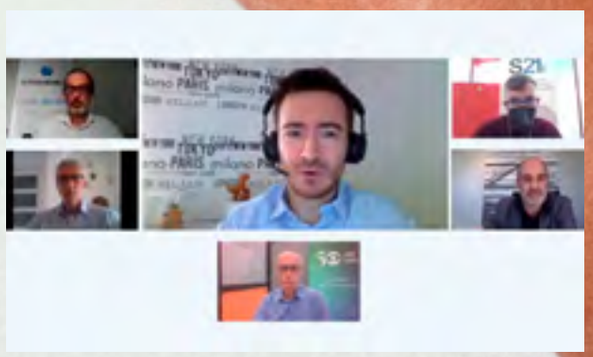
it User
TECH & BUSINESS

nº 66
ABRIL 2021

El puesto de trabajo digital en 2021

Guarda esta revista en tu equipo y ábrela con Adobe Acrobat Reader para aprovechar al máximo sus opciones de interactividad



El fenómeno de la Industria 4.0 en 2021, a debate

EDITORIAL

IT User TECH & BUSINESS

Director Pablo García Reales
pablo.garcia@itdmgroup.es

Redacción y colaboradores Hilda Gómez, Arantxa Herranz, Reyes Alonso, Ricardo Gómez, Belén Juárez

Diseño revistas digitales Eva Herrero

Producción audiovisual Favorit Comunicación, Alberto Varet

Fotografía 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 Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es

Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es

Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es

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

¿Está su perfil profesional entre los más demandados en España?

Ya nadie duda de que la pandemia ha impulsado la digitalización de muchos segmentos, en ocasiones a un ritmo vertiginoso. La transformación digital se está acelerando, realidad que está generando nuevas oportunidades laborales, sobre todo entre las carreras tecnológicas, que a su vez son las mejor pagadas.

El sector TIC emplea en España a 471.500 personas, es decir, alrededor del 2,4% del total de trabajadores de nuestro país. Ha experimentado un crecimiento del 7,3% de ocupación los últimos años y sigue en aumento. De hecho, durante el pasado año vio crecer su número de profesionales, a pesar de la grave crisis que estamos viviendo, tras incorporar 135.828 contratos, la mitad de ellos indefinidos.

La remuneración depende, entre otros factores, de dónde se firme el contrato. Un estudio reciente detecta dos grupos de localizaciones en los que existen diferencias tangibles en cuanto al salario. Por un lado, Madrid, Barcelona y Bilbao registran los sueldos más elevados, mientras que en Valencia, Sevilla y Málaga las remuneraciones suelen ser, de media, un 9% más bajas.

Pero, ¿cuál es el ranking de perfiles profesionales más demandados y mejor pagados de nuestro sector? Tome nota: Data Analyst, Data Scientist, Digital Project Manager, Especialista en Blockchain, Especialista en Inteligencia Artificial, Chief Marketing Officer, Experto en Customer Success, eSports Manager, Especialista en Customer Officer, Ingeniero de Robótica, Especialista en Ciberseguridad y Consultor de Cloud. ¿Se encuentra entre ellos? ■

Pablo García Reales

SUMARIO

Abril 2021

it User
TECH & BUSINESS

EN PORTADA

El puesto de trabajo digital en 2021

TENDENCIAS

El e-commerce crecerá un 24% en España en 2021

Ciberinteligencia, clave para afrontar las amenazas

Crecimiento acelerado de las comunicaciones unificadas como servicio

¿Qué habilidades necesitan los líderes ante el nuevo entorno?

ANUNCIANTES

STORMSHIELD
S21SEC
INFORME MICROSTRATEGY
IT WHITEPAPERS
DOCUMENTO EJECUTIVO IT TRENDS
IT WEBINARS
IMPRESIÓN
ALMACENAMIENTO
TECNOLOGÍA Y EMPRESA
IT DIGITAL SECURITY
IT RESELLER

REVISTAS DIGITALES

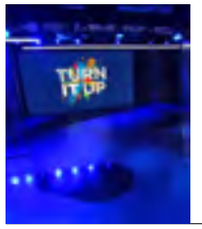
MESA REDONDA

Evolución en España del fenómeno de la Industria 4.0 en 2021, a debate

NO SOLO it

ACTUALIDAD

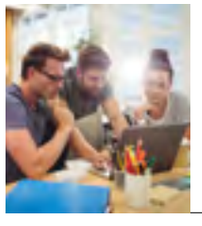
Micro Focus revela su propuesta para "resolver los problemas más desafiantes de la industria"



Cisco aprovecha Cisco Live! para presentar su nueva propuesta de consumo de tecnología como servicio

ServiceNow desvela Quebec, la nueva versión de Now Platform

El mercado de ordenadores seguirá creciendo este año en EMEA



Los profesionales técnicos piden más visibilidad en los entornos de TI, pero también de negocio

Aumentan las inversiones en empresas dedicadas a la Inteligencia Artificial

MÁS DE 40.000 PERSONAS ASISTIERON AL EVENTO ANUAL PARA PARTNERS Y CLIENTES DE LA FIRMA

Micro Focus muestra en Universe 2021 su propuesta para "resolver los problemas más desafiantes de la industria"

Micro Focus ha celebrado Universe 2021, el principal evento para partners y clientes en el que explica cómo su propuesta puede ayudar a las empresas a tener éxito en un momento en el que apostar por la transformación digital es más vital que nunca.

Stephen Murdoch, CEO de Micro Focus, ha sido el encargado de abrir esta edición de Micro Focus Universe 2021. Durante su intervención ha recordado el importante papel que ha jugado la tecnología en los últimos doce meses, explicando que las empresas han tenido que acelerar sus procesos de digitalización para adaptarse a la nueva normalidad.

En este proceso "Micro Focus ha respondido y ha cumplido la promesa de facilitar alta tecnología que permite a nuestros clientes ganar en agilidad y productividad, reduciendo costes y sin olvidarse de la seguridad", ha destacado Stephen Murdoch, quien ha continuado explicando en qué consiste la estrategia de la firma, la cual "está basada en la innovación" y que

busca “lograr un equilibrio entre las necesidades de hoy y las oportunidades del mañana”.

Denominada Run and Transform (Dirigir y Transformar), la estrategia de Micro Focus se sustenta en cuatro ejes: acelerar la entrega de aplicaciones, simplificar la transformación de la TI, fortalecer la ciber-resilencia y analizar a tiempo para poder tomar decisiones.

MÁS DE 40 AÑOS DE EXPERIENCIA

“Escuchamos a nuestros clientes”, ha remarcado Stephen Murdoch quien ha explicado que su compañía está muy bien posicionada para atender las demandas de unas empresas que se tienen que adaptar rápidamente al cambio. “La innovación y nuestras capacidades para ayudar en la transformación digital están avaladas por años de experiencia en el mercado”.

Micro Focus ha realizado más de 1.000 lanzamiento de producto en los últimos 24 meses. “Tenemos las soluciones, la tecnología y la experiencia necesaria para ayudar a nuestros clientes a funcionar y transformarse al mismo tiempo sin sorpresas”.

Bret Fitzgerald, director de relaciones públicas en Micro Focus, ha destacado, durante la rueda de prensa internacional que se ha celebrado, que “tenemos el tamaño, la escala y la experiencia para resolver los problemas más desafiantes de la industria”. La firma tiene una facturación de 3.300 millones de dólares anuales, cuenta con más de 40.000 clientes a nivel global (98 del Fortune 100 trabajan con Micro Focus), más de 7.500 partners y más de 12.000 empleados en las 100 oficinas de 45 países. “Tenemos clientes de primer nivel en sectores como telecomunicaciones, salud, finanzas, utilities, aeroespacial y defensa, gas y petróleo, servicios o ferrocarriles”, que han confiado en Micro Focus y “en nuestro software de misión crítica” para operar en un mundo digital. “La innovación está centrada en nuestros clientes a los que ofrecemos soluciones de confianza que les garantiza el éxito en un mercado como

MICRO FOCUS UNIVERSE 2021 BAJO DEMANDA

> “Nuestra estrategia busca lograr un equilibrio entre las necesidades de hoy y las oportunidades del mañana”
>
> STEPHEN MURDOCH, CEO DE MICRO FOCUS

CONTENIDOS↓

¿Te avisamos del próximo IT User?

el actual, que se caracteriza por la rápida evolución".

Gonzalo Usandizaga, presidente de ventas internacional de Micro Focus, ha sacado pecho por la apuesta que realiza la firma por la innovación. "Todo lo que hacemos, lo hacemos situando al cliente en el centro".

A su apuesta por la innovación hay que sumarle "nuestro sólido ecosistema de servicios", ha remarcado Usandizaga. "Nuestros más de 7.500 resellers aportan un valor fundamental, nuestras alianzas con los proveedores de servicios más respetados del mundo nos ayudan a garantizar el éxito en el funcionamiento de los sistemas, y nuestro equipo interno de expertos y consultores ha ayudado a cientos de organizaciones de todos los tamaños a evolucionar, administrar y modernizar su infraestructura de aplicaciones empresariales".

COMPROMISO CON "HACER LAS COSAS BIEN"

Stephen Murdoch ha aprovechado su intervención para destacar que Micro Focus está comprometida "con hacer las cosas bien", explicando que su compromiso abarca tanto a sus empleados, "haciendo que Micro Focus sea el mejor lugar posible para trabajar", como al mercado, "logrando que seamos una gran compañía con la que hacer negocios", sin olvidarse de sus clientes, "con los que mantenemos una relación profesional basada en la confianza y la integridad". El compromiso con el medio ambiente y con la sociedad son los otros dos ejes del Programa Inspire de Micro Focus.

ACUERDO CON JAGUAR RACING

Tras Stephen Murdoch ha intervenido James Barclay, director del equipo de Jaguar Racing, quien ha explicado cómo la marca trabaja de la mano de Micro Focus para acelerar la entrega, simplificar la transformación, fortalecer la resiliencia y analizar a tiempo para poder tomar decisiones. Algo fundamental para ganar tanto en la sala de juntas como en la pista.

"Micro Focus nos ayuda a ejecutar y transformar nuestros sistemas centrales para que podamos acelerar el avance como equipo". La alianza se centra "en tres áreas específicas: transformación digital, resiliencia empresarial y análisis", ha señalado Bret Fitzgerald. "Ayudamos a que Jaguar Racing corra con resiliencia en el día y se transforme para superar los límites de la competencia, la innovación y la experiencia del cliente".

PRESENTACIÓN DE OPTIC

Durante Micro Focus Universe 2021, la firma ha presentado OPTIC (Plataforma de Operaciones para la Transformación, la Inteligencia y la Nube) la cual simplifica la complejidad de transformar la TI para cumplir con unas expectativas cambiantes.

Durante Micro Focus Universe 2021, la firma ha presentado OPTIC (Plataforma de Operaciones para la Transformación, la Inteligencia y la Nube)

La inteligencia incorporada en el núcleo de Micro Focus OPTIC proporciona un análisis amplio a medida que normaliza, almacena y da sentido a todos los datos producidos por la variedad de soluciones que se encuentran en los entornos de TI, incluidas la mayoría de las herramientas de monitoreo de terceros. OPTIC también permite a los equipos descubrir, monitorear, administrar y gobernar los servicios en la nube en conjunto con un enfoque local, maximizando la experiencia del cliente y el retorno comercial. El objetivo es que las empresas puedan unificar la gestión del rendimiento y la disponibilidad mientras permanecen abiertas a nuevas posibilidades con opciones de implementación de múltiples nubes.

"Una plataforma de TI ideal no debe agravar la complejidad creando una deuda técnica para el mantenimiento futuro, incurriendo en costos adicionales para AI / ML o limitando su capacidad para administrar en la nube y entornos tradicionales", ha asegurado Travis Greene, director sénior de marketing de productos de ITOM de Micro Focus. "Con Micro Focus OPTIC, las empresas pueden transformarse sin ningún problema aprovechando la inteligencia integrada de la plataforma y ampliando las mejores prácticas operativas al tiempo que conservan la agilidad de la nube". ■

MÁS INFORMACIÓN

- Descubre el potencial de la transformación digital
- ¿En qué consiste la estrategia Run and Transform de Micro Focus?
- Todas las características de OPTIC
- Historias de éxito: el caso de Micro Focus y FIATC

SNi20

SNi40

STORMSHIELD

PROTECCIÓN DE **INSTALACIONES INDUSTRIALES**

De amenazas dirigidas a estaciones de trabajo o provenientes de la red

www.stormshield.com

Cisco aprovecha Cisco Live! para presentar su nueva propuesta de consumo de tecnología como servicio

Cisco ha celebrado, de forma virtual, una nueva edición de Cisco Live!, una cita que, en esta ocasión, fusiona en una las ediciones regionales de otros años, lo que concentra la participación de más de 90.000 profesionales y partners de más de 200 países, y en la que la firma quiere mostrar sus propuestas para ayudar a las organizaciones a "conectar, proteger y automatizar en un entorno principalmente cloud". Y uno de los anuncios más significativos del primer día de evento fue Cisco Plus, la estrategia para convertir toda su oferta tecnológica a la modalidad de consumo como servicio, cuyos primeros elementos llegarán al mercado en junio de este año.

Recordaba en rueda de prensa Andreu Vilamitjana, director general de Cisco España, que Cisco Live!, que se celebró bajo el lema Turn IT up, "es un momento único en el año para la compañía", y más en un momento como éste en el que las diferentes versiones geográficas del mismo se concentran en una única cita global. Y en esta cita Cisco quiere mostrar novedades tanto en el área de consumo de TI como servicio, Cisco Plus, como en seguridad y en el despliegue de la Internet del futuro, cons-

CISCO LIVE! 2021 SESIÓN DE APERTURA

cientes de la necesidad de ayudar a las empresas a simplificar y automatizar sus TI, asegurar y dar visibilidad a las mismas, y desplegar una red que permita el desarrollo de la Economía de Internet.

En la sesión inaugural del evento, Chuck Robbins, presidente y CEO de Cisco, apuntaba que el negocio está marcado ahora por una serie de tendencias tecnológicas tales como la aceleración de la experiencia cloud; la optimización de la experiencia de usuario a través de las aplicaciones, un aspecto fundamental para el 90 por ciento de los usuarios; un futuro marcado por un modelo de trabajo híbrido y flexible; el despliegue de la Internet del futuro; la seguridad de principio a fin basada en la simplificación y la automatización; y el incremento de la capacidad de la TI en el Edge. En palabras de este responsable, "nos encontramos en un momento único en el que podemos dar forma al futuro inmediato. Y para ello necesitamos los pilares tecnológicos adecuados. Con las innovaciones que presentamos estos días, nuestros clientes de todo el mundo no solo podrán conectar, proteger y automatizar el futuro de las TI, sino también aprovechar la tecnología para impulsar un futuro verdaderamente inclusivo para todos".

INNOVACIONES EN DIFERENTES ÁREAS PARA CUBRIR DIFERENTES NECESIDADES

Así que Cisco ha presentado en Cisco Live! una serie de novedades entre las que destaca Cisco Plus, su estrategia de transformación de su oferta a un consumo as a service, y cuyas primeras soluciones, que llegarán en junio a algunos mercados internacionales y a las que se accederá a través de un portal de autoservicio, son Cisco Plus NaaS y Cisco Plus Hybrid Cloud.

"Con estas innovaciones, nuestros clientes de todo el mundo no solo podrán conectar, proteger y automatizar el futuro de las TI, sino también aprovechar la tecnología para impulsar un futuro verdaderamente inclusivo para todos"

CHUCK ROBBINS,
PRESIDENTE Y CEO DE CISCO

Cisco Plus no es sólo hardware como servicio o software como servicio, sino que también incluirá soluciones de red como servicio (NaaS, Networking-as-a-Service) que unificarán las redes, la seguridad y la visibilidad en los entornos de acceso, WAN y Cloud.

Por el momento se conocen pocos detalles alrededor del modelo concreto y del calendario diseñado por Cisco para llegar a otras zonas geográficas, como es el caso de España, o cómo se irá ampliando esta oferta de soluciones, pero desde la compañía explican que la ampliación de las soluciones seguirá la línea marcada por las principales necesidades de las empresas, y que el despliegue geográfico también estará motivado por las demandas específicas de cada mercado.

Cisco anunciaba también la integración de la solución de inteligencia de Internet y cloud ThousandEyes con la familia de switching Cisco Catalyst 9000 y con Cisco AppDynamics Dash Studio, presentando la primera solución de visibilidad extendida del entorno tecnológico corporativo.

Además, simplificaba las operaciones de red y seguridad con una arquitectura ampliada de Secure Access Service Edge (SASE), con la posibilidad de adquirir todos los componentes principales en una única oferta y la flexibilidad de pasar fácilmente a un servicio de suscripción unificado en el futuro. Asimismo, anuncia innovaciones en SecureX, su plataforma de seguridad cloud nativa, que ofrece protección desde los terminales hasta la nube. Junto a esto Cisco Secure anuncia la autenticación sin contraseña de Duo, que forma parte de la plataforma Zero Trust de Cisco, y que permite a los usuarios omitir las contraseñas e iniciar sesión de forma segura en las aplicaciones cloud mediante claves de seguridad o la autenticación biométrica incluida en terminales como portátiles y smartphones.

También se añaden a la lista de novedades innovaciones en silicio, óptica, software y sistemas que reinventan las redes a escala masiva y hasta 400 funcionalidades añadidas a Cisco Webex, así como novedades en sus soluciones de Contact Center. ■

MÁS INFORMACIÓN

- Cisco Live! 2021 Sesión de apertura
- Accelerating Digital Agility
- Cisco Live! 2021

it whitepapers

ESPAÑA EN LA ERA POST-COVID: TI para transformar el negocio

La COVID-19 ha trastocado la vida de empresas y ciudadanos que ven con incertidumbre el futuro. A la preocupación sanitaria se le unen unas previsiones económicas, y de desempleo, nada esperanzadoras. Descubre en este IT Research cuáles son las principales previsiones para España y cuál es el papel que va a jugar la tecnología en la recuperación a través de más de 40 gráficos, divididos en seis bloques (Perspectivas Económicas para España, Evolución del Empleo, Situación de las Empresas Españolas, La Transformación Digital en España, la I+D, y la Importancia de los Fondos Europeos), y las opiniones de diversos analistas del sector.

ServiceNow presenta Quebec, la nueva versión de Now Platform

ServiceNow acaba de presentar Quebec, la nueva versión de Now Platform, que ve la luz con el objetivo de ayudar a las empresas a acelerar sus procesos de transformación digital. Para ello, esta nueva versión incorpora capacidades de IA nativa ampliadas y nuevas herramientas de desarrollo de aplicaciones low-code.

Las empresas necesitan acceso rápido a información precisa y automatización de procesos para tener éxito. A menudo, para ello deben pedir al departamento de TI que compre o cree aplicaciones, pero cuando éste no puede satisfacer sus necesidades, muchos analistas de operaciones empresariales recurren a herramientas ineficaces o poco seguras para adquirir datos y gestionar flujos de trabajo, Muchos acaban por depender de hojas de cálculo, correos electrónicos y otras soluciones manuales, o bien recurren a la "TI en la sombra" y adoptan soluciones de colaboración basadas en nube o simplemente vuelven a enfoques antiguos.

ServiceNow propone Now Platform, que permite el desarrollo con muy poco o ningún código, para que los analistas de operaciones empresariales puedan diseñar o crear prototipos de sus propias aplicaciones sin necesidad de programar. Además, proporciona acceso a datos empresariales, funciones y herramientas de gestión del flujo de trabajo y una sencilla interfaz de usuario de arrastrar y soltar. Al mismo tiempo, el departamento de

FACILITANDO EL TELETRABAJO

TI puede validar y aprobar fácilmente nuevas aplicaciones sin emplear mucho tiempo ni dinero.

"Las empresas podrán innovar con celeridad, obtener una rápida rentabilidad, mejorar la productividad y ofrecer grandes experiencias". Now Plarform "fomenta la velocidad digital, la agilidad y la resiliencia que toda empresa necesita para el futuro del trabajo".

Chris Pope, vicepresidente de innovación en Servicenow, destaca la gran acogida que tiene en el mercado Now Platform. "Prácticamente el 80 % de las empresas de la lista Fortune 500 y miles de organizaciones a escala mundial confían en Now Platform para que les ayude a proteger sus ingresos, mantener la continuidad de sus actividades e impulsar la productividad y la seguridad, al tiempo que ofrece grandes experiencias a sus clientes y empleados".

QUEBEC, LA NUEVA ACTUALIZACIÓN DE NOW PLATFORM

Para ayudar a las empresas a continuar sus procesos de transformación digital con éxito, ServiceNow acaba de presentar una actualización de la plataforma. Se trata de Quebec.

Entre sus principales características destacan las incorporaciones de las nuevas soluciones Creator Workflows y App Engine Studio, con las que se acelera "el ritmo de la transformación digital, favoreciendo un rápido desarrollo de aplicaciones con poco código (low-code) en toda la empresa a fin de crear fácilmente flujos de trabajo que permitan superar los retos que afrontan las organizaciones a diario"

Creator Workflows cuenta con las herramientas de desarrollo low-code de ServiceNow, App Engine e IntegrationHub, "que permiten a las empresas transformar sus antiguos procesos manuales en modernos flujos de trabajo digitales a escala". Además, con el lanzamiento de Now Platform Quebec, ServiceNow ha introducido "nuevos productos dentro de Creator Workflows que permiten a los desarrolladores con cualquier nivel de competencias crear rápidamente aplicaciones para flujos de trabajo". La nueva versión de Now Platform incluye otras tres nuevas soluciones de flujos de trabajo que cabe destacar: Process Optimization, Workforce Optimization y Engagement Messenger, y permite a las organizaciones mejorar la productividad con nuevas capacidades de IA nativa. Entre las nuevas capacidades para mejorar la productividad destacan ITOM Predictive AIOps, Virtual Agent y AI Search. ■

MÁS INFORMACIÓN

- Toda la información sobre las tendencias tecnológicas en las empresas
- ¿Cómo está evolucionando el puesto de trabajo?
- Cuál es la propuesta de ServiceNow para ayudar en la transformación del puesto de trabajo

ServiceNow adquiere Element AI

ServiceNow ha firmado un acuerdo para adquirir Element AI, una empresa especializada en inteligencia artificial (IA), que mejorará significativamente el compromiso de ServiceNow de construir la plataforma de flujo de trabajo más inteligente del mundo, lo que permitirá a los empleados trabajar de manera más inteligente y rápida, optimizar las decisiones comerciales y desbloquear nuevos niveles de productividad.

Pionero en la industria de la IA, Element AI cuenta con científicos y profesionales de primer nivel que aportarán su experiencia en la aplicación de la IA moderna y acelerarán la innovación de la IA de forma nativa en la Now Platform. El cofundador de Element AI, Yoshua Bengio, desempeñará el cargo de asesor técnico de ServiceNow.

Con la adquisición de Element AI, ServiceNow creará un AI Innovation Hub en Canadá para acelerar la innovación de la IA centrada en el cliente en Now Platform. Este nuevo centro de innovación en Canadá se suma a inversiones similares realizadas por la compañía para crear centros de desarrollo de tecnología en Chicago, Hyderabad, Kirkland, Washington, San Diego y Silicon Valley.

S21SEC

CIBERSEGURIDAD INDUSTRIAL

Servicios enfocados a una gestión eficiente de los riesgos de ciberseguridad industrial.

Conoce tus sistemas de automatización y control mejor que el enemigo.

Ahuyenta a potenciales atacantes de tus instalaciones industriales.

Vigila a tu enemigo en los procesos industriales.

Lucha contra el enemigo de tus instalaciones industriales.

Para más información puedes visitar www.s21sec.com/es/ciberseguridad-en-el-sector-industrial/ o escribir un correo a marketing@s21sec.com

El mercado de ordenadores seguirá creciendo este año en EMEA

La demanda de ordenadores para el teletrabajo y el estudio remoto continúa siendo fuerte en regiones como EMEA, donde todavía se van a mantener ciertas restricciones de movilidad. Esto hará que el mercado de PC vuelva a crecer este año, especialmente durante el primer trimestre, cuando se alcanzará un récord de ventas.

El año pasado el mercado de ordenadores ha mostrado un crecimiento que nadie podía anticipar, ya que en los últimos tiempos había sufrido un cierto declive y en no había motivos para creer que la tendencia se invertiría en 2020. La escasez de procesadores y la madurez del mercado hacía que los proveedores se guiaran más por los ciclos de renovación empresarial que por novedades que pudieran revolucionar la industria. Pero el confinamiento llevó al teletrabajo y al estudio remoto, y todo cambió.

El año pasado las ventas de ordenadores alcanzaron niveles récord, especialmente en los ordenadores portátiles, pero en ciertos momentos también aumentaron las de equipos de sobremesa y las de estaciones de trabajo. De cara a este año, los expertos de IDC prevén que el mantenimiento de las medidas de con-

finamiento en regiones como EMEA va a seguir impulsando la venta de equipos, lo que permitirá superar las cifras logradas el año pasado

En general, los expertos de IDC prevén que este año las ventas generales del mercado de PC en EMEA podrían crecer un 16% interanual, hasta alcanzar un volumen de 96,4 millones de unidades. Aunque el mayor crecimiento se dará en la primera mitad de año, especialmente en este primer trimestre, cuando se esperan un crecimiento interanual del 39,1%. IDC destaca el buen comportamiento que tendrá el mercado en Europa Occidental, donde se anticipa un aumento interanual del 25,6% en los tres primeros meses, manteniéndose un crecimiento de dos dígitos hasta mediados de año, como mínimo.

Como explica Simon Thomas, analista de investigación de computación personal para IDC Europa Occidental, "a medida que se prolonguen los bloqueo más allá de las expectativas de muchos, la demanda de dispositivos de computación personal seguirá aumentando en paralelo". Explica que, en este tiempo, muchas empresas seguirán avanzando en la transición hacia modelos de trabajo a distancia, mientras que los consumidores seguirán buscando nuevas soluciones de entretenimiento en el hogar durante la pandemia. Por ello, cree que "esto dará como resultado un fuerte crecimiento, a pesar de las numerosas limitaciones causadas por las dificultades de la cadena de suministro".

Así, el mercado de consumo en Europa Occidental crecerá un 60,5% en el primer trimestre de 2021, con un sorprendente aumento de ventas del 21,6% en el segmento de equipos de sobremesa. Esto estará impulsado por el segmento de ordenadores gaming, que no está sufriendo efectos negativos por la salida al mercado de las nuevas videoconsolas. Sobre todo, teniendo en cuenta las graves interrupciones en el suministro que están sufriendo estos dispositivos.

Por su parte, se anticipa un récord de ventas en los equipos portátiles, ya que la transición general hacia este factor de forma sigue progresando, y muchos consumidores aprovecharán la excusa del teletrabajo y el confinamiento en general para actualizar sus equipos. El resultado es una previsión de crecimiento interanual del 70,2% en esta categoría de consumo.

En el caso de la subregión de CEMA, las previsiones de IDC han sido revisadas al alza, no solo en el primer trimestre, sino para todo el año, lo que contribuirá decisivamente a impulsar las ventas generales de EMEA. Nikolina Jurisic, directora de investigación sénior de IDC EMEA, explica que en estos países la demanda de PC no se ha ralentizado, sino que, "por el contrario, sigue siendo muy fuerte en todos los sectores comerciales, así como en el espacio del consumidor, como reacción a la pandemia".

En su informe comenta que los bloqueos en la cadena de suministro han afectado mucho a este mercado regional, y que este año se dará salida finalmente a esta demanda acumulada, lo que resultará en una explosión del mercado. Las previsiones de IDC son que en Europa Central y Oriental (CEE) los envíos alcanzarán unos 4,4 millones de unidades en el primer trimestre, solo un poco por debajo de las cifras de diciembre. Mientras tanto, la región de MEA alcanzará unos envíos de 3,3 millones de unidades, creciendo un 3% con respecto al cuarto trimestre de 2020. ■

MÁS INFORMACIÓN

- El mercado PC seguirá la senda de crecimientos también en 2021
- El mercado PC en EMEA tendrá un crecimiento robusto en el primer trimestre de 2021
- El mercado PC cierra 2020 con un tercer trimestre consecutivo de crecimiento de doble dígito
- El mercado de tablets se mantiene fuerte en EMEA en el primer trimestre

HACIA LA EMPRESA HIPERINTELIGENTE

PATROCINADO POR

MicroStrategy®

Descarga este documento ejecutivo de

itResearch

Los profesionales técnicos piden más visibilidad en los entornos de TI, pero también de negocio

Tres de cada cuatro profesionales de TI piensan que la pandemia ha creado la mayor complejidad tecnológica de la historia y, ante este panorama, lanzan un claro mensaje: están convencidos de que hay que vincular la visibilidad del entorno tecnológico con los resultados de negocio. Así lo considera un abrumador 96% de los participantes en un estudio de AppDynamics.

Los resultados del informe de esta compañía de Cisco revelan un aumento espectacular de la complejidad de las TI provocado por la necesidad de innovación, así como la necesidad urgente de mayor visibilidad y contexto de negocio para gestionar el estado de las TI, eliminar 'ruido' y priorizar lo más relevante para la empresa.

Según esta firma, la evolución hacia modelos de negocio digitales para minimizar el impacto económico de la pandemia ha situado al personal técnico al frente de la respuesta de sus organizaciones. Debido a la aceleración de los proyectos de transformación digital, cuya velocidad media se ha multiplicado por tres, el 89% de los profesionales se sienten bajo una inmensa presión en el trabajo, y el 84% admiten tener dificultades para desconectar. Muchos reconocen frustración por el trabajo (81%) y mayores desavenencias con sus compañeros (63%).

El 75% de los consultados cree que la pandemia ha creado la mayor complejidad de la historia para los departamentos de TI, debido principalmente a un nuevo conjunto de prioridades y retos (80%), la dispersión tecnológica

y un mosaico de tecnologías heredadas y en la nube (78%), la aceleración de la adopción de Cloud Computing (77%) y el uso de múltiples soluciones de monitorización desconectadas (74%).

INCREMENTO DE LOS DATOS CREADOS

Esta mayor complejidad ha incrementado significativamente la cantidad de datos creados en todo el entorno tecnológico, desde las aplicaciones hasta la infraestructura, la red y la seguridad. Así, el 85% de los profesionales de TI afirman que la eliminación rápida del 'ruido' para identificar las causas de los problemas de rendimiento será un reto significativo este año, y tres de cada cuatro ya se están planteando cómo resolverlo. En este sentido, demandan una solución unificada que proporcione visibilidad en tiempo real de todo el parque tecnológico: el 95% destacan la importancia de la visibilidad sobre todo el entorno de TI, y el 96% creen que no tenerla acarreará consecuencias negativas.

También una inmensa mayoría de los profesionales consultados (92%) consideran que la capacidad de vincular el rendimiento tecnológico con resultados de negocio, como experiencia del cliente, ventas e ingresos, será lo verdaderamente relevante para alcanzar los objetivos de innovación este año. El 96% afirman que esta vinculación en tiempo real será esencial para ofrecer experiencias digitales optimizadas y acelerar la digitalización, y el 73% temen que la incapacidad de lograrla sea perjudicial.

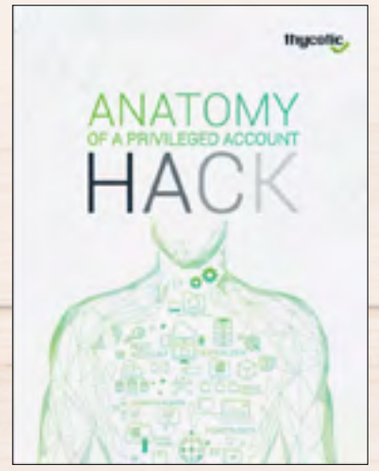
El informe también destaca que, aunque los tecnólogos son muy conscientes de la necesidad de contextualizar el rendimiento de las TI con datos de negocio en tiempo real, más de la mitad (el 66%) no cuentan con los recursos y el apoyo que necesitan, y el 96% señalan al menos un obstáculo que su organización debe superar para adoptar este nuevo enfoque. Tres de cada cuatro consultados subrayan la necesidad de conectar la visibilidad del entorno tecnológico con los resultados de negocio en un plazo de doce meses para mantener la competitividad. ■

MÁS INFORMACIÓN

Agents of Transformation 2021: The rise of full-stack observability

La documentación TIC, a un solo clic

Anatomía del ataque a una cuenta privilegiada



Este documento técnico realizado por Thycotic describe un ataque a una cuenta privilegiada; explica cómo los atacantes externos o los internos malintencionados pueden explotar las vulnerabilidades utilizando ejemplos como la contraseña de una cuenta de correo electrónico comprometida que se convierte en una violación total de la seguridad de la red.

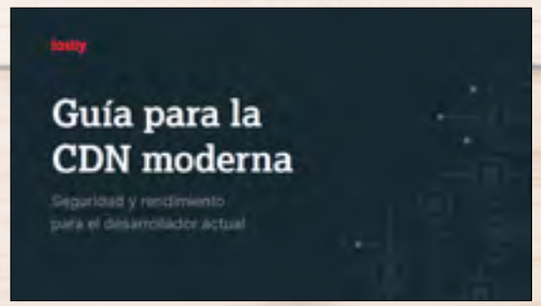
7 consejos para proteger los datos de tu empresa y vencer al ransomware

La pérdida de datos no es una broma. Los ataques de ransomware y malware van en aumento, pero ése no es el único riesgo. Con demasiada frecuencia, las empresas piensan que sus datos están bien respaldados, pero en realidad no lo están. Este documento de Commvault muestra siete razones comunes por las que las empresas pierden datos, a menudo porque nunca estuvieron realmente protegidos, junto con consejos para ayudarte a evitar que te ocurra lo mismo.

Cloud Migration: Apuesta por el futuro de tu organización en la nube

En tiempos de incertidumbre, la migración a cloud supone una ventaja organizacional al obtener una mayor funcionalidad, escalabilidad y flexibilidad, además de accesibilidad en cualquier momento y lugar. Este documento de Making Science recoge las principales ventajas de la migración a la nube, ejemplos de migración y las capacidades que ofrece Google Cloud a las organizaciones.

Guía para implementar una CDN moderna



Este documento de Fastly señala la evolución de la relación de los desarrolladores con la CDN (Red de Distribución de Contenidos) y explica por qué las CDNs tradicionales están obsoletas. El texto también detalla los beneficios que pueden aportar las CDNs modernas, que van desde una mejor visibilidad de los patrones de tráfico hasta el diseño de APIs que potencian una experiencia de usuario personalizada.

Aumentan las inversiones en empresas dedicadas a la Inteligencia Artificial

La Inteligencia Artificial está evolucionando en muchas direcciones diferentes y están surgiendo nuevos jugadores en el mercado con propuestas muy innovadoras, que están llamando la atención de las grandes tecnológicas. Así, en los últimos cinco años los inversores han redoblado su apoyo a las startups de IA, lo que a su vez ha estimulado las fusiones y adquisiciones, en una consolidación que se irá desarrollando a lo largo de los próximos años.

Según un reciente estudio publicado por GlobalData, entre 2016 y 2020 han aumentado rápidamente las inversiones de capital y las fusiones y adquisiciones dentro del campo de la Inteligencia Artificial. Esto se debe a que ha surgido muchas empresas emergentes centradas en diferentes ramas de la IA y en diferentes sectores que demandan soluciones inteligentes para el trabajo con los datos. Aunque en este tiempo se han producido fluctuaciones en el flujo de inversiones y operaciones de M&A, los expertos destacan el crecimiento en la actividad.

Aunque el volumen de acuerdos de financiación ha crecido de forma saludable en estos años, GlobalData destaca que 2020 supuso un

¿Te avisamos del próximo IT User?

varapalo a muchas de las iniciativas que estaban en marcha, y el volumen de los acuerdos se redujo en un 7,1%. Pero el valor de la financiación mantuvo una tendencia de crecimiento positivo, a pesar de las grandes fluctuaciones que se han producido en el período 2016-2020, especialmente en 2017, cuando se redujeron las inversiones y las adquisiciones.

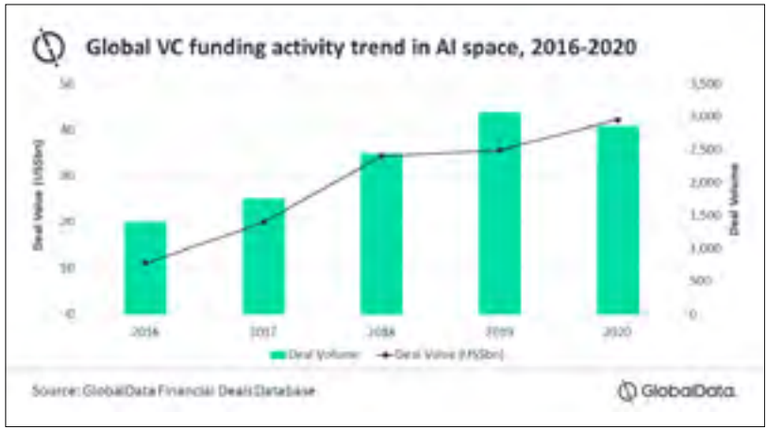
Para Aurojyoti Bose, analista principal de GlobalData, "a pesar de la tendencia fluctuante, el interés de los inversores y los sentimientos de negociación por la IA crecieron significativamente en los últimos años. Con las organizaciones globales reemplazando sus operaciones convencionales con tecnologías disruptivas como la IA, este entorno logró obtener un impulso de inversión significativo".

Entre 2019 y 2020 las inversiones de capital riesgo se redujeron un 7,1%, pasando de 3.075 a 2.856 operaciones, pero el valor de las transacciones aumentó un 18,7% interanual. Esto se vio reforzado por las grandes inversiones de empresas como SpaceX y Manbang Group, que impulsaron las cifras totales. Como explica Bose, "aunque la COVID-19 no impidió que se llevaran a cabo las fusiones y adquisiciones en el espacio de la Inteligencia Artificial, y el volumen de transacciones aumentó en 2020 en comparación con 2019, la menor valoración de los activos parece haber reducido el valor de la transacción".

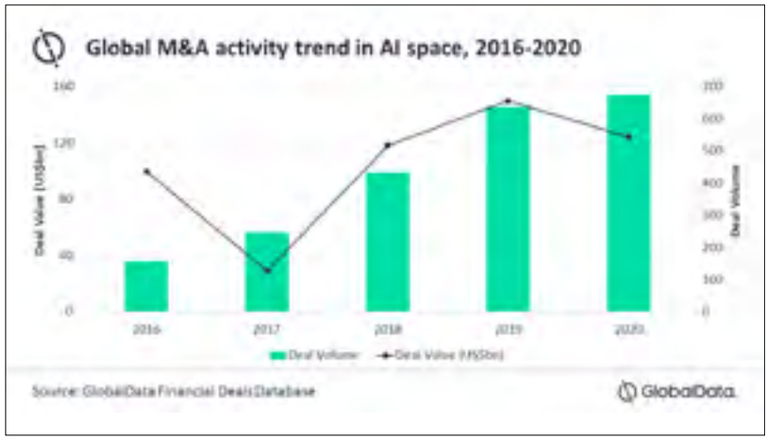
De cara al futuro, una vez superada la incertidumbre económica que ha generado la pandemia, los expertos tiene claro que el espacio de la Inteligencia Artificial seguirá evolucionando y recibiendo nuevos apoyos de los inversores y de los clientes. La IA es uno de los pilares de la digitalización de muchos sectores, y constantemente surgen nuevos enfoques y tecnologías más avanzadas, que recibirán el apoyo de los inversores. Y también se espera que las grandes tecnológicas sigan absorbiendo la capacidad de los innovadores, aunque no se espera que se pueda alcanzar una verdadera consolidación del sector, dado que siguen surgiendo nuevas ideas y soluciones que aprovechan las capacidades de la Inteligencia Artificial.

ESTADOS UNIDOS AUMENTA LAS INVERSIONES EN TECNOLOGÍA PARA LA INTELIGENCIA ARTIFICIAL

Los gobiernos tienen cada vez más claro que la Inteligencia Artificial es una tecnología clave para el futuro de la sociedad y la economía digital, por lo que están tratando de intervenir más en la investigación y desarrollo de las tecnologías asociadas a la IA, tanto a nivel de hardware como de software. Un ejemplo es Estados Unidos, que ante el avance de competidores como China está rediseñando completamente su estrategia en torno a la tecnología, poniendo el foco en la Inteligencia Artificial.



Clica en las imágenes para verlas más grandes



Siguiendo esta idea, la Comisión Nacional sobre Inteligencia Artificial (NSCAI) acaba de publicar un informa en el que explica la necesidad de crear una estrategia integral para abordar los desafíos y las oportunidades que surgirán en la era de la Inteligencia Artificial. En este documento los expertos afirman que se debe asegurar el liderazgo estadounidense en la industria de la microelectrónica para garantizar su supremacía mundial en el campo de la Inteligencia Artificial.

Por ello, solicita al gobierno la creación de una estrategia nacional de microelectrónica que permita reforzar la industria nacional de semiconductores, especialmente en las áreas dedicadas a la infraestructura para Inteligencia Artificial. Como informan desde la Asociación de la Industria de Semiconductores (SIA), para ello hará falta una inversión federal de unos 35.000 millones de dólares, así como el establecimiento de un crédito fiscal reembolsable para la inversión.

Desde su creación en 2019, como parte de la Ley de Autorización de Defensa Nacional (NDAA), la NSCAI se ha dedicado a estudiar y apoyar los avances en investigación y desarrollo de Inteligencia Artificial, aprendizaje automático y otras tecnologías asociadas. En este tiempo ha estado en constante contacto con las empresas e instituciones del país vinculadas a este campo para conocer los desafíos que enfrenta la industria y tratar de apoyar las iniciativas que permitirán mantener el liderazgo de Estados Unidos en el campo de la Inteligencia Artificial.

Este es un ejemplo del esfuerzo necesario para no quedarse atrás ante el avance de otras potencias como China y otros países asiáticos, que están apostando fuerte por el desarrollo de tecnologías de IA propias. Europa está todavía muy lejos, pero la UE está tratando de avanzar en el mismo camino, para que las empresas tecnológicas, las instituciones académicas y los gobiernos colaboren en el desarrollo de un ecosistema propio para contar con una Inteligencia Artificial adaptada a las necesidades y los principios de la UE.

Pero esto requerirá un nivel de compromiso e inversión muy superiores a los actuales, ya que el desarrollo de la IA requiere muchos esfuerzos combinados. Como ejemplo quedan las propuestas de la NSCAI, que está presionando al gobierno federal para que aumente la inversión directa y los mecanismos de financiación destinados a los proyectos de IA. Uno de los campos importantes en este camino es el de los semiconductores, ya que las arquitecturas de hardware para IA son cada vez más especializadas, y requieren tecnologías diseñadas específicamente para ello. ■

España contará con una Dirección General de Digitalización e Inteligencia Artificial

El Gobierno ha aprobado la creación de la nueva Dirección General de Digitalización e Inteligencia Artificial (IA), que dependerá directamente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, a cuyo cargo está Carme Artigas. Al frente de la Dirección General está Ángel Sánchez Aristi, experto economista cuya trayectoria profesional se ha desarrollado entre 1985 y 2017 en el sector financiero, en el que ha ocupado cargos de diferente responsabilidad en Dresdner Bank, Banco Exterior de España, Argentaria y BBVA.

En esta dirección general Sánchez Aristi asumirá, entre otras funciones, el estudio, propuesta y ejecución de la política general, la planificación estratégica y de acción sobre la Transformación Digital de la economía y la sociedad, así como la elaboración, coordinación y evaluación de la Estrategia Española de Inteligencia Artificial (ENIA).

MÁS INFORMACIÓN

GlobalData Inteligencia Artificial

El comercio electrónico crecerá un 24% en España y superará los 40.000 millones de euros en 2021

Más del 80% de los españoles comprará online en algún momento durante el año, aunque es posible que la frecuencia de compra este año no crezca tanto como en 2020, y casi la mitad lo hará desde un smartphone. Los marketplaces son la opción preferida de compra en casi todos los productos, con Amazon como el marketplace líder.

Según datos de Astound Commerce, en 2020 las ventas del ecommerce crecieron un 36% en España. Pues bien, en 2021 se prevé que el gasto medio en el comercio electrónico en España se mantendrá en una media de 900 euros por persona, hasta un total de entre 40.000 y 45.000 millones de euros,

que dependerá de la duración y severidad de la crisis económica y las restricciones derivadas del coronavirus. Esto supone un 24% más con respecto al año pasado, mientras que a escala mundial las compras digitales aumentarán en un 18%, hasta los 665.000 millones de euros.

El estudio muestra que más del 80% de los españoles comprará online en algún momento durante este ejercicio, y casi la mitad lo hará desde un smartphone, superando así los temores iniciales sobre compras seguras. Con todo, es posible que la frecuencia de compra este año no crezca tanto como en 2020, que creció un 51%, ya que se producirá un efecto de normalización en las compras impulsivas, por promociones o pánico.

"Se habla mucho sobre el crecimiento imparable del 'ecommerce' y el impulso provocado por el confinamiento prolongado. En los últimos meses se ha avanzado el equivalente a cinco años, sin embargo, no parece que ese ritmo sea sostenible para 2021 aunque será todavía muy significativo y permanente", afirma Daniel Carnerero, vicepresidente de Astound Commerce para España y Portugal. "Esperamos una desaceleración del crecimiento una vez la actividad vuelva a cierta normalidad, algo que va a tardar más de lo que se proyectaba inicialmente.

Lo que no cambiará es la preferencia por los marketplaces para comprar casi todos los productos. Amazon, con el 15,7% del mercado en 2020, verá acentuado su liderazgo en 2021 (a alrededor del 16,2%), con muchos pequeños comercios incorporándose a su ya amplia oferta. Algo similar ocurrirá con Aliexpress, que llegará al 5%, frente a su participación actual del 4,4%.

CRECE EL COMERCIO ELECTRÓNICO

LAS COMPRAS ONLINE HAN AUMENTADO UN 15% ENCABEZADAS POR LOS MILLENNIALS

SAP y The Economist Intelligence Unit han dado a conocer las conclusiones del estudio El comprador influyente, en el que analizan los hábitos de compra adquiridos durante la pandemia por grupos generacionales. En general, en todos los países en los que se ha realizado la investigación, el incremento del gasto online entre junio y agosto ha sido del 15%, lo que pone de manifiesto el buen momento que está atravesando el ecommerce. Otro aspecto positivo para el mercado de ecommerce es que, el 40% de los encuestados afirman estar más familiarizados ahora con las compras online que antes de la pandemia.

Por grupos generacionales, los baby boomers son los que más han aumentado el gasto online

Clica en la imagen para verla más grande

y los millennials, los que más invierten. Los primeros en 12 puntos porcentuales, al pasar del 25% que representaba este canal en el total de sus ventas entre enero y marzo, a un 37%, en junio y agosto. Les sigue la generación X, que ha pasado del 39 al 47%.

Si se analizan las compras efectuadas en el período de pandemia objeto de este estudio, se observan dos tendencias: por un lado, la consolidación de las compras de productos básicos y, por otro, de productos no esenciales que antes se adquirían en las tiendas, lo que pone de manifiesto un aumento de la confianza en el canal online. La adquisición de productos básicos (comida a domicilio, alimentación, productos de limpieza e higiene personal) aumentó en todos los grupos de edad, siendo especialmente significativa entre los baby boomers. En cuanto a productos no esenciales, como ropa y electrónica de consumo, su peso en el total de compras online se ha incrementado en 10 y 11 puntos porcentuales, respectivamente.

El incremento en la adquisición de productos no esenciales en los canales online se explica por la inseguridad que sienten a la hora de acudir a una tienda física. En España, un 23% son más reacios a acudir a establecimientos físicos. Ese temor se manifiesta también al analizar las ventajas de la compra online, ya que el 44% de los encuestados menciona evitar multitudes, aunque la principal ventaja de los canales online, señalada por un 49%, es la comodidad que proporciona poder adquirir los productos en cualquier momento y desde cualquier lugar.

El estudio también ha querido ahondar en las ventajas que reconocen los consumidores a comprar en tiendas físicas. La primera, para todas las generaciones, es la gratificación instantánea de llevarse el producto directamente a casa. Así lo manifiesta el 57 % de los encuestados. Le sigue la posibilidad de evaluar el aspecto y el tacto del producto, y las ofertas y descuentos.

Cuando la situación provocada por la pandemia mejore y se reduzcan las restricciones, los hábitos de compra adquiridos en estos meses cambiarán, aunque más de 6 de cada 10 encuestados (61%) asegura que mantendrá alguno de ellos. ■

En 2021 se prevé que el gasto medio en el comercio electrónico en España se mantendrá en una media de 900 euros por persona, hasta un total de entre 40.000 y 45.000 millones de euros

MÁS INFORMACIÓN

El comprador influyente

Ciberinteligencia, clave para afrontar las amenazas

El 85% de las empresas utiliza activamente la inteligencia contra ciberamenazas, y el 15% restante tiene planes para empezar a hacerlo en el corto plazo. Las organizaciones reconocen que es clave para detectar amenazas, bloquearlas y responder ante los ataques.

El repunte de las brechas de seguridad en el último año, agravado por los ataques relacionados con el coronavirus, no ha hecho más que aumentar la importancia de la inteligencia contra ciberamenazas como una de las mejoras bazas para evitar los estragos de los cibertataques. Así se desprende de la encuesta SANS Cyber Threat Intelligence 2021, patrocinada por ThreatQuotient, que revela que el 85% de los encuestados afirman ya utilizar activamente la inteligencia contra ciberamenazas, mientras que el 15% restante "todavía no lo hace, pero tiene previsto hacerlo a corto plazo".

La inteligencia contra ciberamenazas ya no se percibe como algo exclusivo de una minoría de las organizaciones, con un cambio sustancial en el número de empresas que reconocen sus beneficios como una apuesta segura para ayudar en la toma de decisiones y en las estrategias de respuesta. Preguntados por la valía de la inteligencia contra ciberamenazas, el 77% de los encuestados afirmó que este tipo de ciberinteligencia mejoraba sus capacidades de detección y respuesta, el 78% calificó que los datos e información fueron aprovechados para detectar amenazas y ataques, el 70% los uti-

CRECE EL ROBO DE CRIPTOMONEDAS

lizó para ayudar a bloquear amenazas, y el 66% para apoyar su respuesta a incidentes.

Casi el 20% de los encuestados indicaron que su implementación de inteligencia de amenazas cambió durante la pandemia, ya que los ciberdelincuentes se aprovecharon de esta situación con un fuerte aumento de los ataques de phishing y ransomware relacionados con la pandemia, dirigidos a empresas de todos los sectores. El cambio masivo hacia la implantación del trabajo a distancia amplió la superficie de ataque de las organizaciones. No obstante, los encuestados identificaron claramente las amenazas del trabajo desde casa, tales como el phishing, la pérdida o el robo de dispositivos, la desprotección de los equipos de red domésticos, el malware recurrente, la divulgación accidental de información de datos sensibles y el acceso no autorizado de los empleados a los activos de la empresa en remoto.

Los resultados también muestran que el trabajo a distancia ha cambiado la forma en la que los equipos de inteligencia contra amenazas, de respuesta a incidentes y de los centros de operaciones de seguridad se comunican. Por un lado, el trabajo a distancia ayudó a los equipos a estar más centrados y a colaborar, mientras que el uso de plataformas basadas en texto ayudó a facilitar la comunicación entre los equipos. Sin embargo, algunos encuestados señalaron que la pérdida de conversaciones cara a cara inhibía el intercambio de información crítica entre ellos.

Según Eutimio Fernández, country manager de ThreatQuotient para España, la pandemia está cambiando la forma en que las organizaciones perciben su propio panorama de amenazas, y los analistas de inteligencia contra ciberataques se están beneficiando de las herramientas y procesos automatizados y del compromiso con los centros de análisis e intercambio de información. “Es increíblemente alentador ver que un número cada vez mayor de empresas, independientemente de su tamaño, dan prioridad a la implantación de esta inteligencia tan ventajosa”, señala.

Para este directivo, antes de que se lleve a cabo un ciberataque, “todavía hay una oportunidad significativa para que las compañías gestionen mejor su inteligencia contra ciberamenazas, para implantar una mayor seguridad y alcanzar una mayor eficacia, con la adopción de las herramientas y los procesos adecuados”. ■

CINCO CONSIDERACIONES PARA PROTEGER LA INFRAESTRUCTURA EN LA NUBE

MÁS INFORMACIÓN

2021, ¿el año de la ciberdefensa?

Crecimiento acelerado de las comunicaciones unificadas como servicio

La crisis sanitaria global está transformando la forma de trabajar de las empresas, impulsando el uso de los servicios en la nube y de herramientas de comunicaciones y colaboración. Como consecuencia, los expertos esperan que el mercado de Comunicaciones Unificadas como Servicio (UCaaS) va a crecer rápidamente en los próximos cuatro años, gracias al desempeño de los proveedores de red y de servicios Over-the-Top, que aprovecharán las nuevas conexiones de banda ancha.

Para la mayoría de empresas, Implementar infraestructura propia para las comunicaciones unificadas supone más complejidad y gastos de capital de lo necesario, por lo que están recurriendo cada vez más a proveedores de Comunicaciones Unificadas como Servicio (UCaaS). Esto está contribuyendo a la rápida expansión de un mercado que se está beneficiando del progreso de la nube y las redes de comunicaciones de alta velocidad.

Como explican los expertos de IDC, los proveedores de Comunicaciones Unificadas como Servicio suelen ser operadores de red y empresas de cable que ofrecen UCaaS de múltiples instancias/inquilinos en la nube, o proveedores de servicios UCaaS over-the-top (OTT) que aprovechan la banda ancha existente. Juntos, representan la mayor parte de este mercado, y los analistas de IDC pronostican que sus in-

gresos seguirán creciendo a una CAGR del 7% entre 2019 y 2025, pudiendo alcanzar unos 16.100 millones de dólares para el año 2024.

Para Denise Lund, directora de investigación de Telecomunicaciones globales y Comunicaciones unificadas en IDC, "existen amplias oportunidades para los proveedores de servicios UCaaS en todo el mundo, ya que las empresas buscan formas de capacitar a los empleados para que se comuniquen fácilmente, compartan información y se reúnan según sea necesario con colegas, clientes y socios".

Pero explica que "la oportunidad también plantea desafíos reales para los proveedores de servicios que aún no han determinado cómo diferenciar sus ofertas y agregar valor para sus clientes. Incluso con una tremenda necesidad del mercado, los proveedores de servicios UCaaS deben estar preparados para expandir y refinar sus ofertas para competir en este mercado".

Según los expertos, el ranking del mercado de UCaaS abarca un gran número de proveedores y está en constante movimiento. En el segmento más bajo se están produciendo grandes cambios con la introducción de nuevas capacidades pensadas para las pequeñas y medianas empresas. Muchas provienen de los segmentos superiores, a medida que la nube facilita el acceso a servicios de alto valor con menos recursos. IDC señala que los operadores de red, empresas de cable y proveedores OTT compiten por mejorar la experiencia de usuario, mejorar la fluidez de las integraciones en soluciones UC&C más amplias y por mejorar los precios.

En palabras de Lund, "las PYMES necesitan un proveedor de servicios que pueda satisfacer sus requisitos de comunicación hoy, crecer con ellos en el futuro y ofrecer una experiencia de usuario excepcional para los empleados. Las soluciones UCaaS que ofrecen un punto de entrada de buen valor son una buena forma para que una PYME comience el viaje".

En cuanto al segmento dedicado a empresas más grandes, IDC explica que la pandemia ha llevado a una adopción masiva de los servicios UCaaS, lo que les ha permitido dotar a sus empleados de capacidades de teletrabajo de forma rápida, pudiendo adaptarse a la situación con bastante agilidad. Por otro lado, las necesidades de las organizaciones trascienden las capacidades básicas de los servicios de una suite UCaaS convencional, ya que las grandes empresas necesitan mayores niveles de seguridad y orquestación de red. Esto es fundamental para lograr una integración total con los servicios de comunicaciones de voz y datos de la organización, y también para proporcionar una experiencia de administración más sencilla.

Otro punto calve que los proveedores deben tener en cuenta es la necesidad de que las soluciones UCaaS se integren mejor con el software empresarial más extendido, lo que incluye las suites de colaboración. Y también es vital la capacidad de combinar paquetes de UCaaS para satisfacer las necesidades comerciales de la organización de forma rentable y eficiente, algo que IDC recomienda tener muy encuenta a los proveedores del mercado.

Como explica Kund, "las empresas necesitan un proveedor de servicios que pueda cumplir la promesa de flexibilidad, confiabilidad, seguridad, integraciones de UCaaS y una visión de cómo contribuye al papel más amplio de las comunicaciones unificadas y la colaboración en toda su organización, especialmente a medida que comienzan a surgir modelos de trabajo híbridos". Por ello, concluye que "lo primordial para el éxito es una cartera amplia y rica de servicios e integraciones de UCaaS, así como servicios de implementación y soporte de nivel empresarial". ■

MÁS INFORMACIÓN

- Comunicaciones Unificadas
- UCaaS: Previsiones 2020-2024, según IDC

TENDENCIAS

¿Qué habilidades necesitan los líderes ante el nuevo entorno?

Las habilidades digitales de los directivos condicionan el éxito de las empresas en el nuevo entorno. Según The Valley, para conducir a sus empresas a la recuperación, es imprescindible tener líderes que dominen las nuevas tecnologías y piensen de forma más analítica.

Para impulsar la recuperación, la digitalización es un paso no se puede dilatar más, y tiene que ser liderada por directivos capaces de definir estrategias y planes de acción adaptados a la economía digital para el que no todos están preparados. Según The Valley, los buenos directivos digitales necesitan tener una mente orientada a resultados, capacidad estratégica y de gestión, dominio de las metodologías de trabajo innovadoras o soft skills.

MENTE ANALÍTICA PARA BASAR LAS DECISIONES EN RESULTADOS

La toma de decisiones importantes es una de las principales responsabilidades de todos los directivos y líderes, sin importar su tipo de empresa o sector. Por ello, pensar de forma analítica es una habilidad imprescindible de los directivos de cara a poder evaluar cada situación de forma objetiva y neutral, teniendo en cuenta todos los factores influyentes, y poder tomar decisiones basadas en datos reales que permitan resolver problemas, lograr objetivos y mejorar resultados.

CAPACIDAD ESTRATÉGICA PARA LIDERAR PROYECTOS

Gran parte del éxito de un directivo recae en su capacidad para liderar equipos. Se habla cada vez más de las diferencias entre un jefe

Determinación y sensibilidad: las dos características personales críticas de los CIO en 2021

y un líder, y es que los profesionales prefieren tener líderes de los que aprender y que les inspiren y motiven, más que jefes autoritarios que simplemente dirijan. Así, cobra especial importancia la capacidad de liderar proyectos teniendo en cuenta factores como la gestión del tiempo de cada persona, el trabajo en equipo, el seguimiento y la confianza.

DOMINIO DE LAS METODOLOGÍAS DE TRABAJO INNOVADORAS PARA AFRONTAR LOS CAMBIOS

En la era digital, el trabajo debe ser lo más eficiente posible. Para ello, existen diversas metodologías de trabajo como Design Thinking, Lean o Agile que los directivos deben saber poner en marcha e integrarlas en sus procesos de trabajo para crear productos innovadores, mejorar en las estrategias de negocio e impulsar el negocio, sobre todo, aquellos que trabajan en el ámbito digital.

CAPACIDAD DE GESTIÓN PARA PONER EN MARCHA NUEVOS MODELOS DE NEGOCIO

Hoy en día es imprescindible que las compañías integren en sus estrategias nuevos modelos de negocio para seguir siendo competitivos en la economía digital y ofreciendo a los consumidores una respuesta a sus demandas y hábitos. A modo de ejemplo, una compañía que se dedique a la venta de productos o servicios, debe contar con canales de venta online como un ecommerce o un marketplace. En este sentido, la formación continua se posiciona como la clave para que los directivos puedan estar al tanto de los diversos modelos de negocio que existen y puedan implementarlos y gestionarlos exitosamente en sus empresas.

SABER DESENVOLVERSE CON LAS NUEVAS TECNOLOGÍAS

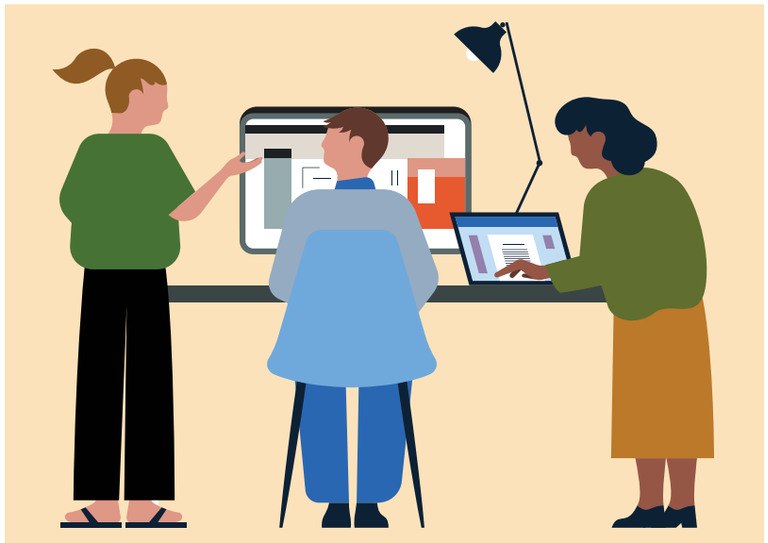
Cualquier directivo que quiera tener éxito en la economía digital debe contar con habilidades digitales y conocimientos tecnológicos. Y no vale con saber utilizar los dispositivos tecnológicos. Para destacar se debe estar familiarizado con las nuevas tecnologías como el IoT, el Blockchain o la Inteligencia Artificial para poder aplicarlas en las estrategias de negocio y aprovechar todos sus beneficios y ventajas.

SOFT SKILLS, TAN DEMANDADAS COMO LAS HARD SKILLS

Más allá de la capacidad analítica o de gestión, o la visión estratégica de negocios, lo directivos deben contar con soft skills que les ayuden a ser profesionales exitosos y buenos líderes. Por ello, son claves habilidades como la creatividad, la gestión del tiempo, la colaboración, la empatía, la capacidad de motivar y reconocer el esfuerzo de los demás o de adaptarse a diferentes situaciones en un entorno tan volátil. ■

MÁS INFORMACIÓN

Informe empleos emergentes



TECNOLOGIA Y SANIDAD:

la mejora en la atención del usuario

Patrocinadores:
COMMSCOPE RUCKUS
GRENKE
SOPHOS
S21SEC

Las TIC en Sanidad: el paciente como eje central de las nuevas tecnologías

En un mundo impulsado por la digitalización, la integración de la tecnología es prioritaria, más si cabe en un sector como el de la sanidad, sometido a significativos cambios durante el último año.

La pandemia generada por el Coronavirus SARS-CoV-2 ha puesto de manifiesto la importancia de contar con un sistema sanitario eficaz, accesible y resiliente, no solo a nivel de capacitación de los profesionales, sino también en lo referente a infraestructuras, servicios de alto valor, y, por supuesto, mejores tecnologías.

Y es que, como en todo, aunque en el sector sanitario con más razón, la adopción de nuevas tecnologías, sobre todo de las centradas en la Información y la Comunicación (TIC), puede aportar un valor diferencial. La Socie-

TECNOLOGIA Y SANIDAD: la mejora en la atención del usuario

dad Española de Informática de la Salud (SEIS) considera las TIC, "imprescindibles para afrontar los retos actuales de los sistemas de salud en sus procesos de modernización y racionalización, y para lograr la transformación digital del sector. Además, su utilización intensiva favorece el tejido industrial, la innovación y la economía del país" .

Sin embargo, en este contexto de evolución digital, es importante tener en cuenta que la transformación tecnológica del sector sanitario debe ir más allá de la mera digitalización de los procesos; también implica ofertar nuevos productos y servicios digitales a los pacientes, además de acercar capacidades de diagnóstico, tratamiento y seguimiento a millones de personas, sin importar su ubicación.

Precisamente, y a lo largo del último año, con el sistema de salud colapsado a causa de la Covid-19, el redireccionamiento de la asistencia a los pacientes a través de la atención y el seguimiento a distancia ha sido más trascendental que nunca, convirtiéndose en muchos casos en la única alternativa, bien como primera capa informativa o canal de comunicación bidireccional entre el usuario y los diferentes profesionales de los distintos niveles asistenciales.

En este sentido, y junto a la telemedicina, Internet se ha alzado como medio idóneo para que los pacientes puedan acceder a asistencia médica sin tener que pasar por hospitales y centros de salud. Así, sistemas de videoconsulta, videollamadas, aplicaciones móviles o chatbots están siendo muy utilizados. También, otras tecnologías como Inteligencia Artificial, Machine Learning, Big Data o la analítica avanzada de datos están permitiendo progresar en cuanto a detección temprana y previsiones de evolución del coronavirus, entre otras. Y, por supuesto, IoMT, el Internet de las Cosas Médicas, un sistema de dispositivos médicos interconectados que utilizan sensores informáticos para así poder intercambiar datos a través de Internet. Con esta tecnología es posible conocer con mayor precisión la situación del paciente, aplicar tratamientos más efectivos y facilitar la prevención.

No obstante, y pese a estos avances, el sistema sanitario español, sobre todo la sanidad pública, sigue aquejado de una escasez de recursos de distinta índole. Años de falta de inversión, barreras administrativas, desajustes estructurales y una segmentación política incesante han lastrado su digitalización, actuando como verdaderos inhibidores. A este respecto, el Índice SEIS 2019 cifra la inversión sanitaria actual en TIC en España en 707.344 euros, un 3% menos que en 2018, mientras que el personal especializado en TIC y el gasto global en plataformas tecnológicas también se ha reducido un 1,86% y un 8,19% respectivamente.

En la actualidad, y tras lo acontecido a lo largo del último año, es de esperar que la tendencia cambie: la Covid-19 ha acelerado la adopción digital en todos los ámbitos, incluido el sanitario, por lo que las TIC se hacen imprescindibles para afrontar los retos actuales.

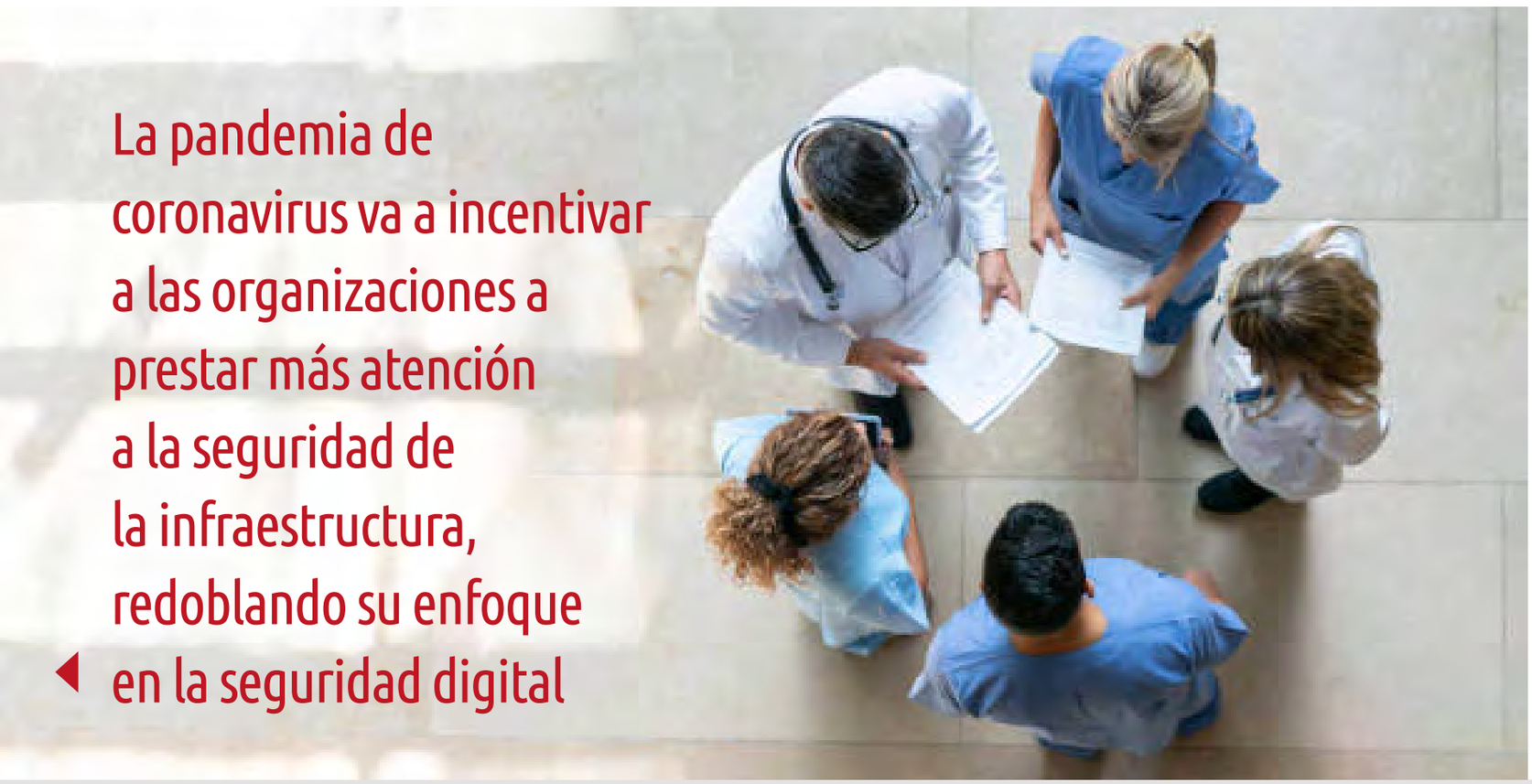
TECNOLOGIA Y SANIDAD: la mejora en la atención del usuario

IMPULSAR UNA ESTRATEGIA DE SALUD DIGITAL

Sobre este necesario avance, la ministra de Sanidad, Carolina Darias, adelantaba el pasado mes de febrero los principales puntos que constituyen la hoja de ruta de su Ministerio para los próximos años y entre los que se encuentran, la digitalización y la innovación de la sanidad. Adicionalmente, el Gobierno de España ha incluido en los Presupuestos Generales del Estado (PGE) para 2021 una dotación de 400 millones de euros para la Renovación de Tecnologías Sanitarias en el Sistema Nacional de Salud (SNS), además de 295,5 millones destinados a acelerar la estrategia digital del SNS.

A nivel privado, empresas como Accenture ya valoran que las empresas sanitarias preparadas para el futuro implementen estrategias digitales más innovadoras. Ya se trate de aplicaciones móviles, nube, EHR o wearables, las organizaciones líderes pueden cambiar fundamentalmente la forma en que se presta la atención médica.

Es de prever, por tanto, que estas iniciativas, y otras que estén por venir, potenciarán la innovación del sector sanitario, un nicho que hasta ahora se ha centrado mayoritariamente en integrar tecnologías dirigidas a modernizar el propio sistema en sí, como la Receta Electrónica o el acceso a la historia clínica electrónica por parte de los facultativos, más que en otras dirigidas a cubrir las necesidades reales de pacientes y profesionales.



La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando su enfoque en la seguridad digital

Preciso es también procesar adecuadamente los volúmenes masivos de información que caracterizan la actividad propia de los servicios de salud y que bien aprovechados pueden generar enormes beneficios.

EL DATO, EL ACTIVO MÁS SENSIBLE

La digitalización de los dispositivos utilizados en el entorno de la sanidad genera una ingente cantidad de información sensible sobre el ser humano. Se estima que en 2020 se alcanzaron los 25.000 petabytes de datos en el entorno sanitario, una cifra que sigue incrementándose de forma exponencial, influida también por el desarrollo de dispositivos IoT, que están contribuyendo a que los datos crezcan a una escala nunca vista.

Tal acumulación masiva de datos hace imposible su gestión a través de sistemas tradicionales, por lo que tecnologías como Big Data, Business Intelligence o la analítica de datos ofrecen nuevas posibilidades para la elaboración de modelos predictivos, patrones de comportamiento o para la provisión de servicios más personalizados en tiempo real. Igualmente sientan la base para la interoperabilidad electrónica de la información sanitaria y allana el acceso a la tan ansiada Medicina 5P (Personalizada, Predictiva, Preventiva, Participativa y Poblacional); el cruce entre la sanidad y Big Data.

El análisis de grandes conjuntos de datos también ha servido como base para la aplicación de la Inteligencia Artificial, Machine Learning o Deep

TECNOLOGIA Y SANIDAD: la mejora en la atención del usuario

Learning en el campo de la salud, como una herramienta fundamental de la medicina personalizada. Estas tecnologías pueden ampliar la analítica con el aprendizaje continuo y los análisis, derivando en una ventaja para el ser humano gracias a mejoras en el diagnóstico precoz de enfermedades, los tratamientos a medida, y una mejor administración eficaz de recursos sanitarios.

Por tanto, no hay duda de que el tratamiento global y sistemático de los datos ha abierto un nuevo mundo en distintas áreas. Sin embargo, el acceso a datos personales por parte de facultativos, máquinas y demás responsables no gusta a todos por igual.

En este contexto, satisfacer las expectativas sobre la privacidad y seguridad de los datos se hace clave para impulsar la sanidad digital. Sin duda, el conocimiento por parte del paciente de la finalidad del uso de sus datos y de los mecanismos de protección empleados incrementará la confianza en la sanidad digital.

PROTEGER Y CUIDAR LOS DATOS

La información confidencial que maneja el sector sanitario es de gran interés para la ciberdelincuencia por lo que se ve continuamente sometida a ataques, además de ser víctima de brechas o fugas de información que generan un gran coste económico (5,8 millones de euros, en 2020, según Data Breach Report publicado por IBM). Y es que, por su importante información, los registros médicos de pacientes tienen un valor en el mercado negro hasta 50 veces superior al de la información financiera personal, lo que explica que los ataques contra el sector sanitario se incrementen sin medida. No hay más que ver que el número de intentos de ataque contra empresas de la salud aumentó a nivel mundial un 45% durante los dos últimos meses de 2020, según indica Check Point, más del doble de lo que creció en todos los sectores a nivel mundial. En el caso de España, el número de ataques contra infraestructuras sanitarias también se duplicó en ese periodo, tal y como revela dicha fuente.

Las amenazas más comunes que afectan al sector salud tienen su origen en el correo electrónico: suplantación de identidad, campañas de phishing, adjuntos maliciosos, aunque es el ransomware el que muestra el mayor aumento, sobre todo la variante Ryuk. Los cibercriminales saben que una interrupción del servicio en un hospital puede ser crítico, por lo que apuntan sus objetivos a estos blancos, más propensos a satisfacer sus demandas de rescate.

SIN VACUNA PARA LOS ATAQUES

En cuanto a las tendencias, es de esperar que la pandemia de Covid-19 siga actuando sobre la mayoría de las amenazas y riesgos, muchos de estos directamente relacionados con el aumento del teletrabajo. En este sentido, el mayor uso de soluciones en la nube, conexiones VPN, servicios de escritorios VDI, redes de confianza cero y gestión de identidades, servicios y tecnologías

La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando estas su enfoque en la seguridad digital

para el acceso remoto, uso de herramientas colaborativas o aplicaciones de videoconferencia generará que los ataques a estos entornos, en especial a los sistemas públicamente expuestos, sigan creciendo . También los ataques y vulnerabilidades relacionados con redes domésticas o dispositivos personales y los dirigidos contra farmacéuticas, laboratorios de investigación dedicados a la Covid-19. Asimismo, y en relación a los ataques de ransomware, es necesario señalar una tendencia, ya consolidada, como es la sofisticación de dichos ataques.

Sin duda, la medicina se usará como señuelo al menos hasta el final de la pandemia. El factor humano es uno de los componentes más importantes de muchos ataques, y la información sobre nuevas restricciones regulatorias, tratamientos potenciales y la salud del paciente seguirá atrayendo la atención de los usuarios. Los expedientes médicos filtrados también se convertirán en parte del gancho de los ataques dirigidos, ya que la información precisa del paciente hará que los mensajes falsos sean mucho más creíbles.

No obstante, también hay buenas noticias. La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando estas su enfoque en la seguridad digital. Es más, según se desprende del Informe de Ciberpreparación de Hiscox 2020, la industria española de Pharma y Salud ha mejorado con respecto a 2019 tanto su ciberpreparación, incrementándose desde el 4% al 12% el número de empresas calificadas como expertas, como la inversión en TI. Las compañías participantes han pasado de invertir el 4,6% del presupuesto de TI en ciberseguridad al 13,73% en 2020. Además, más de la mitad (56%) dicen integrar aspectos de ciberseguridad en todos los procesos y proyectos desarrollados en su plan de negocio, convirtiendo esta área en una variable transversal a toda la organización.

A raíz de esta situación, no hay duda de que las TIC juegan y jugarán un papel determinante en las organizaciones sanitarias, para facilitar la gestión eficiente de los servicios ofrecidos a la ciudadanía y la capacidad asistencial. La necesidad de comunicarse de manera efectiva con los pacientes es una prioridad, como ha quedado demostrado. Por tanto, hay que seguir trabajando para aumentar las conexiones digitales con los pacientes (más datos y análisis en tiempo real) para mejorar la calidad asistencial mediante una medicina basada en la evidencia y en al análisis del dato para la toma de decisiones adecuadas. Es hora de desarrollar una medicina personalizada con la ayuda de las TIC. ■

MÁS INFORMACIÓN

- Índice SEIS 2019
- Hoja de ruta del Ministerio para digitalizar e innovar en Sanidad
- Renovación de Tecnologías Sanitarias en los Presupuestos Generales del Estado
- IBM Data Breach Report
- Incremento de ataques a organizaciones sanitarias por la Covid19

Una infraestructura de red inteligente mejora los resultados, las operaciones y la seguridad a todos los niveles.

Los centros de atención médica super conectados del mañana ofrecen oportunidades casi ilimitadas para potenciar la conectividad universal (cableada, Wi-Fi y celular en interiores) para construir una red estable de servicios, aplicaciones y herramientas que sirven como base de la evolución de su red a largo plazo. Desde la oficina más pequeña hasta el laboratorio de investigación más avanzado y el campus hospitalario más grande, existen nuevas y emocionantes formas de mejorar la atención sanitaria y la eficiencia operativa.

Conozca las soluciones de CommSCope para el Sector Sanitario: **Click aquí**

© 2021 CommScope, Inc. All rights reserved. AD-115564-EN

Transformación tecnológica como paso previo hacia un nuevo modelo de sanidad

El de la Sanidad es un segmento especial, tanto por la necesidad de inmediatez en la respuesta como por la sensibilidad de los datos que manejan. Por ello, este sector debe poner todo de su parte para ofrecer un servicio continuado, pero sin descuidar aspectos como la seguridad de la información o la protección de los dispositivos de salud. Los retos, por tanto, no dejan de crecer. ¿Está la Sanidad española preparada para superarlos?

Para hablar de estos temas y analizar otras cuestiones como el estado actual de la inversión en la Sanidad, nuevas formas de financiación y servicio o conocer qué se está haciendo, tanto desde la sanidad pública como privada para proteger los datos y luchar contra el incremento de ciberataques, hemos contado con la participación en esta #MesaRedondaIT de Bernardo Gómez, territory account manager Iberia de CommScope; Marco Frühauf, vicepresidente de Grenke; e Iván Mateos, Ingeniero preventa de Sophos. Asimismo, incluimos las opiniones y valoraciones de Jairo Alonso, ICS security consultant de S21Sec, quien por problemas de última hora no pudo conectarse al debate.

ESTADO DE SALUD TECNOLÓGICO

Sin duda, y en lo que respecta a la adopción de Tecnologías de la Información y la Comunica-

TECNOLOGÍA Y SANIDAD: mejora en la atención al paciente

“La situación actual puede repetirse, y hay que estar preparados. No obstante, el ritmo de inversión se ralentizará a medio plazo, porque las inversiones se han adelantado. En un año hemos avanzado lo que en condiciones normales hubiese llevado entre tres y cinco”

BERNARDO GÓMEZ, TERRITORY ACCOUNT MANAGER IBERIA DE COMMSCOPE

ción, el sector sanitario ha dado un gran paso de gigante a lo largo del último año. En este contexto, Bernardo Gómez considera que la situación provocada por la pandemia ha servido como “catalizador para impulsar la adopción de este tipo de tecnologías y si bien aún queda mucho camino por recorrer, el sanitario se encuentra en un punto significativamente desarrollado”.

Algo distinto ocurre en lo concerniente a los flujos de caja, donde Marco Frühauf, evidencia algunos desafíos: “durante el último año, algunos subsectores, como el de las farmacias, han tenido que hacer frente a una falta de tesorería, al no recibir, o fluir más lenta, la financiación proveniente de las Administraciones Públicas”. Por tanto, y aunque por su trascendencia este sector demanda estar perfectamente equipado, “también requiere estar bien financiado, y aquí todavía hay aún muchos retos”.

“La rápida digitalización de principios de 2020 abrió la puerta a nuevos riesgos en ciberseguridad, que han tenido que ir mitigándose”, reconoce Iván Mateos. Sin embargo, y aunque la situación actual es más positiva de lo que se preveía, el sector sanitario sigue en el punto de mira de muchos atacantes. No obstante, “las empresas están actuando, tomando decisiones a corto y medio plazo y en ese sentido no vamos por mal camino, aunque hay que seguir avanzando”.

“La sanidad española dispone de prácticamente los últimos dispositivos del mercado”, destaca Jairo Alonso, por lo que, a nivel de equipamiento tecnológico está bastante actualizada para hacer frente a los problemas de ciberseguridad. Sin embargo, “esto no significa que no existan otros equipos y dispositivos tradicionales que sigan funcionando perfectamente”, reconoce este responsable.

INVERSIÓN SIN PLANIFICACIÓN

A raíz de lo comentado, no hay duda de que la inversión en tecnologías a lo largo del último año ha sido muy importante en Sanidad. Sin embargo, ¿se han hecho estas adquisiciones en base a una planificación o las empresas se han dejado llevar por la alarma del momento?

Aunque, en los primeros meses, la aceleración en los procesos de digitalización llevó a muchas empresas a realizar una inversión tecnológica no planificada, Marco Frühauf considera que según se fue avanzando, y teniendo acceso a más información, la situación varió. “Las grandes inversiones se han hecho bien, han sido planificadas. Sin embargo, sobre todo al principio, se tomaron decisiones precipita-

das; se adquirió equipamiento que no era necesario o que no era la solución adecuada, debido a una gran desinformación".

En la misma línea, Iván Mateos coincide en destacar cierta improvisación a la hora de adquirir equipamiento, porque al principio lo que primaba era la productividad. "Hoy con el conocimiento de que esta situación aún se va a extender en el tiempo se impone la planificación, ajustar los presupuestos a las necesidades, ya sin prisa. En su momento se cometieron muchos fallos, se abrieron más puertas de las necesarias y esto trajo distintas consecuencias. "Lo peor ya pasó y ahora estamos intentando hacerlo todo mejor".

Sobre las infraestructuras de comunicaciones, Bernardo Gómez destaca que se han acelerado los tiempos de despliegue de las agendas de digitalización ya preestablecidas, variando las prioridades. "Si antes de la pandemia, hospitales y residencias apostaban por el desarrollo de las redes de uso interno, con la integración de tecnologías como IoT, la nueva situación ha llevado a priorizar las redes de accesos para los pacientes. "Hemos pasado de la incertidumbre a la racionalización de la tecnología, una vez entendido a qué nos enfrentamos".

La adquisición de tecnología debe responder a un plan ya previsto. Así, Jairo Alonso se muestra convencido de que la aceleración en los procesos de digitalización provocada por la Covid-19, ha comprometido la planificación necesaria en cualquier proyecto de digitalización. Es más, según este responsable, "en el mundo de la seguridad la falta de planificación acaba pasando factura a largo plazo, bien sea en forma de ataque, que no sería lo deseado, o bien obligando a las empresas a incrementar sus presupuestos para optimizar su seguridad".

> "La tecnología tiene que ser flexible. Tenemos que poder cambiarla cuando nos convenga. Por ello, tenemos que adoptar un enfoque de pago por uso, y para ello, debe darse un cambio de mentalidad"
>
> MARCO FRÜHAUF, VICEPRESIDENTE DE GRENKE

CIBERSEGURIDAD

Con una amalgama de empresas públicas y privadas, el de la Sanidad es un segmento especial, tanto por la necesidad de inmediatez en la respuesta como por la sensibilidad de los datos que manejan. ¿Son los retos en ciberseguridad los mismos para la sanidad pública y privada?

Independientemente de que sea público o privado, el sector sanitario tiene que ofrecer un servicio continuado. Por ello, Iván Mateos explica que "enseguida entiendes su forma de trabajar". Para el personal de IT, la ciberseguridad es importante, pero lo es más que un dispositivo no funcione o que falle una conexión entre máquinas. "Así, es necesario elevar el nivel de ciberseguridad, pero sin olvidar sus requisitos. Los fabricantes debemos poner ciberseguridad sin implicar dificultad, una vez que lo comprendes, el planteamiento coge buen rumbo".

Sobre esta necesidad de elevar la seguridad, Bernardo Gómez destaca que esta exigencia

es igual tanto en la sanidad pública como en la privada. La diferencia fundamental estriba en la velocidad con la que se adopta y adapta la tecnología, que sin duda es mucho más rápida en el sector privado. No obstante, no hay que olvidar que "la información es crítica, y cada vez hay más dispositivos conectados en el entorno sanitario, por lo que hay muchos riesgos a los que hacer frente".

Para Marco Frühauf la sanidad pública y la privada abordan sus retos de forma totalmente distinta. Así, "hay enormes diferencias en cuanto a la rapidez en la adopción de medidas o en la toma de decisiones, aunque las necesidades sean las mismas". Respecto a la financiación de la tecnología, el sector privado está mucho más abierto a nuevos métodos más alejados de las tradicionales. "Los retos y las posibilidades se entienden mejor y se pueden dar soluciones de un modo mucho más eficiente".

Por su parte, Jairo Alonso reconoce que además de ser un segmento esencial, gran parte de la sanidad, tanto pública como privada, se considera infraestructura crítica. "Esa significación conlleva que deben aplicarse medidas de seguridad más concretas y que apoyen y favorezcan en todo momento la prestación del servicio".

Ahora bien, ¿por qué hay tanta diferencia a la hora de afrontar un escenario de ciberseguridad?

Según Marco Frühauf este contraste se debe principalmente a que el sector público es mucho más complejo. "Hay que lidiar con distintas administraciones y organismos por lo que el proceso de toma de decisiones es mucho más largo y difícil, además de existir cierta opacidad a la hora de interpretar por dónde va la cosa".

En cuanto al ritmo de digitalización, ¿es de esperar que continúe en la misma línea tras la pandemia?

Sobre esta cuestión, Bernardo Gómez observa que esta nueva aproximación a la digitalización se mantendrá. "La situación actual puede repetirse, y hay que estar preparados". No obstante, el ritmo de inversión se ralentizará a medio plazo, porque las inversiones se han adelantado. "En un año hemos avanzado lo que en condiciones normales nos hubiese llevado entre tres y cinco".

Pese a estos avances, toca saber si el dato, está adecuadamente protegido.

El sector sanitario debe gestionar información muy sensible, que no es fácil de manejar, y que si se filtra o se pierde puede traer graves consecuencias. Por ello, Iván Mateos apunta a que es necesario buscar soluciones concretas: "El primer paso es identificar el riesgo, y luego querer abordarlo. Buscar una solución de seguridad concreta para ese problema es más sencillo".

Muy importante es también cumplir con las distintas normativas para la seguridad de la información. En este punto, Jairo Alonso afirma que a nivel TI, normas de seguridad como la ISO 27001 son seguidas ampliamente en el sector, "el problema viene cuando el sector se olvida de su parte industrial, de cumplir con normas como IEC 62443 que afectan a los dispositivos médicos y a sus redes.

"La seguridad como servicio puede suplir muchas carencias, pero la falta de conocimientos y experiencia de los usuarios no es uno de ellos. El factor humano suele ser casi siempre el eslabón débil de la cadena, por lo que es necesaria una capacitación en seguridad"

JAIRO ALONSO, ICS SECURITY CONSULTANT DE S21SEC

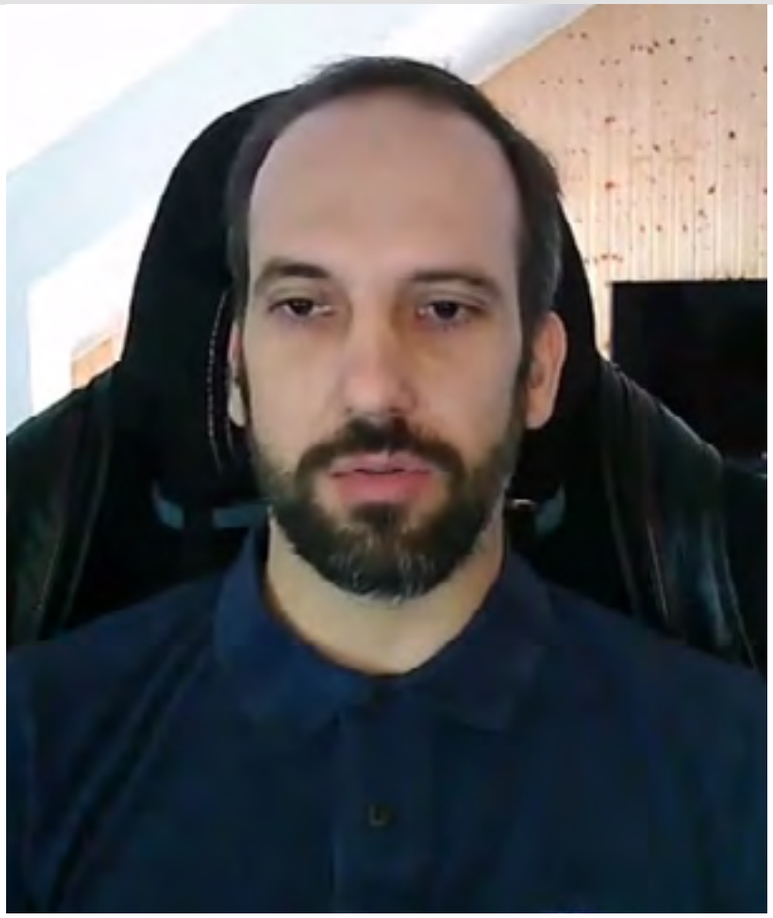
PRINCIPALES RETOS EN SANIDAD

La telemedicina ha llegado para quedarse, tanto en el sector público como privado, por lo que hay que adaptar las infraestructuras para ofrecer un servicio de calidad al usuario.

Así, según Bernardo Gómez es necesario poner los recursos para el personal sanitario en

“Para el personal de IT, la ciberseguridad es importante, pero lo es más aún que un dispositivo no funcione o que falle una conexión entre máquinas. Es necesario elevar el nivel de ciberseguridad, pero sin olvidar sus requisitos”

IVÁN MATEOS, INGENIERO PREVENTA DE SOPHOS



su dispositivo, dotar de conectividad a todo el equipamiento con el que cuentan los centros sanitarios, para que la información fluya libremente, además de garantizar su seguridad: “No solo preocupa que alguien pueda acceder a la información, sino también que pueda modificarla. Estos son los grandes retos”.

Por su parte, Marco Frühauf considera que “la inversión tiene que continuar”, pero es necesario que quienes controlan el dinero, los financieros, cambien su enfoque hacia uno centrado en el pago por uso. “La tecnología tiene que ser flexible. Tenemos que poder cambiarla cuando nos convenga. Por ello, tenemos que adoptar un enfoque de pago por uso, y para ello, debe darse un cambio de mentalidad, que en España está costando bastante”.

Según Iván Mateos, el principal desafío es que el sector sanitario pueda seguir avanzando tecnológicamente, sin incurrir en un riesgo para la seguridad. Una vez llevado este riesgo al mínimo exponente, se podrán ofrecer soluciones en todos los ámbitos: software, hardware y servicios. El reto por tanto pasa porque “tecnológicamente el servicio pueda crecer, que se pueda dar sin interrupción y que la ciberseguridad no sea un problema, para que los trabajadores puedan dedicarse a su trabajo”.

Asegurar una compartición segura de los datos para que los pacientes puedan ser atendidos en cualquier lugar o incluso en remoto y el médico pueda disponer de todo el historial clínico es el principal reto, según considera Jairo Alonso. “Tampoco debe ignorarse la seguridad de los dispositivos que monitorizan y controlan la salud de los pacientes, tanto los que pueden llevar en su propio cuerpo como los utilizados en quirófanos y UCI”.

TECNOLOGÍA Y SEGURIDAD COMO SERVICIO

¿Es el sector sanitario un buen escenario para el despliegue de tecnología como servicio?

Sobre este aspecto Bernardo Gómez reconoce que el sector privado está empezando a desplegar este modelo por su bajo impacto presupuestario y por la rápida evolución de las tecnologías, lo que permiten estar siempre actualizados. A la contra el sector público sigue anclado en el modelo presupuestario tradicional y se muestra más reticente a este tipo de inversiones. “Es una tendencia que acabará cambiando, pero queda tiempo para este cambio de mentalidad”.

En la misma línea, Marco Frühauf también reconoce el avance de la sanidad privada en este punto, sin embargo, valora que el cambio en el sector público tardará bastante tiempo

TECNOLOGÍA Y EDUCACION EN TIEMPOS DE CAMBIO

en producirse. “Con intereses y procesos que cambian, y atrapadas en concursos públicos y partidas presupuestarias ya fijadas, las administraciones públicas son presas de sus propios métodos y o te adaptas a ellos o no juegas. Al contrario que en la privada, es complicado cambiarles el paso”.

Para Iván Mateos ofrecer la tecnología como servicio es la respuesta, también en ciberseguridad. Ante la falta de capacidades tecnológicas y de expertise, la opción más adecuada es contratar un servicio que se dedique a vigilar la infraestructura, implementar soluciones de pago por uso, sencillas de utilizar y que no afecten a la operativa diaria. “Como fabricantes tenemos que facilitarles el trabajo, ofrecerles una tecnología sencilla, que le permita centrarse en su trabajo. Cuanta más tecnología se tiene, más eficiente se vuelve el sector sanitario”.

Por su parte, Jairo Alonso también señala que el sector sanitario es un buen escenario para el despliegue de seguridad como servicio, no obstante, considera que la falta de conocimientos y experiencia de los usuarios no es uno de ellos. “El factor humano suele ser casi siempre el eslabón débil de la cadena, por lo que es necesaria una capacitación en seguridad”. ■

MÁS INFORMACIÓN

Tecnología y Sanidad: mejora en la atención al paciente

Un mensaje para los responsables tecnológicos

Tras el empujón en inversión tecnológica vivido a lo largo del último año, es de esperar que todo esto siga mejorando de cara a maximizar los resultados. ¿Cómo puede lograrse? Sobre este hecho, “es importante aprovechar la inercia”, reflexiona Bernardo Gómez, “continuar invirtiendo en dos líneas críticas a nivel de infraestructura: la digitalización de los procesos de los centros hospitalarios, pero sin olvidar al paciente, a fin de darle capacidad de comunicación en los centros hospitalarios y en las residencias de mayores cuando se encuentre en ellos”.

Asimismo, Marco Frühauf también aboga por sacar partido de la experiencia, aprovechar todas las herramientas existentes para flexibilizar el modelo de gestión de las tecnologías para una mejor toma de decisiones. “Aprovechar la experiencia y el conocimiento para poder tomar las decisiones adecuadas y ser flexibles, manteniendo una inversión permanente”.

Dialogar, escuchar las necesidades de los responsables de tecnología y ciberseguridad es imprescindible para mantener esta tónica de implementación tecnológica, reconoce Iván Mateos. “A lo largo del último año se han visto los beneficios de implementar tecnología; ante un problema, se puede seguir trabajando e incluso la productividad se incrementa. Tanto técnicos como personal sanitario son igual de importantes para que el servicio no se detenga”.

Por último, Jairo Alonso concluye este bloque con un mensaje similar dirigido a las organizaciones de salud, “que no tengan miedo en contactar con empresas de seguridad. Estamos para ayudarles y podemos identificar sus necesidades principales a nivel de seguridad”.

GRENKE

FAST // FORWARD // FINANCE

¿TUS CLIENTES QUIEREN TU TECNOLOGÍA PERO NO TIENEN LA LIQUIDEZ PARA PAGARLA?

CONTACTA CON NOSOTROS

916305672

O CONTIGO@GRENKE.ES

Estar a la vanguardia tecnológica para ser más competitivo es una necesidad, pero en ocasiones resulta complicado sin que esto afecte a la liquidez de tu negocio.

Gracias al renting tecnológico y de equipamiento de GRENKE podrás ayudar a tus clientes a conseguirlo. Ellos pagan cómodas cuotas mensuales, en lugar de desembolsar el total, mientras tu cobras el 100 % de tu factura en 24 horas. ¡Así de fácil!

WWW.GRENKE.ES

JUAN DIZ, ASESOR SÉNIOR TIC SANIDAD

“Hemos visto que la sanidad va retrasada en la Transformación digital y eso conlleva escasa cartera de servicios digitales no presenciales”

La sanidad es un ecosistema de muy diversos actores y muy complejo y por tanto es difícil generalizar con sus profesionales, pero digamos que buscan una excelente usabilidad y movilidad de los sistemas de información

En su opinión, ¿qué carencias desde el punto de vista tecnológico ha destapado la situación de pandemia que estamos viviendo en las Infraestructuras sanitarias?

La obsolescencia de los actuales sistemas de información y la baja calidad del dato han quedado al descubierto con esta pandemia. Asimismo, hemos visto como la sanidad va retrasada en la Transformación digital y eso conlleva escasa cartera de servicios digitales no presenciales, lo que en casos como esta pandemia ha colapsado y retrasado toda la actividad no “covid” existente, impidiendo la accesibilidad y equidad del sistema.

Teniendo en cuenta la criticidad de la Infraestructura sanitaria, ¿qué ventajas aporta la tecnología a los profesionales del sector, tanto desde el punto de vista sanitario como de gestión?

Las tecnologías que subyacen en la Transformación Digital son claves para apuntalar la transformación de la sanidad a la medicina 5P. Los sistemas de “Big Data” son vitales para una medicina poblacional y predictiva, las aplicaciones móviles y portales web son esenciales para una sanidad participativa y preventiva y el “Deep learning” y la Inteligencia Artificial dan soporte a la medicina de precisión o personalizada.

¿Cuáles son las principales demandas tecnológicas de los profesionales del sector sanitario?

La sanidad es un ecosistema de muy diversos actores y muy complejo y por tanto es difícil generalizar con sus profesionales, pero digamos que buscan

“La Sanidad se tiene que transformar a una sociedad digital y eso requiere consensos que permitan cambiar las organizaciones, procesos y por último sistemas”

una excelente usabilidad y movilidad de los sistemas de información que realmente le descargue de tareas burocráticas y de sus procesos, así como que le asista en su actividad profesional de una manera “responsive” no intrusiva y que aprenda y se adapte a cada profesional y su contexto de manera dinámica e incremental

Poniendo en el centro la atención al paciente/usuario, ¿cuáles son las tecnologías más relevantes que impactan en esta atención?

Aquellas que le apoyen en su rol de medicina participativa mediante aplicaciones móviles, asistentes virtuales, portales de paciente y “wearables” sanitarios, los cuales deben aportar datos objetivos de los pacientes. Muchas veces los pacientes y los profesionales establecen una relación de manera verbal con indicación de percepciones que no ayudan a acotar los problemas de salud con eficiencia. Los datos recogidos y cuantificables (hábitos de sueño, actividad, pulsaciones durante las 24h, así como saturación de oxígeno pueden dar una dimensión objetiva de los problemas de salud y son además susceptibles de ser gestionados por sistemas de “machine learning” que descarguen al profesional de tareas de poco valor. La calidad y cantidad de los datos aportan mejor información y como ultimo mejoran el conocimiento de los ciudadanos y sus dolencias.

¿Hasta qué punto la Transformación Digital es una realidad en el entorno Sanitario? ¿Podemos diferenciar entre Sanidad Pública y Privada?

La Transformación Digital en este sector tiene que ser precedida de una Transformación de la Sanidad. La Sanidad se tiene que transformar a una sociedad digital y eso requiere consensos que permitan cambiar las organizaciones, procesos y, por último, sistemas.

La Sanidad en general va atrasada en esta transformación, si bien es cierto que hay tanto en el sector Público como Privado excepciones, pero en todo caso es un proceso muy complejo y lento.

¿Hacia dónde debe evolucionar la Sanidad y cuáles son los aspectos más críticos de mejora?

La sanidad debe y está evolucionando hacia las líneas estratégicas que indica la Sanidad 5P antes mencionada (Poblacional, Preventiva, Participativa, Preventiva y de Precisión/personalización) con el último objetivo de ser medida en base e a resultados de salud, a su valor aportado a la sociedad.

Sin embargo, en tecnología en sistemas de información en Sanidad existen elementos tan básicos por mejorar como la simple identidad única del paciente o la obsolescencia del puesto de trabajo, así como la capacitación digital de profesionales y pacientes, además de escasez de profesionales TIC con experiencia en Sanidad. No tenemos que olvidarnos que venimos de una escasez de financiación TIC en Sanidad que de manera crónica ha retrasado su evolución. Esperamos que los anunciados Fondos Europeos en sanidad transformen para bien un sector tan crítico y esencial como es la sanidad y que la pandemia ha subrayado. ■

Juan Diz, asesor sénior TIC Sanidad

Master en Dirección de Sistemas y Tecnologías de la Información y Comunicaciones de la Salud por la ENS Escuela Nacional de Sanidad del Instituto Carlos III, e ingeniero de Telecomunicaciones Universidad Politécnica de Madrid. Más de 32 años de experiencia en empresas de equipamiento médico de alta tecnología médica, empresas de soluciones digitales de Imagen Medica, así como consultoras TIC de Sanidad.

Las redes de atención sanitaria obtienen más beneficios de una solución de infraestructura llave en mano

COMMSCOPE®
RUCKUS®

Internet de las cosas (IoT) está revolucionando innumerables sectores de la industria, permitiendo una automatización más avanzada y un mayor control de todo tipo de aplicaciones IT y OT. Estas incluyen iluminación, sistemas de seguridad y climatización (HVAC). Si bien casi todas las industrias pueden beneficiarse del IoT, la atención sanitaria ofrece un conjunto particularmente diverso de casos de uso.

Aunque esto supone un futuro apasionante para la evolución de las redes de atención sanitaria, también introduce un considerable nivel de complejidad que puede impedir que una organización médica aproveche plenamente la eficiencia operativa, la mejora de la seguridad y la ampliación de las capacidades que posibilita el IoT, o como se suele denominar en el contexto de las redes sanitarias, el Internet de las cosas médicas (IoMT).

IOMT APORTA UNA ENORME DIVERSIDAD DE APLICACIONES

Pocos espacios comerciales pueden siquiera acercarse al tipo de necesidades de procesamiento de datos de una moderna institución sanitaria u hospital. El movimiento fiable y rápido de información es de misión crítica, la seguridad física y de los datos debe cumplir con estrictos estándares regulatorios, el personal y los pacientes ampliamente distribuidos requieren una conectividad de gran alcance, y tanto el inventario como los equipos deben ser minuciosamente gestionados de forma cercana.

Algunos ejemplos específicos de los dispositivos que responden a estas necesidades son:

- Cámaras y sensores de seguridad conectados por IP en todas las instalaciones
- Señalización digital para dirigir a pacientes y visitantes a sus destinos
- Sistemas de gestión de alerta de cama y desplazamientos que mantienen a los pacientes seguros

“Dado que las instalaciones médicas y sus áreas estériles son lugares difíciles para instalar la infraestructura de red, una solución sencilla y llave en mano puede contribuir a que su inversión en red tenga un retorno de la inversión positivo más pronto”

❖ Acceso a la información y entretenimiento en la habitación a través de la red

❖ Botones de llamada del paciente y alarmas de pánico para garantizar que la ayuda llegue rápidamente

❖ Gestión de inventario mediante RFID o Tags activos WiFi para asegurar que las existencias sean adecuadas y que las auditorías sean sencillas

❖ Automatización de edificios con la integración de las cerraduras de las puertas de acceso con tarjetas, via WiFi, Zigbee y BLE

❖ Software de gestión automatizada de infraestructuras (AIM) que supervisa y protege todas las conexiones de red en tiempo real, automatiza las alarmas y administra toda la documentación de la red en tiempo real para asegurar los datos y garantizar la privacidad de los pacientes

Mirando todas estas funciones, aplicaciones y servicios, parece una tarea casi imposible integrar tantos tipos diferentes de conectividad en una sola infraestructura de red. Sin embargo, eso es exactamente lo que CommScope ofrece a las redes de salud de todo el mundo.

Una infraestructura de red llave en mano que es simple, fiable y adaptable

Con tantas piezas móviles, una red que permita el IoMT no puede permitirse ser una solución fragmentada. Unir un mosaico de tecnologías de infraestructura no solo degrada el rendimiento general, sino que también aumenta el tiempo y los problemas de instalación. Dado que las instalaciones médicas y sus áreas estériles son lugares difíciles para instalar la infraestructura de red (abrir techos y paredes a menudo requiere cerrar partes necesarias y rentables de las instalaciones), una solución sencilla y llave en mano puede contribuir a que su inversión en red tenga un retorno de la inversión positivo más pronto. ■

La comunicación como puntal para la telemedicina

El sector sanitario, sobre todo en lo que tiene que ver con tecnología, ha vivido una catarsis a lo largo del último año. A este respecto, Bernardo Gómez, territory account manager Iberia de CommScope, considera que las agendas tecnológicas sobre digitalización que tanto la sanidad pública como privada tenían concretadas se han acelerado, permitiendo que en poco tiempo se haya avanzado lo que en circunstancias normales habría llevado cuatro o cinco años. Sin duda la tecnología aplicada al sector sanitario ha acelerado este proceso de adopción.

Ahora bien, pese a este paso de gigante en cuanto a adopción de tecnologías, lo cierto es que el sector sanitario tiene por delante aún muchos retos, desafíos que bien encarados, gracias al apoyo de empresas especializadas, pueden suponer no desandar lo ya andado.

Sobre estos retos, Bernardo Gómez reconoce que el principal es que ha cambiado el modelo de negocio de la sanidad. Cada vez surgen nuevas aplicaciones en el entorno sanitario, como la telemedicina, que está muy ligada a la infraestructura de comunicaciones y es precisamente ahí donde CommScope puede aportar valor al sector sanitario, tanto en la parte de infraestructura con redes de cableado y fibra, para toda la parte de comunicaciones de los centros sanitarios; como en lo que concierne a la infraestructura activa con la conectividad inalámbrica y las redes LAN, requisitos indispensables para poder ofrecer un servicio de telemedicina de forma adecuada.

Asimismo, Gómez razona que para desarrollar este modelo de telemedicina es ineludible interconectar todos los centros de toma de decisiones con los puntos donde se genera la información. Esto en el entorno sanitario es crítico porque hay que conectar un ecógrafo o un equipo de radio diagnóstico con un médico que trabaja desde su casa dando tele asistencia a sus pacientes. Es decir, la información generada en diferentes sistemas tiene que fluir de una manera eficiente y de manera segura. Por tanto, es crítico dotar de infraestructuras de comunicaciones robustas y seguras a los centros sanitarios para poder trabajar en este nuevo modelo de servicio.

VALOR DIFERENCIAL

Cuando se plantea una estrategia de comunicación, un director de IT de un centro sanitario tiene que pensar tanto en la conectividad de las personas como en la conectividad de las cosas. Son las dos líneas de actuación críticas, y que permitirán que un médico pueda acceder a toda la información relevante de un paciente.

Para ayudar a las organizaciones del sector sanitario a dar este paso, desde CommScope consideran que estas entidades deben realizar una actualización de sus redes de comunicación empresariales, evolucionando desde una arquitectura tradicional de un punto de acceso inalámbrico, o punto de acceso WiFi, hacia un modelo de nodos de comunicaciones convergentes. En estos nodos de comunicaciones no solo se va a poder dar conectividad WiFi al usuario, a un dispositivo concreto, sino que también va a ser posible adoptar nuevas tecnologías sobre todo del espectro de IoT dentro de esta propia infraestructura.

Gracias a esta correlación, las organizaciones podrán reforzar sus redes LAN para convertirlas en redes multiservicio, dada la convergencia hacia el mundo IT, principalmente hacia el mundo IoT.

Tecnología para una sanidad más eficiente

JUAN CARLOS FARIÑAS, Área Manager de GRENKE España

La pandemia de Covid-19 ha dejado lecciones muy valiosas para el futuro de la sociedad. Una de ellas es la importancia de la tecnología como una herramienta necesaria para la gestión del sistema sanitario. En España, la Sanidad ha visto cómo los avances en materia tecnológica se han convertido en sus mejores aliados durante los meses más virulentos del coronavirus.

Desde las video llamadas, que consiguieron conectar a familiares con enfermos aislados, hasta la telemedicina, una forma de recibir prescripción médica que algunas comunidades autónomas ya han implantado en sus sistemas sanitarios.

La pandemia ha acelerado la puesta al día de la Sanidad con una revolución tecnológica de la que se había quedado descolgada, si la comparamos con otros sectores donde las soluciones y herramientas IT están a la orden del día.

De esta manera, empresas e instituciones sanitarias han visto la necesidad de utilizar esta vanguardia tecnológica para ofrecer una mejor atención al paciente y mejorar el trabajo del profesional.

Conseguir la implementación de los avances tecnológicos en la sanidad es la función de empresas como GRENKE, donde lo que aportamos se traduce en agilizar el trabajo de los sanitarios al favorecer y mejorar el seguimiento de los pacientes con herramientas que pueden evitar que tengan que acudir en repetidas ocasiones a los centros de salud.

Así, ciencia y tecnología se conjugan al cuidado de la salud para el diagnóstico, vigilancia y tratamiento de diversas enfermedades.

“La tecnología sanitaria es, en la actualidad, un instrumento esencial en la asistencia sanitaria, ya que consigue aliviar el dolor, las lesiones y la discapacidad de los pacientes, al tiempo que mejora la eficacia de las prestaciones sanitarias”

Gracias a ella, se obtienen diagnósticos precoces y más certeros, tratamientos menos invasivos y se reduce el tiempo de hospitalización y de rehabilitación, mejorando así la calidad de la atención sanitaria y aumentando la esperanza de vida de los pacientes.

La tecnología sanitaria es, en la actualidad, un instrumento esencial en la asistencia sanitaria, ya que consigue aliviar el dolor, las lesiones y la discapacidad de los pacientes, al tiempo que mejora la eficacia de las prestaciones sanitarias.

Beneficia a miles de millones de personas en todo el mundo, no solo en los hospitales, sino también en residencias y en el propio hogar. Forman parte de ella desde material desechable, como agujas o test de embarazo, hasta sofisticados equipos de diagnóstico, glucómetros, desfibriladores, robots quirúrgicos menos invasivos, máscaras de oxígeno, marcapasos, y un largo etcétera.

El futuro ya está aquí con los avances en tecnología sanitaria centrados en la robótica aplicada a la atención médica, la biotecnología, la telemedicina, los chatbots entre médico y paciente o las aplicaciones móviles orientadas a la salud, entre otros.

TECNOLOGÍA MÉDICA ACCESIBLE

Así y todo, el talón de Aquiles de toda esta revolución tecnológica viene siendo su financiación. No obstante, y al mismo tiempo, la inversión en nuevas tecnologías es fundamental para mantener el ritmo del progreso de las ciencias médicas modernas y para afrontar los retos que se ciernen sobre el sector. Los hospitales, centros clínicos y farmacias experimentan la presión de mejorar la experiencia de los pacientes en lo que se refiere al tratamiento, el diagnóstico, la atención y la comunicación.

Desde GRENKE aportamos soluciones que permiten un acceso a la tecnología de forma asequible y sin castigar su cuenta de resultados; y a sus pacientes disfrutar de lo último en tecnología sanitaria.

La apuesta es sencilla: un amplio portfolio de alternativas a la financiación tradicional de equipos médicos. Hay distintas soluciones de arrendamiento disponibles, y cada una de ellas se puede estructurar de forma diferente para ajustarse a necesidades concretas, ya sea en términos de presupuesto o de uso previsto. El arrendamiento ayuda a garantizar un acceso a las mejores y más recientes tecnologías sanitarias sin necesidad de una inversión sustancial por adelantado.

Y ya hay soluciones reales que van más allá del simple arrendamiento y que cubren toda la gestión del ciclo de vida de los equipos. Algunas de ellas pueden ser el pago por escaneo, los servicios de equipos gestionados y el mantenimiento inclusivo. Un aspecto crucial es que estas soluciones se ocupan del activo al final de su vida útil, de modo que los métodos de reciclaje y eliminación segura no son responsabilidad del cliente.

Al final de lo que se trata es de brindar el acceso a la tecnología repartiendo los costes y el presupuesto con más eficacia. ■

Financiación flexible al servicio de la sanidad

Tecnología y sanidad van de la mano. Sin embargo, en ocasiones el acceso a la tecnología puede ser un proceso complicado bien por la inversión que conlleva o porque el proceso de gestión se torne farragoso. Para ayudar a las empresas sanitarias en su digitalización, existen soluciones financieras flexibles capaces de adaptarse a las distintas necesidades que presentan estas organizaciones. Marco Frühauf, vicepresidente de Grenke, aborda estas alternativas y explica cómo han ido ganando en importancia a lo largo de estos últimos meses.

Desde el inicio de la pandemia, el modo de adquirir tecnología ha ido cambiando. Durante una primera fase el sector sanitario, como tantos otros, se lanzó a adquirir equipamiento tecnológico para dar respuesta a las nuevas necesidades que iban surgiendo a causa del confinamiento, para después, tras unos meses de grandes inversiones, volver a un periodo de mayor moderación. Se ha pasado por tanto de un escenario de prisas y desorganización, de compra y financiación sin análisis previo de las necesidades reales, a otro de mayor mesura y examen, avanzando ya lo que podría ocurrir después del confinamiento.

A este respecto, Marco Frühauf reconoce que ha sido una época de grandes cambios para las empresas del sector sanitario, pero también para compañías como la suya, dedicadas al renting tecnológico, y que han tenido que adaptar sus sistemas y modelo de negocio a cada nueva situación surgida.

En este punto, y teniendo en cuenta, además, que la solvencia de las empresas se ha ido debilitando a causa de las grandes inversiones iniciales, desde Grenke se aboga por que las organizaciones del sector sanitario avancen hacia nuevas fórmulas de financiación que les permitan superar estos y otros escollos que les afectan de cara a adquirir tecnología. En este contexto, los principales desafíos a los que tienen que hacer frente estos actores tienen que ver con su necesidad de hacer inversiones y su incapacidad para realizarlas con las herramientas que normalmente utilizan; una financiación tradicional.

Por eso, Marco Frühauf expone la importancia de que estos agentes, no solo grandes hospitales, comunidades autónomas, sanidad pública, sino también sanidad privada, doctores o farmacéuticos conozcan nuevos métodos de financiación con los que invertir en tecnología y adaptar sus negocios a la situación actual, como puede ser el pago por uso, que permite disponer del uso de tecnología y bienes de equipo sin aumentar el endeudamiento de la empresa.

PAGO POR USO COMO SOLUCIÓN

Ahora bien, ¿es esta situación de pago por uso igual cuando se habla de grandes clientes, pequeños clientes, sector público, privado…?

Por su dimensión, se trata de realidades muy distintas, ya que, por ejemplo, mientras una pequeña farmacia tiene que subsistir con la tesorería que genera, un gran hospital, ya sea público o privado, cuenta con un importante respaldo económico.

No hay que olvidar que el sector sanitario es muy tradicional en cuanto a la gestión y manejo de los fondos y los recursos económicos. Esto le da una gran dependencia de la financiación tradicional, que está en manos de bancos, ya sean comerciales o especializados.

No obstante, toda la banca tradicional está ahora exigiendo un nivel de solvencia o unos requerimientos para ofrecer financiación muy altos, también sobre la documentación a aportar. Por ello, y cuando se trata de operaciones más sencillas, con una menor cuantía para hacer la inversión, el cierre de la operación puede depender más de cómo se gestione la documentación de la financiación que de la propia decisión del dueño del pequeño negocio y del fabricante de hacer la instalación. De este modo, y en un sector en el que se exige que todo sea rápido y sencillo, Gerke apuesta por simplificar este proceso. Realizar una gestión en minutos, sin un solo papel y de forma digital.

Ciberseguridad y funcionalidad, el futuro de los entornos OT

JAIRO ALONSO, ICS Security Consultant, S21sec

Desde la pandemia, el sector sanitario ha cobrado más relevancia que nunca y ha experimentado un rápido proceso de transformación digital. Sin embargo, esto ha provocado que el sector se exponga a importantes riesgos de ciberseguridad, cuya solución requiere de una mayor colaboración entre las empresas de ciberseguridad y el sector sanitario, en especial, los fabricantes de dispositivos médicos. La evolución tecnológica ha ayudado a los hospitales y al personal sanitario a proporcionar una mejor atención a los pacientes, pero la situación de emergencia ha provocado también que se pasen por alto ciertos protocolos de ciberseguridad necesarios en el sector sanitario. Esto no solo supone un riesgo para los trabajadores de los hospitales, sino que también puede repercutir en la salud de los pacientes.

Es comprensible que los fabricantes quieran presentar sus productos al mercado lo antes posible para llevar ventaja con respecto a la competencia, pero, en ocasiones, esa urgencia hace que se salten el primer paso de trabajar conjuntamente con las empresas de seguridad ya que, en un inicio, ahorran tiempo y costes. Aun así, sus productos quedan expuestos innecesariamente a riesgos de ciberseguridad. Además, tampoco suele tenerse en cuenta que al aplicar la seguridad más adelante, dichos dispositivos requerirán de recertificaciones, cuyos procesos suelen ser todavía más lentos y costosos. Es cierto que existen limitaciones a la hora de aplicar ciertas medidas de seguridad en este

“Una de las tácticas más eficaces para prevenir ciberataques es la formación. Es fundamental promover la concienciación entre el personal sanitario acerca de los riesgos informáticos a los que se expone el sector”

tipo de dispositivos, dado que podrían afectar a su funcionalidad. No obstante, este riesgo se puede solventar integrando la ciberseguridad desde la etapa más temprana: su diseño.

La seguridad de los dispositivos médicos es de vital importancia, y la única forma de garantizarla es haciendo que los fabricantes y las empresas de ciberseguridad trabajen de manera conjunta desde un primer momento, para así evitar costes adicionales y otros problemas más graves, como pueden ser los ciberataques. De hecho, desde S21sec hemos tenido constancia de varios ataques de ransomware dirigidos al sector sanitario que implicaban el secuestro de equipos o cifrado de datos, y ha sido una de las razones por las que la ciberseguridad se ha convertido ahora en una preocupación global para los profesionales del sector.

El aumento de la conectividad entre dispositivos, el uso de tecnologías estándar y la acelerada digitalización de los sistemas de automatización, ha provocado que muchos sectores queden expuestos a riesgos de ciberseguridad. En este caso, los ciberataques son una amenaza todavía mayor para el sector de la atención sanitaria, ya que un ataque que interrumpa cualquier actividad puede suponer una cuestión de vida o muerte. Por ello, desde S21sec consideramos que el sector sanitario debe implantar determinadas estrategias con el objetivo de protegerse.

Para empezar, una de las estrategias más eficaces a adoptar es el modelo de ciberseguridad de confianza cero o Zero Trust. En los entornos OT, es básico separar las comunicaciones propias de Internet de la red IP corporativa y de los dispositivos médicos. El enfoque de confianza cero también recomienda y se basa en implementar controles en el tráfico de la red con el fin de evitar y contener ataques de usuarios que aprovechan estas vulnerabilidades para, en el mejor de los casos, hacerse con información personal y confidencial de salud.

Es crucial que el sector sepa cómo protegerse de los ataques de ransomware ya que, como he mencionado anteriormente, desde S21sec hemos detectado varios ataques a centros hospitalarios, infectando sus equipos informáticos y extrayendo información confidencial para posteriormente reclamar un rescate económico. En este sentido, los empleados deben saber qué acciones suyas pueden poner en riesgo la ciberseguridad de la infraestructura y, en última instancia, facilitar una brecha que los atacantes aprovechen para desplegar un ramsomware.

Es por ello, que una de las tácticas más eficaces para prevenir ciberataques es la formación. Es fundamental promover la concienciación entre el personal sanitario acerca de los riesgos informáticos a los que se expone el sector, como estafas en materia de ciberseguridad o tácticas de phishing. Es alarmante que exista tal desinformación en este aspecto, pues la realidad es que hay vidas que dependen de un dispositivo médico, ya sea en su hogar, o en el propio hospital. Ya que es complicado superar la escasez de perfiles cualificados en seguridad, es importante formar al personal y además, confiar en empresas de ciberseguridad que puedan proporcionar respuestas de incidentes desde un SOC-OT.

En definitiva, además de apostar por la formación en ciberseguridad en entornos sanitarios, los fabricantes de los dispositivos médicos y las empresas de seguridad deberían trabajar conjuntamente para diseñar dispositivos óptimos, velando por la seguridad de los pacientes y empleados de los centros sanitarios. En S21sec contemplamos un futuro cercano donde será posible lograr este objetivo que podrá reducir tiempo y costes y, lo más importante, priorizar la seguridad, ante todo. ■

Seguridad y concienciación para evitar ataques

Tres son los retos que tiene el sector sanitario en estos momentos: asegurar la confidencialidad de los datos, proteger la red de comunicaciones y salvaguardar los dispositivos de salud. Para afrontarlos, se debe establecer una estrategia basada en la seguridad de esos activos, pero sin descuidar la formación de las personas.

El sector sanitario se ha alzado como uno de los principales objetivos de los ataques cibernéticos, incrementándose el número de ofensivas alarmantemente. Por este motivo, Jairo Alonso, consultor de sistemas de control industrial de S21sec, explica qué acciones son necesarias para proteger datos y recursos adecuadamente, además de ofrecer otra serie de recomendaciones de seguridad a llevar a cabo.

Efectivamente, por las actuales circunstancias, el sector sanitario se enfrenta a tres retos principales: asegurar la confidencialidad de las historias médicas, proteger su propia red corporativa de comunicaciones, y salvaguardar los dispositivos de salud destinados a monitorizar las constantes vitales de los pacientes cuando están ingresados en un centro médico.

La historia médica no deja de ser información que debe resguardarse ya que se trata de datos críticos que pueden determinar en muchos casos acciones respecto a una persona.

En base a ello, se hace imperativo que esa información no quede alojada en cualquier servidor, sino en servidores internos corporativos. Los datos tampoco deben estar publicados en Internet, ni ser accesibles desde el exterior, y cuando sea necesario realizar un intercambio de información, por un tema de pacientes o similar, utilizar siempre canales seguros. Asimismo, y siempre que sea posible, es recomendable utilizar redes propias, y no recurrir a servicios de terceros que puedan poner en riesgo la información de los pacientes.

No obstante, y pese a seguir estas recomendaciones los datos pueden enfrentarse a amenazas que, como el ransomware, están golpeando con fuerza desde hace meses al sector sanitario.

Como medidas de seguridad y de protección ante este tipo de amenaza, Jairo Alonso recomienda, como primer punto, la formación, a fin de que las personas sean capaces de identificar por dónde puede entrar un ataque de ransomware y

notificar cada vez que detectan una brecha. También es muy importante disponer de herramientas de monitorización de la red del sistema sanitario en general, para que al menor indicio de una posible brecha de seguridad o de un ataque, se tenga constancia, y pueda contenerse. El objetivo es evitar por todos los medios que el ransomware se expanda a otros servicios y que los ciberatacantes consigan cifrar historias clínicas de pacientes, lo que impediría tratar adecuadamente a estos usuarios. Además de acciones para luchar contra el ransomware, Jairo Alonso ofrece tres recomendaciones de seguridad a llevar a cabo.

La primera de tiene que ver con la separación o aislamiento de diferentes componentes que integran la infraestructura tecnológica, como son la red que da servicio a los dispositivos de monitorización de salud, la red en la que se incluyen las herramientas de trabajo habituales del sector (correo electrónico, páginas web, etc.), y las historias clínicas y su acceso. Adicionalmente, es muy importante crear políticas y procedimientos que permitan asegurar y elevar el nivel de seguridad sanitario, imponiendo medidas que impliquen mejoras de dispositivos o adquisición de nuevos elementos de seguridad, entre otros.

El último es la concienciación. Es fundamental que todo el personal, esté muy concienciado y comprenda de dónde puede venir un ataque, y qué medidas se pueden tomar para prevenirlo y que no se produzca.

Ciberseguridad en el sector sanitario en pandemia

IVAN MATEOS, Ingeniero Preventa, Sophos

El sector de la salud es hoy muy vulnerable. En medio de una de las peores crisis sanitarias que ha golpeado a la sociedad moderna, los ciberatacantes están explotando hechos como el aumento del teletrabajo, que en muchos casos se ha iniciado con poca o ninguna experiencia y planificación previa, miedo y ansiedad, y una fuerza laboral médica con exceso de trabajo.

El fallo de los sistemas de atención médica puede tener consecuencias nefastas: problemas en ordenar medicamentos, perder el historial médico de un paciente, programar operaciones o hacer que las ambulancias no estén disponibles a tiempo durante las emergencias. Por otro lado, los ciberdelincuentes aprovechan cada vez más la mayor dependencia de la atención médica de herramientas y dispositivos digitales. Se han aprovechado de esta crisis global lanzando ciberataques a través de correos electrónicos de phishing con temas relacionados con la pandemia, ataques de ransomware spear-phishing, que paralizan la atención médica y comprometiendo emails empresariales.

Además, para adaptarse al número de infecciones en rápido aumento y para respaldar la infraestructura de atención médica existente, muchos países han tenido que crear instalaciones médicas temporales para albergar a los pacientes infectados por COVID-19 o para atender los turnos de vacunación. Dado que estas instalaciones se crean rápidamente y la prioridad es brindar atención al paciente, la seguridad se convierte en una prioridad menor, y se pasan por alto muchos pasos cruciales para proteger las redes y los dispositivos y la información que estos manejan

Un resultado de la pandemia también ha sido el aumento significativo en la cantidad de datos de salud de los pacientes almacenados por el gobierno y las organizaciones de salud. Los datos personales como los parámetros de salud diarios, el estado de salud comórbido, los proveedores de seguros, así como el seguimiento de todos aquellos que entran en contacto con una persona infectada, pueden explotarse para el robo de identidad y venderse por un alto valor en la dark web.

Para que las organizaciones de salud ganen terreno a las ciberamenazas modernas, deben seguir ciertas estrategias clave de seguridad para protegerse correctamente contra posibles ciberataques. A continuación, damos cinco consejos de seguridad para intentar conseguirlo:

1. ADOPTAR EL MODELO DE SEGURIDAD DE CONFIANZA CERO O ZERO TRUST

Un informe reciente muestra que en el sector sanitario hay más infracciones causadas por amenazas internas que externas. Esto puede atribuirse a un error humano, a la falta de supervisión en ciberseguridad o al abuso intencionado del privilegio de acceso a datos y sistemas confidenciales.

Al implementar un enfoque de confianza cero, las organizaciones de salud pueden introducir controles granulares en el tráfico de la red. Esto limita la oportunidad de que los atacantes y los usuarios deshonestos obtengan acceso a información personal confidencial de salud (PHI) mientras permanecen bajo el radar.

2. MEJORAR LA CIBERSEGURIDAD CONTRA LOS ATAQUES DE RANSOMWARE

El ransomware es un arma devastadora en manos de los ciberdelincuentes que tienen como objetivo el sector sanitario, y es responsable de más del 70% de los brotes de malware en el sector.

Estos ataques han detenido operaciones sanitarias, han paralizado los dispositivos y sistemas médicos conectados y han cifrado los registros sanitarios para que los sanitarios no puedan acceder a ellos.

Sophos no sólo ofrece una seguridad líder en ransomware, sino que también realiza un seguimiento del desarrollo de ransomware mediante una rigurosa investigación de SophosLabs. Sophos Intercept X con EDR y Sophos XG Firewall trabajan conjuntamente para interrumpir y rechazar los ataques avanzados de ransomware.

3. SUPERAR LA ESCASEZ DE PERSONAL CUALIFICADO

La falta de personal contratado con los conocimientos y la experiencia adecuados en materia de ciberseguridad es uno de los principales desafíos para los proveedores de servicios de salud. Esto es especialmente un dolor de cabeza para aquellos que no tienen un experto en seguridad a tiempo completo.

Para las organizaciones sanitarias que carecen de recursos en ciberseguridad, Sophos ofrece el servicio de Managed Threat Response (MTR). Este servicio ofrece una supervisión eficaz y una evaluación continua de los riesgos, así como un equipo de expertos dedicado las 24 horas del día, los 7 días de la semana a mitigar y resolver cualquier ataque.

> "Para que las organizaciones de salud ganen terreno a las ciberamenazas modernas, deben seguir ciertas estrategias clave de seguridad para protegerse correctamente contra posibles ciberataques"

Nuestra solución va más allá de las simples alertas, ya que proporciona una respuesta a incidentes reales contra las amenazas, asegurando que el riesgo se identifica, se contiene y que se toman medidas correctivas de inmediato.

4. CUBRIR LOS PUNTOS CIEGOS EN SUS ESFUERZOS DE TRANSFORMACIÓN DIGITAL

Las transacciones de información entre los pacientes, los cuidadores, aseguradoras y otras partes interesadas deben ser fluidas pero tambien seguras.

Es crucial proporcionar un acceso fiable y seguro a los datos clasificados de la asistencia sanitaria en un momento en que muchos hospitales están adoptando nuevas tecnologías como los dispositivos médicos conectados a la red, la telesalud y aplicaciones médicas como los sistemas de comunicación y archivo de imágenes (PACS).

Sophos, con sus últimos dispositivos XG Firewall y SD-RED, hace posible conseguir una conectividad en línea con sus objetivos de seguridad y continuidad. Se permite no solamente enrutar tráfico a nivel de aplicación o usuario sino también aprovechar todas las ventajas de la seguridad sincronizada de Sophos en entornos SD-WAN

5. PROMOVER LA CONCIENCIACIÓN EN CIBERSEGURIDAD

Otra preocupación importante para el sector sanitario es la falta de formación sobre ciberseguridad y la escasa conciencia sobre la privacidad de los datos entre los empleados.

Las organizaciones de atención sanitaria deberían realizar campañas periódicas de sensibilización para que sus empleados, socios y proveedores sean más conscientes de las últimas estafas y de las tácticas de phishing, y así estar mejor preparados para tomar las medidas adecuadas cuando se encuentren con malware o phishing.

Con Sophos Phish Threat, los equipos de seguridad informática pueden simular ataques de phishing con sólo unos pocos clics, y proporcionar formación rapida,automatizada e in situ a los empleados de atención sanitaria según sea necesario. ■

Mantener el servicio activo protegiendo la información

Los ciberataques contra el sector sanitario se han multiplicado en el último año, y este sector se enfrenta al reto de proteger sus activos. Abordando esta realidad, Iván Mateos, Sales Engineer de Sophos, explica por qué el sector socio sanitario está recibiendo más ataques que ninguna otra industria, y ofrece las claves para mantener la actividad diaria sin alteraciones mientras se aseguran todos los activos.

Efectivamente, por las actuales circunstancias, el sector sanitario, no solo hospitales sino también los laboratorios o las farmacéuticas, se ha convertido en una realidad muy visible, hecho que no pasa desapercibido para los ciberatacantes.

En este sentido, Iván Mateos considera que además de lanzar su artillería en modo de ciberataques contra organizaciones, también lo han hecho contra los usuarios, que a diario reciben emails de phishing, con la excusa de una vacuna o de cualquier otro tema sanitario.

Por tanto, y para frenar esta incertidumbre, el sector sanitario tiene que poner remedio, y afrontar algunos retos, siendo el principal el de mantener el servicio lo más activo y productivo posible, pero sin olvidar que lo que manejan y gestionan es información muy sensible: los datos de los usuarios o de los pacientes. De este modo, esta digitalización que está acometiendo el sector sanitario para mejorar la infraestructura debe ir acompañada innegablemente de ciberseguridad, que debe ser tomada como un valor elemental.

DISPOSITIVOS IOT

Importante es también custodiar los dispositivos que manejan datos sensibles, como los dispositivos IoT, que pueden recolectar cantidades significativas de información sobre sus usuarios y su entorno. Por ello, es imperativo minimizar los riesgos de sufrir un incidente de seguridad, protegiendo tanto el dispositivo como la información que gestiona. A este respecto, es necesario salvaguardar la conexión a la red de estos dispositivos, limitar su acceso, (el qué y quién puede acceder a qué).

Hoy en día, en el mercado, ya existen soluciones de segmentación de red, firewalls, y dispositivos de protección que ya tienen en cuenta los equipos de IoT, por lo que es perfectamente compatible la integración de este tipo de dispositivos con la parte de ciberseguridad.

Por último, Iván Mateos lanza también unas cuantas recomendaciones para que los responsables de IT mantengan la seguridad a raya. Entre ellas destaca la importancia de no alargar la vida de equipos que están fuera de soporte, aplicaciones antiguas, sistemas operativos obsoletos. En este sentido reconoce que, aunque es difícil el cambio, hay que entender que estos son problemas de seguridad. Por tanto, hay que intentar mantener aplicativos y sistemas lo más actualizados posibles, optar por soluciones de ciberseguridad que permitan un manejo sencillo, como es el caso de Sophos, que cuenta con una consola para todos los productos, lo que simplifica la ecuación.

Adicionalmente, y para mejorar esta seguridad, Mateos sugiere aplicar el concepto de las tres Cs: cifrado de los dispositivos, con el objetivo de que si se pierde un dispositivo que no se pierda la información; cambio de contraseñas; y, por supuesto, concienciación, con recursos didácticos y de entrenamiento. Si se consigue eso, si se acompañan las herramientas de nueva generación con concienciación, todo puede ser mucho más efectivo.

S21 SEC

CIBERSEGURIDAD INDUSTRIAL

Servicios enfocados a una gestión eficiente de los riesgos de ciberseguridad industrial.

Conoce tus sistemas de automatización y control mejor que el enemigo.

Ahuyenta a potenciales atacantes de tus instalaciones industriales.

Vigila a tu enemigo en los procesos industriales.

Lucha contra el enemigo de tus instalaciones industriales.

Para más información puedes visitar www.s21sec.com/es/ciberseguridad-en-el-sector-industrial/ o escribir un correo a marketing@s21sec.com

Los cuidados sanitarios deben dejar atrás las redes heredadas

Nadie duda de que en plena pandemia es más complicado planificar una actualización tecnológica de amplio espectro en la red de su organización de cuidados sanitarios. Sin embargo, de algún modo, el estrés experimentado por los proveedores de cuidados sanitarios hace que ahora sea el momento perfecto para observar cómo funciona la red desde un nuevo ángulo y determinar qué nuevas e inteligentes posibilidades surgen a raíz de la pandemia

Si hay algo que hemos aprendido todos desde comienzos de 2020 es que la adaptabilidad y la flexibilidad de las redes es incluso más importante de lo que se creía antes. Las redes de atención sanitaria a menudo se ven limitadas por sistemas antiguos ineficaces y aislados que resultan difíciles de mejorar y, algunas veces, imposibles de integrar. Ahora que las normas de atención sanitaria han cambiado radicalmente, estos límites resultan más costosos e insostenibles. Si la eficacia operativa se ve mermada, también se resiente el estado operativo de su organización.

LOS RETOS DEL FUTURO Y LOS QUE YA ESTÁN AQUÍ

El rápido cambio realizado para adoptar interacciones de telemedicina, los servicios digitales de hospitalización y la conexión al Internet de las Cosas Médicas (IoMT) crean nuevos requisitos para la red y su infraestructura.

Para seguir el ritmo y abordar la necesidad de disponer de redes fiables, adaptables y seguras, la actualización de la red es la única opción que permite la forma de suministrar atención médica al paciente. Al mismo tiempo, los elevados costes asociados a la actualización pueden resultar abrumadores y los proveedores de servicios sanitarios deben sopesar las opciones de soluciones con sus necesidades. La inversión debe estar justificada por la duración de la solución, y dicha duración puede determinarse en función de lo sólida y adaptableque sea.

OPORTUNIDADES DISPONIBLES CON LA INFRAESTRUCTURA DE RED ACTUALIZADA

Una red preparada para el futuro es algo más que una infraestructura física más rá-

pida. Supone analizar las estrategias y las soluciones para mejorar el modo en el que se ofrecen los servicios sanitarios y se utilizan las instalaciones. Las soluciones adecuadas pueden hacer posibles nuevos enfoques, arquitecturas y capacidades, como los que se describen a continuación:

- **Capacidades de edificio inteligente** que conectan los sistemas de calefacción, refrigeración, iluminación y otros servicios ambientales y de seguridad a un gestor de redes automatizado que maximiza el bienestar y reduce los costes
- **Robótica y realidad aumentada** impulsadas por redes con ultra alta velocidad que realizan procedimientos complejos para ofrecer decisiones mejor informadas y resultados óptimos para los pacientes
- **Sistemas blockchain seguros** que permiten realizar un registro preciso del inventario y la cadena de suministro, las transacciones financieras, los tratamientos de los pacientes, el procesamiento de reclamaciones de seguros sanitarios y mucho más
- **Plataformas de aprendizaje mejoradas** necesarias para que los médicos y el personal puedan adoptar estas múltiples y beneficiosas prácticas de manera rápida y eficaz y disfrutar así de un uso compartido de datos más eficaz tanto en el ámbito de la práctica médica como en el de la investigación
- **Informática en la nube** que proporciona una plataforma más sólida que la que se obtendría in situ y que aumenta las oportunidades de procesamiento analítico, automatización operativa y comunicación del personal
- **Redes 5G** que ofrecen lo más novedoso en alta velocidad, rendimiento de baja latencia en interiores y exteriores para conectar a médicos, personal, pacientes, visitas y dispositivos IoMT conectados como dispositivos “wearable” para los pacientes
- **Plataformas interoperables** que conectan disciplinas y departamentos con el objetivo de simplificar el uso compartido de información crítica y la toma de decisiones
- **Sistemas basados en IA** que ayudan a obtener diagnósticos precisos y tratamientos eficaces
- **Soluciones de procesamiento del lenguaje natural (PLN**) que pueden generar notas médicas precisas a partir detexto hablado
- **Análisis médicos** que pueden procesar de manera eficaz enormes cantidadesde datos no estructurados para revelar patrones ocultos en tratamientos y resultados de pruebas
- **Análisis operativos** que pueden informar a los responsables de la toma de decisiones del flujo de trabajo, la seguridad, la sostenibilidad y los procesos logísticos para aumentar la eficacia operativa de todos los aspectos del centro

Estas son solo algunas de las nuevas herramientas disponibles para los proveedores de servicios sanitarios que, en una realidad post pandémica, serán cada vez más importantes para el funcionamiento eficaz de una organización de servicios médicos, tanto en el caso de prácticas médicas individuales como hospitales y centros de investigación.

No obstante, el único prerrequisito que comparten todas ellas es una infraestructura de red unificada, sólida y preparada para el futuro, y aquí es donde más destaca el exclusivo valor de CommScope como Partner de soluciones. ■

MÁS INFORMACIÓN

- Soluciones CommScope para el sector sanitario
- Infografia de la Solución de Healthcare
- Infografía de la Solución de Redes

GRENKE. Una amplia experiencia en renting

GRENKE es una compañía especializada en ofrecer a las pequeñas y medianas empresas, y a toda empresa en expansión, el renting como alternativa a la financiación tradicional para la adquisición de tecnología y equipamiento.

Los esfuerzos de GRENKE, van enfocados a combinar el negocio innovador del renting con la rapidez, la confianza y la cercanía, manteniendo siempre vivo nuestro espíritu emprendedor.

La adquisición de equipamiento tecnológico a través del renting es un modelo en alza por sus claras ventajas financieras, fiscales y operativas: Se paga a medida que se usa el bien, no en el momento de la adquisición; las cuotas mensuales son deducibles al considerarse gasto; y al finalizar el contrato se pueden renovar los equipos para así estar siempre a la vanguardia y ofrecer una inmejorable imagen al cliente.

Sabemos que hoy por hoy la tecnología es clave y gracias a nuestras soluciones de renting queremos hacer llegar a todas las empresas, pertenezcan al sector o industria que pertenezcan, la posibilidad de crecer, adaptarse o innovar.

GRENKE permite que el cliente, ya sea un autónomo, una empresa, un organismo público o una startup, pueda arrendar prácticamente todo el equipamiento necesario para el desarrollo de la actividad de su negocio incluyendo software, iluminación, TPV, robots o cualquier otro equipamiento. También permite al cliente obtener una planificación realista gracias a las cuotas fijas y una optimización de su tesorería, mejor pagar por uso que hacer un gran desembolso inicial.

GRENKE ofrece a clientes dos grandes líneas de soluciones:

Contrato Classic: Con esta solución cualquier empresa o negocio podrá adquirir el equipamiento que necesite en un momento dado. Desde una máquina de café hasta un equipo de resonancia.

Póliza Máster: Si la empresa requiere el renting de equipos con regularidad, enton-ces la opción perfecta es nuestra línea de renting,

permitiéndole ahorrar dinero y ofreciéndole ventajosas condiciones.

De esta forma cuidamos y ayudamos a nuestros clientes o partners. Ya que consi-de-ramos cada relación única, debido a que cada negocio tiene necesidades particulares que suponen para nosotros retos distintos cada vez. Por ello trabajamos día a día en soluciones de renting tecnológico y de equipamiento que se adapten 100 % a cada necesidad: contratos desde 500 euros, respuesta a las operaciones en 20 minutos con la mínima documentación y, por supuesto, firma electrónica de los contratos.

En este sentido primero ofrecimos la firma digital eSignature, con la que se pueden firmar los documentos contractuales directamente en pantalla y devolverlos firmados vía digital en un abrir y cerrar de ojos, de forma segura y jurídicamente vinculante. Desde casa, desde la oficina o en movimiento. Todo lo que se necesita es un ordenador, un portátil o un Smartphone, y acceso a internet.

Y ahora, adicionalmente a la firma digital eSignature, nuestros clientes y partners pueden optar por la firma del contrato a través nuestra Signing App. Una carpeta virtual que permite firmar los contratos de manera electrónica sin perder el contacto cercano entre ambas partes.

De esta forma podemos alcanzar nuestro objetivo que no es más que facilitar a los empresarios la puesta en marcha de sus ideas y proyectos. Después de todo, GRENKE también comenzó siendo solo una idea. Cuando empresarios y emprendedores necesitan adaptar la tecnología de su negocio y no disponen de solvencia para hacerlo, el renting de GRENKE es la solución perfecta.

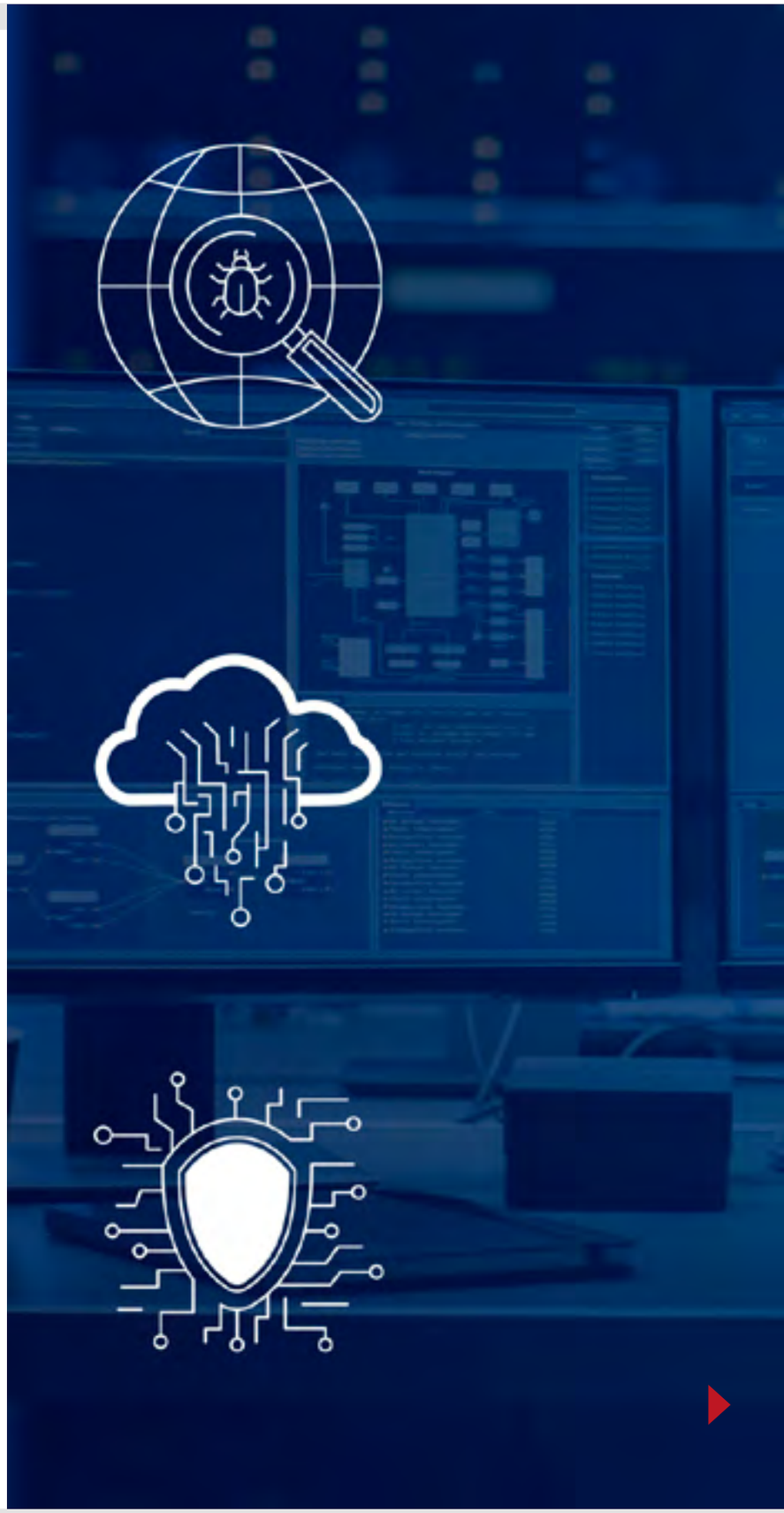
Algo que ya muestra nuestro propio eslogan de marca «Fast. Forward. Finance». Ofrecemos un valor añadido a nuestros clientes porque son nuestra prioridad. ■

MÁS INFORMACIÓN

- Información para partners
- Información renting tecnológico
- Información Productos
- Información Contrato Classic
- Información Póliza Máster
- Información Rent Back
- Información GRENKE para la sanidad

La detección y prevención, claves en la protección

S21sec es la compañía pure-player de ciberseguridad más grande de Iberia con una dilatada experiencia en el sector, lo que le permite ofrecer una cobertura completa de riesgos de ciberseguridad en los procesos de negocio de las organizaciones.



El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones, así como la operatividad de sus sistemas y cumplimiento con el RGPD.

Una plantilla de más de 410 expertos reflejan las capacidades de S21sec para investigar, detectar y prevenir amenazas; piezas clave para reaccionar con mayor rapidez ante cualquier ataque e identificar, diagnosticar y remediar eventuales incidentes en el menor tiempo posible.

Perteneciente al grupo Sonae, S21sec es líder sectorial en España y Portugal por historia, formación, infraestructura y equipo. Está entre las cinco principales compañías de ciberseguridad de Europa, con la aspiración de liderar el mercado europeo a medio plazo.

Además, cuenta con el primer SOC de España, convertido ahora en un multiSOC global distribuido en cuatro localizaciones, que garantiza la integridad de más de 500 organizaciones en España, Portugal y México.

Su porfolio, que aúna soluciones diferentes de manera transversal, está diseñado en torno a cinco necesidades:

1. Identificar: análisis de riesgos y plan general de ciberseguridad, cumplimiento regulatorio, ciberseguridad en la nube y programas de transformación y Red Team.

2. Proteger: diseño y despliegue de arquitecturas y tecnologías, servicios de forma-

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones

ción y concienciación, gestión de dispositivos de seguridad, seguridad de la información y seguridad ATM.

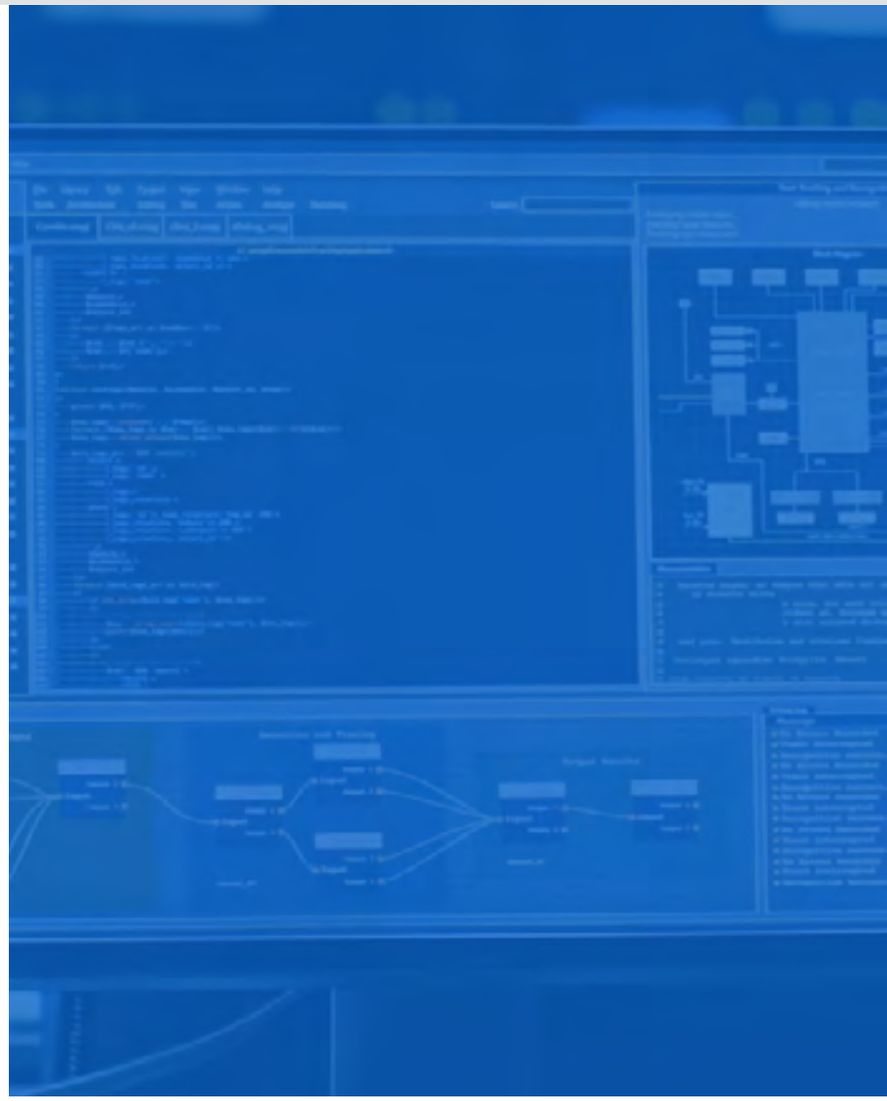
3. Detectar: SOC gestionado y SIEM como servicio, Unidad de Inteligencia de Ciberamenazas, EDR - Detección y respuesta End Point.

4. Responder: CSIRT - Gestión de incidentes de ciberseguridad 24x7, DFIR - Análisis forense digital y respuesta ante incidentes, plataforma de respuesta ante incidentes, SOAR - Automatización, Remediación y Orquestación de la Ciberseguridad y amenazas emergentes - evaluación y perfilación.

5. Recuperar: Continuidad de negocio y planes de respuesta ante ciber-desastres.

Por último, S21sec se guía por una serie de valores clave a la hora de desarrollar e implementar sus soluciones con éxito:

* **Transparencia:** se pone a disposición la información necesaria para la colaboración y la toma de decisiones colectivas.
* **Excelencia:** se persigue ofrecer la más alta calidad gracias a encontrarse en un continuo proceso de aprendizaje.
* **Trabajo en equipo:** se dedica esfuerzo para encontrar la mejor forma de ayudarse entre sí, poniendo el rendimiento de la compañía por encima del rendimiento individual.
* **Innovación:** se busca la diferenciación a través de implementar cambios que mejoran su eficiencia y ventaja competitiva.
* **Confianza:** se construyen relaciones con las personas y las organizaciones basadas en la confianza y la honestidad.
* **Pasión:** se disfruta del trabajo porque siempre se busca de manera proactiva diferenciarse. ■



MÁS INFORMACIÓN

- Rediseños de arquitectura de red en SCI
- Detección de anomalías
- Evaluación y gestión de vulnerabilidades
- Inventario de activos

Proteger las TI a partir del conocimiento de las amenazas

La ciberdelincuencia está cambiando y los ciberdelincuentes cada vez están más preparados y coordinados entre sí, utilizando herramientas muy sofisticadas y difíciles de detectar y de parar, por lo que hay que estar constantemente monitorizando y conocer cuál es la situación de la empresa ante cualquier potencial amenaza.

Las soluciones de Sophos destacadas este año y las que mayor crecimiento están demostrando son:

SOPHOS EDR/XDR

Un completo sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti Exploit, Comportamiento, anti ransomware y anti hacking) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP...) y, por supuesto, EDR o, a día de hoy, XDR, gracias a la integración cruzada de datos con nuestros firewalls y sistemas de protección cloud. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

SOPHOS MTR, MTR-E Y RAPID RESPONSE

Sophos Managed Threat Response (MTR) es un servicio gestionado de Respuesta frente a Amenazas, que ofrece a las empresas funciones de búsqueda, detección y respuesta ante

Sophos dispone de un ZTNA para securizar, las conexiones de usuarios remotos así como los accesos a servicios en nube

posibles amenazas 24/7. Está formado por un equipo de detección de amenazas y expertos en dar respuesta, capaz de tomar medidas para neutralizar incluso las amenazas más sofisticadas. El factor diferencial de esa solución es que, cuando otros sólo notifican, Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y mitigación de la amenaza.

Si aún no es cliente de Sophos, cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response. Un conjuntode productos y un equipo de expertos que son capaces de ver cuál es la situación dentro de la compañía, detener el ataque, si es posible, y detectar cómo ha venido, a quién ha afectado y limpiar para que pueda operar lo antes posible.

SOPHOS ZTNA

Sophos dispone de un ZTNA para securizar, las conexiones de usuarios remotos, así como los accesos a servicios en nube. Todo ello gestionado desde Sophos Central, integrándose con el cliente de Seguridad Endpoint para facilitar los despliegues y adopción de las nuevas metodologías de conexión, evitando los problemas “habituales” de los sistemas VPN y SD-WAN tradicionales. El modelo Zero-Trust Network Access permite a los usuarios conectarse de forma sencilla a los recursos corporativos desde cualquier ubicación y al mismo tiempo mejora su seguridad al verificar de manera constante al usuario y validar el estado y el cumplimiento del dispositivo, así como la red desde donde se conecta.

SEGURIDAD SINCRONIZADA

Sophos lleva ya más de 5 años conectando a través de su Seguridad Sincronizada los distintos sistemas de protección, compartiendo información.

SOPHOS CLOUD OPTIX

Conscientes de que la TI está migrando a la nube, Sophos propone CSWP y CSPM gracias tanto al agente para servidores como a Cloud Optix, el cual audita los recursos que tengamos sobre proveedores de nube pública como AWS, Azure, Google Cloud o Kubernetes tanto en cualquiera de estos entornos como locales. Además, se integra tanto con la protección de instancias y servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el DataLake.

SOPHOS FIREWALL

La seguridad de red no queda desatendida en Sophos. Desde la compra de Astaro en 2008, la han seguido evolucionando hasta llegar a los modernos Sophos Firewall, gestionados de forma centralizada desde Sophos Central, integrándose con el Endpoint y servicios como MTR así como hidratando el lago de datos para permitir detectar, englobándose dentro de nuestra estrategia XDR. ■

MÁS INFORMACIÓN

- Informe de Amenazas 2021
- La evolución de la ciberseguridad: el impacto empresarial de Sophos
- Guía de respuesta a incidentes

El sector sanitario está en el punto de mira de los ciberdelincuentes

Sophos Endpoint

Intercept X with EDR

Impida que su organización se vea afectada por el ransomware.

Sophos Endpoint incluye tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red.

SOPHOS

Cybersecurity evolved.

it TRENDS

CONTENIDOS↓

ABRIL 2021

Cloud, ¿hay opción? Viviendo en la nube híbrida

UNA PUBLICACIÓN DE it Digital MEDIA GROUP

it TRENDS

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 Televisión y Lead Gen
Arancha Asenjo arancha.asenjo@itdmgroup.es
Directora División Web
Bárbara Madariaga barbara.madariaga@itdmgroup.es
Directora de IT Digital Security
Rosalía Arroyo rosalia.arroyo@itdmgroup.es
Director de IT User e IT Reseller
Pablo García pablo.garcia@itdmgroup.es
Director de Operaciones
Ángel Porras angel.porras@itdmgroup.es
Redacción y colaboradores Ricardo Gómez, Alberto Varet, Hilda Gómez, Arantxa Herranz, Reyes Alonso, Belén Juárez
Diseño revistas digitales Eva Herrero
Producción audiovisual Favorit Comunicación, Alberto Varet
Fotografía Ania Lewandowska
Clara del Rey, 36 1º A · 28002 Madrid · Tel. 91 601 52 92

Cloud = Aceleración digital

2020 fue el año en el que la inversión en cloud superó al gasto en data centers propios, según Synergy Research: el año pasado, el gasto en infraestructura en la nube aumentó un 35% rozando los 130.000 millones de dólares, mientras que el gasto en TI empresarial on-premise se contrajo un 6%, quedando en unos 90.000 millones.

El cambio de tendencia comenzó a percibirse en 2019, cuando ambas categorías estaban al mismo nivel. Pero si ya se veía claro que la nube superaría a la TI local, la pandemia ha impulsado este salto en todo el mundo. Cada vez más, las organizaciones se apoyan en servicios cloud para sostener el negocio y avanzar en la transformación digital.

Además, el aumento en las capacidades computacionales, las aplicaciones más sofisticadas y la explosión de los datos están acrecentando la necesidad de servidores, que no terminan instalados en los centros de datos propios, sino en los de los proveedores cloud.

Desde la firma de análisis indican que en los próximos años no se espera ver ya una reducción drástica del gasto en CPD propio, pero sí prevén un aumento rápido en la inversión en la nube, que servirá para sostener la mayor parte del crecimiento digital de las empresas.

Y es que, cuando una compañía necesita más capacidad, puede optar por invertir en su propio data center –espacio ideal para ciertas cargas–, o contar con las posibilidades de flexibilidad, seguridad y crecimiento que ofrece la nube pública; es más, no tiene que casarse solo con una, puede favorecer a su negocio y a su arquitectura de TI con las propuestas de diferentes proveedores y generar un entorno multinube. En la oferta está la opción.

Pero ¿qué supone un entorno híbrido y multicloud desde el punto de vista de la administración de TI? Esto es lo que abordamos en el **Encuentro IT Trends** celebrado este trimestre, y en el que trece compañías nos han ofrecido su visión para la gestión y protección de estas arquitecturas cloud mixtas y múltiples. Gracias a Barracuda, Check Point Software, Commvault, Crayon, Dell Technologies, Entrust, Ikusi, Making Science, Micro Focus, NFON, SonicWall, Sothis y Thales Digital Identity & Security, por haber participado en este evento online que podéis ver aquí y leer su resumen en las siguientes páginas, y a Maica Aguilar Carneros (W4C Spain) y Víctor Escudero Rubio, por aportarnos su visión como expertos tecnológicos.

También en este número de IT Trends descubrimos esas **tendencias tecnológicas que están apuntalando la transformación digital** que se aceleró en muchas organizaciones el pasado año; cómo se está investigando y llevando a cabo proyectos tecnológicos en el entorno universitario de la mano de **Andrés Prado, director TIC de la Universidad de Castilla La Mancha** y miembro de la sectorial TIC de la Conferencia de Rectores de las Universidades Españolas (Crue), y los avances en **computación cuántica** que están haciendo empresas y países. Y ya tenéis disponible el informe IT Trends 2021. Asimilando la aceleración digital, en el que se recoge el estado de las iniciativas TI e intenciones de desarrollo para este año.

Continuemos innovando. ■

Arancha Asenjo
Directora de IT Televisión y Lead Gen Programs

Descarga este **documento ejecutivo** de IT RESEARCH

NUEVO INFORME

2021: tendencias tecnológicas para la maduración digital

Aunque la pandemia ha afectado mucho a la economía mundial, ha tenido un efecto impulsor de la transformación digital para muchos sectores que estaban retrasando este cambio. Una vez superada la primera etapa de esta crisis, las compañías están consolidando sus estrategias de digitalización, lo que acelerará el desarrollo de ciertas áreas en las que la tecnología está evolucionando para proporcionar soluciones de cara al futuro.

Como todo el mundo espera, 2021 será el año en el que vaya estabilizándose la situación sanitaria, aunque las dificultades económicas propiciadas por la irrupción de la pandemia en el devenir global se prolongarán durante varios años. La tecnología ha demostrado su papel salvador en muchas de las situaciones que se plantearon en 2020 y continuará ejerciendo su rol como transformador. En este año seguiremos viendo cómo una serie de tendencias tecnológicas que comenzaron a ganar fuerza el año pasado, están madurando a medida que la situación se va controlando. Cada sector tiene unos objetivos y está siguiendo un camino propio, pero todos tienen como eje principal la transformación

digital. Y también la transición a modelos de negocio digital y la adopción de nuevas estrategias operativas, que aportan flexibilidad y permiten seguir trabajando en situaciones de crisis.

LAS EMPRESAS PRIORIZAN EL TELETRABAJO

Después de que los gobiernos adoptasen medidas de confinamiento, muchas empresas siguieron sus recomendaciones y adoptaron estrategias de teletrabajo para limitar la exposición de sus empleados a posibles contagios. Este es uno de los cambios que se implementaron de forma más apresurada, debido a la urgencia de la situación, pero ha demostrado ser una de las estrategias más inteligentes.

Las restricciones de movilidad han seguir un patrón fluctuante desde la primera oleada de la pandemia, pero la mayoría de las empresas que cuentan con oficinas ha decidido que sus empleados sigan trabajando desde casa, lo que ha sido un acierto. Según los expertos, el éxito que ha tenido esta estrategia en términos generales ha llevado a las empresas de muchos sectores a replantearse su modelo operativo de cara al futuro. Por ello, a partir de este año muchas adoptarán como prioridad el teletrabajo o las modalidades mixtas, que combinan el trabajo remoto y presencial.

Esto tendrá una influencia importante en diferentes mercados vinculados a la tecnología usada en el trabajo desde casa, que verán un aumento importante de la demanda por parte de empresas, instituciones gubernamentales y consumidores. Un ejemplo son las soluciones de comunicaciones unificadas y colaboración, que se han convertido en imprescindibles para muchas empresas.

Aunque las empresas reanuden el gasto en su TI local, seguirán apoyándose en la nube pública para seguir avanzando y para proteger su negocio

Otro es el mercado de ordenadores portátiles, que se ha enfrentado a una demanda muy difícil de cubrir y ha dado nueva fuerza a categorías antes minoritarias como los Chromebooks, que el año pasado registraron ventas sin precedentes y seguirán capturando buena parte del mercado vinculado al teletrabajo. Además, los requisitos que impone esta modalidad laboral están imponiendo nuevos requisitos técnicos que los fabricantes están adoptando para ofrecer equipos más competitivos.

EL MERCADO DE LA NUBE CRECE Y SE CONSOLIDA

Si hay una industria que ha salido reforzada de la crisis causada por la pandemia es la de servicios en la nube. Desde principios de 2020 las empresas han tenido que recortar al máximo el gasto previsto en sus instalaciones y en otras tecnologías, destinándolo a áreas vitales para mantener el negocio en marcha. Esto incluye los servicios cloud, que se han convertido en un apoyo fundamental para garantizar los servicios a sus clientes y la capacidad de sus empleados para trabajar desde sus hogares.

Según los expertos, aunque las empresas reanuden el gasto en su TI local, seguirán apoyándose en la nube pública para seguir avanzando y para proteger su negocio. Esto impulsará el crecimiento del mercado de la nube en los próximos años, generando oportunidades para los proveedores de diferente nivel, que tratarán de capturar cuota en un mercado dominado por unas pocas empresas tecnológicas de gran envergadura. Por ahora, el líder del ranking mantiene un dominio absoluto del mercado y, aunque sus competidores principales están ganando terreno poco a poco, los operadores más pequeños están perdiendo terreno.

LOS CENTROS DE DATOS SE EXPANDEN A NUEVOS MERCADOS

El año pasado las empresas recurrieron más que nunca a las aplicaciones digitales para superar la crisis, generando una gran demanda de tráfico y computación en los centros de datos. A esto se sumó el crecimiento exponencial de los principales segmentos del ocio digital, como los juegos online y los servicios de streaming de contenido

multimedia, que también aumentaron la presión en los centros de datos. Esto obligó a los operadores a incrementar el gasto en infraestructura en sus instalaciones, especialmente en los centros de datos de la nube, una tendencia que continuará a lo largo de este año.

Aunque los expertos afirman que muchos operadores centraron sus inversiones estrictamente en cubrir las necesidades del momento, y los proyectos de construcción y ampliación de centros de datos se vieron ralentizado o paralizados, por lo que el crecimiento del sector fue menor de lo esperado en términos generales. Pero este año la mayoría volverá a ponerse en marcha, y se sumarán otros nuevos proyectos en los principales mercados, que servirán para apoyar la transformación digital en todo el mundo. Además, los expertos destacan que a partir de este año la industria de centros de datos experimentará una rápida evolución, siguiendo tendencias que no se podían anticipar antes de la crisis.

Por otro lado, cabe destacar que no solo se está acelerando la inversión en los grandes mercados de centros de datos, sino que comienzan a ganar peso nuevas localizaciones emergentes en regiones como Asia o Europa, con lugares de gran crecimiento como Madrid, donde se están concentrando nuevas inversiones de la industria. Esta diversificación de la infraestructura global de centros de datos va a continuar en los próximos años, aprovechando la expansión de los nuevos mercados, lo que generará grandes oportunidades para los proveedores de infraestructura y para mercados como el de colocación.

AUMENTAN LOS PRESUPUESTOS DESTINADOS A TECNOLOGÍA

Desde principios de 2020 las empresas han tenido que recortar el gasto al máximo para poder superar la crisis, lo que ha incluido los presupuestos destinados a modernizar y ampliar la TI local. Pero, tras el impacto inicial de la crisis, están volviendo a incrementar el gasto en tecnología para acelerar la transformación digital y mantener su competitividad, una tendencia que continuará este año.

Aunque la pandemia no se ha contenido todavía, y la economía global seguirá sufriendo problemas este año, las empresas de muchos sectores se han dado cuenda de que el futuro de muchos negocios es digital. Para sobrevivir necesitarán invertir recursos en la adopción de nuevas tecnologías, modelos operativos y de negocio basados en lo digital. Esto supone replantear las prioridades de gasto e incrementar los presupuestos destinados a tecnología, algo que los líderes de TI deberán planificar cuidadosamente, en coordinación con otras áreas del negocio que también puedan beneficiarse de estas tecnologías.

LA CADENA DE SUMINISTRO SE MODERNIZA

La pandemia ha puesto de relieve la gran debilidad de la anticuada cadena de suministro global ante situaciones de crisis, ya que el año pasado se produjeron interrupciones graves en el flujo de muchas mercancías fundamentales. Las estrate-

gias tradicionales no permiten anticipar los problemas que se pueden producir ante situaciones complejas en las que confluyen muchas incidencias de forma casi simultánea. Debido a esta rigidez, los integrantes de la cadena no están bien coordinados, por lo que en muchos casos no son capaces de adoptar estrategias que mitiguen posibles interrupciones en el suministro.

Esto está llevando a las empresas vinculadas con toda la cadena de suministro a adoptar tecnologías que les permitan estar más interconectados y poder trabajar en común de forma más flexible e inteligente. Esto abarca desde el seguimiento de activos a través de IoT y 5G a la adopción de sistemas basados en inteligencia artificial para automatizar muchos de los procesos y contar con mejor información de lo que ocurre a lo largo de toda la cadena. Gracias a ello tanto los fabricantes como los distribuidores a lo largo de toda la cadena pueden anticipar las posibles debilidades de la red y los riesgos potenciales de interrupción, pudiendo desplegar a tiempo las estrategias necesarias.

Con el progreso de la digitalización, las organizaciones están capturando y acumulando más activos digitales de alto valor que deben ser protegidos

Especial mención merece el sector de la logística, en el que las principales empresas están adoptando nuevas tecnologías para optimizar las operaciones en diferentes ámbitos. Por un lado, están adoptando sistemas robóticos para automatizar los almacenes y acelerar la gestión de mercancías. Por otro, están desarrollando nuevas plataformas digitales que facilitan el trabajo de los repartidores, optimizando las rutas de reparto y mejorando la conexión con los clientes finales. Además, algunas empresas pioneras están dando los primeros pasos en el desarrollo de los primeros sistemas de reparto de mercancías mediante vehículos autónomos.

NUEVAS TECNOLOGÍAS PARA UNA FABRICACIÓN INTELIGENTE

Hasta el año pasado, la industria manufacturera ha ido adoptando las tecnologías que forman parte del concepto de industria 4.0, pero a un ritmo desahogado. Pero con la pandemia muchas las fábricas han sufrido problemas por la escasez de personal y por los bloqueos de la cadena de suministro. Ante esta situación la industria manufacturera en su conjunto está acelerando la transformación digital, aprovechando los nuevos avances en campos de la tecnología industrial como IIoT, la automatización, la robótica o la inteligencia artificial.

Proteja su experiencia en la nube de Azure.

Soluciones para proteger las aplicaciones y la información en Microsoft Azure y garantizar el cumplimiento de las reglas de seguridad »

Más información:
iberia_team@barracuda.com
barracuda.com

Barracuda Microsoft

STRENGTH IN SECURITY™

Según los expertos, a partir de este año va a acelerarse la adopción de estas tecnologías en la industria de fabricación, especialmente en sectores como la automoción o la electrónica, en los que las cadenas de producción van a seguir automatizándose. Esto permitirá a los fabricantes optimizar todos los procesos de producción, mejorar la calidad de sus productos y ser más eficientes, ahorrando costes una vez que se haya amortizado la inversión inicial.

Aunque, en opinión de los expertos, la automatización de la industria manufacturera todavía tardará unos años y no será completo al 100%, ya que por ahora no hay máquinas capaces de sustituir capacidades superiores del intelecto humano, como los razonamientos avanzados, la intuición y otras habilidades nacidas de la experiencia. Por ello, aunque muchos procesos fundamentales de la industria quedarán al cargo de máquinas robotizadas, los trabajadores humanos estarán al cargo de la toma de decisiones y de ciertos trabajos. Eso sí, en muchos casos asistidos por robots colaborativos, ya sean fijos o móviles, un campo en el que se están llevando a cabo grandes avances.

CIBERSEGURIDAD COMO PILAR DE LA TRANSFORMACIÓN DIGITAL

La seguridad informática siempre ha sido importante para las organizaciones, por lo que tradicionalmente han contratado aplicaciones y servicios

La industria manufacturera está acelerando la transformación digital aprovechando nuevos avances en campos de la tecnología industrial como IIoT

de ciberseguridad para proteger sus sistemas. Pero con el progreso de la transformación digital las empresas han ido ampliando la superficie de ataque, añadiendo localizaciones remotas como la nube o el borde, lo que les ha obligado a incrementar el gasto en ciberseguridad. A esto se suma que los ciberdelincuentes se han vuelto mucho más creativos y han sofisticado aún más sus estrategias, sobre todo a raíz de la pandemia de 2020, lo que ha hecho que las organizaciones incrementen aún más el gasto en ciberseguridad.

Con el progreso de la digitalización, las organizaciones están capturando y acumulando más activos digitales de alto valor, que deben ser protegidos. Como explican los expertos en la materia, los riesgos de sufrir ciberataques aumentan constantemente, lo que está posicionando la ciberseguridad empresarial como uno de los pilares fundamentales de la transformación digital. Por ello, se espera que las empresas eleven este tipo de seguridad a un nivel superior, no solo incrementando el gasto, sino también creando un comité de ciberseguridad en su junta directiva.

Esto les permitirá garantizar que la organización es capaz de enfrentarse a los retos de seguridad que conlleva el progreso tecnológico, algo fundamental de cara al futuro. Porque en los próximos años comenzarán a expandirse nuevas tecnologías en los negocios y en la sociedad que requerirán nuevas estrategias se ciberseguridad. Entre ellas, los expertos destacan la bioseguridad, la cuántica y la seguridad integrada en dispositivos, aunque hay otras tendencias con un gran potencial

ATENCIÓN SANITARIA MÁS DIGITAL Y CONECTADA

Uno de los sectores que más ha sufrido el impacto de la pandemia es el de la salud, en el que los profesionales se han visto sobrepasados por la situación. Por ello, las organizaciones del sector están recurriendo a la tecnología para mejorar la atención sanitaria, ser más eficientes y proteger la salud de los profesionales y los propios pacientes. Los expertos pronostican que a partir de 2021 la industria va a invertir cada vez más en el desarrollo y la expansión de tecnologías como los dispositivos de monitorización remota de salud. Esto permitirá la evolución de conceptos como los wearables empleados en la monitorización de actividades deportivas, que incluirán capacidades y sensores cada vez más avanzados.

Estos dispositivos formarán parte de una nueva generación de plataformas de salud digital

que se alimentarán de grandes cantidades de datos provenientes de los pacientes. Estas plataformas sustituirán a los tradicionales archivos de salud, proporcionando a los médicos gran cantidad de información sobre el historial y el progreso de los pacientes en cada uno de los tratamientos a los que han sido sometidos. Y, para sacar el máximo partido a estas nuevas tecnologías de salud digital, la industria está creando nuevas soluciones de inteligencia artificial para la salud. Esta tecnología permitirá estudiar los datos de los pacientes, en particular y en conjunto, para acelerar la investigación de enfermedades y el desarrollo de tratamientos, algo que durante la pandemia está ayudando mucho a la industria médica y farmacéutica.

Una consecuencia lógica de la transformación digital que se está produciendo en el campo de la salud es un aumento de las ciberamenazas. Porque los datos de los pacientes y de las propias organizaciones de la salud se están volviendo más accesibles para los ciberdelincuentes, a través de los dispositivos remotos y las infraestructuras TI de los centros médicos. Por ello, las organizaciones dedicadas a la salud están cada vez más preocupadas por la ciberseguridad, y a partir de este año aumentarán el gasto en soluciones de seguridad informática.

Los ecosistemas de pago digital se expanden

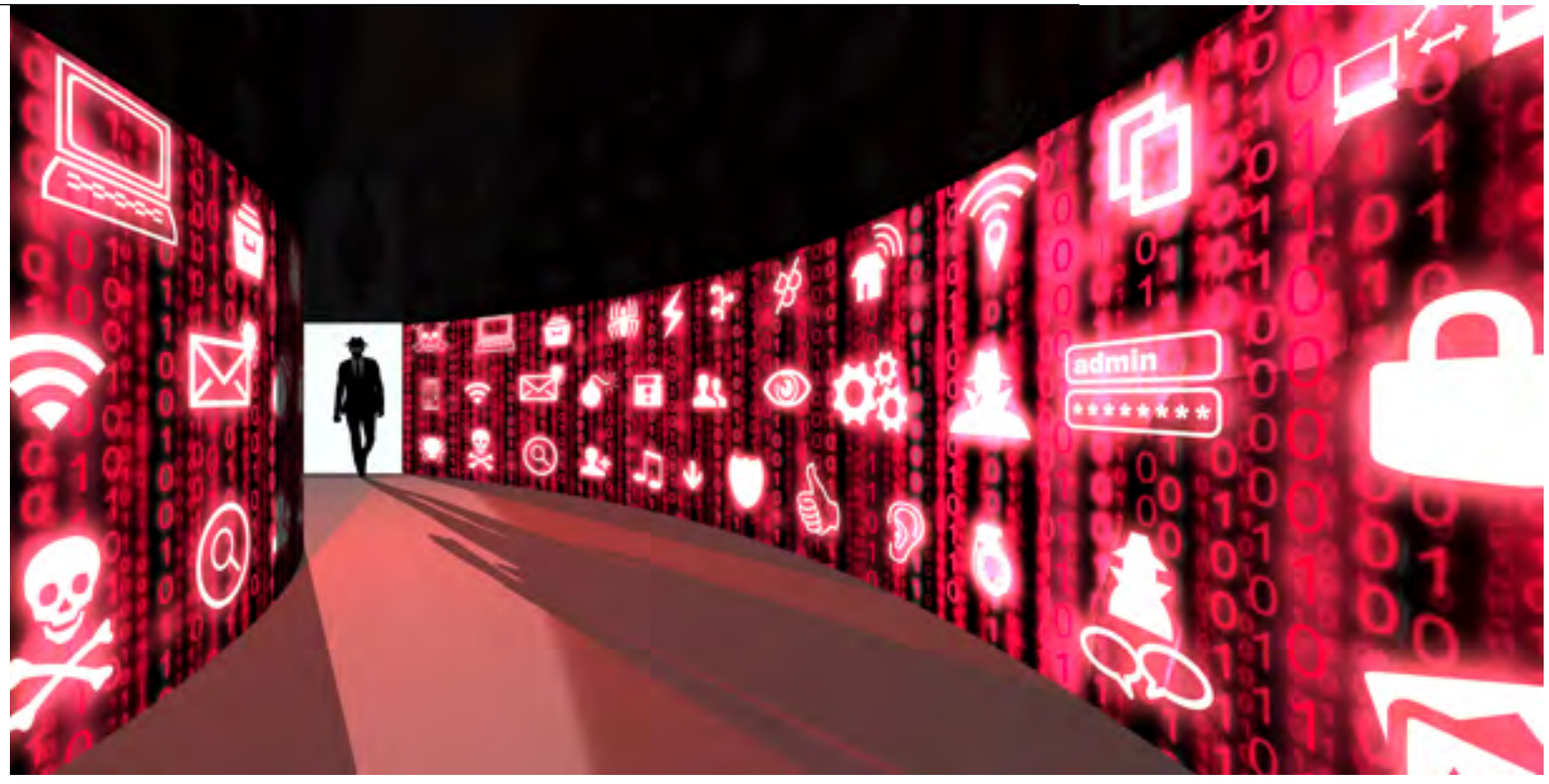
En los últimos años la economía digital ha evolucionado rápidamente, a medida que los consumidores han ido incrementando las compras a través de plataformas de comercio electrónico. En este tiempo han surgido nuevas formas de pago digital que ganan adeptos cada día, como los monederos digitales, que se están integrando progresivamente en la vida y la economía digital de las personas. Se encuentran cada vez más presentes en las plataformas de comercio electrónico y en las tiendas físicas, y los expertos han constatado un aumento considerable del gasto que realizan los consumidores a través de estas herramientas.

Al mismo tiempo, las plataformas de pago móvil se están expandiendo rápidamente, gracias a la necesidad de los consumidores de pagar sin contacto y a que los móviles pueden integrar diferentes medios de pago, desde tarjetas de crédito a monederos digitales y otras aplicaciones de economía digital. Como resultado de la pandemia, los pagos móviles están aumentando considerablemente, y los expertos esperan que sigan haciéndolo este año.

Otra tendencia interesante en el ámbito de los pagos digitales es uso cada vez mayor de la identificación biométrica para validar los pagos móviles. Esto se está logrando gracias a que los nuevos smartphones integran sistemas fiables de lectura de huellas digitales y de identificación de rostros y de voz. Según los expertos, estos sistemas seguirán evolucionando con las nuevas generaciones de dispositivos móviles, acompañando al desarrollo de otras tecnologías de pago móvil.

NUEVAS APLICACIONES PARA LA REALIDAD VIRTUAL Y AUMENTADA

Las tecnologías de realidad extendida (virtual y aumentada) están llegando a un nivel de madurez que permite ofrecer soluciones muy interesantes



Las plataformas de pago móvil se están expandiendo rápidamente gracias a la necesidad de los consumidores de pagar sin contacto

para las organizaciones. Esto generará un gran mercado en el futuro, más allá de las aplicaciones pensadas para el gran consumo. Todos los indicadores muestran que, tras un 2020 desafiante, a partir de 2021 se va a expandir rápidamente el mercado de realidad aumentada y virtual.

Esto se debe a que se están desarrollando nuevos casos de uso comerciales en diferentes industrias, que a partir de este año irán expandiéndose con fuerza, aprovechando que los fabricantes de dispositivos están lanzando nuevos dispositivos portátiles independientes con mejor calidad de imagen, rendimiento y autonomía. Al mismo tiempo, el desarrollo de plataformas y software de realidad aumentada y virtual está avanzando mucho, proporcionando soluciones interesantes en ámbitos como la salud, la ingeniería o la capacitación.

Este ecosistema de proveedores está diversificándose mucho, pero los expertos están convencidos de que en los próximos años va a dar comienzo la consolidación del sector, y anticipan un aumento de las fusiones y adquisiciones en la industria. Así, los grandes jugadores tratarán de absorbes las capacidades de los innovadores en AR/VR, ya que se anticipa una creciente competencia de cara a los próximos años.

INTELIGENCIA ARTIFICIAL MÁS ÉTICA Y EXPLICABLE

La inteligencia artificial se expande rápidamente con la llegada de nuevos casos de uso comerciales y también de ámbito personal. Esto está impulsando la IA a diferentes niveles, desde las aplicaciones más básicas, pensadas para el análisis de datos personales y los sistemas de recomendaciones, a las más sofisticadas, que utilizan las empresas y los gobiernos. Gracias a la IA las organizaciones pueden mejorar sus procesos y contar con mejor información para la toma de decisiones, lo que seguirá impulsando el mercado de inteligencia artificial en los próximos cuatro años.

En este tiempo, además, el concepto de inteligencia artificial irá diversificándose, ya que están surgiendo nuevas formas de entender la tecnología vinculada a la IA. Por ejemplo, las redes de IA distribuida, formadas por enjambres de dispositivos o nodos que cuentan con capacidades de IA propias. Estos son capaces de procesar los datos a cierto nivel, pero forma parte de una arquitectura de IA mayor, donde cada miembro contribuye para proporcionar un mayor nivel de inteligencia. Este enfoque de inteligencia distribuida se desarrollará más a partir de este año,

aprovechando el progreso de tecnologías como las redes 5G y los dispositivos IoT.

Aunque el progreso de la inteligencia artificial conlleva una serie de riesgos que preocupan cada vez más a las autoridades, ya que el tratamiento automatizado de los datos y la toma de decisiones si intervención humana pueden verse afectadas por un sesgo que genere discriminación. Por ello, los expertos en IA están desarrollando códigos éticos que puedan regir el diseño y el comportamiento de la inteligencia artificial, pero no parece que este año se vaya a lograr un avance significativo hacia una ética de IA. Esto se debe a que todavía hay que avanzar más para lograr que los algoritmos de inteligencia artificial sean más explicables, lo que permitiría democratizar el desarrollo de IA para que técnicos menos especializados puedan diseñar aplicaciones que sigan un determinado código ético.

LA BRECHA DE TALENTO DIGITAL SE ACENTÚA

El progreso de la digitalización en las empresas está acentuando un problema que lleva tiempo agrandándose, que es la gran brecha que existe entre la formación de nuevos talentos y las necesidades del mundo laboral. Así, en los últimos años la escasez de personal cualificado para ciertas áreas vinculadas a la tecnología se ha vuelto un problema más grave, y los expertos afirman que gran parte de los trabajadores necesita adquirir nuevas habilidades, muchas de ellas dentro del ámbito digital.

Durante las primeras oleadas de la pandemia muchas empresas han cambiado radicalmente su forma de trabajar, y en los próximos años el puesto de trabajo va a cambiar mucho, integrando nuevas tecnologías y deslocalizándose por la proliferación del teletrabajo. Mientras tanto, se espera que la crisis económica lleve al cierre de muchas empresas, inundando el mercado laboral de nuevos trabajadores, pero muchos de ellos no tendrán la cualificación necesaria para trabajar en los nuevos puestos de trabajo, cada vez más vinculados al uso de tecnologías digitales.

Las empresas y las instituciones públicas tratarán de ir cerrando la brecha de talento, peo esto también requerirá un cambio de mentalidad por parte de las personas. Porque, estudios recientes indican que muchos trabajadores no aplican los conocimientos adquiridos a través de la formación, y esto es un freno para su progreso profesional y para las empresas en las que trabajan. Esto implica que se debe impulsar un cambio cultural en las organizaciones, incentivando a los trabajadores a mejorar a través de un enfoque de aprendizaje constante. ■

Si te ha gustado este artículo, compártelo

CloudGuard

Check Point CloudGuard proporciona seguridad nativa en la nube unificada para todos sus activos y cargas de trabajo, lo que le brinda la confianza para automatizar la seguridad, prevenir amenazas y administrar la postura, en todas partes y en todo su entorno.

Más información:

www.checkpoint.com/es

Check Point®
SOFTWARE TECHNOLOGIES LTD

Tendencias en entornos cloud:

cambios en la arquitectura y perspectivas futuras

El uso de la nube ha crecido exponencialmente en los últimos años y continuará haciéndolo: según IDC, el mercado español de cloud experimentará un crecimiento cercano al 20% anual. La combinación de infraestructura y servicios compartidos para crear un entorno de TI flexible, escalable y bajo demanda ha convertido a la nube en el modelo dominante para entregar y mantener los recursos de TI empresariales, desde el hardware de computación, pasando por el almacenamiento, las redes, hasta el software empresarial.

El mantra de la resiliencia empresarial y digital seguirá pronunciándose este año a medida que las organizaciones se preparen para responder a la continua incertidumbre y disrupción. Para que las empresas puedan ser más competitivas en esta época es esencial que entiendan cómo se está transformando el panorama de TI, incluida la forma de administrar e implementar de manera efectiva los cambios necesarios para permitir la capacidad de respuesta rápida.

En un momento en el que las empresas necesitan agilidad y dinamismo para adaptarse a las circunstancias del mercado, la nube se ha

convertido en un dinamizador de la agilidad y transformación digital, especialmente en su versión híbrida, en el que se pueden unir las capacidades y ventajas de un entorno privado con todos los beneficios de una cloud pública gestionada por un tercero, con todas sus medidas de seguridad, elasticidad, innovación y conocimiento para la administración.

Este año las empresas se están preparando para que la nube llegue a todas las áreas e industrias. Por ello, los dirigentes empresariales deben observar las tendencias actuales para que sus servicios se ajusten a las necesidades de los clientes:

1 La eliminación de las cargas de trabajo innecesarias de la nube será la tendencia más destacada. Reconfigurar la estrategia para maximizar los beneficios, minimizar los costes y reducir la carga es crucial para el éxito de la nube a largo plazo. Contar solo con un proveedor de nube pública puede haber permitido la continuidad del negocio en 2019, pero tras la llegada de la pandemia, cada vez más proveedores están considerando otros modelos como un entorno multicloud como el sistema ideal para todas las operaciones.

2 Volver a activar la gobernanza de la nube para mantenerse seguro. Buscando fortalecer la estrategia de la nube, las empresas pueden reconsiderar los esfuerzos de gobernanza para priorizar la seguridad. Volver a los cimientos de las nubes y desarrollar un plan de gobierno sólido ayudará a las empresas a reforzar la infraestructura de seguridad para corregir la adopción apresurada que muchas realizaron en 2020.

3 Un crecimiento exponencial de la adopción de la nube. El año pasado el mercado global de infraestructura de nube pública creció un 35% a hasta los 100.000 millones de euros, según Forrester.

Además, en 2021 más de la mitad de las empresas aumentará la inversión en Amazon Web Services, Salesforce, Google u otros servicios en la nube este año con Microsoft Azure como la mejor opción.

4 Aumento de la innovación en la nube híbrida. A lo largo de 2021 comenzaremos a ver más estrategias multicloud com-

CINCO CONSIDERACIONES PARA PROTEGER LA INFRAESTRUCTURA EN LA NUBE

binadas con iniciativas de capacitación más amplias tanto de las empresas como de los propios proveedores.

En un futuro cercano, las innovaciones en la nube provocarán que el volumen de datos en la nube se centre cada vez más en los dispositivos que operan con IA para entregar a las empresas datos predictivos fiables para que la toma de decisiones sea fácil para los líderes empresariales. ■

MÁS INFORMACIÓN

- Forrester: Predicciones 2021: Cloud Computing potencia la recuperación de la pandemia
- Gartner predice el futuro de la infraestructura cloud y Edge
- Synergy Research: Los proveedores de cloud europeos luchan por revertir las pérdidas de cuota de mercado

Si te ha gustado este artículo, compártelo

FUERTE CRECIMIENTO DEL MERCADO CLOUD

El gasto total en servicios en la nube, en el hardware y el software que sostiene estos servicios y en los servicios profesionales y administrados vinculados a la cloud, crecerán aun ritmo anual del 15,7% hasta 2024, según IDC. Para entonces, pronostican que estas inversiones generarán oportunidades de negocio por un valor de más de 1 trillón (americano) de dólares en todo el mundo.

Como explica en este informe Richard L. Villars, vicepresidente de grupo de investigación mundial de IDC, "la nube en todas sus permutaciones (hardware/software/servicios/aaS, así como la nube pública/privada/híbrida/multi/edge) desempeñará roles cada vez mayores, e incluso dominantes, en la industria de TI en el futuro previsible".

Afirma que "para fines de 2021, sobre la base de las lecciones aprendidas en la pandemia, la mayoría de las empresas pondrán en marcha un mecanismo para acelerar su cambio a la infraestructura digital centrada en la nube y los servicios de aplicaciones, a un ritmo dos veces más rápido que antes de la pandemia".

Las principales fuentes de crecimiento del mercado asociado a la nube serán los servicios de nube pública (compartida) y los servicios de nube privada, una categoría que seguirá siendo la más grande del mercado, y que en este tiempo mostrará un crecimiento del 21% (CAGR). De cara a 2024, IDC anticipa que la categoría "como Servicio" logrará acaparar el 60% de todos los ingresos mundiales de la nube.

Mientras tanto, la categoría que abarca los servicios profesionales y los servicios de gestión relacionados con la nube crecerán al ritmo más lento (8,3%). Finalmente, el segmento de construcción de infraestructura, que abarca el hardware, el software y el soporte para nubes privadas empresariales y nubes de proveedores de servicios, seguirá siendo el más pequeño, pero crecerá a un saludable ritmo del 11,1% (CAGR).

La sencillez a veces esconde una gran complejidad

Cloud

Cloud

Privada

Cloud Híbrida

SaaS

Pública

Sin-Nube

Edge

Co-location

Sothis
Inteligent Services,
Inteligent Tecnology

www.sothis.tech

sothis

#ENCUENTROSITTRENDS

Ya vivo en la nube, ¿y ahora qué?

Mejores prácticas para desenvolverse en entornos híbridos

Los entornos de TI multicloud e híbridos se están convirtiendo en el modelo hacia el que se dirigen las arquitecturas de TI actuales. Gestionar estas infraestructuras cloud, controlar sus costes, desarrollar nuevos servicios nativos en cloud, asegurar la disponibilidad del negocio basado en la nube, garantizar el cumplimiento normativo y proteger los activos que residen en la cloud, son cuestiones que todo responsable de TI debe tener bajo control.

En IT Trends hemos reunido a diversos expertos para abordar las nuevas propuestas tecnológicas disponibles para una mejor resi-

dencia en una cloud que predominantemente es híbrida, así como para tener una mayor visibilidad entre las diferentes nubes y servicios. En este Encuentro IT Trends participaron Miguel López Calleja (Barracuda), Eusebio Nieva (Check Point Software), Elisa Martínez (Commvault), Jose Manuel Marina (Crayon), Nieves Gonzalez (Dell Technologies), José María Pérez (Entrust), Jorge Marín Sánchez (Ikusi), Miguel López Sánchez (Making Science), Antonio Picazo (Micro Focus), Agustín Sánchez Fonseca (NFON), Sergio Martinez Hernandez (SonicWall), Ceferino Raposo (Sothis), Alfonso Martinez (Thales Digital Identity & Security), Maica Aguilar Carneros (W4C Spain) y Víctor Escudero Rubio. ■

cpl.thalesgroup.com

THALES
Building a future we can all trust

CipherTrust Data Security Platform

Localice, proteja y controle los datos sensibles de su organización en cualquier lugar gracias a la protección de datos unificada de última generación.

Localizar Proteger Controlar

Empiece a localizar, proteger y controlar sus datos hoy mismo

#ENCUENTROSITTRENDS

Conocimiento, adopción y adaptación para gestionar de manera eficiente la nube

Los entornos de Cloud continúan adoptándose en la empresa española de manera progresiva, tras demostrar en estos últimos meses ser un modelo que aporta flexibilidad a las estructuras tecnológicas de las empresas cuando éstas necesitan adaptarse a imprevistos.

Maica Aguilar (W4C Spain) y Víctor Escudero (experto en implantaciones Cloud), conversan sobre los retos que se les plantean a las empresas en su gestión de entornos multicloud. Clic para ver.

“Los estándares de auditoría, trazabilidad y herramientas permiten tener una visión amplia y transparencia en un mundo que ya no es nuestro, sino que se está gestionando por un tercero”

MAICA AGUILAR, WOMEN4CYBER SPAIN

Según la última encuesta realizada por IT Trends, la ciberseguridad será la principal área de inversión en 2021, pero le siguen los servicios y la infraestructura cloud. Además, el número de empresas cuya TI se limitaba a los entornos on premise ha disminuido porque se han unido tanto a la cloud privada como a la cloud pública, de acuerdo con el informe, que recoge que los niveles de infraestructura híbrida son los que más han crecido durante estos meses, y precisamente, son los que mayores inversiones van a recibir en este año. Respecto al número de clouds públicas contratadas, un 49% de los consultados asegura que su empresa cuenta con dos o más de estas nubes públicas. Asimismo, los encuestados consideran que para sus nubes será estratégico en este 2021 la seguridad, la integración de plataformas y la disponibilidad de las aplicaciones.

Ante estos datos, Maica Aguilar, experta en Ciberseguridad y Privacidad y miembro de la Junta Directiva de Women4Cyber Spain, explicó en la primera mesa de debate del Encuentro IT Trends titulado “Ya vivo en la nube, ¿y ahora qué? Mejores prácticas para desenvolverse en entornos de Cloud híbrido”, que “el reto está en la adecuación, en tener capacidad dentro de las organizaciones para conocer el cloud y poder adaptarse al cambio de un modelo tradicional a estos ecosistemas”. Desde su punto de vista, hace años la ciberseguridad era uno de los principales frenos a la hora de migrar al cloud, pero hoy en día la perspectiva de muchas empresas ha cambiado. El cloud actualmente ofrece garantías tanto en la parte de compromiso como en la de ciberseguridad. “Sabemos cómo se están gestionando esas clouds porque tenemos estándares de auditoría, trazabilidad y herramientas que permiten una visión amplia y transparente en un mundo que ya no es nues-

“Los estándares de auditoría, trazabilidad y herramientas permiten tener una visión amplia y transparencia en un mundo que ya no es nuestro, sino que se está gestionando por un tercero”

VICTOR ESCUDERO, EXPERTO EN IMPLANTACIÓN DE CLOUD

tro, sino que se está gestionando por un tercero”, añadió Aguilar.

El coste de la cloud sigue siendo un punto clave en las organizaciones en la migración al cloud. El coste variable o pago por uso continúa siendo predominante en comparación a un pago por la contratación de una infraestructura o un pago por adelantado. “Pero lo más relevante ahora mismo tiene que ver con la escalabilidad y la flexibilidad; en época de pandemia, una empresa necesita saber qué puede crecer con un par de clics. Es decir, no haces una inversión a tres años vista de una infraestructura”, apuntó Victor Escudero, experto en implantación de proyectos Cloud, y compañero de debate. Ambos participantes estuvieron de acuerdo en que la economía de escala a nivel de seguridad no permite hacer inversiones como las grandes compañías, con Microsoft o Amazon como ejemplo. Pero, por otro lado, existen facilidades como el pago por uso para los usuarios residenciales y en consecuencia, muchos servicios de nube son más sencillos de operar y de utilizar. Las grandes compañías de cloud tienen grandes inversiones en ciberseguridad y las pequeñas empresas no pueden asumir esos gastos. Sin embargo, pueden acercarse al modelo cloud y entenderlo”, destacó Aguilar.

Los costes más directos son relativamente sencillos de ver. Sabemos cuánto pagamos por memoria o por consumo de CPU. Aunque es más difícil de ver lo que pagamos en tráfico saliente de datos hacia internet. “Hay que tener en cuenta muchos costes de licenciamiento o pago por uso. Cuando contratas una solución en modelo SaaS estás reduciendo la carga de administradores de bases de datos o de sistemas y estás difiriendo la carga operacional en un proveedor”, explicó Escudero.

Si se quiere parchear máquinas y para ello es necesario acceder a las soluciones de ciberseguridad, el proveedor de nube puede hacerse car-

go de gran parte de las actualizaciones, aunque sea un coste inmenso a nivel operativo. Además, esto provoca que no esté todo actualizado continuamente. "Cuando se calcula el TCO o coste total de oportunidad en tres años, rara vez sale más caro en nube que on-premise. Hay que computar los costes por todo lo que conlleva, no por lo que se ve de manera inmediata", argumentó Escudero.

Por su parte, Maica Aguilar recordó que normalmente las nubes públicas hablan de seguridad compartida si tienen estándares aunque de base no está. Y "como no se puede vivir sin seguridad, no hay que olvidar esa capa tan necesaria en servicios y plataformas a la hora de hacer el análisis de costes".

EL MEJOR MODELO DE CLOUD

Los expertos explicaron en la mesa que no existe un modelo de cloud concreto para un tipo de organización u otra, ya que es probable que en una gran empresa haya determinados procesos que encajen mejor en un modelo público y otros en un modelo privado. La clave está en lo que se quiere hacer y en ir con el partner adecuado. "Nosotros administramos nube pública, nube híbrida y mucho modelo de servicio dependiendo de cada empresa y sus necesidades", subrayó Aguilar, que trabaja en Ferrovial.

Para Víctor Escudero, se pueden valorar las modalidades de consumo de la nube como IaaS, platform o modalidades de software, y señalar en la hoja de ruta los ritmos que ha de llevar la empresa en la transición hacia la nube. "Se puede mover infraestructura puntualmente o ir sacando partido de distintas funcionalidades según se necesiten". Además, deshacer estos cambios suele ser simple.

Otro aspecto a considerar es ver qué capacidades nativas de nube se tienen, ya que algunas capacidades que se hacen de una forma tradicional no tienen una traducción exacta en la nube. "Los modelos de nube son mucho más naturales que los tradicionales. En esa línea, hay servicios legacy que no tiene sentido desglosar en la nube pero hay otros que te pueden interesar, como llevar los frontales y la parte de base de datos dejarla on premise de momento y seguir con ellos en la siguiente fase de la migración", detalló Escudero.

Respecto al uso de entornos multicloud, en opinión de este experto, hay pocas diferencias entre Azure, Amazon Web Services o Google Cloud porque en todos ellos hay multi zona y multi región. Los cambios varían según se escala en cuanto a servicios, siendo los más avanzados en modalidad SaaS en los que hay grandes diferencias

A esto añade Maica Aguilar que "lo que hoy se vive de una forma, en el futuro puede ser de otra pero la clave es pasar por la estrategia multinube para que nuestro negocio evolucione de forma óptima". ■

it whitepapers

IT TRENDS 2021.
Asimilando la aceleración digital

¿Qué tendencias tecnológicas dominarán en el año post-pandemia? En este informe de IT Research desvelamos las principales claves de las estrategias TI para este 2021.

Run and Transform—Your Key to Success

Balance today's needs with tomorrow's opportunities.

When you can run and transform your business at the same time, you have the balance you need to optimize your enterprise and expose new opportunities as your markets evolve. No matter what's driving the change—technology innovation, the digital economy, and even pandemics and disasters—we can help you succeed with a customer-centric, measured, low-risk approach. That's High Tech, Low Drama.

#ENCUENTROSITTRENDS

Prácticas para desenvolverse en entornos híbridos y multicloud y ser competitivos

La combinación de entornos privados con las nubes públicas ha dado lugar a una nueva forma de TI híbrida de la que la empresa obtiene las ventajas de ambas modalidades, pero también sus desafíos: aprender a arbitrar las cargas de trabajo, segmentar las arquitecturas y a la vez integrarlas para poder mover aplicaciones y datos y, además, proporcionar herramientas que aporten agilidad a la administración de estos entornos.

(De izq. a dcha) Jorge Marín (Ikusi), Agustín Sánchez (NFON), Miguel López (Making Science), Nieves González (Dell Technologies), José Manuel Marina (Crayon Software), Antonio Picazo (Micro Focus) y Ceferino Raposo (Sothis). Clic para ver

“Como el entorno multicloud aumenta la complejidad, se necesita una estrategia global y la contratación y retención del personal adecuado”

JOSÉ MANUEL MARINA, CRAYON SOFTWARE

Además, es cada vez más común que las empresas distribuyan sus activos entre varias nubes, lo que puede añadir mayor complejidad a la estructura tecnológica de la empresa. Administrar estos entornos de nube híbrida y mutlicloud es posible con las recomendaciones que dejaron en el Encuentro IT Trends “Ya vivo en la nube, ¿y ahora qué? Mejores prácticas para desenvolverse en entornos Cloud híbridos”, en el que participaron portavoces de Crayon Software, Dell Technologies, Ikusi, Making Science, Micro Focus, NFON, y Sothis.

Para conseguir ser competitivo, el negocio busca mucha innovación y reducir el tiempo de despliegue de nuevos servicios. “IT busca simplicidad, más eficiencia, escalabilidad y elasticidad. Es decir, que en determinados momentos, como en rebajas, un retail pueda coger cargas de nubes públicas y traerlas a las nubes privadas”, ejemplificó Nieves González, Manager Systems Engineer de Dell Technologies durante la mesa redonda sobre prácticas para desenvolverse en entornos híbridos y multicloud, y en cuya opinión, el reto de las empresas es controlar el coste consiguiendo innovación y adaptándose a los cambios.

Para José Manuel Marina, director general de Crayon, el mayor desafío de adaptación al

5 FACTORES CLAVE PARA SIMPLIFICAR SUS OPERACIONES DE TI MULTICLOUD

Dado que las opciones de servicios y soluciones se han multiplicado, hoy en día el consumo de TI multicloud y de nube híbrida ha pasado a ser una realidad en la mayoría de las organizaciones. Lo vemos tanto en las pymes como en las grandes empresas, eso sí con diferentes desafíos para las organizaciones en función de su tamaño y de las soluciones adoptadas. En este e-book encontrará 5 cuestiones a tener en cuenta para lograr la mejor experiencia de usuario y la mayor rentabilidad consumiendo servicios de TI multicloud.

“No todo es consumible desde la nube pública o todo se tiene que transformar desde el data center”

NIEVES GONZÁLEZ, DELL TECHNOLOGIES

entorno multicloud es que el cliente puede no estar preparado realmente. Consumir servicios en la nube de varios proveedores es complejo y difícil de gestionar y hay que hacerlo con una estrategia determinada. “Como el entorno multicloud aumenta la complejidad, se necesita una estrategia global y la contratación y retención del personal adecuado con conocimientos on premise dispuestos a reciclarse de manera continua”, apuntó.

En este contexto, los CIO, además, han de decidir qué tipo de aplicaciones o servicios han de ubicarse en cada tipo de proveedor y dónde ubicar cada carga de trabajo. Cada servicio puede necesitar más registros de seguridad, más requisitos de cumplimiento normativo o más elasticidad. “Tener un servicio en cloud es lo mismo que tenerlo en el data center en el sentido de que es un servicio más que hay que gestionar. Para el cliente el proceso ha de ser totalmente transparente”, destacó Antonio Picazo, preventa de soluciones de Micro Focus.

Desde Making Science, Miguel López, CTO y Head of Infrastructure Operations, señaló que el Cloud, aunque presenta más beneficios que contras, conlleva unas elevadas necesidades de control. Además, “en los últimos años se han unido el multicloud con la contenerización. Pero no hay que olvidarse de la seguridad. Cuando se trabajaba con data centers había que usar máquinas físicas, pero ahora se piden máquinas virtuales dando a un botón

it whitepapers OPTIMIZANDO LA UBICACIÓN DE LAS CARGAS DE TRABAJO EN LA NUBE HÍBRIDA

A comienzos de 2020, IDC investigó acerca de cómo las organizaciones determinan la ubicación de las cargas de trabajo a medida que evolucionan en su transformación digital (DX). Entre sus hallazgos, señala que las principales consideraciones para determinar la ubicación de las cargas de trabajo entre la nube tradicional en las instalaciones y la nube pública y privada incluyen la seguridad, el rendimiento, la facilidad de administración, la disponibilidad, el coste, el cumplimiento, la agilidad, los patrones de uso y la importancia de los datos.

“Las redes tradicionales no están preparadas para abordar las cargas de trabajo tan grandes”

JORGE MARÍN, IKUSI

y esto ha llevado a un problema de gobierno que se está intentando paliar. Muchos proveedores intentan que la gestión de clusters y Kubernetes estén centralizados para tener políticas centralizadas, dando cierta libertad a los diferentes equipos. Pero muchas empresas han dado un salto a cloud sin saber cómo gestionar o controlar. Cada proyecto se ha hecho de manera diferente”.

En este sentido, Antonio Picazo, de Micro Focus, apuntó que ese control tiene que llevarse a cabo desde el primer momento sin perder agilidad. “No puede ocurrir que para que algo sea desplegado pasen días y días. Hay que tener una solución de gestión fácil; es decir, que se pueda acceder solo con un clic, pero centralizada para poder iniciar el control. Y es importante evitar el vendor lock-in de un proveedor de cloud. Las soluciones han de poder mover cargas de un sitio a otro, todavía la tecnología en caliente y tiempo real es complicada, pero hay que tener en cuenta que se puedan tener soluciones que nos ayuden en otro momento”.

Ceferino Raposo, Business Architect de Sothis, indicó que no solo hay que centrarse en la oferta tecnológica, sino que hay que cribarla según las necesidades de la organización. “Además, el número de recursos o soluciones queda limitado si se hace ese trabajo previo. El marco de referencia han de ser los objetivos estratégicos y las mejores herramientas, ya sean locales en el CPD o en la nube. A partir de ahí se pueden establecer los mejores mecanismos y técnicas de control”.

it whitepapers

LA SEGURIDAD DE SU WAN. Los 3 tipos principales de amenazas y cómo superarlos

A medida que su red de área extensa evoluciona, es posible que deba habilitar el acceso directo a Internet en la sucursal, proteger la conectividad a la nube y proteger a todos los usuarios y dispositivos de las amenazas sin comprometer la experiencia del usuario. Es más fácil decirlo que hacerlo, ¿verdad? Lee en este documento cómo la WAN definida por software (SD-WAN) de Cisco puede manejar todas estas exigencias sin dejar atrás la seguridad.

“Muchas empresas han dado un salto a cloud sin saber cómo gestionar y controlar el proyecto”

MIGUEL LÓPEZ, MAKING SCIENCE

Para este experto, es importante la comunicación entre equipos de desarrollo y equipos de sistemas porque no solo hay que ver si una máquina funciona bien o mal, sino si el proceso se está realizando de manera óptima. “Se está produciendo un cambio de cultura en el que los desarrolladores hablan más con los de sistemas. Y eso es un trabajo colaborativo entre todos para que no se disparen los costes. La gente pierde la perspectiva de que lo que va al cloud son las aplicaciones y por eso también se olvidan de que la aplicación se ha diseñado como un silo. Por eso lo mejor es saber de qué manera van a llegar los usuarios a mis aplicaciones. Hay que tener en cuenta lo que quiero hacer, cómo lo quiero hacer y cuáles son los mejores elementos para lograrlo”.

Respecto a la decisión de dónde ubicar las aplicaciones, Nieves González, de Dell Technologies, recuerda que “existen distintas aplicaciones: algunas se despliegan desde las nubes públicas, y otras se mantendrán en el data center. Existe un gran porcentaje de aplicaciones que se transformarán a una nube privada o a una nube pública en función del dato o los controles o tendrán que sufrir una rearquitectura para ser realmente movibles. No todo es consumible desde la nube pública o todo se tiene que transformar desde el data center. Lo que es necesario es que todas aplicaciones han de mantenerse de manera resistente”, puntualizó.

Junto a esta decisión, las empresas también necesitan decantarse por una plataforma de

it whitepapers

CLOUD MIGRATION: APUESTA POR EL FUTURO DE TU ORGANIZACIÓN EN LA NUBE

En tiempos de incertidumbre, la migración a Cloud supone una ventaja organizacional al obtener una mayor funcionalidad, escalabilidad y flexibilidad, además de accesibilidad en cualquier momento y en cualquier lugar. Con Cloud, se obtiene una mejora en la productividad al conseguir una mayor agilidad, mayor eficiencia en el reparto de las cargas de trabajo y una reducción de costes de TI. Este documento recoge las principales ventajas de la migración a la nube, ejemplos de migración y las capacidades que ofrece Google Cloud a las organizaciones.

“Hay que tener una solución de gestión fácil, que se pueda acceder solo con un clic, pero centralizada para poder iniciar el control”

ANTONIO PICAZO, MICRO FOCUS

red adecuada al entorno cloud. En opinión de Jorge Marín, Service delivery manager de Ikusi, la situación de incertidumbre total hace que las empresas necesiten una plataforma inteligente que responda a casi cualquier situación. “Las redes tradicionales no están preparadas para abordar las cargas de trabajo tan grandes, por eso existen armas que se deben facilitar a las empresas como la automatización de las operaciones de networking y el análisis de la IA para tener perspectivas más inteligentes del negocio”, indicó.

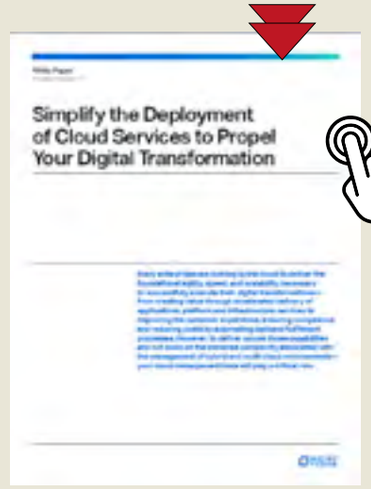
Asimismo, la recomendación de Jorge Marín es una estrategia de red proactiva y multicloud, que alinee las prioridades de la nube, la seguridad y las aplicaciones de los departamentos de IT. Para que esta estrategia tenga éxito tiene que apoyarse en la carga de trabajo, el acceso y la seguridad. “Se debe adoptar un modelo operativo para administrar las políticas de manera más ágil y en cuanto al acceso, hay que implementar soluciones del tipo SD-WAN para reducir los costes operativos. También ha de reducirse el riesgo asociado a los usuarios con distintas soluciones ya que las apps están en diferentes nubes”, explicó Marín.

FLEXIBILIDAD DEL CLOUD SÍ, PERO CONTROLANDO LA INTEGRACIÓN

Agustín Sánchez, responsable de Desarrollo de negocio de NFON, puso en su intervención el foco en el SaaS que presta servicios como las

it whitepapers

SIMPLIFICANDO EL DESPLIEGUE DE SERVICIOS CLOUD PARA POTENCIAR LA TRANSFORMACIÓN DIGITAL



Muchas empresas buscan la nube para ofrecer agilidad, velocidad y escalabilidad para ejecutar con éxito sus transformaciones digitales, desde la creación de valor con la entrega acelerada de aplicaciones, servicios de plataforma e infraestructura, o la mejora de la experiencia del cliente, garantizando el cumplimiento y reduciendo costes mediante la automatización de procesos. Sin embargo, para ofrecer todas esas capacidades y reducir la complejidad asociada con la administración de entornos híbridos y de múltiples nubes, debe contar con las correctas herramientas de administración de la nube.

“El cloud te da proceso, capacidad de almacenaje, pero al otro lado también hay una aplicación de infraestructura que funciona bien, y está el receptor”

AGUSTÍN SÁNCHEZ, NFON

comunicaciones unificadas. Y ejemplificó bien esa complejidad y necesidad de integrar equipos y aplicaciones que se da en el entorno de la infraestructura, con el uso de aplicaciones de telefonía en la nube, para las cuales “hay que comprobar si se dispone del equipo adecuado, con suficiente RAM, y la compatibilidad de los sistemas para usar Teams y el teléfono a la vez”, apuntó.

En su opinión, “el cloud te da proceso, capacidad de almacenaje, pero al otro lado también hay una aplicación de infraestructura que funciona bien, y está el receptor. El mercado, especialmente la pyme, han aprendido que el cloud te permite tener también una buena comunicación sacando fuera el servicio, y ser flexible para poder mover tu centralita on premise a casa si surge un problema. El consumo flexible o quitarle carga de trabajo al responsable de redes han transformado la percepción de los servicios de comunicaciones en la nube”.

Otro efecto de la situación que estamos viviendo es la demanda de teletrabajo. En este sentido, José Manuel Marina, de Crayon, explicó que, en su caso, “hemos ayudado a los clientes a entender qué es lo que tienen que

it whitepapers

SOLUCIONES CLOUD PARA LA CONTINUIDAD DEL NEGOCIO EN ENTORNOS VUCA

La nueva era digital que se dibuja en la actualidad está transformando no solo la forma en que las empresas están gestionando su relación con los clientes reales, sino también la forma en que las organizaciones ofrecen, acceden y consumen servicios y aplicaciones.

En este escenario de continuidad, IDC indica en este documento que las comunicaciones han sido la palanca que ha permitido a las organizaciones poder afrontar el proceso de recuperación y habilitar la transformación del puesto de trabajo, permitiendo la movilidad del empleado y la puesta en marcha de entornos colaborativos.

“El marco de referencia han de ser los objetivos estratégicos y las mejores herramientas, ya sean locales o en la nube. A partir de ahí se pueden establecer los mejores mecanismos y controles”

CEFERINO RAPOSO, SOTHIS

cargar y cómo hacerlo. Ofrecemos una plataforma multinube con nuestra propia IP con la que pueden aprovisionarse de soluciones y detectar posibles incidencias”.

Y sobre la calidad de servicio que apuntaba el portavoz de NFON, Miguel López, de Making Science, señaló que no puede olvidarse la gestión de las expectativas. “El cloud ha permitido tener muchos más KPIs, ya sea on premise o en cloud para sacar métricas de calidad de servicios. Muchos clientes están haciendo análisis con servicios cloud para que no se vaya información confidencial, pero también para transcribir las comunicaciones y analizar sentimiento para saber cual es la media en todos sus operadores”, concluyó.

Para ver la charla completa, accede aquí. ■

Si te ha gustado este artículo, compártelo

NUBE HÍBRIDA O TI HÍBRIDA: PERCEPCIONES PARA LA RESILIENCIA CORPORATIVA

Cuando se produjo la irrupción de la nube, la mayoría de los pronósticos apuntaban a que la migración de las TI corporativas a ese entorno sería la opción general a corto o medio plazo. Y con la aparición de la nube híbrida, parecía que las reticencias al traslado derivadas de las exigencias de seguridad y cumplimientos estaban salvadas y el camino hacia la migración despejado. Sin embargo, hoy se habla de TI Híbrida. ¿Cuál es la mejor estrategia, optar por la nube híbrida o por la TI híbrida? En este dossier, se analizan las diferentes opciones, para intentar allanar el camino de los CIOs hacia la respuesta que se adapte con mayor precisión a las necesidades específicas de su organización.

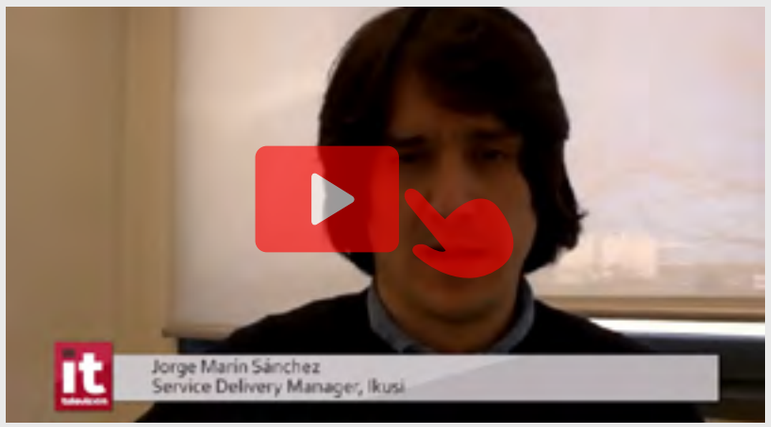
Gestión de entornos multicloud e híbridos, mejores prácticas

“Tratar los datos en los entornos híbridos requiere de una gran capacidad de análisis” (Sothis)

“Apoyamos las necesidades de comunicaciones unificadas basadas en cloud” (NFON)

“Apostamos por una solución que nos permita tener una ventanilla única” (Micro Focus)

“Ayudamos a los clientes a sacar el máximo partido a su transformación digital” (Making Science)



“Las redes inteligentes son uno de los pilares de una estrategia de entornos multicloud” (Ikusi)

“Ayudamos a evitar la repatriación de aplicaciones desde la nube” (Dell Technologies)

“Antes de migrar al cloud hay que prever qué va a ocurrir en el cloud” (Crayon)

making science

BRINGING TECHNOLOGY TO BRANDS

YOUR PARTNER FOR
DIGITAL BUSINESS

www.makingscience.com

#ENCUENTROSITTRENDS

¿Cómo protejo mis activos en un entorno de nube híbrido? Aspectos a tener en cuenta

Uno de los principales escollos del cloud es su seguridad. Así se constata en el informe IT Trends 2021, asimilando la aceleración digital. Un 17% de los consultados adjudica a la seguridad de la nube un papel estratégico para este 2021. Además, la ciberseguridad se considera una inversión prioritaria en estos doce meses. La protección de los datos, las aplicaciones y las infraestructuras que dan acceso y con las que se construyen las nubes híbridas, es una máxima siempre presente en la mente de los responsables tecnológicos de las empresas.

Sobre todo ello debatieron portavoces de Barracuda, Check Point, Commvault, Entrust, Sonicwall y Thales Data Protection, en el Encuentro IT Trends "Ya vivo en la nube, ¿y ahora qué? Mejores prácticas para desenvolverse en entornos de cloud híbridos".

Uno de los primeros puntos que se abordaron en el debate fue la durabilidad de estos

(De izq. a dcha) Elisa Martínez (Commvault), Sergio Martínez (Sonicwall), José Pérez (Entrust), Alfonso Martínez (Thales), Eusebio Nieva (Check Point), Miguel López (Barracuda). Clic para ver

“Muchos clientes creen que el cloud no es tan seguro por la novedad, pero es importante planificar la migración y no dejar que únicamente sean las circunstancias las que nos lleven hacia allí”

MIGUEL LÓPEZ, BARRACUDA

entornos híbridos, un modelo que parece que permanecerá durante mucho tiempo a la luz de las experiencias de los clientes y de las normativas que rigen ciertos mercados. Y así lo deben garantizar las tecnologías que dan soporte a dicho modelo. “Es verdad que existen soluciones 100% cloud, como Office 365 o Salesforce que se despliegan totalmente en la nube, pero también hay situaciones en la que los clientes siguen manteniendo sus aplicativos on premise o legacy, y hay que seguir dándoles protección a estos entornos”, explicó Elisa Martínez, responsable de Metallic para España y Portugal de Commvault, quien se refirió a la normativa de la European Bank Agency, que establece como preceptivo para las entidades financieras que tengan una estrategia de salida del cloud para recalcar la necesidad de acompañar a las empresas allá donde tengan sus activos, “de una manera transparente. Hay que mantener garantizada la calidad de los datos, la integridad de la plataforma y la seguridad del ecosistema”.

Y es que tan seguro puede ser un entorno como el otro, En opinión de Miguel López, Country Manager de Barracuda para la región de Iberia, “todo depende de las medidas que se adopten en cada uno de ellos. El diferencial del entorno de seguridad on premise con el cloud es que este último

it whitepapers

PROTEJA SU EXPERIENCIA EN LA NUBE DE AZURE

Los usuarios de servicios en la nube de Microsoft Azure, pueden tener que enfrentarse a tres grandes retos: garantizar que sus aplicaciones web sean seguras, garantizar que su nueva red en la nube sea segura; y mantener una infraestructura siempre segura. ¿Cómo elegir la solución de seguridad correcta para las infraestructuras de Azure? Este documento explica los criterios para la seleccionar una solución para proteger las aplicaciones y la información en Microsoft Azure y garantizar el cumplimiento de las reglas de seguridad

“Hemos de saber qué herramientas específicas de seguridad tiene que haber en un entorno on premise o en cloud, porque estas herramientas pueden ser específicas de un entorno o de ambos”

EUSEBIO NIEVA, CHECK POINT

ha conseguido democratizar el acceso a la seguridad. Los niveles de seguridad y resiliencia antes eran muy complejos para una empresa pequeña o mediana ya que, para ellas, la seguridad en cloud trae consigo nuevos interrogantes. Muchos clientes creen que el cloud no es tan seguro por la novedad, pero es muy importante planificar la migración y no dejar que únicamente sean las circunstancias las que nos lleven hacia allí”, aconsejó. Y una vez esté claro el plan, “se pueden desarrollar muchos pasos para tener un entorno mucho más seguro que on premise”.

Para tener todos estos entornos bajo control, “es importante contar con herramientas consistentes y homogéneas que permitan desplegar políticas de seguridad y visibilidad en cloud consecuentes con lo que ya tenía la empresa on premise”, sin pasarse por alto algunas administraciones que parecían tener poca importancia.

Aún con todo, “no hay que olvidar que el cloud incorpora nuevas amenazas para los entornos tecnológicos, como las autorizaciones de las administraciones, bajo qué condiciones se suben imágenes o se hace un despliegue de cargas en la nube o qué herramientas de terceros, incluso open source, se despliegan”, apuntó Eusebio Nieva, director técnico de Check Point.

Todo esto era más fácil de controlar on premise. Ahora la mayoría de los problemas surgen por ese tipo de desconfiguraciones. “Siempre

CLOUD SECURITY POSTURE MANAGEMENT

CloudGuard Posture Management permite a las empresas administrar fácilmente la seguridad y el cumplimiento de sus entornos de nube pública a cualquier escala en AWS, Microsoft Azure, Google Cloud Platform y Kubernetes. Además, visualiza y evalúa la actitud hacia la seguridad, detecta configuraciones incorrectas, modela y aplica activamente las políticas estándar y protege contra ataques y amenazas internas. Las organizaciones usan CloudGuard para operaciones de seguridad en la nube más rápidas y efectivas, cumplimiento y gobernanza sin problemas y prácticas de DevOps resistentes.

“De una manera transparente, hay que mantener garantizada la calidad de los datos, la integridad de la plataforma y la seguridad del ecosistema”

ELISA MARTÍNEZ, COMMVAULT

hay que tener en cuenta la parte del perímetro interno o el data center junto con la nube para saber coordinar ambos entornos a la vez y, además, saber qué herramientas específicas de seguridad tiene que haber en uno u otro entorno porque estas herramientas pueden ser específicas de un entorno o de ambos”, destacó. Si una empresa no tiene control, da igual que tenga visibilidad porque va a ser imposible evitar los incidentes.

Además, muchas organizaciones que están en el cloud no son conscientes de la problemática de la protección y la localización de los datos sensibles. En este sentido, Alfonso Martínez, country manager de Thales Data Protection, señaló que “el reto es securizar el entorno híbrido a la vez que el data center y tener visibilidad de los dos mundos. Muchas empresas han saltado a la nube de la noche al día por el miedo tras el año de pandemia y no han podido entrar en este entorno con toda la seguridad que les hubiera gustado”, subrayó. “A eso se le añade que el personal que está usando la nube está sobrecargado y a veces no han sido formados específicamente para manejar estos entornos de nube”. Y ante esto, “es imprescindible herramientas que permitan a las organizaciones descubrir y clasificar su información, independientemente de dónde esté, para luego implementar las medidas oportunas de cifrado, tokenización o enmascaramiento”.

Para José Pérez, Sales Engineer de Entrust, “el cifrado es una herramienta indispensable en el cloud hoy en día y es la última frontera antes de

it whitepapers

7 CONSEJOS PARA PROTEGER LOS DATOS DE TU EMPRESA

La pérdida de datos no es una broma. Los ataques de ransomware y malware van en aumento, pero ése no es el único riesgo. Con demasiada frecuencia, las empresas piensan que sus datos están bien respaldados, pero en realidad no lo están.

Hay formas sencillas de proteger tu organización. Este documento muestra siete razones comunes por las que las empresas pierden datos, a menudo porque nunca estuvieron realmente protegidos, junto con consejos para ayudarte a evitar que te ocurra lo mismo.

“Hay que tener en cuenta qué infraestructuras, qué aplicaciones y qué datos se quieren subir a la nube prestando especial atención a los datos más críticos para añadirles medidas adicionales de seguridad como el cifrado”

JOSÉ PÉREZ, ENTRUST

acceder al dato. El hecho de que las empresas estén sacando datos que tenían dentro de casa hacia afuera, es algo que hace unos años hubiera sido impensable para un auditor. Y otros elementos que explica la importancia del cloud en el cifrados son las regulaciones, como las que tiene que cumplir el sector bancario con PCI-DSS”.

Respecto al acceso a la nube seguro, Sergio Martínez, Iberia Regional Manager de SonicWall, adviertió que “estamos en un momento de aceleración, donde las credenciales son la nueva frontera. Los ataques de ransomware han aumentado en un 60%. Acceder a los recursos de la compañía en remoto, se ha convertido en clave. Hay que desplegar el doble factor de autenticación, pero, ojo, porque los SMS están dejando de ser seguros. Hay que asegurar una defensa por capas para que los dispositivos remotos sean de confianza con un control del endpoint y hacer un enforcement para que los usuarios finales sean de confianza”.

Además, añadió que todo el tráfico ha de ser monitorizado para al menos que en las capas de defensa tradicional sean válidas. “Restituir los end point a las situaciones anteriores es clave. Si todo falla hay que desplegar también antivirus de nueva generación que permitan detectar todo aquello que pueda engañar al usuario”.

Aludiendo a esos volúmenes de ransomware citados por el portavoz de Sonicwall, Elisa Mar-

NUEVAS ESTRATEGIAS PARA LA PROTECCIÓN DE DATOS MULTI-CLOUD

Cifrar los datos de la nube es esencial para proteger la información confidencial y las cargas de trabajo, pero es necesario hacerlo correctamente para ser eficaz y cumplir con los mandatos de cumplimiento. Un reciente informe de Forrester recoge prácticas como el uso de módulos de seguridad hardware (HSM) para almacenar las claves de encriptación de manera independiente a las cargas de trabajo Cloud.

“Hay que asegurar una defensa por capas para que los dispositivos sean de confianza, con control en el endpoint y un enforcement para que los usuarios finales sean de confianza”

SERGIO MARTÍNEZ, SONICWALL

tínez, de Commvault, apuntó que “este año de tremenda aceleración para poder trabajar en casa, ha provocado que se adoptaran multitud de herramientas colaborativas donde la cloud ha sido crítica. Office 365 con Teams y su parte de Exchange han sido uno de los facilitadores y se han convertido en un gran valor para las compañías que las utilizan para gestionar proyectos, contratos u ofertas. Pero lo peor es que un año después de estos despliegues no se tienen en cuenta todas las vulnerabilidades en muchas empresas. Es ahora cuando se están implementando políticas de backup, ransomware y recuperación de la información en el caso de que ocurra, para volver al momento que se encontraba la empresa antes”.

Sobre estos ataques, Miguel López, de Barracuda, señaló que “estamos viendo que el malware funciona en un contexto de coste-beneficio y van a atacar a los eslabones más débiles de la cadena independientemente del tamaño de la compañía, aunque a veces en la prensa solo se vean reflejados los grandes ataques”.

Por esta razón, los CISO demandan ayuda a los proveedores desde el punto de vista de seguridad y, en muchas ocasiones para tener visibilidad, ya que los propios activos en la nube son desconocidos para estos profesionales. “Los departamentos de desarrollo a veces utilizan parte de la nube antes de ofrecer un producto a todos los clientes. Por eso, embeber los controles y los pasos de desarrollo es de lo más importante.

it whitepapers

CÓMO ELEGIR EL FIREWALL DE PRÓXIMA GENERACIÓN PARA PROTEGER TU RED

El firewall ha existido durante más de dos décadas y hoy ha evolucionado hasta convertirse en lo que llamamos un cortafuegos de próxima generación (NGFW). A medida que las empresas investigan NGFW, hay varios factores que deben tenerse en cuenta para asegurarse de que sus redes están debidamente defendidas. Esta guía ayudará a las empresas a elegir el NGFW correcto en función de varios criterios, incluidos características, capacidades de la plataforma, rendimiento y administración.

Esta es una carencia para la mayoría de las compañías", añadió Nieva durante el debate.

Otro punto clave al hablar de la seguridad de la nube es la responsabilidad: "los responsables de seguridad de las empresas tienen que saber securizar los datos después de haberlos subido a la nube. El último responsable de sus datos es la empresa no el proveedor de nube. Se puede proteger con muchos sistemas y controles, pero, si todo falla, hay que cifrar archivos, carpetas y aplicaciones. Es importante que los clientes tengan la posibilidad de compatibilizar nubes ya sea Amazon, IBM Cloud, Google Cloud o la que sea para configurar su propia estrategia", destacó durante la mesa redonda el country manager de Thales Data Protection.

Como remate al encuentro, José Perez, de Entrust, señaló que "l mejor consejo para una empresa es que se deje asesorar por expertos en cloud para poder hacer esa migración. Después hay que tener en cuenta qué infraestructuras, qué aplicaciones y qué datos se quieran subir prestando especial atención a los datos más críticos con medidas adicionales de seguridad, como el propio cifrado".

Para ver la charla completa, accede aquí.

"Son imprescindibles herramientas que permitan descubrir y clasificar información, independientemente de dónde esté, para luego implementar las medidas oportunas de cifrado, tokenización o enmascaramiento"

ALFONSO MARTÍNEZ, THALES DATA PROTECTION

it whitepapers

LAS BASES PARA LA PROTECCIÓN DE DATOS SENSIBLES EN CUALQUIER ORGANIZACIÓN

Con la proliferación de datos en la actualidad, el auge de los reglamentos de privacidad, el aumento en el uso de la nube y la persistencia de amenazas avanzadas, una seguridad centrada en los datos permite tener el control de los datos sin importar dónde estén y evitar así que los ladrones de datos los puedan leer. Pero, para ser efectiva, esta protección debe actuar automáticamente sin depender de la intervención del usuario. Este libro blanco se centra en los desafíos que supone la seguridad de los datos en esta era de proliferación de datos. También ofrece estrategias para localizar y clasificar sus datos críticos y aplicarles una seguridad centrada en los datos.

Si te ha gustado este artículo, compártelo

¿Cómo proteger mis activos en un entorno de cloud híbrida?

“La seguridad de los datos comienza con su localización” (Thales)

“La seguridad SASE Zero Trust es el nuevo paradigma” (SonicWall)

“No es buena idea migrar la nube sin cifrado” (Entrust)

“Las plataformas de backup y recuperación deben asegurar la integridad de la información” (Commvault)

“Lo más importante es una protección unificada y nativa en la nube” (Check Point)

“Proponemos herramientas para tener seguridad, visibilidad y control también en la nube” (Barracuda)

ACCEDIENDO A UNA NUBE SEGURA

LA CONEXIÓN EN LA NUBE NO SIGNIFICA MENOS PROTECCIÓN

ENTRUST

ENTREVISTA

“Necesitamos modelos de infraestructura centralizada que permitan la transformación digital plena en la Universidad”

ANDRÉS PRADO, CRUE UNIVERSIDADES ESPAÑOLAS

La pandemia ha impulsado la transformación digital. También en el ámbito académico, uno de los más perjudicados por la Covid. Ahí es donde el Plan Director 2020, comenzado en 2018 por la conferencia de rectores Crue Universidades Españolas, ha resultado ser visionario. La importancia otorgada en el mismo a tendencias como blockchain y su aplicación en la Universidad, lucen hoy como un faro en la carrera acelerada hacia la adopción de una tecnología que nos ayude a navegar los convulsos tiempos que nos ha tocado vivir. Andrés Prado, Coordinador del grupo de trabajo “Dirección de TI” en Crue, repasa algunas de las claves de este fascinante proyecto.

Arancha Asenjo y Alberto Varet

Uno de los ambientes más trastocados por la pandemia es el de la educación. ¿Cómo conseguir formar a los estudiantes sin clases presenciales? ¿De qué manera pueden las innovaciones digitales solventar los problemas derivados de la Covid? Como si hubiera previsto tan penosa situación, Crue Universidades Españolas, una asociación sin ánimo de lucro formada por 76 instituciones nacionales (50 públicas y 26 privadas), puso en marcha, en 2018, el Plan Director 2020, una estrategia dirigida a estructurar acciones que aplicasen la tecnología a la vida universitaria. El tiempo y las circunstancias han acabado por darle la razón a sus responsables dos años después.

Uno de ellos es Andrés Prado, Coordinador del grupo de trabajo "Dirección de TI" en Crue Universidades Españolas, quien asegura que el valor de esta conferencia de rectores está en "su capacidad para ser la voz de referencia de las universidades con todos los agentes que tienen implicación en el sistema español de educación, investigación y transferencia". Una situación de privilegio que tiene, hoy más que nunca, un fuerte componente tecnológico que el entrevistado desgrana de esta manera: "Crue se estructura en torno a comisiones sectoriales compuestas por expertos dentro del ámbito universitario. Estos son responsables de las actividades que nuestra agrupación considera esenciales. Una de ellas es la

"Tratamos de diseñar un plan director o de actividad centrado no en la tecnología en sí misma, sino en los distintos ambientes de actuación con ellas"

tecnología, de la que surge la sectorial de TI, que tiene tres ejes fundamentales: el primero es el asesoramiento sobre su adopción en las misiones universitarias; el segundo, la evaluación de la capacidad tecnológica aplicable en docencia, investigación y gestión universitaria; y el tercero, el establecimiento de un elemento de colaboración entre esos proyectos con un marcado componente tecnológico".

La aguja que enhebra estos tres puntos es el citado Plan Director 2020, elaborado a iniciativa del rector de la Universidad de Jaén, quien pretendía impulsar una idea que fuera más allá de la asistencia de grupos de trabajo. El resultado acabó por dar visibilidad a la estrategia de Crue en el ámbito tecnológico desde una perspectiva claramente tangencial. "Tratamos de diseñar un plan director o de actividad centrado no en la tecnología en sí misma, sino en los distintos ambientes de actuación con ellas. Nuestra labor, pues, ha ido dirigida a estructurar todo ese tipo de acciones en torno a los susodichos ejes estratégicos, pero no tanto desde el punto de vista de las tendencias como de su aplicación en la universidad", argumenta el Director TIC.

Una esmerada tarea que consta de seis grandes bloques:

1. **Gestión de las TIC en el entorno universitario:** "Tratamos de identificar modelos de referencia en sociedad para luego adoptarlos en las diferentes instituciones".
2. **Tres grandes ejes relacionados con la actividad académica:** "La tecnología en la docencia, el ámbito de la investigación (donde se ha abrazado el prototipo europeo Open Science o ciencia abierta) y la aplicación de las innovaciones en la gestión universitaria".
3. **Administración digital:** "Buscamos un acercamiento a la comunicación en la Universidad marcada por conceptos como la movilidad o la conexión permanente".
4. **Gobierno del dato:** "Se ha trabajado en reconocer diferentes patrones para después decidir cuál era el más flexible a la hora de ser adaptado a las instituciones".
5. **Cultura digital:** "En el más amplio término. Aquí tuvimos en cuenta otro de los elementos más fundamentales en los últimos años: el de las competencias digitales. Es decir, esos temas más candentes que las universidades han tenido que ir adoptando".

6. Empoderamiento de los profesionales de la tecnología en nuestro medio: "Este último año, muchas de las instituciones han puesto en valor nuestras actividades. Nos estamos convirtiendo en una pieza fundamental dentro de esos espacios tan complejos que son las universidades".

Seis verticales muy estimulantes que, sin embargo, pueden ser un quebradero de cabeza a la hora de llevarlos a la práctica. ¿Cómo hicieron desde Crue para financiarlos y ejecutarlos? "Financiación hay poca. Es una labor puramente altruista de profesionales del sector que entienden que en el trabajo conjunto hay beneficio para todos. Es verdad que luego hay iniciativas que tienen un desarrollo más allá de la sectorial y que acaban por convertirse en un proyecto en sí mismas. Incluso en soluciones que sí terminan por llevar una línea de financiación. Pero nuestra labor es de asesoramiento, identificación de buenas prácticas y de tratar en muchos casos que esas buenas prácticas tengan una facilidad de adaptación y adopción por cada una de las universidades".

"Nuestra labor es de asesoramiento, identificación de buenas prácticas y de tratar en muchos casos que esas buenas prácticas tengan una facilidad de adaptación y adopción por cada una de las universidades"

La valía de semejante esfuerzo fue refrendada por el duro y atípico año 2020. Andrés Prado explica cómo llegaron a alcanzar unos números que incluso les sorprendieron a ellos mismos: "El 95% de los 73 proyectos propuestos fueron abordados a pesar de la pandemia, y 44 de estos se han culminado con éxito. Un resultado muy satisfactorio, sobre todo si tenemos en cuenta que algunas de estas líneas de acción tienen aún recorrido".

Una de esas líneas relaciona blockchain con la universidad. Se llama BLUE y ha surgido "de una dinámica de lanzar informes para poner en contexto la tecnología en la universidad". "Fue algo así como un pequeño análisis estratégico en el que incorporábamos diferentes puntos de vista para saber dónde y cómo adoptar blockchain en las instituciones educativas. El trabajo contó con la colaboración coordinada de RedIRIS (red española para Interconexión de los Recursos InformáticoS de las universidades y centros de investigación). Gracias a ellos, avanzamos en la mejora de procesos centrados en la actividad del estudiante. Y luego, tuvimos la suerte de coincidir en el tiempo con una iniciativa a nivel europeo llamada EBSI (The European Blockchain Services Infrastructure), que empezamos asimismo a coordinar, y que tiene un caso de uso dedicado a las certificaciones académicas", expone Andrés Prado.

Aparte de blockchain, la labor con RedIRIS se extiende a otros proyectos también de suma importancia para nuestro país que el entrevistado explica así: "Con ellos y el Ministerio de Universidades trabajamos igualmente para que las líneas de financiación puedan aportar novedosos mecanismos de transformación dentro del sistema universitario español. Es decir, que sean propuestas para mejorar como sistema, pues estamos viendo que hay una verdadera necesidad de adoptar modelos de infraestructura centralizada y consumo distribuido y personalizado que permitan acceder a una transformación digital plena en nuestro ámbito".

Sí, el famoso cambio de paradigma que tantas veces nos ha llevado a preguntarnos por el estado de las cosas en el mundo empresarial es igualmente palpable en el ambiente de la Universidad desde, al menos, 2018. "El informe TIC 360 de hace dos años trataba,

justamente, de la transformación digital de las universidades. Ahí estaban nuestras reflexiones sobre cómo enfocar las cosas en el presente para poder evolucionar en el futuro. 2020 ha puesto de manifiesto la pertinencia de nuestro estudio, así como el estado real de la digitalización de las universidades. El caso es que nunca tuvimos mayor visibilidad en la comunidad universitaria como hoy. Tampoco hubo nunca tanta aceptación de nuestros servicios y adopción de los mismos. Hemos tenido unos reconocimientos insólitos. En el fondo, este año sirvió para poner de manifiesto el valor de los proyectos en los que trabajamos durante mucho tiempo. Unos proyectos que han elevado la cultura digital universitaria", asegura el Director TIC.

Un triunfo meridiano de la propuesta de Crue que nos recuerda que la ruta hacia la digitalización es tan solo un camino que hemos empezado a andar, y que será demasiado arduo sin nuevas vías de financiación. En palabras de Andrés Prado: "Enriquecería mucho en el medio universitario la adopción digital en términos generales. Hablo de consumo de infraestructuras de software como servicio. Creo que ese ámbito personalizado es importante trabajarlo en la educación. Aparte, es necesario hacer una reflexión madura sobre las estructuras de las organizaciones y, dentro de las mismas, de las áreas de innovación. Capacitar a los profesionales en un entorno que se mueve imparable y en el que sus propios roles dentro de la universidad no dejan de evolucionar. La tecnología no se gestiona hoy como hace veinte años, y eso nos debe hacer reflexionar. Es un pilar fundamental para el desarrollo de la actividad universitaria".

La universidad, pues, no sólo como un foco de conocimiento, también como una palanca de la revolución digital en la que vivimos inmersos. ¿Pueden, entonces, ser las instituciones educativas generadoras de ese talento que tantas veces se demanda? Andrés Prado lo tiene claro: "Por supuesto. Las universidades han fortalecido los ambientes de emprendimiento. Esas misiones deben tener cabida igualmente en la universidad moderna. Que ésta no sólo sea transferencia, sino también capacidad para el emprendimiento".■

"Las universidades han fortalecido los ambientes de emprendimiento. Esas misiones deben tener cabida igualmente en la universidad moderna. Que ésta no sólo sea transferencia, sino también capacidad para el emprendimiento"

MÁS INFORMACIÓN

- CRUE Universidades Españolas
- El futuro de la educación pasa por un modelo de enseñanza híbrido
- La educación contribuye a frenar la caída del mercado de redes inalámbricas

Si te ha gustado este artículo, compártelo

Aryse 360°

UNA SOLUCION INTEGRAL AVANZADA PARA TODAS TUS NECESIDADES

Te presentamos Aryse360º, la única solución integral de la industria que unifica Conectividad, Seguridad y Colaboración para que solo tengas que preocuparte por tu negocio.

www.aryse360.com

Cuota mensual
Todo Incluido, HW, SW,
Mantenimiento y
Servicios profesionales

OPINIÓN

Diez empresas Big Tech con aplicaciones prácticas de computación cuántica

Jorge Díaz-Cardiel,
Socio director general de
Advice Strategic Consultants

Abu Dhabi comienza a construir la primera computadora cuántica de los Emiratos Árabes Unidos (UAE); el laboratorio que construye la computadora cuántica también tiene como objetivo producir microchips 'hechos en Abu Dhabi' para fines del verano de este año. Lo más significativo es que Abu Dhabi ha comenzado a fabricar su propia computadora cuántica con el objetivo de generar avances en el descubrimiento de fármacos y tecnología de baterías. Es decir, que hay una finalidad comercial, práctica. Y esto es un grandísimo avance: cuando aquí, en IT User publicamos sobre computación cuántica el 1 de octubre de 2019, aún no había aplicaciones prácticas, versus la computación "tradicional". Y, dejamos claro que la "Ley Moore" seguía siendo plenamente vigente.

El nuevo CEO de Intel Corporation, Pat Gelsinger, va a invertir 20.000 millones de dólares en recuperar el liderazgo que le disputan Nvidia, QUALCOMM, Samsung o Huawei. Para ello, Intel incrementará su dependencia del "outsourcing" en fabricación y renovará sus esfuerzos para proveer semiconductores a terceros. Pat Gelsinger es nuevo CEO, pero no es nuevo en Intel, donde trabajó 30 años con la "vieja guardia" de Andy Grove, "para quien, solo los paranoicos sobreviven". Y no le falta razón. En los últimos años, Intel abandonó sus valores y cayó en la autocomplacencia. Una parte de esa inversión de Intel será destinada a la computación cuántica.

"Y los de Abu Dhabi, con ciudades digitalizadas y rascacielos que tocan el cielo", se lanzan a la búsqueda de aplicaciones prácticas para la computación cuántica, que es el Santo Grial de las Tecnologías de la Información y Digitalización. En nuestro artículo de 2019, Google había hecho experimentos para la NASA (que publicamos en primicia en España en IT User) y decía que "lo llevado a cabo, hubiera costado 10.000 millones de años a la computación tradicional". Recientemente, "los chinos", sin especificar quienes porque son 1.500 millones..., afirman que han desarrollado una computadora cuántica "un billón de veces más rápida que aquella de Google". El que no corre... ¿vuela?

El Instituto de Innovación Tecnológica de Abu Dhabi, el brazo de investigación aplicada del Consejo de Investigación de Tecnología Avanzada de Abu Dhabi, está construyendo la computadora en sus laboratorios del Centro de Investigación Cuántica, en colaboración con Qilimanjaro Quantum Tech, con sede en Barcelona. Barcelona..., España. "Estamos en la cúspide de una nueva era con el advenimiento de la computación cuántica", dice Faisal Al Bannai, secretario general del Consejo de Investigación de Tecnología Avanzada.

En la misma línea, la computación cuántica representa "la capacidad de condensar décadas o incluso siglos de procesamiento numérico, en minutos", asevera un informe compilado por la Cumbre del Gobierno Mundial y PwC.

El laboratorio en Abu Dhabi había optado por usar qubits superconductores, que es la misma tecnología que Google e IBM están usando para construir sus computadoras cuánticas. Pero la computación cuántica es un campo más nuevo, popularizado por el físico teórico John Preskill, a quien se le ocurrió una formulación de supremacía cuántica, o la capacidad de las computadoras cuánticas para hacer cosas que no son posibles para las computadoras ordinarias. Desde entonces, las economías más grandes del mundo, de EE.UU., Rusia, China y Japón, así como los grandes de la tecnología IBM, Alibaba, Facebook y Google, han estado luchando por la supremacía en el campo de la computación cuántica.

Pero hasta ahora, solo se han solucionado problemas computacionales muy limitados con la finalidad de probar la velocidad. Las computadoras cuánticas aún no son capaces de resolver problemas prácticos-prácticos, muy prácticos: no saben poner la lavadora, por ejemplo.

Pero, cuando lo hacen, su potencial es enorme y puede acelerar rápidamente el descubrimiento humano. Por ejemplo, dado que las computadoras cuánticas pueden simular y diseñar estructuras moleculares a nivel atómico, uno podrá ver cómo funcionará un nuevo medicamento en un ser humano, eludiendo algún día las pruebas en humanos o animales.

Una computadora cuántica podría algún día responder preguntas sobre los orígenes del universo y preguntas persistentes sobre el espacio y el tiempo, que ahora solo "vemos" en películas como "Interstellar" o "Timeline".

Como dijimos más arriba, en 2019, Google afirmó que construyó la primera máquina en lograr la "supremacía cuántica"; es decir, una computadora que fue la primera en superar a las mejores supercomputadoras del mundo en el cálculo cuántico. Su prototipo de computadora cuántica completó en menos de cuatro minutos un cálculo que a una supercomputadora le habría llevado 10.000 años completar.

Otros, como IonQ Inc. se están preparando ya para convertirse en la primera empresa que cotiza en bolsa y se centra específicamente en la comercialización de la computación cuántica. Y su camino hacia la Bolsa de Valores de Nueva York es a través de un acuerdo de adquisición con fines especiales (SPAC) que valora la entidad combinada en aproximadamente 2 billones de dólares. IonQ Inc. es una startup de computación cuántica con sede en College Park, Maryland, y se convertirá en la primera empresa que cotiza en bolsa, enfocada totalmente en la comercialización de hardware y software de computación cuántica.

Aunque no es la única empresa. Microsoft Corp., IBM, D-Wave Systems Inc, Amazon, Alibaba, Facebook SpaceX y Google (Alphabet) están compitiendo para construir la primera computadora cuántica escalable de grado comercial. Facebook quiere una Inteligencia Artificial más rápida: al aprovechar el poder de la física cuántica, las computadoras cuánticas ofrecen la promesa de lanzar cálculos algorítmicos complejos para aplicaciones de inteligencia artificial al hiperespacio. Que son aplicaciones en las que Elon Musk (Testa SpaceX) y Jeff Bezos (Amazon) también están trabajando.

Cuando el río suena, agua lleva, dice el refrán. Una docena de grandes empresas tecnológicas norteamericanas desarrollando aplicaciones prácticas de computación cuántica es algo que tomarse muy en serio. Aunque la computación cuántica no sepa aún hacer la colada o llenar el lavavajillas. ■

MÁS INFORMACIÓN

- El gasto en computación cuántica se multiplicará por 35 en la próxima década
- DARPA lanza un programa para acelerar la tecnología de cifrado homomórfico
- Computación cuántica para ayudar a la cadena de suministro automotriz
- Taiwán quiere ser una potencia cuántica

8
ABRIL
11:00 CET

REGISTRO

Sophos ZTNA:
securizando el acceso a organizaciones en cualquier lugar

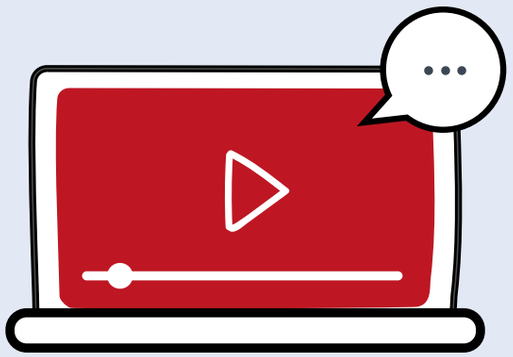
ON DEMAND

Sophos aborda la problemática actual de seguridad a la que se enfrentan las empresas, con un mayor volumen de ataques y la necesidad de extender las medidas de protección a una organización dispersa. Explica, además, qué es Sophos ZTNA (Zero Trust Network Access).

REGISTRO

Operaciones y Kubernetes
Infraestructura para cargas nativas en Cloud

La adopción de Kubernetes está permitiendo a las empresas implementar y administrar contenedores y, al mismo tiempo, administrar aplicaciones heredadas obteniendo ventaja competitiva, capacidad de innovación y productividad en sus entornos de desarrollo.



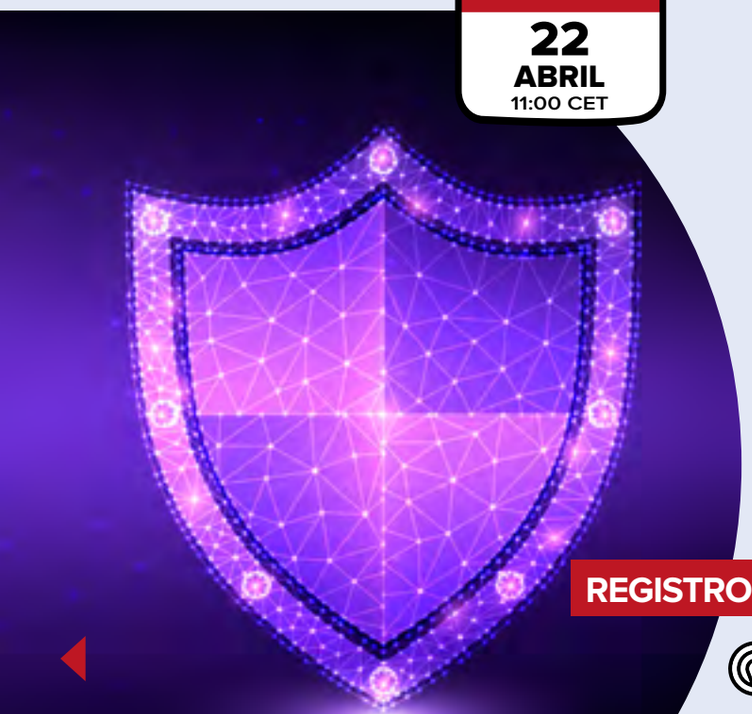
#ITWEBINARS

Aplicaciones,
¿cómo desarrollo y entrego mi mejor software?

6
MAYO
11:00 CET

Porque las aplicaciones son hoy -más que nunca- la cara del negocio...
Únete a este Encuentro IT Trends con expertos y conoce las mejores prácticas y todos aquellos aspectos a tener en cuenta cuando se desarrollan aplicaciones y software, así como a la hora de ponerlos en producción y administrarlos.

22
ABRIL
11:00 CET



REGISTRO

Cómo hacer avanzar y proteger la empresa digital

El mercado de la ciberseguridad está adoptando nuevos o renovados planteamientos para obtener visibilidad de lo que ocurre en la red. En este webinar abordaremos los principios de las tecnologías de EDR, NDR, SIEM y SASE y sus capacidades para proporcionar la seguridad que toda empresa digital necesita.

REGISTRO

ImpresiÓN Digital

CENTRO DE RECURSOS

it

Beneficios de los servicios gestionados de impresión

brother

Beneficios de los servicios gestionados de impresión para empresas y empleados

Los servicios gestionados de impresión son mucho más que una simple solución de alquiler de impresoras. Son soluciones ofrecidas por los principales proveedores de impresión, como Brother, para ayudar a las empresas a gestionar y controlar sus equipos, entre los que se incluyen escáneres, faxes e impresoras multifunción.

Para muchas empresas, la instalación, el mantenimiento y la actualización de sus impresoras puede ser una tarea compleja, que pocas personas pueden llevar a cabo. Por eso las compañías están optando por los servicios gestionados de impresión (MPS,) para simplificar la gestión de sus impresoras y controlar los costes. Como señala Brother, gracias a su flexibilidad y adaptabilidad, las pequeñas empresas también pueden beneficiarse de los servicios gestionados de impresión, cuyos principales beneficios son cinco.

MENOS MOLESTIAS

Muy pocas empresas tienen a su disposición un experto en impresión encargado de gestionar y mantener los equipos instalados. Esto implica una dedicación de tiempo que podría ser empleado en otras tareas más relevantes del negocio. Afortunadamente, un servicio gestionado de impresión evita estas molestias a cualquier compañía.

La gestión completa de las impresoras, incluyendo la provisión de un servicio de aten-

ción al cliente que ha contratado un servicio gestionado de impresión dedicado, a la gestión de consultas y problemas relacionados con la impresión, reduce la gestión y libera tiempo al equipo de TI de las empresas. La supervisión remota, combinada con el servicio automatizado, alertas sobre averías y estado y reposición de los consumibles, garantizan que los usuarios puedan centrarse en sus tareas diarias. Además, en caso de incidencias, el servicio técnico telefónico y el nivel de servicio de reparación acordados previamente garantizarán un tiempo de inactividad de la impresora mínimo.

ADIÓS CAPEX, HOLA OPEX

La tecnología avanza más rápido que nunca, y algunos equipos no tardan mucho en quedarse obsoletos. Esto significa que, si una compañía invierte mucho presupuesto en la adquisición de estos equipos, el coste de adaptarse al ritmo al que avanza la tecnología y a sus cambios acelerados puede ser muy elevado. Estos servicios de pago por uso permiten transformar las operaciones de impresión de gastos de capital (CapEx) a gastos operativos (OpEx), reemplazando esa inversión significativa de capital y los costes variables de funcionamiento continuo por cuotas mensuales fáciles de provisionar.

Además, los proveedores de servicios gestionados de impresión no sólo recomendarán el mejor hardware que se adapte a cada empresa, sino que también le recordarán cuándo actualizar los equipos para contar siempre con la última tecnología.

¿QUÉ SON LOS SERVICIOS GESTIONADOS DE IMPRESIÓN?

MAYOR SEGURIDAD

Un aspecto importante que se debe tener en cuenta al considerar contratar la impresión en modo servicio es identificar los posibles riesgos de seguridad para diseñar un plan de seguridad a medida de cada empresa, con el fin de evitar cualquier ciberataque o violaciones en la privacidad de los datos. Desde restricciones en las funcionalidades hasta la implementación de nuevos protocolos de impresión; una seguridad en la impresión más inteligente puede cerrar cualquier brecha.

Asimismo, se debe insistir en que los dispositivos en red tengan integradas funciones de seguridad de alto nivel, como la protección a través de tarjetas NFC o un código PIN, así como la encriptación a nivel corporativo para proteger la información confidencial que se esté manejando.

REDUCCIÓN DEL IMPACTO MEDIOAMBIENTAL

Si lo que se busca es reducir el impacto sobre el medioambiente, la impresión en modo servicio ayuda a gestionar y controlar la cantidad de papel, energía y consumibles que se usan. La recogida y el reciclaje de los consumibles usados es una opción que puede añadirse como parte del servicio contratado.

Además de reducir los residuos, las soluciones de MPS facilitan el seguimiento y el control del uso de la impresión, y ayudan a identificar las áreas en las que puede optimizar su uso y a aplicar las mejores prácticas para el usuario.

VISIBILIDAD Y CONTROL

Los servicios gestionados de impresión no solo ofrecen una infraestructura de impresión que garantiza la disponibilidad de un equipo y la capacidad de atender el volumen de uso que

La oportunidad de la seguridad de la impresión como servicio

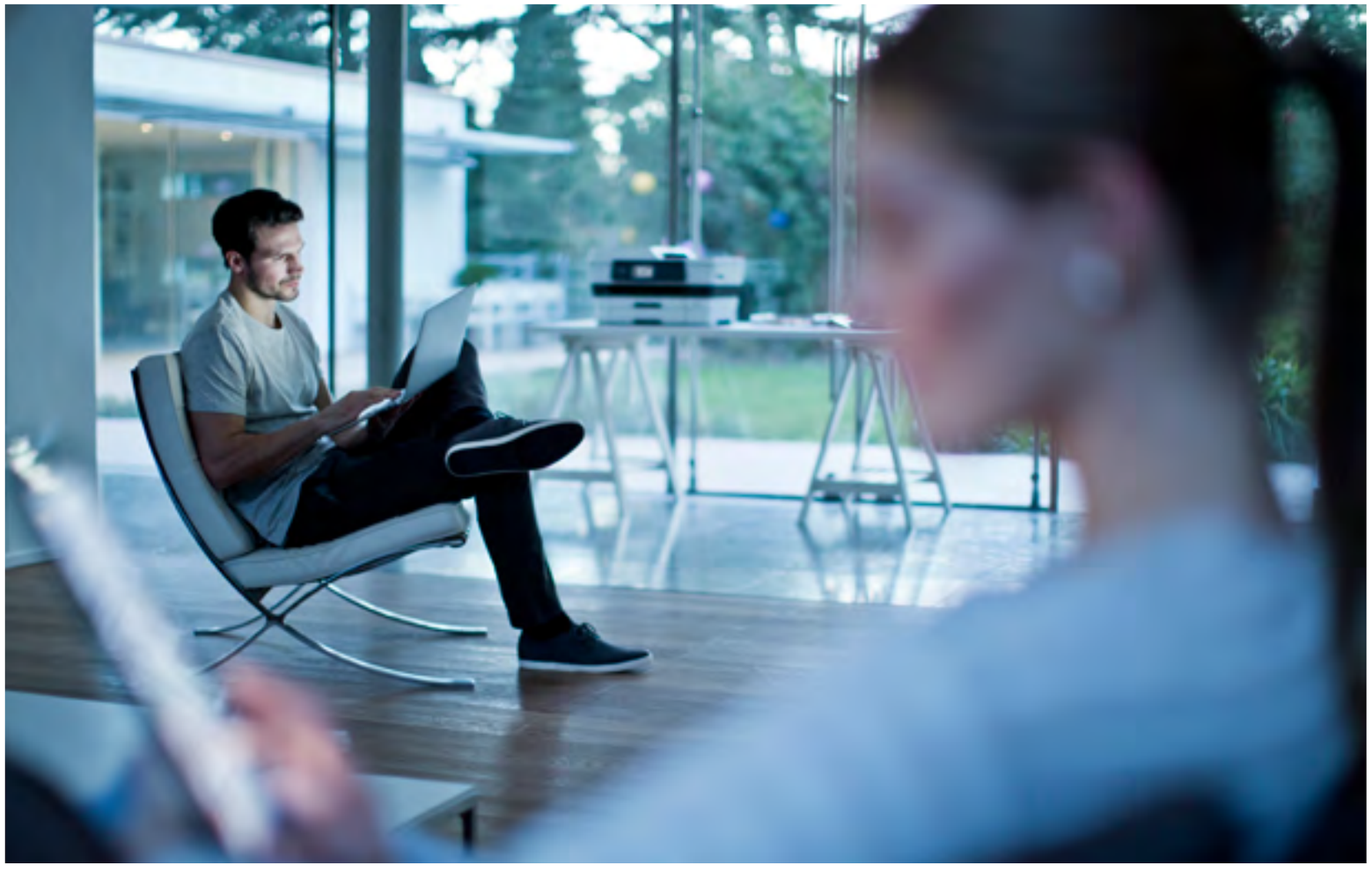
Los responsables de adquirir soluciones de impresión consideran la experiencia en seguridad y las credenciales al seleccionar un proveedor de servicios de impresión gestionados (MPS). La mayoría de los encuestados ya habían incorporado o planeado incluir la seguridad como parte de su contrato de MPS. Sin embargo, cada vez hay más expectativas por parte de los compradores de que los dispositivos de impresión deben ser seguros y que las soluciones y servicios relacionados también serán compatibles de facto. Los proveedores se verán envueltos en una carrera hacia abajo en términos de ofrecer el coste por página más bajo con el número máximo de prestaciones, incluida la seguridad.

IDC cree que hay una ventana de oportunidad para que los proveedores opten por el valor añadido de proporcionar servicios de impresión seguros. El cumplimiento normativo ya no es un proyecto único, sino una parte de la gestión de la infraestructura de impresión y algo con lo que las organizaciones necesitan ayuda constante y continua. Al ofrecer seguridad de la impresión como servicio, ya sea como una sola oferta o como parte de un contrato MPS, los proveedores pueden mejorar y profundizar la relación con el cliente y potencialmente asegurar negocios a largo plazo y más rentables.

Sin duda, la seguridad de impresión empresarial es cada vez más robusta, pero no es impenetrable y los hackers no se quedan parados. Se están produciendo infracciones relacionadas con la impresión y, sin embargo, las impresoras todavía a menudo se pasan por alto como puntos débiles de la red. Los proveedores deben crear conciencia y temor en torno al hecho de que las impresoras son vulnerables y ofrecer los servicios, las garantías y la tranquilidad que los clientes necesitan.

cualquier empresa requiere, sino que también permiten realizar un seguimiento detallado del uso de cada impresora.

Lo más importante es encontrar un proveedor que ofrezca estos servicios a través de la nube para poder monitorizar los equipos de forma constante. Desde la recopilación de datos, pasando por el uso por parte de los empleados, hasta las alertas automáticas sobre la necesidad de sustituir los consumibles. Esta información se refleja en informes regulares que el proveedor debe ofrecer con el fin de identificar oportunidades para optimizar la infraestructura de impresión y tomar realmente el control de los gastos relacionados con la impresión de toda una empresa, independientemente de su tamaño. ■



MÁS INFORMACIÓN

- Toda la información sobre el mercado de impresión
- Cuál es la propuesta de Brother para el mercado de impresión
- Cómo proteger la impresión distribuida híbrida
- Era post-pandemia, una oportunidad para reinventar el negocio
- Inteligencia artificial, ¿cómo afecta al mundo de la impresión?
- La importancia de la seguridad en el mundo de la impresión

Solución de impresión para entornos hiperdistribuidos

Para la mediana y gran empresa con empleados en **teletrabajo**

9,90 € empleado/mes*

Descubre más >

*Precio por puesto de trabajo basado en 25 equipos, modelo MFC-L2710DW, con un contrato a 4 años y un volumen de 200 páginas/mes. Impuestos no incluidos.

“LAS EMPRESAS ESTÁN ADOPTANDO EL MODELO DE DIGITALIZACIÓN DISTRIBUIDA”

JOSÉ RAMÓN SANZ, RESPONSABLE DE MARKETING DE PRODUCTO DE BROTHER IBERIA

2020 ha sido un año atípico, marcado por la pandemia. ¿Cómo va a evolucionar 2021?

Ésta es la pregunta que nos estamos haciendo todos y que, ahora mismo, tiene una difícil respuesta. No obstante, por cómo están transcurriendo los primeros meses del año se puede decir que 2021 tendrá un comportamiento diferente en la primera mitad y en la segunda.

En los primeros seis meses del año todavía va a haber una serie de elementos que afecten a la movilidad de las personas, con lo que esto supone para muchas industrias. A medida que el plan de vacunación avance, la incidencia de la pandemia se reduzca y la presión en el sector sanitario se vaya relajando, lograremos tener una situación más parecida, aunque no igual, que en 2019.

¿Qué implicaciones va a tener esta situación en el sector tecnológico?

Desde Brother creemos que este año se va a fortalecer el componente tecnológico dentro de las empresas.

A esto hay que unir que, una vez que se haya superado la pandemia y se hayan relajado las medidas sanitarias para frenar los contagios, el teletrabajo tendrá su propio peso en la organización del trabajo en las empresas. De hecho, ya existen muchas organizaciones que han adoptado modelos de trabajo mixto, dotando a sus profesionales de elementos técnicos para que puedan realizar sus funciones desde cualquier lugar.

A pesar de esta realidad, todavía quedan empresas que tienen que hacer esta adaptación y fortalecer estas áreas tanto en la oficina como en los hogares. Lo que está claro es que el teletrabajo ha llegado para quedarse.

"EL TRABAJO MIXTO IMPULSARÁ LA IMPRESIÓN DISTRIBUIDA"

¿Cuáles son las tendencias que van a marcar el mercado de impresión en un escenario post-COVID?

En el mundo de las empresas se observan dos tendencias claras. Por un lado, la vuelta a la oficina. Muchas personas que en la actualidad se encuentran todavía teletrabajando volverán a su puesto de trabajo presencial de forma progresiva.

Por el otro, las empresas tendrán que seguir manteniendo una serie de medidas para evitar la confluencia excesiva de las personas o que los dispositivos sean compartidos por varios trabajadores.

La consecuencia es que las empresas adoptarán lo que en Brother denominamos una digitalización distribuida.

¿En qué consiste la digitalización distribuida?

A grandes rasgos, la digitalización distribuida consiste en que, en vez de tener un equipo centralizado, donde todo el mundo confluye a la hora de recoger sus trabajos de impresión o sus actividades de escaneado, se dispone de múltiples equipos más compactos, más pequeños, pero que ofrecen las mismas funcionalidades para que todas las personas puedan hacer su trabajo.

En vez de disponer de un único punto de impresión por planta, habrá dos o tres con el fin de prevenir contagios.

¿Cómo va a influir el teletrabajo en el mundo de la impresión?

Como he mencionado con anterioridad, la tendencia es que las empresas implanten modelos de trabajo mixto. Los empleados desempeñarán sus funciones unos días desde la oficina y otros desde su casa, con lo que eso implica para la organización. Esos hogares todavía hay que dotarlos de equipamiento tecnológico que permita desarrollar la actividad laboral manteniendo los niveles de productividad y, sobre todo, con seguridad.

En 2020 se produjo un desarrollo de compras de productos tecnológicos para paliar el déficit de tecnología que tenemos en los hogares. Estas adquisiciones no son suficientes para lograr toda la productividad que una persona tiene en la oficina. Las empresas también tienen que desarrollar una serie de sistemas a la hora de asesorar, organizar, comprar ese tipo de equipamiento.

¿Qué tendencias de impresión dominarán el ámbito doméstico?

Hemos hablado de las empresas que compran o facilitan equipamiento lógico a sus empleados, pero también dentro de ese trabajo en casa se encuentran las personas que en si mismas son autónomas, que trabajan por su cuenta, y que han hecho de su hogar el centro de su trabajo. Se va a producir una duplicidad de equipos y todo esto hay que prepararlo desde un entorno más doméstico.

En el ámbito de los hogares también existe otro fenómeno que afecta a la impresión o a la digitalización en el domicilio. Se trata de la Escuela en Casa. A pesar de que poco a poco los estudiantes volverán a sus cen-

LA IMPORTANCIA DE LA GESTIÓN DOCUMENTAL PARA LA CONTINUIDAD DE LOS NEGOCIOS

JOSÉ RAMÓN SANZ, Responsable de Marketing de Producto de Brother Iberia

El confinamiento y el teletrabajo han hecho que la gestión documental esté cada vez más extendida, ya que todos nos hemos visto obligados a sumergirnos en este proceso por la distancia generada. Hasta hace cinco años, la gestión documental era algo propio de las empresas (sobre todo de las grandes), y consistía en tener un equipo dedicado a la digitalización de documentos, con herramientas sofisticadas, y procedimientos para digitalizar los documentos en papel. Es decir, cuando un empleado necesitaba digitalizar un documento tenía que recurrir a esos equipos, que luego se encargaban de subirlos a los directorios de la empresa.

Afortunadamente esta situación ha cambiado, y este cambio ha venido acompañado en nuestro país por un incremento de las ventas de los equipos multifunción con capacidad de digitalizar documentos, y de los escáneres documentales, que se han convertido en soluciones más democratizadas que facilitan la digitalización de documentos a cualquier usuario. Además, según datos de IDC 2020, el 57% de los escáneres que se venden vienen equipados con tarjeta de red o WiFi, por lo que cualquiera podemos digitalizar un documento, tanto desde dispositivos móviles como a un equipo conectado en la red corporativa.

Puedes leer la tribuna de opinión entera en este enlace

tros de estudios, se prevé que ciertas materias continúen impartiéndose de manera online, o cada vez haya más cursos que se realicen a través de Internet.

Durante la pandemia hemos comprobado cómo han cambiado los hábitos de impresión en lo que a estudiantes se refiere. Anteriormente el equipamiento que había en los hogares era muy básico y, ahora, se requiere de equipos más sofisticados para satisfacer la demanda de este colectivo.

En lugar de equipos muy básicos y muy baratos se está pasando a equipos con más prestaciones que den servicio a todas las personas que conforman el hogar.

¿En qué áreas se va a centrar su compañía este año?

En Brother estamos trabajando en nuevas soluciones que satisfagan las necesidades de la oficina en casa. El teletrabajo ha llegado para quedarse y nuestras soluciones cubren tanto las necesidades que tienen las empresas como la que demandan las personas.

También estamos trabajando en reforzar nuestra oferta de impresión distribuida. Nuestros próximos lanzamientos facilitarán la impresión como servicio. Estamos hablando de que una empresa pueda adquirir un equipo de impresión y gestionar la compra de un consumible y que, a la par, puedan no hacerse cargo de las tareas administrativas que no suponen valor añadido para su negocio. Esas tareas se pueden realizar desde el fabricante o desde los distribuidores. ■

MÁS INFORMACIÓN

- Toda la información sobre el mercado de impresión
- Cuál es la propuesta de Brother para el mercado de impresión

El mercado de impresión ha experimentado una profunda transformación ayudando a las empresas en sus procesos de digitalización.

¡Descubra en nuestro

Centro de Recursos itUser

cómo está evolucionando un sector clave en la Transformación Digital!

ImpresiÓN Digital

Con la colaboración de: brother

Hay quien dice que la COVID ha hecho más por la digitalización de las empresas que cualquier otra medida o persona responsable. Lo cierto es que ha servido para acelerar la transición en la que estaba inmersa la economía, para reforzar algunos de los puntos fuertes que estaban sobre la mesa y darnos cuenta de algunas de las debilidades de las que quizá no éramos del todo conscientes.

El puesto de trabajo digital en 2021:

¿Qué podemos esperar?

El entorno de trabajo es, más que nunca, digital. De hecho, cuanto más digitalizado esté, mejor estaremos respondiendo a la nueva situación creada. Pero, después de un año en el que el ir a la oficina se ha vuelto casi tan anecdótico como lo era el teletrabajo en muchas empresas antes de la Covid-19, ¿qué novedades podemos esperar en materia de Digital Workplace en este 2021? ¿Está todo escrito, descrito y dicho? ¿Qué pautas se deben seguir para mejorar todos los escenarios laborales posibles?

¿QUÉ ES UN LUGAR DE TRABAJO DIGITAL?

Antes de adentrarnos en materia, quizá es bueno revisar qué queremos decir exactamente cuando hablamos del lugar de trabajo digital.

Simplificándolo mucho, podemos decir que el lugar de trabajo digital es una construcción virtual análoga al lugar de trabajo físico. Consiste en todas las herramientas digitales que necesita para hacer su trabajo, incluido el acceso a datos e información, la capacidad de colaborar con colegas, la capacidad de crear resultados digitales o físicos (crear un PowerPoint o hacer que un robot suelde una pieza a un coche). El lugar de trabajo digital tiene interfaces e interconexiones con nuestros lugares de trabajo físicos y es accesible con total fidelidad, independientemente de la ubicación real de nuestro lugar de trabajo físico.

Aunque antes esto era importante para personas en ciertos roles, de repente se volvió mucho más importante para muchas más personas debido a la pandemia global.

Un lugar de trabajo digital debe tener algunos componente fácilmente reconocibles y comprensibles: el trabajo digital en sí, la capacidad de procesamiento y la experiencia de usuario.

La primera abarca muchas tecnologías, todas aquellas que se utilizan para almacenar los datos sin procesar y que alimentan o crean nuestros procesos comerciales. En la segunda es la responsable de convertir todos estos datos sin procesar en información útil (o procesable). Este procesamiento y transformación puede depender de una plataforma en la nube para impulsar muchos procesos comerciales, o puede usar una única aplicación heredada local con su propio almacén de datos especializado para impulsar un único flujo de trabajo de procesos comerciales.

Por último, el componente de experiencia del usuario (UX) es el elemento más visible, en la que los empleados interactúan con uno o varios sistemas para llevar a cabo sus tareas diarias. Puede incluir herramientas a las que se accede a través de un navegador (SharePoint, Salesforce, SAP, sistemas desarrollados internos personalizados)

4 RECOMENDACIONES PARA IMPLEMENTAR UN MODELO DE TRABAJO HÍBRIDO EN TU EMPRESA

o aplicaciones específicas a las que se accede a través de su ordenador o cualquier otro dispositivo. Este aspecto es fundamental para el éxito y el acomodo al nuevo escenario.

En cualquier caso, lugar de trabajo digital puede ser un entorno amplio, expansivo y complejo, mucho más allá de la idea de un sitio de intranet con algunas aplicaciones vinculadas.

OTRA FORMA DE DEFINIRLO

Sin embargo, lo cierto es que hay muchas formas de definir lo que es un auténtico digital workplace. Para Michel Rodríguez, director de colaboración en Cisco España, el entorno de trabajo digital está compuesto "por tres pilares clave: trabajadores siempre conectados; espacios colaborativos, dinámicos y seguros; y mayor satisfacción y compromiso".

Mientras, Daniel Vázquez, gerente de desarrollo de negocio de Fairview, debe ser colaborativo, ágil y funcional. "El concepto va más allá de la simple implantación de una serie de herramientas digitales. Estas deben hacer posible que los trabajadores hagan uso del espacio virtual independientemente del lugar donde se encuentren y del dispositivo que utilicen para ello", explica. Según él, "hablamos de un nuevo hábitat laboral en el que la mayor parte de las funciones se han digitalizado: la comunicación entre los empleados, el acceso a las aplicaciones y a los datos (siempre en tiempo real) y todo ello realizado de forma segura". Y, por eso, cree que para que un Digital Workspace funcione correctamente "se debe hablar de un modelo híbrido que combine días trabajando desde casa y días de trabajo presencial en la oficina".

Genaro Escudero, workforce solutions principal de Dell Technologies, considera que El digital workspace "se ha convertido en un pilar fundamental sobre el que las organizaciones se apoyarán en los próximos años para impulsar su transformación digital". Es más, sin él "no hay modelo de negocio digital. Y sin éste, poco margen queda para la competitividad. Un espacio de trabajo digital es todo aquel que facilita las aplicaciones y los datos que los empleados necesitan para poder trabajar y que son accesibles desde cualquier dispositivo y lugar", incide.

"El futuro del trabajo implicará una combinación de interacciones remotas y presenciales. Y la tecnología puede ayudar a las organizaciones a adoptar hoy ese futuro"

MICHEL RODRÍGUEZ, DIRECTOR DE COLABORACIÓN EN CISCO ESPAÑA

Para Juan Carlos Fuster, communications and brand manager de Lenovo en Iberia, el digital workplace es "la nueva realidad del mercado laboral y que engloba la integración de forma natural de los procesos de una compañía en la que su plantilla es usuaria de tecnologías digitales, de una manera solvente, segura e inteligente". Es más, considera que es ahora cuando las organizaciones "están cambiando su enfoque hacia el trabajo remoto e híbrido, están mejorando dispositivos, software y servicios para mejorar la satisfacción y conexión de sus equipos".

CÓMO DEBE SER

Pero, ¿qué características debe reunir este espacio de trabajo digital para que pueda ser considerado como tal? Jaime Balañá, director técnico de NetApp España, entiende que un Digital Workspace de una empresa "tiene que permitir a los empleados acceder a sus datos y sus aplicaciones en tiempo real y desde cualquier dispositivo y lugar". Algo para lo que "debería incluir virtualización de aplicaciones y escritorios, herramientas colaborativas, intercambio de ficheros, autentificación unificada y todo ello garantizando la seguridad y la privacidad en

"El digital workplace va más allá de establecer una oficina en casa. Se trata de facilitar un verdadero trabajo colaborativo, tanto remoto como presencial"

DANIEL VÁZQUEZ, GERENTE DE DESARROLLO DE NEGOCIO DE FAIRVIEW

APLICACIONES Y HERRAMIENTAS QUE FACILITAN EL TRABAJO REMOTO

los datos tanto en el acceso y las comunicaciones como en el lugar donde se almacenen".

Eva López, senior Intelligent Workplace GTM specialist en NTT Spain, por su parte, explica que el puesto de trabajo moderno debe "crear una cultura que permita a los empleados una máxima eficiencia, a la vez que les proporcione una buena experiencia de uso". Aclara, además, que el puesto de trabajo tiene que ver "tanto con el lugar donde trabajamos como con el modo en que lo hacemos: cómo nos conectamos e interactuamos con los demás y como utilizamos nuestras habilidades, creatividad e inteligencia para contribuir al éxito de la organización". Y, por ello, cree que es "de vital importancia definir un puesto de trabajo que permita desarrollar todas estas capacidades a los empleados". "Las políticas rígidas en este tema tienen poco recorrido en lo que respecta a la atracción y retención del talento", subraya.

Para Antonio Cruz, director de Modern Workplace de Microsoft en España, un factor clave dentro de la filosofía de digital workspace es "dejar de medir el rendimiento de los empleados por las horas que permanecen en la oficina, sino por sus resultados en base a objetivos establecidos pero igualmente aprovechar la tecnología para ayudarles a equilibrar su vida profesional y personal". En su opinión, "un modelo de trabajo flexible supone trabajadores más satisfechos y una empresa más productiva. En definitiva, el trabajo debe ser una actividad, no un lugar al que desplazarse".

Antonio Abellán, country manager de ServiceNow Iberia, subraya que la clave está en las capacidades. "En los digital workplaces lo principal es la colaboración, y por eso es fundamental que tanto la información como los sistemas de gestión sean de fácil acceso para todos los departamentos", explica. "En segundo lugar, está la acción, porque en el ámbito del workplace digital es fundamental disponer de una plataforma que organice y automatice los trabajos recurrentes y repetitivos. Finalmente, la proactividad es otro elemento importante, ya que las herramientas que se utilizan tienen que ser capaces no solo de solucionar incidencias, sino de predecirlas y prevenirlas", sentencia.

LA EVOLUCIÓN DEL ÚLTIMO AÑO

El máximo responsable de ServiceNow Iberia coincide con el argumento de que la necesidad de trabajar desde casa impuesta por el coronavirus "ha obligado a muchas empresas a digitalizar al menos parte de su trabajo". Sin embargo, cree que "muchas se han limitado a operar con un flujo constante de correos electrónicos y mensajes, lo que finalmente puede llegar a colapsar al trabajador. El objetivo es utilizar herramientas que no solo permitan el trabajo, sino que lo agilicen. Un claro ejemplo en tiempos de pandemia podría ser una solución en la que

"La transformación digital es un cambio mucho más profundo, disruptivo y en cierto modo, revolucionario en el modo de entender las TI dentro de la empresa. Implica tener una visión completa a nivel tecnológico, social y laboral"

GENARO ESCUDERO, WORKFORCE SOLUTIONS PRINCIPAL DE DELL TECHNOLOGIES

¿Te avisamos del próximo IT User?

los empleados indiquen qué días pretenden ir a la oficina y que esta asigne automáticamente las mesas más adecuadas para evitar contagios a la vez que hace un seguimiento en caso de que ocurra un brote".

Con los datos de un estudio publicado por Microsoft junto a KRC Research y BGC, Antonio Cruz recuerda que cace tan solo un año, solo el 15% de las empresas contaba con una política de teletrabajo, mientras que ahora esa cifra ha crecido hasta el 76% en Europa, alcanzando un 83% en España. "Los directivos han visto la oportunidad de mantener el aumento de productividad, reducción de costes y acceso a nuevo talento, al mismo tiempo que logran mejorar la implicación de los empleados", señala, al tiempo que enfatiza que "aquellas empresas que ya confiaban en la nube y contaban con herramientas seguras de colaboración, como Microsoft Teams, han tenido mucho más fácil la puesta en marcha del teletrabajo para dar continuidad a la actividad desde fuera de la oficina de forma segura. Las que todavía no lo habían hecho se han visto obligadas a poner en marcha proyectos tecnológicos en un tiempo récord. En cualquier caso, esta situación ha puesto de manifiesto la importancia de acometer esa transformación digital de la que llevamos hablando desde hace años para mantener la competitividad o, llevado al momento actual, simplemente poder seguir operando".

Porque, tal y como corrobora la senior Intelligent Workplace GTM Specialist en NTT Spain, la situación vivida a raíz de la pandemia del COVID-19 "ha desempeñado un papel fundamental en la definición del nuevo lugar de trabajo, ya que proporcionar protección para la salud y el bienestar de los empleados se ha convertido en un aspecto fundamental hoy en día. Actualmente no se concibe ni se permite un puesto de trabajo que no sea seguro para sus empleados".

Otra consecuencia es que las empresas se han dado cuenta de la necesidad de un lugar de trabajo transformado digitalmente, aunque vinieran abordando la transformación digital "a su propio ritmo", en consideraciones del director técnico de NetApp España. "Aunque los beneficios de una infraestructura de puestos de trabajo virtuales (VDI) son innegables, para muchos clientes la antigua forma de hacer las cosas era a menudo suficiente, haciendo de la transformación digital algo con lo que podían tomarse su tiempo. Pero ahora el trabajo a distancia, la resiliencia y los problemas de continuidad del negocio no son sólo la clave del éxito, sino la clave de la supervivencia", explica. "Como resultado, las empresas están pidiendo a TI que se adapte y transforme rápidamente las operaciones para apoyar las iniciativas de transformación digital del lugar de trabajo, todo ello sin comprometer el riesgo ni superar

el presupuesto. En este sentido, muchas compañías se están moviendo desde sistemas basados en infraestructura en el centro de datos a soluciones basadas en cloud".

LOS ERRORES (PORQUE HABERLOS, LOS HAY)

Podemos decir, de hecho, que las empresas equipadas con tecnología para teletrabajar "se han adaptado perfectamente con las herramientas de colaboración y han continuado su ritmo de trabajo. Las grandes empresas están más preparadas en el corto y medio plazo para afrontar una crisis mundial como la que estamos viviendo. Han sido capaces de adaptarse al nuevo escenario en tiempo récord". Sin embargo, como señala Juan Carlos Fuster, "si bien las pymes y los emprendedores están sufriendo duramente los impactos de esta crisis, también pueden ser parte de la solución por su capacidad para readaptarse a nuevos retos, nuevos entornos de trabajo de forma rápida y estar más acostumbrados a algunas de las tendencias propiciadas por la misma. En el lado más negativo, sí que es cierto que convivimos en la nueva normalidad con la deshumanización que esta crisis ha marcado, especialmente en una sociedad como lo nuestra en la que la parte relacional juega un papel muy importante".

En este camino, más o menos acelerado para lograr ese digital workplace, se están pudiendo cometer algunos errores o fallos. Uno de ellos,

EL TELETRABAJO EMPUJA AL CLIENTE HACIA LAS SOLUCIONES DE COLABORACIÓN ALOJADAS Y EN LA NUBE

"Los dispositivos informáticos resultan críticos a la hora de aumentar la satisfacción de los clientes, incrementar ingresos, y retener al talento. Además, los entornos de trabajo actuales plantean enormes desafíos en lo que a gestión y seguridad a las empresas se refiere"

JUAN CARLOS FUSTER, COMMUNICATIONS AND BRAND MANAGER DE LENOVO IBERIA

según Genaro Escuder es “llamar a todo “digital”, como un adjetivo simple de modernidad. Muchas organizaciones piensan que la transformación pasa por simplemente actualizar sus equipos o implantar alguna herramienta de colaboración cloud”, reflexiona. Y, sin embargo, “la transformación digital es un cambio mucho más profundo, disruptivo y en cierto modo, revolucionario en el modo de entender las TI dentro de la empresa. Implica tener una visión completa a nivel tecnológico, social y laboral. Por eso siempre insistimos en que el centro de este cambio es el usuario y su espacio digital”. Para el responsable de Fairview, el digital workplace “va más allá de establecer una oficina en casa. Se trata de facilitar un verdadero trabajo colaborativo, tanto remoto como presencial. Lo que no implica únicamente utilizar herramientas de chat y de videoconferencia, sino una evolución del puesto de trabajo centrado en la experiencia de usuario, la co-creación y la productividad”.

Algo en lo que coincide el director de colaboración de Cisco. “La evolución hacia el digital workspace implica retos técnicos y de negocio, pero también culturales, de mentalidad y actitud. Y hay que tenerlos todos en cuenta para implantar este escenario con éxito”, explica. En su opinión, “los principales retos técnicos son el soporte adicional para los empleados, el mantenimiento de los niveles de servicio y satisfacción de los clientes y la coordinación diaria de las actividades del personal/equipo. Además, la seguridad y la privacidad deben estar integradas desde el principio”. Mientras, “Las reuniones ‘sociales’ de videoconferencia, y los canales ‘sociales’ de chat se están impulsando para superar el principal reto social: la pérdida de relaciones interpersonales informales de tipo presencial. Por su parte, los cambios culturales, de mentalidad y actitud conllevarán un mayor bienestar de los empleados y equilibrio entre vida personal y laboral, además de una política de contratación más inclusiva que abarque talentos más diversos y personas con discapacidad”.

CÓMO HACER UN BUEN DIGITAL WORKPLACE

Por eso, hemos querido preguntar también a todos nuestros interlocutores qué consejos darían a las empresas de cara a seguir innovando para que, llegada otra situación extraordinaria como el Covid, estén lo más preparadas posibles.

El Gerente de Desarrollo de Negocio de Fairview cree que “si el espacio de trabajo digital está bien construido y ofrece las soluciones adecuadas tanto para empleados como clientes habrá que ir un paso más allá y establecer mecanismos que garanticen la ciberseguridad. Asimismo, habría de considerar las necesidades de los empleados como lo son la socialización y el intercambio con sus compañeros de trabajo, para poder efectuar un digital workspace híbrido que lleve a una mejor colaboración”.

“El primer paso para tener una verdadera experiencia orientada al cliente o al empleado es la vocación de la empresa de apostar por ello. Luego entramos en la fase de medir dónde se encuentra la empresa en ese camino para acometer las políticas de mejora”

ANTONIO CRUZ, DIRECTOR DE MODERN WORKPLACE DE MICROSOFT EN ESPAÑA

“Las empresas están pidiendo a TI que se adapte y transforme rápidamente las operaciones para apoyar las iniciativas de transformación digital del lugar de trabajo, todo ello sin comprometer el riesgo ni superar el presupuesto”

JAIME BALAÑÁ, DIRECTOR TÉCNICO DE NETAPP ESPAÑA

Mientras, Michel Rodríguez cree que el futuro del trabajo “implicará una combinación de interacciones remotas y presenciales. Y la tecnología puede ayudar a las organizaciones a adoptar hoy ese futuro. La clave está en pensar de forma más amplia y creativa y facilitar una experiencia optimizada, tanto presencial como virtual. Esto va más allá de conectar a las personas. La colaboración debe ayudar a crear vínculos, fomentar la cultura y humanizar la experiencia. Y las tecnologías de Inteligencia Artificial integradas en las herramientas de Colaboración juegan un papel esencial para lograr esta colaboración sin barreras, el entorno de trabajo híbrido y experiencias de cliente inteligentes”.

Desde NTT consideran que las empresas deberían “plantearse anticipadamente los objetivos que la empresa tendría que cumplir en una nueva crisis. Es importante que tengan en mente que el puesto de trabajo ha de ser útil para todos los empleados y debe permitir que estos se adapten con rapidez al uso de las nuevas tecnologías que se vayan aplicando”, detalla López. “Es imprescindible tener en cuenta las necesidades de los empleados que vayan a ocupar dichos puestos, porque de otra manera no se sentirán cómodos con su nuevo entorno de trabajo cuando esté listo. Es crítico implicarles en el proceso de puesta en marcha del puesto de trabajo digital. Igualmente, es muy interesante que todos los departamentos de una empresa colaboren en la implantación del digital workplace”.

Antonio de la Cruz considera que para lograr un punto de equilibrio y hacer posible escenarios de trabajo híbridos en los que los empleados se sientan cómodos, “ahora más que nunca, es muy importante implantar una cultura digital, que incluya no solo el área de TI de las compañías, sino que sea transversal, que implique a todos los departamentos y cuente con la implicación y gestión del equipo de dirección.

El primer paso para tener una verdadera experiencia orientada al cliente o al empleado es la vocación de la empresa de apostar por ello. Luego entramos en la fase de medir dónde se encuentra la empresa en ese camino para acometer las políticas de mejora”.

LO QUE QUIEREN LOS EMPLEADOS...

Como estamos viendo, tanto empleados como empleadores han de adaptarse y ajustarse a estos nuevos escenarios. Desde Dell se asegura que los empleados “necesitan, en primer lugar, disponer de los recursos y la tecnología adecuada para trabajar de manera productiva. Esto implica también contar con herramientas de seguridad cibernética para evitar que, tanto sus datos como los de la empresa, puedan ser vulnerados por atacantes externos. En segundo lugar, quieren trabajar desde cualquier lugar y

flexibilizar la jornada laboral, priorizando el trabajo por objetivos".

También Jaime Balañá destaca que las plantillas actuales demandan "libertad para trabajar desde cualquier lugar. Por eso, las organizaciones deben proporcionar una experiencia de computación de usuario final (EUC) sólida y constante, independientemente del tamaño de los equipos, su ubicación o la complejidad de las aplicaciones para que los empleados puedan trabajar desde cualquier lugar y en cualquier momento".

Es decir, que como subraya Antonio Abellán, los empleados quieren una mejor experiencia. "Esto supone reducir las tareas repetitivas y sin valor añadido, el uso de herramientas intuitivas y que funcionen de manera fluida, así como una mayor flexibilidad respecto a sus horarios y lugares de trabajo. En ocasiones nos encontramos con que las herramientas utilizadas en la vida privada son mucho más intuitivas que las que usamos en la vida corporativa, lo que genera un sentimiento de frustración de que la compañía no hace el suficiente esfuerzo por cuidar a sus trabajadores".

Por eso, "es necesario que los empleados se sientan realmente conectados, apoyados y capaces de dar lo mejor de sí mismos en el trabajo con este nuevo modelo de trabajo remoto e híbrido al que se han tenido que adaptar las empresas debido a la pandemia", en palabras del director de Modern Workplace de Microsoft en España. "Ahora, más que nunca, los empleados buscan entornos laborales que impulsen su creatividad, mejoren su productividad y satisfacción, les den autonomía y les hagan sentirse conectados con la cultura y misión de su organización".

"El puesto de trabajo tiene que ver tanto con el lugar donde trabajamos como con el modo en que lo hacemos: cómo nos conectamos e interactuamos con los demás y como utilizamos nuestras habilidades, creatividad e inteligencia para contribuir al éxito de la organización"

EVA LÓPEZ, SENIOR INTELLIGENT WORKPLACE GTM SPECIALIST EN NTT SPAIN

CONTENIDOS↓

ración y Seguridad que, integradas, permitan a los trabajadores innovar y mantenerse productivos desde cualquier lugar, con una gran experiencia de uso para los usuarios y sencillas de gestionar para los departamentos de TI. Y que también ayuden a atraer y retener el talento". Por eso, añade que los proveedores de herramientas de Colaboración "debemos impulsar la innovación para convertir las 'herramientas' en 'experiencias'".

Daniel Vazquez refuerza la idea de que muchas compañías "no estaban preparadas para adaptar su producción a los espacios virtuales y acabaron por adoptar medidas precipitadas que no aportaban todas las soluciones para que el flujo de trabajo fuera efectivo". En Fairview "apostamos por un modelo híbrido remoto/presencial. Donde las comunicaciones se integran de manera fluida de casa la oficina y viceversa, para ello utilizamos herramientas como Pantallas de Reserva de Sala, con las que los empleados pueden comunicar en remoto y a tiempo real si es que una sala de reunión estará ocupada en cierto horario, o Pantallas de KPI donde mostramos la evolución de resultados a los empleados".

Para el brand manager de Lenovo, lo más importante es "ofrecer a los empleados espacios diferentes para que dispongan de la posibilidad de elegir en cada momento dónde y cómo quieren trabajar". En su opinión, son muchos los estudios que demuestran que un entorno acogedor y agradable fomenta una mejor predisposición y actitud de las personas hacia el trabajo. "Algo que va parejo, por supuesto, de una renovación de los equipos, los PC se han convertido en un elemento de importancia crítica para los empleados. Más de la mitad de los empleados a tiempo completo asegura que sus dispositivos informáticos son un factor esencial de su labor cotidiana y la colaboración profesional. No hay duda de que un enfoque renovado sobre los PC genera un mayor impacto sobre los resultados operativos y la satisfacción de los clientes. Y es que los dispositivos informáticos resultan críticos a la hora de aumentar la satisfacción de los clientes, aumentar ingresos, y retener al talento. Además, los entornos de trabajo actuales plantean enormes desafíos en lo que a gestión y seguridad a las empresas se refiere, obligando a las compañías a monitorizar y responder de forma proactiva a posibles ataques. Por tanto, necesitan de una infraestructura que respalde a estos dispositivos, capaz de garantizar la seguridad de este nuevo espacio de trabajo siempre conectado".

¿Te avisamos del próximo IT User?

EL FUTURO DEL DIGITAL WORKPLACE

Jaime Balañá, director técnico de NetApp España, considera que la crisis de Covid-19 "está obligando a muchas empresas a reconsiderar sus estrategias de trabajo flexible a largo plazo. El trabajo en remoto es ahora esencial para la continuidad

del negocio y la retención de talento. Hacerlo bien requiere que las organizaciones formalicen una estructura para el futuro y, no solo ahora por la pandemia, para permitir el trabajo en remoto como una opción ya en el nuevo modelo post-pandemia. De esta manera, tendrán que mitigar sus principales retos, como la tecnología obsoleta, la falta de interacción cara a cara y los problemas de confianza de los empleados".

Mientras, el Workforce Solutions principal de Dell Technologies asegura que, cuando "todo se normalice, la tendencia es hacia un modelo híbrido, que mezclará el teletrabajo y la presencia física en el lugar de trabajo. Incluye beneficios y barreras, pero ha quedado claro que una mayor flexibilidad no provoca que la productividad se vea mermada".

Antonio Abellán, country manager de ServiceNow Iberia, subraya que "la agilidad es un concepto clave. No se trata solo de tener una idea de negocio, sino de ser capaz de implantar conceptos, soluciones y acelerar la producción de productos y servicios conforme sean necesarios. Según un estudio que preparamos con IDC, solo el 21 % de las empresas europeas está en una fase avanzada de la transición hacia unos procesos laborales más agiles. Esto indica que aún hay mucho margen de mejora. En este sentido, mi consejo es que las empresas no se centren tanto en la tecnología en sí, sino más en cómo utilizarla para alcanzar la flexibilidad necesaria para implementar nuevas ideas y poder cambiar el negocio en caso de que sea necesario".

Tal y como concluye el director de colaboración de Cisco, "el futuro del trabajo implicará una combinación de interacciones remotas y presenciales. Y la tecnología puede ayudar a las organizaciones a adoptar hoy ese futuro. La clave está en pensar de forma más amplia y creativa y facilitar una experiencia optimizada, tanto presencial como virtual. Esto va más allá de conectar a las personas. La Colaboración debe ayudar a crear vínculos, fomentar la cultura y humanizar la experiencia. Y las tecnologías de Inteligencia Artificial integradas en las herramientas de Colaboración juegan un papel esencial para lograr esta colaboración sin barreras, el entorno de trabajo híbrido y experiencias de cliente inteligentes". ■

"En los digital workplaces lo principal es la colaboración, y por eso es fundamental que tanto la información como los sistemas de gestión sean de fácil acceso para todos los departamentos"

ANTONIO ABELLÁN, COUNTRY MANAGER DE SERVICENOW IBERIA

LA TRANSFORMACIÓN DIGITAL SE ACELERA

Como decíamos antes, el concepto de trabajo remoto era algo de lo que muchas empresas recelaban. Sin embargo, ahora que llevamos un año trabajando desde casa, la perspectiva sobre el lugar de trabajo digital y las nuevas formas de trabajar está cambiando. Según una encuesta reciente de EY y el Urban Land Institute (ULI), se espera que el trabajo remoto crezca, ya que la mitad de los encuestados dijo que más del 60% de sus empleados trabajarán de forma remota después de esta pandemia.

Ahora más que nunca, las empresas deben implementar las tecnologías y los procesos adecuados para transformar las experiencias de sus empleados. No solo eso, también es importante tener en cuenta la satisfacción laboral y no solo la productividad de los empleados. En el futuro, una mayor priorización de las experiencias, la cultura y el empoderamiento como impulsores del compromiso será fundamental para mejorar el desempeño, la retención y la satisfacción de los empleados.

Escuchar la voz del empleado con un mayor enfoque en el bienestar, la diversidad y la inclusión será fundamental. El enfoque será, cada vez más, cómo las empresas pueden crear un entorno colaborativo, sostenido y de alto rendimiento. La transformación digital, combinada con nuevas herramientas y tecnologías, permitirá un conjunto de activos técnicos y de personas que trabajan juntos para mejorar la experiencia, automatizar tareas, simplificar el trabajo y fomentar la colaboración.

En 2021, incluso con una vacuna, muchos no regresarán a la oficina para el horario estructurado de 5 días en la oficina para turnos de 8 horas. La nueva normalidad en el espacio de oficinas incluirá tecnología para reducir la densidad de los espacios de trabajo a fin de aumentar la confianza para el trabajo en persona y proporcionar a los propietarios las herramientas para eliminar los riesgos de los espacios y obtener mayores rendimientos. Además, los propietarios y empleadores tendrán que ofrecer una gran variedad de opciones para adaptarse a la fuerza laboral multigeneracional.

La crisis de COVID nos enseñó que, si bien la tecnología ha sido una bendición para mantener a los equipos remotos en funcionamiento y de manera efectiva, no es un reemplazo a largo plazo para la construcción de la cultura en el lugar de trabajo, el desarrollo profesional del personal o la colaboración creativa espontánea. El trabajo es mucho más que completar tareas; es un esfuerzo social. Una cultura laboral positiva está formada por personas que no cuentan con las herramientas tecnológicas más novedosas.

MÁS INFORMACIÓN

- Transformando el espacio de trabajo digital
- Productividad en tiempos de incertidumbre
- Cincuenta estrategias para 2050
- Espacio de trabajo digital seguro con conexiones remotas
- Estrategia para el puesto de trabajo digital de la Comisión Europea
- Trabajador Digital
- Mejorando la experiencia del empleado

¿Cuál es el futuro del mercado de almacenamiento?

¿Qué tecnologías son las más adecuadas para las empresas?

Descubra las últimas tendencias en el Centro de Recursos IT User

Almacenamiento it

Con la colaboración de: Synology® NetApp®

El fenómeno de la Industria 4.0 en 2021, a debate

¿En qué consiste el concepto Industria 4.0? ¿Cómo ha evolucionado en los últimos años? ¿Cómo se ha visto afectado por la situación que hemos vivido desde marzo de 2020? Éstas son algunas de las preguntas que quisimos contestar en esta Mesa Redonda IT, junto con otros factores relevantes de este segmento, como si se pueden utilizar los datos de manera más inteligente en el IoT Industrial o si veremos ya este año una aplicación masiva del 5G en estos ecosistemas.

El cambio de paradigma generado por la Industria 4.0 y el IoT Industrial ha mejorado significativamente las capacidades digitales y de conectividad de los Sistemas de Control Industrial en múltiples verticales. Si bien, también se ha abierto las puertas a graves riesgos de ciberseguridad que amenazan con causar daños notables a las operaciones industriales.

En el marco de un año tan complejo como el que hemos vivido, ¿cómo ha evolucionado el fenómeno de la Industria 4.0 en España? Debatimos sobre esta cuestión junto a Miquel Melero, solution leader aggity; Roberto García, director general Ambar; Tomás Villameriel, business manager Ikusi; Jacinto Moral, experto en ciberseguridad de S21Sec; y Borja Pérez, country manager Stormshield.

Así, lo primero que quisimos establecer es en qué momento se encuentra el desarrollo de la

EL FENÓMENO DE LA INDUSTRIA 4.0 EN 2021, A DEBATE

Industria 4.0 en España. En este sentido, Miquel Melero comenta que "la Industria 4.0 ha soportado muy bien esta pandemia y la gran mayoría de las industrias han seguido produciendo con normalidad. Incluso, sectores como el de la alimentación han crecido en este tiempo. La industria quiere acelerar la transformación y la pandemia ha ayudado en el incremento del ritmo, y ahora estamos expectantes ante los fondos europeos. Con todo, creo que la pandemia ha servido como un revulsivo para digitalizar más la industria".

Para Roberto García, "en estos meses hemos visto una evolución muy acelerada. Nadie nos imaginábamos lo que iba a pasar y cómo íbamos a evolucionar. En el ámbito industrial ha habido un avance muy importante para soportar toda esta evolución necesaria, y creo que sí que se ha impulsado la concienciación sobre la necesidad de la digitalización, también en la industria, porque hemos seguido produciendo mientras asentábamos los pilares para seguir el desarrollo de los próximos años, y esperemos que los fondos europeos puedan ser el empuje definitivo a esta digitalización".

En opinión de Tomás Villameriel, "vemos que la Industria 4.0 es un fenómeno que sigue avanzando progresivamente, pero no es una moda, y todas las industrias necesitan habilitar las tecnologías que les permitan desarrollar su potencial en este terreno. Creemos que hay algunos factores que harán que el desarrollo no sea uniforme, como el tamaño de las empresas o los sectores, y el de la alimentación ha sido un claro ejemplo estos meses, o las tecnologías, que algunas están más implantadas que otras. Hemos notado, no obstante, cierta ralentización, centrándose los esfuerzos en mantener la producción, y ahora vemos cierta aceleración en el camino hacia la optimización".

Según explica Jacinto Moral, "hemos visto cierto desarrollo en algunos segmentos que estaban algo más rezagados, y que han aprovechado estos meses, con menor presencia de empleados, para avanzar en aspectos como la seguridad o la implementación de sensores"

Finaliza esta primera ronda Borja Pérez destacando que han visto "un movimiento desde hace meses en empresas de TI que están desarrollando soluciones especificas para el entorno industrial, porque vemos que hay mucho potencial. A raíz del despliegue de los sensores, vemos que la industria empieza a ser objetivo de ataques. Hasta la fecha, hablábamos de entornos muy aislados, pero con la conectividad pasa a ser visible y a ser objetivo de distintos ataques".

OBTENER VALOR DE LOS DATOS

La sensorización y conectividad de la que hablábamos generan datos, pero ¿estos datos se están aprovechando para sacar valor para el negocio? En opinión de Roberto García, "una de las primeras fases es sacar una información inicial, y hay muchas empresas que están en esa fase. A partir de dichos datos, es necesario modelar y ver cómo aprovechar esta información, y muchas corporaciones que están en esta fase, pero es un paso complejo, porque depende de muchos factores y no todas las empresas están igual de maduras, aunque algunos sí están sacando valor de ellos".

"La Industria 4.0 ha soportado muy bien esta pandemia y la gran mayoría de las industrias han seguido produciendo con normalidad"

MIQUEL MELERO, SOLUTION LEADER AGGITY

“Para desarrollar 5G en industria es necesario que la tecnología esté asentada, probada y muy bien desplegada. Y estas premisas todavía no se cumplen”

ROBERTO GARCÍA, DIRECTOR GENERAL AMBAR

Desde el punto de vista de Jacinto Moral, “se están empezando a obtener datos, pero es una gran cantidad, y algunos no los aprovechaban realmente. Ahora se va a empezar a modelar a partir de estos datos y avanzar en cómo pueden sacar valor de esta información. Estamos ahora avanzando en este modelado para mejorar el uso de recursos, los procesos, la producción... Hay que transformar los datos en información de valor para las empresas”.

“La industria genera gran cantidad de datos”, apunta Miquel Melero, “y muchos se acaban perdiendo, de ahí que estemos trabajando en cómo convertir las empresas en entidades data driven, cómo sacar valor de estos datos. Esta información te permiten conocer mejor tus procesos, detectar problemas, encontrar soluciones... y todo ello en base a tus propios datos y a una plataforma que te ayude a entenderlos”.

En esta misma línea encontramos a Tomás Villameriel, que comenta que obtener valor de los datos del IoT Industrial “tiene tres factores clave. En primer lugar, centrarnos en el caso de uso; tenemos muchos datos, pero hay que darles una utilidad y determinar cuáles son los datos valiosos. El segundo, la utilización de herramientas contrastadas para recoger, tratar y analizar estos datos. Y tercero, integrar y validar datos de IT y OT, lo que nos permitirá generar indicadores y optimizar los procedimientos”.

5G, ¿REALIDAD O PROMESA?

¿Va a ser 2021 el año despliegue definitivo de 5G en el segmento industrial? Tal y como explica Borja Pérez, “5G sigue sin ser todavía masivo, pero sí veremos pilotos en empresas innovadoras para proyectos específicos. 5G nos aporta elementos básicos para la industria, pero, de momento, no vamos a ver grandes despliegues”.

Se muestra de acuerdo Tomás Villameriel, que apunta que 5G “va a tener despliegue a nivel de consumidores, pero no en la industria. El ancho de banda ya está disponible, pero a día de hoy estamos todavía en el desarrollo de pilotos. Red.es ha lanzado dos proyectos para desplegar pilotos alrededor de 5G, y nosotros estamos trabajando en ello. No creo que hasta 2022 o 2023 no veremos despliegues masivos en industria”.

También coincide Miquel Melero, que “no ve 5G en industria más allá de pilotos. Es posible algún desarrollo para robots de logística, por ejemplo, o para la Realidad Aumentada, pero el recorrido que tenemos por delante es inmenso”.

Roberto García señala que “dependemos de las operadoras, y el despliegue en determinadas zonas geográficas todavía está pendiente. Para desarrollarse en industria, es necesario que una tecnología esté asentada, probada y muy bien desplegada. Y estas premisas todavía no se cumplen. Conocemos pilotos, pero estamos en una primera fase que tendrá que evolucionar en los próximos dos años, cuando podríamos ver ya proyectos reales”.

DIVERSIDAD DE DESARROLLO SEGÚN LOS SECTORES

En palabras de Jacinto Moral, “los sectores que se van a beneficiar más del desarrollo de Industria 4.0 y el IIoT son aquellos que cuentan con

elementos desatendidos, porque van a ganar en visibilidad, tanto a nivel de producción como de funcionamiento o seguridad".

Tomás Villameriel comenta que hay más desarrollo en algunos segmentos, como lo relacionado con "monitorización del proceso productivo, integrando la información de OT e IT, para compartirla con todos los niveles de la empresa, otorgando una visibilidad total en tiempo real, además de permitir la detección temprana de problemas; gestión de activos clave, aquellos que afectan de forma directa al desarrollo del negocio, con el fin de invertir en el momento en que sea necesario; logística inteligente y todo lo relacionado con la trazabilidad de los productos y la conexión entre proveedor y el cliente, permitiendo que el proveedor tome decisiones en función de las necesidades reales de su cliente; y, por último, el mantenimiento avanzado, más dinámico y eficiente".

Añade Miquel Melero que el concepto Industria 4.0 "es totalmente transversal. Aplica a todos los sectores, porque todos se ven obligados a ello, y todos pueden aprovechar mucho la obtención y tratamiento de datos. Y esto aplica a todos los sectores, y todos están invirtiendo con un objetivo".

También confirma estar transversalidad Roberto García, si bien apunta que "algunos sectores se han acelerado mucho en estos meses, como el de la alimentación, mientras que otros se han ralentizado, como el de la automoción. Pero, de hecho, la industria automovilística se ha dado cuenta de que para ser competitivos tienen que ahondar más en este desarrollo y están incrementando más todavía las inversiones, pese a que son un ejemplo con muchos casos de uso. Se han dado cuenta de que la tecnología no es el fin, sino el camino para ser más productivos. Otro ejemplo ha sido el Retail".

Otro ejemplo positivo, indica Jacinto Moral, "es el de la Sanidad, que es un segmento que tiene un potencial enorme en la gestión y tratamiento de datos, y han apostado mucho por desarrollar su potencial en los últimos meses", siendo el desarrollo de las vacunas en un plazo récord, apostilla Roberto García, un claro ejemplo de este potencial.

Hablando de Sanidad, señala Borja Pérez, "no podemos olvidar que un hospital está utilizando protocolos industriales en sistemas como respiradores o de climatización, por ejemplo. Es una muestra muy buena de integración entre IT y OT", lo que tampoco nos permite olvidar, recalca Jacinto Ramos, "la imperiosa necesidad de contar con una seguridad adecuada".

"Vemos muchos pilotos de optimización de costes, pero el reto está en desarrollar nuevos modelos, nuevos ingresos para el negocio"

TOMÁS VILLAMERIEL, BUSINESS MANAGER IKUSI

INDUSTRIA 4.0: ¿UNA REALIDAD SEGURA?

¿Es la seguridad de la Industria 4.0 la adecuada? Borja Pérez indica que "hablando de Sanidad, hemos visto muchos ataques a centros sanitarios en todo el mundo, pero también en otros verticales. Nadie está libre de estos ataques. Los sistemas actuales que tenemos en la industria hoy en día, no fueron diseñados para estar conectados con el exterior. Igual que en TI hay mucha cultura de

¿Te avisamos del próximo IT User?

búsqueda y resolución de vulnerabilidades, no es igual en la industria de dispositivos para IoT. Hay que poner en práctica medidas externas de seguridad. Además, vamos a ver ataques de supply chain en el segmento industrial, atacando una industria a partir de un proveedor, ya sea de TI o de sensores".

"La seguridad", continúa, "debe cubrir los activos clave, para que no sean accesibles desde el exterior; o los sistemas de monitorización, que en algunos casos no cuentan con la debida securización. Hemos de tener en cuenta que algunos procesos habituales, ahora están expuestos, y hay que protegerlos adecuadamente".

Para Tomás Villameriel, "los sistemas de control de las empresas españolas, salvo algunas excepciones de empresas grandes, podríamos decir que son vintage, por no decir antiguos. Siguen dando servicio, pero no estaban pensados para conectarse con el exterior, por lo que se primó la disponibilidad y no la seguridad. Además, es complicado parchearlos y, por tanto, no se han ido actualizando. Estamos viendo que las vulnerabilidades sobre estos dispositivos han sido un 25% superior a otras, con lo que vemos que los ataque se centran ahora en dispositivos OT más que contra otros elementos. Hay cierto retraso en la ciberseguridad aplicada a las redes OT".

"Pero es lógico", apunta Borja Pérez, "porque no fueron pensados para ello y porque no existe en este segmento la misma cultura de compartir datos sobre vulnerabilidades que sí hay en el mundo TI. Esto hay que llevarlo al mundo OT".

En palabras de Roberto García, "el recorrido en este sentido en TI lleva muchos años de ventaja a OT. Y no podemos olvidar que las PYMES tienen una gran carencia en este sentido. Se centran en su negocio, y no piensan que puedan ser objetivo de un ataque. Las vulnerabilidades quizá sean las mismas, pero ahora están más expuestas y se conocen más. Hay que poner un foco especial, sobre todo en concienciación, tanto a la gente de OT como al resto de trabajadores. Tenemos que ser capaces de proteger todos estos entornos y el OT no es un entorno preparado para ello".

Añade Jacinto Ramos que es "muy importante conocer los nuevos límites de este perímetro industrial. Quién accede a nuestras plantas o a nuestro entorno OT. Si eres capaz de comprometer a una empresa que suministra, acabas comprometiendo a otras muchas más. Atacando una empresa de suministro, abres puertas para otros ataques a otras empresas de la cadena. Por eso es necesario incrementar la protección en este sentido. Descubrir y proteger cualquier puerta de entrada que pueda existir a tu red. Quizá no podremos resolver todas las vulnerabilidades de golpe, pero sí, al menos, tener controlados los posibles puntos de acceso".

Por su parte, Miquel Melero apunta que, precisamente por eso, "muchas empresas industriales tienen cerrada su red de control y la van a seguir teniendo, sacando OT a una red aislada, separándola del área TI. Hay que desarrollar diferentes niveles y capas de seguridad en OT, como antes se ha hecho en TI, pero las empresas tienen que ver las ventajas de abrir estas redes de control".

"El problema", destaca Borja Pérez, "es que no siempre está separado y hay más integración de la que algunas empresas piensan. De alguna manera se comparte red, y aunque la seguridad por capas es una buena alternativa, no

"A veces pensamos que hemos controlado un ataque en la parte TI, pero no tenemos visibilidad suficiente de la parte OT como para saber si se ha visto afectada"

JACINTO MORAL, EXPERTO EN CIBERSEGURIDAD DE S21SEC

siempre la parte OT está tan aislada como algunas empresas piensan".

"A lo que hay que añadir", comenta Jacinto Ramos, "que a veces pensamos que hemos controlado un ataque en la parte TI, pero no tenemos visibilidad suficiente de la parte OT como para saber si se ha visto afectada. Hay que potenciar la visibilidad de la parte OT para garantizar su seguridad".

Y es que la evolución de las herramientas en el mundo TI es mucho mayor que el en mundo OT, indica Roberto García, "y el operador de OT no puede hacer un análisis completo de la seguridad de su entorno", lo que se amplifica, añade Borja Pérez, "cuando hay sucesivas compras y el responsable se enfrenta a una nueva red o redes y no sabe exactamente qué es lo que tiene conectado a la misma".

OTROS RETOS...

Además de la seguridad, Tomas Villameriel destaca, como reto a asumir, "el teletrabajo, algo que ha llegado con la pandemia y va a quedarse, incluyendo control de acceso, soluciones colaborativas, conectividad... va a tener un crecimiento exponencial. Otro reto es la integración de las tecnologías 4.0 con las tecnologías anteriores, sobre todo en las PYMES, que cuentan con tecnologías anteriores, y tienen que conseguir que convivan con las nuevas. El último reto es la monetización de la Industria 4.0. Vemos muchos pilotos de optimización de costes, pero el reto está en desarrollar nuevos negocios, nuevos ingresos para el negocio, algo que habrá que desarrollar en 2021 y en los años siguientes".

Apunta Jacinto Ramos que va a haber "un cambio grande en los sistemas, porque muchas empresas cuentan con servidores on-premise, algo que cambiará con el crecimiento exponencial de los datos. Vamos a tener que ir a cloud queramos o no, porque no habrá otra alternativa, con soluciones As a Service y hosting deslocalizado, que deberá integrarse y trabajar con los sistemas legacy".

Para Miquel Melero, "el resto es obtener valor de los datos, que ayudaría a la empresas a crecer y mejorar. Hay muchos datos y hay que convertirlos en un diferencial con tu competencia".

Un ejemplo de esta monetización lo ofrece Roberto García, cuando señala que un clientes suyo de electrodomésticos, "está pensando en vender la información generada a partir de los datos obtenidos por los propios dispositivos". ■

MÁS INFORMACIÓN

El fenómeno de la Industria 4.0 en 2021, a debate

"Los sistemas actuales que tenemos en la industria hoy en día, no fueron diseñados para estar conectados con el exterior. Igual que en TI hay mucha cultura de búsqueda y resolución de vulnerabilidades, no es igual en la industria de dispositivos para IoT"

BORJA PÉREZ, COUNTRY MANAGER STORMSHIELD

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

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

Descubra las últimas tendencias en el Centro de Recursos itUser

Tecnología para tu Empresa

Con la colaboración de:

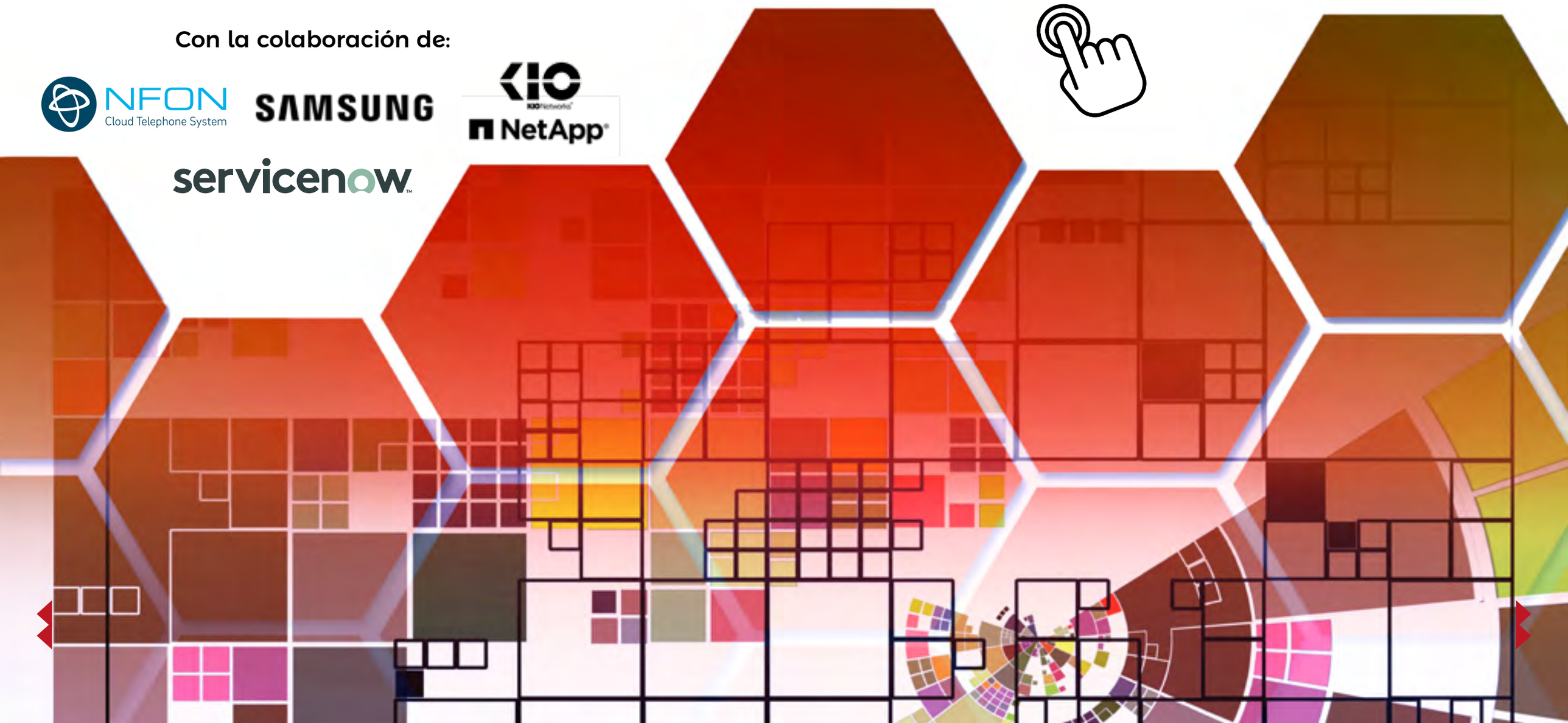
NFON Cloud Telephone System

SAMSUNG

KIO networks

NetApp

servicenow



NO SOLO it

PANEL DE EXPERTOS

TECNOLOGÍA Y NEGOCIO

La realidad del mito del monopolio de las Big Tech

Jorge Díaz-Cardiel,
socio director general de Advice Strategic Consultants

EMPRENDIMIENTO CONECTADO

Uso y ética de los datos recopilados en las empresas

Álvaro Valverde,
docente en creación y gestión empresarial en Udima

MARKETING Y CONSUMO

Mejor un sandbox regulatorio para fortalecer las criptodivisas

José Manuel Navarro,
CMO MOMO Group

ENCUENTROS Y DESENCUENTROS CON LA COMUNICACIÓN

Storytelling en la era de la Internet del Comportamiento

Manuel López,
asesor de comunicación

La realidad del mito del monopolio de las Big Tech

Jorge Díaz-Cardiel

Socio director general de Advice Strategic Consultants

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

¿Las compañías Big Tech compiten o dominan el mercado repartiéndoselo? Tanto en EEUU como en China se da una conjunción de factores que permitiría cualquier opinión. Otra cosa son los datos y su interpretación.

Por ejemplo, Scott Galloway en “The Four” y Tepper Hearn en “The Myth of Capitalism” defienden que Apple, Alphabet (Google, YouTube), Facebook, Amazon y Microsoft dominan el mercado norteamericano de Tecnologías de la Información y Digitalización. En China, de manera parecida, Kai-Fu Lee en “AI Superpowers” y Edward Tse en “China’s disruptors”, sostienen que Alibaba Group (Ant es el holding) y Tencent (We-

CONTENIDOS↓

¿Te avisamos del próximo IT User?

Chat, WeChat Pay...) dominan el mercado y se lo reparten.

Las autoridades, el legislador, el regulador, tanto en EEUU como en China, parecen estar de acuerdo con estos autores. China acaba de abrir expedientes "para el análisis de la competencia" a Tencent y a Ant (Alibaba), por entender que son un duopolio que, por un lado, compiten y, por otro, colaboran con la única finalidad de impedir la entrada de nuevos jugadores en el mercado y, por tanto, "fijar los precios", habitualmente más elevados cuando hay poca competencia real.

Apple, Google, Facebook y Amazon tienen un problema similar a la de sus homólogos/competidores chinos. No se sabe si peor o mejor. En China no hay democracia y, lo que decida el partido será lo que digan tribunales y otras autoridades. Hemos visto cómo el Estado/Partido/Gobierno/Competencia chinos han parado en seco la OPV o salida a bolsa de Ant (que hubiera sido la más grande en volumen en un lustro, con una valoración de mercado de 32.000 millones de dólares). ¿Por qué se paró esa salida a bolsa de una empresa que, al final y al cabo, depende del estado chino? Hoy ya lo sabemos, y por fuentes oficiales chinas: el nuevo culto a la personalidad (concepto acuñado primero por el comunismo soviético entre 1924 y 1953 en torno a la figura de Stalin y seguido por Mao Zedong en China entre 1949 y 1978) del actual premier chino, Xi Jinping, hacía incompatible el protagonismo de un empresario chino de éxito con estudios en Estados Unidos (Jack Ma) y la figura del presidente, secretario general y jefe de las fuerzas armadas chinas, que quiere el protagonismo para él. Durante un mes, Jack Ma estuvo desaparecido y, cuando se le ha vuelto a ver, su aspecto físico es el mismo de siempre, pero su carácter es más tímido y retraído; prudente.

Estados Unidos es una democracia desde 1783. El poder ejecutivo y el legislativo están en manos del partido demócrata, que se encuentra en un dilema difícil de resolver: "Big Tech" es el sector que más ha contribuido económicamente a la victoria electoral de los demócratas. Y no solo las empresas, sino sus empleados, que, en 2020, crearon un PAC (Political Action Comittee) con 3,5 millones de miembros, que recaudaron (mucho) dinero para financiar la campaña demócrata, en las elecciones del pasado 3 de noviembre. Y no olvidemos que, en 2016, cuando se enfrentaron Donald Trump y Hillary Clinton por la presidencia, 150 líderes empresariales de las compañías tecnológicas más importantes, apoyaron públicamente por carta a Hillary Clinton. Allí estaban demócratas como Tim Cook (Apple) y Jeff Bezos (Amazon), pero también, dos mujeres muy destacadas del sector TIC norteamericano que tienen mucho en común: Carly Fiorina y Meg Whitman: ambas, republicanas; ambas presidentas y CEO de la antigua Hewlett-Packard (hoy HP y HPE); las dos, candidatas conservadoras al poder legislativo de California (ambas perdieron); las dos, con larga trayectoria en el sector TIC: Fiorina en Lucent-Technologies y HP; y Whitman en Ebay y, tras su paso por HP, en Quibi.

Tres directivos TIC de máximo nivel se mantuvieron al margen del debate político en 2016 y 2020: Larry Ellison (Oracle), Peter Thiel (Paypal, Palantir)

Hay ámbitos donde los liderazgos dominantes dan miedo a la competencia y a los reguladores, como, por ejemplo, en cloud computing y en Inteligencia Artificial, donde hay pocos jugadores dominantes

y Elon Musk (Tesla, SpaceX). En 2020, Tim Cook y Jeff Bezos no apoyaron a nadie, porque ambos, tras borrascosas relaciones con Donald Trump, acabaron haciéndose amigos y consejeros del expresidente.

Hace 4 décadas, Washington estaba lleno de lobistas de los sectores farmacéutico, tabaquero, aerolíneas, automóvil...; "estos" son hoy nada y menos que nada, comparados con lo que se gastan en lobby las empresas tecnológicas en Washington. 3.500 abogados-lobistas trabajan para estas empresas. Es un factor que tener en cuenta a efectos de lo sucedido en octubre de 2020, cuando los líderes de las empresas TIC comparecieron ante Cámara de Representantes, Senado, FTC (Federal Trade Commission) y demás autoridades que velan por la libre competencia.

Mark Zuckerberg (Facebook), Sundar Pichai (Alphabet-Google), Satya Nadela (Microsoft), Tim Cook (Apple), Jeff Bezos (Amazon) y Jack Dorsey (Twitter) comparecieron durante días ante los organismos oficiales para defenderse de acusaciones tales como: abuso de posición dominante; impedir la libre competencia, vetando la entrada al mercado de pequeños y nuevos jugadores; violación de la privacidad de sus clientes, utilizando sus datos para hacer campañas de marketing y ofertas personalizadas; participación ilegal en las elecciones presidenciales de 2016 (Facebook, el escándalo de Cambridge Analytica) y competencia desleal con los medios de comunicación, entre otras muchas acusaciones. La última, la de la competencia desleal hacia los medios está de moda en todo el mundo: Francia le ha impuesto a Google ya varias sanciones billonarias, porque no paga a los editores franceses sus derechos de autor; Facebook, en Australia ha tenido el mismo problema, al que respondió con la suspensión de su servicio de noticias, movimiento que imitó Google. En cambio, Microsoft se posicionó de parte de los medios de comunicación -dijo Google- para promocionar su buscador, Bing.

Son solo algunos ejemplos. Que Amazon es líder en comercio electrónico, en e-commerce retail..., de todos es sabido. De hecho, tras liderar el comercio digital, ha saltado al retail físico, abriendo tiendas de casi todo lo que se puede vender: muebles, libros o alimentación fresca. Pero hay ámbitos donde los liderazgos dominantes dan miedo a la competencia y a los reguladores. Por ejemplo, en cloud computing y en Inteligencia Artificial, hay pocos jugadores dominantes: en cloud, Amazon, con Amazon Web Services (AWS), Google Cloud y Microsoft Azure. Competir con ellos es muy duro y difícil. Que se lo digan a IBM, a pesar de haber comprado Red Hat para precisamente esto: competir en cloud con los tres grandes. El resultado, aún, deja mucho que desear para IBM.

Otro campo es la publicidad online, para Facebook 95% de sus ingresos y para Google 85% de su facturación. Teniendo en cuenta el volumen de negocio de estas empresas, es fácilmente deducible que al resto de jugadores les quedan las migajas de la publicidad, incluidos los medios de comunicación. La inteligencia artificial la dominan Apple (Siri), Amazon (Alexa), Microsoft (Cortana), Salesforce (Einstein) e IBM (Watson). El resto de jugadores, como diría un es director de la CIA "son meros turistas".

¿Y qué decir de la televisión en streaming? Jugadores hay muchos, pero solo tres se llevan la parte del león en número de suscriptores: por este orden, Netflix, Amazon Prime Video y Disney+. Detrás, están AppleTV+, HBO, Peacock y muchos más, casi irrelevantes. En algunos países hay empresas que actúan como agregadores de contenidos: es el caso de Movistar+ en España, que además de contenidos de otras plataformas digitales

y los suyos propios, "aloja" a otras plataformas, como Netflix y Disney+.

A todas estas empresas les interesa, además, colaborar de manera que no parece intencionada, pero que es causal o correlativa: la demanda de iPhones de Apple, también está motivada por el deseo de los consumidores de utilizar el "search engine" de Google y su correo electrónico, Gmail, por no hablar de las redes sociales (Facebook, Twitter, Twitch, Tik Tok, Instagram...), por no hablar de los servicios de mensajería instantánea. Cuando Amazon provee de servicios baratos de cloud computing, esto se traduce en una mayor venta de aplicaciones de Apple's App Store. Amazon es el principal anunciante de Google. Y Microsoft vende licencias de Android para su teléfono inteligente Surface Duo.

La realidad es que no hay una respuesta nítidamente clara a si las empresas tecnológicas compiten sólo, colaboran sólo o hacen ambas cosas, sólo. Si continuásemos con más ejemplos, como los de más arriba, llegaríamos a la conclusión de que hacen las tres cosas en abundancia. Y, ni legislador, ni regulador, ni autoridad de la competencia van a poder solucionar el problema, porque es extremadamente complejo. Si no lo hizo en épocas más fáciles, menos aún ahora.

Me estoy refiriendo a la ley antimonopolio Sherman de 1890, que hizo el legislador americano tras la segunda revolución industrial y la llamada "Guilded Age" del capitalismo norteamericano, cuando monopolios, duopolios y oligopolios eran lo habitual, fuera en el petróleo o en la fabricación de automóviles. Esa ley, que sigue vigente, no pudo romper a IBM en 1983, cuando dominaba la computación, ni a Microsoft entre los años 1992 y 2002, cuando la compañía de Bill Gates tenía absoluto dominio de los sistemas operativos (Windows) y, el motivo para "romperla" fue que al considerar Microsoft que su browser, Explorer, era una característica más del sistema operativo Windows y, por tanto, no se podía separar, la conclusión es que Explorer acababa embebido en todos los ordenadores de HP, Lenovo, Acer, Dell... y los competidores de Explorer, como Netscape y Altavista, acabaron por desaparecer con un "sayonara, baby" (=en japonés, "hasta luego, Lucas").

> A todas estas empresas les interesa, además, colaborar de manera que no parece intencionada, pero que es causal o correlativa

De los 189 procesos legales antimonopolio abiertos en EEUU entre 1890 y 2020, utilizando la Ley Sherman, solo uno salió adelante en el sector de las Tecnologías de la Información. Se trató de AT&T, dividida por jueces y legisladores en las llamadas "Baby Bells", siete compañías que cubrían un territorio geográfico. ¿Por qué salió adelante aquel proceso antitrust? Porque AT&T fue un monopolio estatal y en la época de Ronald Reagan aquello era anatema.

En estadística hay una norma no escrita que siempre se cumple: "el porcentaje mayor gana al porcentaje menor". Dado el historial de éxito de los procesos antimonopolio contra empresas tecnológicas (un caso positivo, AT&T, versus 188 que quedaron en nada), no es descabellado pensar que, al menos en Estados Unidos, el statu quo de las empresas tecnológicas se quede como está. ■

MÁS INFORMACIÓN

- The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google
- The Myth of Capitalism: Monopolies and the Death of Competition
- AI Superpowers: China, Silicon Valley, and the New World Order
- China's Disruptors

NO SOLO it

Emprendimiento conectado

Uso y ética de los datos recopilados en las empresas

Álvaro Valverde

Responsable de Estrategia en ENISA y docente en creación y gestión empresarial en Udima

Economista. Licenciado ADE, Master Auditoría de Cuentas y en Valoración de Empresas. Responsable de Estrategia en ENISA y Analista de Inversiones. Inquieto, curioso y digital. Humanista y creyente en las personas. Siempre se puede tener una segunda opción; la vida nos la da. Enamorado de mi gente querida y allegada; de los libros, la buena comida, una conversación y sobremesas largas.

El término Macro Datos, o Big Data en inglés, se ha usado desde la década de los noventa, pero es a principios del siglo XXI cuando se popularizó y se planteó una primera definición por parte de la industria, atribuida a John Masley y Doug Laney.

Ambos plantean la definición como una cantidad de datos tal que supera la capacidad del software convencional para ser capturados, administrados y procesados. Se caracteriza esencialmente por las denominadas tres Vs: Volumen, Velocidad y Variedad. Y actualmente, en relación a la propia gestión de los datos, se han incorporado características como el aprendizaje automático y la huella digital. Normalmente cuando se interactúa

con las empresas hoy en día, y utilizando los diferentes dispositivos, móviles o no, se está dejando un rastro que se puede seguir. Ese rastro son bytes, megabytes, terabytes, etcétera, de datos que se deben guardar y que se pueden utilizar para mejorar los servicios, conocer más y mejor el mercado donde se trabaja y conseguir la máxima calidad en todo lo que la empresa hace. Esto hace que convenientemente analizados se puedan determinar patrones y tendencias relacionados con el comportamiento e interacciones humanas. Este hecho es muy valioso porque así se va conociendo lo que cada persona hace.

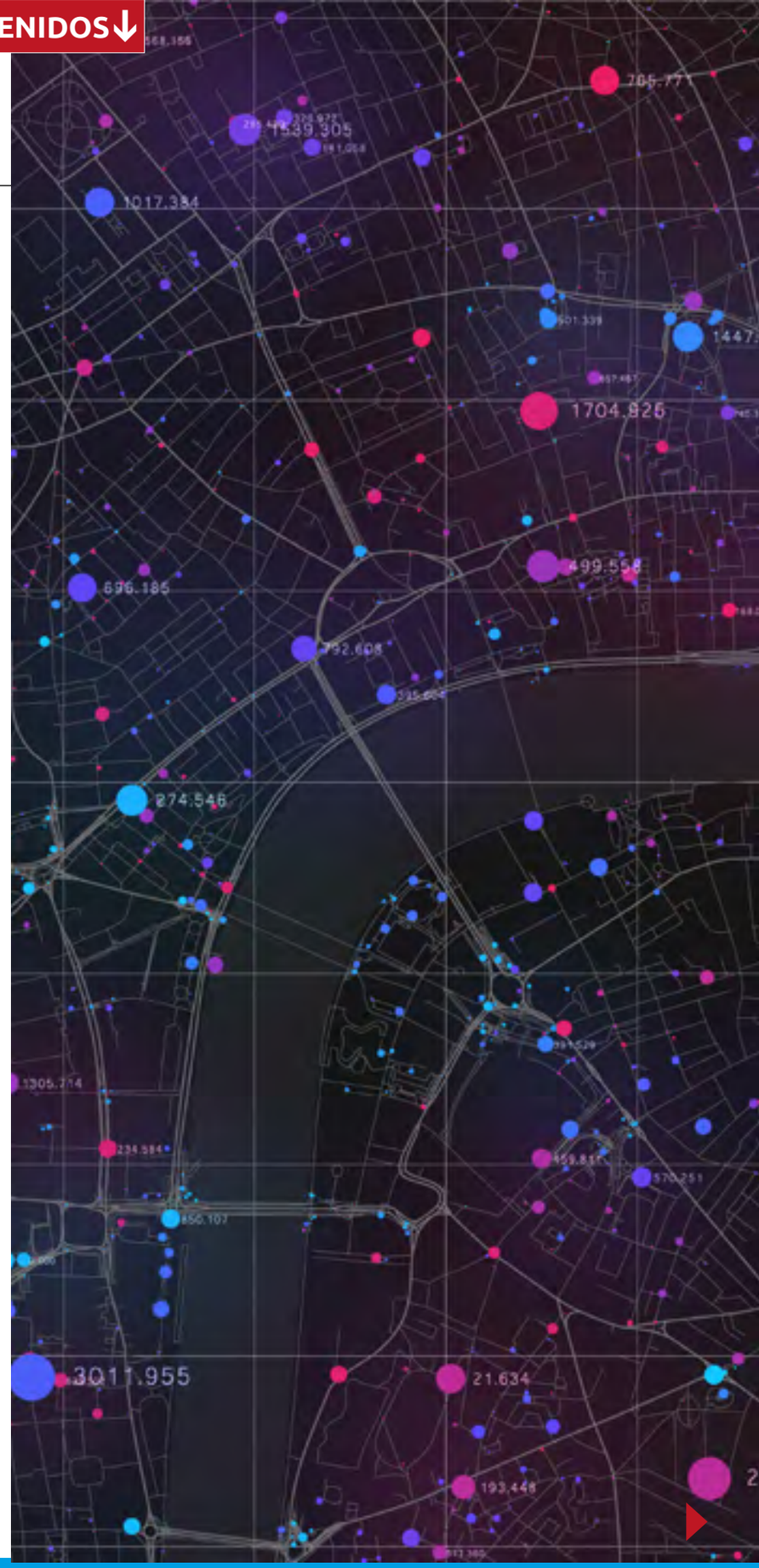
Esto implica que las personas, a veces, serán clientes y siempre son proveedores de datos para las empresas. Esta relación y disyuntiva es difícilmente separable porque la propia persona y su conducta como ser humano es lo que le distingue de los objetos inertes que apenas proporcionan atributos y mensajes. Así las personas son uno de los activos más valiosos que las empresas tienen.

Dicho lo cual, la cantidad ingente de datos de la que actualmente disponen las empresas de sus clientes, de sus productos y de su posición en el mercado y sector, hacen que la gestión de los mismos deba ser buena y eficiente. Estas características son necesarias para que el volumen y la velocidad con los que se generan, no entorpezcan su utilización y además no se vulnera la ley con un mal uso. Así mismo, existen importantes categorías de datos, de naturaleza muy variada y que deben tener procesos de gestión y utilización diferentes. Ante estos atributos se hace necesario que las empresas implementen sistemas de gestión de datos útiles y seguros para garantizar que se protegen de miradas curiosas y malintencionadas.

EL USO DE LOS DATOS

Teniendo en cuenta todo lo expuesto, se inicia un debate muy prolijo entre la doctrina de cuál debe ser el uso que se le dé a determinados datos, de cómo se debe respetar la ley para no vulnerarla y en definitiva, de cómo actuar con los datos. Se introduce así un concepto como la ética en el uso que, en principio, nada tiene que ver con la conceptualización de los datos.

"La necesidad de la ética de los datos del cliente viene de dos factores, el poder de mercado concentrado de unos pocos gigantes tecnológicos digitales que controlan cantidades masivas de datos de los consumidores y las preocupaciones fuertemente asentadas de los consumidores sobre cómo se usan sus datos y cómo se recolectan". Estas son palabras de Mike Mcguire, vicepresidente de Gartner, que demuestra cuán importante es



Se inicia un debate muy prolijo entre la doctrina de cuál debe ser el uso que se le dé a de terminados datos, de cómo se debe respetar la ley para no vulnerarla y en definitiva, de cómo actuar con los datos

hoy en día el debate ético y moral del uso de los datos. Y así las empresas deberán cuidar a sus clientes y ganarse la confianza de los consumidores; se tendrá que hablar mucho más de ética y datos y demostrar, de un modo transparente, su compromiso.

La persona debe tener un respeto escrupuloso a la privacidad de la realidad que muestran los datos y sus acciones, y los datos son de extremado valor ya que contienen direcciones, nombres, domicilios, pautas de comportamiento, es decir, prácticamente todo lo que los clientes de las empresas hacen y dicen. Y hoy en día las redes escuchan y ven "casi" todo. Antes estas situaciones debemos guardarlos, custodiarlos. Y las empresas deben respetar las buenas prácticas y sobre todo España debe acelerar el cumplimiento de normas de protección de datos. Esta situación se ve agravada por las necesidades constantes en las empresas de utilizar ética y moralmente los datos; y también guardar un escrupuloso respeto de la legislación en vigor.

El problema empieza ahí, cuando quien legisla ni siquiera cuenta con la normativa suficiente para actuar éticamente con los datos. Se sanciona a España porque el poder legislativo es incapaz de acelerar una Directiva Comunitaria que lleva esperando su trasposición más de dos años. Y el mal ejemplo cunde entre las empresas y ya se empiezan a ver sanciones por no proteger debidamente los datos de los clientes.

Ante esta situación, es muy importante saber qué tipos de datos recopilar, y de esos cuáles utilizar. Démonos cuenta de que los domicilios de la clientela, por ejemplo, determinan dónde operan, o al menos, establecen un rango inicial del territorio desde el cual operan. Eso es muy valioso para lanzar campañas de geomarketing. O si tenemos una naturaleza o tipología de clientes se pueden planificar campañas de captación optimizando el destinatario de la misma porque ya está cuasi identificado. Esto nos revela la importancia de los datos y su problemática de uso.

Finalmente, concluyamos expresando que la mayoría de las empresas aún no son conscientes de lo valiosos que son los datos que recopilan y están empezando a utilizarlos en sus estrategias de negocio de manera incipiente.

Y decir que ¡esto va a más y aquí estaremos para verlo! ■

MÁS INFORMACIÓN

- España podría tener que pagar 8,9 millones de euros por no trasponer una ley de protección de datos
- Desvelar datos de su empresa le puede salir muy caro
- Ranking de las mayores multas por privacidad

it Digital Security

Todo lo que necesitas saber de Ciberseguridad está a un clic

Una propuesta informativa compuesta por una publicación digital, una página web para profesionales de la seguridad, así como Dialogos ITDS, Webinars o desayunos de trabajo con los principales referentes del sector.... ¡¡¡Y no te pierdas nuestras entrevistas!!!

Mejor un sandbox regulatorio para fortalecer las criptodivisas

José Manuel Navarro

CMO MOMO Group

José Manuel Navarro Llena es experto en Marketing, Durante más de treinta años ha dedicado su vida profesional al sector financiero donde ha desempeñado funciones como técnico de procesos y, fundamentalmente, como directivo de las áreas de publicidad, imagen corporativa, calidad y marketing. Desde hace diez años, basándose en su formación como biólogo, ha investigado en la disciplina del neuromarketing aplicado, lo que le ha permitido dirigir, coordinar e impartir formación en diferentes masters de neuromarketing en escuelas privadas y en universidades públicas. Es Socio fundador de la agencia de viajes alternativos Otros Caminos, 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. Autor de "El Principito y la Gestión Empresarial" y "The Marketing, stupid", además de colaborador semanal desde 2006 en el suplemento de economía Expectativas del diario Ideal (Grupo Vocento).

Las recientes fluctuaciones del valor del bitcoin como respuesta a las noticias aparecidas en medios acerca de la predisposición de grades empresas a usar esta criptomoneda para sus transacciones comerciales o para vender fondos de inversión, han puesto de manifiesto dos cuestiones clave: la primera, la fuerte volatilidad del bitcoin como activo que puede terminar convirtiéndose en refugio para avezados y grandes inversores y, la segunda, las crecientes reticencias por parte de los bancos centrales a que pueda constituirse en instrumento de pago o de intercambio económico.

El espíritu con el que nacieron las criptomonedas como alternativa al sistema monetario convencional, regulado e intermediado por los bancos centrales, tuvo sentido como aspiracional de una parte del mercado que quería jugar con unas reglas diferentes a las impuestas, aprovechando que la tecnología blockchain les facilitaba un entorno altamente seguro, desintermediado y anónimo, pero ha evolucionado a un modelo que sigue las

mismas reglas que el mercado bursátil y, sobre todo, se afianza sobre criterios especulativos basados en la interpretación que hacen sus algoritmos frente a las fobias y filias de sus propietarios ante los movimientos de grandes empresas e inversores.

En este convulso contexto surgen las "stablecoins" (o monedas estables) asociándose al valor de monedas "fiat" (respaldadas por el gobierno o autoridad monetaria emisora) para evitar la volatilidad que sufren las pioneras por su marcada dependencia de los flujos de compra/venta y la escasez de garantías y respaldo financiero real. Las "stablecoins" se configuran como "tokens" que son emitidos por empresas privadas que aseguran contar con el capital suficiente para garantizar el dinero en circulación, pero la sombra de dudas razonables sobre su cobertura total ha hecho que los bancos centrales manifiesten una gran preocupación por su auge. A mismo tiempo, recomiendan a sus gobiernos emitir o planificar la emisión de sus propias criptodivisas, como algunos de ellos ya han hecho con diferente resultado (Venezuela, Dubai, Senegal) y otros (China, Japón, Suecia, Estonia, Israel...) planifican una estrategia favorable que les permita equiparar en sencillez los flujos comerciales en "stablecoins" a los de las monedas legales, sin que ello les afecte a sus balanzas comerciales en relación con las divisas hegemónicas en las transacciones de exportación e importación.

Mientras que se realizan estos movimientos, el BCE da un paso más y avanza en las directivas que regularán el lanzamiento de "stablecoins" condicionándolo a requisitos de capital y liquidez, sometiendo a sus emisores a pruebas de estrés y a una exhaustiva vigilancia para que no escapen al control de los mecanismos de prevención de blanqueo de capitales (sexta directiva europea AMLD6), y para que no influyan sobre la inflación ni pongan en riesgo la seguridad de los sistemas de pagos electrónicos. Con ello, el BCE trata de proteger la estabilidad del mercado y a los usuarios, quienes en el sistema bancario están protegidos por los fondos de garantía de depósitos (al menos hasta 100.000€ por titular en las entidades de crédito y el 100% del saldo en las entidades de dinero electrónico) mientras que en el de las criptodivisas están expuestos al quebranto total debido a posibles estafas, hackeos o pérdida de las claves. Ser custodios de sus propios activos y no existir garantías que respalden la

Crece el valor global del robo de criptomonedas

inversión es un riesgo asumido, pero al que no se le está dando la suficiente trascendencia.

En el caso de España, según el informe anual de banca móvil realizado por ING, una décima parte de los españoles ha invertido en criptomonedas, un 32% espera hacerlo en los próximos meses y el 38% cree que será el medio de pago de un futuro inmediato. Este comportamiento es similar al que está sucediendo en los países latinoamericanos, aunque aquí se usa como alternativa a su deteriorado sistema económico, aquejado de recurrentes períodos de inflación alcista. Ello es indicativo de que los ciudadanos prefieren confiar más en las criptodivisas como valor refugio que en su propio sistema monetario o en otros activos regulados, caracterizados por su baja rentabilidad, aunque posiblemente el 90% de sus titulares no pasarían el Test de Idoneidad y Conveniencia (MIFID) si trataran de realizar ese tipo de inversión en una entidad financiera.

Bitcoin y Ethereum, por ejemplo, están protagonizando en las últimas semanas tendencias alcistas que podrían justificar su aparente fortaleza, ya que las caídas que han sufrido por los comentarios de algunos personajes de relevancia, como Bill Gates o Janet Yellen, han sido compensadas por las recuperaciones impulsadas por otros como Elon Musk. Y tampoco parecen verse afectadas por las voces que las acusan de provocar un excesivo consumo energético durante los procesos de minería. Frente a este panorama optimista empiezan a surgir dudas sobre su futuro en la medida que se las obligue a someterse a una progresiva regulación y a que los bancos centrales aceleren la emisión de criptodivisas soberanas (CBDC). Algo en lo que parece estar de acuerdo el 86% de ellos, al menos en cuanto a explorar y experimentar esa opción (tal como refleja la encesta recogida en el reciente informe del BIS).

Las autoridades monetarias tienen el reto de, sin forzar el mercado, intentar la armonización entre las diferentes versiones sobre el dinero: las stablecoins y las criptodivisas emitidas de forma privada, el legal (sea físico o electrónico) y, ahora, las CBDC (Central Bank Digital Currencies). Plantearlo desde el punto de vista de competencia entre ellas sería un error en la medida que el poder legislativo está de parte de los organismos reguladores y pueden generarse tensiones al limitar la evolución natural e innovadora que se espera suceda. Otra cuestión es crear un marco regulador común (transparente e interoperable) para que los usuarios puedan decidir qué moneda utilizar cuando quieran hacer una inversión de alto riesgo o deseen usarla como medio de pago

seguro. En todo ello tendrá un papel crucial su desarrollo en blockchain, que también permitirá mejorar los sistemas de identificación y autenticación personal con un estándar único y universal (SSI o Auto-Identidad Soberana) que evite fraudes o pérdida de claves y simplifique el proceso de verificación de identidad para todos los entornos operativos.

En torno a un 60% de los bancos centrales ya están haciendo pruebas de concepto para definir el alcance de un lanzamiento de CBDC en su ámbito doméstico y, sobre todo, en el externo, donde deberán tener en cuenta las diferencias transfronterizas entre economías y sus distintos niveles de digitalización. Pero quizá el principal escollo que tendrán que superar es cómo mantener la estabilidad del sistema financiero para que puedan convivir una criptodivisa soberana (valor contra un derecho del banco central) y una moneda legal (valor soportado por el pasivo de un banco privado) en un sistema interbancario no diseñado para ello y en el que están empujando con fuerza las grandes tecnológicas en su intención de convertirse en intermediarios financieros paralelos, a partir de la gestión de sus enormes bases de datos y de sus capacidades transaccionales de pagos digitales.

Quizá, como se recomienda en el informe publicado por el Comité ECON de la Comisión Europea, lo más eficaz sería crear un sandbox regulatorio en el que participen bancos centrales, privados y Fintech, pero en el que también deberían estar las empresas emisoras de criptomonedas y las Bigtech, para alcanzar una mejor comprensión del esquema tecnológico, de seguridad, transparencia, prevención de riesgos (fraude, blanqueo, liquidez...), de especialización en la finalidad de cada moneda (como inversión o medio de pago) y para proveer a los ciudadanos de herramientas sencillas y útiles para organizar sus finanzas y decidir con criterio cuál de las soluciones prefieren usar en cada transacción. ■

MÁS INFORMACIÓN

- Sexta directiva europea AMLD6
- Fondos de garantía de depósitos
- Tercer sondeo BIS sobre monedas digitales de los bancos centrales
- Auto-Identidad Soberana
- Regulación Sandboxes y hubs de innovación para Fintech, Comité ECON

it whitepapers

ESPAÑA EN LA ERA POST-COVID: TI para transformar el negocio

La COVID-19 ha trastocado la vida de empresas y ciudadanos que ven con incertidumbre el futuro. A la preocupación sanitaria se le unen unas previsiones económicas, y de desempleo, nada esperanzadoras. Descubre en este IT Research cuáles son las principales previsiones para España y cuál es el papel que va a jugar la tecnología en la recuperación a través de más de 40 gráficos, divididos en seis bloques (Perspectivas Económicas para España, Evolución del Empleo, Situación de las Empresas Españolas, La Transformación Digital en España, la I+D, y la Importancia de los Fondos Europeos), y las opiniones de diversos analistas del sector.

Storytelling en la era de la Internet del Comportamiento

¿Como llegar a nuestro cliente objetivo en un mundo hiperconectado y con un exceso de ruido comunicativo realmente preocupante?

Con esta pregunta me levanté un día, que para más inri era un frío y gris día de invierno. La pregunta estuvo todo el día rondando mi cabeza. No es que fuera una pregunta que me hubiera hecho un amigo o enemigo, conocido o desconocido, cliente o proveedor. Simplemente nació en mi diálogo interior y siguió campando por sus respetos dentro de mi mente o, mejor dicho, dentro de mi castillo interior.

Hoy le abro la puerta de mi castillo para que salga y de forma misteriosa me lleva a buscar la respuesta en una de las diez tendencias estratégicas de 2021 que Gartner anunció recientemente: “Internet of Behaviours”.

“Internet of Behaviours” o “Internet del Comportamiento” podría explicarse como el uso de la información que puede gestionar una organización (datos de clientes, redes sociales, datos estadísticos públicos o privados, rastreos de ubicación, rastreos de navegación...) para cambiar los comportamientos de las personas. Solamente con esta definición ya se intuye que se puede usar tanto para el bien como para el mal. Con la proliferación de 5G y la explosión de IoT, la IoB llegará a un desarrollo imprevisible.

Manuel López

Asesor de comunicación

Madrileño de nacimiento, horchano de adopción, informático de profesión, con más de 35 años de experiencia en el sector de TI, ha desarrollado la mayor parte de su carrera profesional en Hewlett-Packard, donde ocupó cargos de responsabilidad en diferentes áreas como consultoría, desarrollo de negocio, marketing, comunicación corporativa o PR. Actualmente dedica la mayor parte de su tiempo a asesorar a starups en temas relativos a la comunicación, desde su posición de partner en la plataforma de profesionales goXnext.

NO SOLO it

Encuentros y desencuentros con la Comunicación

No quiero meterme en camisas de once varas y ponerme aquí a elucubrar sobre cómo utilizar la IoB para tener un encuentro o un desencuentro con la comunicación. Solamente quiero continuar mi historia para llegar a una conclusión: para llegar a nuestro cliente objetivo hay que contar historias, dicho de modo más 'cool', hay que usar el "storytellling".

Cuando el ser humano llega a su límite, suele volver al principio y de alguna forma eso es el "storytelling". Como muy bien explica Harari en su libro "Sapiens: de animales a Dioses", el Sapiens no llegó a dominar la Tierra por su fortaleza o superioridad, sino porque fue capaz de reunir a cientos de individuos alrededor de historias y hacer que colaboraran para conseguir los objetivos (cazar, defenderse, atacar...)

Por eso ahora que en comunicación parece que está todo inventado y cada vez es más difícil atraer la atención de unos consumidores, bombardeados hasta la saciedad con todo tipo de noticias, mensajes, anuncios... volvemos a nuestros inicios y nos ponemos a contar historias. Le damos un nombre pomposo como "stroytelling" y ya tenemos un nuevo entretenimiento.

Y como a mi me gusta buscar respuestas entre mis genios de referencia, voy a Leonardo da Vinci y le pregunto: ¿Cómo puedo aprender "storytelling"? Leonardo me contesta: no sé lo que es eso, pero si quieres te explico cómo hacer un mapa mental de tu vida en 7 días. Es sencillo:

Primer día: *Dibuja tus sueños*
Segundo día: *Explora tus metas*
Tercer día: *Aclara tus valores esenciales*
Cuarto día: *Reflexiona sobre tu propósito*
Quinto día: *Valora la realidad actual*
Sexto día: *En busca de conexiones*
Séptimo día: *Traza una estrategia para cambiar.*

Ésta es la recomendación de Michael J. Gelb en su libro "Pensar como Leonardo Da Vinci" para emplear los principios del pensamiento de Leonardo, cuando quieras realizar cambios en tu vida. A mí me parecen especialmente adecuados a la preparación del "storytelling" para comunicar con nuestros clientes objetivo en un mundo como el actual, donde como ya he dicho es tan difícil separar el grano de la paja y encontrar una aguja (mensaje, valor) en un pajar (mundo digital actual).

Cierro con una pequeña reflexión, hablando de comunicación y "storytelling", ¿vaso medio vacío o medio lleno?

No hay que ver el vaso ni medio vacío, ni medio lleno, sino con suficiente espacio para añadirle la historia que nos permita llegar a nuestros clientes.

Hasta aquí el cuento. La realidad es que hoy más que nunca necesitamos comunicar a través de las historias para llegar a nuestros clientes. Cada acción de comunicación debe obligatoriamente contar una historia, pero una historia que transmita un mensaje, ya sea la calidad de nuestro producto, la innovación de nuestra marca o los beneficios a conseguir. Si lo conseguimos tendremos un encuentro beneficioso con la comunicación, si no... no saldremos del ruido y nadie recibirá nuestro mensaje.

Y en esto es en lo que estamos: Encuentros con la comunicación, para evitar desencuentros y frustraciones con la comunicación. ■

MÁS INFORMACIÓN

- Es difícil escucharse entre tanto ruido, Eva Keifenheim, Medium
- Cómo usar el storytelling en tu startup, Paul Alex Gray, Medium
- Liderazgo y storytelling, andy Raskin, Medium
- Doce técnicas de storytelling para potenciar tu discurso, Dave Bailey, Medium
- Pensar como Leonardo da Vinci, Michel J. Gelb

it Reseller
TECH&CONSULTING

Cada mes en la revista, cada día en la web.