos contratos y unas condiciones que ahora Broadcom decide que no le gustan y que, por tanto, modifica a su conveniencia. Hock, parece haber asimilado el refranero español: "Son lentejas". Sabedor de la importancia que tiene VMware para todas estas organizaciones y de la dificultad que tendrían para encontrar una alternativa, decide cambiar las condiciones y de paso, aumentar de forma notable el precio que ve-

nían pagando. Sólo falta que los nuevos contratos exija firmarlos en Sicilia. Así que lo que CISPE pide es que, al menos, se produzca una pausa inmediata en las rescisiones de contratos y la capacidad de los clientes de salir del contrato plurianual impuesto por Broadcom tan pronto haya alternativas viables.

El problema es grave ya que si muchas organizaciones carecen de la capacidad financiera de aceptar unas condiciones que multiplican por 12 el precio que venían pagando por las licencias de VMware y que están avaladas por un contrato (que debería cumplirse) podrían quebrar. Esta situación afectaría a los clientes de todas estas empresas que dejarían de disfrutar de un servicio que a su vez también tenían contratado y que no se va a cumplir por culpa de la política del magnate malayo. Hablamos de servicios de transporte, de ocio, médicos, financieros,... Es decir, no sólo las empresas se van a ver perjudicadas, sino que seremos los ciudadanos los que saldremos perjudicados.

La nueva política impuesta por Broadcom tiene un nombre: extorsión. CISPE es la primera voz importante que lanza la señal de alarma. No sería de extrañar que en los próximos meses aparezcan demandas contra la nueva VMware by Broadcom. Una pena que alguien que sólo busca el beneficio rápido haya matado a una de las mejores compañías TIC de este siglo.

SUMARIO



TEMA DE PORTADA

¿Cuál es el estado de la automatización?

38

N.º 325 • ÉPOCA IV

MKM PUBLICACIONES
Managing Director

Ignacio Sáez (nachosaez@mkm-pi.com)

BYTE TI
Director

Manuel Navarro (mnavarro@mkm-pi.com)

Redacción

Vanesa García (vgarcia@revistabyte.es)

Coordinador Técnico
Regina de Miguel

Colaboradores

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

Fotógrafos

P. Varela, E. Fidalgo

Diseño de portada
Wings Factory

Diseño y maquetación

El Palíndromo Comunicación S.L.

WebMaster

NEXICA
www.nexica.es

REDACCIÓN

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

PUBLICIDAD

Directora comercial: Isabel Gallego
(igallego@mkm-pi.com)
Tel.: 91 632 38 27
Natalie Awe (nawe@mkm-pi.com)

DEPARTAMENTO DE SUSCRIPCIONES

Tel. 91 632 38 27
Fax.: 91 633 25 64
e-mail: suscripciones@mkm-pi.com
Precio de este ejemplar: 5,75 euros
Precio para Canarias, Ceuta y Melilla:
5,75 euros (incluye transporte)

Impresión

Gráficas Monterreina

Distribución

DISPAÑA
Revista mensual de informática
ISSN: 1135-0407

Depósito legal
B-6875/95

© Reservados todos los derechos.

Se prohíbe la reproducción total o parcial por ningún medio, electrónico o mecánico de los artículos aparecidos en este número sin la autorización expresa por escrito del titular del Copyright. La cabecera de esta revista es

Copyrightsafdscsdagtdhgvakjbsdvckjbckasdcj-baskcjbskdjbsdclcbt de Publicaciones Informáticas MKM. Todos los derechos reservados. Publicado con la autorización de Publicaciones Informáticas MKM. La reproducción de cualquier forma, en cualquier idioma, en todo o parte sin el consentimiento escrito de Publicaciones Informáticas MKM, queda terminantemente prohibida. Byte TI es una marca registrada de Publicaciones Informáticas MKM.

ABRIL 2024
Printed in Spain



EDITA

Publicaciones Informáticas MKM

ACTUALIDAD

6



COMPARATIVA

28



TENDENCIAS

58



3 CARTA DEL DIRECTOR

6 ACTUALIDAD

20 WEBINARS y
ENCUENTROS BYTE TI

28 COMPARATIVA

38 TEMA DE PORTADA

50 LEGALIDAD TIC

52 MUJERES TIC

54 UN CIO EN 20
LÍNEAS

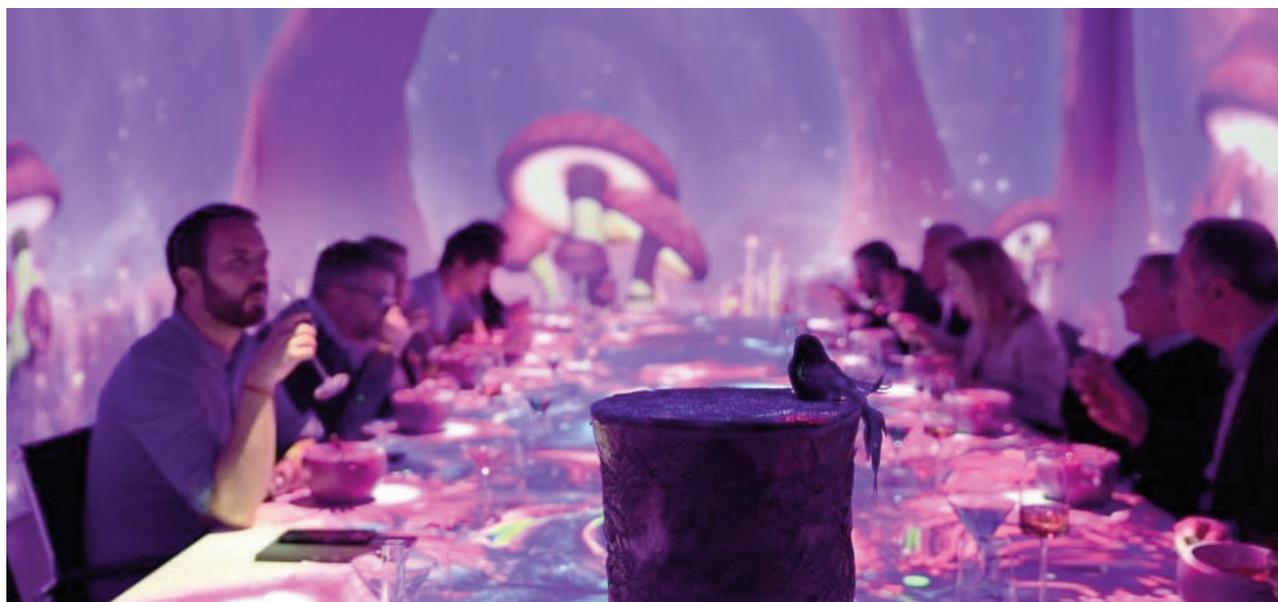
56 APLICACIÓN
PRÁCTICA

58 TENDENCIAS

64 ENTREVISTA

66 CIBERCOTIZANTE

La restauración ante el reto de transformarse



Uno de los sectores que más debe invertir en su transformación digital es el de la restauración. La abundante competencia, la exigencia de los clientes, mejorar la cadena de suministro o adaptarse a las nuevas formas de consumo son sólo algunos de los retos que el sector tiene por delante.

Por Manuel Navarro

La irrupción de la pandemia puso de manifiesto muchas de las carencias que tenía el sector y tras los meses de cierre obligatorio, aquellos bares y restaurantes que supieron adaptarse a la nueva realidad pudieron seguir funcionando. Durante el confinamiento, los clientes pudieron comprobar de primera mano cuáles fueron los locales que se adaptaron de forma más rápida. Aunque el negocio no era el mismo, muchos fueron los que adoptaron soluciones para llevar sus productos a casa de los clientes, bien mediante acuerdos con plataformas de delivery, bien

con el desarrollo de plataformas propias para satisfacer las demandas de sus clientes.

Cuando ese periodo se terminó y se pudo volver a salir, los primeros clientes vieron como sus bares y restaurantes de siempre habían cambiado. De pronto, incluso aquellos más reticentes, habían adoptado soluciones de pago con tarjeta, incorporaron cartas virtuales a las que se accedía a través de códigos QR, las reservas se hacían a través de Internet o de una app, se implementaron herramientas de contabilidad, se acabaron las cajas registradoras para incor-

porar modernos TPVs... En definitiva, el sector comprobó que la transformación digital no sólo era necesaria, sino que debía ser un imperativo

EXPERIENCIAS PERSONALIZADAS

Esa digitalización de los procesos, sin embargo no se han quedado en eso. Algunos han ido más allá. La competencia en el sector de la hostelería es brutal, con una oferta muy amplia y con unos márgenes muy estrechos. En muchas ocasiones, ni siquiera basta con ofrecer una carta de calidad y competitiva. Así que para ganar a la competencia, es necesario, cada vez más, ofrecer al cliente una experiencia exclusiva.

Y eso es lo que ha hecho Sinestesia. Un restaurante único, situado en Madrid, que ha contado con la ayuda de Epson, para ofrecer una experiencia distinta, atractiva y que combina la calidad del producto con un proyecto novedoso, pensado para que el cliente viva, sienta, vea, huelga y oiga cada plato que se sirve. Epson ha ayudado a que Sinestesia combine una propuesta que une tecnología y alta cocina para sumergir a los comensales en un viaje multisensorial. Gracias a esta colaboración, presentada en torno a una única mesa bajo el título “¿A que saben los colores?”, hasta dieciséis comensales pueden vivir una experiencia singular para todos los sentidos que combina sorpresa, diversión y dinamismo gracias a diversos estímulos audiovisuales proyectados en el espacio que van apareciendo a medida que se va presentando el menú, asesorado y coordinado por Kiko Moya, uno de los mejores chef de España, que cuenta con dos estrellas Michelin y tres soles de Repsol.

Acompañados por performance de actores y actrices, el restaurante ha construido una narrativa en la que imágenes, sonidos, mensajes, sabores y texturas, crean una armonía para proporcionar a los clientes una experiencia única de 2,5 horas de duración. Este proyecto, que se ha desarrollado durante cerca de 13 meses, ofrece un menú de estilo mediterráneo compuesto por un aperitivo, seis platos principales, y un postre.

ROMPER LO ESTABLECIDO

Sinestesia pretende romper lo establecido en el mercado gastronómico para ofrecer un producto innovador de restauración organizada. Para lograrlo, sus creadores han diseñado un storytelling y una marca coherentes, y han integrado la tecnología audiovisual a las especificaciones del local para adaptar el servicio a la historia que se quiere transmitir.

La tecnología de Epson ha sido la que ha hecho posible llevar este proyecto a cabo, ya que el material tecnológico requiere de unas necesidades técnicas muy específicas. La experiencia “¿A que saben los colores?” se apoya en la calidad de los proyectores de la marca, que permiten ofrecer una resolución excelente y adaptada al entorno y características del espacio, de una manera fiable, y con la mejor calidad de imagen. Ocho proyectores



Epson de 8000 lúmenes, con tecnología 3LCD y lentes periscópicas de ultracorta distancia, habilitan una experiencia visual 360°, con grandes sorpresas envolventes y dinámicas.

Detrás del nuevo restaurante Sinestesia, ubicado en el centro comercial Caleido del Paseo de la Castellana, se encuentran el empresario alicantino Perfecto Palacio y Jorge Palacio, así como APS Hostelería, empresa consultora líder en el sector de la hostelería con más de 20 años de experiencia. A través de Sinestesia, que es el primer restaurante de estas características en España y el quinto en todo el mundo, los impulsores de este proyecto tienen la intención de convertirse en una de las cadenas de gastronomía inmersiva líderes a nivel global.

LA OPINIÓN DE Fernando Jofre

TechRadar: referencia táctica y estratégica

La consultora tecnológica Devoteam acaba de publicar su tercera edición anual de la guía TechRadar. La de 2024 vuelve a ser sin duda una referencia, una más que interesante fuente de información sobre las últimas tendencias en el sector tecnológico. Y destinada a orientar a los decisores cualificados desde el punto de vista táctico y estratégico en su viaje de continua transformación digital.

Claramente dirigida a CIOs recoge 150 tecnologías agrupadas en diferentes áreas de interés: soluciones de negocio, inteligencia del dato, nube distribuida, automatización, confianza y ciberseguridad, y sostenibilidad.

No pretende ni mucho menos ser una guía exhaustiva ni un estudio de mercado, y para seleccionar y elaborar los contenidos han participado 96 tech leaders altamente especializados de la compañía en las áreas antes mencionadas, procedentes de diferentes países en los que opera la multinacional.

Las tecnologías se muestran en breves resúmenes muy directos que no van más allá de media página de extensión, expuestas desde un punto de vista independiente. Es

más, la propia consultora no trabaja necesariamente con todas las tecnologías mencionadas, si bien han sido analizadas con rigor para ofrecer la mejor opinión a sus clientes, y a los lectores en general. En su análisis además valoran cómo afrontar cada una de ellas... desde mantenerse atento, hasta adoptarlas, pasando por los estados de evaluar y realizar una prueba de concepto para así comprender cómo nos podría beneficiar a mayor escala.

Como no podría ser de otra manera, la Inteligencia Artificial generativa está presente de manera transversal a lo largo de toda la guía, porque está embebida en un tercio de las tecnologías analizadas. TechRadar es una guía de bolsillo altamente recomendable.



Qué podemos esperar de ASLAN2024



Bajo el tema "IA: Un Salto Importante en la Digitalización", se explorará el impacto de la Inteligencia Artificial (IA) en el proceso de innovación y transformación digital en el próximo ASLAN2024.

En su 31ª edición, se destacarán los desafíos y oportunidades que surgen al aplicar IA generativa en el entorno laboral, especialmente a través del espacio dedicado a "Potenciando el Entorno Laboral Digital con IA".

"Venimos recogiendo la historia de un sector que ha ganado relevancia en la economía del país. Este 31º congreso tiene una temática que ha conseguido atraer un 36% más de patrocinadores, y 140 de empresas participantes", explica Alberto Pascual, presidente de @aslan.

Alberto Pascual ha resaltado el aumento en la cantidad de miembros asociados, que alcanzan casi las 200 empresas. Este incremento también se ha reflejado en los datos de la nueva edición del

Congreso. El número de patrocinadores ha aumentado en un 36%, mientras que la participación de empresas ha crecido un 21%, alcanzando un total de 140 participantes.

Además, se ha registrado un incremento del 14% en el número de portavoces y del 21% en las entidades colaboradoras. Con estas cifras, los organizadores del evento también anticipan un aumento en la asistencia.

La evolución del puesto de trabajo hacia modelos híbridos o de teletrabajo ha sido impulsada por la IA generativa, que está transformando la manera en que se realizan las tareas.

Sin embargo, estos beneficios plantean desafíos en términos de privacidad de datos, calidad del contenido generado y casos de uso específicos. Para abordar estos desafíos, una sección del Palacio Municipal de Congresos de Madrid IFEMA reunirá empresas especializadas en sectores como transporte, salud y finanzas para presentar soluciones de IA aplicadas al puesto de trabajo.

ERP

EL MOTOR DE LA TRANSFORMACIÓN INDUSTRIAL Y LOGÍSTICA

GUÍAS GRATUITAS
¡SOLICÍTALAS YA!

El ERP es la herramienta estratégica para la transformación de

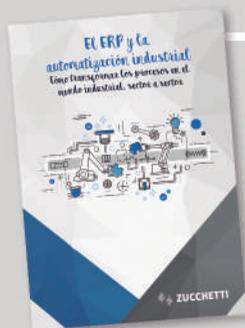
LA INDUSTRIA...

- Decisiones inteligentes, basadas en datos ✓
- Prevé la demanda ✓
- Controla la cadena de suministro ✓
- Optimiza la logística ✓

ERP

...Y LA DISTRIBUCIÓN

- ✓ Automatiza la gestión administrativa
- ✓ Controla la cadena de suministro
- ✓ Y enfócate en lo importante: las ventas y el servicio al cliente



EL ERP Y LA AUTOMATIZACIÓN INDUSTRIAL

Cómo transformar los procesos en el mundo industrial, sector a sector



DISTRIBUCIÓN 4.0.

El Software ERP, el motor de la transformación logística



El software que te acerca al éxito

94 427 13 62
www.zucchetti.es

LA OPINIÓN DE Manuel López

El FOMO de la IA

El término "FOMO" (del inglés "Fear Of Missing Out"), que traducido sería algo así como "temor a perderse algo", fue acuñado por el autor y empresario Patrick J. McGinnis en 2004, describiéndolo como: "una enfermedad que afecta a mucha gente, especialmente a las personas jóvenes, ambiciosas y conectadas".

Sin embargo, el concepto en sí ha existido probablemente desde mucho antes. Siempre ha habido gente que se siente ansiosa o preocupada por estar perdiéndose algo importante, pero la llegada de la era digital ha intensificado esta sensación y ha hecho que sea prevalente en nuestra sociedad.

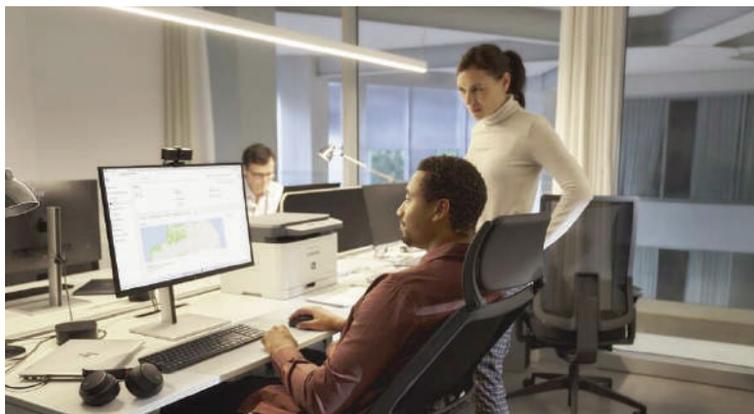
El FOMO, como concepto del mundo digital, se centró inicialmente en las redes sociales, pero se ha ido expandiendo a otras áreas del mundo digital como pueden ser el mundo del gaming, el Metaverso o el streaming de contenidos.

La Inteligencia Artificial no podía ser la excepción y recientemente está apareciendo un miedo atroz a quedarse fuera de la IA.

Este miedo está estallando como la pólvora, a medida que aparecen noticias de empresas que despiden trabajadores para sustituirlos por la IA o predicciones como la que hizo recientemente Sam Altman, CEO de OpenAI, que afirmó que el 95% de las tareas que actualmente son realizadas por profesionales de las agencias de Marketing serán ejecutadas por la IA.

De forma que la inquietud entre los trabajadores se está convirtiendo en ansiedad por querer no perderse nada de lo que está pasando en el mundo de la IA, aunque la mayoría no entienda nada de esta tecnología. Mucha gente asocia IA con plataformas como ChatGPT, que se está convirtiendo en una especie de parque de atracciones donde entretenerse con la IA. Pero lo cierto es que la IA se está integrando en el corazón de los procesos empresariales, sobre todo

El CISO, el profesional que más sube su sueldo



La empresa Setesca Talent, especializada en selección y gestión de talento, ha lanzado su informe anual sobre "Salarios estimados perfiles IT 2024" en la que se concluye que el CISO será el puesto que verá incrementado de forma más elevada su salario. Este estudio proporciona una visión detallada de las tendencias salariales y las condiciones laborales en el mercado de tecnología en España. El objetivo principal de este estudio es proporcionar una visión precisa de las condiciones de contratación para los perfiles tecnológicos en España. Esto permite a las empresas tomar decisiones informadas que se adapten tanto a la oferta como a la demanda del mercado. Según el informe, en este 2024, la posición que espera ver más incrementado su salario es el CISO. El pasado año el incremento fue de un 15% y este año la previsión es que aumente en un 10%. El sueldo en este puesto oscila entre los 90.000 y los 120.000 brutos

anuales. En segundo lugar, se encuentran, en cuanto a previsión de incremento de salario se refiere, el Governance Manager, el Data Manager y el CIO. Se espera que estos perfiles aumenten su nómina en un 5%. Las dos primeras posiciones oscilan entre los 50.000 y los 75.000 euros anuales, mientras que el CIO está entre los 120.000 y los 180.000 euros anuales.

En cuanto a los incentivos más comunes, se encuentra, en primer lugar, la jornada intensiva durante los meses de verano (85%). Le sigue el horario flexible de entrada y salida con un 82% y, en tercer lugar, la formación bonificada (64%). Muy de cerca, con un porcentaje de un 62%, está el teletrabajo.

Entre las principales conclusiones que desvela el estudio se encuentra que se ha registrado un aumento salarial promedio de alrededor del 4% en el panorama laboral del 2024. Este aumento ha sido más notable en áreas como ciberseguridad y consultoría.



Experiencias digitales creadas para ti.

Con la plataforma DXP de Liferay podrás crear experiencias eficaces que aportarán valor añadido a tu organización. Con soluciones para clientes, empleados, proveedores y partners, Liferay te ofrece la flexibilidad necesaria para cubrir las necesidades de tu negocio.



Intranets



Portal de proveedores y partners



Portal de clientes



Sitios Web

Utilizado por más de 1.200 clientes en todo el mundo

Descubre más:



LA OPINIÓN DE
Daniel Puente

Deepfake as a Service

Llevamos meses advirtiéndolo que el abanico de amenazas se amplía y mucho con la llegada de la IA. Una de las novedades con las que nos estamos enfrentando últimamente es con la proliferación de los deepfakes, esas estafas en las que se suplanta a una persona con poder decisorio en una empresa e intenta convencer habitualmente al CFO a que realice una transferencia a una cuenta no conocida y con un argumento en parte peregrino, pero sobre todo de una urgencia inusitada. Pues bien, esos deepfakes acostumbraban a llegar en formato audio, una llamada o incluso una nota de voz en la app de mensajería favorita. La novedad vista en estas últimas fechas es que ya no solo se generan en audio, sino que es posible realizarlas con video, de forma que el usuario destinatario, la víctima, está viendo a su responsable y oyéndole. Esto nos lleva incluso a plantearnos qué tanta culpa tiene en el caso de realizar la transacción en cuestión, y es que, cuando el nivel de sofisticación es tan elevado, la culpa de no reconocerlo creo que no debe caer en la víctima, ya que el método dista mucho de ser burdo. Conocedores de esta problemática, existen ya varias empresas que analizan las reuniones que estás teniendo, en todas las plataformas existentes, y, mediante la forma de mover el rostro, el tono y la musicalidad de la voz, puede llegar a detectar si es una llamada falsa. Como el fin de este tipo de engaños es el lucro máximo, incluso hemos podido constatar que hay grupos vendiendo este tipo de solución como SaaS, debiendo alimentarlos con la mayor cantidad de audio y video posible, pero que prometen resultados a partir de los quince segundos de aportación. Todo esto nos lleva a plantearnos si, una empresa que no adopte alguna de las soluciones de seguridad antes propuestas, estará realizando una dejadez de funciones en materia de seguridad. En mi opinión, el abanico se abre tanto, que cubrirlo entero se está convirtiendo en tarea prácticamente imposible.



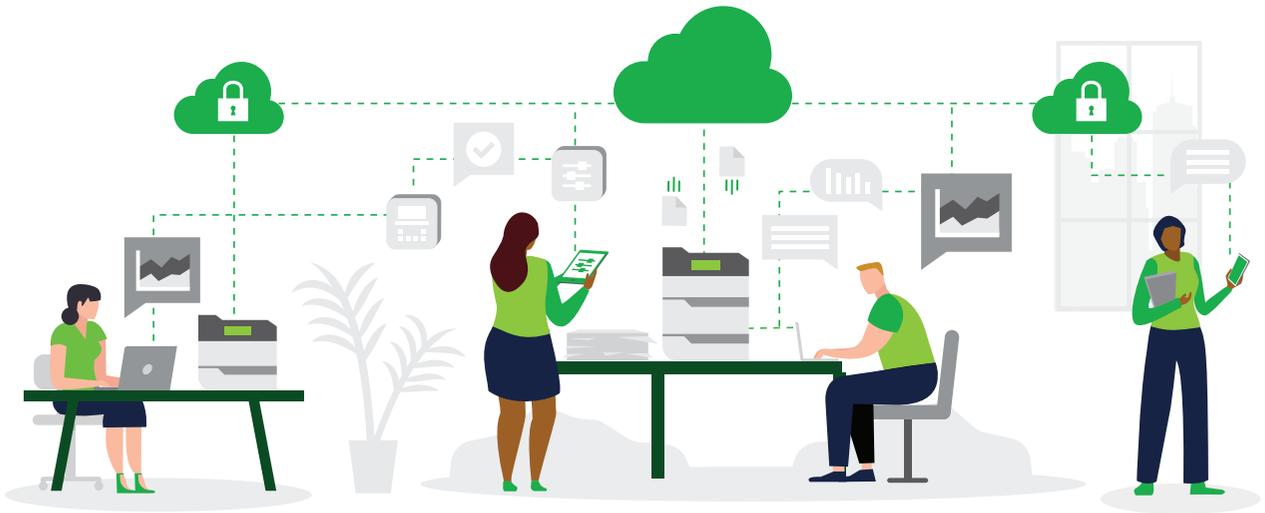
Neoris abre su hub europeo de IA



En un encuentro con los medios especializados, Neoris mostró su satisfacción por los resultados obtenidos en el último año y avanzó unas previsiones optimistas de cara a este mismo año. La compañía involucrada desde hace más de 20 años en la transformación digital de las empresas considera clave la evolución que está teniendo el CIO en los últimos años. Tal y como explicó Luis Álvarez Satorre, presidente de EMEA de la compañía, “el papel del CIO está cambiando. Ahora han pasado de ser responsables de infraestructura a ser los cómplices del negocio. Esto está provocando rotación en el mundo del CIO porque las empresas buscan un perfil diferente”. El máximo responsable cree además que hay dos elementos que van a seguir impactando en las organizaciones en los próximos meses. Empezando por la tecnología de moda: la Inteligencia Artificial generativa. En este sentido, Álvarez Satorre indicó que “en es-

tos momentos, la IA generativa se está asumiendo por parte de las empresas con una mezcla de sorpresa, entusiasmo y escepticismo. La IA generativa cambia el paradigma del mercado pero no era una tecnología que fuera esperada por lo que las empresas no saben que hacer con ella. Nosotros abogamos por el mix Machine Learning e IA generativa”. El directivo señaló que además se va a producir más migración a la nube. Los máximos responsables de Neoris ha anunciado además la apertura de un Hub de IA Europeo en España y el inicio de operaciones en Reino Unido. El Hub de IA Europeo tendrá un enfoque híbrido y combinará un espacio físico, que se emplazará en las oficinas de NEORIS en Madrid y que se inaugurará a lo largo de este año, con una plataforma digital centrada en la creación y divulgación de conocimiento relacionado con esta tecnología. El proyecto europeo analizará, investigará y definirá cómo utilizar la IA y sacarle el máximo partido.

Lexmark Cloud Services



Mejore la conexión en la nube segura y flexible para su gestión de la impresión

La innovación en tecnologías de impresión basadas en la nube continúa creciendo. Aproveche al máximo la tecnología de impresión en la nube líder del sector en conectividad avanzada, gestión remota y soluciones de impresión seguras.

Cloud Print Management

Simplifique la impresión basada en la nube, optimice la gestión de flotas y aumente la seguridad

Cloud Fleet Management

Gestione dispositivos de clientes en cualquier momento y lugar

Cloud Bridge

Potencie la flexibilidad en el lugar de trabajo con una suite de conectividad avanzada.

Cloud Connector

Conecte su empresa sin esfuerzo a las aplicaciones en la nube más populares

Cloud Print Infrastructure

Acceso a un entorno de impresión moderno y seguro a través de un servicio por suscripción, en el que se paga por la capacidad de impresión en lugar de poseer y gestionar la infraestructura física.

Cloud Scan Management

Digitalice y comparta archivos directamente para ahorrar tiempo y recursos

Lexmark Translation Assistant

Traducción de documentos en tiempo real al alcance de su mano

Scan Me



Cómo abordar los retos asociados a la continuidad de negocio



¿Están las organizaciones realmente preparadas para enfrentar los distintos desafíos que amenazan su operativa diaria? El impacto derivado de la interrupción de la actividad de cualquier organización, ya sea pública o privada, es diverso y crítico, desde económicas a reputacionales. Raquel Pinillos, Business Solutions Director de Kyocera, profundiza sobre la importancia de garantizar la continuidad de negocio ante cualquier situación crítica, los principales riesgos que existen y cómo hacerles frente.

La continuidad de negocio, entendida como la capacidad de una organización de mantener su operativa ante cualquier situación, es fundamental para la sostenibilidad de los negocios. ¿Son las organizaciones conscientes de esto?

En un entorno tan cambiante como el actual, tanto las empresas como administración pública están constantemente sometidos a cambios y desafíos imprevistos que pueden poner en

riesgo su operativa diaria. Para afrontar este tipo de situaciones de manera satisfactoria, es fundamental contar con un plan que incluya la identificación de las potenciales amenazas a las que se pueden enfrentar la organización, los impactos sobre las operaciones que dichas amenazas puedan causar y la gestión de la recuperación de las actividades en caso de producirse una interrupción.

Sin embargo, los datos nos demuestran que todavía hay mucho camino que recorrer a la hora de pasar de la teoría a la práctica. Así vemos que las organizaciones son conscientes de los riesgos existentes, pero que podrían no estar preparadas para enfrentarlos en caso de ser necesario. De hecho, del estudio Logicalis Global CIO Survey, que analiza el papel del CIO como agente de transformación digital en el mundo de los negocios, podemos extraer que, aunque nueve de cada diez CIO reconocen que sus empresas sufrirán alguna amenaza seria en los próximos 12 meses, el 60% de los encuestados no cuenta con un plan de continuidad de negocio que les permita garantizar el mantenimiento de su operativa. Este porcentaje es un indicador e implica una oportunidad y reto para Kyocera en el acompañamiento a las organizaciones y asegurar la continuidad de negocio.

¿Cuáles son los principales riesgos que afrontan las empresas e instituciones públicas con relación a la continuidad del negocio?

Cada vez más las empresas y organizaciones tanto de índole público como privado basan su actividad en los sistemas de información. La infraestructura tecnológica que soporta esta actividad pasa a formar parte de uno de sus principales activos. La interrupción de dicha infraestructura puede provocar perjuicios de diversa índole, no solo económicos sino también reputacionales

Además el contexto socioeconómico, que en la actualidad se caracteriza por una gran inestabilidad, es en sí mismo uno de los principales riesgos para el entramado empresarial. De hecho, en los últimos años hemos asistido a distintos acontecimientos que han representado importantes desafíos para la continuidad de muchos negocios: riesgos geopolíticos, escasez de semiconductores, cifras récord de inflación... por no hablar de la crisis de la COVID-19, que supuso un punto de inflexión en este sentido, obligando a muchas organizaciones a modificar por completo sus procesos de trabajo con el objetivo de garantizar el mantenimiento de sus operaciones. Por eso, durante la pandemia pusimos todo el conocimiento y la experiencia de Kyocera al servicio de nuestros clientes, ayudando a asegurar la operativa de servicios esenciales como centros de salud o cuerpos y fuerzas de seguridad del Estado.

Además, durante el I Foro de Continuidad de Negocio que organizamos desde Kyocera el pasado mes de febrero y al que acudieron distintos CIOs de la administración pública y del entorno privado, se pusieron sobre la mesa interesantes temas relacionados con las soluciones que habilitan la continuidad de las operaciones, así como su ejemplificación con buenas prácticas. Tanto los responsables como los agentes tecnológicos que protagonizaron su mesa redonda específica coincidieron en el papel protagonista de la ciberseguridad en el mantenimiento de las operaciones. Gran parte de las situaciones que comprometen la operativa diaria de las compañías están cau-

“En Kyocera consideramos fundamentales cinco pilares para responder al reto de garantizar la operativa TIC: prevención, concienciación, protección, disponibilidad y plan de recuperación”

sadas por ciberataques, que normalmente acceden por herramientas de uso tan cotidiano como puede ser el e-mail.

¿Cómo protegerse ante este tipo de situaciones de riesgo?

Aunque está claro que hay distintas situaciones que surgen de manera improvisada, nuestra recomendación es siempre contar con ese Plan de Continuidad de Negocio que garanticen los 5 pilares que en Kyocera consideramos fundamentales para responder al reto de garantizar la operativa TIC: Prevención, concienciación, protección, disponibilidad y plan de recuperación. Por supuesto, no debemos olvidar que la tecnología, que nos brinda distintas herramientas y soluciones para anticiparnos a todos los posibles problemas de interrupción de la operativa y garantizar la resiliencia del negocio.

En Kyocera llevamos más de 20 años gestionando servicios y operando procesos. Por eso, somos conscientes de la importancia de la continuidad de negocio y los graves inconvenientes que puede acarrear un parón en la operativa. Fruto de nuestra experiencia, el papel de Kyocera es el de aportar experiencia, orquestar conocimiento y ofrecer la mejor respuesta tecnológica seleccionando, desarrollando, integrando y operando soluciones IT en las organizaciones.

Nuestra propuesta de valor y experiencia incluye servicios gestionados IT enfocados a la hiperautomatización y eficiencia de procesos, servicios de desarrollo, orquestación y arquitectura y soluciones TIC para la continuidad de negocio tanto en infraestructura como puesto de trabajo bajo el paradigma de la experiencia usuario.

En cuanto a la continuidad del negocio nuestras soluciones abarcan la prevención, por ejemplo, a través de la observabilidad o el back up; la protección a través de soluciones de protección de correo, AD, compliance, borrado o gestión de identidades; la concienciación, especialmente a través de plataformas de concienciación y formación; la disponibilidad con soluciones de virtualización, replicación, servicios cloud, apps y el plan de recuperación con soluciones de disaster recovery o recuperación de AD, correo, BBDD, file servers.

La verdadera ciberresiliencia empieza antes del ataque



Por **Sandra Espinoza Ávalos**,
SaaS System Engineer Manager
para EMEA+APC de Commvault

En el panorama empresarial actual, se ha llegado a un punto de inflexión, en el que la confluencia de datos, aplicaciones y dispositivos se encuentra con arquitecturas híbridas y una nueva generación de amenazas. Una tormenta perfecta de casos que está dejando a las organizaciones más vulnerables que nunca.

Según un informe de IDC, el 61% de las empresas prevé una pérdida de datos en

los próximos 12 meses, debido a ataques como el ransomware. Y el 59% espera que, si eso ocurre, tardará días e incluso semanas, en recuperar sus datos. Por otro lado, datos de Microsoft apuntan a que el 99% de los objetivos de ataque del ransomware son la seguridad de las empresas y sus herramientas de recuperación. Es decir, los ciberdelincuentes no buscan sólo robar y secuestrar datos para cobrar un rescate, sino destruir. Imaginemos lo que esto supone para la reputación de una empresa.

Hoy en día, el dato es el activo estratégico más importante para una organización. Y eso lo convierte en la gasolina para cualquier atacante. Cuantificar el negocio del ransomware asusta. En 2023 el ransomware movió 30 billones de dólares. Además, cada vez es más sofisticado, y se alimenta de la IA para aumentar su superficie de ataque y poner en marcha nuevas prácticas más rápidamente.

UN GIRO HACIA LA CIBERRESILIENCIA

Por eso es tan necesaria la ciberresiliencia en las empresas. No sólo la búsqueda y detección de malware,

sino la capacidad de responder y de recuperar el negocio en el menor tiempo posible ante un ataque.

Si nos fijamos en marcos de seguridad tan conocidos como MITRE o NIST, vemos que la verdadera ciberresiliencia comienza antes de un ataque y, en realidad, no termina nunca. En nuestro trabajo diario vemos cómo muchas organizaciones dependen aún de un mosaico manual de aplicaciones legacy heredadas y de soluciones de nube que suponen una brecha importante – esto supone puertas de entrada y riesgos latentes.

ALERTA TEMPRANA

La solución se encuentra en una combinación de alerta temprana, salas limpias, análisis de riesgos, tratamiento de datos sensibles y remediación de amenazas, apoyados en la escalabilidad de la nube para inmediatez. Y esto es lo que aporta Commvault Cloud además de la habilidad de probar, probar y probar, ya que comprobar un plan de resiliencia es básico.

Commvault Cloud está especialmente diseñada para la resiliencia cibernética, y permite predecir las amenazas con mayor rapidez, realizar recuperaciones limpias y acelerar los tiempos de respuesta ante las amenazas, todo ello con el menor coste total de propiedad posible. Y, con la arquitectura única de Commvault Cloud, los clientes pueden asegurar y recuperar sus datos a través de cualquier carga de trabajo, infraestructura y desde cualquier lugar a cualquier lugar. Además, utiliza la IA para mejorar la ciberresiliencia y tomar medidas para proteger los datos. Y, por primera vez en la industria, ofrece una cleanroom (o sala limpia) para asegurar las recuperaciones limpias.

Lograr la ciberresiliencia empresarial es algo más que construir muros más altos o fosos más profundos. Requiere un nuevo enfoque que contemple de forma holística todo el panorama, desde la mejor protección y seguridad de datos hasta la inteligencia de datos impulsada por IA y la recuperación ultrarrápida. Con estas capacidades Commvault Cloud es el nuevo estándar en ciberresiliencia.

Optimizar las conexiones en las pymes



La necesidad de una mayor velocidad en las conexiones inalámbricas es una realidad para todas las empresas y negocios que realzan su actividad en el entorno digital. Si con WiFi6E se alcanzan velocidades de hasta 5 Gbps en un punto de acceso, la llegada de WiFi7 multiplica por cinco esa capacidad. El nuevo estándar es una garantía de futuro para la conectividad inalámbrica en el mundo de los negocios. Sin duda es significativamente más rápido y mucho más capaz de soportar altas cifras de usuarios proporcionando una mejor experiencia.

WiFi7 cuenta con 4.096 modulaciones de amplitud en cuadratura (QAM), lo que implica poder enviar más datos en un solo canal, ampliando el ancho de banda. Esta velocidad de transferencia es ideal para gran densidad de datos, como vídeo de alta definición o para realizar videoconferencias, permitiendo conexiones más fluidas, de calidad de imagen y más consistentes, incluso en entornos de alta densidad. Gracias a la aparición de los primeros dispositivos que lo incorporan ya se puede vivir la experiencia, si bien, a lo largo de este año veremos como muchos fabricantes se sumarán a esta corriente para marcar diferencia.

ADELANTÁNDOSE AL FUTURO

Zyxel Networks ha sido uno de los primeros desarrolladores de redes especializados en lanzar un punto de acceso WiFi7, WBE660S, que ofrece velocidades

de hasta 22 Gbps para que los clientes puedan beneficiarse cuanto antes del rendimiento ultraelevado del nuevo estándar. Si bien, en los próximos meses ampliaremos la gama con nuevas soluciones adecuadas a los diferentes casos de uso y escalas de despliegue. WiFi7 añade compatibilidad con nuevos canales extraanchos de 320 MHz en la banda de 6 GHz, lo que duplica la capacidad de ancho de banda para dar cabida a más dispositivos simultáneamente. Además, el rendimiento de la latencia de WiFi 7 ha mejorado significativamente gracias a las nuevas funciones, como la operación multienlace (MLO). La gama de soluciones cuenta con un diseño de antena inteligente que mitiga eficazmente las interferencias entre canales y se adapta dinámicamente para mejorar el rendimiento y la cobertura wifi.

EN LÍNEA CON LAS PYMES

Para el mundo de la empresa, esta tecnología supone un avance decisivo. Hoy utilizamos (PoE) para conectar puntos de acceso WiFi (AP) y otros dispositivos IP, por lo que se necesita un rendimiento más elevado, principalmente por tener que soportar conexiones inalámbricas más rápidas. Y esto es igual tanto para las pymes como para las grandes organizaciones, porque las pymes utilizan las videoconferencias, la ciberseguridad y los datos tanto como las grandes empresas. Sólo tienen redes proporcionalmente más pequeñas. Por eso, Zyxel ha lanzado los switches de la serie XMG1915 de 8 y 16 puertos, que admiten velocidades de 2,5 Gbps y hasta 60 W PoE por puerto (PoE++) en hasta 8 puertos. Estas soluciones tienen el rendimiento y el ancho de banda necesarios para satisfacer las más altas exigencias de las aplicaciones modernas en las pymes. Entre sus ventajas destaca que se pueden configurar y controlar a través de nuestra plataforma en la nube Nebula. Siempre apoyamos a los pequeños y medianos negocios con la tecnología que puede ayudarles hoy a abrir la puerta al futuro.

Por Gonzalo Echeverría
Country Manager Zyxel Iberia

Unificar la seguridad en la nube más allá de los silos



Por José de la Cruz,
director técnico de Trend Micro Iberia

El mercado de la seguridad de la carga de trabajo en la nube (CWS) ha consolidado rápidamente capacidades como la gestión de derechos de infraestructura en la nube (CIEM), la gestión de la postura de seguridad en la nube (CSPM), etc., en su oferta. Pero a pesar de ser un producto más robusto, a menudo sigue estando solo en la infraestructura de seguridad de una organización. Teniendo en cuenta que los ataques no siempre se originan y permanecen en la nube, está claro que un enfoque aislado no es la opción más segura.

Las organizaciones deben priorizar el cambio de herramientas de seguridad individuales para pasar a plataformas de ciberseguridad interconectadas que respondan a las amenazas con mayor eficacia. Cuando evalúe a un proveedor, tenga en cuenta su estrategia a largo plazo y su visión global.

Nuestra estrategia de seguridad con visión de futuro consolida la oferta de CWS en su moderna plataforma de ciberseguridad impulsada por IA para proporcionar visibilidad central, gestión proactiva de riesgos y detección y respuesta más rápidas. Profundicemos un poco más en la ventaja de esta plataforma.

LA VENTAJA DE LA PLATAFORMA

Trend Vision One™ – Cloud Security es una tecnología

avanzada con CSPM, análisis de vulnerabilidades y malware sin agente, visibilidad de API, comprobación de cumplimiento y mucho más. Además, protege las cargas de trabajo tanto si se ejecutan en AWS, Microsoft Azure, servicios GCP, en múltiples nubes o en las instalaciones. Pero más allá de la amplitud y profundidad de sus capacidades en la nube, también forma parte de la plataforma Trend Vision One™.

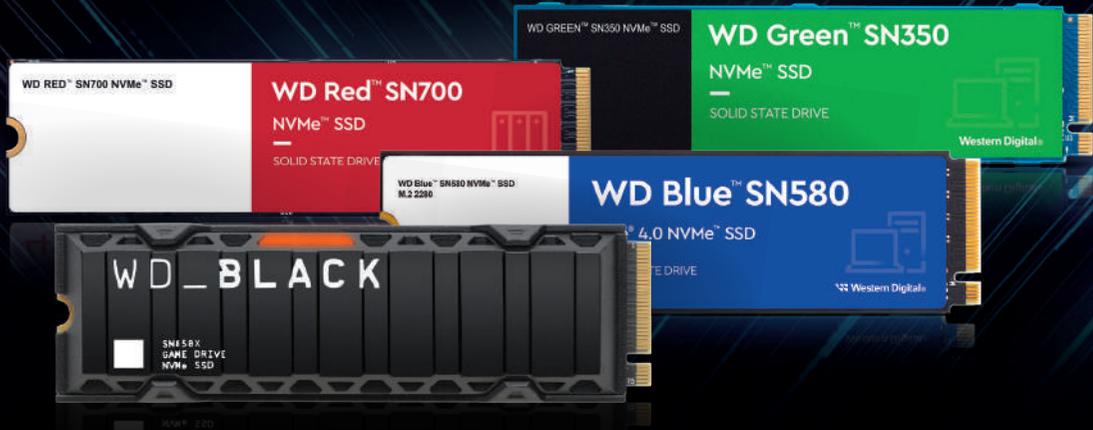
La telemetría de CWS desde los centros de datos hasta las cargas de trabajo en la nube, las aplicaciones y las arquitecturas nativas de la nube se introduce en la plataforma Trend Vision One y se correlaciona con los datos de las redes, cargas de trabajo, endpoints, correo electrónico e identidades. Esta integración es la clave para mejorar la visibilidad en los complejos entornos de nube híbrida y multicloud de una organización, además de ofrecer otras ventajas como una detección de amenazas más rápida impulsada por tecnología XDR; una evaluación de riesgos y priorización más ágiles; aplicación de políticas coherentes; evaluación de riesgos y controles de seguridad independientemente de dónde se ejecuten las cargas de trabajo, todo desde un único lugar; y colaboración entre las distintas partes interesadas en seguridad en equipos de nube, ITOps, SOC, etc., al reunir las herramientas individuales en una sola plataforma.

CONCLUSIÓN

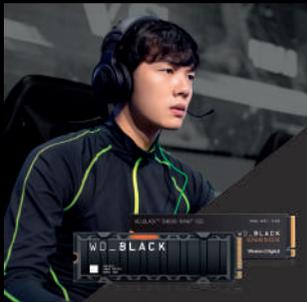
Recuerde: los ataques no siempre se originan y permanecen exclusivamente en la nube. Una oferta de CWS debe consolidarse en una plataforma integral para que los equipos de seguridad puedan ver toda la cadena de ataque y remediar el riesgo antes.

Más allá de elegir la mejor opción de plataforma, elija al mejor partner a largo plazo. Si le han vendido un gran producto, pero no está seguro de si está configurado correctamente para un uso óptimo porque el servicio de atención al cliente es inexistente, ese elegante artilugio no sirve para nada. Y puesto que las ciberamenazas y la delincuencia no van a desaparecer pronto (o quizá nunca), necesita un partner que se comprometa a largo plazo, creciendo y adaptándose con usted al panorama digital y de amenazas en constante evolución.

Lleva tu dispositivo a otro nivel con los discos Western Digital® NVMe™



Las unidades NVMe™ suponen un enorme salto de rendimiento respecto a las unidades SATA, con velocidades de lectura hasta 13 veces superiores*, ya que la interfaz y los protocolos SATA se basan en la tecnología de los discos duros. Todos los nuevos PCs y portátiles utilizan ahora unidades SSD M.2 PCIe® NVMe™ y Microsoft requiere un SSD NVMe™ para la compatibilidad con DirectStorage para juegos acelerados.



WD_BLACK™ con alto rendimiento para gamers y compatibilidad con DirectStorage para juegos de PC de próxima generación, unidades NVMe con licencia para PS5 y gran ancho de banda para aplicaciones exigentes.



WD Blue™ para Creadores, el favorito para los profesionales DIY y creativos.



WD Red™ para NAS, proporciona almacenamiento en caché rápido para un acceso acelerado y pools de almacenamiento de alto rendimiento para máquinas virtuales o edición de vídeo, manteniéndose al día con el creciente ancho de banda de la red.



WD Green™ para mejorar las tareas informáticas cotidianas realizadas con tu PC, como navegar por Internet, estudiar y trabajar desde casa.

JUEGA | CREA | COMPARTE | ACTUALIZA

westerndigital.com/solutions/internal-ssd

*Comparación entre WD_BLACK SN850X y WD Blue SATA SA510 1TB. Western Digital, el diseño de Western Digital, el logotipo de Western Digital, myWD, el logotipo de myWD, WD_BLACK, WD Blue, WD Red y WD Green son marcas registradas o marcas comerciales de Western Digital Corporation o sus filiales en Estados Unidos y/o en otros países. Las marcas con las palabras NVMe y NVMe-oF son marcas comerciales de NVM Express, Inc. PCIe es una marca registrada de PCI-SIG Corporation. PS5 es una marca registrada de Sony Interactive Entertainment Inc. en los Estados Unidos y/o en otros países. Todas las demás marcas pertenecen a sus respectivos propietarios. Las imágenes mostradas pueden diferir del producto real. ©2023 Western Digital Corporation o sus filiales. Todos los derechos reservados.

Adaptando cloud con ciberseguridad



A pesar de la madurez de los servicios en la nube, el 72% de los líderes de TI aún perciben la seguridad como un obstáculo significativo para la adopción del cloud público. El 95% de los incidentes de seguridad se atribuyen a errores de configuración en la plataforma del cliente y el 63% de las aplicaciones SaaS operan sin el gobierno móvil de IT. Con todo ello, es primordial integrar la función de seguridad con el desarrollo, las operaciones y la gestión de riesgos.

Por Vanesa García y Manuel Navarro

Para hablar sobre esto y profundizar en el futuro de la nube y su seguridad, Byte TI organizó el encuentro, "Adaptando cloud con ciberseguridad", con ponentes de algunas de las principales empresas del mercado español y que contó con el patrocinio de Commvault, HPE Aruba, Palo Alto Networks, Infoblox, Trend Micro, AWS, IaaS365, Nutanix, ARCserve, Kaspersky, HornetSecurity y Logicalis.

Tras la apertura del encuentro, Alberto Pérez, Business Development Manager de HPE Aruba Networking analizó cuál es el papel que está jugando SASE en las estrategias de ciberseguridad de las empresas. Tal y como explicó Pérez, "es ne-

cesario establecer un nuevo enfoque en seguridad que garantice un acceso seguro desde el Edge, donde se genera la productividad, abarcando cualquier dispositivo o entidad que maneje datos. Por ello surge SASE, como respuesta a esta necesidad, evolucionando con el paradigma del cloud y superando las limitaciones de los modelos de seguridad obsoletos. SASE redefine la seguridad tradicional al considerar no solo los flujos de comunicación, sino también el perfil y comportamiento de los usuarios y dispositivos, así como la naturaleza de los aplicativos y datos que manejan". Tal y como expuso, en el enfoque que manejan en HPE Aruba se integra la filosofía de se-

guridad en cada nivel, desde la conectividad local hasta la WAN, con una experiencia de usuario consistente, independientemente de la ubicación o el tipo de aplicaciones a las que se accede”.

LOS RETOS DE GESTIONAR LA NUBE

La primera de las mesas de debate abordó cuáles son los principales retos a los que se enfrentan las empresas a la hora de gestionar la nube. Integrada por Víctor Blanco Rodríguez, CIO de Cepsa Exploration & Production; Sandra Pedraza, CIO de Cruz Roja; David Vaquero, CTO de Nationale-Nederlanden; Fernando Calvo Business Development Manager de IaaS365 y Cloud Champion Partner de Nutanix, y Pedro Viana, director de preventa de Kaspersky, se abordó cómo la nube híbrida es el modelo que están adoptando las organizaciones de forma mayoritaria.

Sandra Pedraza, CIO de Cruz Roja, afirmó que en el caso de su organización “realizamos un análisis completo de nuestra situación actual de las cargas, como estábamos gestionando, cómo estaban desarrolladas nuestras aplicaciones previamente a subirlo a la nube, porque sí es verdad que al final si no haces eso, el tema de los costes sale negativo hacia un proyecto que de verdad es ventajoso”.

“En el caso de Cepsa, nosotros estamos en distintas geografías y cada una tiene su regulación. Unas están más abiertas a la nube, otras no, y luego también hay ubicaciones remotas en las que estamos nosotros. Por eso apostamos por un ecosistema de nube híbrida. Lo primero que hay que hacer para migrar a la nube es tener un plan y todos los que estamos aquí, si no lo tenemos, deberíamos intentar tenerlo hoy o mañana, porque el modelo cloud combina muchas cosas”, añade Víctor Blanco Rodríguez, CIO de Cepsa Exploration and Production.

En esa estrategia, definir de forma clara los procesos es uno de los problemas habituales con los que se enfrentan los departamentos de TI. En este sentido, David Vaquero, CTO de Nationale-Nederlanden, afirmó que “es fundamental cuando se migra a la nube y pasamos desde on-premise, identificar todos nuestros componentes funcionales y por tanto, componentes técnicos y no mezclar dentro del componente técnico, no mezclar diferentes nubes, porque entonces tendríamos un problema grave a nivel de integración. Por lo tanto, cuanto más hagamos en la parte de arquitectura y de seguridad también mucho mejor para poder llegar a a buen puerto”

Una vez desarrollada la estrategia, es el momento de pensar en el multicloud. Y apostar por este modelo, conlleva también afrontar la parte de ciberseguridad. En este aspecto, Pedro Viana, director de preventa de Kaspersky, afirmó que “cuando pasamos a un entorno multicloud desaparece el perímetro. En este contexto, la monitorización es fundamental. Hay que entender qué es lo que está ocurriendo. Un buen plan de migración, un plan de un guardia en el cloud, sea público, híbrido, o privado debe contar con la monitorización para proteger los datos”

Por su parte, Fernando Calvo Business Development Manager de IaaS365 y Cloud Champion Partner de Nutanix se centró en explicar cómo ven la transición de los clientes del mundo híbrido al multicloud. Tal y como aseguró, “nosotros somos una empresa que nació 100% cloud y nuestro objetivo siempre ha sido el de ayudar a los clientes a que vean cómo pueden conseguir la mejor optimización de sus recursos. En la transición del mundo híbrido al multicloud, nosotros tenemos herramientas para facilitar la gestión de la parte multicloud. Para

ello nos juntamos con nuestros partners y con nuestros clientes y analizamos cómo son cada una de esas cargas multicloud que tienen. Analizamos costes, recursos, rendimiento,... y a partir de ahí, y viendo todos los factores, desarrollamos la estrategia adecuada para cada cliente”.

RANSOMWARE Y CIBERSEGURIDAD

El ransomware es una de las principales preocupaciones de seguridad que tienen las empresas. Se estima que para el año 2031, los daños causados por el ransomware podrían superar los 265.000 millones de dólares, lo que subraya la urgencia de proteger los datos contra esta amenaza. Jesús Carro, Principal Consultant, Pre-Sales de Arceserve, afirmó en su ponencia que “en la actualidad, nos encontramos en una fase de transición hacia un entorno multicloud desde un modelo anterior de on-premise a cloud híbrido. Por ello, la protección de datos en entornos variados es crucial debido a las diferentes necesidades y regulaciones de cada cliente. En lo que respecta al ransomware, es fundamental tener un plan de acción definido y probado para responder a los ataques. La protección de datos en entornos multicloud y SaaS es necesaria, y es importante mantener copias de seguridad inmutables en diferentes medios y ubicaciones. La inmutabilidad de los datos y las soluciones de almacenamiento inmutable son cruciales para proteger la información contra el ransomware”.

ENSAMBLAJE INFALIBLE

La nube y la ciberseguridad son dos términos que están relacionados desde que las empresas empezaron a adoptar de forma masiva la tecnología cloud. El problema es integrar el poder de la nube con la seguridad cibernética. De esto trató la ponencia de Sandra Espinoza, International SaaS SE Manager de Commvault, quien afirmó que uno de los pasos para que la estrategia cloud de una empresa sea segura, es confiar en una empresa como Commvault que entiende la nube de forma nativa y muy flexible: “Entendemos su sistema operativo, su

idioma y somos capaces de integrarnos con cualquier tipo de nube”.

Para Espinoza, una de las claves es “abarcar la totalidad de los datos independientemente del tipo de dato del que se trate o de cuál es su ubicación. El dato ya no está controlado en un datacenter y en la red corporativa. Ahora reside en entornos híbridos, en nubes públicas o privadas o en el Edge. Por eso es fundamental ser capaces de protegerlo con garantía en todas sus formas y lugares y es aquí donde Commvault ofrece una serie de soluciones para cualquier situación”.

EVOLUCIÓN DE LA CIBERSEGURIDAD

Para analizar cómo se están desarrollando las estrategias de ciberseguridad en las empresas y cuáles son los principales riesgos, tuvo lugar una mesa redonda que contó con la participación de Javier Salas, CISO de Engie; David Moreno del Cerro, director de Sistemas de Seguridad de la Información de TENDAM; José Miguel Parejo IT Security Network Manager de Gestamp; José de la Cruz, director técnico de Trend Micro y Joaquín Gómez Cybersecurity Lead Southern Europe de Infoblox y que fue moderada por Vanesa García, redactora de Byte TI.

Javier Salas, CISO de Engie, señaló que “casi todas las empresas estamos mirando hacia la nube como un patrón nuevo de ataque. Tenemos infraestructuras críticas en la nube que tenemos que proteger, y el cómo lo proteges o cuál es el vector que dejas libre para cualquier ataque es responsabilidad nuestra. El problema es que muchas veces se trasladan cargas a la nube y luego se cuenta con la ciberseguridad cuando lo que hay que hacer es subir las cargas de forma ordenada y protegida desde el principio. El vector de protección en los dispositivos tiene que venir desde el diseño”.

Para Joaquín Gómez Cybersecurity Lead Southern Europe de Infoblox, “la gran estrategia que hay que tener es intentar reducir el tiempo en el que yo detecto algo, y como lo detecto. También reducir el tiempo de operación en contenerlo. Al final, lo que esta-



mos viendo es que las compañías están atacando la seguridad en la fase tardía, cuando ya ha entrado un malware”.

Por su parte, José de la Cruz, director técnico de Trend Micro, cree que “las empresas están añadiendo capas de seguridad una encima de otra, muchas veces sin sentido, y hay que dar un paso atrás. Hay que entender cuáles son los riesgos porque muchas veces ni siquiera se tiene protegido lo más básico y se está incrementando el coste en seguridad sin ni siquiera saber si se tienen vulnerabilidades”.

En este sentido, José Miguel Parejo IT Security Network Manager de Gestamp, afirmó que es muy importante realizar análisis de riesgos para identificar esas vulnerabilidades y construir los procesos e invertir en proteger esos procesos que son realmente críticos para el negocio. Si se cuenta con un determinado presupuesto anual hay que invertirlo en aquello donde se es más vulnerable y que a la empresa la va a suponer un mayor impacto en su negocio”.

ELIMINANDO LOS RIESGOS DE SEGURIDAD

Una de las claves es, precisamente, los riesgos que se asumen a la hora de elevar cargas al cloud. En su ponencia Jaime Querol, Prisma Cloud Sales Specialist de Palo Alto Networks, afirmó que “un 36% de las organizaciones ha optado por la aproximación de llevar la aplicación existente en on-premise a la nube”. Esta opción ha sido criticada por algunos como poco ventajosa económicamente y carente de beneficios tangibles. Por ello, Querol enfatiza que el 27% de las organizaciones ha elegido refactorizar y modernizar la aplicación existente en el datacenter para desplegarla en contenedores o en entornos Serverless, “la construcción desde cero de una aplicación nativa en la nube representa otra opción, que implica trabajar en desarrollo continuo, utilizar equipos de DevOps y desplegar en contenedores Serverless PaaS.”

Para el ponente de Palo Alto Networks, “la seguridad en el entorno de la nube requiere adaptar soluciones y mentalidades debido a que el perímetro tradicional ya no es aplicable. Existe una 'tormenta' entre innovación y riesgo, con el aumento del uso de la nube y la aceleración del desarrollo de software. Los riesgos asociados con las aplicaciones modernas incluyen vulnerabilidades en librerías open source, la creciente sofisticación de actores maliciosos y el desequilibrio entre desarrollo y seguridad”, recalca.



CIO VS CISO

¿Cómo es la relación del CIO y el CISO? Es una de las preguntas que se quisieron responder durante el evento y para ello se contó con la participación de José Luis Ruiz Revuelta y Fabián Vidal de la Fuente, CIO y CISO de Sanitas, respectivamente. Tal y como explicó Ruiz Revuelta, “los temas de seguridad son cosas que a veces puedes planificar y trabajar, y otras llegan en el peor momento. Nuestra interacción exige que nos llamemos mutuamente cuando pasa algo. En seguridad, es tan intenso el día a día que tenemos que estar atentos de lo que pasa, y nos lo comuniquemos cuanto antes”.

El trabajo entre ambos cargos debe ser un trabajo de equipo, tal y como aseguraron ambos ponentes. En este sentido, Vidal de la Fuente, afirmó que “cuando empiezas a gestionar equipos grandes asumes que no te vas a llevar bien con todos, y que no todos se van a llevar bien contigo. En nuestro caso, afortunadamente nos llevamos muy bien. Creo que para que la coordinación entre ambas funciones es muy importante que haya un relación de respeto”.

RETOS FUTUROS PARA GESTIONAR LA NUBE

Finalmente, el encuentro se cerró con los retos futuros en la gestión de la nube. En esta última mesa redonda Javier Torres, CISO de Allfunds; Enrique Martín, CSO de AXA, Gemma Martín, CIO de Grupo Suardiáz; Fernando Elejalde, Senior Cybersecurity Presales Consultant de Logicalis y Pedro Viana, Director Preventa de Kaspersky intentaron dar unas pinceladas de lo que se avencina en un futuro. Así, para Enrique Martín, CSO de AXA, “la IA es la tecnología que mayor impacto va a tener en el futuro en los temas de ciberseguridad. Estamos viendo que la inteligencia artificial está ya aquí. No es una tecnología que venga en el futuro, está aquí, y ya está impactando en los temas de seguridad”

“El tema de la computación cuántica o la alta computación en la nube, es otro de los retos de las tecnologías emergentes, que también van a tener mucho impacto, porque al final para procesar datos vamos a necesitar la velocidad de computación. Y parece ser que el tema de la de la computación cuántica está ya apareciendo, y en poco tiempo yo creo que lo vamos a tener integrado”.

Por su parte, Gemma Martín, CIO de Grupo Suardiáz, cree que una de las

claves es que “tenderemos a subir más cargas al cloud porque todo el almacenamiento es más barato que tenerlo on-premise, y porque toda la parte de la analítica de datos es mucho más fácil”.

Javier Torres, CISO de Allfunds, cree que “las herramientas que existen cloud nativas a día de hoy son mucho mejores que las que hay on-premise. Además, una clave va a estar en la computación cuántica que va a suponer un cambio brutal en lo que a rapidez de generación y de transformación de información se refiere. Y aquí va a estar una de las claves, porque los ciberdelincuentes van a tener exactamente la misma tecnología y un mayor nivel de inversión de lo que tenemos nosotros dentro de las compañías, con lo cual vamos a tener que gestionar tanto a nuestros equipos de negocio como a nuestros grupos de tecnología para indicarles los riesgos que van a tener a la hora de desarrollar esos casos de uso con computación cuántica o con inteligencia artificial”

Fernando Elejalde, Senior Cybersecurity Presales Consultant de Logicalis aseguró que “esta situación, esta lucha entre buenos y malos siempre ha estado ahí. Los malos han intentado atacar utilizando las herramientas disponibles y nosotros íbamos detrás. Ahora mismo la IA la están usando todas las empresas. Prácticamente es el presente. No es un futuro, no es un reto para un futuro un poco lejano, sino que ya es un presente”.

Finalmente, Pedro Viana, Director Preventa de Kaspersky., afirmó que “en lo relativo a la IA, los fabricantes de seguridad, la utilizamos para detectar patrones y comportamientos que nos permitan detectar, por ejemplo, un ataque de phishing. En cuanto a la computación cuántica hay que tener en cuenta que todo evoluciona y que también lo harán los algoritmos predictivos de detección de comportamiento, con lo cual los malos aprovecharán efectivamente ese aumento de capacidad de generación, mientras que nosotros aprovecharemos ese aumento de capacidad trabajando en mejorar aún más los algoritmos de detección”.

El rol de la mujer en el mundo TIC



Byte TI organizó un encuentro en el que se analizó cuál es la situación de la mujer en el sector TIC y por qué cuesta tanto que las más jóvenes apuesten por el estudio de carreras STEM. Al webinar, que contó con el patrocinio de Liferay, asistieron Beatriz Marco Burguete, CIO de Cantabria Labs; Mónica González, South West Europe CIO at PepsiCo; María Rosa Ribó, Directora Proyectos IT en ABACUS Coop y vocal de mujeres y tecnología de Ausape; Maica Aguilar, gerente de seguridad de Ferrovial y Beatriz Escobar, directora de ventas para España y Portugal de Liferay

La primera pregunta era obligada. ¿Cómo llegaron todas ellas al mundo TIC? María Rosa Ribó, Directora Proyectos IT en ABACUS Coop y vocal de mujeres y tecnología de Ausape aseguró que en su caso siempre le gustaron las Matemáticas y la física. Me licencié en física y ya, acabando la carrera, me decanté por temas de electricidad e informática. En seguida entré en una consultora con programación, análisis y luego ya dirigiendo proyectos”.

Por su parte, Beatriz Marco, CIO de Cantabria Labs afirmó que “no esperaba acabar en el mundo TIC y fue un mundo de casualidades. Empecé en el mundo de procesos, calidad y la tecnología ayuda mucho a mejorar procesos. Entonces, apareció una oportunidad de digitalizar muchos procesos, unir procesos, tecnología y personas, y tras esa oportunidad me ofrecieron la Dirección de Tecnología. Al principio me sorprendió, porque cuando te ofrecen la Dirección de Tecnología, piensas que tienes que saber mucho de productos y servidores. Es cierto que cuando empecé como directora de tecnología había muy pocas mujeres, pero lo bueno que tenemos es que cuando vamos apareciendo más mujeres en las áreas de tecnología, también concienciamos y permite ir incorporando mujeres a esas áreas”.

Al igual que ellas, Mónica González, South West Europe CIO at PepsiCo, también era una apasionada de las asignaturas más técnicas: “Tengo una forma de pensar muy lógica. Yo quería estudiar una carrera de Matemáticas o de Ciencias. A mi me influyó mucho una profesora de matemáticas que me sirvió un poco de inspiración y de entender que las mujeres también podemos estar allí. La verdad, yo nunca he pensado que por el hecho de ser mujer no pudiese hacer determinadas cosas, nunca lo he pensado. Pero es verdad que en las mujeres hay algunas cosas que nos pasa, y es que creo que tenemos menos seguridad a la hora de enfrentarnos a temas difíciles.

Beatriz Escobar, directora de ventas para España y Portugal de Liferay, difiere en cuanto a formación del resto: “Yo soy psicóloga, pero comparto su pasión por resolver conflictos, resolver problemas. Y al final lo puedes aplicar a la mente humana o lo puedes aplicar al mundo empresarial y al mundo de las tecnologías. Y por curiosidades del destino y probablemente por la necesidad y la demanda que siempre ha habido de perfiles técnicos, empecé a trabajar en el mundo de la consultoría, sobre todo de gestión documental, de procesos, y a partir de ahí fui un poco creciendo en este mundo de la tecnología. Mi formación de base me sirve porque a veces los clientes y los compañeros son los primeros

LOS PARTICIPANTES

a los que tenemos que entender para llegar a ser mejores. Creo que la mayor dificultad que me he encontrado he sido yo misma muchas veces, porque creo que algo en lo que somos diferentes, los hombres y las mujeres, es que tenemos muchas veces más inseguridad que los hombres”.

Finalmente, Maica Aguilar, gerente de seguridad de Ferrovial, explicó que “en mi caso, soy informática y a mi alrededor no tenía referentes informáticos. Nunca, cuando era pequeña, había habido un Spectrum en mi casa ni conocía a nadie que estuviera vinculado a este mundo. De estudiante era buena en matemáticas o en física, más que en las asignaturas de letras, aunque también se me daban bien. Lo que me llevó hacia la parte tecnológica fue demostrarme que cualquier dificultad es algo alcanzable. Pero es verdad que tenía más el foco en carreras como aeronáutica o como telecomunicaciones que en informática. Informática se presentó porque conocí a una persona que estaba estudiándola y que lo que me contó sobre la carrera me pareció como muy interesante. Así que la elección fue totalmente causal. Pero ahora viéndolo con perspectiva y un poco también en línea con lo que comentaban las compañeras, lo que está claro es que tú no puedes elegir aquello que no conoces. Por tanto, yo creo que todos en nuestro ámbito de actuación, en nuestro día a día, tenemos la responsabilidad de dar a conocer nuestras profesiones, de trasladar qué hacemos y que las siguientes generaciones sepan un poco lo que va detrás de ese trabajo, de ese estereotipo que tenemos en la cabeza. Porque es verdad que cuando tú piensas en informática, las ideas que te vienen a priori es que vas a estar todo el día delante de un ordenador, que vas a ser un poco friki y que no te vas a relacionar con los demás”.

POR QUÉ NO ESTUDIAN STEM

Los datos demuestran que en el bachillerato la rama biosanitaria, que también que es técnica, es elegida por más mujeres que hombres. Sin embargo, no ocurre lo mismo con la rama tecnológica. ¿A qué se debe? Para Maica Aguilar, “está claro que hombres y mujeres, teniendo los mismos derechos y obligaciones, somos diferentes. Y para nosotras, el contacto, la relación con los demás y el sentir que ayudamos a los demás nos motiva, es algo que nos gusta. Por eso creo que la rama biosanitaria tiene más de un 50% de mujeres. Pero hay un dato bastante significativo que me gustaría reseñar aquí. En los años 90 que es cuando yo estaba en la universidad, en la carrera informática, más o menos, en la técnica el porcentaje era 50-50. En la superior, es verdad que ya había menos mujeres, pero podíamos estar en torno a un 30%. Sin embargo, ahora las chicas que están entrando en las carreras de informática es de un 13%. Así que ¿qué es lo que estamos haciendo o qué es lo que no estamos vendiendo bien? Yo creo que es por desconocimiento y por estereotipos que hacen que las jóvenes vayan a otros estudios”.

Beatriz Marco cree que “las cuotas han beneficiado. Hay muchos comités de dirección, muchos consejos de administración, en los que que no había presencia femenina. Y eso ha ayudado mucho a concienciar a todas las compañías a que haya más presencia femenina y que se busque talento femenino. Eso es buenísimo. El problema es que las empresas están buscando talento, pero cuando van a la universidad a encontrarlo se encuentran con que como decía Maica, sólo hay un 13% de mujeres, con lo que, incluso estableciendo una política de cuotas, es muy difícil que haya una paridad”.

Para Mónica González, “estamos en una situación de anomalía total, y ya no solo en el sector de la tecnología, sino también en los puestos de dirección.



Beatriz Escobar, directora de ventas para España y Portugal de Liferay



Maica Aguilar, gerente de seguridad de Ferrovial



María Rosa Ribó, Directora Proyectos IT en ABACUS Coop y vocal de mujeres y tecnología de Ausape

La mayoría de los que llegan ahí son hombres, entonces es un tema de dar un mensaje también. Es verdad lo que dice que Beatriz que de la fuente de la que bebemos talentos no ofrece paridad. Para mí la potencia de las cuotas es el mensaje que estás dando a las generaciones que suben, de que es posible llegar ahí y que hay otras mujeres”.

María Rosa Ribó, cree que “hay que priorizar el talento y los méritos por delante, pero la situación actual, con los porcentajes que hay, es muy delicada y lo que hay que pro-

LOS PARTICIPANTES



Mónica González, South West Europe CIO at PepsiCo



Beatriz Marco Burguete, CIO de Cantabria Labs

mover es la incorporación de la mujer, evidentemente, para conseguir esta paridad. Creo que el talento tiene que ir por delante de todo, independientemente de que sea hombre y mujer, pero que hay que favorecer la incorporación de la mujer. Creo que hay unas políticas que están bien, pero que deberían ser temporales, porque hemos de conseguir dar la vuelta a esta situación. Tiene que haber políticas enfocadas en la educación para que más mujeres accedan a estos puestos y desde las propias empresas". Maica Aguilar se mostró positiva: "Ha habido un avance abismal en los 30 últimos años, pero seguimos teniendo que trabajar en ello. Hay un informe del World Economic Forum del verano pasado en el que decía que para que tengamos paridad de género, a nivel mundial, se necesitarían 151 años. Y en Europa, que estamos mucho mejor, para que llegemos a ese punto de equilibrio, se necesitarían 67 años, si no hacemos nada. Con lo que está claro que si queremos que al menos las dos siguientes generaciones estén en una situación mejor, hay que actuar y hay que ha-

cer cosas. Y bueno, aquí lo que traslado es que todos tenemos la posibilidad de hacer cosas para que esto vaya avanzando y vaya mejor, y que nuestros hijos se encuentren en un mundo más inclusivo, más diverso y con unas capacidades de llegar a todos los sitios más equilibradas". Beatriz Escobar, de Liferay, destacó que "es muy importante el apartado de tener referentes. Si se asocia el trabajo a la tecnología, al friki que está solo delante de un ordenador y no existen referentes positivos, pues es muy complicado que las mujeres se muevan hacia este tipo de desarrollos profesionales. Creo que el hecho de que las más jóvenes tengan referentes es lo que hará subir los porcentajes".

CONCILIACIÓN

La conciliación de la vida familiar y laboral es uno de los apartados más importantes en los que mejorar. La pandemia puso de manifiesto que se podía trabajar desde casa. ¿Ha supuesto esta nueva realidad un cambio o se sigue yendo al modelo presencial por obligación? Para Beatriz Escobar, "la pandemia marcó un antes y un después. Antes de ella se hablaba de temas de flexibilidad del trabajo, conciliación, pero que eran como muy puntuales. Y yo creo que a partir de ahí se demostró de una forma muy nítida que era totalmente viable ser eficiente y trabajar en casa. Y esto permite conciliar la vida de hombres y de mujeres, algo que debe ser fundamental para todos, hombres y mujeres. Yo creo que después de la pandemia, lo que ha habido que hacer es un ejercicio para racionalizarlo, porque ni vale en todos los negocios, ni sirve para todos los roles... Pero creo que sí que ha habido una brecha que bien racionalizada nos está permitiendo mejorar muchos aspectos". María Rosa Ribó apuntó que "el modelo de teletrabajo ha venido para quedarse. Además, en lo que son posiciones técnicas y para incorporar talento, a nosotros, especialmente, nos va a ir muy bien, porque hay muchos profesionales jóvenes que demandan justamente este modelo de trabajo, con lo cual esto nos favorece. Evidentemente, favorece la confianza entre empleados y directivos y la eficiencia. Y el hecho de poder trabajar desde casa tiene un beneficio para el trabajador muy importante. Y creo que, en este sentido, en las profesiones técnicas tenemos unas ventajas que otras no se pueden permitir".

Para Beatriz Marco, en realidad, la conciliación es una cuestión de equi-
pos: "A mí, la maternidad, me suponía un freno mental. No sé si os ha pasado a otras mujeres que pensaba que por tener niños no iba a progresar laboralmente. Eso es así, porque había muchas personas que te decían: "bueno, si tienes niños, organízate bien la vida". Pero nadie hablaba de mi marido. La realidad es que aquí no hay frenos, puedo tener niños, pero lo importante es organizarte y organizarte tanto tu pareja como tú. El teletrabajo ayuda mucho a organizarte en ciertos aspectos, porque si vives en una ciudad grande, si teletrabajas, te evitas desplazamientos que te pueden ayudar a hacer otro tipo de cosas".

Mónica González resumió: "Equipo en casa, medidas de conciliación y flexibilidad laboral en el trabajo. Yo a veces me he ido a las cuatro porque salía la niña a las cuatro y media, no tenía quién me la recogiera y he podido continuar trabajando más tarde. Y un mito importante que hay que quitarse es que a más horas de trabajo, mayor productividad o mejor valoración".

LA PLATAFORMA DE MARKETING AUTOMATION



Soluciones de seguridad de red

En la infraestructura de cualquier red informática, ya sea de tamaño pequeño, mediano o grande, existe un dispositivo que cobra un protagonismo especial. Se conoce con el nombre de equipo de seguridad de red y como su nombre indica su principal finalidad es proteger la red de esa organización, También la de los dispositivos conectados a ella. Esto explica que incorpore un amplio conjunto de características y tecnologías para afrontar cualquier amenaza o ataque. Ofrece, asimismo, otras funcionalidades de interés con el objetivo de preservar también la integridad y disponibilidad de los datos de las empresas como las actividades de monitoreo y detección de cualquier comportamiento que se considere anómalo, o el establecimiento de políticas de control de acceso.

En esta comparativa hemos reunido siete firewalls. El primero es Barracuda SecureEdge, un firewall de nueva generación que se presenta como una solución SASE de un solo proveedor que integra y automatiza sus componentes de manera inteligente. Le sigue Cisco Secure Firewall 3100: potencia el trabajo híbrido y emplea tecnologías de aprendizaje automático para identificar pasivamente las posibles amenazas en el tráfico encriptado sin descifrarlo para detectar más malware.

También contamos con la participación de HPE Aruba Networking CX 10000, que destaca por su combinación de switch y firewall. Por su parte, SonicWall Serie NSa 2700 brinda prestaciones como control de aplicaciones, seguridad DNS, servicios botnet, prevención de intrusiones... Finalmente se encuentr Sophos Firewall que está impulsado por el motor de inspección de paquetes de Xstream para un análisis del tráfico para IPS, AV, protección web y control de aplicaciones en un único motor de transmisión. Nuestra recomendación pasa por los modelos de HPE Aruba, Sophos y Barracuda.





Barracuda SecureEdge

La seguridad web basada en la nube y el acceso a la red Zero Trust son algunos de los componentes integrales de este firewall de nueva generación.



Se creó desde el principio como una plataforma de seguridad para gestionarse y entregarse en la nube. También para que estuviera disponible en forma de servicios periféricos gestionados automáticamente para cualquier tipo de dispositivo, implementación o plataforma. Dentro de este marco, Barracuda SecureEdge se presenta como una solución SASE (Secure Access Service Edge) de un solo proveedor que integra y automatiza sus componentes de manera inteligente. Sus servicios principales están disponibles como SaaS, aunque también para Azure Virtual WAN e in-

cluso como instancias privadas.

¿QUÉ SUPONE SASE?

La conectividad se crea, a este respecto, mediante la implementación sin intervención de un dispositivo desplegado localmente con una optimización automática de SD-WAN para el servicio. Mientras, los trabajadores remotos que se encuentran en cualquier sistema operativo se autoinscriben con el agente de SecureEdge Access que está disponible en cualquier tienda de aplicaciones (incluso para Linux) y que incluye hasta cinco dispositivos por usuario para ZTNA y acceso seguro

a Internet. Todo esto se gestiona y aplica de forma centralizada a través del administrador de SecureEdge basado en la nube. La optimización integrada del tráfico de Internet desde el servicio hasta el agente de SASE facilita, mientras tanto, que los terminales aprovechen una mayor parte del ancho de banda disponible en las líneas de Internet compartidas para mejorar el rendimiento de las aplicaciones. La tecnología subyacente que se usa para solucionar la pérdida de paquetes se basa en códigos de red lineales aleatorios (RLNC, por sus siglas en inglés), un avanzado esquema de codificación. Los algoritmos basados en los códigos RLNC reaccionan, en este caso, mucho más rápido ante las pérdidas y las corrigen más deprisa sobre la marcha, lo que requiere menos retransmisiones de paquetes y reduce la sobrecarga de los dispositivos.

La plataforma SASE de SecureEdge le permite crear miles de aplicaciones predefinidas, así como otras privadas que se pueden alojar en cualquier lugar. Constituye un procedimiento rápido, sencillo y que solo hay que seguir una vez para, a continuación, compartirlo con las definiciones de políticas de seguridad de SD-WAN y ZTNA. Todas las optimizaciones de redes y enrutamiento necesarias se llevan a cabo de forma completamente transparente en segundo plano y



se aplican de forma automática a cada sitio web, usuario o instancia de servicio.

La incorporación de oficinas (y otros elementos que se necesiten) a la plataforma SASE de Barracuda SecureEdge destaca por su sencillez. Con tan solo un par de clics, los usuarios completan la configuración en el administrador basado en la nube y los dispositivos a desplegar localmente se enviarán directamente a la ubicación remota. La implementación sin intervención conecta de modo automático los dispositivos desplegados localmente y los dispositivos de IoT al punto de entrada de SecureEdge más cercano.

VENTAJAS PRINCIPALES

Con acceso seguro a las aplicaciones, una seguridad basada en la nube para los terminales y conectividad SD-WAN automatizada para instalaciones de cualquier tipo o tamaño, Barracuda SecureEdge

emplea una inteligencia de seguridad derivada de la IA que va más allá de la implementación habitual de oficinas o servicios en la nube, proporcionando de esta manera seguridad a cualquier usuario con independencia del dispositivo que utilice y el servicio al que acceda. Cuenta, asimismo, con Zero Trust y filtrado de URL, mientras que los dispositivos se implementan sin necesidad de intervención conectándose automáticamente a los servicios en la nube. Asimismo, optimizan el tráfico de enlaces ascendentes en la nube a través de la reducción de la pérdida de paquetes y otras funciones avanzadas de optimización de SD-WAN para que las organizaciones prescindan del gasto que suponen las líneas alquiladas.

Las compañías que adquieran Barracuda SecureEdge disfrutarán, en otro orden de cosas, de un acceso directo y seguro a todas las aplicaciones autorizadas con una

evaluación continua de la seguridad y su idoneidad, indistintamente de dónde estén alojadas y del dispositivo que empleen los trabajadores. Las empresas tienen, por otro lado, la posibilidad de optimizar el tráfico de red de última milla para aprovechar al máximo los enlaces de Internet compartidos. También destaca que los dispositivos del sitio web de SecureEdge protegen el perímetro de la oficina y cualquier dispositivo que se encuentre en esta contra el malware, el spyware y otros contenidos no deseados de Internet; todo ello se ejecuta en el dispositivo o en los servicios de SecureEdge.

Las organizaciones tienen a su disposición hasta siete configuraciones entre las que elegir (T100B, T200C, T400C, T600D, T900B, T93A y T193a) en función de sus necesidades: opción de implementación, rendimiento del sitio, número de usuarios recomendados, sesiones concurrentes, nuevas sesiones por segundo... El hecho de poder integrar varios componentes a la perfección en cada uno de ellos permite a las compañías recopilar las soluciones de distintos proveedores en una sola; beneficiarse de una mejor cobertura de seguridad; un acceso más rápido a las aplicaciones; una mejor conectividad del sitio; y una mayor agilidad en sus funciones de TI.

Barracuda

Tel: +44 118 338 4600

Web:

www.barracuda.com

Precio: A consultar

HPE Aruba Networking CX 10000

Proporciona 800 G de firewall stateful distribuido para el tráfico este-oeste, segmentación zero trust y telemetría intensiva.



La serie de switches HPE Aruba Networking CX 10000 ofrece un enfoque flexible e innovador para abordar las demandas de rendimiento de seguridad, agilidad y escalabilidad tanto de los centros de datos empresariales tradicionales como de los emergentes y distribuidos. Provista de una DPU AMD Pensando totalmente programable, responde a las órdenes de HPE Aruba Networking CX, un sistema operativo moderno que se sostiene en bases de datos que automatizan muchas tareas de red críticas y complejas; por sus características, permite asimismo que clientes y desarrolladores utilicen scripts de software para la resolución de problemas históricos y análisis de tendencias pasadas, lo que ayuda a predecir y evitar problemas futuros. Debido a que el sistema operativo HPE Aruba Networking CX está construido sobre una arquitectura modular Linux con una base de datos con estado, este proporcio-

na varias características que son de interés para las organizaciones: fácil acceso a toda la información del estado de la red para su visibilidad y análisis, secuencias de comandos Python para una programabilidad detallada de las tareas de red, una arquitectura de microservicios que permite la integración total con otros sistemas y flujos de trabajo... Todo ello se va a traducir en una serie de beneficios para las empresas que disponen de un firewall con estado, protección DDos, segmentación segura, servicios de telemetría y políticas Zero Trust, entre otros.

Las compañías optimizan, asimismo, los flujos de tráfico de red, el ancho de banda y el rendimiento, lo que reduce la complejidad asociada con la unión de servicios. Destaca también que simplifican las operaciones que llevan a cabo a través de la red unificada, la automatización y gestión de la seguridad con HPE Aruba

Networking Fabric Composer. Se trata de un software de conmutación que reduce las operaciones al proporcionar capacidades de automatización, analítica distribuida, seguridad y alta disponibilidad a redes de campus, sucursales y centros de datos. Igualmente, al brindar una gestión unificada de red y seguridad para la plataforma de conmutación, esto proporciona configuraciones automáticas de conmutadores y redes, al mismo tiempo que unifica la política de seguridad y los firewalls distribuidos en todo el tejido de conmutación. Dicha gestión unificada de política de seguridad y redes simplifica tanto las operaciones como la resolución de problemas. Hay que tener en cuenta, en otro orden de cosas, que la capacidad del sistema operativo HPE Aruba Networking CX para mantener un estado sincrónico en planes de control duales fa-



cilita una solución única de alta disponibilidad llamada HPE Aruba Networking Virtual Switching Extension: conocida por sus siglas VSX, se entrega a través de la redundancia obtenida mediante la implementación de dos chasis con un enlace entre conmutadores donde cada chasis mantiene su control independiente.

RESOLUCIÓN DE PROBLEMAS

En la propuesta de la firma norteamericana, la arquitectura de servicios distribuidos de los conmutadores es independiente de la arquitectura de implementación de la red. Esto proporciona flexibilidad para habilitar la entrega de los servicios cuando se implementan como acceso, parte superior del bastidor (ToR) o extremo de la fila (EoR) en un centro de datos; los switches ofrecen 3,6 Tbps de capacidad de conmutación de velocidad de línea con configuraciones de interfaz que admiten 10/25 GbE (SFP/SFP+/SFP28) y seis puertos 40/100 GbE (QSFP+/QSFP28). HPE Aruba Networking CX 10000 ha sido dotado, por otra parte,

con HPE Aruba Networking Analytics Engine. Así, para mejorar la visibilidad y la resolución de problemas, este motor de análisis de red (que brinda información en tiempo real sobre toda la red para acelerar la resolución de problemas y las tareas de planificación) 'interroga' y analiza automáticamente los eventos que pueden afectar al estado de la red. Mientras, la telemetría (antes citada) y la automatización avanzada permiten a las organizaciones identificar y solucionar problemas que están relacionados con las redes, la seguridad, los sistemas o las aplicaciones empleando no solo agentes de Python sino API REST. Por su parte, la base de datos de series temporales (TSDB) almacena datos operativos y de configuración para ayudar a resolver también problemas de red. Los datos se pueden emplear para analizar tendencias, identificar anomalías y predecir requisitos de capacidad futuros.

TAMBIÉN DE INTERÉS

Más allá de los enfoques tradicionales de implementación Zero

Touch que requieren de un importante trabajo inicial, los asistentes guiados y fáciles de usar de AFC ofrecen flujos de trabajo llave en mano que guían a los clientes a través del proceso de implementación de la estructura, simplificando las operaciones. AFC es independiente de la topología y puede admitir igualmente la estructura VXLAN EVPN basada en estándares, así como las implementaciones VSX tradicionales sin problemas. Como cualquier complejidad de la implementación de la estructura permanece oculta, esto garantiza que los operadores de red no necesitan comprender ni los protocolos ni los comandos del sistema operativo para poner en práctica arquitecturas de mejores prácticas.

HPE

Tel: 900 990 011

Web:

www.hpe.es

Precio: A consultar

Sophos Firewall



Su motor de inspección de paquetes de Xstream ofrece análisis del tráfico para IPS, AV, protección web y control de aplicaciones en un único motor de transmisión.



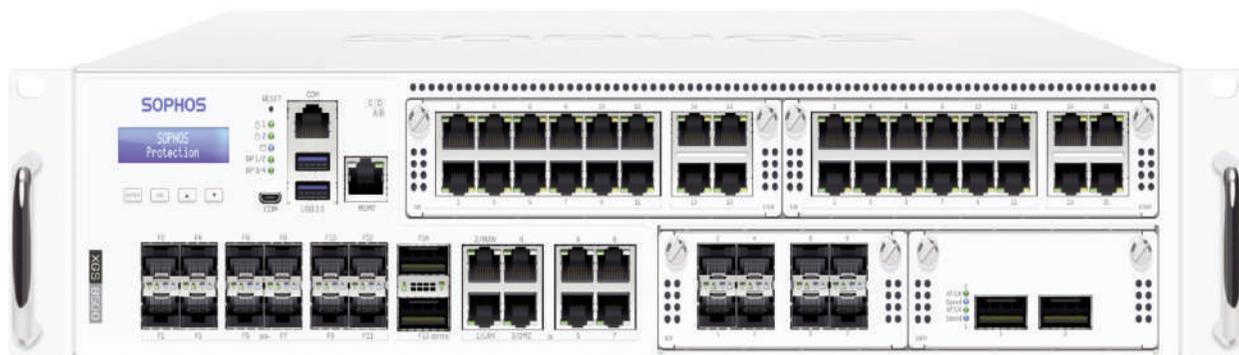
La propuesta de Sophos se caracteriza por integrar una arquitectura de Xstream diseñada para ofrecer unos altos niveles de visibilidad, protección y rendimiento para afrontar algunos de los mayores desafíos con los que se encuentran los administradores de redes hoy día. Dentro de este contexto, Sophos Firewall destaca por incorporar un motor de inspección TLS 1.3, los últimos paquetes de cifrado para una compatibilidad máxima y una visibilidad mejorada de los flujos de tráfico cifrado directamente desde su panel de control.

A estas características hay que añadir que Sophos Firewall incluye un motor de inspección detallada de paquetes (DPI) de alta velocidad para que escanee el tráfico en busca de amenazas sin un proxy que ralentice el proceso: dado que la pila del firewall descarga por completo el procesamiento al motor DPI reduce notablemente la latencia y mejora la eficiencia general. La solución de la multinacional británica también bloquea el ransomware y las filtraciones más recientes con la DPI de transmisión de alto rendimiento que incluye IPS next-gen, protección

web y control de aplicaciones, además de Deep Learning y espacios seguros con la tecnología de SophosLabs Intelix. Esta facilita la clasificación de las amenazas y el análisis exhaustivo de objetos limpios y maliciosos conocidos como archivos, páginas web y direcciones IP. Las organizaciones reciben, asimismo, análisis detallados justo a tiempo para objetos sospechosos de contener amenazas; como este servicio se presta desde la nube de SophosLabs, la protección facilitada no afecta al rendimiento.

APLICACIONES Y SD-WAN

Una parte significativa del tráfico de red es tráfico de aplicaciones empresariales de confianza destinado a sucursales, usuarios remotos o servidores de aplicaciones en la nube. Como tal, no se requiere escaneado de seguridad adicional para buscar amenazas o malware, y el tráfico puede dirigirse de forma inteligente a la ruta rápida FastPath. ¿El resultado? La latencia se reduce, el rendimiento general se optimiza y se libera capacidad para el tráfico que sí necesita una inspección detallada de paquetes. Sophos Firewall acelera el tráfico de SaaS, SD-WAN y en la nube como VoIP, vídeo y otras aplicaciones de confianza automáticamente o a través de las políticas que tenga cada compañía, ubicándolas en la ruta rápida.



da FastPath a través del procesador de flujo Xstream.

Por su parte, administrar el enrutamiento del tráfico de aplicaciones a través de múltiples enlaces WAN e interconectar una red distribuida son elementos esenciales de cualquier solución SD-WAN y tareas mucho más complejas de lo que debieran. Así, de la mano de Sophos Firewall con SD-WAN de Xstream, se está brindando una solución SD-WAN potente e integrada con selección de enlaces y enrutamiento basados en el rendimiento; equilibrio de carga; transiciones de cero impacto entre enlaces en caso de interrupción; orquestación centralizada administrada en la nube; y aceleración en FastPath de Xstream del tráfico de túnel VPN.

OTROS ASPECTOS

Para garantizar la protección y el rendimiento más avanzados, el producto de Sophos emplea procesadores de flujo Xstream programables que descargan flujos de tráfico importantes y aceleran la

inspección de tráfico cifrado, así como el enrutamiento de VPN y aplicaciones. De igual forma identifica y detiene automáticamente las amenazas activas, y aísla (de manera automática también) los hosts comprometidos evitando el movimiento lateral y las comunicaciones externas hasta que sea posible investigar y limpiar la amenaza. Sophos Firewall se integra con Sophos Endpoint, Sophos XDR y Sophos MDR para responder a cualquier amenaza o ataque identificado en el cortafuegos, el endpoint o por un analista de seguridad.

Todo ello gestionado a través de una única consola. Con Sophos Central, el gestor de seguridad obtiene una única plataforma de gestión en la nube para todos los productos de Sophos incluidas herramientas avanzadas para la gestión de firewalls de grupo (es posible visualizar su uso y estado) sin costes adicionales, orquestación de redes superpuestas SD-WAN, ZTNA, gestión para conmutadores y puntos de acceso inalámbricos,

paneles e informes completos en profundidad... De igual forma, es posible consultar el estado de todos los demás productos de Sophos si la organización dispone de alguno, y las infracciones de políticas, aplicaciones y actividades de riesgo. Como plataforma de administración de seguridad en la nube, Sophos Central mantiene, por otra parte, los datos de registro de los firewalls de las empresas en la cloud con herramientas que facilitan la generación de informes; gracias a ellos, las compañías analizan y visualizan su red a lo largo del tiempo. Incluso auditan y monitorizan los cambios en esta red en tiempo real.

Sophos

Tel: 91 375 67 56

Web:

www.sophos.com/es-es

Precio: consultar

SonicWall Serie NSa 2700

Control de aplicaciones, seguridad DNS, servicios botnet, prevención de intrusiones, VPN y Geo-IP son algunas de las prestaciones que proporciona este dispositivo.

El firewall seleccionado por la empresa estadounidense de seguridad forma parte de su serie Gen 7 NSa e incluye prestaciones de seguridad completas como prevención de intrusiones, VPN, control de aplicaciones, análisis de malware, filtrado URL, seguridad DNS, Geo-IP y servicios botnet, protegiendo así el perímetro contra amenazas avanzadas sin formar cuellos de botella. Además, la citada serie ha sido creada desde cero con los últimos componentes de hardware, todos ellos diseñados para proporcionar un rendimiento multi-gigabit de prevención de amenazas, incluso para el tráfico cifrado. Con una alta densidad de puertos, incluidos múltiples puertos 40 GbE y 10 GbE, la solución soporta la redundancia de red y de hardware con alta disponibilidad y dos fuentes de alimentación.

La serie Gen 7 NSa utiliza, por otro lado, SonicOS 7.0, un sistema operativo creado también desde cero con el objetivo de ofrecer una interfaz de usuario moderna, flujos de trabajo intuitivos y un diseño centrado en el usuario. A este respecto, SonicOS 7 brinda una configuración de políticas sencilla, implementación sin necesidad de intervención y una gestión flexible, todo lo cual permite a las empresas mejorar tanto su seguridad como la eficiencia de sus operaciones.



Este mismo sistema operativo reúne una serie de características de interés. A nivel de hardware proporciona, por ejemplo, inspección dinámica de paquetes, protección contra ataques DDoS, autenticación biométrica para el acceso remoto, dentro de notificaciones, resumen de tráfico y usuarios principales, información sobre las amenazas... Destacan, asimismo, sus capacidades de descifrado e inspección TLS/SSL/SSH, prevención de intrusiones, identificación de aplicaciones, VPN, y tareas de gestión, monitorización, soporte, depuración y diagnósticos.

El modelo Serie NSa 2700 integra las siguientes interfaces: una consola, puerto de gestión, 3x10G SFP+, 2 USB 3.0 y 16x1 GbE. Con una capacidad de almacenamiento de 64 GB M.2 y ranura de expansión de hasta 256 GB, soporta un total de 512 puntos de acceso. Sus opciones de cifrado y autenticación inclu-

yen DES, 3DES, AES (128, 192, 256 bits)/MD5, SHA-1 y criptografía Suite B.

Que pueda gestionarse de forma centralizada, al igual que el resto de dispositivos de esta familia (versión NSa 3700 NSa 4700 NSa 5700 y NSa 6700), la hace idónea tanto para las empresas medianas como distribuidas que acceden de forma segura a los recursos de Internet que se encuentran en la sede corporativa o en una nube pública, mejorando considerablemente la latencia de las aplicaciones.

SonicWall

Tel: 91 210 46 00

Web:

www.sonicwall.com

Precio: 5.250 euros

Cisco Secure Firewall 3100

Potencia el trabajo híbrido y usa tecnologías de aprendizaje automático para identificar pasivamente las posibles amenazas en el tráfico encriptado.

Cisco Secure Firewall 3100 es una familia de dispositivos de seguridad frente a amenazas que proporcionan resiliencia empresarial con una defensa superior y que se ajusta a las cambiantes necesidades de las medianas empresas. En concreto, estas capacidades de rendimiento están habilitadas por una arquitectura de CPU moderna junto con un hardware diseñado específicamente para optimizar las funciones de firewall, las de tipo criptográficas y de inspección de amenazas.

Además, los firewalls de la serie 3100 utilizan tecnologías de aprendizaje automático para identificar pasivamente aplicaciones de usuario y amenazas potenciales en el tráfico cifrado con el objetivo de detectar una mayor cantidad de malware. Consta de cinco modelos que ofrecen una amplia gama de niveles de rendimiento para abordar diversos casos de uso, desde el edge computing hasta el centro de datos y la nube privada. A su vez, cada uno de estos equipos puede ejecutar software ASA o Firewall Threat Defense (FTD), y la plataforma implementar tanto en modo firewall como en modo IPS dedicado. Para conjuntos en línea e interfaces pasivas, la serie 3100 admite Q-in-Q (VLAN apilada) con hasta dos encabezados 802.1Q en un paquete.

Estos dispositivos brindan diversas mejoras significativas en cuanto a rendimiento y eficiencia



para las organizaciones, y sus ventajas se concentran en cuatro aspectos principales. El primero está relacionado con el trabajo híbrido: los firewalls de Cisco están diseñados para admitir más trabajadores híbridos, así estén donde estén pueden disfrutar de un rendimiento de VPN hasta 17 veces más rápido. El segundo beneficio tiene que ver con la protección de la inversión. Y es que estos dispositivos de seguridad ayudan a garantizar un sólido retorno de la inversión a las organizaciones por su flexibilidad de alta densidad de puertos y sus clusters que permiten escalar la infraestructura.

La tercera ventaja es que proporcionan un conocimiento avanzado al emplear tecnologías de aprendizaje automático para identificar aplicaciones de usuarios y posibles amenazas en el tráfico cifrado para detectar mayor cantidad de malware. Finalmente, se encuentra la satisfacción de los em-

pleados. Según explica Cisco, los firewalls de la serie 3100 ofrecen una capacidad de procesamiento de inspección hasta siete veces superior y calidad de servicio basado en aplicación, permitiendo a los usuarios experimentar videoconferencias sólidas y seguras. Para unificar la administración de cada uno de estos firewalls se encuentra Firewall Management de Cisco, una solución que combina el control de aplicaciones, la prevención de intrusiones, el filtrado de URL y la defensa contra el malware.

Cisco

Tel: 91 201 20 00

Web:

www.cisco.es

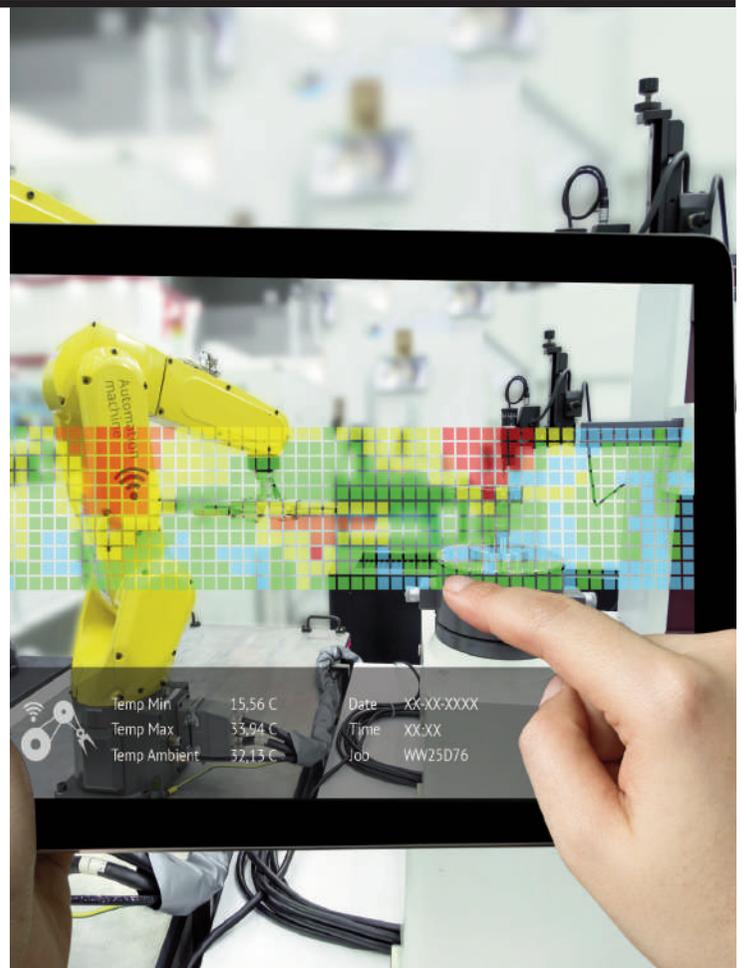
Precio: consultar

¿Cuál es el estado de la automatización?



Las herramientas y soluciones de automatización están copando cada vez un mayor tipo de protagonismo entre las empresas españolas. Abordamos en este número esta temática en crecimiento.

Por Vanesa García



La adopción de tecnologías de automatización en las empresas españolas presenta una disparidad notable entre las grandes corporaciones, que se equiparan en madurez a las de países avanzados, y las pequeñas o medianas empresas, que, aunque rezagadas, están dando sus primeros pasos en la automatización con casos de uso limitados.

En cuanto a los sectores, las tecnologías de automatización y RPA tienen aplicabilidad en empresas de todos los tipos, siempre que existan operaciones o procesos repetitivos que se realicen manualmente. Desde la industria hasta la banca, seguros, retail y logística... existe una amplia gama de sectores en los que numerosos procesos u operaciones son idóneos para la automatización. Aunque cabe destacar que España, en comparación con otros países de Europa y especialmente con Estados Unidos, es un mercado difícil y complejo, pues como explica Toni Parada, Head of Digital Solutions de aggity, “existe más resistencia para invertir con el objetivo de un ahorro futuro, en el caso de la automatización, las empresas entienden rápidamente el potencial de la automatización y, una vez, que empiezan a obtener resultados en

TEMA DE PORTADA

determinados procesos, son proclives a extender su uso dentro de la organización”.

Siguiendo este punto, el mercado está avanzando hacia una automatización basada en casos de negocio en los que es posible definir un modelo claro de ahorros y costes, “hecho que permite industrializar los programas de automatización. Adicionalmente podemos ver que la automatización de procesos sigue ayudando a que las compañías puedan hacer crecer sus negocios sin necesidad de que sus costes estructurales se incrementen exponencialmente. Esto hace que estemos convencidos que la automatización ha venido para quedarse muchos más años”, recalca Marc Román Martínez, Head of Hyperautomation Iberia, Business Process Automation de DXC Technology.

Pero no solo el sobrecoste puede disminuir las expectativas de las empresas a la hora de introducir esta automatización, factores como no entender en que consisten estas herramientas puede llevar a las compañías a decepcionarse con la RPA, “las herramientas de RPA automatizan tareas recurrentes y basadas en reglas, pero no procesos integrales. Las empresas que entienden esto se entusiasman con las soluciones de automatización, pero las empresas que esperan una automatización de procesos realmente completa de una solución RPA a menudo se sienten decepcionadas”, explica Rudy Kuhn, Lead Transformation Evangelist de Celonis. Para entender esto, desde Celonis definen este proceso como Purchase-to-Pay: todas las actividades desde la solicitud de compra inicial hasta el pedido, la recepción de mercancías y la factura hasta el pago. “Sin embargo, los proveedores de RPA suelen definir un proceso como el acto de copiar datos de una hoja de cálculo en un formulario de un sistema ERP. Se trata de una tarea potencialmente importante, pero no deja de ser una única actividad. Si alguien tiene que copiar datos repetidamente de una aplicación a otra, automatizar esta tarea tiene sentido y aporta valor. Pero llamarlo automatización de procesos es inexacto y contribuye a la desconexión entre las expectativas de la empresa y las promesas del proveedor”, añade Kuhn.

VENTAJAS DE LA AUTOMATIZACIÓN

La automatización de procesos ha emergido como una herramienta destacada para potenciar la eficiencia y la rentabilidad en los negocios. Su popularidad se atribuye en gran medida a las ventajas que brinda a las empresas, especialmente en términos de mejoras en la eficiencia. Al automatizar procesos, se logra ejecutar tareas de manera más ágil y precisa, lo que resulta en una mayor eficiencia operativa y una utilización más efecti-





va de los recursos disponibles.

En palabras de Ramón Riquelme, Solutions Consulting en Appian, las soluciones de automatización ofrecen flexibilidad para adaptarse a cambios en la demanda, "lo que permite a las empresas ser ágiles y responder rápidamente al mercado sin comprometer los estándares de calidad y normativos. Además, reducen costos y facilitan el análisis avanzado de datos al recopilar y procesar grandes volúmenes de información, proporcionando insights tanto para investigaciones detalladas como para decisiones estratégicas y optimización de procesos".

Otro punto a favor de la automatización es la reducción del margen de error, como comenta José Aznar, Business Solutions Manager de Kyocera, "sin duda alguna la mayor ventaja es la mejora de la eficiencia, pues los procesos automatizados son generalmente más rápidos y precisos y reducen el margen de error aumentando la eficiencia general. Estas ventajas pueden contribuir significativamente al crecimiento y la competitividad de una empresa en el mercado actual".

Coincidiendo con sus compañeros, Cecilia Olaso, Responsable de Marketing de Yooz, recalca que las soluciones de automatización ofrecen ventajas como, "la mejora de la eficiencia, la reducción de costes, la mejora de la calidad, el aumento de la productividad, la agilidad empresarial y una mejor experiencia del cliente".

IDENTIFICAR LOS PROCESOS

La identificación de los procesos que pueden automatizarse y que aportarán más valor a la empresa en línea con sus objetivos es una fase clave, que determinará el éxito en el uso de esta tecnología. Hay empresas que tienen un conocimiento más profundo de la tecnología y tienen claro qué, cómo y con qué objetivos automatizar. Pero, son una minoría y la mayoría no tienen claro de partida por dónde empezar o cómo hacerlo.

Justamente con ese objetivo, desde aggyt realizan con las empresas una serie de sesiones en la que aplican su metodología "The Lab", "en la que explicamos los conceptos (RPA, IA, Machine Learning...) y sus principales aplicaciones, compartimos ejemplos de caso de uso en su sector/ departamento, y posteriormente realizamos un trabajo de brainstorming y puesta en común para identificar todas las iniciativas potenciales, las aterrizamos y las priorizamos en un workshop con el equipo directivo", dice Parada.

Mientras que desde DXC, creen que para identificar qué procesos se pueden o no automatizar, primero hay que saber diferenciar entre proceso y tarea, "es crucial identificar la madurez de los procesos organizacionales para definir la mejor estrategia de Discovery. Una vez establecidos estos puntos, se pueden identificar con mayor

precisión los procesos candidatos, utilizando tecnología como Process Mining para mejorar la calidad de los datos y obtener una visión objetiva de los mismos. Sin embargo, estos procesos suelen ser identificados de forma incorrecta o parcial, principalmente debido a la baja madurez de los procesos en muchas compañías, que se centran en la automatización sin considerar la reingeniería y la mejora organizativa de los equipos", explica Martínez.

Para Celonis la minería de procesos es base en esta identificación, "con ella, si se descubren problemas, no deben automatizarse como acto reflejo, porque la mejor solución a un problema no es la automatización, sino la eliminación del problema. Ahora bien, no todos los problemas, como los retrasos, pueden resolverse eliminando la tarea asociada. Y si se puede simplificar, quizá también se pueda estandarizar, de modo que la nueva tarea se ejecute siempre mejor que la original. Y sólo entonces deberíamos pensar en la automatización. Este enfoque se describe con el acrónimo ESSA: Eliminar, Simplificar, Estandarizar y Automatizar". Otra forma, añade Kuhn, es simplemente preguntar a los empleados qué tareas les hacen sentirse como robots, "porque hacen lo mismo una y otra vez. De este modo, obtendremos una serie de buenas sugerencias para la automatización".

Por su parte, en Appian abogan por contar con un buen equipo multidisciplinar técnico y de negocio, "contar con un entorno que facilite esa comunicación, por medio de herramientas de alto rendimiento y capaces de abordar situaciones de alta complejidad, pero que al mismo tiempo permita una lectura comprensible y una modificación sencilla, hace mucho más sencilla esta comunicación. El enfoque Low-Code de Appian proporciona una amplia gama de herramientas gráficas que simplifica el buen entendimiento entre ambas partes de la ecuación", aclara Riquelme.

A pesar de tener todo esto en cuenta, algunas empresas incurren en errores como creer que pueden prescindir totalmente del trabajo humano, personalizar en exceso los procesos o establecer cronogramas demasiado estrictos... "Estos errores pueden llevar a una acumulación de tareas vencidas y a la pérdida de la visión global del flujo de trabajo diario. Para evitarlos, es crucial realizar un análisis detallado de los procesos y mantener un equilibrio entre la automatización y la intervención humana", alertan desde Kyocera.

Y es que, como resume el portavoz de Yooz, "la falta de planificación, la falta de capacitación del personal, sobrestimar la tecnología, descuidar la experiencia del usuario, no medir los resultados y descuidar la seguridad y la privacidad, pueden ser los errores más comunes

a la hora de automatizar procesos en una empresa.

RESISTENCIA AL CAMBIO Y ESCALABILIDAD

Hace ya algunos años, cuando surgieron los primeros proyectos de automatización, se identificaba una resistencia al cambio significativa la que dificultaba el avance de estos proyectos. Actualmente y dada la madurez de estos programas de automatización, para Marc Román Martínez, dicha resistencia ya no es tan patente. A lo que añade que, “si que es imprescindible disponer de una gestión del cambio y plan de comunicación adecuados para conseguir que las diferentes áreas de la organización se sientan y estén involucradas en estos programas de automatización”.

Siguiendo este punto, Toni Parada apunta que esta resistencia al cambio depende mucho del tamaño, la tipología y la cultura de la organización. A pesar de ello, “no es la principal barrera. Por supuesto, y como sucede en cualquier proyecto de digitalización que supone una transformación de la forma que hacer las cosas, hay que tener muy en cuenta a sus empleados. Es fundamental, por tanto, analizar la compañía en su totalidad en lugar de focalizarse en un punto/área concreta y también sa-



TEMA DE PORTADA



ber que existen distintas modalidades para la adopción de estas tecnologías, alineadas con las necesidades, objetivos y requerimientos de cada compañía”.

A diferencia de sus compañeros, Ramón Riquelme opina que este sí que es un factor que incide de cara a los problemas de automatizar procesos, "muchos empleados pueden sentirse amenazados por la idea de que la automatización reemplace sus tareas o cambie la forma en que realizan su trabajo habitual. Para abordar este desafío y desarrollar un proceso de cambio cultural fluido y sin miedos entre los empleados, desde Appian recomendamos mantener una comunicación clara y transparente ya que esto ayuda a generar confianza y reducir la incertidumbre. Ofrecer capacitación adecuada sobre las nuevas tecnologías y procesos es esencial para ayudar a los empleados a adquirir las habilidades necesarias y sentirse cómodos con los cambios”, explica.

En relación con lo anterior, el estudio “Tecnologías habilitadoras del Smart Working” realizado por IDC en colaboración con Kyocera destaca que los principales desafíos identificados con el proceso de digitalización son las barreras culturales, las tecnológicas y las económicas. Sobre ésta última, supone uno de los principales problemas al cambio; la automatización lleva asociada inversiones y precisa de ciertas certidumbres. Esto hace que sea imprescindible crear una hoja de ruta que per-



mita optimizar las inversiones en las tecnologías necesarias para cada una de las fases de implementación.

“Sobre la correcta gestión para el proceso del cambio pasa por poner a las personas en el centro y, en este caso, en los empleados. Deben estar en el núcleo del modelo, con un enfoque horizontal y colaborativo en el que se sientan empoderados, con capacidad de tomar decisiones y aportar valor de negocio. La formación y competencias digitales son fundamentales para convertir a los empleados en parte del proceso y pilar de la evolución de la cultura corporativa”, señala José Aznar.

Por otro lado encontramos la escalabilidad, que se puede garantizar implementando ciertas estrategias como el desarrollo de soluciones de automatización que sean modulares y puedan adaptarse fácilmente a diferentes necesidades y volúmenes de trabajo, o asegurarse de que las herramientas de automatización puedan integrarse fácilmente con los sistemas y aplicaciones existentes en la empresa, incluidos los sistemas ERP, CRM y de gestión de la cadena de suministro. Que en palabras del Solutions Consulting de Appian “facilita la interoperabilidad y la transferencia de datos entre diferentes plataformas. Además, utilizar servicios en la nube que proporcionen recursos informáticos escalables según la demanda, o implementar herramientas de monitoreo y análisis que permitan supervisar el rendimiento de las soluciones de automatización para realizar los ajustes necesarios son también estrategias que cualquier empresa debería seguir”.

TENDENCIAS EMERGENTES

Los objetivos fundamentales que tienen las empresas cuando abordan un proyecto de transformación digital y, específicamente de automatización, son dos: la mejora de la eficiencia y la mejora de la experiencia de los clientes/proveedores/partners o UX (User Experience). Con ese doble objetivo, la tendencia pasa por la combinación del dato, la tecnología RPA y la IA para complementar herramientas clave de la era digital entre las que destacaría cuatro.

Primero, y en opinión del Head of Digital Solutions de aggyt, “RPA para automatizar y hacer más eficientes los flujos de trabajo; segundo, los Asistentes Cognitivos con nuevas formas de comunicación, más abiertas, cercanas y fáciles de usar (voz, mail, WhatsApp, mail) pilotados por una IA que tiene al RPA como aliado; tercero, como apoyo a People Analytics, donde con el objetivo prioritario de atraer, motivar y fidelizar talento, el RPA permite a los departamentos de RRHH y a los gestores de talento liberarse de trabajos “rutinario” para dedicarse a labores de mayor valor.... Y, cuarto, la evolución tecnológica y la

migración a cloud. Donde ante las dificultades que tienen las empresas para manejar diferentes tipologías de sistemas, aplicaciones y soluciones tecnológicas, resultan fundamentales soluciones de RPA para integrar datos, interconectar sistemas y monitorizar y automatizar procesos de back office o labores de TI”.

Por otro lado, el Business Solutions Manager de Kyocera añade que la fuerza de trabajo conectada aumentada y la automatización basada en entornos cloud están emergiendo como tendencias clave, “el modelo cloud permite adicionalmente la automatización inteligente de procesos y habilita al empleado a incrementar su productividad, pudiéndose utilizar en todas las áreas de la empresa. Esto aporta una ventaja competitiva crucial para las pymes, lo que redundará en una mejor diferenciación y percepción de sus productos y servicios entre su cliente final”.

Otra tendencia destacada es la orquestación de procesos, para el Lead Transformation Evangelist de Celonis, el software de orquestación de procesos se sitúa por encima del nivel de automatización de tareas y combina las automatizaciones individuales en un todo mayor. “La visión es que un día un proceso estará realmente totalmente automatizado y quizás incluso se ejecute de forma autónoma, es decir, sin intervención humana. O, para describirlo con una imagen, la automatización hasta la fecha es como los limpiaparabrisas automáticos, los faros y otros dispositivos de asistencia del coche. Pero toda esta automatización no hace que el coche sea totalmente autónomo, aunque haga la conducción más fácil y segura para el conductor. Para convertir un coche en un vehículo autónomo, hay que controlar todos los sistemas, enriquecerlos con datos de numerosos sensores como cámaras, radares, ultrasonidos, etc. y utilizar software inteligente, es decir, IA para orquestarlo todo de modo que el coche pueda realmente conducirse solo”.

Destacan también, “tendencias emergentes como automatización cognitiva, la automatización basada en eventos, la hiperautomatización, herramientas sin código/low code, automatización inteligente de documentos, soluciones en la nube y automatización de procesos de negocios inteligentes (BPA) con análisis avanzado”, concluye la Responsable de Marketing de Yooz.

EL IMPACTO DE LA IA GENERATIVA

Las herramientas de automatización actuales funcionan muy bien cuando se trata de tareas recurrentes y, sobre todo, basadas en reglas que utilizan datos estructurados. Sin embargo, cuando hay que convertir datos no estructurados en estructurados, las decisiones basadas en la experiencia humana han sido tradicionalmente superior-



res a los bots. Ahora, la IA generativa es capaz de extraer información, como un cambio de dirección o de datos bancarios, de un correo electrónico no estructurado, convertir esa información en un formulario estructurado y, a continuación, modificar automáticamente los datos maestros del cliente.

Por ello, como bien apunta Kuhn, “si la IA se entrena con la información adecuada, también puede tomar decisiones que no se basen en datos individuales, sino en la suma de la información, es decir, en la experiencia. Y los chatbots modernos son capaces de comunicarse tan bien con un humano que, en determinados escenarios, da igual que haya un humano o un bot al otro lado de la línea. La IA generativa tiene el potencial de permitir la automatización en áreas hasta ahora inexploradas”.

Sobre esto, en Appian utilizan la IA en tres líneas principales, “por un lado con la introducción de las AI Skills que permiten a los diseñadores aprovechar fácilmente la IA generativa en una arquitectura de IA segura y privada integrándola por completo y acelerando sus procesos comerciales. Por otro, con la disposición de herramientas de GenAI que intervienen en el propio diseño de las aplicaciones y nos permiten por ejemplo que se genere automáticamente una interfaz a partir de un documento. Y por último con componentes directamente disponibles para los usuarios finales que les permiten “conversar” con un conjunto de datos o con un documento para obtener métricas, analítica, resúmenes...”, destaca Riquelme. Al final, las empresas lo que persiguen es hacer las cosas más rápidamente, de formas más sencillas y robustas, “y para ello la combinación de RPA y la IA Generativa es muy importante al permitirnos llegar a un nivel más avanzado de hiperautomatización o Cognitive Automation, y la buena noticia es que cada vez es más fácil la combinación de estas tecnologías en una misma plataforma. Podemos utilizar RPA dentro de workflows de trabajo o BPM (Business Process Management) y combinarla con Decision Rules y Case Management para una toma de decisiones más complejas, y con la IA Generativa podemos ir más allá, incluyendo la predicción y la optimización de las decisiones. Otra posibilidad, que hemos comprobado que también funciona muy bien, es aplicar Process Mining para supervisar, analizar y mejorar los procesos utilizando técnicas de machine learning”, sintetiza Parada.

En resumen, “la (IAG) está transformando el mercado de la automatización, impulsando la eficiencia y la productividad empresarial. Según un estudio de McKinsey, un tercio de las organizaciones ya están utilizando IAG en al menos una función empresarial. Además, se espera que estimule la adopción de otras herramientas, aunque la adopción general de IA se ha mantenido estable desde 2022”, dice Aznar.

QUÉ ESTRATEGIAS SEGUIR PARA EL ÉXITO

Que un proyecto tenga éxito depende de muchos factores, pero es importante seguir una estrategia integral que abarque diferentes aspectos como identificar y seleccionar los procesos más adecuados para la automatización, aquellos que ofrecen el mayor potencial de mejora en términos de eficiencia, productividad, calidad y costes. Además, es crucial tener una comprensión clara de los objetivos que se desean alcanzar con el proyecto de automatización.

“Estos objetivos deben ser específicos, medibles, alcanzables, relevantes y con plazos definidos. Por último, sería necesario establecer métricas de desempeño claras y objetivas para evaluar el impacto de la automatización en los procesos y resultados empresariales, y realizar un seguimiento continuo del progreso para identificar puntos de mejora”, explica Ramón Riquelme, Solutions Consulting en Appian.

Toni Parada, aggy Head of Digital Solutions por su parte menciona la ciberseguridad, como base para el éxito de una empresa, “es un imperativo para cualquier empresa, también cuando hablamos de automatización y, específicamente, cuando hablamos de procesos en los que se trata información sensible o confidencial, o se manejan elementos como, por ejemplo, certificados digitales, ya que en caso de un mal caso o de caer en manos maliciosos, podría generar problemas”.

Además, debemos tener en cuenta estrategias como, “establecer indicadores claros de éxito para el programa y evaluarlos de manera regular, elaborar un plan de comunicación sólido, implementar una metodología integral que cubra todo el ciclo de vida (desde el Discovery hasta el control), una vez identificados los casos de uso, definir las tecnologías necesarias para el programa, establecer un servicio de soporte para los automatismos en producción y enfocarse en la automatización de procesos extremo a extremo con un impacto significativo en la organización, dejando de lado la automatización de tareas o procesos menores”, resume Marc Román Martínez, Head of Hyperautomation Iberia, Business Process



TEMA DE PORTADA

Automation de DXC Technology.

Por otro lado, un punto a tener en cuenta es que no hay que automatizarlo todo por reflejo, solo porque sea técnicamente posible, “las empresas deben seguir el principio ESSA (eliminar, simplificar, estandarizar, automatizar) para tener éxito. Y deben saber exactamente cómo y cómo funcionaba un proceso antes y después de la automatización”, explica Rudy Kuhn, Lead Transformation Evangelist de Celonis

De esta forma, una estrategia requiere de un proceso de cambio planificado, en el que juega un papel fundamental contar con un partner de confianza y con experiencia acumulada, como es el caso de Kyocera. “Para que un proyecto de automatización sea exitoso, es crucial seguir una estrategia bien definida y se debe implementar un seguimiento continuo y ajustes iterativos para garantizar que la automatización cumple con las expectativas y mejora constantemente”, comenta José Aznar, Business Solutions Manager de Kyocera.

En otras palabras, para lograr el éxito en un proyecto de automatización, según Cecilia Olaso, Responsable de Marketing de Yooz, las empresas deben, “definir objetivos claros, seleccionar tecnología adecuada, involucrar a partes interesadas, planificar y gestionar el cambio, iterar y mejorar continuamente, medir y hacer seguimiento de resultados, celebrar logros y aprender de ellos”.



LA OPINIÓN DEL CIO



Joan Barceló,
CIO de World2Meet

¿Cuál es el estado de la automatización en la empresa española actualmente?

La mayoría de las empresas españolas entienden los beneficios de la automatización, aunque su adopción es desigual y depende del tamaño de la organización, sector y madurez de sus procesos. Grandes empresas de sectores como banca, seguros, industria, y logística han avanzado en su implantación en los últimos 4 años, aunque son pocas las que están totalmente

automatizadas. Por otra parte, departamentos transversales como marketing, finanzas o recursos humanos han progresado en todos los sectores, gracias a los avances que se incorporan en las soluciones tecnológicas de los principales fabricantes. En World2Meet, en el sector turístico, nos estamos centrando en dos grandes bloques: todos los procesos directamente relacionados con la mejora de la experiencia de cliente, y todos los procesos de backoffice para mejorar la eficiencia y productividad de usuario.

¿Cuáles son las tendencias emergentes que más están influyendo en la automatización de procesos? ¿Qué aportará la Inteligencia Artificial tanto al RPA como al BPA?

En los últimos años ML y Cloud han impulsado la automatización, no obstante la tendencia emergente que más influye actualmente es la IA Generativa. El potencial en RPA y BPA es disruptivo, ya que permite dar un paso más allá de la automatización de tareas repetitivas. El análisis de contexto, la capacidad de procesar un mayor volumen de datos y el aprendizaje permiten tomar mejores decisiones y ser mucho más eficientes y productivos.

Nosotros creamos en 2023 una unidad específica de IA y automatización, denominada IPA (Intelligent Process Automation), para explorar las posibilidades de la automatización inteligente. Los resultados son prometedores. El primer proyecto consistió en analizar información procedente de diferentes canales (email, mensajería instantánea, etc.) combinado con documentos no estructurados que proporcionan contexto para la asignación de tareas con datos normalizados. La mejora de eficiencia es un éxito y aplica en todos los ámbitos: procesado inteligente de miles de facturas electrónicas al día, smart dispatchers de tareas a partir de emails con adjuntos, smart readers de mensajería instantánea que estructuran información para la preparación propuestas de nuestros agentes, etc.

¿En qué ha beneficiado la nube al desarrollo de las herramientas de automatización?

Sin duda, los principales beneficios son la accesibilidad, eliminando barreras de entrada y habilitando una rápida implantación tecnológica en cualquier tipo de empresa, y la escalabilidad, que proporciona flexibilidad para extender el uso y absorber picos de demanda. Otros beneficios son la inmediata disponibilidad de actualizaciones y mejoras, facilitando la innovación continua si los fabricantes incorporan nuevas tendencias como la IA. Sin embargo, hay diferentes aspectos que deben analizarse con detenimiento, desde los relacionados con seguridad, privacidad y compliance, a la complejidad de integración con los datos de la empresa o los costes de transición en el caso de necesitar cambiar de fabricante por cualquier motivo.

Por otra parte, es muy importante impulsar el uso eficiente de recursos, para evitar costes innecesarios, y valorar si hay procesos que requieren alta capacidad de proceso de datos o latencia mínima para evitar sorpresas desagradables.

¿Cómo saber cuáles son las tareas adecuadas para automatizar en una empresa?

Hay que combinar los factores tradicionales con la oportunidad de transformación. Los factores tradicionales se basan en analizar si la tarea es repetitiva desde un punto de vista de frecuencia, el volumen de trabajo que representa y si es predecible para que se pueda automatizar fácilmente. También se analizan conceptos para mejorar eficiencia, como buscar cuellos de botella que pueden retrasar otras tareas, y conceptos para mejorar precisión, como identificar aquellas tareas propensas a errores humanos. Sin embargo, este ejercicio es incompleto, ya que no cuestiona si el proceso es el más adecuado o si debería realizarse de otra forma. Una automatización sin pensamiento crítico puede escalar ineficiencias y se pierde una oportunidad de transformación.

La automatización puede incrementar el riesgo de sufrir ciberataques, ¿cómo se pueden proteger las empresas de posibles ciberataques a sus herramientas de automatización?

Es innegable que la automatización aumenta la superficie de ataque, y es un aspecto clave a considerar tanto en el plan de seguridad de la información, como en los planes de contingencia, de continuidad de negocio y de recuperación de desastres. La protección debe incluir, por una parte, las medidas de protección estándar de cualquier otro sistema de información: control estricto de accesos, securización de apis e integraciones, securización de redes y comunicaciones, mantener actualizado software a últimas versiones, monitorización, tests periódicos de penetración, devsecops, etc.

Sistemas de detección de amenazas: ¿seguridad o vulneración de privacidad?



En el mes de julio de 2021, el Parlamento Europeo derogó temporalmente la Directiva 2002/58/CE, conocida como ePrivacy, permitiendo a los proveedores de servicios de correo electrónico y mensajería instantánea rastrear, de manera

automática mediante Inteligencia Artificial, todas las comunicaciones entre ciudadanos. El objetivo de esta derogación era localizar contenido potencialmente sospechoso sobre pornografía infantil en internet.

El sistema, conocido coloquialmente como “Chat

Control”, fue aprobado a pesar de su impopularidad, ya que una encuesta realizada a la población de la Unión Europea recogió que el 72% de los encuestados se oponía al seguimiento general y automático de sus comunicaciones, al suponer una vigilancia masiva de toda la mensajería privada entre particulares y, en definitiva, el fin del secreto de la correspondencia digital.

Tras más de dos años de presión ciudadana, con multitud de detractores y cada vez menos impulsores, el pasado 26 de octubre de 2023 se hizo público que la comisión de Libertades Civiles del Parlamento Europeo había votado en contra del escaneo masivo de los mensajes privados de todos los ciudadanos europeos.

MARCHA ATRÁS

Es decir, Bruselas ha reulado en la aplicación generalizada del Chat Control, estableciendo que la normativa tan solo permitirá la interceptación de comunicaciones de aquellos individuos o grupos sospechosos de difundir material pedófilo.

A pesar de lo anterior, hace unos días nos encontramos con una noticia en los medios de comunicación que relataba la rocambolesca historia de un joven británico de 19 años que había sido juzgado ante la Audiencia Nacional al haber sido detenido por enviar un mensaje a un grupo privado de amigos en la plataforma Snapchat en el que, minutos antes de coger un avión de Londres a Menorca, aparecía una fotografía suya y un texto en inglés que decía: “De camino a volar el avión (soy miembro de los talibanes)”.

Una vez interceptado este mensaje por las autoridades, un EUROFIGHTER del ejército español escoltó el avión y, ya en tierra, detuvo al supuesto terrorista, que fue puesto en libertad de manera casi inmediata al comprobar que se trataba de una broma entre amigos y no una amenaza real.

Pero la historia no acabó aquí, pues la Fiscalía y la Abogacía del Estado solicitaron una condena para el joven de 22.500 euros de multa por un delito de desórdenes públicos provocados por una falsa amenaza de bomba y el pago de una indemnización de 94.782 euros al Ministerio de Defensa por el coste de movilizar la aeronave militar.

ABSOLUCIÓN

Finalmente, la Audiencia Nacional absolvió al jo-

ven al concluir en su sentencia que los mensajes “se realizan en un ambiente estrictamente privado, entre el acusado y sus amigos con los que vuela, a través de un grupo privado de la que solo ellos tienen acceso, por lo que ni remotamente el acusado podía suponer (como expresamente señala éste en el juicio), que la broma que gastaba a sus amigos pudiera ser interceptada o detectado por los servicios británicos, ni por terceros ajenos a sus amigos que reciben el mensaje”.

La sentencia hace constar que se desconoce cómo llegaron los servicios británicos a conocer la fotografía y mensaje enviados, lo que evidencia que la interceptación de estas comunicaciones se había realizado como consecuencia de ese escaneo masivo de mensajes privados entre particulares.

RASTREO MASIVO

Pese a que los hechos enjuiciados tuvieron lugar el 3 de julio de 2022, es decir, antes de que el Parlamento Europeo votara finalmente en contra del rastreo masivo y automático de mensajes privados, esta historia reaviva la tradicional polémica sobre dónde debe situarse el límite entre la seguridad (en este caso nacional) y la privacidad, más teniendo en cuenta que el acceso de las autoridades a este mensaje enviado en una conversación privada se produjo al amparo de un sistema supuestamente destinado a combatir la pornografía infantil.

El famoso cifrado de extremo a extremo (E2EE), usado por plataformas como Whatsapp o Telegram, tiene como principal objetivo proteger las comunicaciones privadas para que únicamente el emisor y receptor de un mensaje puedan tomar conocimiento de su contenido, impidiendo así que terceros -e incluso las propias plataformas que prestan el servicio- puedan acceder a él. Es evidente que este sistema está pensado para preservar la privacidad de los intervinientes, no obstante, a su vez favorece a aquellas personas que, conociendo esta hermeticidad, lo puedan utilizar como medio seguro para realizar actos ilícitos.

Juanjo Hdez. Bonache
manager de Écija Abogados

Lucía Castro Díaz, Gerente de DATALife

Fecha de nacimiento: 6 enero 1977

Hijos: uno

Hobbies: música en directo, literatura

Estudios: Licenciada en Química, doctorada en Ciencias de materiales

¿Cómo llegaste al mundo de las TIC?

Empecé como una usuaria de tecnología, quizás con un interés mayor que la media...

Pero a nivel profesional diría que entro en el mundo de las TIC cuando me incorporé a Mestrelab Research, una empresa que produce software para el análisis de datos de laboratorio. Allí estuve involucrada en gestión de proyectos de I+D y fue una gran experiencia de aprendizaje para mí.

¿Qué es lo que más valora de su trabajo?

Aprendo todos los días cosas nuevas, trabajo con un gran equipo y siento que estamos en la vanguardia de la innovación, ayudando a definir el futuro de cadenas de valor muy importantes para Galicia.

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

Probablemente sea un cúmulo de cosas que arrancan en la infancia, cuando se empieza a crear una imagen de que las STEM están más asociadas a los hombres; y continúa cuando profesionalmente los ambientes profesionales de las ciencias están muy masculinizados.

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

¿Cuál debería ser la solución?

Sí, en muchas empresas, TIC o no, existe un techo de cristal relacionado con la percepción del desempeño de las mujeres, en un liderazgo que habitualmente no encaja en las ideas tra-

dicionales, etc. La solución es que quien toma las decisiones sobre ascensos trabaje en los sesgos que todos tenemos y que las mujeres accedan a puestos de responsabilidad.

¿Una política de cuotas puede resolver el problema?

Sí, podría ser una de las soluciones.

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

No percibí ningún tipo de dificultad. Pero sí es cierto que es habitual que en situaciones de networking, si me acompaña alguno de mis compañeros, las personas que no nos conocen asuman que él tiene más responsabilidades que yo, por ejemplo, o que entiende mejor aspectos técnicos. Y tener que demostrar tu valía es algo que puede generar cierto hartazgo añadido al puesto.

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

En DATAlife desde el principio hay mujeres con responsabilidad, por ejemplo en nuestra junta directiva, que son un gran modelo para mí. Además al dedicarnos a la transformación digital y siendo conscientes de la brecha de género que existe, visibilizar a mujeres del mundo de las TIC ha estado presente en nuestra estrategia desde el principio.

¿Cómo compatibiliza su vida laboral con la personal? ¿Tiene su empresa planes para poder compatibilizar ambas?



Soy estricta con la separación entre ambas, desconectando fuera del horario laboral. En DATAlife tenemos flexibilidad horaria para respetar la vida personal del equipo. Tenemos un horario “común” en el que todos coincidimos y el resto de horas de la jornada las hacemos según nos convenga a cada uno. Reforzaremos esta estrategia de equilibrio con la implementación de un plan de igualdad con varias medidas que ayuden a la conciliación.

¿Qué cree que hay que mejorar en general para que se pueda compatibilizar mejor la vida privada o personal? ¿Es un problema de las empresas, de las relaciones de pareja o de uno mismo?

Hay que desechar el presencialismo, la idea de que muchas horas equivalen a ser mejor en el trabajo, más productivo. Resulta completamente falso... Siempre digo que prefiero un equipo que pueda atender a sus obligaciones familiares, que esté descansado, a uno que pone muchas horas. La gente que está tranquila y descansada es más creativa y tiene más capacidad de resolver problemas y generar un buen ambiente, algo esencial para el buen funcionamiento de una entidad como la nuestra que trata de fomentar la colaboración.

Un 35% de alumnos no logra acabar ni el bachillerato ni la FP equivalente, ¿está en la educación el problema de la falta de perfiles especializados?

Yo procuro ser prudente con los temas de la educación. Es algo muy complejo para lo que no me siento capacitada. Sí que veo que nuestra educación está muy centrada en memorizar, en vez de experimentar y esto desmotiva a una parte del alumnado. También veo a gente entre 15-17

años que no conocen toda la oferta formativa existente, que desconocen las salidas que cada opción les podría dar e incluso algunos para los que hacer un grado supone un esfuerzo económico que no se puede permitir su familia... Lo dicho, un tema serio y muy complejo.

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

Me han servido las habilidades “blandas”, como hablar en público, escribir, gestionar tiempos, etc. De vez en cuando me ayuda en proyectos concretos. Por ejemplo, hicimos unas sesiones formativas para la digitalización del laboratorio y fue muy útil tener conocimientos de microscopía o técnicas de espectroscopia.

Si tuviera que aconsejar a un joven qué estudiar de cara a obtener un futuro laboral estable, ¿por dónde le orientaría?

Siempre les aconsejo que hagan algo que les guste porque son demasiado jóvenes para ponerse a adivinar qué tendrá salidas cuando tengan 30 años. También que hablen con alguien que ya se dedica a algo que les interesa y les pregunten sobre su día a día, para ver si lo que viene después de los estudios se acerca a esa idea preconcebida de lo que les gustaría ser de mayores.

¿Hacia dónde cree que va el sector TIC? En su opinión, ¿cuáles van a ser las tendencias que realmente van a transformar la sociedad?

Hacia una eliminación de tareas rutinarias que dejará espacio para que las personas puedan ser creativas y ejercer de personas, no de engranajes en una máquina, por así decirlo. También será crítico en aportar soluciones a nuestros grandes retos, como la sostenibilidad, el envejecimiento activo, la medicina personalizada, etc.

IA, automatización, robótica, ¿de verdad cree que el futuro pasa por las personas?

Si el trabajo lo puede hacer una máquina, es probable que una persona no disfrute haciéndolo, ¿no crees?

Siempre digo que los trabajos del futuro serán aquellos donde necesitemos ser personas de verdad, como aquellos relacionados con los cuidados, con la creatividad, la innovación...



“Una de las mejores decisiones ha sido la apuesta por la nube”

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

Gobierno y gestión del dato;
Automatización; Ciberseguridad;
Gestión de plataformas cloud y
Desarrollo de nuevos productos

¿En qué área se está invirtiendo más este año?

Principalmente, en el gobierno y gestión del dato de cara a relanzar otras inicia-

tivas con impacto en el resto de los servicios de la entidad.

¿Qué proyecto es del que está más satisfecho?

La realización del proyecto de migración e implantación tecnológica de CHC Energía ha sido increíblemente gratificante. Después de salir de la joint venture que se mantenía con EDP, nos enfrentamos al desafío de implementar to-

da la plataforma tecnológica para poder albergar y migrar a los más de 400.000 clientes que gestionaba EDP sobre su plataforma operativa y tecnológica en tiempo muy acotado de dos años.

Tuvimos que implementar desde cero la nueva plataforma tecnológica de CHC Energía para seguir brindando servicios a nuestros más de 400.000 clientes, y delegados distribuidos en más de 160 delegaciones comerciales. Este proyec-

to, fue un verdadero hito. Toda esta implantación sin basarnos en una aproximación Cloud First nativa hubiese sido impensable teniendo en consideración los plazos de los que se disponía .

Si le pusieran todos los beneficios de la empresa a cargo del departamento de TI, ¿qué le gustaría implementar?

Sinceramente nada distinto de lo que estamos haciendo ya. Creo que hoy en día, la tecnología está al alcance de todo el mundo y es mucho más accesible de lo que venía siendo. SI es verdad que el poder disponer de mas tiempo muchas veces si es una ventaja.

¿Qué retos tiene un sector como el suyo?

Uno es la alta competitividad: El mercado eléctrico en España es muy competitivo, con numerosas comercializadoras compitiendo por clientes. Esto dificulta la diferenciación y puede reducir los márgenes de beneficio, lo nos obliga a innovar, ser muy eficientes ofreciendo productos y soporte de primer nivel. Otro reto es la regulación y normativas cambiantes: El sector eléctrico está sujeto a una regulación estricta y normativas que pueden cambiar con frecuencia. Los últimos años ha sido muy intensa en este sentido. Es mandatorio para nosotros ser capaces de implementar estos cambios normativos de una manera ágil y en tiempo. Esto nos empuja a adoptar soluciones basada en SaaS y desarrollos sobre metodologías DevSecOps que nos permitan ser eficientes, seguros y flexibles. Además añadiría la sostenibilidad, la digitalización, la fidelización de clientes: y la gestión de datos y la privacidad.

¿En qué va a ayudar la irrupción de la IA a una empresa como la suya?

Optimización en los cálculos de demanda y compra de energía: Nos permite ser más eficientes a la hora de predecir necesidades y comprar energía y la gestión de precios.

Personalización de servicios y precios: Nos permite analizar el comportamiento de nuestro buyer persona y los datos de uso de energía (bajo su consentimiento) de cara a personalizar los servicios y los precios según las necesidades individuales de cada buyer persona. Esto podría incluir programas de gestión de la demanda, tarifas dinámicas según la hora del día o incentivos para fomentar el uso eficiente de la energía.

Mejora de la experiencia del cliente: Mediante el uso de chatbots y sistemas de atención al cliente basados en IA, podremos ofrecer un servicio al cliente más eficiente y personalizado. Además nos va a permitir personalizar la oferta comercial de cada cliente de una manera perfilada.

¿Qué áreas son las que tienen más automatizadas? ¿Qué áreas van a automatizar más?

Trabajamos la automatización apoyándonos principalmente tres tecnologías que son cross a la inteligencia IA: RPA, Low-Code, Process Mining. Estas tecnologías en nuestra compañía se cubren de mayor a menor medida en los siguientes ámbitos: Procesos administrativos repetitivos; Servicio al cliente y atención al cliente; Gestión de recursos humanos; Operaciones financieras y contables y desarrollo y mantenimiento de aplicaciones por parte de los usuarios : Estamos intentado ayudar a los usuarios sean autónomos para crear sus propios aplicativos via plataformas LowCode e incorporando poco a poco los modelo CoPilot .

Óscar Monrío,
CIO-CTO de
CHC Energía

Lo de extraer el valor del dato, ¿supondrá de verdad la evolución de empresas como CHC?

Extraer el valor de datos y entender bien al cliente han de ser ejes críticos de toda compañía. No soy capaz de vislumbrar un modelo de compañía que pueda triunfar o sobrevivir y que no incorporen en su ADN estos dos puntos tan importantes.

¿En la nube u on-premise?

Una de las decisiones más acertadas ha sido la selección de implementar la infraestructura y desarrollos en la nube apoyándonos en distintos hyperscalers. Esta estrategia nos permitió aprovechar lo mejor de cada proveedor, maximizando así los beneficios y minimizando los riesgos asociados a depender de una única plataforma.

Además, la decisión de adoptar esta modalidad operativa para toda la entidad y en todos los ámbitos ha consolidado aún más el éxito del proyecto. Se decidió apostar por la innovación y la flexibilidad que ofrece la nube, permitiendo adaptarse rápidamente a las demandas cambiantes del mercado y optimizar los recursos disponibles.

El resultado final ha sido un gran paso, con un proyecto entregado en un tiempo récord, sin comprometer entre otros puntos la seguridad. La escalabilidad inherente a las plataformas en la nube nos permitió crecer de manera sostenible y escalar en momentos puntales de manera crítica y por tiempo limitado.

AVENET IT y Arcserve securizan los datos críticos de Patatas Meléndez

Con la instalación de su nueva fábrica, Patatas Meléndez dio un paso más en la digitalización de procesos, desarrollando un cambio de paradigma en la seguridad de sus datos. La demanda de sistemas que respaldaban la parte industrial requería una tecnología IT avanzada que garantizara el almacenamiento, custodia y acceso a la información. Un desafío que se abordó con éxito mediante una solución global de backup, implementando medidas de seguridad y optimizando las buenas prácticas de protección de datos con la estrategia 3-2-1-1 de Arcserve.

Patatas Meléndez inauguró su nueva fábrica automatizada con tecnología de la Industria 4.0. Al ser tecnológicamente más avanzada y automatizada pasó a generar un mayor volumen de datos desde múltiples fuentes que debían ser procesados y custodiados adecuadamente, ya que aportan un valor estratégico en la toma de decisiones y en su operatividad diaria.

Por ello, su necesidad principal era proteger toda esa tecnología a nivel de respaldo y optimizar la seguridad de la información frente a los posibles ataques ransomwares.

Tal y como asegura Sergio Calvo, Director de Sistemas de Patatas Meléndez, “sabiendo que el dato es el nuevo petróleo, es fundamental tener una herramienta que permita tener un poco de descanso frente a los ciberataques a los que estamos expuestos las empresas. Necesitamos más seguridad. Lo que teníamos no nos parecía suficiente”

LA SOLUCIÓN

Para dar respuesta a este desafío Arcserve junto con Avenet IT desarrolló un proyecto de seguridad que incluyó un modelo Appliance 9012, un dispositivo inmutable OneXafe 4512-96 TB, así como un entorno mixto de almacenamiento en la nube Cloud Hybrid.

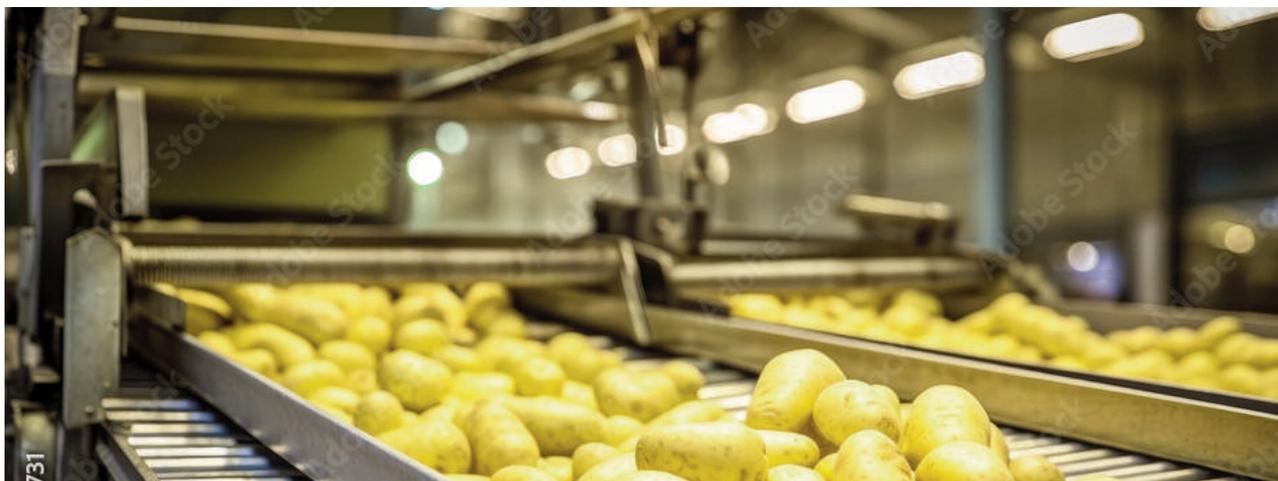
“La política de protección de datos que seguía históricamente la empresa era un modelo tradicional en el que hacíamos copias de seguridad basadas en backups completos de manera mensual, semanal o quincenal, y realizando, en períodos intermedios, backups incrementales o diferenciales. Este tipo

de copia ha sido sustituida por una copia más moderna, los incrementales infinitos, donde partimos de un backup completo inicial y todo lo demás van a ser backups incrementales, ya sean cualquier tipo de dato, información en un NAS, entornos virtuales o entornos hiperconvergentes, los vamos a copiar de manera incremental infinita”.

Ahora, con este cambio de paradigma al modelo 3-2-1-1 se incluyen 3 copias de los datos en 2 medios de copia diferentes -en 1 localización remota y en 1 almacenamiento inmutable (local)-. Se realiza una copia en el appliance que se réplica al dispositivo inmutable y permanece en él por un tiempo de 5 años, y al mismo tiempo, se replica a Arcserve Cloud Hybrid utilizando los incrementales infinitos del appliance con duplicación global y en origen. De esta manera se elimina riesgo de impacto en caso de ataque ransomware o pérdida de datos. Además, se incluyó un End Point para proteger al sistema protector de Arcserve.

LOS RESULTADOS

Las soluciones implementadas por Arcserve y Avenet IT han conseguido mejorar el proceso de almacenamiento, custodia y acceso a la información. Aunque se trató de un proyecto tecnológicamente muy avanzado, se incrementó la seguridad de los datos de una manera muy sencilla y clara a partir de la infraestructura inicial de la empresa. De esta manera Patatas Meléndez garantiza la seguridad de los datos contra diferentes escenarios de ciberataques. Esta transición hacia una mayor seguridad no requiere interrupciones en los procesos de pro-



ducción ni ha supuesto dificultades para los equipos de trabajo.

Tal y como afirma Sergio Calvo, Director de Sistemas de Patatas Meléndez, “el proyecto implementado por Arcserve y Avenet IT ha supuesto el crecimiento de una solución que ya teníamos, para llevarla a un nivel superior y para poder tener nuestro dato perfectamente protegido. Es como un seguro que probablemente no tengas que usar nunca, pero que en caso de que lo necesites, sabes que te ofrece una respuesta magnífica”.

MÁS DETALLES

Puedes conocer más detalles de cómo se llevó a cabo este caso de uso en el webinar que se celebrará el próximo 17 de abril a partir de las 11:00. Accede a través del QR



“Pasamos de realizar copias tradicionales a copiar de manera incremental infinita”.

Sergio Calvo, Director de Sistemas de Patatas Meléndez

El futuro de la oficina será virtual: ¿cómo preparar al empleado?

La idea que se tenía de los trabajos de oficina ha cambiado radicalmente en los últimos años. Ahora existen modelos híbridos y remotos que ofrecen una mayor flexibilidad; y cada vez más empresas ofrecen edificios en formato “campus”, con servicios y estética que se asemejan a los de los hoteles y cafeterías de moda, y “hot desks”, en lugar de asientos asignados. El dinamismo de estos nuevos conceptos de oficina no es compatible con entornos plagados de expedientes y archivos en papel, así que digitalizar todo este pasivo con las herramientas adecuadas, procurando trabajar únicamente en digital, es algo cada vez más imprescindible.

Pero ¿cuál será el siguiente paso en la evolución de las oficinas? Para saberlo, hay que analizar de cerca los lugares de trabajo del futuro, cuáles pueden ser algunos de sus principales avances y cómo pueden las organizaciones preparar a todo su personal, desde los recién llegados hasta los altos directivos, para el cambio.

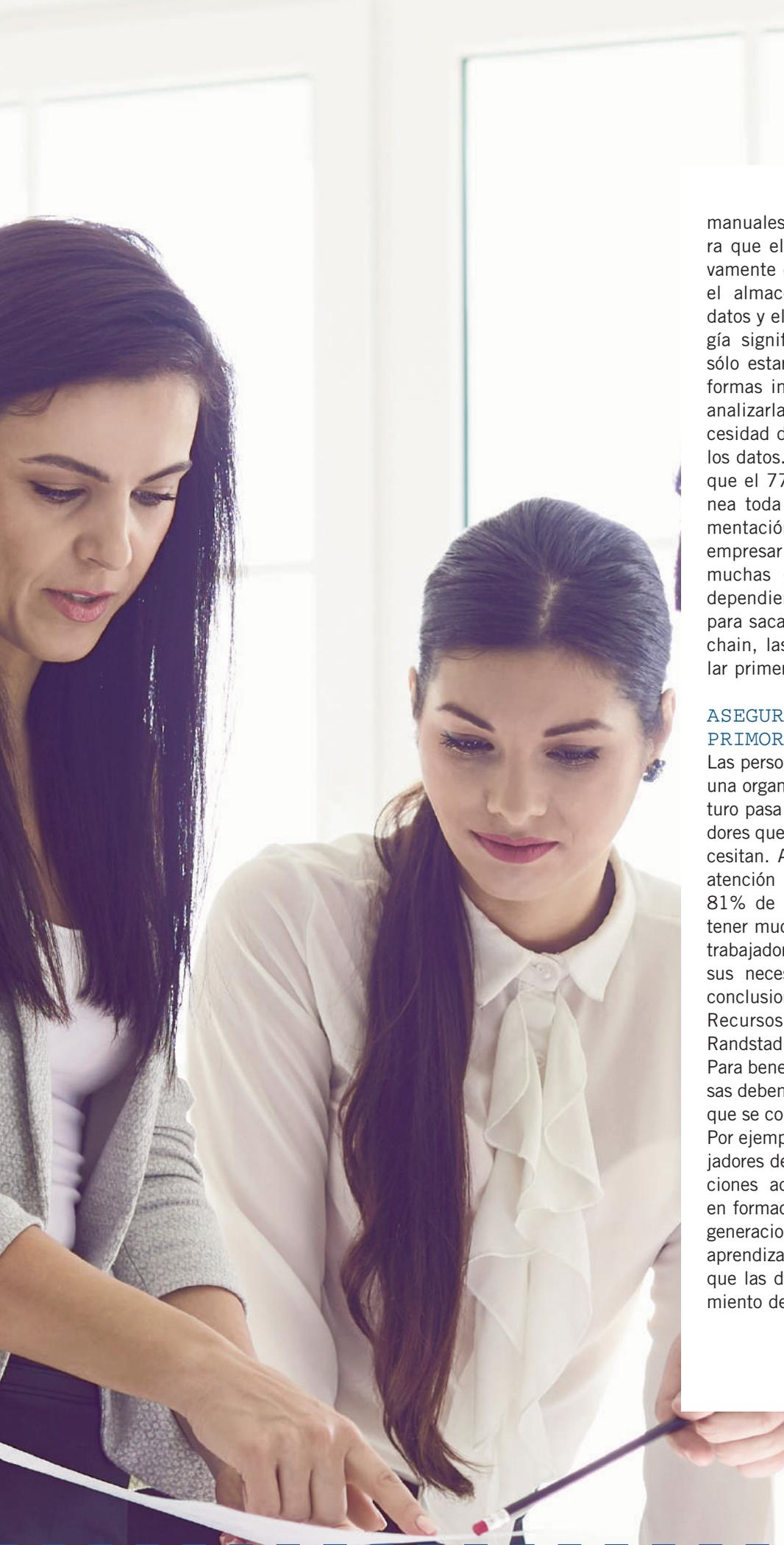
TRABAJO HÍBRIDO, A DISTANCIA O EN EL METAVERSO

El aspecto más obvio que hay que abordar al hablar de las oficinas del futuro son los modelos de trabajo híbridos y a distancia, que se han convertido en un elemento básico de la vida empresarial después de la pandemia. Aunque España es uno de los destinos favoritos de los nómadas digitales, según la última encuesta de población activa del INE, sólo el 14,4% de los trabajadores españoles declaró haber trabajado alguna vez desde casa en el cuarto trimestre de 2023. Si comparamos este dato con el de otros países más avanzados en este ámbito, como Reino Unido, en donde el 38% de los empleados teletrabaja al menos parte de la semana, nos damos cuenta de que a las empresas españolas les queda un largo camino por recorrer. Es necesario invertir en tecnología que permita

una experiencia de usuario totalmente fluida y eficiente para los profesionales tanto dentro de la oficina como fuera, y apostar por soluciones para aumentar la productividad, colaboración o movilidad, además de ayudar a completar la transformación digital. Sobre este último punto, si bien las organizaciones intentan adaptarse a los cambios, muchas aún no tienen controlados los procesos adecuados de gestión de documentos para su seguridad, acceso y fiabilidad. Los archivos en papel pueden suponer un problema cuando no se almacenan adecuadamente o no existe un proceso para destruir las copias físicas. Garantizar que los lugares de trabajo dispongan de copias digitales elimina el riesgo de que se pierda información valiosa o de que caiga en manos equivocadas, por lo que formar al personal en estos protocolos es esencial. Llevando esto un paso más allá, el metaverso tendría el potencial de crear un mundo completamente digital desde el que se pudiese trabajar y en el que los empleados no necesiten reunirse cara a cara (en formato físico) en absoluto. Pese a que esta tecnología está todavía en sus primeras fases, muchas empresas están dando pasos significativos en este ámbito. Microsoft quiere integrar su plataforma de RV/AR Mesh con Teams y ha anunciado futuros espacios inmersivos dentro de la aplicación de mensajería, mientras que Meta ha construido Horizon Workrooms para celebrar reuniones con gafas Oculus, lo que traerá consigo nuevos retos.

EL AUGE DE LA IA Y EL BLOCKCHAIN

Los modelos de procesamiento del lenguaje natural tienen la capacidad de automatizar completamente muchos procesos y hacer que el trabajo sea más eficiente. Muchas organizaciones se han dado prisa a la hora de mejorar las ineficiencias físicas, pero sus procesos administrativos, como los flujos de aprobación, siguen dependiendo en gran medida de las intervenciones



manuales del personal. También se espera que el blockchain avance significativamente en 2024. Más allá de la nube, el almacenamiento descentralizado de datos y el cifrado mediante esta tecnología significarán que la información no sólo estará más segura, sino que habrá formas innovadoras de acceder a ella y analizarla. Esto muestra de nuevo la necesidad de digitalizar y almacenar todos los datos. Un estudio de Quocirca revela que el 77% de las organizaciones escanea toda o la mayor parte de la documentación directamente en sus procesos empresariales, lo que indica que hay muchas empresas todavía que siguen dependiendo únicamente del papel. Y para sacar partido a la tecnología blockchain, las organizaciones deben controlar primero su gestión documental.

ASEGURAR EL TALENTO ES PRIMORDIAL

Las personas son el activo más valioso de una organización, y prepararse para el futuro pasa por conocer tanto a los trabajadores que se tienen como a los que se necesitan. Aunque cada vez se presta más atención a la educación, actualmente el 81% de las empresas españolas afirma tener muchas dificultades para encontrar trabajadores cualificados que se ajusten a sus necesidades específicas, según las conclusiones del informe Tendencias de Recursos Humanos, elaborado por Randstad Research y la CEOE.

Para beneficiarse en un futuro, las empresas deben abordar este problema antes de que se convierta en un lastre competitivo. Por ejemplo, si se garantiza que los trabajadores de más edad tengan las cualificaciones adecuadas mediante inversiones en formación, se evitará una gran brecha generacional dentro de un entorno de aprendizaje permanente y se garantizará que las decisiones se tomen con conocimiento de lo último en tecnología.

Por Paola Sánchez Ramírez,
Gerente de Marketing en Onum

El coste de integración en la gestión de los datos

Hoy los datos ofrecen una ventaja competitiva para cualquier empresa, ya que permiten tomar decisiones de manera más informada. Pero solo si se gestionan de manera efectiva. En un entorno tan complejo como el actual, existe un reto añadido debido a las distintas regulaciones y normativas, como la GDPR, la Schrems III, la Ley de Servicios Digitales de la UE (DSA), así como las leyes de inteligencia artificial recientemente aprobadas por la Unión Europea.

Ante los problemas generados por la escalabilidad y el cumplimiento normativo, las organizaciones recurren a herramientas específicas para la gestión de sus datos. Sin embargo, estas herramientas generan coste y complejidad adicionales.

¿QUÉ ES LA 'TASA DE INTEGRACIÓN' EN LA GESTIÓN DEL DATO?

Cualquier compañía genera datos de manera constante, bien sea a través de sensores IoT, infraestructura en la nube, dispositivos móviles, sitios web... Además, estos se encuentran alojados en múltiples entornos, tanto en la nube como en local. De hecho, según un reciente estudio que hemos realizado, dos de cada tres organizaciones en España están adoptando estrategias híbridas, y dentro de este colectivo, un 70% de ellas apuestan por un modelo multi-cloud. Esta complejidad está provocando que sea cada vez más difícil extraer información de los datos y gestionarlos a lo largo de todo su ciclo de vida, desde la creación y almacenamiento hasta el análisis y generación de valor para el negocio.

Para desbloquear todas las posibilidades del dato (desde la ingesta y transformación, hasta la capa de inteligencia artificial y Machine Learning), muchas empresas han tenido que generar un complejo ecosistema donde conviven múltiples soluciones específicas para cada una de las fases de vida del dato. Aunque estas soluciones pueden ayudar con casos de uso y procesos específicos, todas estas empresas

se están encontrando con que también agregan costes ocultos, asociados con el esfuerzo realizado para integrarlas.

Basado en este estudio, prácticamente todos (99%) los responsables de la toma de decisiones de TI de España ven como un desafío la integración de todas estas múltiples soluciones específicas para la gestión del ciclo de vida de los datos, de entre los cuales, un tercio de ellos (34%) calificaron el desafío como "muy importante". Los CIOs no solo deben tener en cuenta el coste técnico de la integración, sino también la formación especializada que los usuarios finales necesitarán para utilizar cada aplicación, ya que todas requieren de habilidades distintas. Esto puede impactar drásticamente en el retorno de inversión (ROI) a medio y largo plazo, suponiendo de manera efectiva un 'impuesto a la integración de datos' (en inglés, 'Data Integration Tax')

En la actualidad, y de manera práctica, más del 78% de los encuestados españoles creen que la integración de estas aplicaciones de análisis y gestión de los datos ha aumentado significativamente el coste total de propiedad. Como resultado, en la actualidad, las empresas españolas están destinando hasta un 30% de su presupuesto de TI a la gestión del ciclo de vida de los datos.

Para cualquier organización, es fundamental tener visibilidad y control de manera unificada de todo el entorno de datos, incluida la nube, para mantenerlo seguro y garantizando que se gestiona cumpliendo con las regulaciones pertinentes.

Para dar respuesta a estos desafíos, las organizaciones deben tender hacia unificar sus datos, consolidando las múltiples aplicaciones específicas en una plataforma que aporte una visión holística del dato, con todo integrado por defecto. Unificar de esta manera permite reducir costes ocultos (y algunos no tan ocultos) asociados con la gestión de estas mencionadas soluciones específicas.

El cambio tecnológico va siempre acompañado de un cambio cultural. Las organizaciones deben trabajar



hacia una estrategia de datos centralizada que agrupe las necesidades de todos los equipos y usuarios finales, en lugar de dejar la elección en manos de cada departamento o equipo individual. Debe, además, establecer una gobernanza sólida, con los formatos y las estructuras de datos gestionadas de manera centralizada en toda la empresa. Esto, por su lado, ayudará a reducir el tiempo y esfuerzo requeridos para transformarlos, al tiempo que mejorará la consistencia y calidad de los que ya estén integrados. Con este enfoque, las organizaciones pueden conocer y comprender mejor todos sus datos, para ponerlos a disposición de manera segura para quienes necesiten explotarlos. Adicionalmente, con este tipo de enfoque, las empresas se beneficiarán de una postura de seguridad y gobernanza ya incorporadas por defecto.

UN TRAMPOLÍN HACIA EL ÉXITO

Es evidente que la explotación de los datos forma parte de la estrategia de cualquier empresa moderna. Incluso el éxito de las tecnologías más actuales, como la inteligencia artificial generativa (GenAI), depende en última instancia de la calidad de los inputs con los que se entrena. En la actualidad, es un hecho que muchas organizaciones tienen dificultades para hacer una gestión eficiente de su ecosistema de datos, debido principalmente al uso de múltiples aplicaciones específicas, que no cumplen con su promesa de dar una solución integral, y además aumentan los costes exponencialmente.

Con un enfoque de plataforma unificada, los departamentos de TI pueden reducir su tasa de integración de los datos, despreocupándose de la complejidad intrínseca en materia de cumplimiento, regulación y normativa. Esto les permite liberar tiempo y recursos para generar valor a negocio de manera más rápida y frecuente (reduciendo el time-to-market), y por tanto, abriendo la puerta a la innovación continua y a la toma de decisiones basada en datos.

Por Javier Feixas,
Cloud Sales Specialist, Cloudera

Microservicios y Kubernetes: una guía para ecosistemas de software

El desarrollo de software es un proceso similar a la jardinería. En ambos casos hay que ser capaz de entender cómo diferentes elementos trabajan juntos para conseguir un resultado bello y productivo. De la misma forma, tanto en la jardinería como en el desarrollo de software surgen polémicas sobre cómo abordar multitud de aspectos.

Las plantas son los elementos más importantes en un jardín. Son los organismos vivos que lo componen y contribuyen a su belleza y funcionalidad. De manera similar, los microservicios son los principales componentes de las aplicaciones de software modernas. Son servicios individuales que realizan funciones específicas y trabajan juntos para crear una aplicación más grande y compleja.

Al igual que las plantas, los microservicios varían en tamaño, forma y propósito. Algunos son pequeños y especializados, y tienen la tarea de llevar a cabo una única operación. Otros son más grandes y se encargan de tareas menos concretas. Además, pueden estar formados por un grupo de componentes más pequeños. Por ejemplo, la planta de la fresa es pequeña y sólo produce fresas. Es parecida a un microservicio que solo procesa transacciones con tarjetas de crédito (pequeño y especializado). Sin embargo, una planta como el cilantro no solo produce las hojas que se utilizan en salsas y guacamoles. También sus tallos, raíces y semillas están presentes en los platos de multitud de gastronomías. El cilantro puede ser similar a un servicio que gestiona la autenticación de los usuarios, un proceso más amplio y general.

Contenedores: las macetas de los microservicios

La mayoría de las plantas necesitan plantarse en la tierra, de la que extraen nutrientes y humedad. Si dejamos sus raíces al aire, lo más seguro es que muera rápidamente. Aunque las plantas puedan introducirse directamente en el suelo, muchos jardineros prefieren utilizar macetas, ya que esto les permite utilizar la tierra más adecuada para cada planta y les facilita la defensa contra posibles plagas. Además,

pueden mover más fácilmente las plantas por distintas zonas del jardín o meterlas en un invernadero, buscando la luz o la temperatura más adecuada en cada estación del año. De manera similar, existen múltiples opciones a la hora de alojar un microservicio, y la más común es un contenedor. Un microservicio en un contenedor tiene todo lo que necesita para ejecutar la aplicación y se puede mover fácilmente por distintos entornos de ejecución.

KUBERNETES: LAS HERRAMIENTAS DE JARDINERÍA

Podemos tener nuestros microservicios (plantas) en nuestros contenedores (macetas), pero para implementarlos, mantenerlos y escalarlos necesitamos herramientas. Aquí es donde entra en juego Kubernetes, una plataforma que proporciona muchas funciones y complementos dirigidos a facilitar la gestión y el mantenimiento de los microservicios, y que se considera la herramienta clave para la orquestación de contenedores. Por ejemplo, Kubernetes proporciona balanceo de carga automatizado, descubrimiento de servicios y capacidades de autorreparación, algo que para los desarrolladores supone un ahorro de trabajo en las tareas de mantenimiento y monitorización. ¿Y cuándo se pretenda que los microservicios (plantas) produzcan más? Kubernetes soporta actualizaciones continuas y escalado automático para mantener un correcto funcionamiento de las aplicaciones de microservicio. Aquí hay que tener en cuenta que otras alternativas a Kubernetes, como Docker Swarm y HashiCorp Nomad, ofrecen, prácticamente, las mismas funcionalidades.

MICROSERVICIOS SIN KUBERNETES

Hemos establecido los argumentos a favor del uso de Kubernetes para gestionar microservicios y evitar que las aplicaciones se descontrolen. Pero Kubernetes y los contenedores no siempre son necesarios. Dependiendo de la complejidad de la aplicación, po-





dría optarse por utilizar una plataforma de máquina virtual o, incluso, física que pueda implementarse o provisionarse mediante herramientas de automatización. Estas herramientas no proporcionan el mismo nivel de automatización y escalabilidad que Kubernetes, pero es posible que sean una solución para aplicaciones poco complicadas o no críticas. Finalmente, existe la opción de utilizar plataformas sin servidor (como AWS Lambda) que permiten ejecutar código de microservicios en respuesta a eventos sin tener que preocuparse por la infraestructura subyacente.

Los jardineros expertos saben que con plantaciones complementarias (por ejemplo, caléndulas junto a tomates) se consigue un mejor uso de los recursos y un jardín más saludable. De igual manera, Kubernetes proporciona una amplia gama de funciones y complementos que hacen que esta plataforma sea buena para algo más que para la gestión de microservicios. Kubernetes se puede utilizar para aplicaciones que no sean de microservicios (como modelos de aprendizaje automático o monolitos). Muchas organizaciones utilizan Kubernetes para administrar microservicios y otras aplicaciones, y algunas de ellas, incluso, implementan máquinas virtuales (VM) dentro de Kubernetes. Esta puede ser una excelente opción para las organizaciones que están realizando la transición de aplicaciones monolíticas heredadas a una arquitectura orientada a microservicios.

Llegando a la raíz del asunto

- No todo lo que se implementa en Kubernetes es un microservicio. Las características y complementos que proporciona Kubernetes convierten a esta plataforma en una herramienta muy útil en una gran variedad de ecosistemas.
- No siempre es necesario gestionar los microservicios con Kubernetes. Algunas aplicaciones florecen con herramientas alternativas y con enfoques de jardín salvaje.

Por José Manuel Flores,
ingeniero de soluciones en F5

JULIO CAMPOY, REGIONAL VP IBERIA AND LATAM BROAD MARKETS EN APPIAN



“Appian es una plataforma que actúa como
un lienzo en blanco”

Appian cubre las necesidades de digitalización de cualquier tipo procesos de negocio. Hablamos con Julio Campoy, Regional VP Iberia and Latam Broad Markets en Appian sobre automatización y la apuesta de las AAPP por esta tecnología. **Por Manuel Navarro**

La automatización es una de las tecnologías que más importancia está teniendo entre las empresas ¿Qué tipo de soluciones de automatización de procesos ofrece Appian y cómo se adaptan a las necesidades de cada sector?

Lo que Appian ofrece es una plataforma unificada de hiperautomatización completa de procesos que añade las capacidades de desarrollo de low-code para hacer toda esa labor de una forma mucho más ágil, más rápida y más eficiente. El objetivo principal de Appian es ayudar a las compañías, independientemente del sector industrial al que pertenezcan, en sus iniciativas de transformación, digitalización y automatización de los procesos de negocio, en donde lo que se busca principalmente es la eficiencia tanto de los procesos como de los recursos humanos disponibles, además de conseguir mayor eficiencia y productividad.

Pero no sólo les ayudamos en lo que al apartado tecnológico se refiere, sino también en el apartado cultural porque este tipo de proyectos de automatización suponen un cambio en la forma en la que trabajan las empresas. Por eso, nosotros, a través de nuestros partners o de los servicios profesionales de la propia compañía, les ayudamos para que sean capaces de conseguir el valor y los beneficios para su negocio en línea con sus objetivos de negocio y que justifican la adopción de este tipo de tecnologías.

¿Cómo se define un proyecto de automatización? ¿Saben elegir las empresas cuáles son los procesos que deben automatizar?

Podemos decir que Appian es una plataforma que actúa como un lienzo en blanco en donde nuestros clientes pueden definir, construir e implantar cualquier tipo de proyecto de automatización, permitiendo a la empresa construir prácticamente cualquier tipo de solución, servicio o nuevo producto que tenga que ver con el mundo de los procesos a través de un desarrollo ágil y rápido de aplicaciones. En este sentido, si bien se puede construir prácticamente casi cualquier cosa, nosotros a nuestros clientes que empiezan a utilizar Appian por primera vez, siempre les recomendamos que escojan aquellos proyectos que para ellos sean más críticos, más importantes y donde la automatización les va a aportar mayor valor.

El problema con la automatización es que está sucediendo lo mismo con la IA: el Consejo de Dirección quiere implementar soluciones de automatización por aumentar la productividad, pero sin saber qué procesos son los más adecuados, ¿no?

Hay varios factores. A veces lo que ocurre es que cuando se lanza una iniciativa de automatización, el cliente lo que quiere es automatizar todo. Y eso no es así. Hay que ver qué tiene sentido automatizar y qué no tiene sentido. Cuando esa automatización tiene sentido porque aporta un valor, su adopción

va a aportar un beneficio al negocio del cliente que va a hacer que merezca la pena. Por eso, en Appian siempre le hacemos al cliente una precalificación de forma que le ayudamos a identificar cuáles son los casos de uso más adecuados para él. Con ese asesoramiento, el cliente, en primer lugar, consigue validar la tecnología, testarla y ver que efectivamente es lo que necesita. Y en segundo lugar, puede verificar de forma rápida el retorno de la inversión que le va a producir el despliegue de la misma. Es más, a algún cliente le hemos tenido que decir en alguna ocasión que no es conveniente que implemente un determinado proyecto porque no le va a aportar valor esperado.

Una de las ventajas que tiene Appian es que puede convivir con otro tipo de tecnologías de otros fabricantes...

Sí. Por ejemplo, ¿qué sucede si el cliente tiene un RPA?. La implantación de Appian en un ecosistema ya existente en el cliente no supone el dejar de usar esa solución si él cliente está contento con ella. Appian va a convivir con ella, pudiendo actuar como el pegamento y/o el orquestador de toda la arquitectura de sistemas existentes en el cliente. Para ello, Appian proporciona todas las capacidades avanzadas integración necesarias para integrarnos prácticamente con cualquier tipo de tecnología, incluidas por supuesto las tecnologías existentes de RPA en el mercado. De hecho, en el caso particular de soluciones de RPA, lo que le vamos a dar al cliente es un valor adicional. Vamos a permitir que se produzca un proceso más global y más completo.

En Appian estáis haciendo mucho hincapié en que las AAPP incorporen tecnologías de automatización. ¿Por qué en España van tan retrasados los organismos públicos en este aspecto?

Es cierto que la administración pública española ha comenzado con en este tipo de iniciativas de digitalización más tarde que otras instituciones europeas o americanas. Pero eso está cambiando y estamos viendo cómo las AAPP españolas están confiando en Appian porque tenemos la experiencia de más de 22 años trabajando con administraciones públicas de otros países en donde ya hemos ejecutado este tipo de proyectos de transformación de forma muy exitosa.

Lo que yo estoy percibiendo es que ahora mismo las diferentes instituciones del sector público español se están lanzando a incorporar iniciativas de este tipo. La gran mayoría de ellas ya están empezando a hacer sus proyectos piloto y en algunos casos ya tienen procesos más avanzados y están apostando por proyectos de mayor calado. Creo que este cambio que se está produciendo en la administración tiene que ver con la necesidad de mejorar la experiencia del ciudadano en los servicios que ofrecen.

Los malos atacan los servicios públicos



José Joaquín
Flechoso,
presidente de
Cibercotizante.

Los ciudadanos demandamos cada vez más eficacia por parte de las Administraciones Públicas y éstas, a su vez, trabajan para mejorar la eficiencia de los servicios que prestan a la ciudadanía facilitando trámites y reduciendo tiempos y por eso están entre los principales objetivos de los ciberdelincuentes que persiguen pedir rescates millonarios con sus ciberataques. Tal y como se señala desde distintos informes y estudios, alrededor del 34% de los ciberataques en España están dirigidos a entidades públicas de diversa naturaleza.

Según datos del CCN-CERT, en 2022, las administraciones y organismos públicos sufrieron 55.000 ciberataques, que aumentaron en 2023 a 107.000.

A pesar de ese incremento en el número de ciberataques, las previsiones señalan que esta cifra tenderá a dispararse en el presente año pues ya se han detectado entre enero y febrero de 2024, algo más de 25.000 ciberataques lo que supone un mal presagio para lo que queda de año. Si lo analizamos bien, se avista un aumento de un 190% con respecto a los mismos meses del año anterior.

Ante esto cabe preguntarse si realmente nos estamos protegiendo de forma cibersegura. Sabemos del peligro, pero en ocasiones aspectos presupuestarios, metodológicos o incumplimientos nor-

mativos obvian lo recogido en el Esquema Nacional de Seguridad (ENS) o la Directiva NIS 2 que imponen la adopción de unas medidas mínimas de seguridad.

Uno de los casos más recientes fue comunicado por la Cyberzaintza, la agencia vasca de seguridad, que confirmó que seis instituciones públicas vascas sufrieron ataques perpetrados por un grupo de ciberdelincuentes prorrusos debido a que en España se estaba formando a soldados ucranianos.

De entre la variedad de ciberataques y malware con el que se pretende atacar a las administraciones públicas, el ransomware se confirma como uno de los ataques más destacados contra las administraciones públicas. Con ellos los ciberdelincuentes pretenden obtener datos muy valiosos y de paso, si pueden, recibir el pago de un rescate. Otros de los ataques más habituales son aquellos dirigidos a la suplantación de identidad.

Un ciberataque tiene múltiples consecuencias y puede afectar gravemente al funcionamiento de los servicios públicos, pero, el impacto económico también puede ser muy alto, conllevando posibles sanciones por incumplimiento normativo. Por último, está el daño reputacional, algo de enorme gravedad, puesto que el prestigio y la confianza en la organización pueden verse gravemente afectados.



Forma parte de la comunidad ByTIC

Comunidad de innovación y tecnología
exclusiva para la Administración Pública

- ✓ Encuentros VIP presenciales de **estrategia** tecnológica con **Líderes y Consultoras TIC**
- ✓ Encuentros VIP presenciales de **mejores prácticas de empresa privada** para el Sector Público
- ✓ **Sesiones informativas** on line sobre el estado de la inversión TIC en España
- ✓ **Plataforma de innovación**
Encuesta + Informe + Evento presentación + 4 meses de Innovación con ITDM's al año
- ✓ **Barómetro del talento digital**
Entrevistas + Informe + Evento presentación + 4 meses de Innovación con ITDM's al año
- ✓ Sesiones informativas on line de buenas prácticas de Organismos Públicos para Organismos Públicos (Representante de comité + ByTIC + organismo)
- ✓ **Boletín personalizado** mensual ByTIC
- ✓ Acceso personalizado a plataforma **Adjudicacionestic.com**
- ✓ Invitación evento anual **PREMIOS a la INNOVACIÓN TIC** en Sector Público
- ✓ Invitación a **eventos TIC** organizados por BYTIC
- ✓ **Formación TIC** condiciones preferentes
- ✓ Invitación a encuentros anuales de **golf y pádel** ByTIC Media
- ✓ **Suscripción** gratuita a **Revista Byte TI**

 **Exclusivo** para responsables de **Administración Pública**

AI

ASLAN 31 ED 2024

17 y 18 ABRIL > MADRID

congreso.aslan.es

IA. UN GRAN AVANCE EN DIGITALIZACIÓN. TODO CAMBIA...



DATA RESILIENCE



CYBER SECURITY



DIGITAL WORKSPACE



CLOUD DATACENTER



INTELLIGENT NETWORKS

Todo cambia.

La irrupción de la IA está produciendo grandes cambios en la industria de la innovación digital. El Congreso ASLAN2024 es una oportunidad única para conocer cómo está evolucionando la ciberseguridad, el puesto de trabajo digital o la gestión del dato gracias a la inteligencia artificial y cómo afrontar los nuevos retos para redes, entornos multi-cloud, centros de datos y otras infraestructuras digitales.

Juntos aceleramos la transformación digital.



GLOBAL SPONSORS



EVENT SPONSORS



El gran evento anual en España organizado por la Asociación nacional de la industria tecnológica

@aslan/35 años