it Digital MAGAZINE

Nº 9 · OCTUBRE 2023

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

it Reseller TECH&CONSULTING

MERCADO PC: LA INESTABILIDAD DE UN NEGOCIO CLÁSICO

it User TECH & BUSINESS

TECNOLOGÍAS CONECTADAS PARA CIUDADES INTELIGENTES

it Digital Security

DATOS E IDENTIDADES: EL CENTRO DE GRAVEDAD PARA UNA ESTRATEGIA DE SEGURIDAD GLOBAL

ENTREVISTA A ESTHER MATEO, DIRECTORA GENERAL DE SEGURIDAD, PROCESOS Y SISTEMAS CORPORATIVOS DE ADIF

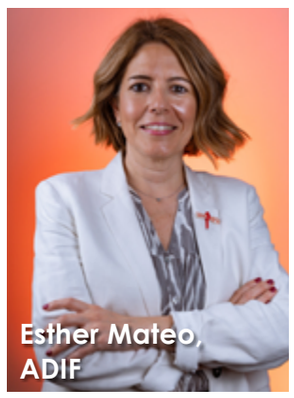
#CONTENIDOS IT

TECNOLOGÍAS CONECTADAS PARA CIUDADES INTELIGENTES

MERCADO PC: LA INESTABILIDAD DE UN NEGOCIO CLÁSICO

DATOS E IDENTIDADES: EL CENTRO DE GRAVEDAD PARA UNA ESTRATEGIA DE SEGURIDAD GLOBAL

ENTREVISTAS



Esther Mateo, ADIF

Tomás Concha, CTT

José Battat, Trend Micro

Raúl Guillén, Trend Micro

ACTUALIDAD

NO SOLO IT

ÍNDICE DE ANUNCIANTES

it Digital MAGAZINE

Nº 9 · OCTUBRE 2023

TENDENCIAS

>> Crece la adopción de modelos cloud híbridos en los servicios financieros

>> La mitad de los empleados trabajarán de manera híbrida o remota en el futuro

REVISTAS DIGITALES

it Digital MAGAZINE

Nº 9 - OCTUBRE 2023

Director
Pablo García Reales
pablo.garcia@itdmgroup.es
Redacción y colaboradores
Hilda Gómez, Reyes Alonso,
Ricardo Gómez, Alberto Varet
Diseño revistas digitales
Eva Herrero
Producción audiovisual
Miss Wallace, Alberto Varet
Fotografía
Mayte Madariaga, Ania Lewandowska

it Digital MEDIA GROUP

Director General
Juan Ramón Melara
juanramon.melara@itdmgroup.es
Director de Contenidos
Miguel Ángel Gómez
miguelangel.gomez@itdmgroup.es
Directora IT Events & Lead Gen Programs
Arancha Asenjo
arancha.asenjo@itdmgroup.es
Directora División Web
Bárbara Madariaga
barbara.madariaga@itdmgroup.es
Directora IT Digital Security
Desirée Rodríguez
desiree.rodriguez@itdmgroup.es

Clara del Rey, 36 1º A · 28002 Madrid
Tel. 91 601 52 92

CAUTELA EN TORNO AL CRECIMIENTO DEL EMPLEO TIC EN ESPAÑA

Como de todos es sabido, el tecnológico ha sido uno de los sectores que más crecimiento ha experimentado con relación a la creación de empleo en los últimos años en España. De hecho, en el primer semestre de 2023 ha vuelto a cosechar un incremento del 6,3% en materia de contrataciones. No obstante, diversos organismos coinciden en que el incierto entorno económico y político que estamos padeciendo, lastrado por las actuales condiciones financieras, induce a una mayor cautela entre las organizaciones. De hecho, los datos de junio muestran un crecimiento interanual del 5,6%, la tasa más baja desde octubre de 2021. Además, la facturación por empleado también se modera, con un ritmo de crecimiento del 6,6%, el menor desde diciembre de ese mismo año.

Según un panel de empresarios españoles consultados por la Comisión Europea durante el mes de agosto, la capacidad para atender nueva demanda con los recursos actuales se sitúa en el 87%, lo que da una idea de que solo un gran impulso de las expectativas económicas o una mejora súbita del entorno pueden hacer pensar en una vuelta a la senda de creación de empleo en el rango de los últimos años. Sin duda improbable. En opinión de las empresas, los factores limitantes para su actividad son, por este orden, los problemas de demanda (nuevos proyectos), la falta de recursos humanos competentes (el problema se ha triplicado desde 2020) y las restricciones financieras, derivadas del nuevo perfil restrictivo de la política monetaria.

Se aprecia, por tanto, cierto enfriamiento en materia de contrataciones a futuro, aunque no debemos olvidar que en los últimos 12 meses se han producido 31.826 nuevas afiliaciones y la base de profesionales en el sector de los servicios digitales se sitúa en los 455.600. El nuestro es un sector que de manera consistente se encuentra entre los más activos a la hora de incorporar talento. Lo que resulta evidente es que se han de acelerar los mecanismos necesarios para formar a los profesionales, ya que corremos el riesgo de comprometer el avance de un sector que, al ser transversal, resulta crítico para la economía del país. ■

PABLO GARCÍA REALES, Director

Únete a nosotros en ISE 2024.

Your Destination for Innovation.

integrated systems europe 20 years

Fira Barcelona | Gran Vía
30 de enero - 2 de febrero de 2024

20 años definiendo, dando forma e impulsando a la industria.

ISE es la mayor feria mundial del AV y la integración de sistemas: durante dos décadas hemos ayudado a la industria a conectarse, colaborar y crear. Únete a nosotros en 2024 e inspírate para innovar.

Adquiere tu entrada GRATIS
Registrándote con el código: **itreseller**
iseurope.org

Una joint-venture entre AVIXA CEDIA

La industria del datacenter está creciendo a un ritmo acelerado para dar soporte a la digitalización, elevando rápidamente su consumo energético y su impacto en el medio ambiente. Para lograr un desarrollo más sostenible empresas como Schneider Electric apuestan por un consumo responsable de recursos y por las últimas tecnologías de hardware y software enfocadas a optimizar los centros de datos, entre las que tienen cabida la refrigeración líquida o la inteligencia artificial.

UN FUTURO MÁS SOSTENIBLE PARA LOS CENTROS DE DATOS

RICARDO GÓMEZ (MILÁN)

El sector de centros de datos está expandiéndose rápidamente y también lo está haciendo su impacto en el medio ambiente, dado que se considera como un gran consumidor de recursos como la electricidad y el agua. Ante esta realidad, empresas como Schneider Electric, especialista en soluciones de energía, refrigeración y gestión de centros de datos, están enfocándose en construir un futuro más sostenible para esta industria. Desde hace años apuesta por ser más respetuosa con el medio ambiente, cambiando el modelo de obtención de materias primas y la adaptando sus procesos de diseño y producción

para optimizar el uso de recursos y fabricar productos más eficientes.

Durante una reciente visita a la fábrica que Schneider Electric tiene en la localidad italiana de Conselve, y bajo el lema “Powering the path to a sustainable digital future”, expertos de la compañía nos mostraron cómo aplican la sostenibilidad a sus procesos desde las primeras etapas de desarrollo de sus productos hasta llegar al cliente final.

DESAFÍOS DE SOSTENIBILIDAD EN LA INDUSTRIA

En este encuentro, Marc Garner, vicepresidente senior de la División Power Secure para Europa de Schneider Electric, explicó los desafíos a los que se enfrenta la industria europea de centros de datos para alcanzar el objetivo “net-zero”, y cómo contribuye su organización a esta transformación. El primer reto proviene de la gran dependencia de fuentes de energía derivadas de los combustibles fósiles (70% del total en la región) y de la compra masiva de energía a países extranjeros.

En su opinión, no existe una verdadera escasez energética, sino un gran desaprovechamiento de recursos que debe combatirse a través de un consumo más responsable y enfocándose en ser más sostenibles. Garner explicó que más del 80% de las emisiones de CO^2 provienen de la producción y el consumo de energía, y el uso masivo e ineficiente de combustibles fósiles eleva el riesgo de sufrir cortes de suministro en el futuro. Considera que la seguridad energética y la sostenibilidad son dos caras de la misma moneda y la industria TI y de centros de datos tienen un papel clave para construir un futuro digital sostenible.

> “ES FUNDAMENTAL QUE APROVECHEMOS EL PODER DE LOS CENTROS DE DATOS Y LA INFRAESTRUCTURA DIGITAL PARA UN FUTURO MÁS VERDE Y SOSTENIBLE”

MARC GARNER,
SVP Power Secure Division en **Schneider Electric** Europa

TRANSFORMACIÓN DEL SECTOR DATACENTER

Marc Garner afirma que en el actual entorno de incertidumbre también se presentan oportunidades para el sector y que para situarse a la vanguardia se debe acelerar la transformación hacia el paradigma de Electricidad 4.0 en todos los ámbitos de la sociedad y la industria. Según su visión, este se apoya en cuatro pilares fundamentales:

- **Eficiencia energética y digitalización:** búsqueda de un mayor aho-

REFRIGERACIÓN LÍQUIDA E INTELIGENCIA ARTIFICIAL

La IA consume grandes recursos de CPU y GPU, generando mucho calor en los equipos, y en los próximos años su impacto crecerá sensiblemente. El Sustainability Research de Schneider Electric estima que entre 2023 y 2028 la carga de trabajo de los centros de datos aumentará un 24%-36%, pasando de 54 a unos 90 Gigavatios. Y el porcentaje correspondiente a la IA crecerá del 8% actual a un 15%-20% (de 4,3 GW a 13,5-18 GW). Consideran que esto impulsará la colaboración en la industria para desarrollar tecnologías de enfriamiento líquido estandarizadas que permitan soportar la mayor densidad de TI y el aumento de cargas de trabajo de IA.

rro energético a través de tecnologías digitales.

➤ **Electrificación:** transición de ecosistemas industriales y de consumidor final hacia energía eléctrica, por ejemplo, con vehículos y otros sistemas eléctricos.

➤ **Energía verde:** mayor uso de fuentes renovables o no derivadas de combustibles fósiles, como la nuclear, e impulso del almacenamiento energético.

➤ **Flexibilidad:** búsqueda de una mayor resiliencia de la red eléctrica a través de la digitalización y otras tecnologías.

En el entorno de los centros de datos, este paradigma de Electricidad 4.0 se centra en la neutralidad en carbono y en el aprovechamiento de recursos como electricidad y agua. Esto requiere tecnologías de suministro energético, enfriamiento y sistemas digitales de gestión de las instalaciones más eficientes, que en Schneider se diseñan de forma personalizada para las necesidades de cada centro de datos.

FÁBRICA EN ITALIA

La planta de Schneider Electric en Conselve (Italia) produce equipos de suministro eléctrico y refrigeración para centros de datos aplicando la sostenibilidad a todos sus procesos.

Clica en la imagen para ver la galería completa

NUEVOS ENFOQUES SOBRE REFRIGERACIÓN

La creciente densificación de TI en los racks, la expansión de tecnologías con altos requisitos de computación, como la IA, y el progresivo movimiento de los proveedores de servicios hacia arquitecturas hiperescala están elevando los requisitos de enfriamiento en las instalaciones. La mayoría de centros de datos emplean sistemas de refrigeración por aire para mantener los niveles de temperatura establecidos por la ASHRAE pero, a medida que aumenta la potencia por rack y la generación de calor, esto resulta más costoso y dificulta alcanzar los objetivos de sostenibilidad de la industria.

Schneider Electric estima que a partir de 50 Kilovatios o más por rack el enfriamiento por aire podría no ser viable si busca la sostenibilidad, y ahí es donde la refrigeración líquida puede aportar soluciones eficaces. Andrew Bradner, general manager

Cooling en Schneider Electric, explicó que su compañía basa su estrategia de Liquid Cooling en el agnosticismo sobre la tecnología, buscando la combinación de refrigeración por aire y/o líquida más adecuada en cada caso de uso. Además, ofrecen a sus clientes un diseño personalizado de principio a fin en base a sus requisitos y emplean tecnologías innovadoras que tratan de simplificar el diseño de las instalaciones.

Desde hace años la compañía ofrece diferentes soluciones, tanto para Edge como para instalaciones de mayor envergadura, y actualmente abarca refrigeración líquida directa a chip, de inmersión de chasis y de inmersión en tanques. Además, en sus instalaciones de Conselve también fabrican varias categorías de Unidades de Distribución de Refrigerante (CDU) y sistemas de intercambio de calor (chillers y coolers) para mover y enfriar el líquido que extrae el calor de los equipos. ■

Clica en la imagen para ver la galería completa

UN EJEMPLO EUROPEO DE CENTRO DE DATOS EFICIENTE

La visión de Schneider Electric sobre el futuro de la industria se materializa en una de las instalaciones más avanzadas de Europa. Se trata del centro de datos MIL01 que STACK tiene en Milán, el primero del país en obtener la certificación Tier 4 del Uptime Institute, que acredita el más alto nivel de rendimiento y confiabilidad. Este proveedor de colocation comparte la visión de Schneider sobre la sostenibilidad, algo que han aplicado en estas instalaciones desde el diseño, logrando alcanzar unas métricas de eficiencia en el uso de energía (PUE) operacional anual de ~1,3 y de efectividad en el uso de agua (WUE) del ~0,8, siguiendo las directrices térmicas de ASHRAE TC9.9.

Para lograrlo, en el área MIL01A han empleado varias tecnologías clave de Schneider Electric, como el SAI Galaxy VX de Schneider Electric, racks, unidades de aire acondicionado para salas de ordenadores (CRAC) y sistemas de distribución eléctrica de la marca. Además, en el apartado de software STACK utiliza la plataforma EcoStruxure de Schneider Electric, con diversos módulos enfocados a mejorar la gestión de las operaciones a través de la monitorización, la automatización y la optimización del consumo energético.

MÁS INFO +

» Schneider Electric

» Schneider y STACK colaboran por un futuro digital sostenible

Fue en 2013 cuando la división de servicios de digitalización de Deutsche Telekom anunció la construcción de un CPD en la localidad catalana de Cerdanyola del Vallés. Dos años más tarde, T-Systems y Vertiv firmaron una alianza que en su momento fue definida como de "pionera" y que tuvo como resultado el nacimiento "del mayor datacenter modular de España y el primero construido de este modo por T-Systems en todo el mundo".

EL DATACENTER FUE DESARROLLADO JUNTO A VERTIV

BÁRBARA MADARIAGA,
CERDANYOLA DEL VALLÉS (BARCELONA)

EFICIENTE Y SOSTENIBLE, ASÍ ES EL CPD MODULAR DE T-SYSTEMS EN CERDANYOLA DEL VALLÉS

Hace ocho años T-Systems decidió apostar por Vertiv para desarrollar su centro de datos modular de nivel III. ¿Los motivos? Materializar su visión estratégica de proporcionar servicios en la nube y satisfacer su necesidad de expandir sus centros

de datos. Para ello, se mostraba imperativo conseguir “una combinación de factores” en lo que, a disponibilidad, fiabilidad, seguridad, escalabilidad, transparencia, rendimiento y sostenibilidad se refiere, además de un rápido despliegue.

La construcción modular de contenedores fue la opción elegida, ya que permite conseguir una rápida disponibilidad y una alta escalabilidad, y facilita futuras fases de expansión, además de una inversión escalonada.

El resultado es un datacenter que presenta, como principales características, 1,1 MW de carga de TI, escalable hasta 5 MW, topología eléctrica 2N, un índice de efectividad en el uso de energía (PUE) de 1,3 y Certificación de nivel III del Uptime Institute.

REDUCCIÓN DE COSTES OPERATIVOS

Uno de los hitos más importantes fue que se logró reducir los costes operativos y se ahorró un 30% en tiempo de construcción, desplegando el CPD modular en 9 meses (el tiempo de construcción medio para un centro de datos de nivel III como el de Cerdanyola oscila entre los 24 y los 30 meses).

“El CPD de Cerdanyola del Vallés ha sido un referente desde su construcción por sus dimensiones y por su capacidad para seguir creciendo. Actualmente clientes de todo el mundo

LA IMPLICACIÓN DE VERTIV EN EL PROYECTO AYUDÓ A AHORRAR UN 30% EN EL TIEMPO DE CONSTRUCCIÓN, DESPLEGANDO EL CPD MODULAR EN 9 MESES

reciben soporte en servicios de infraestructura desde este centro que sigue actualizándose para afrontar los retos del mundo actual reduciendo su consumo energético y alimentado únicamente por energía verde" destaca David Mañas, VP of Cloud & Cibersecurity de T- Systems Iberia.

Estas instalaciones han recibido también el premio Data Centre Market al proyecto más innovador en España, y el reconocimiento del Uptime Institute al proporcionar un 99,98% de disponibilidad.

APUESTA POR LA SOSTENIBILIDAD

Mención especial por la apuesta por la sostenibilidad de ambas empresas. Para lograr los objetivos de protección del medioambiente "fue imprescindible un diseño de alta eficiencia de la nueva instalación" que se tradujo en ese PUE de 1,3, "lo que permite a T-Systems reducir su consumo total de electricidad en un 30%", asegura Vertiv.

"Nuestros esfuerzos se han centrado en conseguir que este CPD sea de gran eficiencia. Si se tiene en cuenta que entre el 30 y el 40% de los costes operativos de un centro de datos se gasta en energía, se puede percibir el impacto en nuestros costes de producción,", señala Josep Linares Jiménez, Head of DCI-Production & DCI Uptime Engineering. "Desde su construcción se pensó en la sostenibilidad. El objetivo de Deutsche Telekom es ser una compañía de emisiones cero en enero de 2025".

LA ALIANZA ENTRE VERTIV Y T-SYTEMS TUVO COMO RESULTADO EL MAYOR DATA CENTER MODULAR DE ESPAÑA

La intención de T-Systems es continuar trabajando y mejorando las infraestructuras de este CPD y tiene previsto seguir ampliando el uso de energía solar como fuente de alimentación del centro. Una práctica que en 2021 le llevó a reducir en un 90% las emisiones de su edificio de operación a través de la instalación de paneles solares.

"Su diseño innovador y la tecnología de Vertiv implementada en la instalación facilita la eficiencia energética. Cuenta con tecnología de freecooling indirecto, que permite ahorrar en producción de agua enfriada y lograr una temperatura de climatización óptima gracias a sus pasillos de frío confinados y enfriamiento por districooling", confirma José Alfonso Gil, director de Ventas de Servicio para el Sur de Europa de Vertiv.

PRINCIPALES CARACTERÍSTICAS

El centro de datos tiene una superficie de 2400 m2, cuenta con 2 salas con densidad potencia estándar 2.5 kW/RACK, una sala con alta densidad de potencia 10 kW/RACK para cloud y consta de 38 módulos integrados que albergan cerca de 300 racks Knürr, más de 60 unidades de Thermal Management Liebert y varios sistemas de alimentación ininterrumpida Chloride. La infraestructura modular incluye aislamiento, protección frente a incendios, supervisión y control de acceso seguro. ■

MÁS INFO

» Entrevista con Mario Vasconcelos, Sales Director Enterprise Accounts, Spain & Portugal en Vertiv

» Opinión: Agua y energía, el desafío de la sostenibilidad en los centros de datos

» Caso de éxito: Vertiv y T-Systems desarrollan el primer centro de datos modular de España

COMPARTIR EN REDES SOCIALES

e-VOLUCIONA

Juntos, transformamos tu negocio

Descubre el programa e-voluciona de Esprinet

¡Descarga la app Atrivity y únete a e-voluciona hoy!
Escanea el código QR de App Store o Play store:

DISPONIBLE EN Google Play

Consíguelo en el App Store

esprinet®

#ACTUALIDAD

EL VALOR DE LA ECONOMÍA DIGITAL EN ESPAÑA ALCANZÓ 163.900 MILLONES DE EUROS EN 2021

Según las cifras recientemente publicadas por COTEC e IVIE, destaca el peso de información y comunicaciones en el PIB digital, ya que aporta al menos un 19% del total, seguido de las actividades profesionales, las administraciones públicas y las actividades financieras y de seguros. Madrid y Cataluña concentran algo más de la mitad del valor de la digitalización del país.

BÁRBARA MADARIAGA

COTEC ha presentado el estudio La economía digital en España: avances y retos por regiones y sectores, elaborado en colaboración con el Instituto Valenciano de Investigaciones Económicas (IVIE), que muestra que la economía digital en España alcanzó los 163.900 millones de euros en 2021, lo que representa más del 15% del PIB nacional. Esta cifra muestra una tendencia creciente desde 2011, cuando suponía un mínimo del 10%.

ANÁLISIS POR SECTORES

En el análisis por sectores destaca el peso en el PIB digital de información y comunicaciones, ya que aporta al menos un 19% del total, seguido de las actividades profesionales (18%), las administraciones públicas (defensa, educación y sanidad, con un 14%) y las actividades financieras y de seguros (12%). En el lado opuesto, los dos sectores con menor contribución a la economía digital son agricultura y pesca, además de industria de la madera, corcho, papel y artes gráficas.

Si se tiene en cuenta la intensidad digital, es decir, el peso que el Valor Añadido Bruto (VAB) digital tiene en el VAB de cada conjunto productivo, destaca sobre el resto de los sectores información y comunicaciones, que genera el 72% del VAB por lo digital. En el lado opuesto, se observa cómo en otros sectores importantes para la economía española, como la construcción o la hostelería, este porcentaje se sitúa muy por debajo, alrededor del 5%.

La penetración de la digitalización en el capital (equipamiento, infraestructuras...) ha sido superior a la experimentada en el trabajo. Entre 2011 y 2021, el capital digital pasó del 9% al 19% de sus rentas correspondientes, frente a la renta de los trabajadores digitales, que solo incrementó tres puntos porcentuales su participación en la renta del trabajo (10% en 2011, 13% en 2022). Esto significa que la digitalización está avanzando fundamentalmente por la inversión en activos digitales (hardware, software y bases de datos, equipos de comunicaciones, I+D) más que por la transformación de la estructura de la mano de obra (hacia un mayor peso de trabajadores digitales y de su remuneración).

DESIGUALDAD TERRITORIAL

El estudio también detecta una importante polarización regional en la aportación a la economía digital española. Madrid (31%) y Cataluña (21%) concentran algo más de la mitad del valor de la digitalización del país, frente al 19% que aporta cada uno de estos territorios al PIB total de la economía española. Andalucía (10%), Comunidad Valenciana (8%) y País Vasco (6,5%) siguen a distancia a las dos regiones líderes en digitalización.

Madrid destaca también por la penetración de la digitalización en su estructura productiva, ya que el 24% de la renta generada en la región es digital. También destacan Cataluña y País Vasco (17% y 16%, respectivamente), mientras que el resto de las regiones se sitúa por debajo de la media del país.

El papel central de estas tres regiones líderes marca las diferencias en términos de digitalización, muy concentrada en estos tres polos. Además, no se constata que las regiones estén convergiendo en la intensidad con la que penetra la digitalización. ■

LA ECONOMÍA DIGITAL EN ESPAÑA: AVANCES Y RETOS POR REGIONES Y SECTORES

DESCARGAR

MÁS INFO +

» La economía digital en España: avances y retos por regiones y sectores

COMPARTIR EN REDES SOCIALES

MICROSTRATEGY MUESTRA EL POTENCIAL MULTIPLICADOR DE UNIR IA Y BI

Durante la celebración en Madrid de AI/BI Simposium, MicroStrategy ha dado a conocer las principales novedades recientemente incorporadas a su plataforma One, que incluyen nuevas capacidades para mostrar la información así como un paso adelante en la integración de la inteligencia artificial, lo que implica un efecto multiplicador en el incremento de productividad que las compañías pueden obtener de su Business Intelligence.

MIGUEL ÁNGEL GÓMEZ

El AI/BI Simposium de Madrid supone, por una parte, una parada en nuestro país de un evento con el que MicroStrategy está recorriendo diferentes países para dar a conocer las novedades de su plataforma y el potencial que puede aportar la inteligencia artificial a sus clientes, y, por otra parte, la recuperación de las reuniones presenciales de este tipo tras el impás impuesto por la pandemia. Con su celebración, la compañía se acerca de nuevo a sus partners y clientes, algo esencial para la firma, porque, como reconocía en su intervención de apertura Severino Gala, country manager para España

y Portugal de MicroStrategy, “somos una empresa de tecnología, pero esta, sin su aplicación, sirve de poco”. Y, por eso, los clientes y los casos de uso de la tecnología fueron puntos esenciales en las ponencias.

Hablando de los clientes, recordaba este responsable el rol de estos en el proceso de innovación de la compañía, que se ejemplifica con las 1.800 peticiones de cambios que han recopilado en los dos últimos años a partir de reuniones con clientes en los diferentes países donde MicroStrategy está presente, con especial protagonismo de nuestro país, donde la caravana se detuvo en dos ocasiones.

NOVEDADES EN LA PLATAFORMA

Intercaladas entre las presentaciones de los clientes, MicroStrategy fue desgranando las principales novedades incorporadas a la plataforma One a finales del mes de septiembre, si bien la más destacada es la incorporación de la inteligencia artificial para amplificar el potencial de la inteligencia de negocio sobre la propia plataforma de la compañía, porque, como señalaba Carlos Cepero, senior sales engineer de MicroStrategy, “es el momento de la IA, y no hay que tener miedo, sino que hay que aprender”.

De hecho, la visión de la multinacional pasa por “aprovechar el potencial de la IA para ser más eficientes, y vamos a poner en vuestras manos las herramientas para ello”, algo que convive con un gran interés en el mercado por la inteligencia artificial, que Gartner sitúa en el 78% de las organizaciones que están explorando la IA generativa.

Las novedades que incorpora la plataforma, potenciadas por “la modernización que hemos llevado a cabo en los últimos años, abriendo la arquitectura a base de API y de microservicios”, convierten a One “en la mejor opción para aprovechar la IA en analítica”, sentenciaba Carlos Cepero, que añadía que “One da co-

ROL PROTAGONISTA DE LOS CLIENTES

Como decíamos, los clientes y sus experiencias con la tecnología MicroStrategy tuvieron un protagonismo esencial en este AI/BI Simposium. De hecho, fueron cuatro las presentaciones donde clientes de diferentes sectores y ubicaciones mostraron lo que la tecnología aporta a sus negocios y cómo han implementado las capacidades de MicroStrategy para potenciar sus organizaciones.
Así, responsables de Abanca mostraron las capacidades que a la entidad bancaria les aporta Adata, el nuevo portal corporativo securizado que se posiciona como un punto único de toda la información que pueda necesitar el usuario; BBVA explicó a los asistentes cómo están desarrollando su viaje a la nube con su plataforma de datos, Datio; el Centre de Telecomunicacions i Tecnologies de la Informació (CTTI) dieron a conocer cómo están consolidando el BI corporativo de las diferentes organizaciones que lo componen; e Hijos de Rivera demostraron cómo están optimizando la labor de sus trabajadores con el valor que les aporta la Hiperinteligencia sobre los datos de su BI.

> “ESTAMOS EN UN MOMENTO INCREÍBLE, AL QUE HEMOS LLEGADO CON LA EVOLUCIÓN OFRECIDA POR LAS SUCESIVAS OLAS DE INNOVACIÓN”

ERIKA MORENO,
VP product manager de
MicroStrategy

bertura a todos los casos de analítica necesarios ahora y en el futuro".

Además, la reciente actualización ofrece nuevas experiencias de acceso a la información adecuándose a las necesidades de cada uno de los diferentes perfiles de usuario.

EL VERDADERO POTENCIAL DE LA INTELIGENCIA ARTIFICIAL

Ampliando los detalles de las nuevas capacidades aportadas por la integración de la IA, Erika Moreno, VP product manager de MicroStrategy, señalaba que "estamos en un momento increíble, al que hemos llegado con la evolución ofrecida por las sucesivas olas de innovación".

Para esta responsable, la suma de IA y BI aporta un poder impresionante, y los clientes de MicroStrategy puede aprovecharlo de forma más eficiente "sobre la plataforma de datos sólida que ya tienen".

Tal y como explicaba, la pregunta no es si aplicar la IA en las organizaciones, sino cómo implementarla, "y hemos detectado un gran número de casos de uso", además de definir cuatro líneas de desarrollo en las organizaciones: experiencia de usuario, con la creación de una app capaz de llegar a todos los usuarios; confianza, ofreciendo un acceso protegido a datos de confianza; capacidades, desarrolladas y amplificadas por la facilidad de uso sobre la plataforma One; e integración, dado que el desarrollo creado debe estar integrado con el resto de recursos de la organización.

Junto con esto, desglosaba Erica Moreno los cuatro primeros elementos asociados a la IA que se han integrado en la plataforma en esta actualización. En primer lugar, Auto Dashboard, un asistente para la creación de cuadros de mando según la información que la plataforma ofrece con los Dossiers. En segundo lugar, Auto SQL, un asistente para crear y optimizar tareas a partir de lenguaje natural; Auto Expert, un chabot para resolver dudas e, incluso, poner conectar con el equipo de soporte en caso de que sea necesario; y Auto Answers, un bot que ofrece sugerencias a partir de los Dossiers que maneja la organización mediante lenguaje natural o en formato visual.

A partir de estos primeros pasos, MicroStrategy trabaja en otras opciones futuras, como la capacidad de las empresas de crear sus propios bots con la personalidad y la apariencia que decida la organización, la posibilidad de integrar en estos elementos tanto datos estructurados como no estructurados, la incorporación de un asistente para la creación de esquemas, ampliar las capacidades de integración con la nube con la opción de trabajar con Kubernetes, la opción de integrar MicroStrategy como elemento nativo en Teams, o el enmascaramiento de datos.

Pero antes de estos desarrollos futuros, en los próximos meses MicroStrategy anunciará la integración de la plataforma en Google Cloud, complementando la oferta actual sobre Amazon Web Services y Microsoft Azure. ■

> "SOMOS UNA EMPRESA DE TECNOLOGÍA, PERO ESTA, SIN SU APLICACIÓN, SIRVE DE POCO"
>
> **SEVERINO GALA,** country manager para España y Portugal de **MicroStrategy**

MÁS INFO +

- "Cada vez vemos más empresas que convierten sus datos en un activo de negocio", Severino Gala, MicroStrategy
- MicroStrategy toma el pulso de sus clientes en Roadmap Summit Series

COMPARTIR EN REDES SOCIALES

DMI Computer

KIOXIA

Ready for the Next Adventure

EXCERIA HIGH ENDURANCE

EXCERIA PLUS

EXCERIA G2

HPE ARUBA NETWORKING POTENCIA LA EXPERIENCIA DIGITAL DE LA RYDER CUP 2023

HPE Aruba Networking convierte la cuadragésima cuarta edición de la Ryder Cup en la mayor instalación inalámbrica para un evento temporal deportivo con el objetivo de potenciar la experiencia de usuario, tanto para los asistentes como para los profesionales, en Marco Simone Golf & Country Club de Roma.

MIGUEL ÁNGEL GÓMEZ (ROMA)

Roma se convierte este fin de semana en el epicentro del mundo del golf con la celebración de la 44ª edición de la Ryder Cup, el evento en el que Europa y Estados Unidos compiten de forma bianual. Cinco años después de la última edición en terreno europeo, en París en 2018, la cita ha evolucionado y, de la mano de HPE Aruba Networking, se ha convertido en la edición más digital de la competición apoyándose en cuatro pilares básicos, conectividad, datos, seguridad y sostenibilidad, sobre la base tecnológica integrada en la propuesta del fabricante tras la adquisición de Athonet.

LA EDICIÓN MÁS DIGITAL DE UNA COMPETICIÓN CENTENARIA

Y es que el despliegue tecnológico que soporta la cita romana se apoya en la tecnología 5G privada de Athonet y la tecnología wifi de HPE Aruba Networking, con el fin de proporcionar nuevas capacidades, mayor nivel de seguridad, una cobertura más amplia y mejores experiencias para los aficionados, se esperan alrededor de 250.000 espectadores en los diferentes días de competición, y para el personal.

Tal y como ha explicado HPE, la solución unifica las capacidades de las redes wifi y 5G privadas. La primera aporta conectividad de alta capacidad, para soportar las conexiones simultáneas de los aficionados, mientras la 5G privada ofrece cobertura de área amplia en las zonas más remotas del campo de golf, así como una red privada segura dedicada para el personal de operaciones críticas. Se trata de una visión que, tal y como explicaba Michael Cole, director de tecnología del grupo European Tour y de la Ryder Cup Europe, muestra lo que serán las redes del futuro, una visión que tuvo HPE con la adquisición de Athonet en junio de este año.

En palabras de este responsable, “la 5G privada aporta enormes ventajas operativas, ya que nos proporciona una red totalmente privada que no se verá afectada por la gran demanda de aplicaciones de gran ancho de banda por parte del público. La misma nos proporciona una cobertura total del campo para los dispositivos móviles que prestan servicios críticos como la seguridad, el acompañamiento, la venta de entradas y el marcador que, de otro modo, podrían haber tenido que depender de las redes de telecomunicaciones locales sometidas a presión”.

En este sentido, Phil Mottram, vicepresidente ejecutivo y director general de HPE Aruba Networking, comentaba que este evento “es un escaparate perfecto para la integración de 5G privada y Wi-Fi, con la 5G privada que proporciona un mayor alcance y fiabilidad para el personal de operaciones, mientras que Wi-Fi 6E facilita conectividad de alta capacidad a miles de aficionados concentrados en las zonas claves”.

LA SOLUCIÓN TECNOLÓGICA

La red desplegada aprovecha las últimas tecnologías Wi-Fi 6 y Wi-Fi 6E, ofreciendo el doble de capacidad que en París 2018, a través de más de 800 puntos de acceso inalámbrico. El core de la red se basa en 200 conmutadores HPE Aruba Networking CX con HPE Aruba Networking Central con IA para la gestión de la red que proporciona un único punto de visibilidad y control en toda la red. El panel de control de HPE Aruba Networking Central también proporciona información impulsada por IA sobre lo que está sucediendo en todo el entorno desde una perspectiva de solución de problemas, optimización y seguridad de la red. Por su parte, HPE Aruba Networking ClearPass facilita un control de acceso y una incorporación seguros y eficientes para mejorar la experiencia del espectador en toda la infraestructura Wi-Fi. Ejecutar la red y el entorno informático desde la plataforma HPE GreenLake edge-to-cloud significa que se necesita menos equipo in situ y que es más rentable y rápido de implementar y gestionar.

DATOS, SEGURIDAD Y SOSTENIBILIDAD

Pero, además de la conectividad, son otros tres los pilares que soportan esta experiencia, los datos, recogidos por sensores IoT a lo largo del campo y que proporcionan información muy valiosa tanto para alimentar la aplicación ofrecida a los aficionados, con contenidos enriquecidos y una experiencia personalizada, como para la propia gestión del campo y del evento; seguridad, un elemento clave para ofrecer la mejor experiencia de uso; y sostenibilidad, con lo que esta edición de la Ryder Cup se convierte en uno de los primeros casos de uso global del nuevo panel de sostenibilidad de la plataforma HPE GreenLake, que ofrece información clave sobre el consumo energético de las TI, las emisiones de carbono y los costes de electricidad. El panel aprovecha los análisis avanzados de todo el parque tecnológico para permitir la toma de decisiones que mejoren la sostenibilidad global. ■

MÁS INFO +

- HPE completa la adquisición del especialista en redes 5G privadas Athonet
- “Cada vez más, los clientes nos piden información sobre la huella de carbono para decidir su compra de TI”, John Frey, HPE
- Ryder Cup 2023

INGRAM MICRO CELEBRA EL 20 ANIVERSARIO DE SU SIMPOSIUM ANUAL

El mayorista Ingram Micro celebra el 10 de octubre su Simposium anual, en el que miles de profesionales del canal podrán ponerse al día de las últimas novedades tecnológicas. Con motivo de su 20 aniversario Ingram ha escogido una nueva ubicación en Barcelona para albergar a un mayor número de fabricantes y ofrecer a los asistentes un amplio abanico de actividades.

RICARDO GÓMEZ

El próximo 10 de octubre, Ingram Micro organiza su Simposium 2023, una de las citas destacadas del sector donde las marcas de su catálogo exponen sus últimas novedades en Cloud, Core Business, gestión de datos o ciberseguridad, entre otras tecnologías. Este año el evento celebra su 20 aniversario, una ocasión especial en la que la compañía pretende superar las cifras de asistencia del año pasado, y que, según la organización, estará "lleno de novedades y sorpresas".

La cita tendrá lugar en el pabellón 2 de la Fira Gran Vía, en Barcelona, un espacio emblemático empleado en

grandes ferias tecnológicas, capaz de albergar las numerosas actividades, corners y espacios que la organización ha preparado para este año. Esa misma mañana, entre las 9:00 y las 10:00, Ingram Micro celebrará una rueda de prensa previa al Simposium en el Hotel Puerta Fira, en la que hará un balance de cómo ha ido el negocio durante el último año.

MÁS EXPOSITORES Y ACTIVIDADES

En su presentación inicial del Simposium 2023, Jaume Soler, director general de Ingram Micro, señaló que "va a ser un salto de calidad y una oportunidad para evolucionar nuestro Simposium en Barcelona, por lo que creemos que vamos a poder organizar un evento a la altura de las expectativas de nuestros partners y clientes". En esta edición del evento el mayorista reunirá en un espacio de más de 4.500 m^2 (casi el doble que en el evento original) a más de 2.500 profesionales del canal y más de 100 fabricantes que mostrarán los últimos avances en tecnología en un espacio pensado para poner en contacto a empresas y proveedores del sector TI.

Para ello Ingram ha preparado numerosas zonas de exposición de productos y soluciones, talleres prácticos, ponencias y demostraciones. También ha dispuesto un área específica para celebrar el almuerzo, que un año más será la ocasión perfecta para el networking de los asistentes. Otro de los momentos clave del Simposium 2023 de Ingram Micro será a las 16:00, cuando se celebrará una conferencia a cargo del Mago More, habitual en distintos eventos del sector tecnológico, titulada "el poder positivo del cambio".

Como en años anteriores, la compañía llevará a cabo su tradicional entrega de premios a los asistentes y, una vez finalizado el evento principal, ha organizado una "celebración post-Simposium". En esta ocasión ha escogido The Sea Garden, un espacio con vistas al mar, situado en Moll Vell, donde se ofrecerá a los asistentes al Simposium música, aperitivos, etcétera, hasta pasada la medianoche. ■

MÁS INFO +

» Simposium 2023 Ingram Micro

COMPARTIR EN REDES SOCIALES

XVANTAGE POTENCIA EL NEGOCIO DE INGRAM MICRO

Una de las mayores novedades de Ingram Micro desde finales del año pasado ha sido la puesta en marcha de Xvantage, una plataforma basada en un gemelo digital que la compañía ha creado para modernizar su ecosistema de servicios a través de los datos. Esta ha permitido optimizar procesos de negocio y alcanzar un nuevo nivel de personalización para sus clientes que, según las últimas cifras de la compañía, está teniendo éxito en su misión. A mediados de verano Ingram Micro anunció que, a raíz de la plena implantación de su plataforma Xvantage, ha logrado **incrementar en un 16% toda su operativa web**.

Uno de los valores que ha aportado a la compañía es la unificación de todos los productos y servicios a través de una plataforma que adapta la oferta a las preferencias de los clientes y amplía las capacidades de autoservicio, entre otras cosas. En su anuncio, Estibalitz García de Salazar, Business OPS Manager & Project Leader Xvantage de Ingram Micro Spain, destacó que Xvantage ofrece "un entorno versátil, personalizable, seguro e inteligente pensado para la digitalización de sus negocios de forma honesta y eficiente". Y destacó que las capacidades de esta plataforma "buscan mejorar las posibilidades de elección, compra, gestión y configuración de los clientes" e un entorno que facilita el contacto entre proveedores y partners".

Descubre las soluciones traulux by Charmex AV TECHNOLOGY

MONITORES INTERACTIVOS PARA EMPRESA Y EDUCACIÓN

*Con 5 años de garantía y reinstalación de equipo incluida para España y Portugal.

PANTALLAS LED INSTALACIONES FIJAS INDOOR, OUTDOOR Y RENTAL

Imágenes HD de alto contraste y colores vivos.

Charmex AV TECHNOLOGY

PROYECTOS Y SOLUCIONES AV A TRAVÉS DEL CANAL

Una experiencia completa. Nos adaptamos a tus necesidades para optimizar tus proyectos. Estaremos ahí para acompañarte de principio a fin, gracias a nuestro equipo I+D y el servicio técnico postventa, nuestro valor añadido.

Visita nuestras redes sociales
Charmex Internacional S.A

“Cuando tienes un ciberataque, ya no hay tiempo de mejorar procedimientos”

ESTHER MATEO RODRÍGUEZ, DIRECTORA GENERAL DE SEGURIDAD, PROCESOS Y SISTEMAS CORPORATIVOS DE ADIF

DESIRÉE RODRÍGUEZ

Hablar de seguridad es, en nuestro sector, discurrir acerca de ciberataques, cibercriminales o tecnología, pero, para la entrevistada de este mes el concepto de seguridad incluye tanto el ámbito digital como el terreno físico. Descubre la opinión de Esther Mateo Rodríguez, directora general de seguridad, procesos y sistemas corporativos de Adif, sobre las tendencias y retos que vive el sector en esta entrevista.

ENTREVISTA >> ESTHER MATEO RODRÍGUEZ, ADIF

> SUFRIR UN CIBERATAQUE ES COMO APUNTARTE A UN MÁSTER ACELERADO, PERO CON GESTIÓN DEL ESTRÉS AÑADIDO

¿Cuál es el mayor desafío de estar por encima de figuras clave como CIO, CISO y CDO, entre otros, en una empresa como Adif? ¿Cómo es su relación con los diferentes departamentos?
El mayor reto que ha conseguido Adif, que es infraestructura crítica y servicio esencial, y por cuya red circulan seis mil trenes diarios, es que toda la organización comprenda que tiene una función de seguridad. Lo que no tiene es la misma todo el mundo, pero todos contribuimos, aportamos y conformamos una cultura de seguridad conjunta.

Si dejas pasar detalles de seguridad, contribuye al resto de funciones. Con lo cual, para mí lo esencial es que se entienda en toda la organización que algo no es seguro porque alguien de seguridad lo verifique sino porque se diseña de forma segura y, durante todo el proceso, desde que se diseña hasta que se pone en servicio, en todo el ciclo de vida, hay personas que velan por la seguridad.

¿Cómo es su relación con otros departamentos?
Por suerte en Adif, dentro del comité de dirección hay otras direcciones generales muy trascendentes. El core de Adif es la operación, es la circulación y es el mantenimiento. Por tanto, esta Dirección General que yo dirijo actualmente hilvana todos los procesos de la organización, es totalmente transversal y garantiza y ayuda a que el resto de las direcciones generales realicen la función de seguridad que tienen encomendada, a parte de la suya propia. Con lo cual, el leitmotiv de la Dirección General es estar al servicio del resto de direcciones generales pero siempre marcando unas políticas y unas directrices de cumplimiento exquisito de toda la normativa.

La idea es avanzar siempre y mejorar la seguridad en lo que se puede con lo cual la relación es fluida pero no te voy a negar que con una gestión de conflictos dinámica y fantástica.

¿Ha adquirido la ciberseguridad mayor importancia en los últimos años?
Organizativamente está claro, porque el CIO y el CISO están representados por mí en la organización y se toman decisiones claras marcadas tanto por la estrategia digital como por la de ciberseguridad.

Desde WannaCry, las empresas en España fueron muy conscientes de la necesidad de estar mejor preparadas. Apareció un departamento específico que no había y se empezó a tener conciencia de que no se trata solamente de un descuido en un correo.

Se vio que hay organizaciones con un volumen de negocio muy rentable y que los cibercriminales tienen todo el tiempo del mundo, y todos los recursos, para intentar entrar y extraer información. Y eso obliga a redoblar esfuerzos tecnológicos, humanos y de procesos para estar más preparado. Esa conciencia no se tenía antes.

Tener la conciencia y la sensibilización es el primer paso para que apruebe el presupuesto, para que se tenga un cuadro de mando interesante donde se mida no sólo cómo se gobierna sino cómo se protege, haya transparencia para contar el número de ataques y cómo se responde, la capacidad para reponerse... son muchos términos que hace nada no se manejaban en las organizaciones. Y es que,

cuando tienes un ciberataque, ya no hay tiempo de mejorar el procedimiento, tienes que ejecutarlo y medir si es eficaz. Al contrario de lo que ocurre en security y safety, aquí la aspiración no es coger al "malo" sino reponer el servicio lo antes posible.

Hablemos del ataque que Adif sufrió hace unos años, ¿qué aprendieron de este incidente? ¿Cuál es el mayor reto que se presenta cuando se da esta situación?

En 2020 estábamos todavía confinados y fue un ataque relevante, que Adif no ha negado nunca y que yo personalmente he ido a contar en numerosas ocasiones porque creo que compartir información es la única forma de que las empresas aprendan de nuestra experiencia.

El mayor aprendizaje fue cómo funciona el equipo humano. Fue un ejercicio de rigor en la forma de afrontarlo, de confidencialidad por supuesto y de trabajar todos a una como teníamos marcado. ¿Se encontraron debilidades? Sí, y eso nos ha servido para mejorar nuestra forma de reaccionar ante un incidente.

Y se aceleraron despliegues tecnológicos que teníamos pendientes. Es como apuntarte a un máster acelerado, pero con gestión del estrés añadido. No le recomiendo a nadie que tenga que pasar por un ciberataque pero creo que es la mejor lección, el aprendizaje más potente porque, aunque te dotes de los de los medios tecnológicos, la prueba de fuego no la pasas igual.

¿Cuál es para Adif la prioridad en ciberseguridad a día de hoy?

Te mentiría si te dijese que solo tenemos una, hay varias. Si tuviese que resumir sería:

➤ **Afrontar el mundo OT:** tenemos un despliegue de equipamiento en la red que supone el 85% de nuestros sistemas y que no se diseñó pensando en protegerse de nada. Sin embargo, realizan bien su función, pero tenemos que ser capaces de gobernarlo y gestionarlo de una forma más eficiente. Esa convergencia IT/OT es vital y hemos pretendido que esa madurez que tenemos en IT se consiga también en OT.

➤ **La cadena de suministro:** nosotros tenemos una parte subcontratada muy importante. Tanto de personal como de tecnología. Por lo que hay que estar seguros de que no lleguen ataques a través de esa cadena.

> "EL MAYOR RETO QUE HA CONSEGUIDO ADIF ES QUE TODA LA ORGANIZACIÓN COMPRENDA QUE TIENE UNA FUNCIÓN DE SEGURIDAD"
>
> **ESTHER MATEO RODRÍGUEZ,** directora general de seguridad, procesos y sistemas corporativos de **Adif**

➤ **La cultura de la ciberseguridad:** en Adif tenemos una edad media alta. Esto es algo muy positivo porque hay personas con una experiencia enorme, pero en poco tiempo va a haber una renovación de unas 6.000 personas y, aunque es una oportunidad porque todas las personas que entren serán nativos digitales, es importante que esa concienciación en seguridad y nuestra forma de hacer las cosas vaya calando e interiorizándose en la organización desde el inicio.

¿Cree que la seguridad se ha convertido ya en una prioridad para la empresa española?

Sí, sin duda la ciberseguridad es ya una prioridad absoluta. Creo que no hay un mapa de ruta que no plantee esta realidad. Pero sí creo que el riesgo se afronta con menos angustia que otras seguridades y creo que esto tiene que ver con la percepción que tiene la propia sociedad del riesgo de la ciberseguridad donde todos estamos afectados de alguna forma.

Esto ha llegado y es para quedarse. No tanto el riesgo sino la conciencia de que hay que invertir en ello: en personas, procesos y tecnología. Y que no es un gasto. Otro de los cambios relevantes es considerar que el producto o servicio que sea, si no es seguro pierde enteros en su valor, con lo cual la seguridad no es un gasto es una inversión.

Entrar van a entrar. Lo que hay que intentar es que entre lo más tarde

posible y que tardemos el menor tiempo posible en reponernos y expulsarlos. Todas las organizaciones van a acabar pasando por ese punto, la ciberseguridad cien por cien no existe y hay que estar preparado.

Por eso, el que haya un ambiente sano donde la información se traslade sin miedo a la represalia creemos que ayuda a que la organización aprenda más rápido. El comportamiento humano es muy relevante en este ámbito de la ciberseguridad.

Me ha nombrado 3 patas Esther: humanos, procesos y tecnología. Hablemos de esta última, ¿qué tecnologías de ciberseguridad deberían ser básicas en cualquier empresa?
El concepto Zero Trust define bastante bien el ámbito que deberíamos de trabajar. El perfilado del de los de los usuarios y el que no se pueda llegar a cualquier sitio. Pero también la capacidad que tienen ya los sistemas de detectar comportamientos anómalos. Pasar de ciudadela a aquí no se confía en nada más que la garantía de que las identidades están controladas, que sabemos dónde estamos y que estemos acostumbrado a que lo natural es que estemos monitorizados porque eso otorga garantías. Se trata de confianza. Y eso es precisamente lo que estamos intentando trasladar de la parte IT a la parte OT.

¿Qué papel cree que juegan estos servicios gestionados en ciberseguridad y qué papel jugarán en el futuro?
En la administración pública creo que es una gran apuesta. Tenemos que ser conscientes de que jamás tendremos un departamento interno lo suficientemente potente y menos con la explosión que está viviendo el sector y los sueldos que se están pagando fuera. Irremediablemente entramos en un modelo mixto en el que reforzamos los departamentos pero tenemos departamentos externos mediante procesos de pliego y de adjudicación.

En cuanto a las PYME, creo que tienen un problema pues posiblemente ellos no tengan ni capacidad para tener a un responsable (tendrían que tenerlo compartido) ni la posibilidad de acceder a soluciones de grandes empresas por lo que puede que no estén tan bien protegidas. También pueden unir recursos organizándose en grupos de PYME y así acceder a un nivel superior en capacitación. Algo que me parece muy interesante y positivo. ■

MÁS INFO +

- Adif
- Brechas de seguridad, ¿existen opciones?

COMPARTIR EN REDES SOCIALES

INGRAM MICRO®

SIMPOSIUM

LA REVOLUCIÓN DEL CAMBIO

Martes, 10 de octubre de 2023

Fira Barcelona Gran Vía

Fira Barcelona

REGÍSTRATE

#Simpo23Ingram

“Queremos ser más una empresa tecnológica que de paquetería tradicional”

TOMÁS CONCHA,
CHIEF INFORMATION OFFICER DE CTT EXPRESS

MIGUEL ÁNGEL GÓMEZ

Recientemente, Tomás Concha se incorporaba a CTT Express como CIO, con la misión de dar continuidad a los procesos de mejora e innovación de la compañía, así como con el objetivo de aportar al negocio de la paquetería novedades e implementaciones tecnológicas que han demostrado su valor en otros sectores. Para conocer cómo pueden ayudar las TIC y cómo va a desarrollar su labor, hemos conversado con él.

El pasado mes de julio se incorporó a CTT Express. ¿Cuál ha sido su evolución hasta este momento?

Yo empecé mi trayectoria profesional en el mundo de la consultoría, primero en Accenture y luego en Everis, y desde el principio siempre con dos características, mucha exposición a temas internacionales y al sector industrial. En 2019 doy el salto al mundo de la innovación y la disrupción, entrando a formar parte de una división muy pequeñita del grupo NTT, que estaba enfocada a la innovación disruptiva y de ahí paso a CTT Express como responsable de sistemas de información, innovación y proyectos.

¿Qué tiene más peso en su trabajo en la organización, los sistemas, la innovación o los proyectos?

CTT Express es una empresa que lleva ya unos años apostando mucho por la tecnología, la innovación y por cómo aplicar esa tecnología al mundo del reparto de paquetes. Y eso es lo que se quiere potenciar con mi incorporación, aplicar mis experiencias en otros negocios a este mundo del reparto de paquetes. De hecho, CTT Express quiere posicionarse como una empresa más tecnológica de lo que sería una paquetería tradicional, y ese es el mandato que he recibido, ver cómo se pueden aplicar procesos y herramientas innovadoras dentro de este mundo.

En su trayectoria profesional, ha pasado por diferentes verticales, diferentes compañías. ¿Cuáles son los retos con los que llega a CTT Express para traer esas líneas de innovación y mejora en el negocio de la entrega de paquetes?

Hay una serie de procesos o de iniciativas que ya se pusieron en marcha en los últimos años. CTT Express en España arranca a principios de 2020. En ese momento hay un nuevo CEO y equipo ejecutivo que le dan vuelta a nivel de negocio. Y en ese momento también se inicia un camino de transformación dentro del mundo de sistemas de la información, que es en la que estamos. Se viene de un mundo más tradicional, monolítico, de un sistema grande en el que hacer cualquier cosa es muy farragoso y se intenta ir a un mundo mucho más abierto, con operaciones basadas en la nube, microservicios... en fin, nuevas tecnologías, procesos y maneras de hacer las cosas mucho más modernas y abiertas. La idea es conseguir incorporar nuevas herramientas tecnológicas muy innovadoras, incluso llegando a integrar IA para algunos procesos, por ejemplo.

Últimamente no hay conversación tecnológica en la que no sea protagonista la inteligencia artificial. En su caso, ¿han determinado casos de uso en los que pueda aportarles valor o todavía están en fases anteriores?

> “CTT EXPRESS ES UNA EMPRESA QUE LLEVA AÑOS APOSTANDO MUCHO POR LA TECNOLOGÍA, LA INNOVACIÓN Y POR CÓMO APLICAR ESA TECNOLOGÍA AL MUNDO DEL REPARTO DE PAQUETES”

Hemos podido identificar dos áreas en las que tiene bastante sentido. Una, área core de nuestro negocio, es todo lo que se refiere a la optimización de las rutas. Este es un sector donde los costes son muy importantes y los márgenes muy pequeñas, y todas las optimizaciones, mejoras y eficiencias que podamos aportar al proceso de la entrega redundan en un mejor servicio al cliente, una reducción de costes y una mayor sostenibilidad por aquello de reducir la huella de carbono. Pero hay otra área bastante clara de aplicación, si bien, en este caso, es más transversal. Se trata de todo lo relacionado con mejorar o intentar automatizar la atención al cliente. Veo que ya hay herramientas en esta línea y que nosotros podemos hacer uso de ellas.

En el día a día de un CIO hay que equilibrar tres elementos: negocio, tecnología y clientes. En su caso, ¿cómo coloca estas piezas? ¿En qué orden?
En mi opinión, van unidos. Está claro que no solo nosotros en el departamento de Sistemas de Información, sino en toda la compañía, trabajamos para el cliente, obviamente, que es al final al que le tenemos que dar el servicio. Para eso, tenemos que soportar unos procesos y un negocio muy eficiente, y eso, naturalmente, se consigue a través de unas buenas herramientas tecnológicas y unos buenos sistemas de la información. En nuestro caso, tenemos unas herramientas muy potentes para tomar decisiones, y una serie de herramientas para atender a los clientes que yo creo que alcanzan un nivel de madurez bastante elevado. Con lo cual, son tres piezas que son caras de la misma moneda.

A la hora de innovar, ¿de dónde parte la mayoría de las iniciativas? ¿Cómo arrancan el proceso de innovación?
Depende del caso concreto, pero normalmente es una mezcla. Obviamente hay situaciones en las que nosotros, desde la parte de tecnología, somos capaces de proponer mejoras que detectamos en el mercado y que pensamos que pueden ser interesantes. Pero hay veces que las peticiones nos llegan desde el propio negocio, desde áreas que también están al día de las tendencias y que ven lo que es nuevo tanto dentro como fuera de este sector.

Por tanto, es esencial la colaboración entre tecnología y negocio. ¿Cuál es su papel en este sentido?
Mi papel es el de facilitador, el de ayudar a que fluyan esas iniciati-

> “MI PAPEL ES EL DE FACILITADOR, EL DE AYUDAR A QUE FLUYAN LAS INICIATIVAS Y A APOYAR LA IDENTIFICACIÓN DE POTENCIALES ÁREAS DE INNOVACIÓN Y DE MEJORA”
>
> **TOMÁS CONCHA,**
> Chief Information Officer
> de **CTT Express**

vas y a apoyar esa identificación de potenciales áreas de innovación y de mejora. Además, tenemos también una figura específica para esto, y es que a la hora de innovar, contamos con equipos conjuntos de tecnología y negocio para poder identificar esas posibilidades de innovación y ver cómo llevarlas a la realidad.

A la hora de innovar, suelen presentarse algunos frenos en las organizaciones. Normalmente, destacan dos: falta de implicación de la dirección y falta de talento especializado. ¿Han encontrado ustedes alguno de estos hándicaps?

En nuestro caso, tanto el CEO como el resto de la junta directiva, más que frenos son realmente habilitadores de la innovación. En el día a día nos empujan para aportar innovación a la organización. Por eso, en nuestro caso el principal freno lo tenemos en la vorágine del día a día, que nos llevan a trabajar en líneas de innovación a más largo plazo, tratando de mantener separado el día a día y la innovación para que no nos impida avanzar en paralelo.

¿Y la falta de talento? ¿Es una complicación en su caso?

Obviamente la sufrimos como en todas las empresas. Al final, que los perfiles con conocimientos tecnológicos son altamente demandados ahora y competimos mucho con organizaciones, tanto nacionales como internacionales, de dentro y de fuera del sector, por el mismo talento. Para luchar contra ello, estamos siendo lo más flexibles que podemos, ofreciendo todos los elementos que demandan ahora los perfiles tecnológicos, como el trabajo remoto, nuevas maneras de compatibilizar la vida laboral y la vida personal.... Con ello, estamos intentando combatir o mitigar esos riesgos de la captación y la retención del talento.

A día de hoy, ¿qué proyectos tienen en marcha?

La línea más relevante es prepararnos para ser mucho más ágiles en el futuro, que es lo que nos demanda el negocio, movernos a sistemas más abiertos y a arquitecturas más ágiles. Yo creo que esa es la guía más importante que tenemos. Luego, adicionalmente, obviamente hay otras muchas iniciativas, pero yo creo que esa es la más relevante y la que tiene más visibilidad dentro de la casa, porque es la que nos va a permitir estar en una posición adecuada para soportar el negocio y para reaccionar ante los cambios de la manera más eficiente. Sin esa transformación interna es muy complicado mantener el nivel para competir en un negocio como el nuestro.

Por último, si pudiéramos dejar a un lado los posibles frenos o las exigencias del día a día, ¿cuál sería el proyecto que le gustaría poder desarrollar?

Desde luego, un proyecto que nos permita que se incremente la eficiencia todavía más en las operaciones en planta. Creo que es, probablemente, lo que ahora mismo podría ser más innovador dentro del sector. Ahora tenemos una base muy buena y estamos invirtiendo también mucho en conseguir tener unos sistemas de ayuda a los repartidores asociados que tenemos, pero ese nuevo paso sería una de las cosas más importantes a realizar a medio plazo. ■

MÁS INFO +

» CTT Express

COMPARTIR EN REDES SOCIALES

La ciberdelincuencia en España representa el 15,6% de los hechos delictivos*.

No dejes que los ciberdelincuentes acaben con tu negocio.

b-fy

TU BIOMETRÍA SOLO CONTIGO

b-fy.com

b-fy.com

*** Informe sobre la Criminalidad en España 2021.**

“Si la comunicación entre Trend Micro y el partner es perfecta, el cliente va a estar satisfecho”

› DESIRÉE RODRÍGUEZ

JOSÉ BATTAT,
DIRECTOR GENERAL DE TREND MICRO IBERIA

RAÚL GUILLÉN,
CYBERSECURITY STRATEGY DIRECTOR EN TREND MICRO

Con tres décadas a sus espaldas, Trend Micro puede presumir de ser uno de los fabricantes de software de seguridad más solventes. En la entrevista de este mes nos acompaña José Battat, director general de la firma japonesa en Iberia, y Raúl Guillén, Cybersecurity Strategy Director en Trend Micro.

ENTREVISTA >> JOSÉ BATTAT Y RAÚL GUILLÉN, DE TREND MICRO

En estos siete años bajo tu tutela, Trend Micro ha consolidado su presencia en España, ampliando la plantilla, abriendo oficinas en Barcelona y ampliando su equipo comercial en el norte de España. Cuéntenos, ¿qué veremos de aquí a finales de año?

Bueno, de acá a finales de año lo que vamos a ver es la consolidación de todo lo que hemos empezado. Pero esto no es todo, yo creo que este es el principio de un plan de crecimiento celular. Un plan que va generando células idénticas a la casa matriz, que está en Madrid, en distintos territorios.

Ya estamos empezando a hacer cosas en el sur, estamos empezando a hacer cosas en Portugal, también en Galicia... España no es unificado, sino descentralizado. Entonces realmente deberíamos tener sedes y subsidiarias en todas las comunidades autónomas.

Pero si me preguntas cómo veo Trend Micro en los próximos 10 años, diría que con eso, con una unidad de negocios en cada una de las comunidades autónomas.

Todo este crecimiento va acompañado del negocio que, apoyado en una política firme de canal con la que estáis consiguiendo grandes números. De hecho, tienen entre sus clientes al 50% de las empresas del Ibex y el 30% del mercado español en su conjunto. ¿Cuál es la clave de este éxito?

Bueno, lo fundamental es el canal. Yo crecí con esto y cuando llego a España lo que intento es establecer una estrategia basada hacer que todo venga a través de canal. De todos nuestros clientes, el 60-70% son oportunidades que vinieron de canal. Y esto es muy sencillo: siendo fiel, siendo honesto y transparente con el partner y apalancándonos en el negocio con ellos, siendo socios construimos un triángulo dorado.

Si la comunicación entre Trend Micro y el Partner es perfecta, el cliente va a estar satisfecho. Entonces, las buenas experiencias con los partners los clientes las perciben. Entonces, evidentemente esa conjunción con el partner es lo que es el principio de nuestra estrategia, es nuestra clave de éxito, y es hacia dónde vamos.

Y hablando de ese camino de hacia dónde vamos, cuál es para usted el reto que afrontan hoy los responsables de IT y de ciberseguridad?

Esta diversificación que hay en ciberseguridad es tan compleja, los ataques son tan variados y tan estructuralmente complejos que cada vez es más difícil para el cliente, si no tiene un buen SOC, dado por un buen integrador, con unas buenas soluciones integradas y que se interconecten entre sí.

Yo siempre lo comparo con la casa. Si yo quiero asegurar mi casa, pongo una puerta con una empresa, una ventana con otra empresa, uno que me monitoriza las cámaras con una tercera empresa. Pero si no tengo a alguien que correlacione todo y lo unifique, es casi imposible que mi casa esté segura.

Y hablando de retos, uno de los verticales con más desafíos en ciberseguridad es la industria. Ustedes cuentan con una solución específicamente para estos entornos ¿qué es lo que aporta TX-One a la protección OT?
La integración de la protección OT a la protección IT. No podemos contemplarlo como estructuras separadas dentro de las empresas. Para las empresas, evidentemente, la parte OT es algo fundamental. Pero es una parte que antiguamente estaba desconectada y ahora está conectada. Entonces, nosotros la ventaja que tenemos es que le proporcionamos al cliente una solución unificada.

Y en cuanto a comunicaciones, ¿qué puede decirme de CT-One, la parte que cubre esa seguridad 5G que estamos viendo cada vez más desarrollada en nuestro país?
Bueno, esto me enorgullezco en decirlo: creo que somos el único proveedor de seguridad que tiene una solución para 5G Y la verdad es que el 5G es algo que viene, es algo que evidentemente ya está teniendo mercado. Es algo que siempre hace Trend Micro, siempre estamos tres o cuatro años por delante de las necesidades del cliente. Esta solución lleva en desarrollo desde 2018 o 2019, antes de la pandemia.

Este adelantarnos a las tendencias del mercado a veces nos sale bien y a veces nos sale mal. He visto productos que hemos sacado de avanzada que después el mercado no necesitó. Sin embargo, eso nos asegura que cuando llega la necesidad nosotros ya tenemos soluciones consolidadas.

Hoy la 5G es una necesidad y nosotros hace cuatro años que tenemos soluciones dedicadas a estos entornos, a protegerlos de punta a punta. Y esa es la ventaja de Trend Micro. De hecho, ya estamos trabajando con el coche conectado, que hoy no es una necesidad pero lo será y ya tenemos una división que se dedica solo al coche conectado. En Trend siempre logramos estar un paso por delante.

> “ESTA DIVERSIFICACIÓN QUE HAY EN CIBERSEGURIDAD ES TAN COMPLEJA QUE CADA VEZ ES MÁS DIFÍCIL PARA EL CLIENTE”
>
> **JOSÉ BATTAT,**
> Rdirector general de **Trend Micro** Iberia

Trend Micro ocupa el primer puesto en cuota de mercado mundial de seguridad de cargas de trabajo en la nube ¿qué supone para ustedes seguir siendo líderes en este segmento?
Bueno, un gran desafío, ¿no? Porque todo lo que tenga que ver con el cloud se hace muy rápido, hay empresas que salen muy rápido, empresas nuevas, por ahí un poco más modernas, más ágiles, más rápidas. ¿Por qué? Evidentemente, con un tamaño de estructura, los procesos son mucho más ágiles. Y para poder acompañar ese movimiento del mercado, nosotros debemos ser muy ágiles y muy rápidos. Yo creo que ese es nuestro mayor desafío.

Y hablando de desafíos, no podemos terminar esta entrevista sin hablar de inteligencia artificial y para ello preguntamos a Raúl Guillén, Cybersecurity Strategy Director en Trend Micro.

¿Qué ventaja supone la utilización de IA en la nueva versión de la plataforma Trend Micro Vision One?
Bueno, cuando hablamos de AI, hablamos fundamentalmente de eficiencia. Esto afecta y aplica tanto a los malos como a los buenos. De hecho, nosotros investigamos también mucho qué hacen los malos para podernos adelantar a esas prácticas y esos abusos de la IA.

Pero cuando hablamos de usos constructivos, llevamos más de 15 años utilizando IA en nuestras soluciones. Incorporamos de forma pio-

nera soluciones de protección de phishing avanzado, por supuesto, o protección de amenazas persistentes. Todo esto lo llevamos utilizando en todas nuestras soluciones de protección y detección desde hace más de 15 años. Sí que es cierto que aprovechando este boom de la IA generativa y de otras técnicas de IA como el LLM, lo que hemos hecho es llegar a un acuerdo con Azure OpenAI, que es la solución de IA de Microsoft para el entorno empresarial.

Tenemos un Tenant entrenado específicamente por nosotros para enfocarlo desde un punto de vista de la eficiencia, para que los equipos de CSYS, los equipos SOC, tengan la posibilidad de hacer más con menos.

Recordemos también que hay una brecha de talento importante, con lo cual buscamos hacer más eficiente la operativa de la ciberseguridad. Tenemos un asistente que además nos va a permitir medir el nivel de riesgo en entornos de empresa. La ciberseguridad es un punto crítico y tenemos soluciones que nos van a permitir medir el riesgo a lo largo del tiempo y sobre todo contextualizar cualquier anomalía y cualquier respuesta a incidentes para, desde el punto de vista de la eficiencia, ser mucho más productivos y que nuestros partners, que además dan un servicio gestionado, puedan hacer más con lo mismo, hacer más con menos.

Ahí, gracias a Trend Micro Vision One Companion, ofrecemos multitud de casos de uso donde, fundamentalmente, lo que hacemos es contextualizar, dar recomendaciones, anticiparnos en la detección de amenazas en fase temprana y, por supuesto, medir y ver la evolución del nivel de riesgo.

Con lo cual, como siempre, el uso de tecnologías habilitadoras para utilizar la ciberseguridad del futuro en los problemas del presente.

Y hablando de esa anticipación ¿qué cree que veremos en los próximos meses en ciberseguridad?

Yo creo que el nuevo paradigma del mundo hiperconectado donde todo, el IoT, el Internet de las cosas o como dice un buen amigo mío, el Internet of Troubles, será la clave.

Es fundamental que busquemos soluciones que nos aporten, soluciones de nicho, donde demos una cobertura global, extremo-extremo, a todos estos vectores que están conectándose en el mundo empresarial: 5G, IoT, OT, cloud híbrida, vehículo conectado... al final tenemos que usar todas estas tecnologías habilitadoras para simplificar la operativa y hay que hablar de conceptos de plataforma. Yo creo que aquí Trend Micro es pionero, huimos de los silos, huimos de las soluciones de nicho y como comentaba José, les damos herramientas a nuestros partners para que, desde un único punto y con un equipo, puedan dar respuesta a toda esta convergencia y toda esa transformación digital que está ocurriendo a nivel social y a nivel empresarial. ■

> CON TREND MICRO VISION ONE BUSCAMOS HACER MÁS EFICIENTE LA OPERATIVA DE LA CIBERSEGURIDAD

RAÚL GUILLÉN,
Cybersecurity Strategy Director en **Trend Micro**

MÁS INFO

» Trend Micro

» Cómo proteger el nuevo perímetro de ciberseguridad

COMPARTIR EN REDES SOCIALES

ACTUALIZACIÓN SEMESTRAL EN:
SONICWALL.COM/THREATREPORT

2023

INFORME DE CIBERAMENAZAS DE SONICWALL

EL CAMBIANTE PANORAMA
DEL CIBERCRIMEN

SONICWALL®

sonicwall.com | @SonicwallSpain

« CRECE LA ADOPCIÓN DE MODELOS CLOUD HÍBRIDOS EN LOS SERVICIOS FINANCIEROS »

El sector ha avanzado significativamente en la adopción de cloud durante el último año, con un 64% de las entidades financieras que utilizan múltiples entornos de TI. La elevada complejidad de estos hace que la gran mayoría de los profesionales de TI considere que lo ideal sería disponer de una única plataforma para gestionar sus diversas infraestructuras.

BÁRBARA MADARIAGA

Nutanix ha publicado los resultados de su quinto estudio anual Enterprise Cloud Index (ECI), que mide el progreso de las empresas en la adopción de cloud, en este caso, del sector de servicios financieros. La investigación revela que los despliegues mixtos entre las entidades financieras se sitúan en el 64%, ligeramente por encima de la media mundial. Esta notable tasa de adopción refleja el compromiso de este sector altamente competitivo para mejorar la experiencia del cliente, aprovechando los despliegues híbridos multicloud para impulsar las capacidades avanzadas de análisis de datos y modernizar las aplicaciones.

INCREMENTO DE LA DIVERSIDAD

"El aumento de la diversidad de infraestructuras y un mayor énfa-

sis en el almacenamiento de datos, la gestión, la seguridad y los servicios nativos cloud están llevando a todos los profesionales de TI a buscar operaciones híbridas que trasciendan la infraestructura privada y pública. Como demuestran las recientes medidas regulatorias, como la Ley de Resiliencia Operativa Digital (DORA), la resiliencia operativa y el riesgo de concentración son factores adicionales que impulsan la adopción de modelos híbridos", afirma Ian Haynes, EMEA Field CTO de Nutanix. "Las entidades de servicios financieros han emergido como pioneros, superando a muchos otros sectores en la adopción del enfoque híbrido multicloud".

RETOS DE LOS ENTORNOS MULTICLOUD PARA LOS EQUIPOS DE TI

La adopción multicloud híbrida se ha acelerado y se espera que aumente en servicios financieros.
El sector ha avanzado significativamente en la adopción de cloud durante el último año, con un 64% de los encuestados que utilizan múltiples entornos de TI, ya sea una combinación de nubes privadas y públicas, múltiples nubes públicas o infraestructuras privadas locales y alojadas.

La ciberseguridad es el mayor impulsor de las infraestructuras de TI. El sector financiero y los encuestados de todo el mundo dieron prioridad a la ciberseguridad por encima de todo lo demás. Esto no es sorprendente, dada la creciente sofisticación de los ciberataques.

Los entornos mixtos crean nuevos retos y exigen un único lugar para gestionar todas las cargas de trabajo y los datos. El 96% de los profesionales de TI coinciden en que lo ideal sería disponer de una única plataforma para gestionar sus diversas infraestructuras privadas y públicas. Sin embargo, sólo el 42% declaró tener realmente esa visibilidad. Los resultados de visibilidad indican una brecha en las capacidades, destacando la necesidad de herramientas integradas para mejorar las operaciones de TI híbrida. Sin visibilidad, los equipos de TI son incapaces de gestionar, proteger, sincronizar; no se puede analizar aquello que no se ve.

El principal habilitador para mover aplicaciones entre entidades de servicios financieros es mejorar la velocidad de acceso a los datos. Todos los encuestados (100%) indican que habían trasladado aplicaciones entre infraestructuras de TI en los últimos 12 meses. Casi la mitad (49%) citó el deseo de acelerar el acceso a los datos como principal motivo, seguido de un refuerzo de la seguridad o de cumplir con los requisitos normativos, así como de obtener la capacidad de integrarse con servicios nativos en la nube, como la IA y el machine learning.

La mayoría de los encuestados sitúan el control de costes encabezando su lista de retos. Por ejemplo, el 87% describió el control de costes de la nube como un reto en la gestión de sus infraestructuras TI actuales, y aproximadamente un tercio dijo que era un reto importante. ■

MÁS INFO +

» Nutanix Enterprise Cloud Index (ECI)

COMPARTIR EN REDES SOCIALES

LA MITAD DE LOS EMPLEADOS TRABAJARÁN DE MANERA HÍBRIDA O REMOTA EN EL FUTURO

La mayoría de las empresas están de acuerdo en que el trabajo híbrido presenta beneficios de diversidad, igualdad e inclusión. Las compañías buscan un mejor soporte de sus socios proveedores de tecnología digital y proveedores de servicios, con un 76% que están reconsiderando sus relaciones existentes con proveedores digitales.

REYES ALONSO

Los resultados del nuevo estudio Omdia - Future of Work han encontrado que, a medida que los estilos de trabajo continúan diversificándose, el 57% de los líderes de recursos humanos y TI informan que la satisfacción de los empleados en el trabajo ha mejorado. El estudio también muestra que los empleados están menos satisfechos en el trabajo cuando se exige un regreso a la oficina, y que en torno al 50% trabajarán permanentemente de manera híbrida o totalmente móvil en el futuro.

La mayoría de las empresas están de acuerdo en que el trabajo híbrido presenta beneficios de diversidad, igualdad e inclusión (DEI). Específicamente, el 69% está de acuerdo en que el trabajo híbrido permite a los empleados con diferentes necesidades de accesibilidad buscar más oportunidades; el 67% está de acuerdo en que permite a los empleados eliminar las barreras de ubicación; el 63% está de acuerdo en que hace que los empleados se sientan conectados dentro de un equipo cohesionado; el 61% está de acuerdo en que permite a los empleados sentirse menos marginados; y el 59% está de acuerdo en que ayuda a cerrar las brechas de género en el reclutamiento.

BÚSQUEDA DE NUEVOS SOCIOS DE TI

Las empresas también buscan un mejor soporte de sus socios proveedores de tecnología digital y proveedores de servicios, con el 76% de las empresas reconsiderando sus relaciones existentes con proveedores digitales.

Las capacidades que las organizaciones buscan al seleccionar socios para apoyar sus objetivos de transformación en el lugar de trabajo son un enfoque en mejorar las prácticas ambientales, sociales y de gobierno corporativo (ESG) (28%); socios que subcontratan los servicios que planean utilizar, como servicios de TI, recursos humanos y servicio al cliente (27%); y una plataforma digital que mejora la forma en que buscan el apoyo de los socios (26%).

"Los estilos de trabajo más diversos han impactado la productividad, la satisfacción y la experiencia de los empleados, y las empresas necesitan la ayuda de socios, procesos y tecnologías digitales para navegar por iniciativas exitosas sobre el futuro del trabajo", afirma Adam Holtby, analista principal de Omdia, Mobile Workspace y autor del informe Future of Work.

EL ESTUDIO MUESTRA QUE LOS EMPLEADOS ESTÁN MENOS SATISFECHOS EN EL TRABAJO CUANDO SE EXIGE UN REGRESO A LA OFICINA, Y QUE EN TORNO AL 50% TRABAJARÁN PERMANENTEMENTE DE MANERA HÍBRIDA O TOTALMENTE MÓVIL EN EL FUTURO

CASI 9 DE CADA 10 TRABAJADORES PREFIEREN UN MODELO HÍBRIDO DE TRABAJO

Unisys ha presentado un estudio en el que se destaca que el 86% de los trabajadores prefiere un modelo híbrido de trabajo, a pesar de que hasta tres de cada cuatro empleados admite que puede llegar a perder hasta 5 horas de tiempo debido a problemas con la tecnología. De hecho, la mitad de los profesionales asegura que contar con la tecnología idónea para desempeñar sus tareas es uno de los puntos clave para asegurar la fidelidad a su compañía, por encima del salario o de la formación. ■

MÁS INFO +

» Omdia - Future of Work

COMPARTIR EN REDES SOCIALES

Barracuda®

PARA LOS ATAQUES DE CORREO OTROS NO PUEDEN.

Barracuda Email Protection usa AI de primera clase para bloquear amenazas avanzadas.

Defensa férrea para un mundo de amenazas complejas.

barracuda.com

El concepto de Smart City se apoya en tecnologías como los dispositivos IoT, que recopilan datos fundamentales para mejorar la gestión urbana a todos los niveles. Aplicando otros avances como los gemelos digitales, o la inteligencia artificial se está conformando un amplio ecosistema digital enfocado a optimizar recursos y mejorar la calidad de vida de los ciudadanos, que en el futuro se expandirá más allá de las grandes ciudades.

RICARDO GÓMEZ

TECNOLOGÍAS CONECTADAS PARA CIUDADES INTELIGENTES

Las ciudades modernas llevan años invirtiendo en digitalización para mejorar la gestión urbana y la prestación de servicios públicos, un proceso de transformación que ha dado lugar al concepto de Smart City. Este continúa evolucionando a medida que surgen nuevas tecnologías y una de las más importantes proviene del paradigma de Internet of Things, que contempla casi cualquier dispositivo conectado imaginable, capaz de generar y transmitir datos.

En el ámbito urbano esto se materializa en redes de sensores y dispositivos conectados que generan datos y pueden ser controlados a distancia desde un centro de operaciones. Estas tecnologías forman parte de una arquitectura TI más amplia que incluye redes de comunicaciones, centros de datos e infraestructuras perimetrales, con un gran componente de software y herramientas de ciberseguridad. En España las administraciones públicas y las empresas de servicios están invirtiendo cada vez más en IoT, y la industria tecnológica está respondiendo a la demanda desarrollando soluciones para las iniciativas Smart City.

MERCADO IOT PARA SMART CITIES

Según un estudio publicado por Statista, este año el mercado mundial de IoT alcanzará unos 1.106.00 millones de euros en ingresos, y para 2028 podría crecer a una CAGR del 14,29%, alcanzando 2.157.00 millones de euros. Estos expertos pronostican que el segmento de IoT automotriz dominará el mercado por ingresos para final del período, pero el de Smart Cities seguirá ganando fuerza, ocupando la tercera posición en cuanto al número de conexiones, por detrás del IoT de consumo y el industrial (IIoT).

Miguel del Moral, Channel Sales director para el Sur de Europa en Vertiv, señala que “el mercado de Smart Cities es una de las áreas de crecimiento más importantes en el campo de IoT”, ya que “las ciudades inteligentes buscan utilizar la tecnología para mejorar la calidad de vida de sus residentes, optimizar la gestión de recursos y reducir su impacto ambiental”. Según sus previsiones, “la demanda de soluciones IoT en la gestión urbana seguirá creciendo a medida que las ciudades busquen abordar desafíos como la urbanización rápida, la sostenibilidad, la eficiencia y la calidad de vida de sus habitantes”.

> “LA DEMANDA DE SOLUCIONES IOT EN LA GESTIÓN URBANA SEGUIRÁ CRECIENDO”

MIGUEL DEL MORAL,
Channel Sales Director Southern Europe en **Vertiv**

Opina que “algunas de las áreas de gestión urbana en las que se está viendo una mayor demanda de soluciones IoT incluyen: transporte Inteligente, gestión de residuos, gestión de la energía, calidad del aire y medio ambiente, seguridad pública, gestión del agua y servicios públicos y mantenimiento de infraestructura”. Y lo que más demandan sus clientes tiene que ver con el Edge Computing, ya que muchas aplicaciones no pueden permitirse retrasos a causa de la latencia.

Por su parte, Víctor Jiménez, CTO de Huawei Enterprise España, comenta que las perspectivas de su compañía para este mercado son muy positivas y que “si queremos lograr una sociedad totalmente digital y conectada debemos impulsar las ciudades inteligentes como verdaderos núcleos de innovación. A través de ellas se vertebrará la mayoría de los servicios esenciales para los ciudadanos, como por ejemplo sanidad, transporte o educación”.

REDES E INFRAESTRUCTURAS TI

Los ecosistemas IoT urbanos requieren toda una infraestructura TI dedicada a la recopilación y procesamiento de datos, con una arquitectura independiente y resiliente que garantice los servicios. Esto abarca desde centros de datos y TI perimetral a redes de ámbito privado. En el

apartado de conectividad los principales proveedores de infraestructura apuestan por las redes 5G, WiFi 6 y sus posteriores iteraciones. Sus ventajas radican en su capacidad de gestionar múltiples conexiones de banda ancha para la transmisión de grandes flujos de datos como los que transmiten las cámaras IP, ciertos sensores y las infraestructuras perimetrales que preprocesan los datos IoT.

En este ecosistema también tienen cabida otras tecnologías inalámbricas de bajo consumo que se están utilizando en el ámbito IoT, que dotan de más autonomía a los dispositivos que generan menos datos. En estos casos también se está expandiendo el uso de protocolos de redes de área amplia para largas distancias, como LoRaWAN, que se sirven de tecnologías de redes inalámbricas similares a las celulares, WiFi o bluetooth. Como sucede en entornos industriales, en el futuro se verá una gran heterogeneidad de tecnologías inalámbricas que conectarán desde alumbrado público y señalización digital a cámaras de tráfico y videovigilancia, sensores ambientales, vehículos y una amplia variedad de dispositivos IoT.

LA NUBE COMO TECNOLOGÍA VERTEBRADORA

Los datos son la base para adquirir un conocimiento más preciso que apoye la toma de decisiones en la gestión urbana y el creciente volumen de datos requiere grandes recursos de procesamiento y almacenamiento que pueden ser muy costosos de construir y mantener para una administración local o una empresa de servicios. En este sentido, la nube ofrece enormes posibilidades, ya que los proveedores brindan capacidades de computación y almacenamiento escalables en un entorno que admite todo tipo de aplicaciones y servicios.

Víctor Jiménez, de Huawei, asegura que “la nube lo es todo, es el nexo que facilita y potencia la interconexión y el flujo eficiente de datos y servicios en el ecosistema de las Smart Cities”. Considera que la nube simplifica la integración de ecosistemas heterogéneos y proporciona “una plataforma centralizada para gestionar recursos, compartir datos y escalar soluciones que se adapten a cada caso y proyecto concreto”. Desde su compañía han apostado por estas tecnologías con ejemplos como IoT Device Management e IoT Device Access, que forman parte de su porfolio de servicios cloud.

GEMELOS DIGITALES EN LA GESTIÓN URBANA

Sacar partido a la información proveniente de IoT requiere software que permita entenderla en su con-

> “DEBEMOS IMPULSAR LAS CIUDADES INTELIGENTES COMO VERDADEROS NÚCLEOS DE INNOVACIÓN”

VÍCTOR JIMÉNEZ,
CTO en **Huawei** Enterprise España

texto, algo que ofrecen los gemelos digitales, duplicados virtuales de un entorno físico que permiten conocer lo que está sucediendo en tiempo real o casi real. Esto se puede aplicar a casi cualquier sistema o entorno, desde el transporte a las redes de suministro, los servicios de recogida de residuos, la monitorización de espacios públicos o la gestión hídrica en zonas verdes.

Además, los gemelos digitales permiten realizar simulaciones para saber cómo actuar ante determinadas situaciones. Por ejemplo, para anticipar los flujos de personas en un evento multitudinario y evaluar la seguridad, o conocer el impacto en la ciudad de un episodio de calor, lluvias torrenciales o cualquier otra situación de riesgo potencial. Esto supone una gran ayuda para acelerar los tiempos de respuesta y tomar mejores decisiones ante situaciones imprevistas, y muchas entidades al cargo de servicios públicos están adoptando esta tecnología en las grandes ciudades.

Poco a poco, los gemelos digitales se están expandiendo y se tiende hacia una mayor integración de estos sistemas. Magnum Garzillo, IT Partners Account Manager en Sch-

> LA TECNOLOGÍA DE REDES 5G PRIVADAS ES UNA DE LAS MÁS PROMETEDORAS DEBIDO A SUS CAPACIDADES Y SU FLEXIBILIDAD

CARLOS CORDERO,
CTO de **Fujitsu** España

EDIFICIOS INTELIGENTES

Paralelamente a la digitalización urbana se está produciendo un movimiento similar en el ámbito de los edificios. El sector inmobiliario y las propias constructoras están incorporando avances digitales para modernizar la gestión de los inmuebles, haciéndolos más inteligentes, seguros y sostenibles, implementando sensores y dispositivos conectados para monitorizar y automatizar los servicios generales, la gestión de espacios o el mantenimiento.

Con el tiempo, estos avances acabarán vinculándose a los ecosistemas digitales de una Smart City, y en Huawei apuntan que "los residentes y negocios pueden proporcionar feedback sobre servicios y productos, y recibir información y alertas relevantes para su edificio o barrio", además de integrarse mejor con los servicios de seguridad y de respuesta a emergencias. En Schneider Electric van más allá y opinan que los propietarios de estos edificios no solo serán consumidores ", sino prosumidores, capaces de consumir y generar según estímulos del mercado, precio y disponibilidad de energía", participando de la flexibilidad de los mercados energéticos y beneficiándose de sus esfuerzos en eficiencia y sostenibilidad.

neider Electric, comenta que “la convergencia de datos de múltiples fuentes, como la gestión del tráfico, el transporte público y los suministros, en un único gemelo digital integral, permite una gestión más eficaz y una visión completa de la ciudad. Esto facilitará la coordinación y mejorará la eficiencia en la gestión de una ciudad inteligente”. Garzillo comenta que siguen mejorando sus herramientas de gemelo digital para empresas de agua y energía en las ciudades, y destaca su solución EcoStruxure Water Cycle Advisor, centrada en ayudar a los clientes a alcanzar sus objetivos de calidad, eficiencia y sostenibilidad”.

Otro ejemplo de esta tendencia integradora es Social Digital Twin de Fujitsu. Carlos Cordero, CTO de Fujitsu España, destaca que esta plataforma “se basa en implementaciones de varios gemelos digitales federados entre sí, que modelizan cada una de las áreas de foco en la ciudad, incluyendo fluidez del tráfico, estado del transporte público, logística urbana y monitorización de emisiones”. Dice estos son los tres principales intereses para las grandes ciudades y por ello Fujistu se ha sumado como patrocinador al Madrid Green Urban Mobility Lab, que cuenta con varios grupos de trabajo dedicados a estas áreas.

Además, pone en valor que los algoritmos de inteligencia artificial son fundamentales “para el proceso de datos y flujos de video que terminan alimentando un modelo de gemelo digital de la ciudad”. Y que aportan grandes ventajas y posibilidades “tanto para la predicción como para los modelos de simulación”.

CIBERSEGURIDAD IOT

Construir una red de infraestructura TI para la gestión urbana implica grandes riesgos de ciberseguridad, dado que se emplean tecnologías de muy diversa naturaleza. Borja Pérez, Country Manager de Stormshield Iberia, comenta que “la elección de los equipos es esencial, ya que la seguridad afecta a cada equipo de comunicación, a la infraestructura de redes y sistemas, a los centros de explotación y también a los usuarios”. Recomienda escoger sensores de proveedores que tengan en cuenta la ciberseguridad, pero alerta de que hay muchos dispositivos fabricados sin considerar este aspecto. Por ello, aconseja “microsegmentar servicios IoT mediante firewalls que puedan instalarse de manera transparente, que filtren los protocolos no seguros y cifren las comunicaciones entre sensores y centros de control”.

En Trend Micro también están sensibilizados con los riesgos deri-

> “LA CONVERGENCIA DE DATOS DE MÚLTIPLES FUENTES EN UN ÚNICO GEMELO DIGITAL PERMITE UNA GESTIÓN MÁS EFICAZ Y UNA VISIÓN COMPLETA”

MAGNUM GARZILLO,
IT Partners Account Manager en
Schneider Electric

> LAS CIUDADES INTELIGENTES ESTÁN CADA VEZ MÁS CONECTADAS... PERO TAMBIÉN MÁS EXPUESTAS A LOS CIBERRIESGOS

BORJA PÉREZ,
Country Manager de **Stormshield** Iberia

> LA SECURIZACIÓN DE LAS INFRAESTRUCTURAS QUE RESPALDAN LOS DESPLIEGUES DE IOT EN LAS CIUDADES ES UN DESAFÍO MULTIFACÉTICO

RAÚL NÚÑEZ,
Technical Pre-sales en **Trend Micro** Iberia

vados de IoT en los entornos urbanos. Raúl Núñez, Technical Pre-sales en Trend Micro Iberia, explica que basan la protección de estos ecosistemas en dos puntos: protección de redes 5G privadas y protección de comunicaciones y endpoints con la gama de productos TXOne para redes industriales.

Más allá de los dispositivos IoT, la ciberseguridad de una ciudad conectada abarca toda la infraestructura subyacente, desde las redes a los equipos centrales. Raúl Núñez, de Stormshield, dice que estos entornos "son un punto de convergencia de diferentes sistemas de información de una gran variedad de actores, con diferentes bloques tecnológicos (5G, IoT, Edge, AI), distintos equipos (mobiliario urbano, semáforos, alumbrado público, sensores, etc.) y diversas interfaces que amplían considerablemente la superficie de ataque de una Smart City". Esto, junto con la coexistencia de numerosos entornos IT y OT, complica establecer una política de seguridad global, y aconseja aplicar diferentes normas de seguridad, "garantizando la interoperabilidad entre soluciones para aumentar el nivel de seguridad".

Para Trend Micro, proteger la infraestructura digital de una Smart City plantea innumerables desafíos de ciberseguridad, tanto a nivel técnico como humano. En cuanto al primer punto, destacan la vulnerabilidad de dispositivos, la gestión de identidades y accesos, las actualizaciones de seguridad, la gestión del ciclo de vida de seguridad, la privacidad de los datos, la integración con sistemas existentes y la resistencia a ataques distribuidos. En el lado humano, los desafíos más destacados serían la educación y concienciación de los ciudadanos y las autoridades, la coordinación entre las partes interesadas y las limitaciones de presupuesto y recursos en las administraciones y empresas de servicios. ■

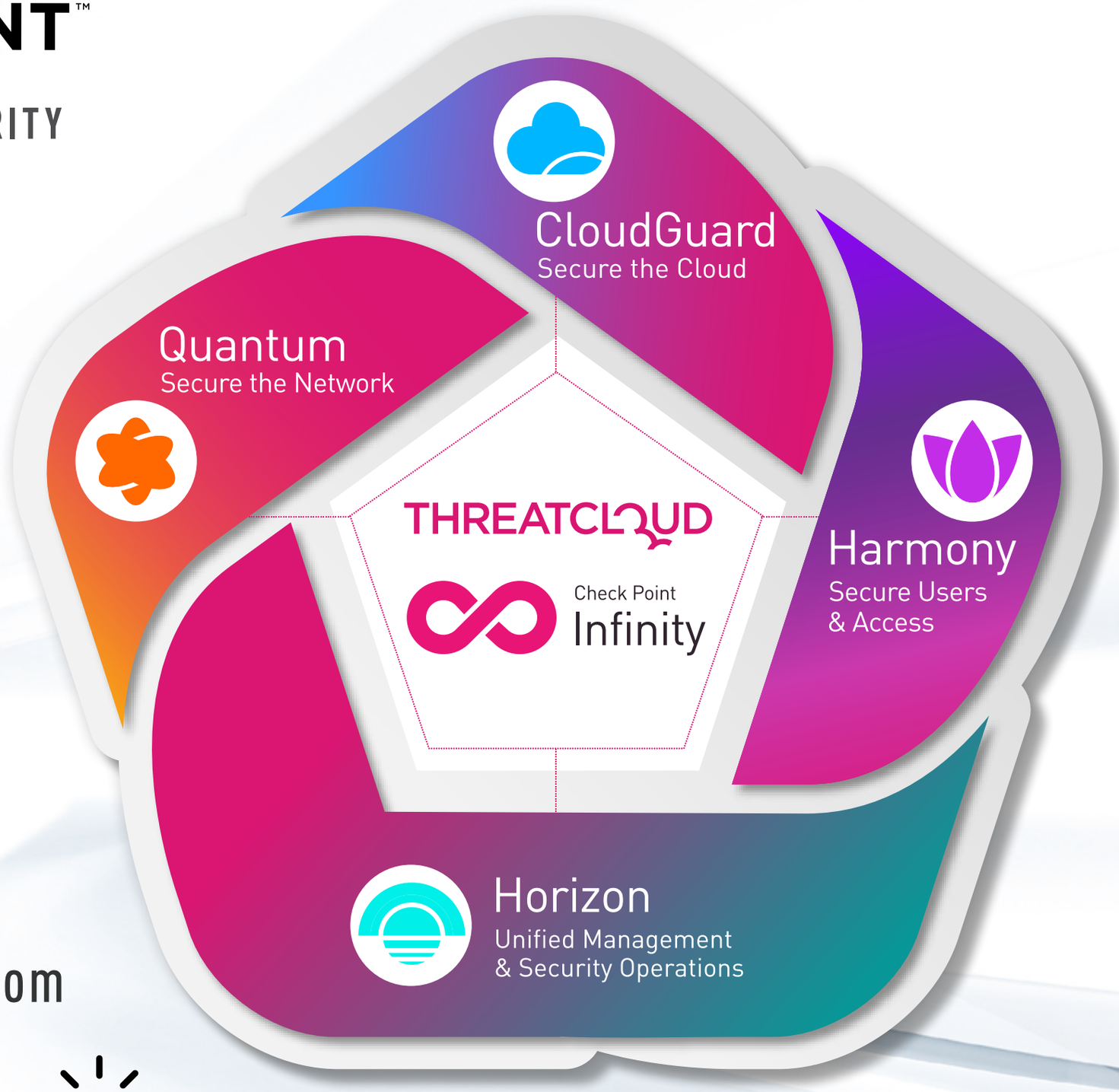
MÁS INFO

» Implementación de IoT en España

COMPARTIR EN REDES SOCIALES

CHECK POINT™

YOU DESERVE THE BEST SECURITY



MÁS INFORMACIÓN:

www.checkpoint.com/es

info_iberia@checkpoint.com

MERCADO PC:
LA INESTABILIDAD DE UN NEGOCIO CLÁSICO

MIGUEL ÁNGEL GÓMEZ

En 2020 y 2021, durante la pandemia, el mercado PC vivió un momento dulce, dado que las empresas tuvieron que adaptarse a las nuevas exigencias del negocio, poniendo en manos de sus profesionales equipos que les permitieran seguir con su trabajo sin necesidad de ponerse delante del equipo de la oficina. Sin embargo, ahora nos encontramos en un momento de cierta inestabilidad, si bien no todo es negativo. Descubramos qué momento vive el negocio PC y hacia dónde se encamina.

Para conocer los principales detalles de este negocio, hemos conversado con algunos de los jugadores más destacados de este negocio. Tal y como nos explica Marcos Manzano, field product manager de Dell Technologies Client Solutions Spain, "si tomamos como referencia el inicio de la pandemia en marzo de 2020, vemos que la demanda durante los 18 meses siguientes experimentó un fuerte crecimiento de los dispositivos que ayudaron a desempeñar el trabajo desde una ubicación remota. Lógicamente en los siguientes dos años la demanda se ralentizó en lo que se refiere al número de unidades vendidas, aunque hemos visto que las empresas están adquiriendo ordenadores con unas configuraciones más avanzadas que les permitan incrementar la productividad de sus usuarios con el uso de nuevas herramientas como son las aplicaciones colaborativas".

Para Herminio Granero, executive director Core Solutions de Ingram Micro, "el mercado de PC es bastante dinámico, y especialmente en los últimos años, donde se ha vuelto imprescindible en todos los ámbitos, por lo que, tanto en empresas e instituciones como en el hogar, existe una renovación constante tratando de adaptarse a la innovación del mercado. Desde hace algunos años el portátil ha sido el principal protagonista de este mercado, pero el fuerte crecimiento del gaming ha provocado también un incremento de las ventas de ordenadores de sobremesa, que en ocasiones responde mejor a los requerimientos que tiene este público. Y aunque en empresas hemos visto cómo desde la pandemia se acometió una renovación de equipos para apostar por portátiles y convertibles, estamos viendo cómo el sobremesa sigue manteniendo su crecimiento".

Desde el punto de vista de Patricia Núñez, product management and operations director en Lenovo Iberia, "si miramos atrás, el mercado total del PC, tanto enfocado a consumo como a profesional, se ha comportado como una montaña rusa. Durante la pandemia vimos un crecimiento fuerte en las ventas. De cara a este 2023 tenemos una previsión de que el mercado decrezca un 16% y para 2024 prevemos un crecimiento del 5%. En otras palabras, el mercado del PC ha pasado por momentos inestables, pero actualmente el mercado de consumo está bastante estable, con un decremento del 11%, y desde Lenovo ya estamos empezando a ver brotes verdes de recuperación de cara a fin de año. De

> "HEMOS VISTO QUE LAS EMPRESAS ESTÁN ADQUIRIENDO ORDENADORES CON UNAS CONFIGURACIONES MÁS AVANZADAS QUE LES PERMITAN INCREMENTAR LA PRODUCTIVIDAD DE SUS USUARIOS CON EL USO DE NUEVAS HERRAMIENTAS COMO SON LAS APLICACIONES COLABORATIVAS"
>
> **MARCOS MANZANO,**
> field product manager de **Dell Technologies** Client Solutions Spain

hecho, todos aquellos equipos vendidos durante el pico de ventas que se produjo en la pandemia tendrán casi tres años a finales del 2023, por lo que se espera que reemplacen esos dispositivos durante la recta final del 2023 y la primera mitad del 2024. En cuanto al mercado comercial, venimos de caídas por encima del 25%, pero también estamos empezando advertir una recuperación especialmente en los segmentos de administración pública y educación…”

Finaliza esta primera ronda de opiniones Juan Antonio Álvaro, director de compras/purchasing manager de MCR, comentado que “la venta de PC está atravesando uno de los momentos más delicados de los últimos años, prácticamente sustentada por los equipos de sobremesa dedicados a la industria del gaming. Tras unos años explosivos y hasta hoy, la venta de este tipo de dispositivos se ha ido recuperando pero siempre por debajo del crecimiento del mercado. Este 2023 presenta fuertes caídas en el número de unidades. No obstante, según el último Indicador global de PC de IDC, ya se empiezan a detectar signos de crecimiento y prevén que las ventas crezcan finalmente en 2024”.

UN PILAR DEL MERCADO TI

En palabras de Herminio Granero, “tanto para nuestra industria como para Ingram Micro la venta de ordenadores, y todo lo relacionado con su ecosistema, es uno de los pilares del negocio, y lo ha sido desde nuestros inicios hace ya más de 40 años, porque suponen una herramienta fundamental para el trabajo y ocio de los usuarios finales. Nuestra labor es ayudarles a encontrar la solución que mejor se ajuste a sus necesidades, de manera que es una gran oportunidad para trabajar junto a nuestros clientes, y el gran reto de estar a la altura de sus expectativas. Aprovechando nuestra oferta multi-

> “EL NEGOCIO DE PC ES BASTANTE DINÁMICO, Y ESPECIALMENTE EN LOS ÚLTIMOS AÑOS, DONDE SE HA VUELTO IMPRESCINDIBLE EN TODOS LOS ÁMBITOS, POR LO QUE EXISTE UNA RENOVACIÓN CONSTANTE TRATANDO DE ADAPTARSE A LA INNOVACIÓN DEL MERCADO”

HERMINIO GRANERO,
executive director Core Solutions de **Ingram Micro**

tecnológica compuesta de equipos de consultoría y preventa especializados, además de una oferta única de servicios, nos ha permitido seguir creciendo, teniendo cada vez más empresas que confían en Ingram Micro para acompañarlas en su viaje para una digitalización honesta, asequible y eficiente".

Desde el punto de vista de Juan Antonio Álvaro, "en MCR como expertos en gaming quizá seamos los que menos estamos sufriendo la caída en ventas, pero en términos porcentuales sobre el total de nuestra facturación, supone unos porcentajes muy pequeños que están en torno al 1% de nuestra cifra de negocio".

Para Patricia Núñez, "según los datos publicados en los últimos resultados de Lenovo, el negocio de PC representa aproximadamente el 60% de la facturación total de la compañía. No obstante, contamos con varias líneas de negocio que están presentando un crecimiento muy notable, como, por ejemplo, las áreas de infraestructura, soluciones y servicios. Estas áreas seguirán creciendo durante los próximos años y el negocio de Lenovo también continuará diversificándose".

Según Marcos Manzano, "la venta del PC nos permite establecer una relación directa y a diario con nuestros clientes. Esta relación fluida nos permite conocer las necesidades de los usuarios de primera mano y tomar decisiones en el diseño de los equipos que nos permita satisfacer las necesidades diarias de nuestros clientes"

UN DISPOSITIVO EN CONSTANTE EVOLUCIÓN

Continúa Marcos Manzano explicando que "el PC ha tenido una evolución natural a lo largo de los años, cada vez tenemos más formatos disponibles que se adaptan a las distintas necesidades de cada perfil de usuario. El PC es el dispositivo que permite a los trabajadores recibir información, procesarla y tomar decisiones en función de los resultados obtenidos y en este sentido es donde entran en juego los distintos formatos del dispositivo ya que los fabricantes buscamos ofrecer a cada perfil de usuario el dispositivo que le permita desarrollar su trabajo de la mejor manera posible, y no solamente en lo que se refiere al PC propiamente dicho sino también a los accesorios que nos permiten incrementar nuestra productividad. Sobre los formatos que han adquirido protagonismo en esta evolución cabe destacar los portátiles en formato dos en uno convertible, ya que ofrecen al usuario la posibilidad de interactuar con el dispositivo bien a través de la pantalla, del teclado, del ratón, de un lápiz e incluso de la voz".

Desde la perspectiva de Patricia Núñez, "estamos viendo como el segmento profesional está inclinándose hacia vender servicios y soluciones alrededor del PC, donde Lenovo ya es líder, y, por otro lado, vemos cómo se está incorporando la inteligencia artificial en todos los productos. Mirando al mercado de consumo, advertimos un crecimiento en la demanda de las configura-

> "EL MERCADO DEL PC HA PASADO POR MOMENTOS INESTABLES, PERO ACTUALMENTE EL MERCADO DE CONSUMO ESTÁ BASTANTE ESTABLE, Y DESDE LENOVO YA ESTAMOS EMPEZANDO A VER BROTES VERDES DE RECUPERACIÓN DE CARA A FIN DE AÑO"
>
> **PATRICIA NÚÑEZ,**
> product management and operations director en **Lenovo** Iberia

ciones más premium: estas son las que cuentan con mejores paneles, CPU y mayor capacidad de disco duro. Además, también están desarrollándose los segmentos como el gaming, que cuentan con unos precios medios muy por encima de la media, que ya tiene una cuota del 15% del mercado total de consumo".

Según Herminio Granero, "hemos pasado por una etapa en la que los portátiles copaban gran parte del mercado, hasta casi arrinconar a los sobremesa. Ahora vemos una vuelta de los sobremesa, ya sea en sus formatos tradicionales de monitor + torre, o en los nuevos todo en uno, que integran en un mismo dispositivo monitor y torre. Esto no implica que el portátil haya caído, justo lo contrario, ahora tenemos y queremos tener más movilidad, por lo que son equipos más necesarios que nunca. La tendencia es a diversificar contando con los dos productos: un sobremesa para el trabajo en la oficina o para ocio en casa, y un portátil o convertible para moverse, y que además cada vez sea más ligero, precisamente para poder llevarlo consigo de viaje o a lugares públicos en los que trabajar, como cafeterías o centros de coworking. Podemos decir que estamos delante de una pequeña revolución en lo que respecta al mercado PC".

En una línea similar se posiciona Juan Antonio Álvaro, que comenta que "claramente, ha pasado de ser una herramienta imprescindible en el entorno laboral, cediendo mucho terreno ante los dispositivos portátiles como notebooks. Pensamos que ahora mismo el PC de sobremesa se identifica más con dispositivos gaming y de altas prestaciones tipo workstations". ■

¿QUÉ PODEMOS ESPERAR?

De cara a los próximos meses, tal y como lo ven desde MCR, "después de la caída que estamos viviendo en 2023 pasarán a estabilizarse las ventas para 2024".

El portavoz de Ingram Micro añade que "el fuerte incremento en ventas durante 2020 y 2021 provocado por la sobredemanda en tecnología en los años de pandemia hace que volvamos a tener la oportunidad de renovación de equipos a partir de 2024 y 2025. Confiamos en que las campañas que están por venir de forma inminente van a refrendar nuestras expectativas, y estamos preparando Black Friday, campaña de Navidad y rebajas que esperamos ayuden a empujar el negocio a través de importantes promociones para liquidar stock".

En este sentido, desde Lenovo comentan que "además de las categorías que comentábamos antes de equipos premium y gaming, también estamos viendo excelentes perspectivas en convertibles premium y en los equipos convertibles con doble pantalla táctil".

> "LA VENTA DE PC ESTÁ ATRAVESANDO UNO DE LOS MOMENTOS MÁS DELICADOS DE LOS ÚLTIMOS AÑOS, PRÁCTICAMENTE SUSTENTADA POR LOS EQUIPOS DE SOBREMESA DEDICADOS A LA INDUSTRIA DEL GAMING"
>
> **JUAN ANTONIO ÁLVARO,** director de compras/ purchasing manager de **MCR**

HYPERINTELLIGENCE®

Las respuestas le encontrarán

MicroStrategy®
Intelligence Everywhere

DATOS E IDENTIDADES:

EL CENTRO DE GRAVEDAD PARA UNA ESTRATEGIA DE SEGURIDAD GLOBAL

“Se dice que los datos son el petróleo del siglo XXI, pues al igual que en el siglo pasado, no es poderoso quien los posee sino aquel que sabe cómo utilizarlos y protegerlos”, sentencia Emilio Serravalle, Business Development Manager en VU. Y precisamente de cómo proteger y utilizar este oro del siglo XXI, hablaremos en este reportaje.

DESIRÉE RODRÍGUEZ

A medida que muchas organizaciones con visión de futuro adoptan el potencial de transformación de las arquitecturas innovadoras en la nube, surgen nuevas dimensiones de riesgo, centradas en la privacidad, el cumplimiento y la protección de datos confidenciales. Este cambio ha catapultado la seguridad de los datos en la nube a la cima de la agenda de los CISO convirtiendo los datos en el punto clave de la estrategia de seguridad de muchas compañías.

De hecho, en la Cumbre de seguridad y gestión de riesgos de Gartner, Gartner citó algunas de las prioridades apremiantes para los CISO como salvaguardar los datos en sus diversas formas, simplificar el enfoque de ciberseguridad, optimizar los recursos y minimizar los riesgos y maximizar el valor. Pero ¿cómo puede conseguirse todo esto en una época en la que los ciberataques no dejan de crecer y las técnicas utilizadas por lo ciberdelincuentes son cada vez más variadas?

Si preguntamos a los expertos parece que el mayor reto está en el crecimiento exponencial pero también en los cambios en la exposición. Tal y como apunta Anastasia Sotelsek, Principal Sales Engineer de CyberArk “Las cosas solían ser más simples en un mundo solo local. Sobre todo, porque, aunque una empresa tuviera múltiples operaciones en diferentes países, tan solo necesitaba configurar, para cada nueva operación, una nueva infraestructura local y los datos se almacenarían en silos en dicha ubicación local, en el país en el que estaba operando.”

Parece claro que la explosión de la “datificación” en las empresas atañe nuevos riesgos e implica una imperiosa necesidad de gobernar la información, atendiendo a la seguridad y el cumplimiento normativo, lo que implica cada vez un mayor esfuerzo en la localización, clasificación y protección del dato.

Para Eusebio Nieva, director técnico de Check Point Software para España y Portugal: “Una estrategia de seguridad efectiva debe comenzar por la autenticación y autorización adecuadas, seguidas de la implementación de controles de acceso granulares. La monitorización constante y la detección de amenazas son cruciales para proteger tanto los datos como las identidades, ya que permiten identificar y responder a tiempo a posibles ataques.

Los equipos de seguridad tienen muchas herramientas de seguridad en la nube a su disposición, desde Cloud Security Posture Management (CSPM) y Cloud Native Application Protection Platform (CNAPP) hasta Cloud Access Security Broker (CASB) herramientas valiosas para identificar y priorizar riesgos y amenazas en la

> “NO ES PODEROSO QUIEN POSEE (LOS DATOS) SINO AQUEL QUE SABE CÓMO UTILIZARLOS Y PROTEGERLOS”
>
> **EMILIO SERRAVALLE,** Business Development Manager en **VU**

infraestructura, la red y las aplicaciones, pero lo que realmente importa es la capacidad de localizar y proteger los datos, estén donde estén y estén cómo estén. No olvidemos que, tal y como apunta Serravalle, “los datos pueden estar en tránsito o en reposo y se deben implementar mecanismos de seguridad en ambos entornos”.

Sin olvidar, por supuesto, que se ha de ser capaz de distinguir la naturaleza de los datos y su prioridad para la estrategia de negocio. En este ámbito parece que “La conciencia de las organizaciones es cada vez mayor” asegura Jorge Pages, Senior Sales Engineer de WatchGuard Technologies, a lo que añade que ya son familiares “protecciones como son el MFA o protecciones contra la suplantación de la identidad, aunque sigue existiendo por parte de los usuarios cierta resistencia al cambio”.

Teniendo en cuenta estos desafíos y cómo la protección de datos ha evolucionado y se ha complejizado en los últimos años, parece necesario revisar las estrategias de protección y proyectar una nueva estrategia capaz de hacer frente a la nueva realidad. La clave a la hora de establecer este nuevo “camino a seguir” según el portavoz de Watchguard, está en tener en cuenta que “una política de protección de datos se divide en partes:

- **Regulatorio:** debemos cumplir con la regulación ya que esto nos llevaría a graves sanciones
- **Corporativo:** criticidad de la información, debida protección de acceso y respaldo. quién, cuándo, dónde, qué, y cómo se accede a los datos corporativos. Es esencial para evitar brechas y disponer de una debida auditoria y conocimiento de donde está el riesgo.
- **Crisis:** cómo responder ante un problema, ante una brecha de datos.

La idea es disponer de una política que cubra tanto el antes de los datos y sus posibles brechas de seguridad como las consecuencias de cualquier acto sobre ellos” asegura.

SE TRATA DE LOS DATOS

La primera pregunta lógica, al hablar de protección de datos, ha de ser entonces qué tipo de datos almacena la empresa, seguida de la criticidad de esos datos, cuánto riesgo representan para la organización y si se alinean con las políticas de seguridad específicas que se han configurado para protegerlos. Estos, en su conjunto,

> “LA CONCIENCIA DE LAS ORGANIZACIONES ES CADA VEZ MAYOR”
>
> **JORGE PAGES,**
> Senior Sales Engineer de **WatchGuard** Technologies

son los factores críticos que determinan el riesgo real en caso de pérdida o exposición por ciberataque. Y digo exposición porque cada vez son más los ataques que no sólo buscan el robo de datos sino que amenazan a las empresas con su exposición. En la industria se conocer como triple amenaza o "triple extorsión" y representa un riesgo añadido para las empresas pues supone en muchos casos una violación importante de las regulaciones GDPR de la UE y las leyes de privacidad de datos. Además, lejos de disminuir parece que esta tendencia va en aumento y ya se habla de "cuádruple extorsión" en los casos de ransomware. Con este nuevo nivel de extorsión se trata de garantizar que la entidad afectada abone el pago exigido por los atacantes como rescate por la realización del ciberataque.

Proporcionar una hoja de ruta clara parece clave para el futuro de la protección de datos. Más, si cabe en un mundo donde las amenazas cibernéticas evolucionan y la capacidad de actuar de manera rápida y coordinada se vuelve cada vez más crucial para proteger los activos digitales más valiosos: los datos y las identidades.

Y es que, los datos son el centro gravitacional de los sistemas de seguridad a día de hoy pero las identidades se han convertido en el eje central del buen funcionamiento de muchos sistemas. Así lo piensa Sergio Martínez, Iberia regional manager en SonicWall, quien afirma que "las identidades son la "joya de la corona", lo que buscan los ciberdelincuentes para realizar cualquier ataque. Por lo que la defensa de las credenciales, el nuevo perímetro, es absolutamente crítica y esencial". Las cifras lo corroboran: "el 80% de brechas se producen por cuestiones relacionadas con claves o identidades, por tanto, el peso dentro de la estrategia de seguridad debe ser grande" sentencia Pages.

Todos sabemos que a menudo los riesgos más potentes están ligados al robo de datos confidenciales y que, desde hace unos años, una de las formas más habituales de lo-

> HAY QUE EVITAR LA "BARRA LIBRE" EN EL ACCESO

SERGIO MARTÍNEZ,
Iberia regional manager en **SonicWall**

> PARA IR POR DELANTE DE LAS AMENAZAS HAY QUE ADOPTAR UN ENFOQUE MÁS PROACTIVO

EUSEBIO NIEVA,
director técnico de **Check Point** Software para España y Portugal

grarlo pasa por hacerse primero con las credenciales necesarias para usurpar la identidad de un usuario y así pasar desapercibido. Teniendo esto en cuenta, no es de extrañar

> LA TENDENCIA ES IR AL CONTROL DE ACCESO BASADO EN ROLES (RBAC)

ANASTASIA SOTELSEK,
Principal Sales Engineer de
CyberArk

que para el directivo de Sonicwall el almacenamiento de datos requiera "una nueva ciberdefensa, basada en estrategias ZTNA, cero confianza, y en la compartimentación de los mismos. Hay que evitar la "barra libre" en el acceso".

EL FUTURO DE LA PROTECCIÓN DE DATOS

A la luz de estas prioridades, Gartner también destacó la tendencia fundamental de los sistemas de seguridad integrados. Imagine un ecosistema holístico donde los controles proactivos y predictivos armonizan con las medidas preventivas y los mecanismos de detección. Dicho entorno permite a los profesionales de la seguridad monitorear, evaluar, detectar y responder continuamente a riesgos multifacéticos. Este enfoque integrado cataliza el paso de la reacción a la anticipación y la resolución a la prevención.

Así lo cree también Eusebio: "No cabe duda en que la protección de datos seguirá siendo una prioridad y se volverá aún más integral en las estrategias de ciberseguridad de las empresas a medida que la tecnología y las amenazas evolucionen". Sin embargo, avisa: "para ir por delante de las amenazas hay que adoptar un enfoque más proactivo".

Para Anastasia, la tendencia es ir "al control de acceso basado en roles (RBAC). Con este tipo de controles es posible configurar políticas de acceso basadas en la ubicación, que garanticen que quienes necesitan acceso a los datos (y solo quienes necesitan acceso, según las leyes y reglamentos de esa región) tendrán acceso. De esa manera, puede satisfacer los requisitos de cumplimiento mientras disfruta de los beneficios de usar una solución centralizada que le otorga visibilidad de sus secretos en todos sus entornos". ■

MÁS INFO +

» La autoridad española de Protección de Datos lanza una nueva versión de Gestiona RGPD

» ¿Qué preocupa a los CIO y CISO españoles en ciberseguridad?

LAS TRES PATAS DE LA PROTECCIÓN DE DATOS

Hablar de protección no es tarea fácil en el mundo en el que vivimos. Sin embargo, parece claro que las claves de una buena protección pasan por tener en cuenta 3 aspectos fundamentales:

>> **Regulatorio:** debemos cumplir con la regulación para evitar sanciones y posibles problemas derivados

>> **Corporativo:** debemos tener claro quién, cuándo, dónde, qué, y cómo se accede a los datos corporativos. Es esencial para evitar brechas y conocer dónde está el riesgo.

>> **Ciberresiliencia:** debemos tener una hoja de ruta que muestre cómo responder ante un problema, y haberlo practicado.

Cloud complexity?
Find simplicity.

In one platform.

NUTANIX

BIOMETRÍA PARA LA GESTIÓN DE IDENTIDADES, UNA OPCIÓN EFICIENTE Y ÓPTIMA PARA EL USUARIO

it User TECH & BUSINESS

bFY

BIOMETRÍA, ¿EL FUTURO DE LA GESTIÓN DE IDENTIDADES?

Si hay un elemento crítico en las operaciones empresariales actuales es la gestión de identidades y acceso de los usuarios, conocido habitualmente por sus siglas en inglés, IAM. Tradicionalmente, esta gestión se ha llevado a cabo con nombres de usuario y contraseñas, pero se ha demostrado que ya no es una forma eficaz por la cada vez más frecuente y efectiva actividad de los hackers. Frente a esta visión tradicional, la seguridad biométrica se consolida como una alternativa efectiva, sencilla de implementar y, sobre todo, con una mejor experiencia de uso.

La tecnología forma parte de todas y cada una de las actividades de los usuarios, tanto a nivel personal como profesional. Esta tecnología está en constante evolución, por lo que las prácticas y herramientas que han sido efectivas y eficientes durante un tiempo, pueden dejar de serlo frente a otras alternativas que aporten un mayor valor a los usuarios y las organizaciones. Y este es caso de la identificación de usuarios mediante nombre de usuario y contraseña, que ya no aporta la seguridad que necesitan las empresas e instituciones actuales, sobre todo por la actividad de los hackers, cada día más importante, efectiva y nociva.

En los últimos años, las violaciones de seguridad han aumentado de forma muy considerable y, según el Informe Cost of Data Breach Report de IBM, “las credenciales robadas o comprometidas no solo fueron la causa más común de filtración de datos, sino que, con 327 días, fueron las que mayor tiempo tomaron para ser identificadas”. De hecho, según la firma, el promedio del coste de estas brechas de seguridad superaba los 150.000 dólares.

Las soluciones de Gestión de Identidad y Acceso (IAM) deben ser efectivas para gestionar y asegurar el acceso a información crítica dentro de las organizaciones solo por usuarios autorizados. Es, en definitiva, un marco habilitador de los procesos empresariales, políticas y tecnologías para la gestión de identidades digitales, permitiendo el acceso solo a aquellos usuarios realmente capacitados para ello.

UNA NUEVA REALIDAD CADA DÍA MÁS PRESENTE

Sin embargo, como ya hemos mencionado, los métodos tradicionales de autenticación de identidad, como

LAS SOLUCIONES DE GESTIÓN DE IDENTIDAD Y ACCESO (IAM) DEBEN SER EFECTIVAS PARA GESTIONAR Y ASEGURAR EL ACCESO A INFORMACIÓN CRÍTICA DENTRO DE LAS ORGANIZACIONES SOLO POR USUARIOS AUTORIZADOS

contraseñas y nombres de usuario, se muestran ineficaces contra los niveles y eficiencia de los ciberataques actuales. Con lo que era necesario poner sobre la mesa una alternativa que sirviera para reemplazar estos elementos. Así, la tecnología de autenticación biométrica ha surgido como una de las propuestas más efectivas para la IAM, dado que se basa en características fisiológicas o comportamentales únicas, como huellas dactilares, reconocimiento facial y escaneo del iris, para verificar la identidad de un usuario, y esto provoca que sea una opción más segura que la autenticación basada en contraseñas tradicionales, ya que no es factible que los hackers repliquen datos biométricos de otra persona.

> **LA TECNOLOGÍA DE AUTENTICACIÓN BIOMÉTRICA HA SURGIDO COMO UNA DE LAS PROPUESTAS MÁS EFECTIVAS PARA LA IAM, DADO QUE SE BASA EN CARACTERÍSTICAS FISIOLÓGICAS O COMPORTAMENTALES ÚNICAS, COMO HUELLAS DACTILARES, RECONOCIMIENTO FACIAL Y ESCANEO DEL IRIS**

Y las cifras de las consultoras respaldan esta percepción. Así, según los datos que maneja la consultora MarketsandMarkets, el mercado mundial de autenticación e identificación biométrica, situado en torno a los 42.900 millones de dólares en 2022, podría suponer hasta 82.900 millones en 2027, lo que supone un incremento anual medio del 14,1%, un incremento que, según el análisis de la consultora no se centra en un único sector económico, sino que se apoyaría en una creciente demanda de este tipo de soluciones en diferentes segmentos económicos y verticales industriales.

VENTAJAS QUE APORTA LA BIOMETRÍA A IAM

Como decíamos, la tecnología biométrica es altamente efectiva para asegurar los sistemas de IAM. De hecho, una reciente investigación de Biometrics Institute señalaba que el uso de la tecnología biométrica reduce de manera destacada el riesgo de violaciones de seguridad y robo de datos, y mejora la seguridad general de los sistemas de IAM.

Así, son varias las ventajas que aporta la biometría a IAM, y algunas de las más destacadas son:

➤ **Facilita el acceso en cualquier lugar.** En la actualidad las personas necesitan todo el tiempo sus identidades para utilizar servicios y recursos. En ese sentido, requieren acceso a cualquier plataforma sin límites utilizando sus identificaciones, eliminando así las barreras para que los clientes ingresen a la plataforma en cualquier momento y lugar.

➤ **Favorece la conexión entre las distintas partes.** La transformación digital que está produciéndose cada vez entre más organizaciones, obliga a la necesidad de que las personas, las aplicaciones y los dispositivos se mantengan conectados unos con otros. Y, como era de esperar, todos estos procesos traen consigo algunas amenazas de seguridad.

➤ **Mejora la productividad.** IAM por biometría automatiza el ingreso de nuevo personal y te facilita el acceso a todos los componentes del

sistema con el que funciona la empresa. Esto permite reducir tiempos en la entrega de accesos para que comiencen a producir de inmediato.

➤ **Optimiza la experiencia del usuario**. Recordar tantos nombres de usuario y contraseñas para acceder a las redes sociales, a las entidades bancarias y a demás servicios en Internet se convierte en un reto para las personas. Con IAM por biometría se obtiene una identidad que brinda acceso a diferentes sistemas.

LOS USUARIOS PREFIEREN SISTEMAS DE AUTENTICACIÓN BIOMÉTRICA

Un informe de Transparency Market Research apunta que la industria biométrica mundial elevará sus ingresos hasta superar los 136.000 millones en 2031, lo que representan un incremento medio anual por encima del 13%.

La clave puede encontrarse en una **encuesta publicada por PYMNTS**, que confirma más de uno de cada tres usuarios está dispuesto a utilizar métodos de autenticación biométrica. De hecho, uno de cada dos afirma estar preparado para decir adiós a las contraseñas. Unos datos que coinciden con los de otra **encuesta publicada por VISA**, según la cual, en EE.UU. más del 85% de los usuarios de consumo tiene interés en usar la biometría para identificarse o para realizar pagos, mientras que 7 de cada 10 piensan que es más sencillo que otros métodos, y casi la mitad cree que es más seguro que las contraseñas.

También son coincidentes los datos del **informe de Servicios de Identidad Digital de iProov**, que indican que el 55% de los encuestados ya utiliza biometría, ya sea reconocimiento facial o reconocimiento de huellas dactilares, para desbloquear sus dispositivos móviles.

➤ **Incrementa la rentabilidad:** La autenticación biométrica hace que no sea necesario emitir y reemplazar continuamente tokens de autenticación ni restablecer contraseñas olvidadas. Además, ayuda a prevenir las pérdidas económicas debido a violaciones de seguridad, la implementación de hardware o los gastos asociados al envío de mensajes de texto (SMS) cada vez que se requiere autenticación.

➤ **Se trata de una solución escalable:** La autenticación biométrica puede escalar fácilmente para satisfacer las necesidades de las grandes organizaciones, lo que la convierte en una solución ideal para empresas con muchos empleados. ■

MÁS INFO +

» Cost of Data Breach Report

» Next generation biometric technologies market

COMPARTIR EN REDES SOCIALES

#ENTREVISTA

Nuestra estrategia es brindar nuestra innovación, tecnología y protocolo de acceso, como marca blanca para la institución

RODRIGO JIMÉNEZ, MANAGING DIRECTOR DE B-FY

La gestión de identidades es uno de los elementos clave en la seguridad de las empresas e instituciones, y uno de los puntos de entrada de los atacantes. Utilizando la biometría se ofrece una solución más amigable con los usuarios y más robusta desde el punto de vista de la seguridad. Para ver cómo afronta este reto B-FY, hemos hablado con su Managing Director en nuestro país.

¿Cuáles son los principales problemas de seguridad a los que se enfrentan las empresas? ¿Cómo ha ido evolucionando esta realidad en los últimos meses/años?

> “B-FY OFRECE UNA SOLUCIÓN INNOVADORA, QUE CREA UN NUEVO PROTOCOLO DE ACCESO UTILIZANDO LA CAPACIDAD BIOMÉTRICA DEL DISPOSITIVO MÓVIL DEL USUARIO, SIN USO DE CONTRASEÑAS, NI ENVÍO DE PATRONES BIOMÉTRICOS POR INTERNET”

Según informes recientes de empresas de ciberseguridad, los robos tanto de datos personales como de contraseñas se están disparando. El informe anual Global Digital Fraud Trends de TransUnion (publicado en marzo de 2022) revela que entre 2019 y 2021, el crecimiento en la tasa de sospecha de fraude digital a escala global aumentó en un 52,2 %. La mayor parte de los ataques parten del robo de bases de datos y venta de identidades o credenciales.

Según el Microsoft Digital Defense Report, entre julio de 2020 y junio de 2021, el mundo fue testigo del florecimiento de la economía del ciberdelito que registró un fuerte aumento. Este informe afirma que la ciberdelincuencia es un mercado maduro que sigue creciendo, tanto en tamaño como en sofisticación, mientras que los ciberdelincuentes cambian continuamente “de táctica, valiéndose de los eventos actuales para aprovecharse de objetivos vulnerables y avanzar en su actividad a través de nuevos canales”. De acuerdo con el mismo estudio, el robo de identidad real aumentó un 81% en todas las industrias en el mismo período.

Los métodos de los ciberdelincuentes son cada vez más agresivos y, en los últimos tiempos, se orientan con mayor frecuencia a PYMES e individuos que, a diferencia de las grandes corporaciones, no tiene los medios o la capacidad de defenderse. El método de autenticación de identidad basado en usuario y contraseña es el eslabón más débil –el método menos seguro, en otras palabras– en todo el esquema de ciberseguridad.

Los sistemas tradicionales de seguridad basados en la autenticación del conocimiento están demostrando ser ineficientes contra el cibercrimen. Además, los usuarios se ven abrumados por la necesidad de hacer seguimiento a un sinfín de contraseñas, que, según un estudio reciente, no son menos de 100 por persona. Como es de esperar, nadie va a memorizar 100 contraseñas distintas. Al final las personas terminan reutilizando un pequeño grupo de contraseñas para todos esos servicios. Además, en muchos de los casos, las contraseñas serán muy básicas, es decir, fácilmente vulnerables.

Por otro lado, los sistemas de seguridad de autenticación multifactor (MFA) se ponen a prueba todos los días. Aunque MFA es bueno, muchas de las implementaciones actuales son vulnerables, consumen mucho tiempo de los usuarios y son difíciles de implementar para las empresas.

¿Qué retos, tanto de seguridad como normativos, tienen que afrontar las empresas actualmente?

Para el 83% de las empresas, según el informe Cost of a data breach 2022 de IBM, la cuestión no es si se producirá una filtración de datos, sino cuándo. A escala global, el coste total medio de una filtración de datos ronda los 4,35 millones de dólares. Si hablamos de EE.UU., el coste se duplica, para llegar a los 9,44 millones de dólares, según este mismo informe.

Para las empresas, tener procesos seguros de identificación y autenticación son fundamentales tanto para el alta de nuevos clientes y empleados, así como para la prestación de servicios. Así, el uso de la tecnología biométrica para la autenticación de identidad se está convirtiendo rápidamente en la solución preferida de las empresas. No obstante, existen algunas preguntas fundamentales que las empresas deben hacerse antes de abordar cualquier proyecto que involucre datos biométricos. Para los usuarios, mantener la privacidad de sus datos también es una gran preocupación. Alrededor del 74% de los usuarios de Internet en los EE.UU. están

más preocupados que nunca por su privacidad en línea y el 79% de los usuarios de Internet de todo el mundo sienten que han perdido por completo el control sobre sus datos personales.

También en el frente del consumidor, la investigación de KPMG Corporate data responsibility: Bridging the consumer trust gap informa de que alrededor del 47% de los encuestados señaló estar preocupado por la posibilidad de que sus datos fueran hackeados, mientras que el 51% estaba preocupado porque pudieran venderlos.

Por lo tanto, dado que la vida se vuelve cada vez más digital, asegurar los datos de los usuarios no es solo una cuestión económica, sino una cuestión de confianza. La de los usuarios en relación con cómo las empresas que recopilan su información personal pueden usarla o mantenerla segura.

En los últimos años, casi todos los países del mundo han emitido algún tipo de regulación para proteger la privacidad de los datos. Estas leyes profundizan en cómo se recopila la información, cómo se informa a los interesados y qué control tiene un interesado sobre su información una vez que se transfiere.

> "EL CIBERATAQUE Y EL FRAUDE ONLINE SON UNA AMENAZA REAL Y CRECIENTE EN TODAS LAS EMPRESAS, INSTITUCIONES DE CUALQUIER VERTICAL, TANTO EN ESPAÑA, COMO EN EL EXTRANJERO"
>
> **RODRIGO JIMÉNEZ,**
> Managing Director de **B-FY**

¿Cuál es la respuesta que ustedes les dan para afrontar estos retos?
Como hemos visto, RGPD se considera un estándar en lo que respecta a la protección de datos, incluidos los datos biométricos. Uno de los pilares sobre los que se asienta esta empresa es proteger a las personas frente al fraude y proteger su identidad. El protocolo de identificación de B-FY ha sido diseñado de acuerdo con las directivas europeas de privacidad de datos, cuidando al máximo la privacidad del usuario y la de la empresa. Al utilizar el sistema B-FY para identificar a sus usuarios, nuestros clientes integran nuestro servicio a través de una librería en su aplicación. B-FY no recopila ni almacena datos biométricos de los usuarios.

Para verificar la identidad del usuario, B-FY solo necesita su correo electrónico y su número de teléfono, asociándose el dispositivo a una sola persona. Los datos de registro (teléfono y correo electrónico) se almacenan en una base de datos, que se encuentra en una red estanca solo accesible desde la propia plataforma B-FY. El factor biométrico del usuario está asociado al dispositivo que ha registrado como suyo, y sus datos quedan siempre bajo su control y custodia.

¿Cuál es el elemento diferencial de B-FY para ayudar a las empresas? ¿Cuál es vuestra estrategia de negocio?
Nuestra misión es identificar personas, eliminar el fraude y proteger la privacidad. Hemos vistos desde hace varios años, el auge del smartphone a nivel mundial, y sobre todo la mejora y robustez de la tecnología biométrica que vienen en estos dispositivos. Se predice que para el 2024, un 65% de todas las identificaciones de los individuos procederán de la capacidad biométrica del móvil. Segundo, el crecimiento de las aplicaciones móviles por parte de las instituciones. También ha ocurrido el aumento de los ciberataques por robos de credenciales o fraude de ID y el endurecimiento de las leyes de protección de datos y privacidad del usuario, sobre todo en Europa.

Por ello, B-FY lanzó al mercado, en 2022, una solución innovadora, creando un nuevo protocolo de acceso, utilizando la capacidad biométrica del dispositivo móvil del usuario, sin uso de contraseñas, ni envío de patrones biométricos por internet. Nuestra estrategia es brindar nuestra innovación, tecnología y protocolo de acceso, como marca blanca para la institución. De tal forma que, para el usuario final, esto sea transparente, y vea a la institución, ofreciendo este servicio a todos sus clientes finales, a través de su App móvil.

Cualquier usuario: el cliente, empleado, colaboradores, dirección, equipos de seguridad y tecnología, podrán usar su dispositivo móvil para identificarse de forma segura, sin uso de contraseñas, usando la App de la institución como herramienta omnicanal, tanto para accesos a espacios físicos como digitales. B-FY es una solución de identificación como servicio que aplica el principio identity-first (identificar siempre a la persona antes

de dar acceso al servicio). La identificación veraz de la persona autorizada es el punto más importante del modelo zero-trust. B-FY utiliza la biometría que los usuarios poseen en sus dispositivos móviles para poder identificarse verazmente, eliminando la necesidad de patrones biométricos en servidores centralizados, contraseñas y tarjetas de acceso, para obtener acceso a los servicios a la cual están autorizados, todo ello mediante un método muy simple y escalable.

Nuestro modelo de acceso con biometría descentralizada evita el riesgo de las soluciones basadas en biometría centralizada, que almacenan los patrones biométricos de los usuarios en sus servidores, provocando un alto riesgo para la protección de privacidad de los usuarios y la suplantación de identidad por parte de los ciberatacantes.

Con B-FY, se elimina la necesidad de enviar, almacenar, comparar datos sensibles de los usuarios, que finalmente pueden ser robados y utilizados posteriormente para atacar a las instituciones. De esta forma, los ciberatacantes se ven desarmados de su método usual de ataque, que es a través del robo de credenciales y de suplantación de identidad. La solución omnicanal de B-FY, a través de la App de la institución, permite una excelente experiencia de usuario englobando todos los casos de uso más frecuentes en una empresa. B-FY permite identificar clientes finales, empleados, personal externo, equipo de dirección, equipos de seguridad e IT, para poder darles acceso a servicios y espacios tanto físicos como digitales, utilizando tecnología de vanguardia que deja fuera a los ciberacriminales y evita fraudes por suplantación de identidad.

> “CON B-FY SE ELIMINA LA NECESIDAD DE ENVIAR, ALMACENAR, COMPARAR DATOS SENSIBLES DE LOS USUARIOS, QUE FINALMENTE PUEDEN SER ROBADOS Y UTILIZADOS POSTERIORMENTE PARA ATACAR A LAS INSTITUCIONES”

¿Cuál es el perfil adecuado de cliente con el que suelen trabajar?
B-FY utiliza la biometría que los usuarios poseen en sus dispositivos móviles para poder identificarse verazmente, eliminando la necesidad de patrones biométricos en servidores centralizados, contraseñas y tarjetas de acceso, para obtener acceso a los servicios a la cual están autorizados, todo ello mediante un método muy simple y escalable.

Todas aquellas empresas que dispongan de una estrategia de seguridad de nivel crítico y una fuerte orientación al cliente y en concreto, que dispongan de una aplicación móvil como oferta fundamental de servicio para sus clientes finales, corresponden con el perfil de clientes que buscamos.

¿Qué verticales de negocio son las que más foco ponen en la seguridad?
En líneas generales, son las grandes corporaciones, instituciones y multinacionales las que están más preparadas ante posibles ataques o fraudes. Estas disponen de mayores recursos financieros y humanos para establecer una robusta estrategia de seguridad, junto con un equipo interno especializado en ciberseguridad. Esto es así en todos los sectores donde operan y en diferentes verticales.

Por la misma razón, las PYMES, tanto en España como en el extranjero, son las que ofrecen mayor vulnerabilidad ante posibles ataques o fraudes, al disponer de menores recursos económicos y de personal experto en seguridad, para poder afrontar estos nuevos retos de posibles ataques o fraude.

El ciberataque y el fraude online son una amenaza real y creciente en todas las empresas, instituciones de cualquier vertical, tanto en España, como en el extranjero. No obstante, desde B-FY, tenemos un foco especial a los sectores de Finanzas, Salud, Educación, Energía y Telecomunicaciones que responden a un alto índice de criticidad en la seguridad y a la vez disponen de una importante estrategia de servicios y atención al cliente a través de sus aplicaciones móviles. ■

¿POR QUÉ LA BIOMETRÍA ES UNA SOLUCIÓN ESENCIAL EN LA EVOLUCIÓN DE IAM PARA GARANTIZAR LA SEGURIDAD DE LA INFORMACIÓN?

RODRIGO JIMÉNEZ
Managing Director de B-FY

La IAM abarca la autenticación, autorización, gestión de usuarios y en este artículo, exploraremos cómo la tecnología biométrica se ha convertido en una solución esencial para abordar los desafíos actuales en ciberseguridad y protección de datos personales.

La Gestión de Identidad y Acceso (IAM) se ha convertido en un componente esencial de las operaciones empresariales modernas debido a la creciente amenaza de ciberataques, la necesidad de cumplir con regulaciones de privacidad de datos, la complejidad de las infraestructuras tecnológicas, el aumento de la movilidad y el trabajo remoto de los empleados, así como la búsqueda de experiencias de usuario mejoradas y la protección de la privacidad del usuario.

MEJORAR LA AUTENTICACIÓN

A medida que los métodos tradicionales de autenticación, como contraseñas y nombres de usuario, se han vuelto cada vez más vulnerables a los ciberataques, la tecnología de autenticación biométrica ha surgido como una de las soluciones más efectivas para la IAM.

La tecnología biométrica se basa en características únicas y difíciles de replicar, como huellas dactilares, reconocimiento facial y escaneo del iris, para verificar la identidad de un usuario.

Esta tecnología ofrece una ventaja significativa en términos de seguridad. Es prácticamente imposible que alguien pueda replicar los datos biométricos de otra persona. Según un informe de MarketsandMarkets, se espera que el mercado global de autenticación e identificación biométrica crezca a una tasa anual compuesta del 14,1%, alcan-

zando los 82,900 millones de dólares en 2027 debido a la creciente demanda de sistemas seguros de autenticación e identificación en diversas industrias.

IMPLEMENTACIÓN DE MEJORES PRÁCTICAS

A pesar de sus ventajas, la tecnología biométrica también enfrenta desafíos. Para aprovechar al máximo su potencial, las organizaciones deben implementar las mejores prácticas:

- **Evaluaciones de riesgos.** Se deben realizar evaluaciones periódicas de riesgos para identificar posibles vulnerabilidades en el sistema.
- **Almacenamiento seguro de datos biométricos.** Los datos biométricos deben almacenarse y cifrarse de manera segura para proteger la privacidad de los usuarios.
- **Políticas claras y transparencia.** Se deben proporcionar políticas y pautas claras para el uso de la tecnología biométrica, y los usuarios deben tener la opción de optar por no utilizarla si tienen preocupaciones sobre la privacidad.

VENTAJAS DE LA BIOMETRÍA EN IAM

La investigación ha demostrado que la tecnología biométrica es altamente efectiva para asegurar los sistemas de IAM. Un estudio del Biometrics Institute reveló que el uso de la tecnología biométrica puede reducir significativamente el riesgo de violaciones de seguridad y robo de datos, mejorando la seguridad general de los sistemas IAM. Algunas de las ventajas clave de la biometría sobre los métodos tradicionales de IAM incluyen:

> “OFRECEMOS UNA ALTERNATIVA RENTABLE Y ALTAMENTE SEGURA A LOS MÉTODOS TRADICIONALES DE IAM, LO QUE PERMITE A LAS ORGANIZACIONES MEJORAR LA SEGURIDAD Y LA EXPERIENCIA DEL USUARIO”
>
> **RODRIGO JIMÉNEZ,** Managing Director de **B-FY**

1. **Mayor seguridad.** La autenticación biométrica es inherentemente más segura que las contraseñas, que pueden ser hackeadas o robadas.
2. **Experiencia del usuario mejorada.** La autenticación biométrica es más rápida y conveniente para los usuarios, eliminando la necesidad de recordar contraseñas o llevar tokens de autenticación.
3. **Rentabilidad.** La autenticación biométrica puede ser más rentable a largo plazo al evitar la emisión y el reemplazo continuo de tokens de autenticación y la recuperación de contraseñas olvidadas.
4. **Escalabilidad.** La autenticación biométrica puede escalar fácilmente para satisfacer las necesidades de organizaciones de todos los tamaños.

LA SOLUCIÓN DE B-FY

En B-FY, nuestra principal preocupación es proteger a las personas y su identidad. Nuestro sistema utiliza la biometría para autenticar a los usuarios de manera segura y eficiente, eliminando la necesidad de contraseñas que pueden ser hackeadas o robadas. Además, no almacenamos patrones biométricos del usuario, lo que garantiza la privacidad.

Nuestra solución es fácil de usar y se integra sin problemas en las operaciones de nuestros clientes. Ofrecemos una alternativa rentable y altamente segura a los métodos tradicionales de IAM, lo que permite a las organizaciones mejorar la seguridad y la experiencia del usuario. La tecnología biométrica descentralizada que utilizamos garantiza la protección de los datos de los usuarios y la prevención de ciberataques.

En un mundo digital en constante evolución, la tecnología biométrica se ha convertido en un pilar fundamental para la Gestión de Identidad y Acceso. Con B-FY, estamos comprometidos a brindar una solución de IAM que sea segura, eficiente y orientada al usuario, ayudando a las organizaciones a abordar los desafíos actuales y futuros de seguridad y privacidad de datos. ■

MÁS INFO +

- State of Biometrics
- Biometric systems market

EL SECTOR EDUCATIVO, EN CONTINUO APRENDIZAJE TECNOLÓGICO

Tras la crisis sanitaria de 2020 el sector educativo español se vio obligado a adoptar nuevas tecnologías para habilitar la formación a distancia, forzando una digitalización para la que no había un plan bien definido. A lo largo este Encuentro ITDM Group analizamos cómo ha evolucionado este ámbito en los últimos años y qué desafíos afronta la enseñanza a medida que se adentra en la era digital.

Abordar la transformación digital supone un reto para cualquier industria y requiere una buena planificación, recursos y tiempo para llevarla a cabo. En el caso del sector educativo español no ha sido así, ya que antes de la pandemia apenas había iniciativas digitales sólidas, menos aún un plan de transformación digital, y este episodio impuso grandes cambios. En el "Encuentro ITDM Group: El sector Educativo, en continuo aprendizaje tecnológico", hemos reunido a expertos en tecnología y en el entorno de la enseñanza para conocer en profundidad en qué estado se encuentra el sector en términos de digitalización, qué iniciativas se han puesto en

marcha y cómo está transformándose el modelo educativo al adoptar las nuevas tecnologías.

Lo hacemos a través de dos mesas redondas en las que han participado responsables de diferentes proveedores de infraestructura, servicios digitales y ciberseguridad, y representantes de instituciones educativas que están viviendo en primera persona esta transformación. Además, entrevistamos a Andrés Prado, responsable TIC de la Universidad Castilla-La Mancha, quien nos habla sobre cómo han cambiado su enfoque de ciberseguridad tras sufrir un ataque cibernético en 2021. También contamos con una ponencia a cargo de José Luis Pérez, director de Análisis de la firma Penteo, que analiza en detalle el estado de la digitalización en el sector educativo español y cómo están evolucionando las estrategias formativas a raíz de esta modernización. Además, explica qué tecnologías han irrumpido en la enseñanza y cómo afectará la llegada de innovaciones como la inteligencia artificial generativa.

RETOS DE LA DIGITALIZACIÓN EDUCATIVA

La primera mesa de debate de este Encuentro ITDM Group, patrocinada por las firmas B-FY y Sonicwall, reunió a representantes de un gran número de instituciones de enseñanza, la mayoría de ellos con un perfil técnico alto y con responsabilidades en el ámbito digital, que hablaron sobre su situación y las problemáticas a las que se enfrentan. Concretamente, asistieron José Ignacio García, Deputy Digital Innovation de ESIC Business & Marketing School; Marc Paús, Deputy Director Information Technology de IESE Business School; Juan Luis Moreno, Chief Product & Innovation Officer de The Valley Digital Business School; Noelia Gutiérrez, Directora de IT de la Universidad Católica de

DESCARGA EL DOCUMENTO COMPLETO

DESCARGAR

ENTREVISTA>> Andrés Prado explica cómo ha cambiado la estrategia de seguridad de la UCLM a raíz del ataque sufrido en 2021.

MESA REDONDA>> Debatimos sobre los desafíos que acompañan a la transformación digital del sector educativo español.

Ávila; Juan Manuel Corpa, Vicerrector de Ordenación Académica y Digitalización de la Universidad CEU Cardenal Herrera; Juan Ramón Velasco, Vicerrector de Innovación Docente y Transformación Digital de la Universidad de Alcalá; Susana Álvarez, Vicerrectora de Innovación Docente y Transformación Digital de la Universidad de Valladolid; Daniel Magaña, Director de la Agenda de Transformación Digital de la Universidad Nebrija; Víctor Robles, Vicerrector de Estrategia y Transformación Digital de la Universidad Politécnica de Madrid; y Nayra Deníz, CTO de U-TAD, Centro Universitario de Tecnología y Arte Digital. Por la parte de proveedores tecnológicos, la mesa contó con la presencia de Rodrigo Jiménez, Managing Director de B-FY; y Eduardo Brenes, Iberia Territory Manager de SonicWall.

Uno de los temas principales sobre los que debatieron los asistentes es la necesidad de modernizar las estrategias formativas a través de modelos híbridos, que combinen la forma tradicional de impartir clases con las nuevas posibilidades que habilita la tecnología, tanto para la educación a distancia como para complementar la docencia con herramientas y contenidos digitales. Otro tema clave de este debate es el impacto cada vez mayor que tienen las nuevas herramientas de inteligencia artificial generativa en el ámbito estudiantil, y cómo se debería integrar esta tecnología para maximizar sus beneficios y evitar los riesgos que supone para el sector y para los propios estudiantes.

La gestión del talento digital también preocupa al sector de la enseñanza, ya que la introducción de nuevas tecnologías genera una importante resistencia. También existe una patente falta de conocimientos digitales entre el profesorado y los propios alumnos, una brecha que se debe cerrar para que los modelos educativos puedan adaptarse a una época en la que lo digital está permeando todas las capas de la sociedad. Los representantes de los proveedores tecnológicos que asistieron a esta mesa redonda escucharon las inquietudes y necesidades de las instituciones de ense-

PONENCIA>> José Luis Pérez comenta el progreso digital del sector y el impacto de tecnologías como la IA.

MESA REDONDA>> Debatimos sobre el progreso digital de la enseñanza y los riesgos cibernéticos a los que se enfrenta.

ñanza y plantearon cuáles pueden ser las tecnologías clave para lograr los objetivos del sector educativo, aportando soluciones y destacando el papel de las tecnologías disruptivas como la inteligencia artificial.

EL SECTOR EDUCATIVO, EN CONTINUO APRENDIZAJE TECNOLÓGICO, Y SU CIBERPROTECCIÓN

En la segunda mesa redonda que forma parte de este encuentro analizamos cómo ha evolucionado la enseñanza en España a nivel digital y qué retos enfrentan los centros educativos de cara al futuro, poniendo especial foco en la ciberseguridad. Para ello contamos con la presencia de Antonio Anchustegui, Channel Manager de Barracuda Networks para España; Eusebio Nieva, director técnico de Check Point Software para España y Portugal; Fernando Gutiérrez-Cabello, responsable de Cuentas de MicroStrategy y Sandra Chíchina, Territory Account Manager de Nutanix.

En este bloque los participantes repasaron el estado actual del sector educativo y cómo se ha ido adaptando a los cambios impuestos durante la pandemia, cuando se impulsaron nuevos modelos de enseñanza híbridos en los que la tecnología juega un papel fundamental. Este acelerón digital ha sido una imposición y no hubo tiempo para diseñar un plan a largo plazo, algo fundamental para seguir avanzando. Los expertos coinciden en que la tecnología ha llegado al sector para quedarse y se deben buscar fórmulas para aprovechar sus ventajas y minimizar sus riesgos.

La introducción de herramientas digitales y arquitecturas TI en los centros plantea varios problemas y los más acuciantes tienen que ver con la ciberseguridad, ya que estas instituciones manejan datos de miles de alumnos cada año. Los miembros de la mesa analizaron cuáles son las principales ciberamenazas que enfrentan y cómo se deben proteger puntos clave como el control de accesos, las redes o el correo electrónico. Aunque lo primero debería ser diseñar una estrategia de ciberseguridad clara sobre la que se puedan implementar las medidas de protección necesarias.

Los expertos también debatieron sobre las prioridades digitales de los centros de enseñanza y destacaron la importancia de contar con una plataforma sólida, bien diseñada, sobre la que poder construir servicios que mejoren las operaciones y apoyen la estrategia formativa. También recomendaban realizar un ejercicio de reflexión para analizar los cambios implementados desde la pandemia y determinar si se ha seguido el camino correcto o si, por el contrario, es necesario replantearlo. Y hacen hincapié en los beneficios de apoyarse en expertos externos, especialmente en todo aquello que tenga que ver con la estrategia de ciberseguridad, que pueden aportar conocimiento y experiencia para ayudar a la transformación digital del sector educativo. ■

MÁS INFO +

» Encuentro ITDM Group

COMPARTIR EN REDES SOCIALES

Descarga este informe

LOW CODE EN EL ENTORNO DE SERVICIOS FINANCIEROS: DE LA TRANSFORMACIÓN EMPRESARIAL A LA INNOVACIÓN

El sector financiero es uno de los motores de la digitalización de la economía española, si bien es un claro ejemplo de cómo el legacy en las organizaciones puede acabar poniendo trabas a la innovación. Para eludir este hándicap y aportar más agilidad, eficiencia y eficacia a las operaciones, aplicaciones servicios de estas compañías, entra en escena la metodología low code.

Para conocer de primera mano qué elementos de estas plataformas de desarrollo de código bajo, la Comunidad ITDM ha organizado una mesa redonda Low Code en el entorno de servicios financieros: de la transformación empresarial a la innovación en la que participaron portavoces de **Allfunds Bank, Banco Caminos, Bestinver, Evo Banco, Nationale Nederlanden Spain** y **Sanitas**, con la colaboración de **KPMG** y **OutSystems**.

El primer tema que surgió en el debate fue la necesidad de las empresas del ámbito financiero de responder a las exigencias del negocio con toda la agilidad posible a la hora de desarrollar nuevos aplicativos. En este sentido, los diferentes responsables participantes en la conversación dejaron claro que la generación de nuevas capacidades y servicios es una constante para todos ellos. Para ello, una de las opciones que se han acabado imponiendo en las organizaciones es la creación de equipos multidisciplinares que aporten la necesaria visión tecnológica y el imprescindible conocimiento del negocio, porque este debe estar cerca de la planificación, generación y despliegue de las nuevas soluciones para que el valor que se entrega a los

MESA REDONDA IT >> Hablamos de cómo la filosofía Low-Code puede potenciar la innovación en el sector financiero de la mano de Allfunds Bank, Banco Caminos, Bestinver, Evo Banco, Nationale Nederlanden Spain y Sanitas, con la colaboración de KPMG y OutSystems.

clientes responda a las exigencias y necesidades de estos.

Sin embargo, los diferentes portavoces reconocían que, si bien es esencial aportar soluciones rápidas al negocio, también lo es asegurarse del conocimiento funcional de los equipos. Además, otro hándicap con el que se encuentran los responsables de TI de las compañías es que esta apertura a nuevos perfiles a la programación, hace imprescindible una gobernanza mayor para evitar posibles inconvenientes en la interrelación de las nuevas soluciones con el ecosistema y la infraestructura que soporta el negocio.

Otra ventaja de la apuesta por Low Code es la evidente reducción de costes así como de los plazos de entrega de los aplicativos a negocio, que ha pasado de meses a semanas o incluso días, abriendo la puerta al desarrollo de pruebas de concepto sin que esto suponga un problema que retrase otras entregas o la solución a otras necesidades de la compañía.

Sin embargo, las organizaciones deben ser conscientes de que esta velocidad en el front, en la entrega al negocio para dar servicio al cliente, no es la misma que la del back, con lo que deben adecuar los desarrollos a lo que puede asumir la infraestructura que, en muchos casos en este tipo de compañías, es resultado de un legacy que se ha mantenido en el tiempo y que lastra, en ocasiones, la necesidad de innovación que tiene negocio. Pero, como reconocían los participantes en la mesa redonda, Low Code es un elemento acelerador porque permite separar las dos realidades que conviven en las empresas actuales, la necesidad de adecuarse a la exigencia de innovación que impone el negocio, y el avance en eficiencias internas que permitan a las empresas seguir manteniendo el día a día.

Preguntados sobre el uso de plataformas Low Code en sus propias organizaciones, reconocían los diferentes portavoces que la velocidad de integración de estas plataformas no es uniforme, si entre las distintas compañías, ni, dentro de estas, entre las varias áreas, porque todavía se encuentran, en su mayoría, en un proceso de implementación de estas soluciones en casos de uso concreto. Afirmaron, eso sí, que esta filosofía de desarrollo aporta evidentes ventajas, como la facilidad de uso para los usuarios no tecnológicos; la reducción de los costes de desarrollo, algo cada vez más esencial en las organizaciones financieras; o la facilidad para acercar negocio y tecnología, si bien ponían sobre la mesa la necesidad de aportar racionalidad a estas aplicaciones para que no comprometan recursos de la organización por perder de vista el conocimiento de la eficiencia que aporta TI. Con todo, establecieron la premisa básica de que el éxito del despliegue de estas soluciones, más allá de la tecnología, está en clarificar la seguridad y gobernanza adecuadas, porque no todo vale y porque no todos los perfiles de negocio tienen los conocimientos mínimos necesarios para poder ser autónomos en sus desarrollos.

A la vista de las diferentes opiniones expresadas a lo largo del debate, Joao Mena de Oliveira, country manager de Outsystems, destacaba que los tres principales casos de uso de su plataforma son, por orden de peso en su negocio, la innovación en el front-end y en la movilización de la interacción con el cliente, el incremento de la eficiencia interna y el desarrollo de nuevos cores de negocio, algo esencial en un sector, como el financiero, tan atado, tecnológicamente hablando, por tecnologías legacy que complican la innovación.

Por último, surgió en el debate la dicotomía entre el desarrollo interno o la apuesta por terceros, lo que suscitó una opinión mayoritaria, y es que siempre es interesante el desarrollo interno, que permite retener en la organización el conocimiento necesario, si bien es positivo apoyarse en profesionales externos, cuando sea necesario, siempre y cuando se mantenga dentro de la organización el control y el conocimiento de negocio. ■


itv
La seguridad de tu información es tan
importante como la de tu vehículo.
¡En Securízame te ayudaremos a pasar la ITV!
https://www.securizame.com/servicios
SECURIZAME

JOSÉ MANUEL NAVARRO
experto en marketing

EL EFECTO TRANSFORMADOR DEL MARKETING EN EL SECTOR FINANCIERO

LORENZO MARTÍNEZ RODRÍGUEZ
experto en ciberseguridad

¿TIENE TU ORGANIZACIÓN LA “ITV” AL DÍA?

EL EFECTO TRANSFORMADOR DEL MARKETING EN EL SECTOR FINANCIERO

JOSÉ MANUEL NAVARRO
Experto en marketing

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

Un reciente estudio publicado por Planet sobre pagos en el mercado europeo evidencia la preferencia de los usuarios por los medios de pago alternativos, como son las billeteras digitales, frente a las tradicionales tarjetas de débito y crédito. Esta tendencia está muy ligada a la experiencia de compra tanto en entornos físicos como online, así como a los modelos que facilitan el pago aplazado, como el cada vez más demandado "Buy Now, Pay Later" (BNPL), el cual alcanza importantes índices en el sector retail en Europa: Alemania (43%), Austria (43%), Finlandia (40%) o Suecia (61%).

La experiencia de compra no sólo es un atributo que permite diferenciar unos negocios de otros, sino que también posiciona a los países como referentes para los viajeros y turistas, de manera que las preferencias de los consumidores también marcan tendencias respecto del atractivo de pagar en un país u otro cuando se visita el extranjero. El informe de Planet destaca que un 6% de los encuestados afirma que comprar en otros países es igual o menos atractivo que hacerlo en el propio. Este dato, como media, es importante para los pequeños y medianos comercios ya que proporcionar una buena experiencia de compra a clientes internacionales puede basarse, más allá del proceso de pago (en el que es determinante la sensación de seguridad que proporciona la autenticación reforzada de la operación, SCA), en cuestiones como facilitar el pago en la moneda propia y con el dispositivo preferido por el usuario, gestionar el reembolso de las tasas, proporcionar información sobre el ahorro ocasionado conjugan-

do diferentes ofertas promocionales, seleccionar el envío a domicilio cuando se adquiere el producto en tienda física o canalizar de manera sencilla la devolución de éste. Estas sencillas acciones contribuyen a la satisfacción del consumidor y, más importante, a incrementar el gasto medio y a facilitar la recurrencia de las compras.

Una de las funcionalidades que, desde las áreas de marketing, se han venido reclamando desde hace años y que en la actualidad la tecnología permite, es la autenticación mediante sistemas biométricos para agilizar los procesos de identificación reforzada, sea para iniciar cualquier tipo de transacción o para confirmar su ejecución. Detección de huella dactilar, escaneo de retina o reconocimiento facial o de voz son las más usadas como consecuencia de su utilización para acceder a los actuales dispositivos móviles. El informe presentado por Paysafe destaca cómo los usuarios aprecian la seguridad en los procesos de pago, si bien la condicionan a la conveniencia de los sistemas usados en función de qué tipo de entorno y de compra se trate. Las empresas deben conjugar la confianza y la operatividad (procesos sin fricciones o barreras) con las exigencias de seguridad como mecanismo de prevención de fraude para ofrecer una experiencia de compra satisfactoria.

La evolución de la autenticación biométrica vendrá condicionada por dos aspectos clave: la innovación tecnológica que venga a mejorar los sistemas actuales para hacerlos más robustos estando soportados en hardware “unhackable” y, el segundo, la sofisticación de la inteligencia artificial aplicada a su uso y gestión ayudará a mejorar los patrones de autenticación multifactor (MFA) para hacerlos más amigables en su uso sin perder su consistencia y confiabilidad.

Las soluciones de autenticación biométrica aportan solidez a las transacciones de pago mediante cualquier dispositivo, medio, contexto o fórmula elegida (débito, crédito, aplazado…), pero intervienen en el proceso de compra una vez ésta ha sido decidida. En cambio, el marketing también plantea nuevas fórmulas de compra en las que la toma de decisión se difiere en el tiempo, permitiendo que el usuario antes ahorre el suficiente dinero para afrontar el gasto. Frente al modelo BNPL se alza el concepto SNBL (Save Now, Buy Later). En realidad, no se trata de un sistema novedoso (es algo que nuestros abuelos ya practicaban, ahorrando poco a poco hasta juntar el dinero suficiente para afrontar un gasto, pequeño o grande, sin necesidad de recurrir a préstamos o a empeños), pero sí lo es abordarlo como experiencia de pago instrumentado, desde la perspectiva parafinanciera del comercio, como plan de ahorro aderezado con acciones promocionales y/o de fidelización.

En momentos de crisis económica y laboral, de incertidumbre financiera y de un panorama alcista de tipos de interés, empresas y entidades financieras temen el incremento de impagos de los créditos al consumo y de los pagos aplazados sin exigentes análisis de riesgo. Por ello, fórmulas como SNBL abren la puerta a generar un nuevo modelo de negocio que permite potenciar los depósitos, apalancando los ingresos periódicos hasta alcanzar el saldo comprometido que permitirá la compra; y, para los consumidores, supone disfrutar de cierta tranquilidad, tanto por la personalización de la oferta que le pueden hacer (soportada en modelos de IA) como por la recepción de intereses, hasta ahora muy bajos o inexistentes. Ambas cuestiones se traducen en una mejora de la experiencia del cliente y en una mayor percepción de bienestar financiero.

Entidades bancarias han comercializado históricamente planes de ahorro finalista que solían estar respaldados por seguros de ahorro, algunos de ellos incluso tuvieron beneficios fiscales (como los promovidos para la compra de vivienda), pero

las preferencias de los clientes y las tendencias del mercado (así como los cambios en la legislación tributaria) hicieron que estos productos fueran desapareciendo. El modelo SNBL cambia el enfoque y lo traslada a otros actores como las Fintech y los proveedores de pago, de tal manera que el consumidor puede crear su propio plan de ahorro en un punto de venta físico o virtual de un comercio, aprovechando beneficios adicionales como recompensas e incentivos promocionales, descuentos o pago de intereses encaminados a favorecer, adicionalmente, la puesta en marcha de acciones de "cross y up selling" orientadas a incrementar la retención, prevenir el abandono y ampliar la cartera de clientes mediante la recomendación.

Los profesionales del marketing que nos hemos aproximado a la economía del comportamiento sabemos que existen determinados sesgos cognitivos que operan tras muchas decisiones financieras. Cuando se trata de ahorrar, de comprar al contado o aplazar el pago, existen determinados "atajos mentales" como la aversión a la pérdida (la sensación negativa de una pérdida económica es mayor que el posible beneficio que supone la adquisición de un bien o un servicio), la contabilidad mental (organización y clasificación del dinero disponible en función de su aplicación), el efecto gradiente (tendencia a continuar con un esfuerzo con el que nos hemos comprometido en términos de inversión de dinero, sobre todo cuando el objetivo está cerca) o el sesgo de impacto (interpretación errónea de que las situaciones negativas o positivas del futuro van a ser mucho peores o mejores que lo que en realidad son). Saber construir ofertas financieras teniendo en cuenta estas cuestiones, permitirá dar ese pequeño empujón (R. Thaler) a los consumidores para tomar la decisión de adoptar soluciones, en este caso de SNBL avaladas por otros aditamentos o alicientes que las hacen más atractivas.

Hay quien compara a los profesionales del marketing con alquimistas o magos de los datos, sobre todo a partir de que la posibilidad de obtener estos se ha multiplicado exponencialmente mediante el acceso a infinidad de registros de conducta y a diversidad de herramientas para rastrearlos, obtenerlos, analizarlos e interpretarlos, siempre con el enfoque puesto en obtener perfiles muy próximos a la realidad y en predecir conductas. Y también para estimular éstas a través de una comunicación personalizada y contextualizada.

En el sector financiero, la abundancia de datos de un cliente es posiblemente la más rica que se puede tener ya que conjuga la información relativa a posiciones económicas, riesgo crediticio, apetencia inversora, formación financiera, preferencias de aseguramiento...; y, ahora con los sistemas de Open Banking y Embedded Finance, también se puede acceder a la conducta de consumo, a los patrones de gasto, a las habilidades digitales, a la predilección por el uso de determinados dispositivos y medios... El resultado final es un perfil completo y complejo de cada consumidor, lo cual implica un potencial de aprovechamiento responsable casi sin límites, pero también conlleva la obligatoriedad de garantizar prácticas transparentes y comprometidas con la legislación vigente en materia de privacidad, de prestación de servicios de pago y de acceso a datos financieros (atención a la nueva directiva PSD3), y con los principios éticos corporativos.

En el nuevo mundo de la banca y las finanzas descentralizadas, los profesionales del marketing no sólo son perseguidores de la creación de valor en cualquiera de las ofertas que se realicen, sino que deben ser merecedores de confianza a través de la implementación de experiencias bancarias (multidispositivo) integrales y sin fisuras.

La irrupción de los nuevos actores financieros y una legislación europea cada vez más estricta, pero habilitadora de nuevas posibilidades de interrelación entidad-comercios-cliente, está teniendo un impacto ciertamente transformador, con el que surgen oportunidades para redefinir los paradigmas tradicionales del marketing y establecer nuevas estrategias, más arriesgadas pero emocionantes. ■

MÁS INFO +

- Pagos en el mercado europeo
- SCA
- Los usuarios aprecian la seguridad en los procesos de pago
- Bienestar financiero
- Directiva PSD3

¿TIENE TU ORGANIZACIÓN LA "ITV" AL DÍA?

LORENZO MARTÍNEZ RODRÍGUEZ
Experto en ciberseguridad

Lorenzo Martínez Rodríguez es ingeniero en Informática por la Universidad de Deusto. Perito informático forense, actualmente es director de la empresa Securízame. Igualmente, es conferenciante habitual en congresos de Ciberseguridad.

Los propietarios de un vehículo hemos de estar preocupados por tener el papel que certifica que se le hace periódicamente una batería de pruebas concretas, para que pueda seguir circulando sin ser un peligro para los demás conductores y peatones. Esto es la ITV, correspondiente a las siglas de Inspección Técnica de Vehículos.

Sobre la naturaleza de las pruebas y su rigurosidad no voy a entrar. Luego se ven por la calle determinados medios de transporte que tiran un humo negro descomunal, que emiten un nivel de decibelios ensordecedor, o que da la sensación de que tiene las piezas sujetas con esparadrapo, y uno se pregunta: ¿realmente esta masa de hierros ha pasado la ITV?

Abrimos cualquier medio de información o red social y nos enteramos de que la entidad pública X o la empresa Y han sido atacadas por un grupo de ransomware y todos sus datos están secuestrados porque han sido cifrados. Por supuesto, no contaban con un sistema de copias de seguridad a prueba de ransomware, por lo que la vuelta al funcionamiento de la organización está totalmente en manos de los ciberdelincuentes. Además, ves que, en su comunicación institucional, dicen que no hay de qué preocuparse porque no ha habido robo de información sensible ni datos personales.

Los grupos de ransomware de los últimos años se aseguran el robo de información, previo al cifrado de la misma, para garantizarse el pago. En muchos casos implementan lo que se llaman técnicas de múltiple extorsión. Piden dinero a cambio de la devolución de los datos, así como de la no publicación o subasta de estos, y por la promesa de no contactar con clientes y proveedores de la empresa. Es decir, que los grupos profesionalizados de ransomware siempre se llevan datos que usar a posteriori si la empresa no paga, por lo que negar el acceso a los datos por parte de los ciberdelincuentes como parte de una estrategia de comunicación es algo que tarde o temprano sale a la luz, ya que, en caso de que la organización no pague el rescate, los publican o subastan. He visto casos que, incluso hasta habiendo pagado, terminan utilizándolos.

El equivalente a pasar la ITV para una organización es lo que llamamos en el sector "llevar a cabo una auditoría de seguridad", un "vulnerability assessment", un "pentest" o un "ejercicio Red Team". En realidad, los cuatro conceptos son distintos en cuanto a su contenido, pero en todos ellos se pide una cosa: un informe que diga que la organización está limpia de polvo y paja. En otras palabras, un certificado que puedan presentar a sus clientes diciendo: hemos pasado la ITV y no tenemos defectos graves que nos impidan circular por las calles.

Como director de Securízame recibo semanalmente múltiples contactos de empresas en los que se me solicita llevar a cabo este tipo de trabajos. La mayor parte de ellos buscan obtener el papel que diga que "se ha revisado todo" y que el resultado ha sido que no hay nada grave. Son minoría aquellos que, lo que quieren realmente, es verificar si las medidas de seguridad implementadas en sus servicios expuestos son suficientes. Hay una parte aún menor que lo que piden parte de enunciados como: "Quiero que me dejes esto blindado, que sea más seguro que el Fort Knox y que sea IMPOSIBLE hacer un estropicio por un atacante". A estos últimos directamente les digo que lo que piden no se lo puedo garantizar ni yo ni nadie, puesto que las tecnologías cambian, evolucionan, se descubren vulnerabilidades explotables que quizá no existían en el momento de la realización de las pruebas, y les explico que siempre habrá alguien mejor que nosotros al otro lado, que sea capaz de ver algo que nosotros no hemos sabido explotar.

Analizando los primeros casos descritos, los que quieren un informe o un certificado de realización de trabajos previstos sin deficiencias graves, muchas veces requieren varios informes, en distintas fases del trabajo. Uno inicial en el que se observan lo realmente encontrado y en el que se recomienda una implementación de medidas para la resolución y/o mitigación y uno posterior en el que, tras volver a testear la plataforma, se puede decir que estas han sido resueltas.

El segundo escenario, en el que el cliente lo que busca además es saber si está o no seguro, al no requerir un certificado para presentar a clientes como los del caso anterior, se toma la

resolución con demasiada calma, y en algunos casos incluso no llegan ni a solucionarlo nunca, esgrimiendo alguna excusa de lo más peregrina.

En cualquiera de los casos descritos, siempre dejo constancia del alcance de lo analizado. Esto es especialmente importante, porque si en la ITV solo se fijan en si los neumáticos tienen la profundidad y el dibujo mínimos aceptables, deberían indicar que lo único que han mirado es eso. Siguiendo esta misma analogía, si lo que se ha analizado es únicamente los servicios expuestos a internet por una organización, y lo que se nos hace auditar es un número determinado de direcciones IP o de aplicaciones o API web, y luego la empresa tiene otros accesos distintos igualmente expuestos que han posibilitado el acceso a un ciberdelincuente, queda constancia escrita de lo que realmente se ha analizado.

En otros casos, el alcance se amplía a auditorías en redes internas, en las que normalmente se multiplica el número de hallazgos, desvelándose muchas veces problemas de segmentación de red o incluso nulas políticas de seguridad implementadas en los cortafuegos, que están "de adorno" haciendo la labor de meros routers, pero que realmente no están bloqueando nada. Si nosotros fuésemos operarios de la ITV, verificaríamos el check "Tiene Firewall" Sí/No, y tendríamos que decir que sí, que lo tiene, aunque realmente su configuración actual no genere ningún tipo de protección.

Ya no digo nada cuando lo que preguntamos es por la política de copias de seguridad, así como la implementación de estas. En muchos casos se nos habla de backups que se hacen en el propio servidor, otros en un NAS accesible desde cualquier parte, y otras en una nube de no sé qué proveedor, de los que también hemos visto a intrépidos atacantes que han dejado a los pies de los caballos a una organización presionando al cliente, terminando en la baja del servicio de backup, y derivando en una pérdida total de los datos, o que una vez más sea el atacante el único valedor para la recuperación del negocio. Así, cuando les hablas de soluciones de copia de seguridad a prueba de ransomware lo mueven a la página 3 de su lista de prioridades puesto que: "ya tienen un backup, y el check de la ITV solo dice "Hay copia de seguridad" SI/NO". ■

LOS GRUPOS DE RANSOMWARE DE LOS ÚLTIMOS AÑOS SE ASEGURAN EL ROBO DE INFORMACIÓN, PREVIO AL CIFRADO DE LA MISMA, PARA GARANTIZARSE EL PAGO Y, EN MUCHOS CASOS, IMPLEMENTAN LO QUE SE LLAMAN TÉCNICAS DE MÚLTIPLE EXTORSIÓN

MÁS INFO

- Catorce nuevos grupos de ransomware empezaron a operar en el segundo trimestre
- El sector educativo, el más castigado por el ransomware en 2023
- Aumentan el volumen y el impacto de los ataques de ransomware dirigidos
- Un sistema de copias de seguridad a prueba de ransomware

FORO it Digital Security

NUEVOS MODELOS DE CIBERSEGURIDAD

PARA PROTEGER A LA EMPRESA GLOBAL

24 de octubre · 9.30 h

©freepik

it Digital MEDIA GROUP