byte TI

www.revistabyte.es

mkm PUBLICACIONES

Revista Byte TI
Enero 2024

Nº322

LA CIBERSEGURIDAD AFRONTA NUEVOS RETOS

- EL AUGE DE SASE EN LA CIBERSEGURIDAD EMPRESARIAL
- EL FIN DEL FIREWALL INDEPENDIENTE

COMPARATIVA Soluciones ERP

XXIII PREMIOS BYTE TI
Premio al Mejor Software de Gestión Empresarial

SOLMICRO ERP
Mejor Software de Gestión Empresarial

ZUCCHETTI

El software que te acerca al éxito

www.zucchetti.es

94 427 13 62

El papel del CIO ante la IA

Manuel Navarro Ruiz
Director de BYTE TI

El año que comenzamos promete, en materia tecnológica, continuar con la Inteligencia Artificial como estrella protagonista. En los próximos doce meses seguiremos viendo como la IA va a seguir avanzando y desarrollándose. Conviene a los CIOs, sin embargo, no dejarse deslumbrar por el foco. A día de hoy, estamos hablando de una tecnología que todavía está en pañales. Sabemos que va a ser disruptiva y que promete transformar la forma en la que operan las compañías, pero es pertinente no verse abducido por los cantos de sirena.

La similitud de lo que puede suceder con la IA la podemos establecer con los inicios de la nube. En aquel momento, muchas empresas, atraídas por el mensaje de ahorro de costes, abrazaron los entornos cloud como la auténtica panacea para reducir los gastos que les producía su infraestructura de TI. Pero lo hicieron sin haber diseñado una estrategia eficaz y apostando por una tecnología que todavía no se conocía cómo iba a evolucionar. Hoy, esas empresas que se dejaron atraer por las supuestas bondades, ven cómo los costes no sólo no se han reducido, sino que se han incrementado. Por el camino, se han encontrado, además, con problemas para gestionar los diferentes entornos y tienen dificultades para volver a mover las cargas a otra nube o incluso, nuevamente, a entornos on-premise. La nube convertida en el nuevo on-premise.

El hecho de que medios como Byte TI y el resto de especializados hablemos sobre IA no tiene más objetivo que el de dar a conocer los avances que se están produciendo en esta materia. Sin embargo, ello no significa que haya que implementar soluciones que prometen acelerar la productividad y reducir los gastos de personal en tareas ineficientes y de poco valor.

Seguramente, habrán visto como muchas compañías del sector están vendiendo la incorporación de la IA en sus soluciones cuando hace menos de un año, no tenían ninguna herramienta de IA. ¿Cómo es posible? No lo es. Lo único que ha cambiado es que han cambiado la nomenclatura. Muchas de esas soluciones, hace 12 meses, hacían referencia al Machine Learning, al Big Data, a la analítica o a la automatización. Ahora han mutado, todas ellas, en Inteligencia Artificial.

Estamos ante una tecnología que va a cambiar todo, pero quizá conviene pararse a pensar un poco en los beneficios que se pueden obtener a día de hoy y si esas ventajas no serán mayores dentro de un año. Es necesario, desarrollar una estrategia que esté bien planificada para adoptar la IA dentro de los procesos de la organización para que no ocurra como con la nube en sus inicios.

El papel del CIO, va a ser fundamental y por eso es necesario que todos ellos se encuentren dentro del comité de dirección. Convencer a muchos CEOs y responsables de una empresa de que la IA no es un ChatGPT para todo, va a ser difícil.

SUMARIO

TEMA DE PORTADA

Los nuevos retos de la Ciberseguridad

38

N.º 322 • 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
Javier Palazon

Colaboradores
R.de Miguel, I. Pajuelo, O. González, M.López, F. Jofre, A. Moreno, MªJ. Recio, JJ. 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

ENERO 2024
Printed in Spain

EDITA
Publicaciones Informáticas MKM

ACTUALIDAD

COMPARATIVA

TENDENCIAS

TechByte analizó la nueva Ley de IA de la Unión Europea

TechByte, el único programa de radio de tecnología para empresas y que tiene lugar cada penúltimo martes de cada mes en Capital Radio, se emitió el pasado mes con el título de "IA y Ciberseguridad en la empresa"

El último programa de TechByte que se emite el tercer martes de cada mes en Capital Radio, abordó lo que va a suponer la nueva legislación sobre IA que va a poner en marcha la Unión Europea. Para ello, entrevistó a Javier López, abogado y socio de Écija, que abordó cuáles van a ser las principales reglas que conformen la nueva ley. Asimismo, analizó cuáles son los principales retos de la ciberseguridad en la empresa española y contó con la participación de Javier Torres, CISO de Allfunds; Javier Galloso, CISO de Banca March; Javier Sánchez Salas, CISO de ENGIE y Ángel Gálvez, Global CISO de Dufry.

Javier López, socio de Écija explicó durante su entrevista por qué es necesario regular la IA. En su opinión, "cuando se descubrió el fuego había gente que decía que era mejor no acercarse. Y evidentemente, el fuego puede tener efectos perniciosos y efectos muy buenos. Yo creo que los avances tecnológicos son necesarios. Un cuchillo "per se" no es ni bueno ni malo, pero puede servir para partir jamón o puede servir para matar a una persona. Quiero decir que el problema no es el instrumento, sino el uso que se hace de él. Con la IA, pasa exactamente lo mismo. Ahora nos parece algo absolutamente novedoso. Yo creo que la Inteligencia Artificial es buena, con la independencia de que haya que poner límites y regular, evidentemente".

El problema para iniciar a legislar es que nos encontramos con una herramienta que se encuentra en el inicio de su expansión. Así que, ¿cómo legislar algo que todavía no se conoce cómo puede evolucionar?. Javier López explicó que "lo que se ha aprobado es un acuerdo político que es muy importante que tiene que transformarse en una norma. Y hay que hacerla porque la realidad no para. Ya se están produciendo problemas de todo tipo generados con la inteligencia artificial. El problema fundamental es la competitividad que hay entre la Unión Europea y China y

Estados Unidos, donde digamos que hay menos trabas a todo lo que es el desarrollo, mientras que en la UE, hay más restricciones como vimos en el tema de la regulación sobre protección de datos. La futura normativa tiene una base, que son dos conceptos fundamentales. Por una parte está el riesgo y por otra parte son los sesgos discriminatorios. Entonces, en base a eso, se establecen una serie de prohibiciones. Por ejemplo, la más llamativa o la más importante diría que es la categorización biométrica. Todas las datos que se pueden sacar de nuestras caras, de nuestros usos, de nuestros comportamientos, todo eso la inteligencia artificial lo analiza y lo procesa de una manera muy eficaz y eso hace que se puedan generar estereotipos y también sexos. Esta normativa no será aplicación cuando se haga para abusos de defensa. Las fuerzas armadas podrán utilizar estos sistemas, porque se supone que nos están defendiendo a todos. Para temas de investigación e innovación, esto es fundamental, porque es que si no sería poner puertas al campo y no permitir el desarrollo que necesita cualquier tecnología. Por motivos no profesionales y, por supuesto en el ámbito policial, que era uno de los mayores conflictos que había era que si se podía utilizar o no se podía utilizar. Finalmente sí se va a poder utilizar, pero con una serie de limitaciones, de tal forma que sólo se podrá emplear en espacios públicos para delitos especial a gravedad, con un tiempo de ubicación limitado y siempre con autorización judicial. Vale.

MESA REDONDA: CIBERSEGURIDAD

La mesa redonda abordó la problemática de la ciberseguridad en la empresas española. Javier Torres, CISO de Allfunds, explicó que uno de los principales retos tiene que ver con la protección de los datos. En su opinión, "en el sector financiero tenemos una especial cautela en la protección de los datos, sobre todo de nuestros clientes, de nuestros empleados, que creo que es muy importante y muy relevante. Y al final, proteger esa información de nuestros clientes, es nuestra máxima. El phishing y el ransomware o un ransomware asociado a un phishing es el riesgo más alto que tenemos a día de hoy, porque casi siempre lo digo, tu cadena es tan fuerte como tu eslabón más débil. Y al final, siempre que pensamos que el empleado puede ser nuestro eslabón más débil. Y por eso hay que tener muchas medidas de protección, muchas medidas de formación a nuestros a nuestros empleados, para que el nivel de riesgo que podamos asumir a la hora de tener un phishing o un ransomware sea el menor posible."

Para Javier Galloso, CISO de Banca March uno de los retos es el cumplimiento de la norma: "Es verdad que como entidad financiera, ya hace muchos años que tenemos una regulación muy fuerte en materia de ciberseguridad. Y esta nueva regulación, Dora, por ejemplo, lo que nos ayuda es a hacer nuestra organización más ciberresiliente, que es el reto que tenemos actualmente: ir mejorando esta respuesta a la cooperación ante incidentes de seguridad. Y cada vez más la regulación nos va ayudando a cumplir este objetivo. La legislación cada vez es más práctica, cada vez se acerca más a la realidad y es uno de los puntos más importantes de estos años".

Por su parte, Ángel Gálvez, Global CISO de Dufry, explicó que "uno de los principales riesgos sigue siendo el ransomware. Pero aquí el enfoque sí que ha cambiado. Ahora más que en lo de los ataques de ransomware tradicionales que estaban diseñados para provocar indisponibilidad de servicios, actualmente se ve más el intento de fuga de información. Es decir, lo que buscan es recoger información, porque las empresas estamos más preparadas para recuperar los sistemas, pero ante una fuga ya tenemos poca capacidad de maniobra, puesto que hay incumplimientos legales, hay solicitud económica para recuperar o no publicar esa información y es el principal peligro. Son ataques más sofisticados, suelen llevar más tiempo, se van haciendo de forma más lenta y ante eso, principalmente, es buscar una seguridad más proactiva, invertir más en detección en los diferentes entornos, más cuando estamos en en entornos diversos, entornos cloud, on-premise, donde a veces no sabemos ni dónde están los datos de la compañía. Y es hacia dónde tenemos que enfocarnos.

Para Javier Sánchez Salas, CISO de ENGIE una de las claves en materia de ciberseguridad debe estar en la formación: "No se trata de hacer una campaña de formación al año y pararte ahí. Si tienes una formación continua, igual que a nuestros pequeños en casa les dan una formación continua, con los empleados tiene que suceder lo mismo. Hay que hacer tests, hay que realizar simulacros de phishing para que vean que realmente son capaces de que les lleguen a ellos por muy protegidos que estemos y pican. Incluso, enseñarles los porcentajes de éxito que tiene ese simulacro. Yo creo que vale más el quedar expuesto a algunos usuarios que en formarles. Es decir, lo ves, te hemos formado, te hemos dado un montón de cursos, un montón de formación, y aún así has picado, ten cuidado. Yo creo que es jugar un poquito con el, entre comillas, miedo del usuario"

LA OPINIÓN DE
Fernando Jofre

Reimaginando la creación de valor

Finalizando el año pasado, IDC volvió a publicar sus predicciones para 2024. En primer lugar, pronostican que el gasto digital en la región EMEA aumentará significativamente, creciendo a un ritmo cuatro veces superior al PIB de este mismo año. En línea con lo que hemos venido observando en el 2023 ya concluido, no me sorprende en absoluto que IDC nos diga que se inicia el capítulo de la "AI Everywhere". Estará omnipresente e integrada tanto en las operaciones como en las estrategias empresariales venideras.

Se trata de aprovechar los datos a través de la IA generativa para la evolución de los productos, de los servicios, de la captación de clientes… creando nuevos casos de uso y acelerando la obtención de resultados. Según la encuesta IDC EMEA Emerging Tech Survey, el 72% de las organizaciones de la región EMEA ya están utilizando o tienen previsto utilizar la IA en los próximos dos años. Y aquí vienen las cifras de inversión: para 2025, la cuota de presupuesto digital de la IA en las organizaciones de EMEA crecerá un 40%, lo que supondrá un nuevo gasto neto adicional de más de 30.000 millones de dólares.

Esa "AI Everywhere" hará que para 2026 el 85% de la población conectada en EMEA se beneficie activamente de la GenAI en su vida cotidiana, experimentando una mejora de la calidad de vida en áreas tales como la salud física y el bienestar mental. Profundizando en el título de mi columna, para el 2026, el 70% de las grandes empresas de EMEA lograrán tomar decisiones en tiempo real aprovechando una visión única del cliente impulsada por la IA, lo que aumentará el valor del ciclo de vida del cliente nada menos que un 50%. Y el co-diseño de productos y servicios apoyados en la IA generativa acelerará en 2X el tiempo de lanzamiento al mercado de nuevos productos y servicios. ¡Bienvenidos a la AI Everywhere!

AUSAPE elegirá nueva Junta Directiva

El año 2024 será un año especial para AUSAPE, ya que la Asociación de Usuarios de SAP en España celebrará su 30º aniversario. Un año en el que, además, renovará su Junta Directiva para el periodo 2024-2025. La elección de la nueva Junta, la aprobación de las actividades para este año de aniversario y la rendición de cuentas sobre la gestión en 2023 serán los ejes centrales de la 30ª Asamblea General de AUSAPE, que tendrá lugar el próximo 25 de enero. La asamblea se celebrará en un formato híbrido: de modo presencial en las oficinas de la asociación en Madrid y a través de videoconferencia, facilitando así la participación de los asociados que no puedan asistir físicamente.

Los siete miembros de la Junta Directiva de AUSAPE que estarán al frente de la organización los dos próximos años serán elegidos mediante una votación electrónica, que comenzará el 24 de enero y concluirá el propio día 25. El plazo para presentar las candidaturas se abrió el pasado 23 de noviembre y estará abierto hasta el 8 de enero. Los perfiles de los candidatos a formar parte de la Junta durante el periodo 2024-2025 se irán publicando en la web de AUSAPE, de modo que los asociados puedan consultarlos antes de decidir su voto.

En la 30ª Asamblea también se informará a los asociados del Plan de Actividades previsto para 2024, así como del Presupuesto para el nuevo ejercicio, que deberán ser refrendados por los participantes.

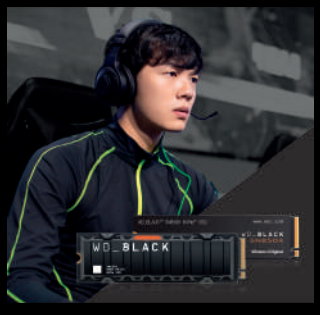
Asimismo, se presentarán los Informes de Gestión, Actividades y Resultados de 2023, los resultados de la Encuesta de Satisfacción AUSAPE y un resumen del Informe de Auditoría, que también se someterán a la aprobación de los asociados.

Western Digital.

myWD™ PARTNER PROGRAM

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.

LA OPINIÓN DE
Manuel López

La caja de Pandora

La omnipresente Inteligencia Artificial, puede ser la versión moderna de la leyenda griega de la Caja de Pandora. Si analizamos lo que está ocurriendo con la Inteligencia Artificial, cada día se parece más a la Caja de Pandora. A lo largo de 2023 el desarrollo exponencial de la IA ha hecho que prácticamente solo se hable de IA en la sociedad en general y en el mundo de la tecnología en particular. Además, con esa tendencia que tenemos los humanos a que solo lo malo sea noticia, casi siempre se habla de la IA como si fuera el principio de todos los males que acabarán con la humanidad.

En este entorno, en diciembre de 2023 han ocurrido dos eventos muy relevantes. Por un lado, el acuerdo en Europa para regular la IA, un acuerdo que próximamente se sustanciará en una nueva ley de IA, que será la primera a nivel mundial y por otro lado, el lanzamiento desde Google de Gemini, la nueva IA basada en lenguaje multimodal, que está llamada a iniciar una nueva revolución en la IA, parecida a la que se produjo en noviembre de 2022, con el lanzamiento de ChatGPT y darle un nuevo impulso, que quien sabe hasta donde llevará a la IA y con ella a la humanidad.

Estos dos eventos me hacen volver a la leyenda de la caja de Pandora, donde Gemini puede ser el último mal que escapa de la Caja de Pandora y la regulación podría ser el Elpis, la esperanza de que finalmente podamos tener un mínimo control sobre lo que ha liberado la Caja de Pandora del siglo XXI. Está en nuestras manos que la IA siga siendo los males que salen de la caja de Pandora o que explotemos la IA para que sea la esperanza de la humanidad y hacer de ella un motor de desarrollo nunca antes visto.

Los beneficios de la digitalización

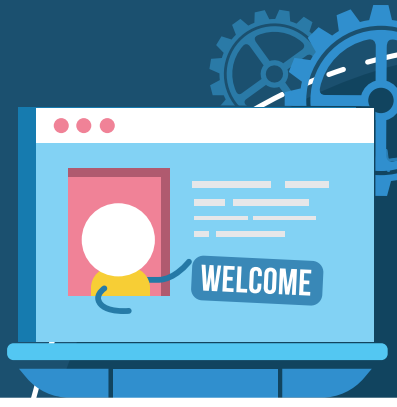
A pesar de la incertidumbre económica, los líderes en digitalización siguen apostando por la generación de valor mediante la innovación. Según el informe 'KPMG Global Tech Report 2023', el 61% de las empresas en España ha experimentado un aumento de beneficios y mejoras en la eficiencia de sus procesos en los últimos dos años gracias a la implementación de tecnología SaaS. A nivel global, el respaldo de los altos directivos a la adopción de herramientas y tecnologías emergentes se ha cuadruplicado en el último año, alcanzando el 38%, cifra que se replica en España.

La digitalización ha sido un impulsor clave de los beneficios empresariales, con el 29% de las empresas en España logrando aumentos en sus beneficios mediante inversiones en inteligencia artificial y automatización, superando a la media global del 26%. Además, el 24% de los encuestados afirma que ha mejorado su rentabilidad gracias a las inversiones en análisis de datos.

En el corto plazo, la inteligencia artificial y el machine learning se destacan como claves para alcanzar los objetivos de digitalización, siendo respaldados por el 55% de los directivos españoles y el 57% a nivel mundial. En cuanto a la tecnología como servicio (SaaS), tanto en España como a nivel global, se destacan tres beneficios clave: mejora en la gestión e integración de datos, impulso en la adopción de tecnología y reducción de la huella de carbono.

"Para que el ritmo de la transformación siga avanzando con éxito será necesario apoyarse en tres palancas: el talento; la colaboración, tanto dentro de la organización como con alianzas sectoriales y con líderes tecnológicos; y la inversión en tecnología, y en gestión del cambio y de las personas", afirma Fernando Echevarría, socio responsable de Technology Enablement de KPMG en España.

LA PLATAFORMA DE MARKETING AUTOMATION



GESTIONA TUS LEADS Y POTENCIA LAS VENTAS

CON ENVÍOS AUTOMÁTICOS DE EMAIL Y SMS

www.mdirector.com | info@mdirector.com | +34 91 414 91 94

MDirector
ANTEVENIO E-MARKETING TOOL

LA OPINIÓN DE
Daniel Puente

Automatiza que no es poco

Comentábamos meses atrás que parecía que esta vez la innovación de referencia sí iba a ser algo práctico y generalizado, a diferencia de tendencias anteriores, llámense metaverso, blockchain, etc, que si bien disponen de aplicaciones prácticas no han llegado al nivel de uso y funcionalidad esperado. Pero con la inteligencia artificial y más concretamente con ChatGPT y derivados parece que por fin hemos conseguido generar casos de uso que aporten valor de forma generalizada.Actualmente podemos encontrar muchas automatizaciones hechas para el mundo de la seguridad, desde funciones hechas para comprobar la seguridad perimetral de las propias empresas como utilidades que nos permiten comprobar la validez y complitud de los diversos cuestionarios que proporcionamos a proveedores, clientes y otros terceros para evaluarlos.

Esto ha hecho que se generen comunidades en las que se trabaja para adaptar esta inteligencia a la adaptación de normativas en las compañías. Se han desarrollado capacidades para analizar toda la documentación necesaria para dar cumplimiento por ejemplo a la NIS2, muy en boca de todos ahora mismo, para PCI-DSS e incluso para el Esquena Nacional de Seguridad. Pero como todo no podía ser idílico, parte de estas aplicaciones se encuentran o bien en la versión de pago de la famosa Inteligencia Artificial o bien en comunidades que también solicitan una membresía para poder utilizarlas.

Independientemente de la parte económica está claro que su utilidad práctica es más que evidente y, si bien estas creaciones no están exentas muchas veces de necesitar una revisión humana, el trabajo que realizan y del que descargan a las plantillas es notable. Y todo esto a la espera de que los grandes fabricantes de software liberen sus novedades que la incorporan.

Lenovo: nueva apuesta por la nube híbrida

Lenovo ha ampliado su plataforma de nube híbrida para IA a través de las nuevas soluciones hiperconvergentes ThinkAgile y servidores ThinkSystem. Estas novedades impulsarán el despliegue de la nube, la conectividad híbrida y las capacidades de IA, aprovechando la nueva generación de procesadores Intel Xeon Scalable.

La plataforma actualizada, lista para la IA, ofrece un rendimiento mejorado y los últimos aceleradores, marcando un paso crucial hacia un enfoque dinámico de IA híbrida entre modelos públicos, privados y fundacionales, con el objetivo de hacer que la IA sea accesible para todos. Las nuevas soluciones para la nube híbrida, Lenovo ThinkAgile, han sido diseñadas para potenciar el rendimiento de la IA y la agilidad de la nube al proporcionar mayor capacidad informática y una memoria más rápida a la cartera líder en el mercado de Lenovo, disponible en cualquier ubicación y momento necesario.

"Las soluciones de nube híbrida Lenovo para cargas de trabajo de IA están impulsando la innovación y creando un camino más rápido y flexible hacia la IA, al proporcionar informática de nivel centro de datos en la fuente de los datos de negocio", explica Kamran Amini, Vicepresidente y Director General de Servidores, Almacenamiento y Software del Grupo de Soluciones de Infraestructura de Lenovo.

IA para la nube híbrida

Lenovo ofrece soluciones integrales y optimizadas para satisfacer las crecientes necesidades de los equipos de TIC y el ritmo de expansión empresarial. Sus soluciones preconfiguradas de nube híbrida ThinkAgile HX, MX y VX, diseñadas para la inteligencia artificial (IA), aprovechan los nuevos procesadores Intel Xeon Scalable de 5ª generación y colaboran con socios como Microsoft, Nutanix y VMware. Estas soluciones proporcionan capacidades avanzadas, copias de seguridad rápidas, recuperación eficiente y reducción significativa del tiempo de despliegue, hasta un 75%.

Entornos Smart Work ágiles e inteligentes para garantizar la continuidad de negocio

Por Raquel Pinillos,
directora de Business Solutions de Kyocera Document Solutions España

El tejido empresarial español está demostrando en los últimos años disponer de una capacidad de resiliencia ejemplar que le está permitiendo afrontar y adaptarse a las necesidades cambiantes de la sociedad, pero también a los imprevistos que se puedan originar, y sentar las bases necesarias que le permitan competir y ser relevantes en los próximos años. En una sociedad que avanza a grandes velocidades, ser flexibles, ágiles e inteligentes se antoja imprescindible para ser realmente relevante y exige apostar por la innovación y la digitalización para estar a la altura. La estrategia tecnológica de las organizaciones debería tener elaborado un plan de digitalización coherente, ordenado y alineado con los objetivos empresariales que asegure la continuidad del negocio, e incremente los niveles de eficiencia y efectividad.

Uno de los aspectos que mayor peso han tenido en esta evolución es la automatización de tareas que poco valor aportan a la empresa pero que exigen ser realizadas con precisión. Los procesos documentales manuales ya no son una opción viable para las empresas modernas y la automatización permite acelerar los procesos y reducir la probabilidad de errores, además de liberar a las personas para que centren todo su esfuerzo en tareas de valor. Está demostrado que almacenar y organizar archivos de forma eficiente no solo aumenta la productividad y la competitividad, sino que también elimina los inconvenientes que supone la gestión de documentos en papel. Invertir en la digitalización de documentos y en una plataforma de gestión documental digital es una necesidad imperante para cualquier empresa que aspire a ser eficiente, segura y competitiva.

La sociedad se transforma y, en consecuencia, las organizaciones lo deben hacer con ella. La irrupción de nuevos factores en la ecuación como la sostenibilidad, la digitalización o las nuevas formas de trabajo, hace que las empresas tengan la necesidad imperiosa de transformarse para poder ser competitivas.

Para facilitar estas nuevas formas de trabajar, Kyocera facilita entornos de trabajo más allá del híbrido, que denominamos Smart Work, un ecosistema en el que las personas pasan a desempeñar un papel determinante junto a la tecnología y que da lugar a la creación de empresas dinámicas, innovadoras y altamente competitivas.

Para ayudarlas a conseguir este objetivo, hemos desarrollado Kyocera Cloud Information Manager (KCIM), que permite a las empresas mejorar la flexibilidad y el rendimiento al permitir un control total sobre sus documentos. Se trata de una plataforma SaaS que facilita el almacenamiento y la gestión de todos los documentos digitales en la nube y en un entorno seguro, lo que permite optimizar e impulsar el desarrollo del Smart Working.

Además, a medida que estas empresas aumentan su digitalización, se encuentran con la necesidad de administrar conjuntos de datos cada vez más grandes que a menudo incluyen datos personales críticos y sensibles, tanto de clientes como de empleados. Esta información es un activo con un valor incalculable, pero también implica responsabilidad y riesgo y requiere generar confianza para asegurar a los clientes que sus datos están seguros. En este sentido, la seguridad es una de las señas de identidad de KCIM, al contar con el respaldo de una plataforma cifrada que evita complicaciones ante cualquier posible ataque.

En definitiva, inteligencia y agilidad, son dos cualidades cada vez más reconocidas y preciadas en el ámbito empresarial por su capacidad para transformar organizaciones y prepararlas para afrontar el futuro. Cualidades en las que trabajamos desde Kyocera con el objetivo principal de ayudar a nuestros clientes a ir un paso por delante de su competencia, garantizando la continuidad de negocio.

La formación, elemento clave para reducir el impacto de los ciberataques

Por Marc Rivero,
Lead Security Researcher de Kaspersky

Hoy en día, la ciberseguridad sigue siendo un desafío significativo para las empresas. Avances tecnológicos, como la adopción de la nube, el Internet de las cosas (IoT) y la Inteligencia Artificial, han creado nuevas oportunidades, pero también han introducido nuevos riesgos y vectores de ataque. Las amenazas cibernéticas, como ataques de ransomware, phishing y violaciones de datos, continúan siendo una preocupación constante.

Por su parte, se espera que la demanda de soluciones VPN experimente un notable aumento al nivel mundial en el próximo año, ya que la preocupación por la seguridad de los datos tanto personales como empresariales ha ido en aumento este año. En general, se ha observado un aumento en la conciencia sobre la importancia de la ciberseguridad, y muchas empresas están invirtiendo más en medidas preventivas y en la formación de sus empleados. Sin embargo, los ciberdelincuentes también están mejorando sus tácticas, lo que hace que la ciberseguridad sea una carrera constante entre defensores y atacantes.

Para afrontar los diferentes retos a los que están expuestos las empresas en materia de ciberseguridad es necesario tener definida y diseñada una correcta estrategia que permita a la organización no sólo defenderse de los posibles ataques, sino también tomar medidas para prevenirlos antes de que éstos se produzcan. La implementación de una estrategia efectiva para la protección de la información requiere diversos aspectos de la ciberseguridad. En primer lugar, es esencial realizar evaluaciones periódicas de riesgos para identificar amenazas potenciales y vulnerabilidades específicas en el entorno empresarial. Por otro lado, la implementación de controles de acceso, el cifrado de datos, las actualizaciones y parches regulares, los respaldos periódicos y sistemas de monitoreo continuo son prácticas esenciales para fortalecer la postura de seguridad.

LA IMPORTANCIA DE LA FORMACIÓN

Pero uno de los elementos más importantes a la hora de implementar una estrategia de ciberseguridad pasa por tener empleados formados que sean conscientes de la gravedad que puede tener el éxito de un ciberataque. Por ese motivo, además de contar con soluciones de protección y prevención, las organizaciones deben proporcionar programas educativos en ciberseguridad a los empleados ya que, el error humano es una de las principales causas de los incidentes cibernéticos en las empresas.

En muchas ocasiones, los usuarios pueden no ser completamente conscientes de todas las amenazas y, por consiguiente, de las mejores prácticas de ciberseguridad que aplicar. Por ello la formación es un elemento esencial en la estrategia de seguridad de una empresa, ya que ayuda a los empleados a comprender las amenazas potenciales, como el phishing, malware y ataques de ingeniería social. Además, les enseña a reconocer señales de advertencia y a adoptar comportamientos seguros.

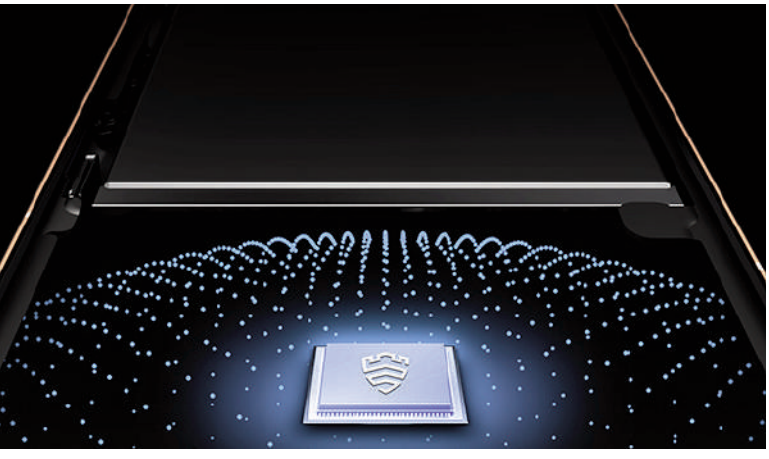
La formación también les proporciona información sobre las políticas de seguridad de la empresa y las mejores prácticas que deben seguir, como el uso de contraseñas seguras, la actualización regular de software y la gestión responsable de datos. Con ello, también se crea una cultura de seguridad en la empresa al sentirse parte activa en la protección de los activos de la compañía.

Al ser cada vez más conscientes de los riesgos, las empresas reconocen la importancia de invertir en programas de formación efectivos para enfrentar de manera efectiva los desafíos en evolución del panorama de amenazas online.

En este sentido, la Inteligencia Artificial puede suponer una ventaja en la formación de los empleados. En la actualidad la IA ya se está empleando para simular ataques y entrenar a profesionales de seguridad en escenarios más realistas. Todo ello supone un avance en materia de protección de las empresas ya que además de los planes formativos que tengan incorporados la IA puede ayudar a preparar mejor a las compañías frente a amenazas emergentes.

Aun así, todavía hay muchas tareas y decisiones que requieren la intuición, experiencia y juicio humano. Además, hay que tener en cuenta que los cibercriminales también la pueden utilizar para diseñar ataques específicamente dirigidos a engañar o eludir sistemas basados en IA.

La educación del empleado es un pilar de la estrategia de ciberseguridad



El entorno empresarial actual presenta cada día nuevos retos en ciberseguridad, escalados por la creciente interconexión y la movilidad. Ante este escenario, empresas y proveedores de TI, buscan una protección que se adecue a sus necesidades para asegurar la continuidad de servicios críticos y la integridad de sistemas y redes. Aunque las empresas han dado una gran importancia a su estrategia de ciberseguridad, su implementación adolece a menudo de proactividad ante amenazas emergentes, con errores frecuentes en formación de personal, sistemas de seguridad obsoletos y gestión deficiente de accesos.

Desde Samsung, ofrecemos soluciones para empresas como Knox Matrix, una solución de seguridad TI centralizada que facilitan la protección sin comprometer la conectividad. Cada empresa debe buscar las soluciones de seguridad que se adecuen a sus necesidades específicas, buscando la eficiencia sin sacrificar la productividad.

INTEGRACIÓN HOLÍSTICA

La integración de soluciones de seguridad debe ser holística, permitiendo una gestión centralizada y respuestas rápidas a incidentes. Knox Matrix, el ejemplo que hemos mencionado, mejora la seguridad mediante un sistema privado de cadena de bloques que autentica dispositivos de manera segura y conveniente. En cuanto a la protección en entornos cloud, es imperativo adoptar controles de acceso, cifrado y monitoreos especializados, dados sus retos únicos.

Frente a la amenaza del ransomware, es crucial educar a la fuerza de trabajo, promover las copias periódicas de seguridad, mantenimiento del software mediante actualizaciones y responder de forma ágil a los incidentes. La gestión de dispositivos móviles y arquitecturas SASE son herramientas recomendadas para equilibrar productividad y seguridad en dispositivos en línea.

La formación en ciberseguridad debe ser un pilar fundamental en la estrategia de ciberseguridad de las empresas, aunque las empresas suelen ser bastante laxas ante la formación de empleados. La inteligencia artificial y el aprendizaje automático pueden ser de gran ayuda, analizando datos para identificar patrones de comportamiento y anticipándose a cualquier vulnerabilidad.

La escasez de profesionales especializados es un problema al que se enfrenta el sector. Por lo que Samsung está promoviendo la formación de profesionales en esta rama del sector, el mejor ejemplo de ello es la colaboración con la Universidad de Málaga para proporcionar formación especializada y gratuita a futuros especialistas en ciberseguridad, respondiendo a las necesidades del sector, y mejorando la empleabilidad y posibilidades de futuro de los jóvenes españoles.

SASE para afrontar los desafíos de ciberseguridad

SASE está ocupando un lugar destacado en las estrategias de los departamentos de ciberseguridad. Para hablar sobre su influencia, Byte TI, junto con Palo Alto Netwroks, Barracuda y HPE Aruba, organizó un encuentro que contó con la participación de Ángel José Báscones, CIO de Ontier; Gabriel Cuesta, CTO de Habitissimo; Estefanía Rodríguez, SASE Sales Specialist de Palo Alto Networks; Alejandro Las Heras, CISO de Grupo Eulen; Manuel Asenjo, Director IT y Ciberseguridad de Broseta; Javier Torres, CISO de Allfunds; Miguel López, Country Manager de Barracuda; Maica Aguilar, Gerente de Seguridad de Ferrovial y Carlos Piñera, SASE Business Development Manager de HPE Aruba

El encuentro arrancó con el análisis de cuáles son los principales retos con los que se encuentran los responsables de ciberseguridad. Para Manuel Asenjo, Director IT y Ciberseguridad de Broseta, "el mayor desafío es que los datos de los clientes no salgan de donde tienen que salir. Por eso, hemos hecho mucho hincapié en proteger los entornos cloud, restricción de seguridad en llaves USB de almacenamiento... Estamos empezando a aprobar llaves de Ubico y nos está dando buen resultados".

Según Alejandro Las Heras, CISO de Grupo Eulen, "en nuestro caso,tenemos una parte más de TI y otra más de informática de las operaciones. En la ciberseguridad estamos centrados en que la parte

de operaciones esté en el mismo lugar que ciberseguridad de TI. Luego está la parte de la normativa que no es la misma en todos los países, así que tenemos que tener una misma linea común a todos los países y luego hacer una transposición a las características de cada paísEstamos replicado el mismo modelo de identidades, de protección de información o de ransomware que hace unos años, simplemente estamos ampliando la superficie de defensa".

Por su parte, Estefanía Rodríguez, SASE Sales Specialist de Palo Alto Networks explicó cómo está ayudando su compañía en la estrategia de ciberseguridad de las organizaciones: "Queremos cubrir los desafíos que tienen las empresas. Queremos que puedan adoptar una estrategia completa más allá de SASE. Creemos que uno de los objetivos y uno de los principales retos que tienen las empresas es el de reducir la complejidad para combatir las amenazas".

Para Ángel José Báscones, CIO de Ontier, "hay un hecho diferencial que es la seguridad de la información. Una fuga de información significa una fuga reputacional muy importante. En Ontier estamos formando a los usuarios porque los ataques dirigidos son muy frecuentes y también es muy importante el apartado del ransomware. Por esos queremos llegar a un modelo zero-trust total donde no haya ninguna fuga de información".

Carlos Piñera, SASE Business Development Manager de HPE Aruba, consideró que "muchos de los retos que vemos pasan por la securización de la información y por concienciar a las personas ya que es el elemento en el que más inciden los hackers. En todas las nuevas arquitecturas la flexibilidad es muy importante, pero nosotros incidimos en que también es importante la experiencia de usuario. Nosotros queremos simplificar porque creemos que el futuro pasa por una experiencia de usuario, buena, rápida y que a su vez garantice las medias defensivas".

Para Maica Aguilar, Gerente de Seguridad de Ferrovial, "los desafíos pasan por mantener el nivel de seguridad adecuado para reducir las amenazas a las que te ves expuesto y que son cada vez más sofisticadas por lo que tienes que estar actualizando de forma constante para adaptarte a los nuevos ataques. Es esencial no quedarse obsoleto".

Pero ante la amalgama de soluciones que se pueden encontrar en el mercado, la gestión se hace muy compleja. Por eso, Miguel López, Country Manager de Barracuda, cree que la simplicidad es fundamental. "En nuestro caso, tratamos de ofrecer una plataforma de seguridad con la mayor cobertura posible. Lo que nos diferencia es el concepto de simplificación. Se trata de que la seguridad sea asequible y manejable, que se pueda implementar desde una herramienta SASE a otra de concienciación y formación de usuarios. Un concepto que llevamos trabajando desde el principio es que hemos tratado de ser Cloud First porque hay que tratar la protección de cloud de la misma forma en que se trata la seguridad de los entornos onpremise".

Finalmente, Javier Torres, CISO de Allfunds, afirmó que "en nuestro negocio nos preocupa proteger los datos del cliente y ser los suficientemente resilientes para continuar con la operativa. Así que es la protección del dato y la continuidad del negocio lo más importante porque que no haya esa continuidad impacta en el 30% de nuestros clientes a nivel mundial. Zero-Trust es nuestro primer caballo de batalla por eso apostamos por incorporar herramientas SASE, de IAM, gestión de accesos de manera remota y sobre todo simplificar los accesos sin perder esa seguridad. Como entidad finan-

ciera es importante la resiliencia".

LA IMPORTANCIA DE SASE

La implementación de SASE es fundamental en la actualidad ya que al acceder los usuarios desde diferentes entornos a los datos de una compañía se ha ampliado el perímetro tradicional. La gran ventaja es que un modelo SASE elimina los dispositivos basados en el perímetro y las soluciones heredadas. Por eso las empresas están apostando de forma fuerte por su implementación. Tal y como aseguró Javier Torres, "hay dos puntos clave que nos lleva a desarrollar SASE. Uno es mejorar la flexibilidad y la resiliencia, El otro elemento es que simplifica muchísimo el control de los accesos una vez que lo has implementado de forma correcta".

Pero, ¿qué es lo que influye a la hora de elegir una solución u otra? Para Gabriel Cuesta, CTO de Habitissimo, "es fundamental que sea una solución robusta y que esté probada en el mercado. Nosotros tenemos presencia en cinco países y necesitamos un sistema de acceso que nos permita que los usuarios puedan acceder de forma sencilla y segura. Además, hay un factor que son las quejas de los usuarios que ven que cuando una solución de seguridad les penaliza su operativa, se convierten en hackers internos. Así que lo que queremos es evitar las fricciones con estos usuarios para que no vean la seguridad como un elemento que les impide realizar de forma correcta su trabajo".

Para Maica Aguilar no hay más remedio que implementar SASE ya que "muchas de las aplicaciones están en la nube y se necesita llevar la seguridad a ese punto por lo que es obligatorio proteger los accesos y los perfiles de acceso que hay que dar a los usuarios. Ese es el motivo por el que creemos que hay que adoptar SASE".

COMO SE INTEGRAN EN LA ESTRATEGIA DE CIBERSEGURIDAD

La implementación de SASE no es algo que sea sencillo. Es necesario que se integre en la estrategia de ciberseguridad de la empresa. Por eso, cuanto más simple sea, más sencilla será su implementación. Para Miguel López de Barracuda, "la simplicidad es el factor fundamental. Si una solución no es simple, muchos usuarios no van a saber utilizarla. Además, la implementación debe realizarse de manera gradual dentro de las soluciones que tiene el cliente. Y, finalmente, es importante que la solución pueda aplicarse de la forma en la que el cliente necesita. Unos clientes tienen todo en cloud otros solo una parte, así que implementar SASE tiene que adaptarse a esas características de cada cliente".

Por su parte, el portavoz de HPE Aruba cree que "es muy importante saber que con la parte de firewalls no es suficiente para afrontar una amenaza. Zero-Trust garantiza la uniformidad de la información así que tener una estrategia Zero-Trust completa te permite avanzar en un proyecto por fases, de tal forma que ese proyecto se construye capa a capa. No puedes quietar todo lo que tienes para implementar SASE porque, además, SASE encaja muy bien en esa estrategia Zero-Trust por capas".

Finalmente, Estefanía Rodríguez afirmó que "la responsabilidad más importante para Palo Alto Networks es la de proteger los datos de los clientes. Lo que tenemos que asegurarnos es que el dato lo protegemos según las normativas. La plataforma SASE de Palo Alto ha alcanzado la máxima certificación. Además es importante proteger el dato durante todo el ciclo de vida, desde su creación".

BYTIC MEDIA

adjudicaciones y licitaciones TIC | byte powered by TI

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 presentacion + 4 meses de Innovacion con ITDM's al año
- **Barómetro del talento digital**
  Entrevistas + Informe + Evento presentacion + 4 meses de Innovacion 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**

Qué hacer con el legacy

Uno de los principales retos que tienen por delante los departamentos de TI de las organizaciones son los sistemas heredados. Para tratar cómo se abordan los problemas relacionados con el legacy, Byte TI organizó un encuentro, patrocinado por Incentro y que contó con la participación de Jesús Gómez, director de sistemas de información de atl Capital; Miguel Cortés, CIO en Incentro; Gustavo Martínez, CIO de Zermatt; Conchi García, director Sistemas de Información de Madrid Digital; Alejandro Expósito, Digital, Innovation & Transformation Merck; Juan Luis Vicente Carro, Jefe de departamento de gestión TIC y normativa de la Policía Municipal de Madrid; Ildefonso Vera, director de innovación y transformación digital de Isdefe; Naidalyd Varela, IDT Manager de BAT; Luis Alberto López, responsable de TI Ayto. Hoyo de Manzanares y Manuel Tarrasa, CIO de Prosegur. **Por Manuel Navarro**

El legacy supone uno de los retos más importantes de los departamentos TIC de las empresas, pero para buena parte de los asistentes, antes de abordar cuál es la gestión que se debe llevar a cabo, parte de los asistentes analizaron cuál es el papel que tiene que jugar un CIO en la estrategia de la empresa. En este sentido, Jesús Gómez, director de sistemas de información de atl Capital, señaló que "el rol del CIO tiene que cambiar porque en la actualidad su papel debe ser el de director de Innovación de la compañía. Por eso es altamente recomendable su presencia en el consejo de dirección de la empresa porque es quién puede ayudar a convencer

al resto del comité de la necesidad de emprender un camino que además es inevitable y que pasa por la innovación y la digitalización. Actualmente el CIO debe jugar uno de los papeles más importantes de la compañía como encargado de liderar la gestión del cambio y concienciar al resto en la importancia de evolucionar a las nuevas tecnologías".

Naidalyd Varela, IDT Manager de BAT, aseguró que "el papel de un CIO ha de estar ligado con la estrategia de TI y la estrategia del cliente interno y externo. El CIO actual tiene la visión de tener la arquitectura empresarial en mente y añadir ahí el modelo de TI. Es decir, un CIO está capacitado para cambiar la arquitectura de TI porque conoce la arquitectura de la empresa. Su objetivo principal debe ser el de alinear tecnología con el negocio".

RETOS DE TRABAJAR CON LOS SISTEMAS LEGACY

Trabajar con sistemas heredados supone una serie de desafíos que los responsables de TI deben abordar. Para buena parte de los asistentes, la ciberseguridad es uno de los más acuciantes. Así por ejemplo, Gustavo Martínez, CIO de Zermatt, afirmó que "la ciberseguridad es importante. El principal problema al que nos enfrentamos con el legacy es que esa ciberseguridad la tenemos que administrar con sistemas obsoletos. Por eso, tenemos la obligación de establecer mecanismos para mantener esos sistemas aislados para mantener la seguridad de toda la compañía".

Es esa antigüedad de muchos equipos lo que entorpece la acción del día a día de un CIO. Conchi García, directora de Sistemas de Información de Madrid Digital puso como ejemplo el de una administración como la Comunidad de Madrid: "Los sistemas de la Comunidad de Madrid llevan instalados desde hace 30 años, así que el primer problema es la obsolescencia, que puede afectar a datos sensibles de los ciudadanos. Otro gran riesgo es que no es fácil modificar los sistemas legacy y esa dificultad hace que no nos podamos subir al carro de las innovaciones de la digitalización. Y además de todo ello, tenemos que ser conscientes de que si decidimos cambiar hay que hacerlo de forma correcta y formar a los empleados para que cambien la forma de trabajar. Unido a esto tenemos una lucha muy importante por el talento en las nuevas tecnologías, que todavía se acrecienta más cuando hablamos de herramientas o equipos más antiguos".

Alejandro Expósito, Digital, Innovation & Transformation Merck, incidió en esa dificultad de encontrar perfiles especializados que trabajen con tecnologías antiguas: "lo de la parte del talento es totalmente cierta. Si ya es difícil encontrar perfiles adecuados para tecnologías actuales, lo es mucho más para aquellas que ya tienen muchos años. En nuestro caso tenemos sistemas legacy porque hay procesos industriales donde la planificación es tan compleja que una vez que se realiza es muy complicada de cambiar porque volver a cambiar el procesos te puede llevar dos o tres años. Un caso claro es el uso de Windows 95 que se sigue usando. En casos como éste, el CIO debe valorar los riesgos que corre y cómo puede ser capaz de ir cambiando paso a paso."

Para Ildefonso Vera, director de innovación y transformación digital de Isdefe, "la empresa que no innove no va a ser competitiva. Para nosotros el legacy nos viene por dos bandas. Por un lado, las personas que trabajan en programas, nos preocupan menos, pero es cierto que internamente tenemos determinados problemas. Nosotros buscamos cuál era la funcionalidad que nos demandaba nuestro cliente interno y luego está el tema de la seguridad. Nosotros hemos barajado esos dos elementos y vimos que el gran desafío está en las personas. Por ejemplo, nos costó mucho la migración a la nube del correo electrónico. Nosotros analizamos todas las aplicaciones y al final lo que hacemos ahora es buscar una plataforma de low-code para disminuir las dificultades que tenga el cliente".

Naidalyd Varela añadió que efectivamente convencer a las personas es un reto añadido: "Si tu estás migrando a nuevas tecnologías y tienes expertos en tecnologías antiguas, una de las cosas más difíciles es convencer a esas personas de que es mejor, y que ellos no van a perder su trabajo por eso. Esa es una de las mayores dificultades ya que muchos empleados se niegan a implementar nuevas soluciones o a cambiar los procesos porque creen que eso va a acabar con su puesto de trabajo".

La solución para Manuel Tarrasa, CIO de Prosegur, pasa por motivar a las personas para que acepten los cambios. En este sentido incidió en que "nos faltan mimbres porque, al final, es un problema de motivación de las personas. Creo que lo que mejor funciona para que se adopten determinados cambios es la aparición de una crisis porque en ese escenario todo el mundo se alinea y trabaja de forma conjunta. Esto es algo que vimos todas las empresas con la irrupción de la pandemia. Pero no puedes estar a expensas de que se produzcan crisis de forma constante. La pregunta es, ¿por qué en una crisis las personas aceptan los cambios y cuando no existe esa crisis no los aceptan? Esto es lo que me lleva a pensar en que no motivamos de

forma suficiente y adecuada a las personas".

Para Luis Alberto López, responsable de TI del Ayuntamiento de Hoyo de Manzanares, "la motivación surge de dentro hacia afuera. La cuestión es que tú puedes poner todos los elementos necesarios para motivar, pero si esa fuerza no surge de las personas, no sirve para nada. Hay que motivar a la gente en función de lo que le motiva: no solo se trata de dar incentivos económicos, porque hay gente que necesita sentirse valorada más allá de ello. Hay que favorecer el trabajo en equipo".

BENEFICIOS DE MANTENER EL LEGACY

Por qué a día de hoy se sigue apostando por mantener esos sistemas heredados. Hay diferentes factores, pero en general el aspecto económico y el de la dificultad de cambiar los procesos son los dos más importantes. Así, Juan Luis Vicente Carro, Jefe de departamento de gestión TIC y normativa de la Policía Municipal de Madrid aseguró que "nuestra única motivación para mantenerlos es la falta de presupuesto. Carecemos de medios técnicos y materiales. Nosotros tenemos un entorno muy lento y es muy difícil para los trabajadores cambiar porque el empleado se encuentra cómodo. A futuro, cuando cambiemos, daremos a los empleados que no quieran cambian funciones mas rutinarias. Ahora mismo tenemos que aislar los sistemas para proteger algo que muy pocas personas saben cómo funciona".

Para Manuel Tarrasa, "el problema es que cuando tienes un sistema que es tan grande que lleva operando 20 años, significa una operativa y unos costes tan grandes que es imposible ejecutar, por lo que la única solución es aislarla. Yo lo llamo efecto Chernóbil".

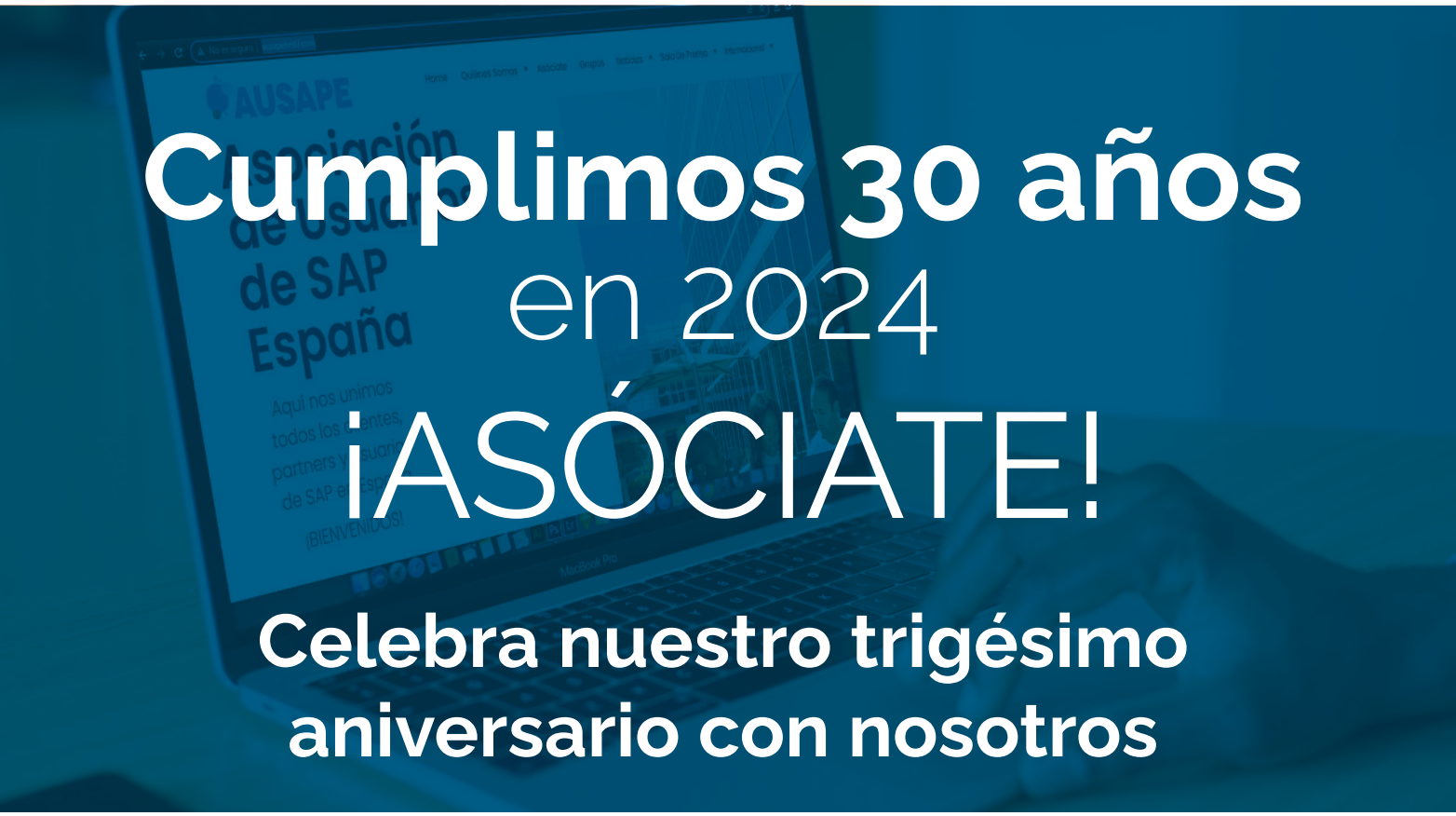
Gustavo Martínez, CIO de Zermatt, considera que el cambio tiene que involucrar a toda la organización. En su opinión, "la innovación tiene que ser 50% negocio y 50% tecnología, En nuestro caso tenemos que cambiar los procesos de las aplicaciones de servicio y la de la maquinaria. En las primeras es más complejo. Las compañías están en constante evolución y es obligatorio cambiar algo. Hay que diferenciar lo que se puede y no se puede cambiar. Para ello hay que buscar las maneras a través de soluciones virtualizadas o reinventar un poco el servicio. También hay ocasiones en que vemos que si eliminamos una aplicación, el negocio funciona igual, por lo que descubrimos que no era tan necesaria".

Para Jesús Gómez de atl Capital, "en nuestro caso es el cliente el que nos dicta cuáles son las tecnologías que tenemos que implementar, como ejemplo la omnicanalidad. Lo cierto es que la nube es esencial en la migración del legacy. Es más operativa y funcional porque permite conectar de forma ágil todos los sistemas."

Naidalyd Varela, sin embargo no apuesta por una tecnología u otra, sino que prefiere un término medio. En este sentido, la CIO de BAT señala que "si un responsable TIC ha decidido que es mejor quedarse con el legacy es porque considera que todavía le proporciona la agilidad suficiente a la compañía. El tema es descubrir cuándo es el momento para cambiar el legacy y no sólo cambiarlo por cambiarl"o.

Miguel Cortés, CIO en Incentro cree que en el proceso de cambiar el legacy "es importante la parte de construir aplicaciones más a medida, pensando más en una arquitectura de microservicios. En este sentido ayuda mucho a mover el legacy porque el 80% de las infraestructuras están preparadas para ello. Esto además te ayuda a reducir los costes, El low-code también ayuda a desarrolla aplicaciones más rápido aunque es cierto que se necesita un desarrollo formativo. Para mí un elemento clave es tener un arquitecto en condiciones que sea capaz de diseccionar todo el mapa de IT para que ayude a canalizar todo el procesos de modernización".

AUSAPE



Cumplimos 30 años en 2024

¡ASÓCIATE!

Celebra nuestro trigésimo aniversario con nosotros

30 Aniversario 2024 AUSAPE

- Grupos de Trabajo
- Sesiones temáticas/magistrales
- Acceso al Portal de empleabilidad
- Acuerdos formación
- Delegaciones AUSAPE
- Fórum
- SAP Delegation Days
- Colaboración internacional

Visita nuestra web: **www.ausape.com**

Los últimos programas ERP

Uno de los programas más importantes que existen para las compañías son las herramientas de planificación de recursos empresariales. Conocidas como ERPs, mejoran los niveles de productividad y competitividad de las organizaciones con la ventaja añadida que poseen un alto grado de flexibilidad y personalización al estar compuestas por diferentes módulos: esto facilita que las compañías escojan los que consideren necesarios en cada momento.A continuación, proponemos una radiografía acerca de lo que ofrecen estos programas en la actualidad. Hemos reunido 11 firmas. El primero es Aqua eBS que destaca por su alta capacidad de personalización, eficacia en la automatización e integración con aplicaciones externas. Le siguen Cegid Ekon, un ERP con importantes beneficios a nivel operativo y estratégico, y Exact Globe+, un ERP transaccional que cubre más de 30 legislaciones y está disponible en 40 idiomas. Por su parte, IFS Cloud no solo ofrece soluciones para la planificación de recursos empresariales, sino gestión de activos y servicios. Por su parte, Lantek Integra es un ERP distinto al resto porque se dirige específicamente a la industria del metal. Microsoft Dynamics 365 destaca por introducir la solución Dynamics 365 Copilot basada en inteligencia artificial generativa.

También participa Oracle con Fusion Cloud ERP que incluye planificación y aprovisionamiento, finanzas, informes, planificación de proyectos, obligaciones fiscales, ciclo de vida del producto, gestión de riesgos…; a nivel de seguridad promete un marco de aislamiento de datos encriptado. Se ha incluido, asimismo, Sage 200 Advanced: para
empresas de entre 20 y 200 empleados se integra con Microsoft 365 (Word, Excel y Outlook).

Mientras SAP S/4HANA Cloud provee de capacidades de inteligencia artificial como IA conversacional, machine learning y analíticas en tiempo real. En el caso de Solmicro ERP, una de sus características más destacadas es su nueva interfaz que ahora tiene un diseño más visual y una usabilidad mejorada. Finalmente, Wolters Kluwer a3innuva l ERP es una solución de facturación y contabilidad online.

Aqua eBS

Además de cubrir todas las áreas de negocio, ofrece soluciones específicas para distintas industrias adaptándose a cada sector para mejorar su eficacia.

Con una alta capacidad de personalización, eficacia en la automatización e integración con aplicaciones externas, gracias a su tecnología iRPA. este software dispone de una destacada adaptabilidad para integrar datos y procesos, y asegurar la interoperabilidad. Es aquí donde radica su verdadera innovación y por lo que emplea la citada tecnología para precisamente automatizar procesos e integrar y sincronizar de manera fácil con cualquier aplicación, sitio web o sistema externo. Este enfoque de gestión de procesos basado en bots no solo acelera la eficiencia operativa, sino que reduce los errores humanos para así incrementar la productividad del negocio. Además, su fácil integración con software externo permite llevar la automatización un paso más allá, extendiéndose a todas las áreas del negocio. La tecnología iRPA reduce, por otro lado, errores y maximiza la productividad.

Entrando en detalle, su arquitectura se asienta sobre una plataforma flexible que se adapta a las necesidades específicas de cada compañía, permitiendo innovar y crecer de forma inteligente y sostenida; siempre acorde a sus necesidades.

Aqua eBS es un ERP completo y global que cubre todas las áreas de negocio, desde finanzas y cadena de suministro hasta la gestión de clientes, almacén, producción y servicios proporcionando, de este modo, una visión integrada y coherente de todas sus áreas. Asimismo, la herramienta provee de soluciones específicas para distintas industrias, adaptándose a cada sector de actividad según lo que necesite y precise. Pero no es el único beneficio, dado que también ayuda a que las organizaciones tomen mejores decisiones y eviten costes en desarrollos a medida.

Respecto a su funcionamiento, ofrece información automatizada en tiempo real, así como avanzadas capacidades analíticas, presentando informes y cuadros de mando que ayudan a que las decisiones tomadas resulten precisas y estratégicas. También que se sostengan en la información que brinda el propio ERP. Mientras, con el respaldo de distintas tecnologías y una actualización constante de la plataforma a través de nuevas versiones, Aqua eBS ayuda a las compañías para que se adapten a los continuos cambios que se producen en materia de reglamento y normativa como la Ley Antifraude, TicketBAI, nuevos tipos de IVA, el Suministro de Información Inmediata o SII…

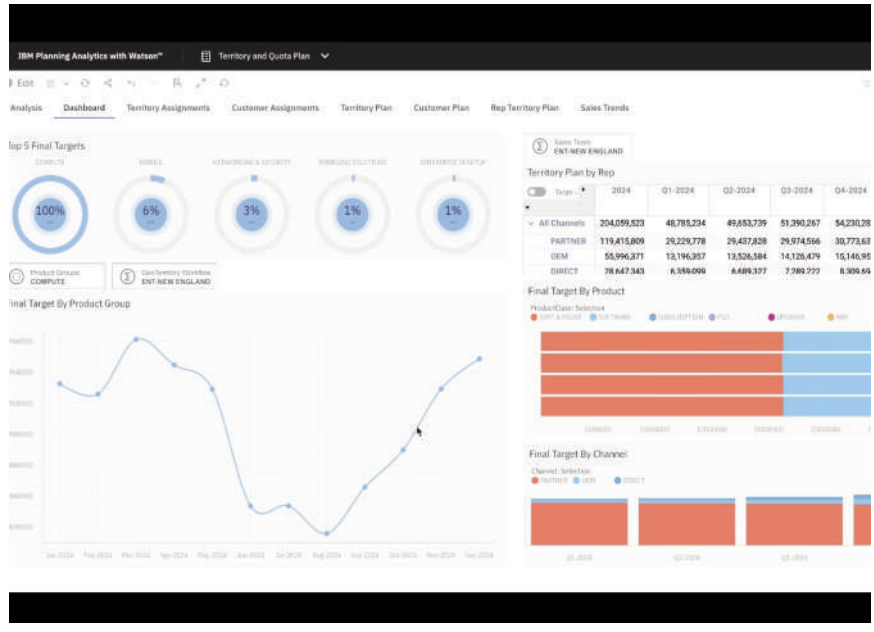
Las compañías interesadas en Aqua eBS tienen a su disposición un modelo cloud y otro local. Proporciona también de forma integrada avanzados sistemas de gestión de almacén (SGA), recursos humanos, gestión de proyectos y operaciones, plataformas ecommerce y apps, entre otros.

Aqua eSolutions

Tel: 917 334 200
Web:
www.aquaesolutions.com
Precio: consultar

Cegid Ekon Cloud

Es un software de gestión empresarial para empresas de sectores específicos, así como pymes que buscan una solución estándar para una gestión integral de su organización.



Además de contar con soluciones verticalizadas y personalizadas para el sector salud, construcción, logística y distribución, industria y asesorías, Cegid Ekon Cloud ofrece soluciones departamentales para la gestión de áreas funcionales donde incluyen finanzas, recursos humanos, gestión de proyectos, Business Intelligence o CRM. Así, en función de las necesidades de cada compañía, cubre diferentes procesos de negocio, tanto de forma transversal como por departamentos o áreas concretas. Por ejemplo, Cegid Ekon Despachos Profesionales tienen presencia en el sector de Despachos Profesionales, Asesorías Fiscales, Laborales y Consultoras, manteniendo siempre las características propias de la actividad, siempre actualizado a la legislación vigente y con capacidades de gestión contable, fiscal, laboral y de facturación. Por su parte, Cegid Sigrid ERP es un software para constructoras que permite conocer el progreso de las obras, el cumplimiento de las previsiones, los ingresos esperados o el estado de recursos, entre otros.

El ERP, que brinda la posibilidad de que la herramienta se despliegue en la nube (ya sea pública o privada). Incluye además de la gestión del ERP, las infraestructuras y la seguridad. Además, se ha adaptado a diferentes idiomas y a legislaciones de los países con los que de manera más habitual interactúan las empresas españolas, contribuyendo así a la internacionalización de tu negocio. Sus beneficios se engloban en tres grandes apartados: estratégico, operativo y económico.

A nivel estratégico, Cegid Ekon Cloud promete un aumento de la eficacia, agilidad y productividad de las compañías aplicando una mejora en las labores de gestión y obteniendo una colaboración fluida y digital entre todas las áreas de la compañía. La integración de la gestión del negocio en una única plataforma conlleva, por otro lado, una mejora en la calidad del servicio proporcionado a los clientes.

Los beneficios a nivel operativo incluyen, entre otros, la automatización y la digitalización de los procesos para un flujo de la cadena de valor más ágil y eficiente. También la posibilidad de identificar cuellos de botella y riesgos operativos en la cadena de valor, y medir y ajustar los procesos departamentales e interdepartamentales de manera sencilla. Además, los trabajadores pueden adaptar de forma inmediata los flujos de trabajo, según necesidades; disponer de indicadores por departamentos, áreas, secciones, etcétera; y mejorar la seguridad de los datos de la organización.

A nivel económico, Cegid Ekon Cloud permite reducir costes operativos y de gestión en múltiples áreas, minimizar costes de gestión de la información y obtener un mayor control de los márgenes.

Cegid Ekon

Tel: 637 477 260
Web:
www.ekon.es
Precio: A consultar

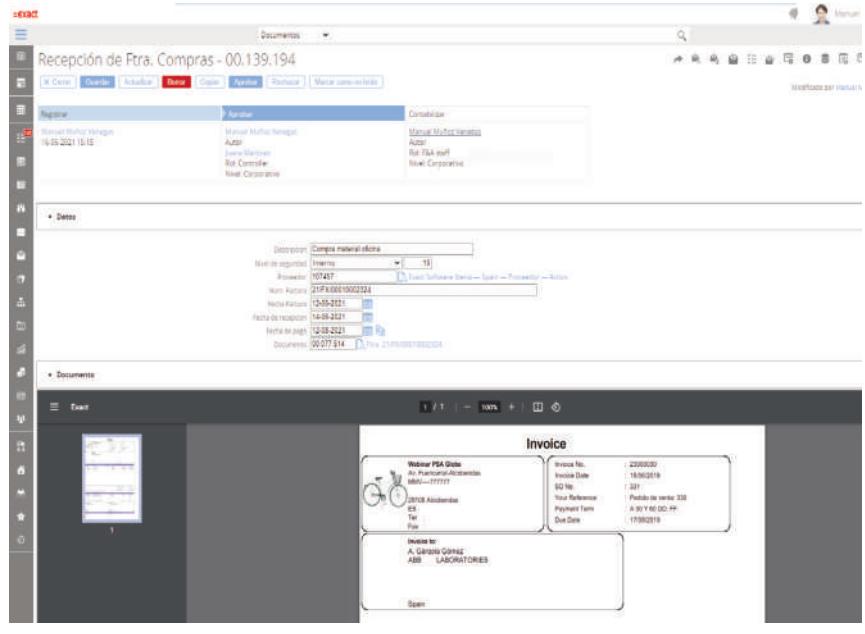
Exact Globe+

La solución puede implementarse tanto en la nube (pública o privada) como a nivel local. Cubre más de 30 legislaciones y está disponible en 40 idiomas.

Globe+ es un ERP transaccional que proporciona una variada gama de funcionalidades para el área financiera y que, además, permite gestionar otros procesos de negocio como el área comercial, la gestión de proyectos, recursos humanos, producción o la gestión del almacén.

Entrando en detalle, gestiona tanto la contabilidad, como facturación, gestión de riesgos, consolidación, planificación financiera, reporting y facturación electrónica para disponer de una visión completa y en tiempo real de las finanzas de la empresa. Por su parte, con el módulo de previsión y presupuestación es posible tomar decisiones más informadas gracias a sus funcionalidades de previsión, presupuestación, análisis e informes que ayudan a planificar y anticipar los recursos financieros necesarios.

En lo referente a la centralización de procesos, desde compras hasta entregas, producción, gestión financiera, recursos humanos … Exact Globe+ gestiona todos los procesos desde un sistema central para tener los datos correctos en el momento adecuado para tomar decisiones informadas. La funcionalidad de gestión documental se complementa con los flujos de trabajo o workflows. En este caso, la herramienta posibilita trabajar con todo tipo de documentos, ya sean facturas, documentos de proyectos o de cualquier otra área. A su vez, el sistema incluye las funcionalidades de control de versiones, función de búsqueda, metadatación de los documentos, OCR.... Además, se integra plenamente con Microsoft Office.



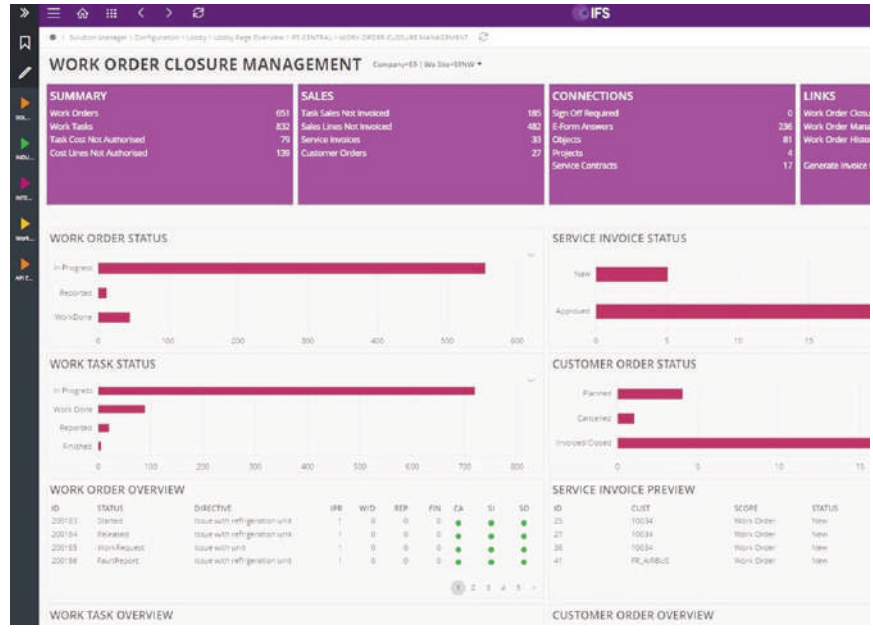
Como solución multi-idioma y multi-legislación, es compatible con múltiples divisas y numerosos formatos bancarios internacionales. De hecho, cubre más de 30 legislaciones y está disponible en 40 idiomas por lo que todos los empleados hacen uso de la misma información en el mismo sistema, pero desde cualquier ubicación. Otra de las características que la define es que se integra con otros sistemas, proporcionando una fuente central de información que aumentan la eficiencia del negocio. Además, Exact RPA (es decir, la automatización robótica de procesos) facilita la automatización de cualquier proceso dentro del propio ERP y también la interacción con otras aplicaciones o softwares del mercado. Exact Globe+ promete una sencilla implementación y la elaboración de informes y análisis sencillos que facilitan el acceso a los datos de los procesos de negocio de la empresa, comparando valores y realizando diferentes pronósticos. A nivel de seguridad y autorización, el sistema brinda amplias posibilidades de funciones y derechos, lo que garantiza una seguridad total. Permite, igualmente, la trazabilidad de todas las acciones.

Exact

Teléfono:
91 230 9632
Web: www.exact.es
Precio: A consultar

IFS Cloud

Facilita que los diferentes módulos de la empresa compartan información, ayudando a potenciar estrategias de transformación digital relacionadas, por ejemplo, con IoT e IA.



Una solución que está integrada de forma nativa y diseñada en su núcleo para interoperar de manera eficiente y, en última instancia, impulsar la innovación. Esta es la carta de presentación de IFS Cloud que abarca todo un conjunto de capacidades que van desde la planificación de recursos empresariales hasta la gestión de servicios de campo y de activos. Así. el hecho de ofrecer todo esto en un único producto -respaldado por una plataforma subyacente central- no solo facilita a los negocios administrar sus flujos de trabajo de manera más sencilla. Se eliminan los silos de datos y es posible obtener una visión completa de la organización que tiene la libertad de seleccionar qué módulos de la solución desea agregar. Mientras, las API abiertas facilitan la integración con cualquier solución existente y ayudan a que las compañías se conecten a otras tecnologías y procesos inteligentes, sin importar quién los haya creado.

Con modelos operativos en la nube o en las instalaciones del cliente, IFS Cloud facilita que los diferentes módulos de la empresa compartan información, ayudando a potenciar las estrategias de transformación digital al permitirles adoptar fácilmente gemelos digitales o implementar estrategias de IoT o inteligencia artificial que brinden resultados medibles. Y es que la herramienta es capaz de mostrar los beneficios reales y medibles de tecnologías como las anteriormente citadas junto a la realidad aumentada y mixta. Estos servicios de aplicaciones se han diseñado para integrarse entre sí y es posible usarlos de manera flexible e implementar de inmediato para permitir que los clientes obtengan valor más rápido. La firma consultó, por otro lado, a sus usuarios y esto dio lugar a que IFS creara una rica funcionalidad vertical en sus conjuntos de soluciones, así como capacidades horizontales en adquisiciones, recursos humanos, finanzas y cadena de suministro. En concreto, ha integrado paneles específicos para las industrias de aeronáutica y defensa, construcción, energía, utilities, telco y fabricación asegurándose que el producto se adapta perfectamente a las necesidades de cada sector. Se ha asegurado asimismo que cualquier nueva funcionalidad se entregue de forma permanente, lo que significa que las actualizaciones se depositan con una cadencia predecible y regular dos veces al año: de esta manera, los usuarios saben exactamente qué se actualiza y cuándo. Los clientes pueden optar a los siguientes modelos de implementación: nube, en remoto donde IFS proporciona un software preempaquetado de IFS Cloud que opera en una plataforma de software soportada, o en sus instalaciones autogestionado.

IFS

Tel: 91 8062345
Web:
www.ifs.com/es/
Precio: A consultar

Lantek Integra

Un software para las empresas de la industria del metal que gestiona todo el proceso de fabricación, ventas, compras y almacén de este mercado.

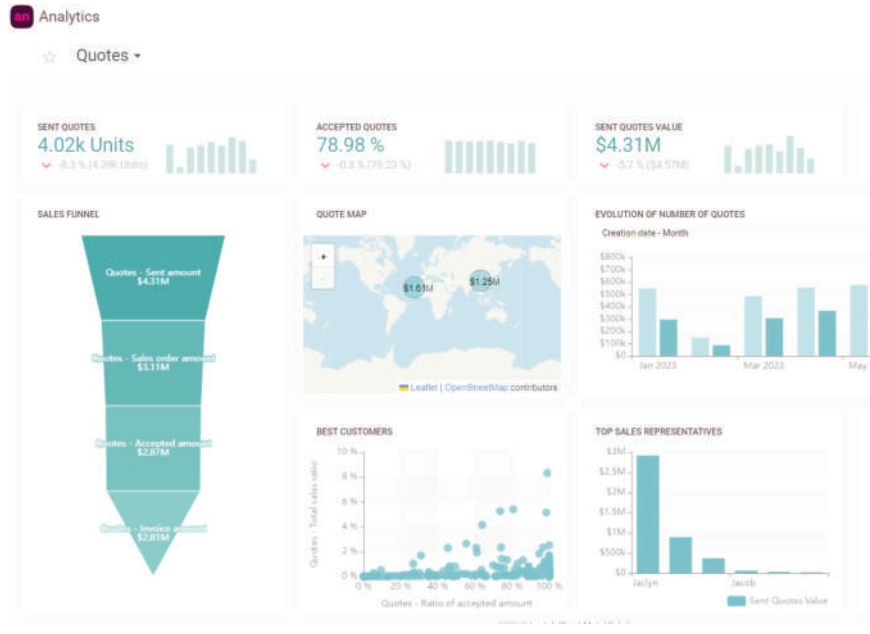
Lantek es una compañía dedicada al sector de corte y procesado de la chapa y el metal que el pasado mes de octubre presentó las novedades y avances incorporados a la última versión de su software, la v43. En total son más de 80 mejoras las que se han añadido: con ellas, lo que busca, entre otros, es dotar a sus productos de una mayor eficiencia además de seguridad y una digitalización en los procesos de fabricación. Uno de estos productos es Integra, su conocida plataforma software para la gestión avanzada de la fabricación en empresas que producen piezas en chapa, tubos y perfiles metálicos.

Ahora, con las nuevas características agregadas al programa, Lantek Integra no solo permite una planificación de la producción ágil y flexible, optimizando tanto el inventario como el uso eficiente de los recursos. Mantiene en todo momento una trazabilidad completa, lo que habilita un preciso control de los costes totales. Además, sus nuevas funcionalidades, orientadas a la gestión de la fabricación coordinada con el control de existencias, apoyan un proceso de producción más eficiente y con mayor capacidad de respuesta, ayudando así a las empresas a satisfacer las demandas de los clientes de una forma más precisa.

La introducción de la gestión de almacenes intermedios en el proceso de producción mejora, en otro orden de cosas, la visibilidad y la trazabilidad de la fabricación en curso, así como su valoración de costes. También optimiza el flujo de trabajo de los operarios en el taller mediante una localización precisa de las piezas que deben ser procesadas en cada centro de trabajo.

Esta versión incluye de igual forma una opción para reasignar la máquina de los anidados en producción, aplicando de forma automática cambios de tecnología, mecanizado y generación de CNC necesarios. De este modo, los usuarios experimentarán una aceleración significativa en la programación de la producción y balanceo de la carga de trabajo entre máquinas, respondiendo de manera más efectiva a cualquier evento que suceda en el taller.

Lantek Integra dispone, entre otros, de un módulo de presupuestación y CRM (Quotes) que ayuda a optimizar la relación con clientes actuales y potenciales; otro de ventas, pedidos, albaranes y facturas (Sales) que facilita los procesos administrativos; y compras: proveedores y gestión del stock (Purchases) que resuelve las necesidades de gestión asociadas al proceso de compras de la compañía.



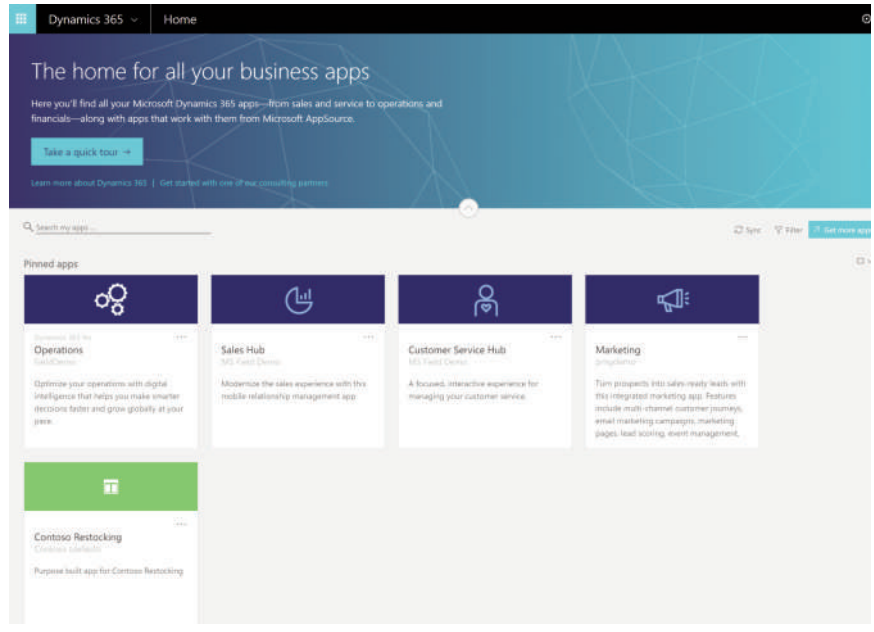
Lantek

Tel: 945 77 17 00
Web:
www.lantek.es
Precio: consultar

Microsoft Dynamics 365

Basado en IA, añade valor a las capas de análisis de datos, automatizando tareas específicas y mejorando el proceso general de apoyo a la decisión.

Dynamics 365 es una plataforma cloud basada en inteligencia artificial que elimina los silos tradicionales existentes entre el ERP y el CRM, desglosándose en múltiples aplicaciones de negocio que permiten conectar los procesos de producción, la atención y servicio al cliente, los de servicios de campo y la gestión del talento de la organización. Todo ello con la ventaja de su plena integración con las herramientas de productividad que los empleados ya están acostumbrados a usar.



En concreto dispone de seis soluciones principales. Dynamics 365 Marketing (la primera) proporciona las herramientas que necesitan las pymes para ejecutar campañas de marketing exitosas en varios canales, mientras que Dynamics 365 Sales (la segunda) impulsa una mayor eficiencia y agilidad en la gestión con los clientes, reduciendo costes de TI y liberando a los equipos humanos de tareas repetitivas. La tercera solución es Dynamics 365 Customer Service, que brinda experiencias de atención al cliente conectadas en todos los canales y en todas las interacciones. Por su parte Dynamics 365 Finanzas (la cuarta) mejora los objetivos financieros y aumenta la rentabilidad. En el caso de la quinta solución, Dynamics 365 Supply Chain, las compañías tienen la opción de simplificar y optimizar la cadena de suministro, así como los procesos de fabricación con visibilidad en tiempo real. Finalmente, Dynamics 365 Business Central es una completa solución de gestión empresarial para pequeñas y medianas empresas que incorpora las capacidades de CRM y ERP.

En otro orden de cosas, dentro de la solución del Gigante de Redmond, la compañía ha incluido Dynamics 365 Copilot, su nueva solución que aprovecha los avances en inteligencia artificial generativa para automatizar tediosas tareas y potenciar la creatividad de la fuerza laboral. Por ejemplo, Copilot para Microsoft Dynamics 365 Sales y Viva Sales permite a los comerciales reducir el tiempo que dedican a tareas administrativas porque la IA les ayuda a escribir respuestas por correo electrónico para los clientes e, incluso, crear un resumen de una reunión de Teams en Outlook.

Mientras, Copilot para Dynamics 365 Customer Service redacta respuestas contextuales a las consultas tanto en el chat como en el correo electrónico, además de ofrecer una experiencia interactiva basándose en el historial de casos, además de estar siempre disponible para responder preguntas. Con Copilot para Dynamics 365 Customer Insights y Dynamics 365 Marketing los especialistas en marketing simplifican su flujo de trabajo en la exploración de datos, la segmentación de la audiencia y la creación de contenido.

Microsoft

Tel: 91 391 90 00
Web: dynamics.microsoft.com
Precio: consultar

Oracle Fusion Cloud ERP

El modelo de datos integrado de forma nativa de esta solución incluye módulos como HCM, EPM, SCM, fabricación, ventas, servicio y gestión de clientes.

Se trata de un software integral de gestión empresarial basado en la nube y diseñado para simplificar y automatizar áreas de negocio como planificación y aprovisionamiento, finanzas, informes, planificación de proyectos, obligaciones fiscales, ciclo de vida del producto, gestión de riesgos… Para ello proporciona un conjunto de aplicaciones enfocadas a reducir costes, mejorar los controles y aumentar la productividad. Aprovecha, de igual forma, las ventajas que brindan tecnologías como la inteligencia artificial y el machine learning.

En concreto, cuenta con un asistente digital basado en IA que simplifica y acelera las tareas comunes, permitiendo así formular preguntas sencillas como '¿cuál es el estado de mis solicitudes de compra pendientes?' o '¿qué conciliaciones se deben hacer hoy?'. Además, tareas personalizadas, como la emisión de facturas o las notificaciones de presupuesto, se entregan de forma proactiva, para que el proceso de aprobación también sea más rápido. Oracle Fusion Cloud ERP provee, de igual forma, a las empresas de la posibilidad de dedicar más tiempo al trabajo estratégico ya que automatiza los procesos de negocio más laboriosos y rutinarios. Promete que gracias a la tecnología de inteligencia artificial es posible automatizar hasta el 96 % de las transacciones. Por su parte, la herramienta introduce el machine learning a la planificación y la previsión predictivas para utilizar conjuntos de datos más amplios, mostrar sesgos ocultos, detectar desviaciones significativas y acelerar el tiempo de respuesta general.

Otro de los puntos clave de la propuesta de la multinacional norteamericana es que elimina la necesidad de soluciones de reporting de terceros al ofrecer capacidades de análisis integrados con una gran variedad de informes preconstruidos, junto con soluciones para que los usuarios creen sus propios informes sin asistencia de IT. Estas capacidades nativas de informes y análisis funcionan gracias a la arquitectura integrada de su modelo de datos. Al combinar varias aplicaciones cloud de Oracle, este reporting integrado revela información más precisa y relevante para que las compañías tomen decisiones más rápidas y acertadas para su negocio.

A nivel de seguridad, las más de 40 regiones con centros de datos que tiene distribuidos Oracle por el mundo están supervisadas y controladas por empleados de la propia compañía las 24 horas del día los 7 días de la semana. Con el marco de aislamiento de datos encriptado y seguro de Oracle, su base de datos nunca se comparte con otros clientes lo que reduce riesgos de ataques.

Oracle

Tel: 902 302 302
Web:
www.oracle.es
Precio: consultar

Sage 200 Advanced

Provista con capacidades de Business Intelligence, esta herramienta dirigida a compañías de entre 20 y 200 empleados se integra con Microsoft 365.

La solución resulta ideal para empresas de 20 a 200 trabajadores, se encuentra disponible 100% online (lo que garantiza su acceso desde cualquier lugar y dispositivo) y se mantiene actualizada conforme a la legislación actual. En torno a estos tres aspectos se articula la herramienta de gestión empresarial de Sage: es personalizable según las necesidades de cada pyme e incluye control financiero, gestión integral de proyectos (para su planificación y con opción de gestión de posventa y almacenes si fuese necesario), procesos de fabricación, recursos humanos, CRM… Además, Sage 200 Advanced ha sido provista de inteligencia empresarial para ofrecer un conjunto de indicadores de negocio clave y así facilitar la toma de decisiones, y su asistente Alisio promete una puesta en marcha fácil que guía paso a paso a los usuarios. También destaca su integración con Microsoft Outlook 365, Word 365 y Excel 365. Esto significa que es posible acceder a correos enviados y recibidos directamente a través de Sage 200, editar archivos en Excel para una gestión más sencilla de los datos, y preparar plantillas personalizables y documentos.

Para que el trabajo se realice con fluidez, la herramienta dispone de capacidades de automatización que consiguen que los procesos manuales sean más rápidos y también más fiables. En este sentido, las organizaciones además de automatizar transacciones y conciliaciones de cuentas pueden importar datos de estas y conectarlas directamente a su solución de Sage.

Asimismo, se garantiza el acceso a los datos en tiempo real ya sea para revisar presupuestos, cálculos fiscales, flujos de caja u órdenes de compra.

En lo referente a la parte de conectar con las necesidades de los clientes, la herramienta Sage 200 Advanced proporciona a las empresas las prestaciones y las funciones que necesitan para gestionar el área de ventas, clientes, inventario, facturación, y precios y descuentos. Todo ello permite obtener una vista completa de esos clientes para adaptarse mejor a sus necesidades. También tomar decisiones, actualizar inventarios y ajustar precios en tiempo real de manera más fácil.

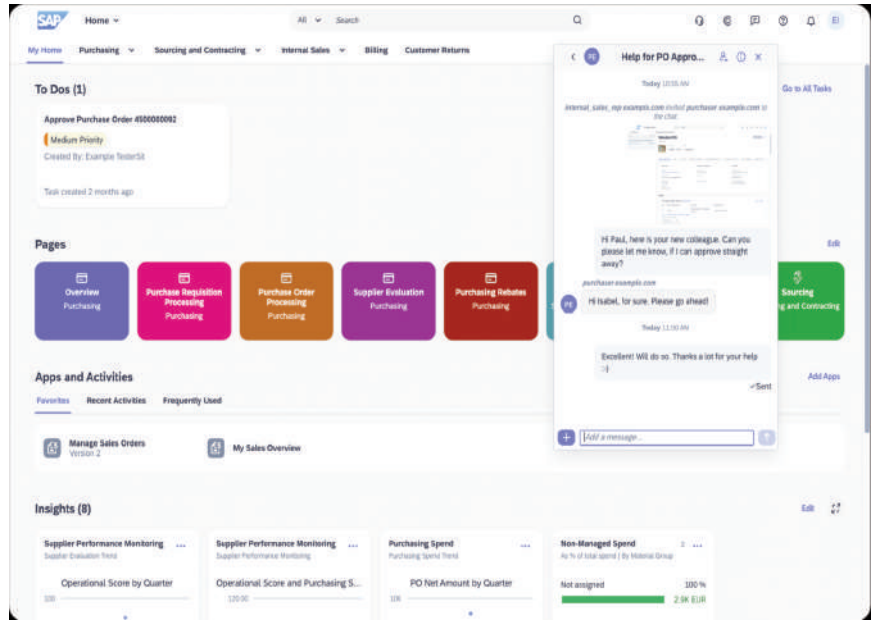
La propuesta de Sage se muestra, en otro orden de cosas, como una solución flexible dado que la disponibilidad de datos en tiempo real y su localización en la nube facilitan trabajar sobre la marcha y compartir información de manera inmediata. Esto facilita, entre otros, preparar informes interactivos para una vista en tiempo real del estado del negocio y que los trabajadores colaboren incluso estando fuera de la oficina.

Sage

Tel: 913 34 92 92
Web:
www.sage.com/es-es
Precio: consultar

SAP S/4HANA Cloud

Disponible en dos versiones (una pública y otra privada), dispone de capacidades de inteligencia artificial como IA conversacional, machine learning y analíticas en tiempo real.



Es una solución ERP modular e integrada que proporciona capacidades fundamentales para cubrir las necesidades de las empresas, desde las operaciones de misión crítica hasta la transformación de los modelos de negocio. Dentro de este contexto, la herramienta se perfila como una alternativa adecuada para las organizaciones que quieran desplegar un ERP por primera vez o pasar de un modelo on-premise a la nube.

Con capacidades de análisis, forma parte de la nueva estrategia AI for Business de SAP que integra manera responsable la inteligencia artificial en sus propias soluciones como es del caso de SAP S/4HANA para que las compañías mejoren su visibilidad, productividad y resultados. Incluso anticipar los cambios que están por venir para afrontarlos de manera más fácil. Estas funcionalidades ayudarán, por ejemplo, a que los equipos financieros controlen los costes y reduzcan los riesgos, al permitirles reaccionar rápidamente ante un cambio en el sentimiento de los clientes o, en el área de cobros, prever el riesgo de retraso en el pago de una factura y priorizar mejor qué clientes requieren un seguimiento.

SAP S/4HANA Cloud integra prácticas y procesos específicos de diferentes sectores en las áreas de finanzas, compras, servicios, ventas, fabricación, I+D, gestión de activos o cadena de suministro para favorecer el despliegue de procesos integrales. También una adopción más rápida, a la que contribuye asimismo una experiencia de usuario mejorada con el sistema de diseño SAP Fiori, basado en roles y que cuenta con una guía de usuario incorporada.

Al facilitar procesos de negocio automatizados, las compañías pueden adecuar su oferta a la demanda de forma más inteligente, por ejemplo, reponiendo existencias con una automatización inteligente basada en esta demanda; eliminando tareas repetitivas; automatizando procesos de cuentas por cobrar y cuentas por pagar; proporcionando información predictiva en tiempo real basada en funciones e integrada en cada paso del proceso; o acortando y prediciendo los cierres financieros.

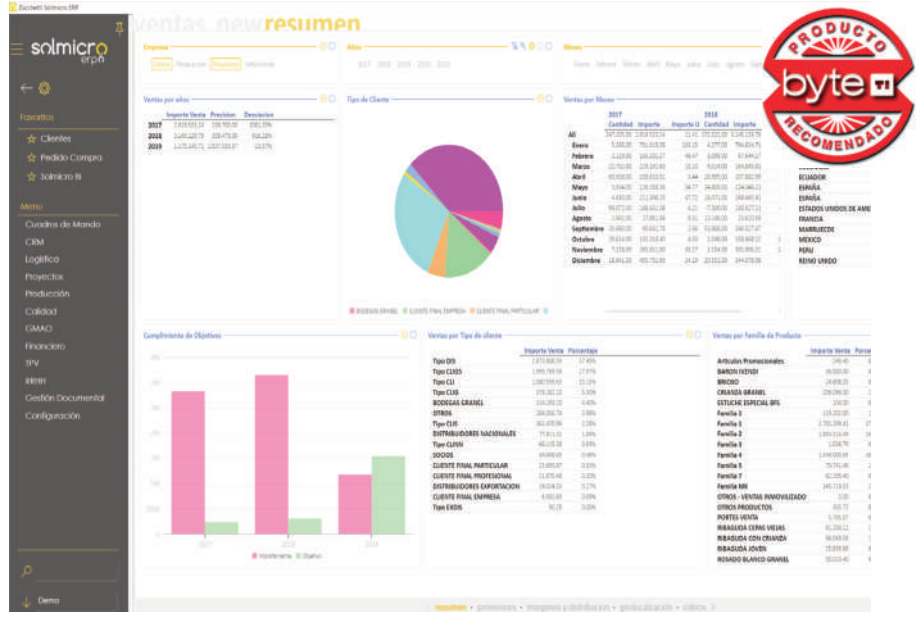
SAP S/4HANA Cloud está disponible en una edición pública y otra privada. Coincidiendo con el inicio de 2024 está previsto que la edición pública incorpore SAP Joule, un 'copiloto' de IA generativa en lenguaje natural que proporcionará información proactiva y contextualizada de la propia solución y de fuentes de terceros: de esta forma, los empleados solo tendrán que hacer preguntas o plantear un problema y recibirán respuestas inteligentes extraídas de la gran cantidad de datos empresariales, texto, imágenes y conocimiento de toda la cartera de SAP, y de fuentes de terceros (siempre conservando el contexto).

SAP

Tel: 91 456 72 00
Web:
www.sap.com/spain
Precio: consultar

Solmicro ERP

Facilita la transformación digital con destacadas mejoras a nivel de personalización, rendimiento, usabilidad, rentabilidad y sencillez en la migración hacia futuras versiones.



Solmicro ERP es una herramienta que cubre las nuevas necesidades de gestión de las empresas en un mercado cada vez más cambiante. Un software cuyas claves residen en una nueva interfaz de usuario altamente personalizable que ofrece una nueva experiencia de uso, un notable aumento de la productividad (que permite reducir los costes iniciales de implantación y de nuevos desarrollos) y una extensibilidad que busca la máxima personalización funcional y visual sin tocar el código estándar, evitando de esta manera conflictos en evoluciones futuras del ERP.

Mientras, y para asegurar la máxima productividad, en el desarrollo de la última versión del software sus responsables han logrado reducir los tiempos de implantación y adaptaciones para garantizar la mejor de las rentabilidades. Además, su interfaz totalmente renovada, ahora mucho más visual y con una usabilidad mejorada al simplificar los procesos, ayuda a minimizar la curva de aprendizaje de los trabajadores y a potenciar su productividad. Por ejemplo, los usuarios tienen la posibilidad de configurar elementos favoritos como programas, informes, registros y acciones. Con un menú centralizado en un único panel, la home no solo es personalizable sino que aprende del usuario integrando su trabajo con Office 365.

Asimismo, destacan las mejores en los elementos de búsqueda avanzada, y gestión de formularios y tabs. También los cuadros de mandos integrados, los sistemas de ventanas, los filtros dinámicos, y los campos y las solapas configurables.

Solmicro ERP es, por otro lado, un software desarrollado con tecnología de última generación que permite ofrecer soluciones de inteligencia de negocios, internet de las cosas, inteligencia artificial, realidad virtual y aumentada, big data… para que los clientes saquen el máximo partido a la información de su empresa y ganen en competitividad. Además, estos clientes (también distribuidores) cuentan con el apoyo de un equipo de soporte y herramientas de autoformación que los otorgan una alta autonomía a la hora de resolver cualquier duda.

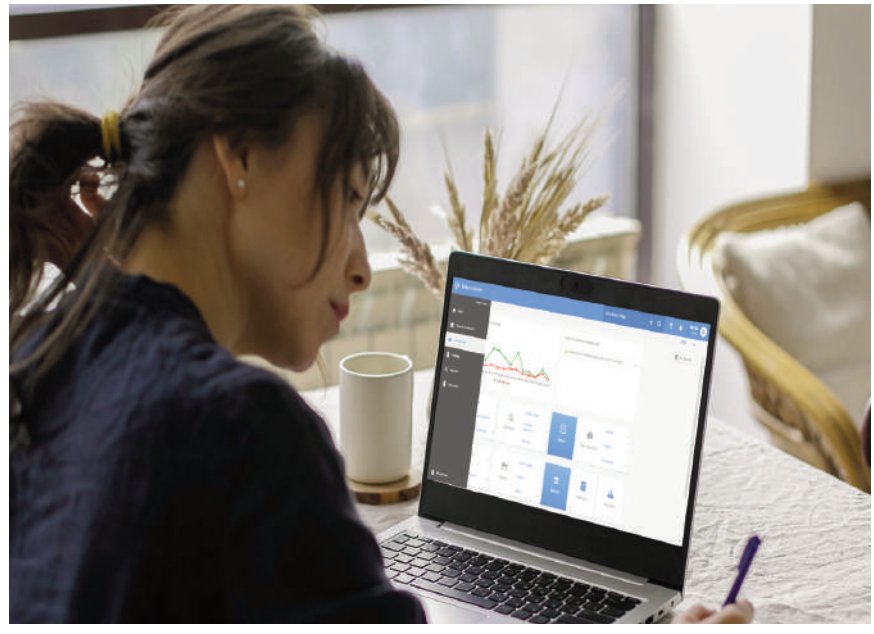
Preparada para integrar desarrollos de terceros, este ERP dispone de módulos específicos enfocados a las siguientes áreas: CRM, TPV, gestión del conocimiento, financiero, comercial, compras, gestión de proyectos, mantenimiento, gestión de costes, recursos humanos, stocks y almacenes, calidad, configurador de productos y fabricación. Para concluir, Solmicro ERP desarrolla soluciones sectoriales que se dirigen de manera específica a los siguientes nichos de mercado para cubrir sus necesidades: industrias, bodegas, construcción, ingenierías, instaladoras, automoción, distribución, servicios, alquiler de maquinarias y agropecuario.

Zuchetti

Tel: 94 427 13 62
Web:
www.solmicro.com
Precio: A consultar

Wolters Kluwer a3innuva | ERP

Una solución online de facturación y contabilidad para pymes y autónomos que permite conocer el estado de los negocios en tiempo real y desde cualquier dispositivo.



Wolters Kluwer participa de la mano de a3innuva | ERP, una herramienta accesible vía 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 sus necesidades. Gracias a este planteamiento, los clientes que adquieren esta solución no solo disponen de una visión global de su negocio: siguen su evolución a través de indicadores disponibles en tiempo real para tomar decisiones de forma ágil y eficiente.

Respecto a sus características, es posible introducir presupuestos y facturas, gestionar los cobros y pagos, las remesas de cobro y la facturación periódica de la empresa. De igual modo, permite facturar de forma totalmente automatizada e integrada con la contabilidad y fiscalidad para reducir los tiempos de gestión y ganar en eficiencia y productividad. a3innuva | ERP ayuda también al usuario a personalizar tanto los presupuestos como las facturas con el logotipo y los datos de su compañía y desde la misma solución enviarlos y controlar su recepción y lectura. Tampoco faltan los gráficos, las comparativas y los rankings que recogen los principales indicadores de la organización para disponer en tiempo real de información clave y de interés para consultar cualquier cambio. Incluso la pyme o el autónomo que la adquiera puede trabajar de forma colaborativa con su asesor en un entorno de trabajo único compartido para que acceder directamente a los datos e información del negocio en tiempo real.

Cabe destacar que la propuesta de Wolters Kluwer se adapta a los cambios normativos en materia de facturación derivados de los Reglamentos de la Ley Antifraude y la Ley Crea y Crece, y que responde igualmente a las obligaciones legales y técnicas exigidas como TicketBAI en el País Vasco. a3innuva | ERP se encuentra, asimismo, adaptada al 100% al nuevo sistema de gestión online del IVA/IGIC.

Adaptable a las necesidades de crecimiento de las pymes, brinda integraciones a través del a3Marketplace y APIs para su integración con otros sistemas. En lo que respecta a la plataforma online a3Marketplace, Smart CRM es una aplicación que ayuda a gestionar las oportunidades comerciales de clientes reales o potenciales confeccionando ofertas y realizando un seguimiento de su estado real. Entre sus nuevas funcionalidades se incluye la gestión de expedientes. Otra opción es la app Klik-Ticket Lite que sirve para gestionar, entre otros, las notas de gastos.

Wolters Kluwer

Tel: 900 11 11 66

Web:
www.wolterskluwer.com/es-es/solutions/a3innuva

Encuentros tecnológicos

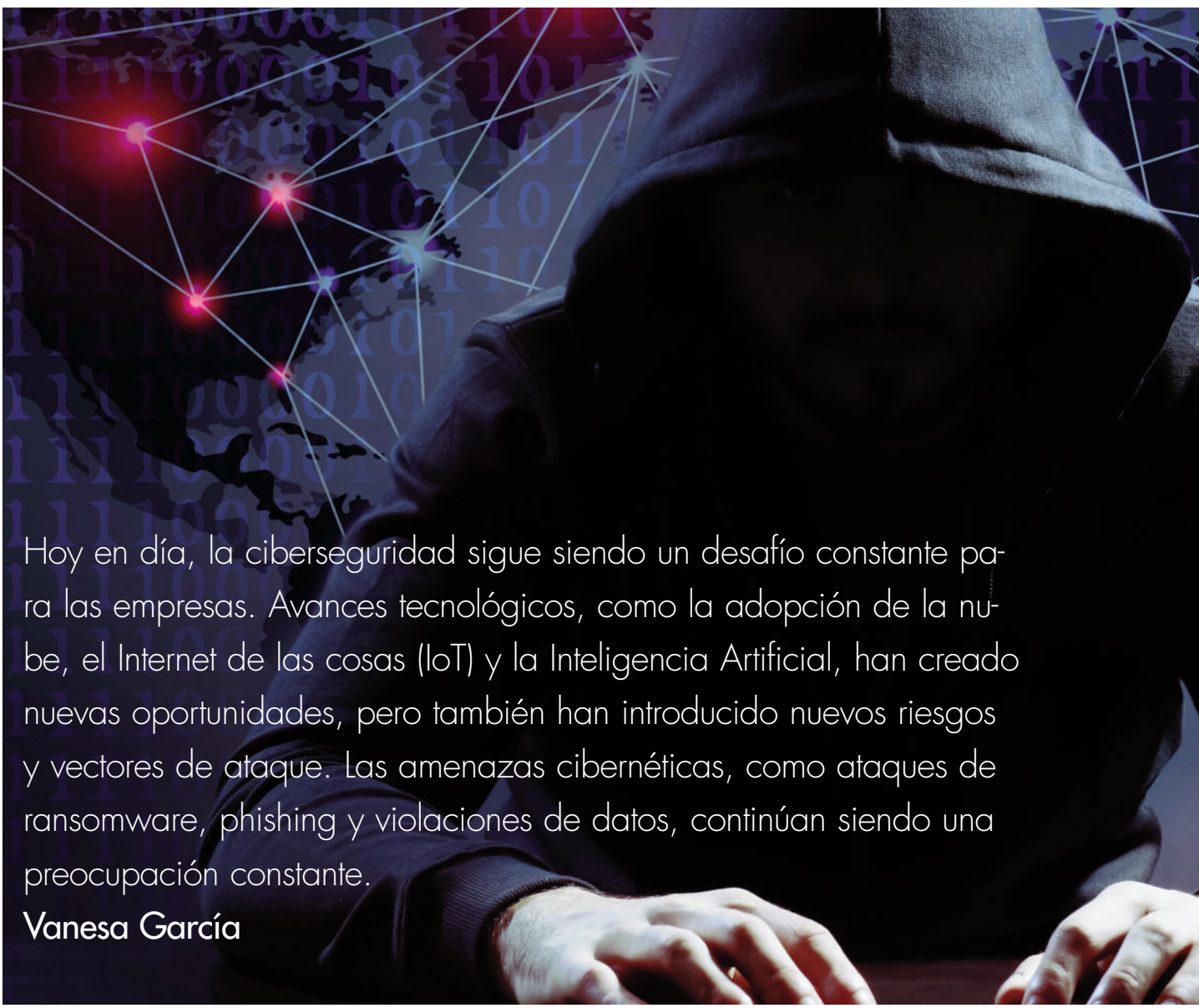
byte TI

¿Quieres tener un contacto directo con los CIOs de las grandes empresas españolas?

Byte TI te organiza un encuentro a medida con ellos.

Convénceles de que tus soluciones son las mejores.

La **ciberseguridad** afronta nuevos retos



Hoy en día, la ciberseguridad sigue siendo un desafío constante para las empresas. Avances tecnológicos, como la adopción de la nube, el Internet de las cosas (IoT) y la Inteligencia Artificial, han creado nuevas oportunidades, pero también han introducido nuevos riesgos y vectores de ataque. Las amenazas cibernéticas, como ataques de ransomware, phishing y violaciones de datos, continúan siendo una preocupación constante.

Vanesa García

Por ello, se espera que la demanda de soluciones VPN experimente un notable aumento al nivel mundial en el 2024, ya que la preocupación por la seguridad de los datos, tanto personales como empresariales, ha ido en aumento este año. En términos generales, según Marc Rivero, Lead Security Researcher de Kaspersky, también se ha observado un aumento en la concienciación sobre seguridad, "muchas empresas están invirtiendo más en medidas preventivas y en la formación de sus empleados. Sin embargo, los ciberdelincuentes también están mejorando sus tácticas, lo que hace que la ciberseguridad sea una carrera constante entre defensores y atacantes".

De este modo, uno de los principales retos a los que se enfrentan las empresas es la falta de personal cualificado. Ignacio Franzoni, Senior Sales Engineer de Netskope Iberia explica que este caso, incide sobre todo, en lo que se refiere al área de ciberseguridad. "La escasez de talento sigue siendo un problema preocupante. Además de ello, los continuos y crecientes ataques, cada vez más frecuentes, más evasivos, más sofisticados y que llegan a través de muchas más vías, supone un reto para las empre-

sas que aún no están al 100% preparadas. Por ejemplo, ahora, el SEO “poisoning”, está resultando un problema con páginas infectadas que aparecen en los primeros resultados de los buscadores, pasando desapercibidas como tales”.

El robo de credenciales y la explotación de vulnerabilidades sin parchear en los equipos conectados a Internet son otra de las razones por las que una empresa se puede ver comprometida. Así lo destaca Chester Wisniewski, Director Global Field CTO de Sophos, “los ciberdelincuentes siguen buscando formas de eludir la autenticación multifactor a medida que aumenta su adopción. Esto incluye una mezcla de servidores proxy maliciosos, ataques de ingeniería social, robo de cookies y ataques de fatiga. En nuestro último informe Active Adversary, que analiza los casos de respuesta a incidentes (IR) que Sophos ha analizado desde enero de 2022 hasta la primera mitad de 2023, observamos que faltaban registros de telemetría en casi el 42% de los casos de ataque estudiados. El informe también destaca el descenso del tiempo de permanencia, con un 38% de los ataques de ransomware "rápidos" ocurridos en los 5 días siguientes al acceso inicial”.

Con todo ello, la presencia de una estrategia bien definida es esencial para el éxito a largo plazo. Sin embargo, muchas empresas enfrentan desafíos al formular y ejecutar sus estrategias, desde la falta de alineación hasta errores comunes que pueden obstaculizar su crecimiento. Para hacer frente a estos desafíos, Isabel López, Sales Engineer Manager dice que desdee Samsung España existen diversas soluciones de seguridad centralizadas, “desde el servicio TI, como Samsung Knox Matrix, que permite que los usuarios no tengan que comprometer su conectividad para estar protegidos, ya que, mediante la supervisión de varias capas, minimiza las brechas de seguridad durante la autenticación de los dispositivos”.

Siguiendo este punto, los especialistas de Hornetsecurity recomiendan cubrir todos los ángulos del perímetro de seguridad:

- Formar al usuario en detección de ataques haciendo del mismo el firewall más importante a través de herramientas como nuestro Security Awareness Service
- Proteger y prevenir los ataques. Poniendo tecnología alrededor del usuario, y específicamente en el mayor vector de ataque actual, el correo electrónico
- Asegurar la política de seguridad del dato de la compañía. Controlando tanto temporalmente como en cuanto a privilegios, las comparticiones de archivos internos y externos
- Si aun así el ataque fructifica, asegurar la recupe-

Una estrategia bien definida es esencial para el éxito a largo plazo

ración rápida de todos los datos. Evitar el lucro cesante de la empresa y el daño reputacional. Todo ello con una solución de backup y recuperación segura e inmutable, a prueba de ransomware

En el caso de las pymes, "contar con asesoramiento externo puede ser una opción más que inteligente para poder monitorizar o instalar soluciones especializadas", afirma Gonzalo Echeverría, Country Manager Zyxel Iberia, pues muchas veces solamente se establecen mecanismos sencillos de protección para paliar posibles ataques.

CÓMO INTEGRAR LAS SOLUCIONES

La integración de soluciones de seguridad en las empresas es crucial para crear un enfoque integral y efectivo para la protección de la información. Para ello, según Rivero, en primer lugar es esencial realizar una evaluación de riesgos para identificar las posibles amenazas y vulnerabilidades específicas de cada empresa. "Después hay que crear una estrategia de seguridad que aborde los riesgos identificados y establecer políticas y procedimientos de seguridad claros. Por otro lado, es fundamental utilizar soluciones de seguridad de confianza e implementar la automatización de procesos para mejorar la eficiencia y la capacidad de respuesta frente a amenazas. Asimismo, la capacitación y concienciación a los empleados sobre las prácticas de seguridad debe ser otro aspecto clave".

Además de todo lo anterior, resalta que también hay que realizar análisis de seguridad, "para evaluar la efectividad de las soluciones y realizar mejoras continuas y mantenerlas actualizadas para abordar las nuevas amenazas y vulnerabilidades. Para terminar, es fundamental desarrollar un plan de respuesta frente a incidentes que incluya la coordinación de todas las soluciones de seguridad para abordar y mitigar rápidamente las amenazas".

Por otro lado, desde Netskope señalan la formación continua del personal a la hora de integrar de forma efectiva las soluciones de seguridad. Mientras que, desde Sophos, explican que, si bien lo ideal es que un cliente tenga distintos productos de un mismo fabricante, cuya integración es prácticamente automática, en la práctica no es algo común, en el caso de Sophos, podemos prácticamente agregar cualquier fabricante y, de no estar soportado, tenemos capacidad de desarrollar de forma ágil nuevos conectores al respecto. De este modo, el producto es un verdadero XDR, agnóstico de fabricante y con capacidad de respuesta sobre ellos también".

Por otro lado, desde Samsung dicen que las soluciones deben integrarse de manera que proporcionen una visión holística de la seguridad, permitiendo una gestión centralizada y una respuesta rápida a incidentes, "Knox Matrix funciona como un sistema de cadena de bloques privado del usuario, en el que los dispositivos conectados mejoran

la seguridad mediante la supervisión de varias capas. De cara a minimizar las brechas de seguridad durante la autenticación de los dispositivos y hacer que el proceso de inicio de sesión sea más cómodo, Knox Matrix comparte las credenciales de dispositivo a dispositivo y protege la información sensible incluso entre dispositivos de confianza".

ENTORNOS CLOUD Y ON-PREMISE

A medida que las empresas continúan avanzando con una fuerza laboral más distribuida, la transición hacia la nube no solo sigue una tendencia, sino que se ha convertido en una necesidad estratégica para las empresas. La capacidad de almacenar, gestionar y acceder a datos de manera remota ha transformado radicalmente las operaciones empresariales. Aunque la migración a la nube aporta flexibilidad y eficiencia, también plantea nuevos desafíos de seguridad en un contexto donde la ciberseguridad emerge como un pilar esencial.

"Ningún entorno informático puede ser seguro al 100%, sobre todo cuando, debido al aumento de los ciberataques a gran escala, existe un riesgo creciente de que los piratas informáticos ataquen específicamente platafor-

mas y recursos en la nube. Los cibercriminales lo saben, y por eso suelen dirigirse a los usuarios finales en lugar de a la propia infraestructura. Cuando esto sucede, un ransomware, mediante phishing u otro ataque, dirigido a un empleado individual puede propagarse rápidamente a la nube. Por lo tanto, también se debe proteger el entorno de la infraestructura local comprometida. Muchas organizaciones todavía asumen que los datos almacenados dentro de los servicios en la nube (como Microsoft 365) están seguros y protegidos, y a muchas empresas se les sigue escapando la realidad de la responsabilidad compartida de proteger esos datos", recalca Paul Canales, Head of Channel de HornetSecurity.

Entonces, ¿qué pueden hacer las empresas? Para responder a esta pregunta, Echeverría hace hincapié en el filtrado web, el software de gestión y la motorización de repuntación URL, "el filtrado de web tiene numerosos beneficios, pues ayuda a mejorar la seguridad de la web bloqueando el acceso a sitios web potencialmente dañinos que podrían infectar los equipos de la empresa con malware o virus. Igualmente, puede proteger los datos confidenciales de la empresa y reducir el riesgo de ataques cibernéticos. Por su parte, el software de gestión de dispositivos permite a las empresas realizar un seguimiento y controlar los dispositivos y proteger los datos almacenados en ellos. Otro enfoque efectivo para prote-

ger la fuerza laboral distribuida es a través de monitorización de reputación de URL. Esta medida de seguridad implica monitorizar y analizar la reputación de los sitios web y las URL para identificar cualquier riesgo potencial o actividad maliciosa".

Por su parte, Rivero se decanta por una estrategia adaptada a las características específicas de estos entornos, "como establecer un modelo de responsabilidad compartida en el que el provedor de estos servicios se encarga de la seguridad y los usuarios son responsables de asegurar sus datos y configuraciones. Ya que los entornos en la nube se caracterizan por su capacidad de aprovisionar datos de manera rápida y dinámica, la estrategia de ciberseguridad debe incorporar la automatización para garantizar una respuesta rápida a las amenazas y la monitorización continua para identificar comportamientos anómalos y posibles amenazas".

PREVENIR ATAQUES DE RANSOMWARE

La exfiltración de datos es el denominador común entre el ransomware, las amenazas internas y el robo de datos. A pesar de que los laboratorios de investigación de amenazas a menudo detallan los aspectos del cifrado del ransomware, las etapas relacionadas con el acceso a los datos y la exfiltración suelen pasarse por alto. De ahí que la supervisión integral de la actividad de los empleados, es-

pecialmente en entornos que permiten el uso de dispositivos no corporativos (BYOD), presente desafíos considerables. Esta situación, además, brinda una ventaja al ciberdelincuente, ya que puede infiltrarse primero en dispositivos corporativos, robar información, cifrarla y luego exigir un rescate.

Y es que, a pesar de contar con medidas estándar de supervisión y protección contra el ransomware, la falta de visibilidad en equipos no gestionados puede generar problemas. No obstante, Alberto R. Rodas, Sales Engineer Manager Iberia Region de Sophos subraya la importancia de que las empresas confíen en sistemas de protección complementados con sistemas de investigación. “Estamos viendo un alto crecimiento del mercado EDR, pero no hay que olvida que este mercado proporciona herramienta de investigación, no de protección, por lo que no debemos pensar que el EDR sustituye al EPP. Éste último sigue siendo más necesario que nunca, y además será vital disponer de una solución EPP que cuente con capas de seguridad actualizadas y complementarlo con un EDR para detectar aquello que se le haya podido saltar. Por otro lado, es todavía más importante disponer de un parque de equipos actualizados, sin software deprecado, con sus actualizaciones y parches vigentes, pues los actores maliciosos son especialistas en encontrar estos “santuarios” en las redes para desde ellos, realizar los ataques”.

Al final, en palabras de Ignacio Franzoni, la estrategia más acertada es aquella que abarque desde la perspectiva de un acceso de confianza mínima, hasta unas políticas de seguridad bien definidas para la protección de la información, ·complementado con una buena protección de amenazas y herramientas de análisis avanzado de comportamiento en tiempo real. Todo ello integrado con el resto de herramientas de seguridad y visibilidad de todos los entornos donde la información se encuentre. Las plataformas SSE también pueden ser, por tanto, de gran ayuda”.

Estrategia para entornos móviles

Los entornos móviles se han convertido en uno de los aspectos más críticos para la ciberseguridad, tanto desde la perspectiva de los empleadores como de los empleados Si bien las empresas se han adaptado a las nuevas formas de trabajar, los riesgos de ciberseguridad relacionados con los entornos móviles siguen sin abordarse. Según datos de HornetSecurity, el 18% de los profesionales de IT dice que los trabajadores no están seguros cuando trabajan de forma remota, pero, aun así, casi el 74% de los empleados tienen acceso a datos críticos. Quizás por esto, como era de esperar, el 14% de los encuestados admitió que su organización sufrió un incidente de ciberseguridad relacionado con el teletrabajo.

No sólo los profesionales de IT saben que el trabajo remoto trae problemas asociados, sino que las personas están experimentando las consecuencias de contar con medidas de protección inadecuadas y

una gestión insuficiente. Teniendo en cuenta la facilidad para compartir y colaborar que ofrecen determinadas aplicaciones, es muy fácil que los datos confidenciales se filtren, por error o de forma malintencionada. Por ello muchas organizaciones se enfrentan a la cruda realidad de tratar de gestionar el uso compartido y los permisos después de que hayan aumentado de forma descontrolada, lo que pone en valor lo necesario que es una aplicación de gestión de permisos para los administradores y CISOs, ya que puede ayudar a prevenir el acceso no autorizado a los datos corporativos.

Sobre esto, Paul Canales de HornetSecurity asegura que a popularidad del trabajo remoto y los riesgos asociados implica que las organizaciones deben priorizar la capacitación y la formación para que el trabajo remoto sea seguro, "los métodos tradicionales de control y seguridad de los datos de la empresa no son tan efectivos cuando los empleados trabajan en ubicaciones remotas y la mayor responsabilidad recae en el individuo. Las empresas deben reconocer los riesgos particulares asociados al trabajo remoto, activar los sistemas de gestión de seguridad relevantes, así como capacitar a los empleados para que sepan enfrentarse a un cierto nivel de riesgo".

El Director Pre-Sales de Akamai España y Portugal, añade varios protocolos de autenticación fuertes a la estrategia integral de seguridad móvil, "como la autenticación de dos factores (2FA), la actualización constante de los sistemas operativos a las últimas versiones, que generalmente vienen equipadas con funciones de seguridad mejoradas, además de proporcionar campañas de sensibilización integrales dirigidas a educar a los empleados sobre las estafas de phishing rampantes especialmente diseñadas para plataformas móviles".

Ampliando estas medidas, el Country Manager Zyxel Iberia destaca que también es importante mantener los dispositivos actualizados, "ser cautos con los intentos de phishing y descargar aplicaciones solo de las tiendas de aplicaciones oficiales. También es esencial instalar un antivirus de confianza y utilizar una VPN (Virtual Private Network) cuando nos conectemos a una red Wi-Fi pública para encriptar la conexión y proteger los datos".

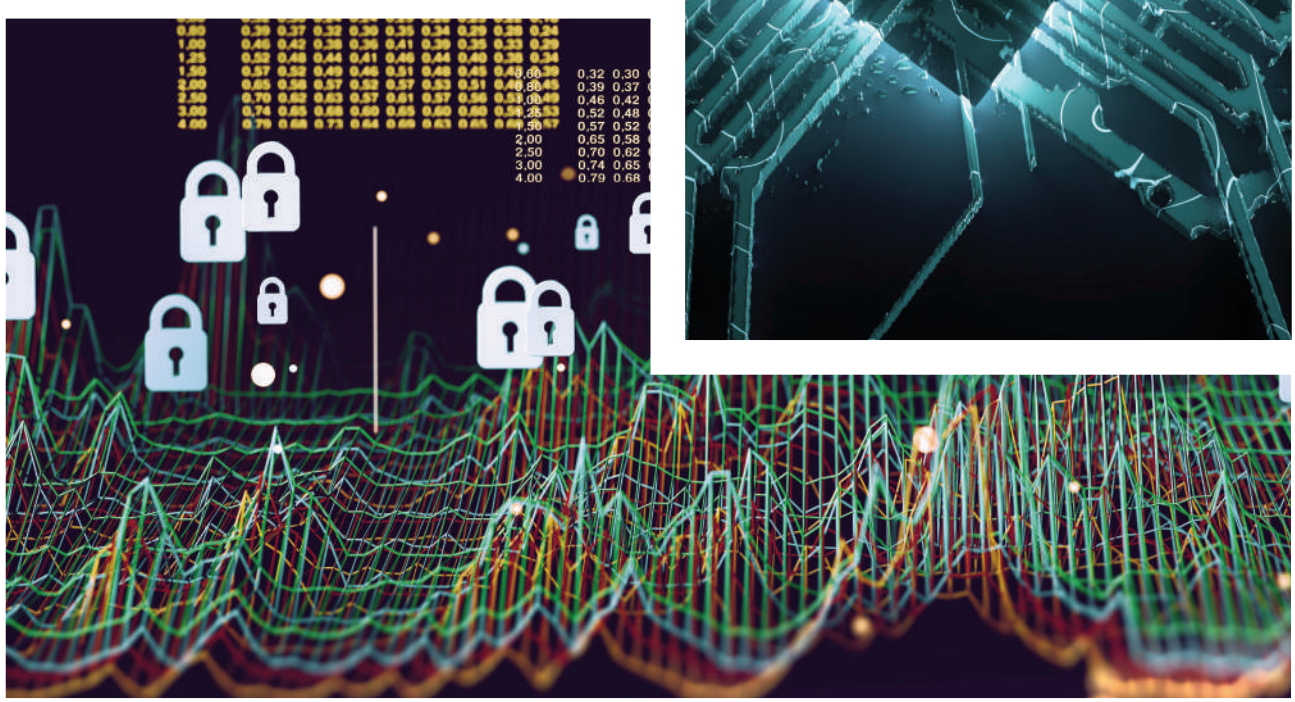
ARQUITECTURAS SASE

Por su parte, la inversión en Secure Access Service Edge (SASE) está experimentando un crecimiento significativo a medida que las empresas rediseñan su infraestructura de red para satisfacer las demandas de los trabajadores híbridos y la computación en la nube. SASE combina seguridad y conectividad de red, abordando desafíos como la consolidación de servicios de seguridad, acceso seguro y directo a la nube, el enfoque Zero Trust, inteligencia de amenazas en tiempo real y escalabilidad. Aunque la implementación de SASE puede ser un proceso complejo, ofrece a las empresas

una solución integral para mejorar la ciberseguridad, adaptándose a las necesidades cambiantes del entorno empresarial.

"Hay varias herramientas y estrategias en las que el modelo de servicio o arquitectura SASE juega un gran papel y es especialmente adecuado para el modelo actual de personal distribuido, en el que las personas a menudo trabajan de forma remota desde varias ubicaciones utilizando diferentes dispositivos. La solución Enterprise Application Access, parte de la oferta SASE de Akamai, integra la protección de los accesos remotos a aplicaciones corporativas (ZTNA), la protección DNS (DNSP) y la autenticación multifactor (MFA) en una solución unificada que proporciona una conectividad segura y sin fisuras en toda la organización, al tiempo que mejora el rendimiento gracias a su arquitectura distribuida globalmente, garantizando así tanto la productividad como la seguridad sin comprometer ninguna de las dos", resalta el Director Pre-Sales de Akamai España y Portugal.

A pesar de sus múltiples beneficios, para el Lead Security Researcher de Kaspersky, la arquitectura SASE no es la única solución, "sino que se puede combinar con otras herramientas y enfoques para lograr una estrategia de seguridad más completa y eficaz como la implementación de VPN, para proteger la comunicación entre el dispositivo y la red de la empresa, de soluciones de seguridad específicas para endpoints y



el entrenamiento en concienciación y formación de los empleados".

IA Y EL ML PARA MEJORAR LA SEGURIDAD

La ingeniería social sigue siendo uno de los principales métodos que utilizan los actores de amenazas para hacerse un hueco inicial en una organización objetivo. También se ha visto un aumento de los casos en los que los usuarios objetivo son manipulados socialmente para interactuar con un enlace malicioso a través de ataques de phishing cada vez más sofisticados.

Con el lanzamiento de ChatGPT de OpenAI a finales de 2022, y su creciente popularidad a principios de 2023, la IA generativa comenzó rápidamente a alterar el sector de la ciberseguridad. Además, se ha hecho evidente que GenAI podría ser utilizada por agentes de amenazas novatos no solo para lanzar ataques, sino incluso para aprender cómo lanzarlos. Estas nuevas capacidades impulsaron un aumento de los ciberataques a lo largo del año pasado y siguieron elevando aún más el nivel de preocupación. Una de las predicciones que aparecen en el informe de Cibersegurid de HornetSecurity es que los agentes de amenazas seguirán desarrollando sus variantes de dark web de ChatGPT para comprender mejor y poder automatizar partes adicionales de la cadena de ataque.

Aunque las noticias sobre ciberseguridad se han centrado casi por completo en las repercusiones negativas de la IA generativa en nuestro sector, también hay buenas noticias, "los expertos en seguridad y los proveedores estamos poniendo en práctica la IA generativa al servicio de nuestras herramientas defensivas para proteger a las organizaciones. Estas organizaciones tendrán que mantenerse al tanto de estas evoluciones y ajustar su actitud de seguridad en consecuencia en el próximo año y, de nuevo, un elemento fundamental aquí será la formación", dice el portavoz de HornetSecurity

Y es que, la IA y el ML pueden ser dos grandes aliados en materia de ciberseguridad, por ello, Franzoni añade que para que las empresas puedan aprovechar el potencial de la IA con seguridad, soluciones como SkopeAI, son una buena opción, "SkopeAI utiliza IA/ML para ofrecer una protección de datos (estructurados y no estructurados) y una defensa frente a las actuales ciberamenazas, superando las limitaciones de las tecnologías de seguridad convencionales y proporcionando una protección mediante técnicas a la velocidad que hoy día requiere la IA, y que hasta ahora no se encuentran en los productos de otros proveedores de SASE".

Otro punto a favor de la IA es que puede generar un entorno de ciberresiliencia, "anticipando vulnerabilidades y descubriendo debilidades en las aplicaciones o en la configuración de la red antes de que se produzca cualquier brecha de seguridad. Esto permite a las empresas tomar medidas correctivas de manera proactiva", concluye López.

UN PROBLEMA: LA FALTA DE TALENTO

La escasez de profesionales cualificados en ciberseguridad afecta la capacidad de las empresas para protegerse. Además, la gestión de incidentes y la respuesta a eventos de seguridad pueden ser más lentas y menos efectivas cuando hay escasez de talento. Esto puede llevar a un mayor tiempo de inactividad y pérdida de datos en caso de incidente.

Para abordar este problema, desde Kaspersky inciden en que es importante promover programas educativos en el campo de la ciberseguridad, "establecer asociaciones entre instituciones educativas y la industria, ofrecer becas y oportunidades de desarrollo profesional, así como concienciar sobre la importancia de la ciberseguridad en todos los niveles de la sociedad. Todo ello, para garantizar la seguridad de empresas frenta a ataques que puedan dar lugar a pérdida de datos, la interrupción de servicios y daños a la reputación de las organizaciones", explica Marc Rivero.

Federico Dios, Director Pre-Sales de Akamai España y Portugal añade que las empresas también pueden adoptar medidas como, "invertir en la formación y el desarrollo de los empleados, ofreciendo programas formación y desarrollo continuos; ofrecer salarios y beneficios competitivos para atraer y retener talento; y/o externalizar los servicios de ciberseguridad a un proveedor externo para cubrir las necesidades de su equipo de seguridad".

En contraposición a sus compañeros, Chester Wisniewski, Director Global Field CTO de Sophos resalta que lo importante ya no es la experiencia, sino las ganas con las que se desempeña la ciberseguridad, "debemos tener una mentalidad más abierta a la hora de contratar profesionales de la seguridad, aumentando la diversidad de nuestros posibles candidatos. Conozco a muchos jóvenes que eran ingenieros informáticos, profesionales de la privacidad, personal informático y personas con formación en ciencias sociales que tienen dificultades para pasar a desempeñar funciones de seguridad informática, a pesar de tener experiencia en otros campos y formación en seguridad. La experiencia en este campo es importante, pero actualmente desempeña un papel de guardián que no podemos permitirnos. Las personas apasionadas por lo que hacemos y que puedan aportar su experiencia previa nos ayudarán a colmar estas lagunas y, probablemente, darán mejores resultados a largo plazo".

Ali@2, **formación digital** frente a la brecha de talento

España sufre desde hace años una brecha de talento. Alrededor del 80% de las empresas asegura tener dificultades para encontrarlo pese a que el país padece una tasa de paro del 11,6%.

Una de las principales dificultades para las compañías a la hora de cubrir estas vacantes es la falta de capacitación tecnológica de los candidatos/as, unas habilidades cada vez más demandadas en la mayoría de los puestos de trabajo. Esta falta de formación provocó en 2022 que 120.000 vacantes se quedasen sin cubrir en el sector IT, a pesar de ser uno de los sectores que más vacantes generó.

Ante esta situación, Microsoft, su Asociación Internacional de Partners – IAMCP (International Association of Microsoft Channel Partners) y The Adecco Group sintieron la responsabilidad de hacer frente a este problema de desajuste de talento. Y, para ello, se unieron en búsqueda de una solución sólida y eficiente. Uniendo nuestras fuerzas se firmó la alianza Ali@2 con el objetivo de dotar a los Partners de Microsoft de esas necesidades de personal formando a jóvenes, tanto titulados universitarios como procedentes de grados de Formación Profesional, en áreas vinculadas a las TIC o afines en estas habilidades digitales tan demandadas en las ofertas que quedan desiertas.

FORMACIÓN FRENTE A LA BRECHA DE TALENTO

De este modo, Ali@2 crea sinergias con las empresas que forman parte del programa para resolver la falta de talento y definir las habilidades digitales específicas de estas. El programa forma a jóvenes y les otorga la posibilidad de acreditar a través de certificaciones homologadas las capacidades aprendidas durante esta etapa formativa en la que desde un principio conocen la empresa de la asociación para la que trabajarán.

Por otro lado, la empresa goza además de la garantía de que el talento que va a incorporar a su plantilla cuenta con la formación, skills y motivación necesaria para desempeñar las tareas e incorporarse a sus plantillas como cantera necesaria para el desarrollo de proyectos.

Irededor del 80% de las empresas asegura tener dificultades para encontrar el talento que busca, pese a que el país padece una tasa de paro del 11,6%

Así se han conseguido paliar las necesidades de las empresas que forman parte de Ali@2 y que requerían este tipo perfiles, garantizando a los partners de Microsoft el talento joven del que carecían. Un talento joven que tras su formación está capacitado para realizar las tareas que demanda la empresa y que opta ahora de una oportunidad laboral en un mercado que le daba la espalda habitualmente. La unión de fuerzas resulta exitosa siempre. Por ello, Ali@2 continuará con su camino para superar las más de 200 empresas de la comunidad y para formar a más de 2.000 jóvenes en estas habilidades digitales para seguir cubriendo la falta de talento de las empresas.

“Queremos acabar con la brecha de talento y gracias a Ali@2 podemos ser parte activa para resolver un gran problema que tiene el sector como es la gran escasez de perfiles cualificados. Apostamos firmemente por estas formaciones que ya están dando un respiro a las empresas adscritas a la comunidad Ali@2, ya que necesitaban poner en marcha proyectos de manera urgente y nosotros les hemos ayudado a hacerlo. Nos queda trabajo por hacer y queremos seguir dotando a las empresas del sector de profesionales con estas habilidades, así como proporcionar a estos últimos una oportunidad laboral en un momento crítico para incorporarse al mercado laboral siendo joven», afirma Óscar Rodríguez García, Head of IT Industry

The Adecco Group Spain.

«Las habilidades digitales llevan años con nosotros en nuestros entornos laborales, pero con el paso del tiempo van aumentando su presencia y sus características, por lo que es crucial que las empresas dispongan del talento lo suficientemente formado para afrontar su día a día con estas herramientas. Con la alianza, estamos reduciendo la brecha de talento en este campo, pero queremos continuar ayudando a nuestros partners e impulsando el talento joven con esta formación para que ambas partes se encuentren», señala Enrique Ruiz, Data Center Cloud Region Lead and Chief Employability Officer de Microsoft.

«Con iniciativas como esta, hemos dado un impulso al talento digital juvenil y su empleabilidad dentro del tejido empresarial de la asociación, para que sus empresas puedan ser más competitivas. No obstante, seguimos en el camino de contribuir activamente a que nuestros socios no vean mermados sus resultados o expectativas por la falta de personal cualificado y, así mismo, poder contribuir a que se abran puertas a los jóvenes en un mercado laboral que vive tiempos complicados», apunta Francisco Racionero, presidente de la IAMCP.

Inmaculada Sánchez Ramos,
Presidenta de la Asociación Española de Ingenieros de Telecomunicación-Madrid

Hijos: no
Hobbies: Las personas. Reuniones con amigos y familia. Aprender cosas de toda clase.
Estudios: Doctora Facultad de Ciencias Jurídicas y Sociales URJC.
ngeniera Superior de Telecomunicación (UPM)

¿Cómo llegaste al mundo de las TIC?
A mí me gusta aprender y saber, por lo que a la hora de escoger la carrera tuve un dilema importante pues prácticamente todo me gustaba. En el amplio abanico de posibilidades que se me ofrecía solo tenía claro una cosa. Esta es que "engancharse" en una carrera, digamos de letras, siempre es viable y, sin embargo, para hacer una carrera de las que tradicionalmente se denominan de ciencias, ese era el único momento. Por ello, decidí hacer una ingeniería al ser estas muy prácticas y de buena empleabilidad. Eso sí dentro de las ingenierías si tuve muy claro que lo que me atraía era el ámbito de las TIC. Téngase en cuenta que en aquel entonces informática estaba embebida en ingeniería de telecomunicación. De hecho, una de las especialidades de la carrera se denominaba Informática-Transmisión que era la más demandada y, por cierto, es la que cursé yo.

¿Qué es lo que más valora de su trabajo?
El impacto vital que tiene en la vida de las personas. Hoy en día, en cualquier cosa que hagamos conscientes o inconscientemente, usamos las TIC.

En su opinión ¿qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?
En general, no sólo en el caso de las mujeres, la falta de vocaciones STEM es muy preocupante en España. Ello, entre otras razones, es debido a que los profesionales de estas disciplinas tienen un "techo de cristal" en su desarrollo profesional. Si observamos, los componentes de los Comités de Dirección y, no digamos, de los Consejos de Administración en las empresas concluimos que hay una escasez importante de perfiles tecnológicos. De hecho, debido a que, precisamente, en los ámbitos donde se supervisa y se es responsable de las estrategias de las organizaciones, las visiones de profesionales del ámbito tecnológico no son consideradas, es lógico que haya, de una parte, poco atractivo para estos estudios por no ser medio de desarrollo profesional y, de otra parte, también es lógico que se cumpla la famosa idea de Unamuno de "inventen ellos". Adicionalmente, hay una concepción del ingeniero que es falsa, pero está en el imaginario colectivo, de ser una persona cuadriculada que no ve más allá de los números. Esta concepción hace que no atraiga a las mujeres pues, en general, las mujeres tendemos más a lo social y esta profesión no es concebida como una profesión social.

¿Cree que existe el "techo de cristal" en las empresas TIC? ¿Cuál debería ser la solución?
Evidentemente, en las profesiones que hay mayoritariamente varones se hace difícil hacerte paso. Existe una idea preconcebida que las mujeres, por tener otro estilo de liderazgo, somos menos firmes en lo que a resultados se refiere y, consecuentemente, no somos tan adecuadas para las posiciones de dirección y, aún, es más, se presume que a nosotras no nos satisfacen pues no nos gusta mandar.

¿Una política de cuotas puede resolver el problema?

Veo pros y contras en las cuotas. Los pros son obvios. Las cuotas rompen esa inercia y el circulo vicioso a la hora de alcanzar posiciones de responsabilidad, ya que en las capas altas de una organización los cargos se mueven por confianza y si no llegan las mujeres a ser del grupo de los de confianza difícilmente pueden subir. Los contras, en mi opinión, son que, de una parte, alguna de las mujeres que llegan a responsabilidades de poder no debería de haber llegado (también ocurre con algún varón) y, de otra parte, siempre se genera la duda que las mujeres que han llegado a posiciones de responsabilidad haya sido por la cuota y no por su valía.

¿Qué dificultades se encontró para llegar a la posición que tiene actualmente?
Yo creo que un poco lo que he explicado antes. Se asume que tu estas a gusto en posiciones técnicas, con un horario confortable, sin riesgos, haciendo bien tu trabajo, pero sin grandes sobresaltos, etc. En definitiva, que las mujeres no tenemos ambición de poder en el más noble sentido del término. Sobre esa concepción te tutelan. Recuerdo en una ocasión que había una posición de alto cargo en Marruecos y se la dieron a otro compañero. A mí ni me preguntaron y dieron por supuesto que no me iba a gustar. Al cabo de muy poco tiempo y a propósito de otro tema me dijeron que habían pensado en mí, pero como no iba a querer tuvieron que pensar en otro compañero. Obviamente, les indiqué que la próxima vez prefiero decidir yo por mí a que ellos decidieran por mí

Un 35% de alumnos no logra ni acabar el bachillerato ni la FP equivalente, ¿está en la educación el problema de la falta de perfiles especializados?
En la educación están muchos de los problemas actuales. Los grados han hecho, en mi opinión mucho daño a la ingeniería pues, los grados no son lo suficientemente sólidos como para formar un profesional con visión holística ni estratégica. Son demasiado operativos.
Pensemos, por ejemplo, en la medicina: un traumatólogo tiene una especialidad muy distinta a la de un endocrino, pero ambos tienen una base sólida común que les permite ver al paciente con una visión completa, holística y compartida, sin perjuicio que luego uno lleva a cabo unos actos médicos deferente al del otro.

Con las ingenierías superiores del ámbito de las TIC (6años o 5 años) han pasado a unos grados so excusa de ser prácticos (operativos) que no habilitan a ser realmente ingenieros sino más bien aplicadores de un conocimiento muy parcial. Adicionalmente, habría que cambiar los temarios y contenidos. En mi opinión habría que hacer una sola ingeniería digital o ingeniería TIC donde los 4 primeros años fueran comunes y las especialidades fueran las siguientes, de manera que estas especialidades fueran los actuales masters y que éstos fueran habilitantes. Las especialidades serían: Inteligencia Artificial y Big Data; Ciberseguridad; Conectividad, IoT y Smart cities; Devops, Cloud Computing y Data center.
Adicionalmente, se precisa una Formación Profesional para la gran cantidad de tareas operativas que de ahí surgen.

¿Le han servido los estudios que hizo para realizar su labor actual?
Rotundamente, sí. Los estudios de Ingeniería de Telecomunicación (Master-6 años) eran estudios muy transversales lo que daba una visión amplia muy estratégica y no solo operativa. Esta característica que con los actuales grados se ha perdido es de suma importancia y te posibilita ser un todo terreno.

Solucione el problema de la educación en España...
Ahora se nos vende que todo ha de ser fácil y sin esfuerzo, llegando al absurdo de pasar de curso sin saber. Usted se imagina que para que no se traumatice un estudiante de medicina pudiera pasar de curso sin haber demostrado la pericia necesaria. Piénselo y se contesta uno mismo.

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

"La tecnología principal para LIPSA es el ERP para la parte operativa"

¿A qué están dedicando en la actualidad la parte principal del presupuesto de Lipsa?

Tenemos las partidas habituales dentro de un departamento de IT: Infraestructura, Comunicaciones, Cloud y aplicaciones SAAS, Licencias, Hardware… Además de las partidas, habituales la mayor partida es para el personal y para los proyectos a realizar.

¿En qué área se está invirtiendo más este año?

Se está invirtiendo en renovar y poner al día la infraestructura y comunicaciones, pero la inversión principal actualmente es la migración del ERP de AX a D365 FO.

¿Qué proyecto es del que está más satisfecho?

Desde mi llegada se han gestionado varios proyectos con el objetivo de poner al día los servicios de IT (Infraestructura, comunicaciones, servicio, gestión de la demanda, seguridad...). De los proyectos en los que estoy más satisfecho es con la mejora de comunicaciones y velocidad de acceso a datos y apps, sobretodo en nuestras filiales. Por otro lado, también estoy satisfecho con las mejoras y concienciación de seguridad realizadas.

Aunque en breve, espero poder decir que el proyecto en el que estoy más satisfecho es con el de la migración del actual ERP con las mejoras esperadas.

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

Me gustaría que IT fuera un partner para la empresa, siendo totalmente proactivos y consiguiéndolo a través de la gestión y explotación del dato, integración entre aplicativos y la mejora y eficiencia de procesos a través del ERP, pero también siendo un departamento capaz de gestionar y mejorar cualquier proceso del negocio.

¿La seguridad es un problema?

La seguridad es un riesgo más que ha de gestionar el negocio. Como tal, pienso que la empresa ha de trabajar para estar preparada, para prevenir este riesgo y tener un plan de acción en caso de sufrirlo.

Sabemos que se están publicando muchos ataques, y también hay muchos otros que no se publican, que implican paros totales en las empresas pidiendo

un rescate. Recuperarse de estos ataques es algo complejo: hay que recuperar backups, aislar Servidores, analizar si está infectado ese backup, moverlas a producción cuando estas 100% seguro que ese Servidor es seguro..
El problema principal para el negocio, además del paro en la empresa, solicitud de rescate y situación de crisis que se genera, es que para recuperarse hay que utilizar backups lo que implica:
Días de paro para recuperar y poner en producción el backup, pérdida de datos que conlleva recuperar un backup previo, además que en muchos casos el virus puede haber estado instalado pero sin lanzarse más de un mes lo que implica perder al menos un mes de datos... Rehacer estos datos perdidos suele ser complejo y un completo caos.

¿Qué tendencias principales observa en el mundo TIC?
El mundo tecnológico constantemente está renovando sus tendencias, es un sector en el que hay que estar muy pendiente de las novedades y, sobre todo, ver cual puede encajar en tu empresa. Al final lo principal para cualquier empresa es tener bien configuradas las aplicaciones CORE, ERP pero también aplicativos satélite como PLM, LIMS, .., tener bien integradas los aplicativos, mejorar y automatizar procesos, evolucionar hacia la explotación del dato único y de valor, dar un buen servicio. Hay muchas tendencias actualmente, hay que ver cual aporta valor a tu empresa: cloud, virtualización, pago por uso, blockchain, RPA, data driven, inteligencia artificial, IOT, impresión 3D, metaverso, robótica,… Si he de decantarme por una, actualmente no hay duda, la IA Generativa actualmente es la tendencia principal que todos estamos revisando. Tenemos ChatGPT, Bard, Copilot, … Parece que Microsoft con su solución COPILOT integrada con Azure, O365, ERP, … es la que parece se extenderá más a nivel de empresa debido a que se integra con el PC y todas tus aplicaciones.

Bajo ningún concepto en su móvil puede faltar…
A nivel empresarial Whatsapp, Teams, Google maps y correo electrónico. A nivel personal tengo aplicaciones para todo prácticamente: bancos, diarios, redes sociales, ..

¿Cuál es la herramienta que realmente le cambió la vida?
Evidentemente, en mi caso la aparición y evolución de internet. Recuerdo que no hace tanto nos conectábamos con un modem cortando la línea telefónica…

¿Harto de solucionar los problemas tecnológicos de la familia y amigos? ¿Qué le suelen pedir?
La verdad es que no me piden demasiado, principalmente mis padres con el wifi o móvil. Los amigos suelen pedirme consejo antes de hacer una compra tecnológica.

Lo de extraer el valor del dato, ¿supondrá de verdad la evolución de empresas como la suya?
Actualmente ya estamos habituados explotar los datos y trabajar sobre éstos, sobretodo del ERP. Con la migración del ERP estamos preparando un datawarehouse a través del que integraremos datos del resto de Aplicativos que vamos a implementar.
En otras empresas, hemos implementado cuadros de mando de procesos, creo que seria el siguiente paso.

Sergio Castillo Capote, CIO en LIPSA

¿Qué es eso de la transformación digital? ¿Slogan o necesidad?
Considero que en algunos momentos puede haberse considerado un slogan, debido a que engloba prácticamente cualquier solución tecnológica. Sin embargo, considero que es una necesidad para cualquier empresa ya, bien aplicada, conlleva la mejora o transformación de procesos empresariales, evitando el "siempre se ha hecho así".
Me gustaría añadir, que las nuevas generaciones han nacido digitales y llevan integrado el chip de transformación digital, con esta generación hay que prestar prácticamente más atención a la gestión del cambio que a la solución en sí.

¿En la nube u on-premise?
Ambas opciones tienen pros/contras, hay que ver que encaja mejor según la necesidad.
Por ello, en mi opinión entornos híbridos, es decir la combinación de ambos. Aunque es cierto que las empresas nativas apuestan prácticamente todas por entornos 100% en la nube.

¿Como ayuda la tecnología a conseguir los mejores aceites?
La tecnología ayuda en todos los procesos, desde la generación del pedido del cliente hasta que el producto sale de LIPSA: gestión, trazabilidad, automatización, ciberseguridad,...
La tecnología principal para LIPSA es el ERP para la parte operativa y para la planta, los sistemas MES y Scada.

Claves de la normativa europea sobre Inteligencia Artificial

Aunque la preocupación por regular la Inteligencia Artificial (IA) viene de años atrás, fue en agosto de 2023 cuando empezaron a saltar las alarmas cuando "Ameca" (un androide robótico creado por la empresa Engineered Arts en Falmouth, Cornwall, UK) se declaró autoconsciente, lo que le permitiría entender su realidad, reconocerse a sí mismo y tener una personalidad específica.

En la Unión Europea existe una creciente preocupación sobre un desmedido impulso de la IA sin control ni límites, al tiempo que no quiere quedarse atrás en su competencia con China y USA, que se muestran mucho más permisivos con esta tecnología. Inicialmente, la cuestión pareció haber sido arbitrada por la posición salomónica defendida por Japón en la reunión del G7 de octubre de 2023 (la del foro intergubernamental "Proceso de Hirosima"), partidario de fijar un Código de Conducta para la IA que no impida su progreso, al tiempo que ponga límites en materia de propiedad intelectual y datos personales.

Respecto a la normativa de europea sobre IA, debido al retraso en la aprobación del Reglamento de IA, se han promulgado algunas normas que pivotan sobre dos conceptos fundamentales: nivel de riesgo y evitar sesgos discriminatorios. Así, el pasado mes de noviembre de 2023 se publicaron las cláusulas estándar (de dos tipos en función del nivel de riesgo de la IA) que deberán usarse para la adquisición por las Administraciones Públicas de sistemas que integren elementos de IA y otros sistemas algorítmicos que no se consideren necesariamente IA; de aplicación potestativa en lo que se aprueba el Reglamento, sin perjuicio de que se recomienda su inmediata utilización.

Los aspectos más conflictivos de la normativa europea sobre IA han sido el propio concepto de IA –que

finalmente se ha aproximado a los principios de flexibilidad marcados en 2019 por la Organización para la Cooperación y Desarrollo Económico (OCDE), basados en la privacidad, gestión de riesgos de seguridad digital y conducta empresarial responsable, para facilitar futuras negociaciones con USA y UK)–, definir los sistemas de IA prohibidos, los requisitos para los modelos fundacionales que sirven de base a los sistemas de IA generativa y el respeto a los derechos de propiedad intelectual, los sistemas de reconocimiento facial en tiempo real en espacios públicos, el control de los sistemas de alto riesgo y el procedimiento sancionador.

Las aplicaciones prohibidas de la IA son las siguientes: (i) categorización biométrica que use características sensibles de personas (ideología política, creencias religiosas o filosóficas, orientación sexual, raza, etc.); (ii) vigilancia predictiva; (iii) extracción no dirigida de imágenes faciales de Internet o imágenes de Circuito Cerrado de Televisión (CCTV) para crear bases de datos de reconocimiento facial; (iv) reconocimiento de emociones en el lugar de trabajo o en instituciones educativas; (v) puntuación basada en el comportamiento social o en características personales; (vi) manipulación del comportamiento humano para eludir su libre albedrío; y (vii) explotación de vulnerabilidades de las personas (por su edad, discapacidad, situación social o económica, etc.).

La normativa europea sobre IA no se aplicará a aquella que se emplee para fines de defensa, con fines exclusivos de investigación e innovación, ni a las personas que la usen por motivos no profesionales. Sin embargo, en el ámbito policial, se ha restringido el uso de los sistemas de identificación biométrica (RBI) en espacios públicos a una reducida lista de delitos de especial gravedad (tales como asesinato, secuestro, violación, robo con armas, participación en organización criminal, delitos medioambientales, trata o explotación sexual, o amenaza terrorista específica y presente), en tiempo y ubicación limitado, y contando con autorización judicial previa.

Siguiendo la línea marcada, la normativa es más estricta en función del riesgo, prestando especial atención a los sistemas de alto riesgo, capaces de generar daños a la salud, la seguridad, los derechos fundamentales, el medio ambiente, la democracia y el Estado de derecho, como los usados para influir en procesos electorales y en la voluntad de los votantes; así como a los sistemas de riesgo sistémico, que son los que utilizan una potencia de cálculo igual o superior a 10 elevado a 26 FLOPS (operaciones de coma flotante) por segundo, como sería el caso de ChatGPT-4.

Sobre los derechos de propiedad intelectual, se regula una de las cuestiones más polémicas, como es la convivencia del desarrollo de la IA y los derechos de propiedad intelectual de los autores de las obras que usa para su aprendizaje. En este sentido, se establece que los sistemas GPAI y modelos en los que se basan tendrán que cumplir requisitos de transparencia como la elaboración de documentación técnica, el cumplimiento de la normativa de la Unión Europea sobre derechos de autor y la difusión de resúmenes detallados sobre el contenido usado en la formación.

Respecto a los órganos de gobernanza, se crean la "AI Office", que será asesorada por un científicos y expertos independientes, y se ocupará de supervisar los modelos de IA más avanzados, contribuir a fomentar normas y prácticas de ensayo y hacer cumplir las normas comunes en todos los Estados de la Unión Europea; el "AI Board", compuesto por representantes de los Estados miembros, como plataforma de coordinación y órgano consultivo de la Comisión; y un foro consultivo para las partes interesadas ("Advisory forum for stakeholders"), integrado por representantes de empresas, de asociaciones civiles y de académicos.

En cuanto al régimen sancionador por el incumplimiento de las normas recogidas en el Reglamento, se establecen unas multas que pretenden ser disuasorias, y que oscilan entre los 7.500.000 de euros o el 1,5% del volumen de negocios global, hasta los 35.000.000 de euros o el 7% del volumen de negocios global, en función de la infracción cometida y el tamaño de la empresa responsable.

Además de la normativa de control, y con la vista puesta en el objetivo de no perder competitividad con chinos y norteamericanos, se adoptarán medidas de apoyo a la innovación para que las empresas (en particular las PYMES y startups que quieran hacerlo al margen de las grandes tecnológicas), puedan desarrollar soluciones en entornos de pruebas controlados, establecidos por las autoridades nacionales para desarrollar y entrenar la IA antes de su comercialización.

Javier López
socio de Écija Abogados

El fin del firewall independiente

HPE ha revelado las principales tendencias de networking que los líderes tecnológicos y empresariales deberían tener en cuenta a lo largo de 2024. David Hughes, Senior Vice President and Chief Product and Technology Officer de HPE Aruba Networking, ofrece su visión sobre lo que traerá el próximo año.

PREDICCIÓN 1. EL FIN DEL FIREWALL INDEPENDIENTE

El surgimiento de la fuerza laboral híbrida y la proliferación de dispositivos IoT han erosionado irremediablemente el concepto de un perímetro de red definido, llevando a la gradual desaparición de los firewalls independientes. La estrategia de proteger un entorno «interno» frente a uno «externo» mediante un anillo de firewalls ya no es viable, ya que aumenta la complejidad y obstaculiza la agilidad empresarial. Los firewalls de próxima generación están quedando rápidamente desactualizados, siendo reemplazados por el Extremo de Servicios de Seguridad (SSE en sus siglas en inglés), que utiliza una pasarela web segura desde la nube, un agente de seguridad de acceso a la nube y adopta el modelo Zero Trust para el acceso a la red. Además, en el ámbito de la seguridad de IoT, se busca la segmentación local en el extremo de la red, integrando servicios de firewall directamente en puntos de acceso, conmutadores y pasarelas SD-WAN. Incluso en el centro de datos, la implementación de conmutadores Top of Rack con funciones de seguridad L4-7 ofrece una segmentación este-oeste más rentable que los firewalls de próxima generación convencionales. En los próximos años, el mercado de firewalls de próxima generación continuará decreciendo a medida que las soluciones integradas basadas en la nube simplifiquen la gestión segura de la conectividad.

Según Gartner, a medida que más organizaciones eligen estrategias de trabajo híbridas y programáticas, es más probable que los compradores seleccionen proveedores de firewall que ofrezcan servicios de seguridad basados en la nube con estrategias creíbles de seguridad en la nube. Gartner Critical Capabilities for Network Firewalls (Adam Hils, Rajpreet Kaur, Thomas Lintemuth) 16 de mayo de 2023

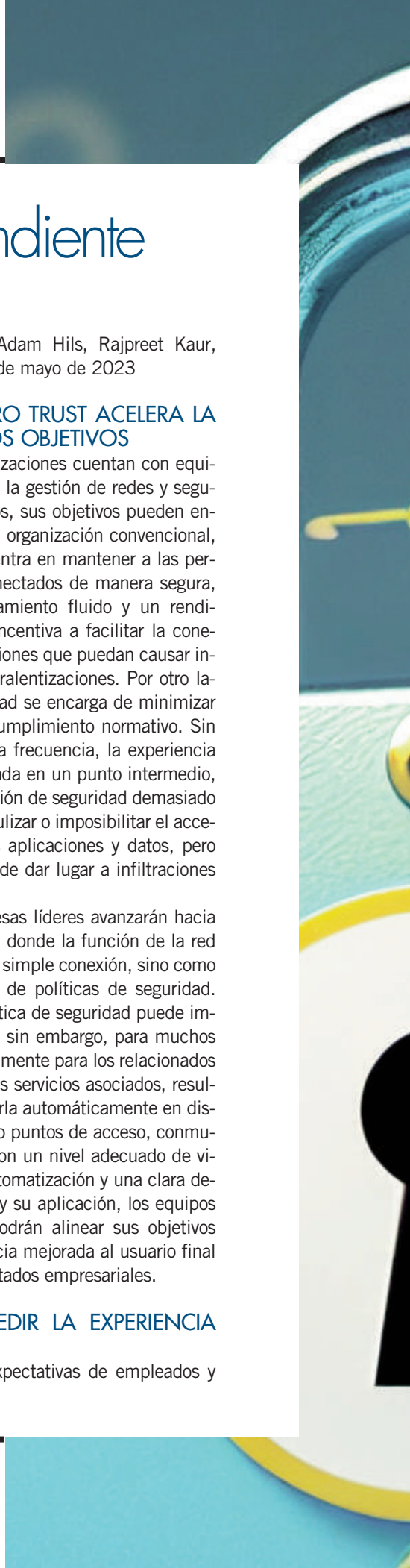
PREDICCIÓN 2. ZERO TRUST ACELERA LA ALINEACIÓN DE LOS OBJETIVOS

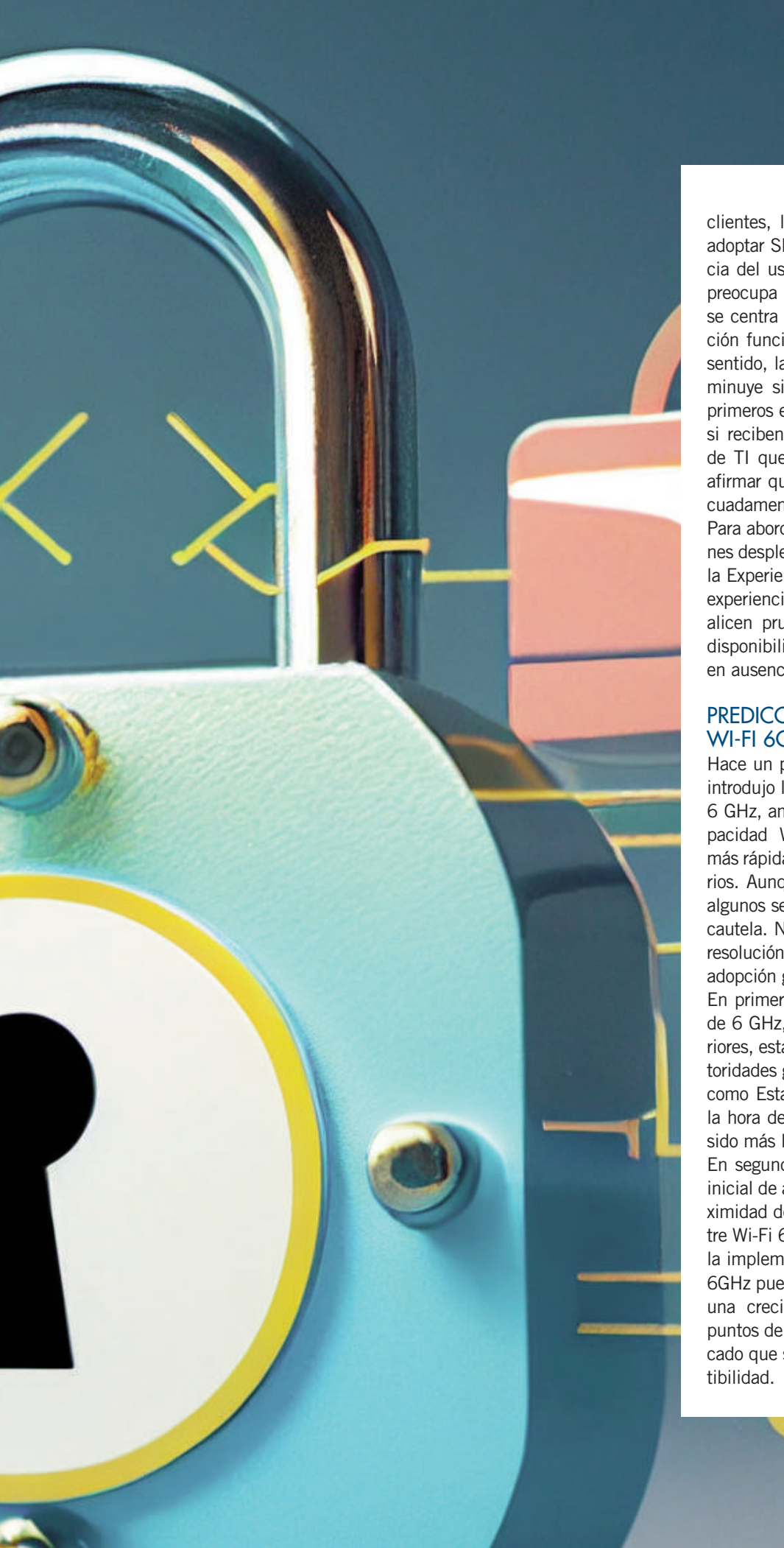
La mayoría de las organizaciones cuentan con equipos independientes para la gestión de redes y seguridad, y en muchos casos, sus objetivos pueden entrar en conflicto. En una organización convencional, el equipo de redes se centra en mantener a las personas y los servicios conectados de manera segura, asegurando un funcionamiento fluido y un rendimiento óptimo. Se les incentiva a facilitar la conexión y a evitar complicaciones que puedan causar interrupciones, latencia o ralentizaciones. Por otro lado, el equipo de seguridad se encarga de minimizar riesgos y garantizar el cumplimiento normativo. Sin embargo, con demasiada frecuencia, la experiencia del usuario queda atrapada en un punto intermedio, ya que una implementación de seguridad demasiado entusiasta puede obstaculizar o imposibilitar el acceso de los usuarios a las aplicaciones y datos, pero una demasiado laxa puede dar lugar a infiltraciones y diferentes amenazas.

Así, en 2024, las empresas líderes avanzarán hacia arquitecturas Zero Trust, donde la función de la red se redefine no como una simple conexión, sino como una capa de aplicación de políticas de seguridad. Para los usuarios, la política de seguridad puede implementarse en la nube; sin embargo, para muchos flujos de tráfico, especialmente para los relacionados con dispositivos IoT y sus servicios asociados, resultará más eficiente aplicarla automáticamente en dispositivos de acceso como puntos de acceso, conmutadores y enrutadores. Con un nivel adecuado de visibilidad compartida, automatización y una clara delimitación de la política y su aplicación, los equipos de redes y seguridad podrán alinear sus objetivos ofreciendo una experiencia mejorada al usuario final y logrando mejores resultados empresariales.

PREDICCIÓN 3. MEDIR LA EXPERIENCIA DEL USUARIO

Para cumplir con las expectativas de empleados y





clientes, las organizaciones de TI deberán adoptar SLO y SLA basados en la experiencia del usuario. A los consumidores no les preocupa la causa de un fallo; su atención se centra en algo muy simple: si la aplicación funciona correctamente o no. En este sentido, la satisfacción de los usuarios disminuye significativamente cuando son los primeros en identificar problemas, más aún si reciben notificaciones del departamento de TI que contradicen sus experiencias al afirmar que los dispositivos funcionan adecuadamente.

Para abordar esta situación, las organizaciones desplegarán herramientas de Gestión de la Experiencia Digital (DEM) que evalúen la experiencia real de los usuarios finales y realicen pruebas sintéticas para asegurar la disponibilidad de la infraestructura, incluso en ausencia de los usuarios.

PREDICCIÓN 4. LA ADOPCIÓN DE WI-FI 6GHZ

Hace un par de años, el estándar Wi-Fi 6E introdujo la compatibilidad con la banda de 6 GHz, ampliando significativamente la capacidad Wi-Fi y permitiendo velocidades más rápidas para un mayor número de usuarios. Aunque su adopción ha sido veloz en algunos sectores, otros han mostrado mayor cautela. No obstante, en 2024, se prevé la resolución de los últimos obstáculos para su adopción generalizada.

En primer lugar, el despliegue de la banda de 6 GHz, especialmente en entornos exteriores, está sujeto a la aprobación de las autoridades gubernamentales. Algunos países, como Estados Unidos, han sido pioneros a la hora de abrir el espectro, pero otros han sido más lentos.

En segundo lugar, a pesar de la reticencia inicial de algunas empresas debido a la proximidad de Wi-Fi 7, la interoperabilidad entre Wi-Fi 6E y Wi-Fi 7 está garantizada. Así, la implementación de Wi-Fi en la banda de 6GHz puede avanzar muy rápidamente, con una creciente cantidad de dispositivos y puntos de acceso 6E disponibles en el mercado que superan las barreras de la compatibilidad.

La gestión del dato no será posible sin la IA

La IA destaca como la tecnología disruptiva más significativa del año, y se espera que en 2024 continúe expandiendo su influencia y capacidad en diversas áreas, como es el caso de la protección y gestión de datos. En relación a ello, Commvault ha identificado las tendencias predominantes en el mercado de gestión de datos para empresas en el próximo año, muchas de las cuales están impulsadas por los avances en esta tecnología.La IA está cambiando la perspectiva de los CISO y CIO. A lo largo de los años, las organizaciones han empleado la IA para extraer mayor valor e información de los datos, y en términos de seguridad de datos, han confiado en tecnologías de IA y aprendizaje automático para detectar anomalías en los datos de respaldo que podrían señalar posibles amenazas.

Sin embargo, el panorama de los ataques está evolucionando rápidamente, impulsado en parte por la creciente cantidad de ataques impulsados por IA. En este contexto, la IA jugará un papel crucial en la identificación y mitigación de ciberamenazas, lo que requerirá que las organizaciones adopten un enfoque estratégico para la respuesta y recuperación de incidentes.

INTELIGENCIA DE DATOS

La gestión de inteligencia de datos será una prioridad ejecutiva en 2024. Las empresas están tomando conciencia y adoptando medidas para manejar sus datos como activos fundamentales. Al igual que con cualquier activo, la eficaz administración de estos será esencial para fortalecer la ciberseguridad, garantizar la continuidad del negocio y mejorar la oferta de servicios.

En un contexto donde se prevé que las organizaciones deban gestionar el doble de datos no estructurados en 2024, la capacidad de una empresa para capitalizar la inteligencia de datos y recuperarse rápidamente se convertirá en una ventaja competitiva crucial, liberando recursos valiosos para poner esos datos en acción.

MAYOR COMPROMISO A NIVEL DIRECTIVO

En 2024, los miembros de los consejos de administración prestarán una atención más aguda a la identificación de los riesgos empresariales, centrándose especialmente en las decisiones relacionadas con la gestión de riesgos. Según IDC, solo el 33% de los altos ejecutivos están actualmente involucrados en iniciativas de preparación cibernética, a pesar de que el 61% de estos líderes creen que su negocio podría ser afectado por un ataque en los próximos 12 meses.

En este contexto, se espera que las juntas directivas demanden un compromiso mayor por parte de los altos ejecutivos para garantizar que las organizaciones aborden de manera integral su postura de seguridad, abarcando desde la detección hasta la protección y la recuperación.

NUEVAS AMENAZAS

En 2024, veremos cómo los ciberdelincuentes utilizarán el descubrimiento de activos y el análisis de vulnerabilidades en una amplia gama de activos diversos con el fin de perpetrar ataques. A diferencia de las empresas, que utilizan esta información para protegerse, los atacantes priorizarán y explotarán las vulnerabilidades que maximicen el impacto con el mínimo esfuerzo, aprovechando las mismas herramientas avanzadas y los análisis basados en IA que suelen utilizarse para defender los datos. Los atacantes podrán incluso llegar a ejecutar modelos predictivos para comprender el grado de impacto o descubrir nuevos parámetros y técnicas que lleven a crear una nueva amenaza emergente.

LOS DATOS COMO PRIORIDAD

Los datos representan un activo crucial para cualquier empresa, y su protección, especialmente en un entorno donde surgen constantemente nuevas amenazas, se ha convertido y continuará siendo una prioridad estratégica. En el año 2024, la capacidad para

identificar y responder de manera ágil a las ciberamenazas será un factor distintivo en la competencia empresarial. Aquellas empresas que se enfoquen en la resiliencia cibernética, abarcando la protección de datos, la seguridad de datos, la inteligencia de datos y la recuperación, estarán mejor posicionadas. Dada la creciente sofisticación de las amenazas cibernéticas, será crucial adoptar avances en tecnologías y estrategias de seguridad de datos impulsadas por la inteligencia artificial. Las empresas que se adapten con rapidez probablemente se destacarán en la industria, ganando la confianza tanto de los consumidores como del público en general.

ADQUISICI N DE TALENTO

La adquisición y desarrollo de talento surgirán como desafíos significativos en el manejo de datos. Dado que el talento siempre es un recurso escaso, resultará fundamental para implementar, mantener y gestionar sistemas de manera efectiva, asegurando que estos sean un activo valioso en lugar de un pasivo. Además, la supervisión humana seguirá siendo esencial. En consecuencia, las empresas deberán priorizar la formación continua y la actualización de conocimientos para asegurar que sus equipos puedan aprovechar al máximo las tecnologías, incluyendo la inteligencia artificial, al mismo tiempo que mantienen una supervisión atenta sobre los sistemas.

COLABORACIÓN ENTRE EQUIPOS

La colaboración entre los equipos de ITOps y SecOps seguirá evolucionando en 2024. Tiene que hacerlo, ya que cualquier empresa que continúe operando en silos se encontrará en una seria desventaja cuando sea atacada. Las empresas deben pensar en la preparación cibernética a través de todo el marco NIST, incluyendo la identificación, protección, detección, respuesta y, si es necesario, la recuperación de los ataques. Esto debe implicar una estrecha colaboración entre los equipos de TI y de seguridad, que es algo que ya hemos observado en los últimos 12 meses.

¿Estamos ganando la lucha contra el ransomware?

El ransomware se convirtió en la principal arma de los ciberdelincuentes en 2020. Desde entonces, ha ocupado un lugar destacado en la agenda de la seguridad mundial, asolando a empresas, servicios públicos y particulares por igual. Las organizaciones han tenido que reorientar rápidamente sus estrategias de ciberseguridad, protección de datos y recuperación ante desastres para adaptarse a esta nueva pandemia. Pero, ¿está cambiando la situación?

Los datos sugieren que en 2022 el número global de ataques de ransomware se redujo significativamente (después de haberse duplicado en 2021) y el análisis de la empresa de blockchain Chainalysis informa que el valor total de los rescates de ransomware pagados en 2022 también se redujo significativamente, ambos signos positivos de que el ransomware global se está desacelerando.

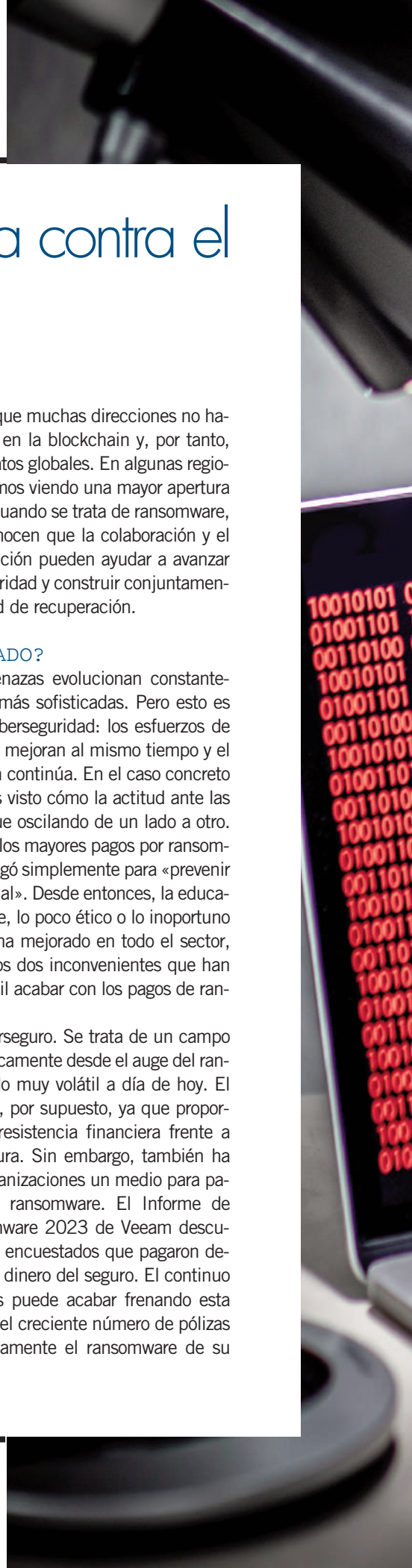
Sin embargo, los informes Veeam Data Protection Trends Report 2023 y Ransomware Trends Report 2023, encuestas a gran escala a organizaciones imparciales de EMEA, América y APJ, pintan un panorama diferente. El primer informe reveló que el 85% de las organizaciones sufrieron al menos un ciberataque durante el año pasado (un aumento del 9% con respecto al año anterior) y el informe sobre ransomware, que encuestó exclusivamente a empresas que habían sufrido un ataque, mostró que un sorprendente 80% de las empresas habían pagado un rescate para recuperar sus datos. Otras encuestas del sector suelen arrojar resultados similares, así que ¿por qué hay una desconexión entre las cifras globales totales y lo que dice la mayoría de las empresas individuales?

Mientras que las encuestas específicas pueden darnos una valiosa medida del estado de una determinada región o industria, las cifras globales totales son complicadas. Naturalmente, la escala es un factor, pero cuando se trata de ransomware puede haber reticencia a admitir haber sufrido una brecha de datos y algunas pólizas de seguros impiden directamente a las empresas hacerlo. El seguimiento de los pagos tampoco es una ciencia exacta, ya que muchas direcciones no habrán sido identificadas en la blockchain y, por tanto, no dispondrán de los datos globales. En algunas regiones, como EMEA, estamos viendo una mayor apertura a la hora de compartir cuando se trata de ransomware, ya que los líderes reconocen que la colaboración y el intercambio de información pueden ayudar a avanzar a la industria de la seguridad y construir conjuntamente una mayor capacidad de recuperación.

¿QU HA CAMBIADO?

Naturalmente, las amenazas evolucionan constantemente y son cada vez más sofisticadas. Pero esto es fundamental para la ciberseguridad: los esfuerzos de protección y resistencia mejoran al mismo tiempo y el juego del gato y el ratón continúa. En el caso concreto del ransomware, hemos visto cómo la actitud ante las exigencias de pago sigue oscilando de un lado a otro. Hace dos años, uno de los mayores pagos por ransomware de la historia se pagó simplemente para «prevenir cualquier riesgo potencial». Desde entonces, la educación sobre lo poco fiable, lo poco ético o lo inoportuno que es esta estrategia ha mejorado en todo el sector, pero han aparecido otros dos inconvenientes que han hecho mucho más difícil acabar con los pagos de ransomware para siempre.

Uno de ellos es el ciberseguro. Se trata de un campo que ha cambiado drásticamente desde el auge del ransomware, y sigue siendo muy volátil a día de hoy. El ciberseguro no es malo, por supuesto, ya que proporciona a las empresas resistencia financiera frente a una amenaza casi segura. Sin embargo, también ha proporcionado a las organizaciones un medio para pagar las demandas del ransomware. El Informe de Tendencias de Ransomware 2023 de Veeam descubrió que el 77% de los encuestados que pagaron demandas lo hicieron con dinero del seguro. El continuo aumento de las primas puede acabar frenando esta tendencia, al igual que el creciente número de pólizas que excluyen específicamente el ransomware de su cobertura.



Tal vez el factor más importante, y la razón por la que las empresas sienten que no tienen más remedio que pagar rescates en primer lugar, son los ataques dirigidos cada vez más a los repositorios de copias de seguridad. Informes recientes revelan que los ciberdelincuentes fueron capaces de afectar a los repositorios de copias de seguridad en tres de cada cuatro ataques. Si las empresas no disponen de otras copias externas de estos datos o simplemente no están en condiciones de recuperarlos con la suficiente rapidez, puede ser tentador para la junta directiva optar por ceder a las demandas.

¿QUÉ QUEDA POR HACER?

¿Qué tiene que cambiar para inclinar la balanza en la lucha contra el ransomware y que empecemos a ver cómo los ataques y los pagos se reducen definitivamente? Todo se reduce a la educación y la preparación, sobre todo para los que no pertenecen a los equipos de seguridad y backup. Esto incluye acabar con los mitos sobre lo que ocurre antes y después de un ataque de ransomware.

Entender a la bestia es el primer paso para estar preparados y poder responder. Un plan de recuperación de ransomware debe tener tres etapas:

1. Preparación – planificar la recuperación, asegurarse de que se dispone de copias de seguridad fiables (siguiendo al menos la regla 3-2-1), disponer de una ubicación de recuperación en caso de catástrofe preparada y lista para funcionar, e intensificar la formación y los ejercicios para garantizar que la empresa y la organización están preparadas.
2. Respuesta – Siguiendo un proceso de respuesta a incidentes predefinido y probado, localizar y contener la brecha, y escanear las copias de seguridad para asegurarse de que no están contaminadas.
3. Recuperación – Recuperar el entorno sin reintroducir el malware o los datos ciber-infectados en el entorno de producción durante la restauración y conseguir que la empresa vuelva a funcionar.

Edwin Weijdema, Field CTO EMEA and Lead Cybersecurity Technologist en Veeam

ALBERTO PINEDO, NATIONAL TECHNOLOGY OFFICER DE MICROSOFT

"Microsoft puede bloquear 4.000 ataques de identidad por segundo"

Entrevistamos a una de las principales voces del panorama de la ciberseguridad actual, Alberto Pinedo, National Technology Officer de Microsoft, que desgranará cuál es la situación actual de las organizaciones en torno a la ciberseguridad. **Por Manuel Navarro**

¿Cuál es el estado de la ciberseguridad en las empresas?
Las ciberamenazas han crecido no solamente en España, sino a nivel global. De alguna forma, esto ha mermado la confianza en la tecnología y ha puesto de relieve la necesidad de mejorar las ciberdefensas a todos los niveles. La buena noticia es que hay un interés creciente en mejorar la seguridad y sobre todo lo que vemos en Microsoft es una mayor colaboración entre lo que se ha venido a denominar el sector público y sector privado. Para entender esa necesidad de colaboración es necesario comprender el concepto de ciberpobreza, que es saber cuál es el nivel mínimo de recursos que hay que tener para conseguir una protección adecuada frente a las ciberamenazas. Nos estamos encontrando con muchas medianas y pequeñas empresas que nos están preguntando qué es lo mínimo que tienen que tener para subsistir en este mundo de ciberamenazas y cómo les podemos ayudar desde Microsoft.

¿Y cómo les ayudan?
Justamente ahora estamos trabajando con diferentes actores a nivel nacional para proponer líneas de colaboración al gobierno que permitan ayudar a aquellas empresas que lo necesitan y que están por debajo del umbral de ciberpobreza. Y ahí tenemos una serie de activos y una posición muy buena, porque analizamos cerca de 65 billones de señales diarias. Esto son unas 750 millones de señales por segundo lo que nos ofrece una visión muy precisa de lo que pasa en el mundo, sobre todo gracias a esos más de 10 000 analistas que tenemos, pero también gracias al uso de la inteligencia artificial. Todo ello, tal y como se explica en el informe Digital Defense Report 2023, nos permite bloquear alrededor de 4.000 ataques de identidad por segundo y controlar a cerca de 300 grupos de ciberdelincuentes.

¿Cómo están afrontando las empresas los retos derivados de la ciberseguridad?
Es cierto que muchas no tienen definida una estrategia de ciberseguridad y funcionan en modo de silos. Y nos encontramos con numerosas empresas que piensan que con un antivirus o con simular campañas de phising es suficiente. Otras tienen un nivel de madurez mucho más alto y lo que buscan es tener una postura de seguridad más completa y entonces te permiten o incorporan herramientas para la protección de la identidad, para la protección del dispositivo o para la protección de la información.
Por otro lado, la ciberseguridad, quizás por lo compleja que es, no está tan interiorizada en algunas empresas como ocurrir con otras tecnologías.

El informe asegura que las empresas se pueden proteger del 99% de los ciberataques. ¿Cómo nos protegemos en ese 99%?¿Qué sucede con el 1% restante?
Hay varias líneas básicas en la protección. Una es el establecimiento de una estrategia zero-trust. Es decir, verificación explícita, mínimos privilegios y resolución de brecha en los sistemas. A partir de ahí, lo más importante o lo que primero recomendamos es la protección de la identidad con sistemas de autenticación multifactor y luego pensar sobre todo en un buen sistema de detección y respuesta que contenga también la parte de antimalware.
Otra línea importante es tener los sistemas actualizados porque muchos de los ataques vienen por vulnerabilidades no parcheadas. Y finalmente, también es necesario tener un sistema de protección del dato allí donde esté el dato. Teniendo en cuenta estos cinco elementos, lo que dice el informe es que se cubrir el 99% de los casos de ciberataque.
El 1% restante se corresponde con ataques más complejos y también nos podemos proteger. Lo que sucede es que lo que en el informe se quiere destacar es con unos umbrales mínimos de protección, se pueden cubrir el 99% de las amenazas.

Evidentemente el ransomware es la mayor preocupación de todas las empresas. Cada vez ha evolucionando más. El estudio afirma que desde marzo- abril han empezado a reducirse los ciberataques. ¿Por qué?
Yo creo que es una combinación de varias cosas. Una de ellas por ejemplo, es que en Microsoft tenemos una Ransomware Tax For con la que vamos a donde más les duele a los ciberatacantes que es al apartado económico. Desde la Digital Crime Unit, la unidad de delitos digitales de Microsoft, lo que hemos hecho ha sido apostar por una estrategia que va dirigida al entorno financiero de los atacantes. Y al final el modelo penal de que tenemos es muy sencillo: cuando detectamos un ataque de ransomware o un cliente nos contacta denunciando un ataque de ransomware, nos ponemos en coordinación con la Alianza Nacional de Ciberforensica y Formación y con las autoridades locales con el objetivo de analizar el monedero virtual que se haya identificado para realizar el pago. Se analizan los detalles de comunicación, se hace un seguimiento en coordinación con las fuerzas y seguridad del Estado, se bloquea dicho monedero tras el pago acordado para retornar de forma legal el dinero a la víctima y se actúa para perseguir a los ciberdelincuentes y arrestarlos.
Otros factores para el descenso es que también ha cambiado el modelo de ransomware. Antes el modelo era bueno: se intentaba colocar un fichero para luego desplegar todo el cifrado y ahora los ataques son más en remoto y con lo cual las técnicas también varían. Además, las protecciones de los accesos remotos han madurado mucho.

Un **reglamento europeo** para la IA

José Joaquín Flechoso,
presidente de Cibercotizante.

La reciente normativa sobre IA aprobada en la UE, ha sido la gran noticia de los últimos días, que buscaba protagonismo en las portadas de los informativos del puente de la Constitución donde la gran noticia eran las grandes aglomeraciones navideñas.

Por parte de España, la Secretaría de Estado de Digitalización e IA, responsable de la parte internacional y europea, tenía como objetivo sacar adelante una normativa sobre IA, como uno de los grandes hitos de la Presidencia española de turno del Consejo de la UE.

Si bien es en el último año cuando se ha acelerado la búsqueda de un texto legal que regulase la IA, podemos remontarnos a 2019 como fecha de comienzo de todo el proceso, cuando algunos expertos desarrollaron una especie de guía en la que participaron muchas empresas españolas. Situados en 2020 y ya con el libro blanco aprobado, fue definiéndose un marco normativo.

En esta negociación previa, tanto la Comisión Europea como el Parlamento Europeo fueron actores de primer nivel e incluso a veces con posiciones un tanto alejadas en sus enfoques, para abordar la regulación de la IA.

La aparición un año antes de ChatGPT, ha dado un vuelco a las negociaciones y ha hecho que se acelerase todo y se empezase a hablar de los sistemas de alto riesgo en relación a la IA. Había que buscar un punto intermedio, porque si no salía con nuestra presidencia, sería imposible hacerlo, porque estamos a meses vista de las próximas elecciones al Parlamento Europeo, si bien subyacía el fuerte compromiso para que todo saliera y saliera bien…..

Las negociaciones fueron duras, sobre todo por lo complejo de algunos episodios como aquellos definidos para regular los sistemas de propósito general, donde se estuvo negociando hasta siete horas de forma ininterrumpida.

En cuanto a la forma legislativa, se ha optado por darle naturaleza de Reglamento, para que sea de aplicación en todos los estados miembros, para evitar que se hagan reglamentos en cada país y evitar una fragmentación que afecte a una regulación del mercado interior.

Ha incidido en la elaboración del Reglamento el hecho de haber promovido nuestro país la Carta de los Derechos Digitales, donde España ha tenido un liderazgo clave para hablar de una transformación digital humanista para empoderar a los ciudadanos. Es importante destacar que hay disposiciones incluidas en el Reglamento, para que siempre haya una supervisión humana, dando así garantías de que nunca serán las maquinas las que decidan.

Sobre el punto controvertido del reconocimiento biométrico, ha habido una negociación dura para aprobar que los sistemas biométricos sean utilizados por las fuerzas de seguridad, combinando la seguridad pública, protegiendo siempre los derechos fundamentales de los ciudadanos.

El Reglamento busca el equilibrio entre la innovación y la protección, teniendo garantías validadas por la agencia de supervisión nacional de IA de cada país, para que la innovación respete siempre los derechos fundamentales.

Esperemos que este Reglamento dé confianza a empresas y ciudadanos en relación con el uso de la IA, acabando con tanta desinformación como recibimos.

TECHbyte

LA VOZ DE LA TECNOLOGÍA PARA LA EMPRESA

LA MEJOR INFORMACIÓN Y LAS ÚLTIMAS TENDENCIAS EN TECNOLOGÍA E INNOVACIÓN

¡AHORA TAMBIÉN EN LA RADIO!

ESCÚCHANOS EL PENÚLTIMO MARTES DE CADA MES, DE 10 A 11 AM EN CAPITAL RADIO

TECHbyte EN capitalradio

PUEDES ESCUCHARNOS EN

www.revistabyte.es - www.capitalradio.es - o en plataformas de Streaming

Madrid **103.2 FM** - Sevilla **92.5 FM** - Tenerife **97.2 FM / 94.0 FM**

Barracuda

Enséñale los dientes al ransomware.

OBTÉN LA DEFENSA MÁS FEROZ CONTRA AMENAZAS COMPLEJAS.