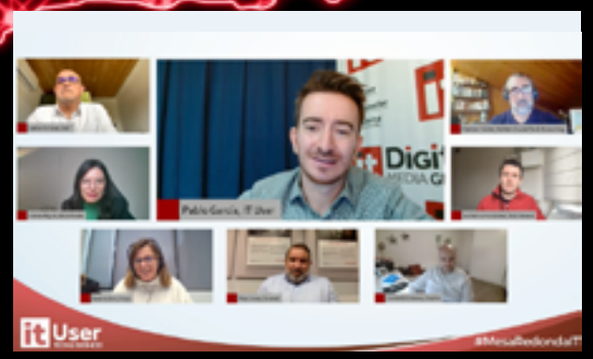
it User
TECH & BUSINESS

nº 77
ABRIL 2022

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

España: ¿hub de centros de datos?

Entrevista a Jorge González, CIO Global de Adolfo Domínguez



Avanzando en la digitalización de la pyme española, 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

Diseño revistas digitales Eva Herrero

Producción audiovisual Miss Wallace, 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 Events & Lead Gen Programs
Arancha Asenjo arancha.asenjo@itdmgroup.es

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

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

¿Cómo está afectando el conflicto entre Rusia y Ucrania al mercado TIC mundial?

El pasado 24 de febrero Rusia inauguraba un nuevo y dramático escenario al invadir Ucrania, lo que, entre otros muchos efectos colaterales, generaba la consiguiente respuesta diplomática y económica, que abría un punto de inflexión crítico para Europa y el mundo. El mercado de las TIC también se ha visto afectado por el conflicto, así como por las sanciones económicas y otras medidas impuestas a Rusia. El escenario geopolítico en evolución afectará indudablemente a la demanda tecnológica mundial en los próximos meses y años. Por lo pronto, más de la mitad de las empresas consultadas por IDC recientemente están reevaluando sus planes de gasto en tecnología para 2022, y el 10% prevé realizar fuertes ajustes en sus proyectos de inversión.

Si bien se espera una fuerte caída y una lenta recuperación del gasto TIC en Rusia y Ucrania, su impacto global será algo limitado. Combinados, los dos países solo representan el 5,5% de todo el gasto TIC en Europa y el 1% en todo el mundo. Sin embargo, el probable impacto de la crisis en el comercio, las cadenas de suministro, los flujos de capital y los precios de la energía afectará a la economía mundial en una escala más amplia con consecuencias negativas para el mercado de las TIC tanto a nivel regional como mundial. Entre ellas, una fluctuación de la demanda tecnológica; un aumento, como ya estamos padeciendo, de los precios de la energía y de la presión inflacionaria; una reubicación de personal e infraestructuras; desafíos en la disponibilidad de crédito y efectivo; problemas en la cadena de suministro; y fluctuaciones en los tipos de cambio.

Además de las consecuencias citadas, se pueden esperar otros impactos a corto y largo plazo, incluido el aumento de la volatilidad del mercado de valores y la especulación del mercado; riesgo de un mayor número de ciberataques y el potencial de una guerra cibernética más amplia; la interrupción de los entornos de start-ups tanto en Rusia como en Ucrania; y la creación de nuevas alianzas comerciales y científicas para reemplazar las rotas por las hostilidades.

La intensidad de estos graves desafíos dependerá en buena medida del tiempo que perdure una trágica realidad que nunca debería haber cristalizado. ■

Pablo García Reales

SUMARIO

Abril 2022

it User TECH & BUSINESS

EN PORTADA

España: ¿hub de centros de datos?

NO SOLO it

ACTUALIDAD

ANUNCIANTES

TENDENCIAS

REVISTAS DIGITALES

MESA REDONDA

Avanzando en la digitalización de la pyme española, a debate

ENTREVISTA

Jorge González Pérez, CIO Global de Adolfo Domínguez

Digitalización es Futuro

ASLAN 29 Ed 2022

18 y 19 MAYO MADRID

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

▶▶▶ www.congreso.aslan.es

DATA MANAGEMENT | CYBER SECURITY | DIGITAL WORKSPACE | CLOUD DATACENTER | INTELLIGENT NETWORKS

GLOBAL SPONSORS

aws · DELL Technologies · Innovation Built-In intel. · Hewlett Packard Enterprise · econocom · eset ENJOY SAFER TECHNOLOGY™ · NFON Cloud Telephone System

EVENT SPONSORS

aruba a Hewlett Packard Enterprise company · citrix · Councilbox · DARKTRACE · DE CIX · dynatrace · Extreme Customer-Driven Networking · hp

IKUSI volatile · cisco Partner · INFINIDAT · kaspersky · MICRO FOCUS · MongoDB. · NetApp · NUTANIX · PURESTORAGE®

Qlik LEAD WITH DATA · SAP · SCALITY · solarwinds · SOPHOS Cybersecurity evolved. · Symantec. · DEUTSCHE TELEKOM GLOBAL BUSINESS · VECTRA SECURITY THAT THINKS®

Creamos espacios de encuentro y divulgación tecnológica gracias al apoyo de más de 150 empresas asociadas

ORGANIZA

@aslan | Aceleramos la Transformación Digital

ICC 360º: presente y futuro de los servicios de digitalización documental

Jesús Cabañas, Iberia regional director PFU

El pasado 29 de marzo, PFU, la compañía de la corporación Fujitsu dedicada a la comercialización de escáneres documentales, organizó en Madrid un evento que, bajo el título "ICC 360º Tecnología en los servicios de digitalización documental: presente y futuro", y con IT User como Media Sponsor, buscaba analizar las nuevas oportunidades y retos que tienen las empresas alrededor de la gestión de la información, y cómo una adecuada introducción de ésta en los flujos de trabajo de las organizaciones puede suponer un valor competitivo muy destacado, sin olvidar que escanear no es lo mismo que digitalizar, y que ésta es la clave para aprovechar el valor potencial de los datos.

Y para mostrar en todas sus dimensiones esta nueva realidad que ha configurado la Transformación Digital, la compañía ha contado con el respaldo y el apoyo de algunos de sus socios más destacados, que ofrecieron su visión del segmento de la digitalización documental. Asimismo, se celebraron dos mesas redondas, moderadas por Pablo García, director de IT User, en las que se debatió sobre la evolución de los servicios de digitalización, así como sobre herramientas y tecnologías innovadoras en los servicios de captura de información. Además, el evento apostó por generar networking y desarrollar espacios para la co-creación.

DE LA OFICINA SIN PAPEL AL NEGOCIO DEL DATO FIABLE

En su presentación, Jesús Cabañas, Iberia regional director PFU, destacó cómo ha cambiado el mundo de las oficinas, resaltando el papel fundamental en esta evolución de la gestión de la información. Aprovechando algunas conclusiones sacadas de un estudio realizado entre diferentes organizaciones por su compañía, este responsable destacó que para el 86% de los encuestados,

administrar la cantidad de información de la que disponen sus negocios es un gran reto; que el 56% de los registro se almacenan tanto en papel como en formato digital; y que un 61% cree que es posible prescindir del papel en sus empresas.

A partir de estas premisas, y con la experiencia del conocimiento de la evolución vivida por este segmento del negocio, su compañía pone el foco tanto en las necesidades del cliente como en la calidad del dato, apoyándose en una completa gama de escáneres, herramientas de proceso de imagen y software de captura, y en la creación de ecosistemas de trabajo que permitan el desarrollo y la adopción de soluciones, tanto con ISV como con empresas locales. En el caso del hardware, Fujitsu apuesta por la innovación, como muestran las 32 nuevas patentes generadas por la última familia de escáneres; la flexibilidad de las soluciones; y la amplitud de la gama, mientras que, en el caso del software, la apuesta principal es PaperStream, una plataforma de aplicaciones que optimizan y agilizan la captura, almacenamiento, automatización y gestión de la información.

SERVICIOS Y SOLUCIONES DE CALIDAD ALREDEDOR DEL HARDWARE

Como decíamos, la compañía contó en este evento con la participación de algunos de sus principales socios. En este sentido, Alessio Angeli, account executive de Dyanix, quiso mostrar la visión de un mayorista de valor añadido alrededor de este tipo de soluciones, con herramientas que aportan flexibilidad y calidad, y servicios que arropan la propuesta el cliente.

Por su parte, Patrice Chakroum, senior solution architect & presales consultant de Scalehub, destacaba el papel incremental que tiene la confluencia en este tipo de soluciones de la automatización, la Inteligencia Artificial y la inteligencia humana, algo que ofrece en formato como servicio Scalehub a sus clientes, alcanzando, tal y como recordaba este responsable, una ratio del 99% de automatización en la solución, lo que elimina el fallo humano de la ecuación. Para ello, la compañía se apoya en una solución multihilo en la nube y en servicios de crowdsourcing para ofrecer "el procesamiento preciso de datos a gran escala".

EVOLUCIÓN DE LOS SERVICIOS DE DIGITALIZACIÓN

El primero de los debates, moderado por Pablo García, director de IT User, media sponsor del evento, se centró en la evolución de los servicios de digitalización: desde la captura de la imagen a la información de valor, y contó con la participación de Jesús Cabañas, Fujitsu; Alessio Angeli, Dyanix; Patrice Chakroum, Scalehub; Jaume Barella, director BPO de Inetum; y Elena Cortés, Subdirección General de Archivos del Gobierno de España.

Y el primer tema que se trató en esta mesa redonda es si es posible la digitalización masiva de documentos, algo con lo que se mostró de acuerdo Elena Cortés, que señaló que "el patrimonio documental español es muy extenso y es de todos los españoles, y tenemos la obligación de preservarlo para futuras generaciones". Habla esta responsable de un volumen de documentación que, contando los 8 archivos nacionales, ocuparía una extensión de más de 250 kilómetros, algo muy llamativo, pero que empequeñece cuando

El primero de los debates se centró en la evolución de los servicios de digitalización: desde la captura de la imagen a la información de valor, y contó con la participación de Fujitsu, Dyanix, Scalehub, Inetum, y la Subdirección General de Archivos del Gobierno de España

El segundo de los debates de la jornada se centró en herramientas y tecnologías innovadoras al servicio de la captura de la información y el dato fiable, y contó con la participación de Fujitsu Data Intelligence, AWS, ABBYY, UiPath, y Transkryptium

se piensa que en España hay unos 35.000 archivos, entre entidades públicas y privadas.

Para esta digitalización, indicaba la propia Cortés, las barreras son "el volumen de información, el coste de la digitalización y la tecnología, si bien ésta ya no es una excusa. Ahora el problema es el cambio de cultura".

Coincidía con ella Jaume Varela, que indicó que "hay un reto presupuestario importante. Pero hay que ir más allá de la digitalización y aportar valor sobre esa información, que es lo que nos permitirá realmente democratizar el acceso a esa información. El primer paso es la digitalización, pero debemos seguir avanzando hacia el segundo, la disponibilidad de la información".

Precisamente en la disponibilidad es donde ponía Jesús Cabañas el principal reto, sobre todo por la gran diferencia que existe actualmente "a la hora de compartir y consumir esta información".

Un cambio que tiene que llegar también a los Archivos Nacionales, porque, como apostillaba Elena Cortés, "es necesario cambiar la percepción y agilizar los procesos de la propia Administración para facilitar la labor".

Volvía a referirse al presupuesto como un freno Patrice Chakroum porque, "además de la tecnología, necesitamos el factor humano, que debe incrementarse en la medida en que se necesite acelerar el proceso".

Alessio Angeli, por su parte, comentó que "hay muchos servicios disponibles, pero el tamaño de los presupuestos es el que marca la profundidad y la inmediatez de estos".

En esta idea profundizaba Jesús Cabañas, que añadió que "en ocasiones, hay elementos del coste que no siempre se ven, como puede ser el consumo energético, que, a veces, depende de otro área del negocio. Para cambiar la cultura de las empresas hay que tomar decisiones muy valientes. Nuestra propuesta pasa por combinar hardware y software para aportar calidad, agilidad y eficiencia en costes al proceso de digitalización".

Hablando de eficiencia, recordaba Alessio Angeli que "el asesoramiento es fundamental para elegir la mejor solución", porque, añadía Jaume Varela, "no hay una única solución, y cada proyecto necesita su propio equilibrio entre eficiencia, coste y tipo de trabajo".

Al hilo de estos comentarios, apuntaron los diferentes portavoces que, por la Pandemia, se ha reducido el consumo de papel, pero se han generado otros problemas de compatibilidad. Y, precisamente de estos retos que superar siguieron hablando. En el caso de Elena Cortés, recordó que "estamos en un entorno de 27 legislaciones diferentes y, en nuestro caso, con 17 variantes, lo que complica mucho la situación".

Sobre legislación habló Patrice Chakroum, que apuntó la obligatoriedad "de cumplir con la legislación, especialmente GDPR", algo que no afecta a los datos anonimizados, pero, como añadía Jaume Varela, "el problema aparece cuando queremos obtener valor de la información, no cuando mejoramos los procesos para almacenarla. Pero claro, estamos todavía en el principio del proceso, porque necesitamos obtener valor de la información, no solo almacenarla".

Para finalizar el debate, Jesús Cabañas ponía el foco en los Fondos NextGen. Tal y como indicó, "estamos ante una gran oportunidad, pero la complicación es ver cómo la convertimos en proyectos concretos", a lo que añadía Elena Cortés

> "Para cambiar la cultura de las empresas hay que tomar decisiones muy valientes. Nuestra propuesta pasa por combinar hardware y software para aportar calidad, agilidad y eficiencia en costes al proceso de digitalización"
>
> JESÚS CABAÑAS, IBERIA REGIONAL DIRECTOR PFU

que “en el caso de los Archivos Nacionales, es una gran oportunidad porque ya hay muchos proyectos en marcha que deben ser asumidos por jugadores que puedan implementarlos”.

Para mostrar en todas sus dimensiones esta nueva realidad que ha configurado la Transformación Digital, la compañía ha contado con el respaldo y el apoyo de algunos de sus socios más destacados, que ofrecieron su visión del segmento de la digitalización documental

INTELIGENCIA DIGITAL PARA CAMBIAR EL NEGOCIO

La primera ponencia tras el debate corrió a cargo de Alicja Wolanczyk, innovation consultant de ABBYY, que centró su intervención en la necesidad de optimizar los procesos de automatización y digitalización, “hay que ver cómo podemos aplicar las tecnologías y nuevas tendencias en los procesos internos de las compañías, integrándolas con la tecnología existente”, y recordaba que “el 80% de los procesos se basan en documentos, y la clave está en cómo tratar la información contenida en ellos”.

También de la introducción de inteligencia en el proceso de digitalización habló Óscar Jarabo, global portfolio manager en Fujitsu Data Intelligence, que recordó la necesidad de una extracción inteligente del dato “para hacerlo más efectivo y eficiente, lo que genera más valor, más productividad y menos coste. El problema es que las soluciones actuales se centran principalmente en fuentes estructuradas y semi-estructuradas de datos”, mientras que también existen las fuentes de datos no estructuradas. Para este responsable, los datos estructurados y semi-estructurados son el primer paso, pero los datos desestructurados son muchos y la obtención de la información necesita otras tecnologías. El siguiente paso, por tanto, es aplicar la lógica de negocio para establecer relaciones entre los datos de fuentes no estructuradas”.

En el caso de Fujitsu IDP, partiendo del documento se genera una estructura mejorada, a partir del texto plano, para analizar la información y detectar las relaciones entre los datos, obteniendo con ello un valor real para las empresas, que debe ser evaluado por un humano antes de su estructuración para su uso en soluciones más complejas, como las de analítica o de gestión del conocimiento.

AUTOMATIZACIÓN Y CLOUD, UN BINOMIO GANADOR

Zigor de la Quintana, enterprise sales manager de UiPath, centró su participación en lo que denominan la Hyperautomatization, esto es, la combinación de la Automatización y la Inteligencia Artificial, emulando el razonamiento que seguiría una persona, pero incrementando la velocidad y reduciendo los errores. De hecho, con los datos de consultoras como IDC o Everest Research en las manos, la Automatización reduce los costes en un 35%, los errores en un 52%, el tiempo de procesado de documentos en un 17%, mientras que incrementa la productividad en un 40%.

Y otra de las grandes tendencias tecnológicas ya asentadas en los últimos años es la nube, y de ella habló Ángel Zarramera, solutions architect de AWS, que recordó las posibilidades que ofrece su plataforma para la modernización de los flujos de trabajo documental, integrando en el proceso las capacidades de la nube y de la IA. “El objetivo”, señaló, “es reducir los costes de la intervención humana, aprovechando las posibilidades de la Automatización en los procesos documentales”.

HERRAMIENTAS Y TECNOLOGÍAS INNOVADORAS

El segundo de los debates de la jornada se centró en herramientas y tecnologías innovadoras al servicio de la captura de la información y el dato fiable, y contó con la participación de Óscar Jarabo, Fujitsu Data Intelligence; Ángel Zarramera, AWS; Alicja Wolonczyck, ABBYY; Zigor de la Quintana, UiPath; y Vicent Bosh, Transkriptorium, moderados todos ellos por Pablo García.

El encargado de abrir esta mesa redonda fue Vicent Bosh, que destacó la complejidad a la que se enfrentan al tratar con textos antiguos manuscritos, "por eso, ofrecemos soluciones para aportar más calidad en las transcripciones que nos permitan extraer todo el conocimiento de las fuentes históricas, para ello no nos vale solo con la IA sino que necesitamos todo el conocimiento de paleógrafos especialistas".

De ahí la importancia de la IA, destacó Ángel Zarramera, "para entender el problema que quieres resolver, cómo puedes extraer la información y qué puedes hacer con ella".

En opinión de Alicja Wolonczyck, "obtener un dato fiable es posible, pero siempre hay que diferenciar entre esta fiabilidad y su valor real o su significado".

No se mostró de acuerdo con ella Óscar Jarabo, que apuntó que la fiabilidad total "es imposible, sobre todo porque el dato inicial puede no ser totalmente fiable, pero sí que podemos avanzar hacia procesos más ágiles y confiables. Los datos, los documentos, y los escenarios cambian, y los algoritmos deben evolucionar con ellos".

En palabras de Zigor de la Quintana, "los sistemas son más capaces cada vez de identificar datos, pero lo importante es ver hasta dónde vamos a lograr llegar con esos datos".

Eso sí, apuntaba Vicent Bosh que, "por muy fiable que sea el dato, siempre va a ser necesaria la intervención humana para tomar determinadas decisiones".

La seguridad del dato también tuvo su peso en este debate. Señalaba Óscar Jarabo que "son muchos los niveles de seguridad a la hora de acceder al dato y al documento. Hay que estar a la altura de la legislación". Y coincidía con él Vicent Bosh, que apuntó que "los grandes actores tienen muy claro lo que hace falta para asegurar el dato, pero también hay una seguridad adicional por el significado de ese dato".

Con todo, "la seguridad es lo más importante", sentenció Ángel Zarramera, "pero, en nuestro caso, esta responsabilidad es compartida con el cliente".

Y es que, cuando hablamos de soluciones Cloud, reconoció Zigor de la Quintana, "a algunos clientes todavía les cuesta, y, como nuestras soluciones se basan en datos, es algo que complica los proyectos". Coincidía con él Alicja Wolonczyck, que añadió que "es cierto que hay ciertas reticencias por parte de algunos clientes, y hay que darles la opción de tener versiones on-premise de las soluciones".

Indicó también Zigor de la Quintana que cada vez hay más clientes "que quieren automatizar más proyectos repetitivos, y la tecnología les permite hacerlo cada día en más pasos del camino a más empresas. Porque no es algo solo de grandes organizaciones. Sin embargo, el Sector Público va un poco por detrás en este terreno, si bien se detecta un interés muy claro".

Coincidía con él en la importancia de RPA Vicent Bosh, que apuntó que "tiene gran utilidad para garantizar los flujos de validación y son muchas las sinergias a explotar". Además, apuntó Alicja Wolonczyck, "permite a las personas poner el foco donde aportan valor. Es importante también por los cambios que implica para los procesos de las organizaciones".

Para finalizar, se planteó la disyuntiva entre soluciones propias de los clientes o aprovechar las soluciones más generales. Mientras Ángel Zarramera, Vicent Bosh y Alicja Wolonczyck destacaron que los clientes prefieren centrarse en su negocio, no en la tecnología, Zigor de la Quintana y Óscar Jarabo comentaron que el cliente prefiere tener el mayor control posible sobre la solución para no tener que depender de terceros". ■

MÁS INFORMACIÓN

- Fujitsu PFU
- PaperStream
- Fujitsu Fi-8000 Series

Wolters Kluwer

BE THE NEXT

Be the next en digitalizar
tu negocio con los
Fondos Next Generation EU

CONSIGUE TU KIT DIGITAL

www.kitdigitalparati.com
tel 900 11 11 66
a3clientes@wolterskluwer.com

El volumen de negocio de los servicios TIC en España creció por encima del 20% en 2021

Los servicios TIC registraron su mayor crecimiento en 16 años durante 2021. Su volumen de negocio aumentó un 20,7%, según el último TIC Monitor, que aporta los datos de diciembre del año pasado.

El sector de servicios TIC en España ha cerrado el ejercicio 2021 con un crecimiento interanual en su facturación del 20,7%, una cifra récord que implica el mayor incremento visto en 16 años. Así lo confirma la última entrega del barómetro mensual TIC Monitor, elaborado conjuntamente por VASS y el Centro de Predicción Económica CEPREDE.

Este repunte en términos de facturación ha permitido concluir el año con un crecimiento medio anual del +9,7%, compensando así la contracción experimentada en 2020. Es más, según sus resultados, los buenos datos de los últimos meses hacen que el promedio interanual de facturación por empleado lleve ya

cuatro meses en el terreno positivo, registrando una tendencia al alza.

Estas cifras positivas invitan al optimismo entre los empresarios españoles, a corto plazo. En este sentido, cerca del 78% de los empresarios TIC españoles espera un crecimiento de su cifra de negocio. Un indicador que, de nuevo, supera a las expectativas del promedio de la Unión Europea, que se sitúa en el 63% donde el porcentaje de optimistas alcanza el 63%.

Ese optimismo respecto a la facturación también se refleja de forma clara en las expectativas de empleabilidad a corto plazo, ya que el informe señala que el 84,6% de las empresas TIC en España tiene expectativas de aumentar su plantilla entre marzo y mayo de este año. Por tanto, se seguirá la línea de creación de empleo del año pasado, durante el cual creció un 5,8%.

Con todo, el responsable de TIC Monitor, Antonio Rueda, se muestra cauto, aunque valora la recuperación del mercado. "Tendremos que estudiar el impacto de la guerra en Ucrania y la incertidumbre que pueda llevar asociada en los países más expuestos al comercio con los países en conflicto, por un lado; y la repercusión de una inflación desbocada en rúbricas trascendentes como la energía o los alimentos", explica.

LA TRANSFORMACIÓN DIGITAL IMPULSA LOS INGRESOS DE LAS EMPRESAS DE CONSULTORÍA, SEGÚN LA AEC

La facturación de las empresas de consultoría aumentó un 8,8% en 2021, según el avance del informe anual que realiza la AEC, cuyos resultados finales se conocerán en junio.

El avance, que recoge los datos agregados de 18 empresas pertenecientes a la Asociación Española de Empresas de Consultoría, constata que los ingresos de las consultoras en 2021 aumentaron un 8,8% respecto al año anterior, un incremento impulsado por los procesos de transformación digital de las organizaciones españolas. Sus compañías asociadas incrementaron sus plantillas en casi un 9%.

En 2021, los servicios de consultoría han crecido un 6,2%, y representaron el 24% de los ingresos de las empresas de la AEC. Asimismo, ha aumentado la demanda de servicios de desarrollo e integración y de outsourcing respecto a 2020. El sector financiero se consolida como el mayor demandante de servicios de consultoría, y supuso casi el 34% del total de los ingresos de las empresas de la Asociación. Le siguen las Administraciones Públicas, que en 2021 representaron el 18,3% de los ingresos e incrementaron su demanda un 18,2% respecto al año anterior.

En lo que respecta a las previsiones, esperan que, este año, los ingresos crezcan por encima del 7%.

El sector de servicios TIC en España ha cerrado el ejercicio 2021 con un crecimiento interanual en su facturación del 20,7%, una cifra récord que implica el mayor incremento visto en 16 años

LA INVERSIÓN EN TI DEL SECTOR PÚBLICO EN ESPAÑA CRECERÁ UN 4,58% EN 2022

Las inversiones en tecnología del sector público van a seguir creciendo en 2022, según un nuevo análisis de Adjudicaciones TIC. El incremento con respecto a 2021 será del 4,58%, y se situará en 2.085 millones de euros. Esta cifra llegará a los 3.282 millones de euros si se incluye los mecanismos de recuperación y resiliencia.

Por ministerios, en el capítulo de gastos corrientes de los Presupuestos Generales del Estado, destaca el incremento en inversiones de los Ministerios de Sanidad, con una previsión de crecimiento del 85,6%; el de Asuntos Económicos y Transformación Digital, con una estimación del 41,3%; o el de la Presidencia, con una perspectiva de alza del 30,3%. En el lado contrario, el Ministerio de Hacienda y Función Pública, cuyas previsiones de gasto se reducen un 15,5%.

Por el lado de las inversiones en tecnología, los ministerios más dinámicos serán durante 2022 los de Hacienda y Función Pública, con

unas estimaciones de inversión superiores al 58%; y Asuntos Exteriores, UE y Cooperación, con una previsión del 40,1%. Por el contrario, las áreas que más reducen sus inversiones en tecnología en este período serán Educación y Formación Profesional, con una reducción del 22,2%; y Derechos Sociales y Agenda 2030, con un 16,4% menos de inversión estimada.

Según Carlos Canitrot, su director de consultoría, "estas cifras no se han visto nunca, por lo que las oportunidades de negocio para las empresas que trabajan con las AAPP son inigualables". ■

En 2021, los servicios de consultoría han crecido un 6,2%. Asimismo, ha aumentado la demanda de servicios de desarrollo e integración y de outsourcing respecto a 2020

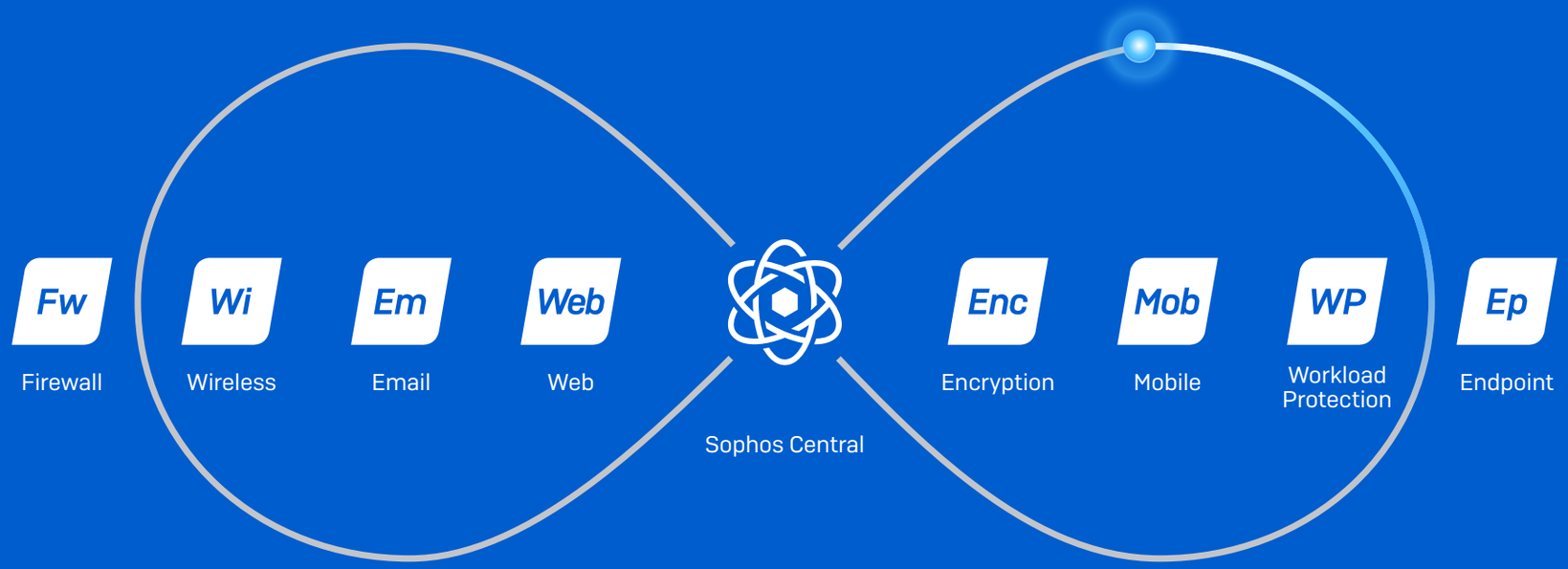
MÁS INFORMACIÓN

- Toda la actualidad de la Administración Pública
- Tendencias Tecnológicas Digitales 2022
- TIC Monitor Diciembre 2021

TENDENCIAS DISRUPTIVAS QUE MARCARÁN LA DIGITALIZACIÓN EN 2022

La velocidad de la Transformación Digital de las empresas en nuestro país se ha acelerado mucho en los últimos 24 meses. Los retos y exigencias puestos sobre la mesa por la situación generada por la pandemia han provocado que en este tiempo se haya recorrido un camino que estaba previsto para varios años. Sin embargo, esta evolución no se detiene, y las compañías tienen que seguir integrando nuevas tendencias tecnológicas en sus procesos de negocio porque en la economía digital el que no avanza se queda atrás.

Synchronized Security



Una de cada tres pequeñas organizaciones fue atacada por ransomware en el último año No sea la próxima víctima

Con las ayudas del gobierno para el KIT DIGITAL puede contar con SOPHOS para la mejor ciberseguridad

Contacte con nosotros:
www.sophos.com/es-es · 913 756 756 · ComercialES@Sophos.com

SOPHOS
Cybersecurity delivered.

Europa da los primeros pasos para liderar la industria de semiconductores

33.000 millones de euros en la primera fase y hasta 80.000 millones de euros en la próxima década. Ésta es la inversión que va a realizar Intel en la Unión Europea. Concretamente la inversión se realizará en Francia, Alemania, Irlanda, Italia, Polonia y España y tiene el objetivo de "impulsar un ecosistema de semiconductores de clase mundial en Europa".

Intel acaba de anunciar una inversión de hasta 80.000 millones de euros en la Unión Europea durante la próxima década. Concretamente, la inversión se realizará "a lo largo de toda la cadena de valor de los semiconductores, desde la investigación y el desarrollo (I+D) hasta la fabricación y las tecnologías de envasado más avanzadas".

En una primera fase, Intel va a invertir 33.000 millones de euros entre los que se incluyen 17.000 millones de euros para crear una "megafábrica de semiconductores de vanguardia en Alemania" que supondrá la creación de 7.000 empleos durante la construcción de la fábrica y 3.000 empleos permanentes de alta cualificación en Intel. Además, también va a desarrollar un nuevo centro de I+D y diseño en Francia e invertirá en I+D, fabricación y servicios de fundición en Irlanda, Italia, Polonia y España.

"Con esta inversión histórica, Intel planea traer su tecnología más avanzada a Europa,

ÚRSULA VON DER LEYEN COMENTA EL ANUNCIO DE INTEL DE INVERTIR EN LA EU

creando un ecosistema de chips europeo de nueva generación y abordando la necesidad de una cadena de suministro más equilibrada y resistente", destaca la firma en un comunicado.

IMPULSAR LA INNOVACIÓN EN LA UE

"Nuestras inversiones previstas son un paso importante tanto para Intel como para Europa", ha destacado Pat Gelsinger, CEO de Intel. "La Ley de Chips de la UE permitirá a las empresas privadas y a los gobiernos trabajar juntos para hacer avanzar drásticamente la posición de Europa. Esta amplia iniciativa impulsará la innovación en I+D de Europa y traerá la fabricación de vanguardia a la región en beneficio de nuestros clientes y socios de todo el mundo. Nos comprometemos a desempeñar un papel esencial en la configuración del futuro digital de Europa durante las próximas décadas".

Intel destaca que el programa de inversión se centra "en equilibrar la cadena de suministro de semiconductores a nivel mundial con una importante expansión de las capacidades de producción de Intel en Europa". En la fase inicial, Intel tiene previsto desarrollar dos fábricas de semiconductores en Magdeburgo (Alemania), la capital de Sajonia-Anhalt que estarán en funcionamiento en 2027.

Intel también invertirá 12.000 millones de euros en su proyecto de expansión de Leixlip (Irlanda) y 4.500 millones de euros en habilitar una fábrica de back-end de última generación en Italia. En Francia construirá un nuevo centro europeo en Plateau de Saclay que supondrá la creación de 1.000 puestos de trabajo, mientras que el laboratorio de I+D en Polonia se ampliará.

En el caso de España, Intel destaca que "durante la última década el Barcelona Supercomputing Center e Intel han colaborado en la arquitectura de exaescala. Ahora, están desarrollando una arquitectura de zettascale para la próxima década. El centro de supercomputación e Intel planean establecer laboratorios conjuntos en Barcelona para avanzar en la computación".

PRIMER LOGRO IMPORTANTE DE LA LEY DE CHIPS EUROPEA

El "primer logro importante" de la Ley de Chips. Así ha definido Úrsula Von der Leyen, presidenta de la Comisión Europea, el anuncio que ha realizado Intel y en el que ha comunicado que, en una primera fase, va a invertir hasta 33.000 millones de euros en la creación de un ecosistema de semiconductores global en la Unión Europea.

"Con la Ley de chips de la UE, queremos convertir a Europa en líder de la producción mundial de semiconductores. Y también queremos reforzar nuestra capacidad de resistencia, con tecnologías seguras y de producción propia, que son activos inestimables en el mundo turbulento en el que vivimos", ha destacado Von der Leyen en un comunicado.

> "La Ley de Chips de la UE permitirá a las empresas privadas y a los gobiernos trabajar juntos para hacer avanzar drásticamente la posición de Europa"
>
> PAT GELSINGER, CEO DE INTEL

La presidenta de la Comisión Europea ha recordado que el objetivo es "tener el 20% de la producción mundial de microchips en Europa, para 2030. Es decir, el doble que hoy, en un mercado que se duplicará en la próxima década".

MÁS ALLÁ DE LAS CIFRAS

Pero, no se trata sólo de cantidad. “Quiero que Europa cruce nuevas fronteras en materia de innovación. Romper la barrera de los nodos de 3 nanómetros, por ejemplo. Creando chips energéticamente eficientes. Y también desarrollar nuevas tecnologías, nuevos productos y aplicaciones, que nuestras mentes ni siquiera pueden concebir hoy”. Ante este reto, Von der Leyen reclama la creación de “una red de institutos de investigación, prototipos, pruebas e instalaciones avanzadas de producción y embalaje, en todo el continente. En resumen: necesitamos un verdadero enfoque de toda Europa”.

Para lograr esto, “es necesario invertir”. En total, se invertirán más “de 43.000 millones de euros de inversión pública, tanto de la UE como de los países”, para apoyar la Ley de chips de la UE hasta 2030. “Hará de Europa un lugar más atractivo para que las empresas tecnológicas inviertan en el desarrollo y la producción de chips de última generación”.

En relación al anuncio de Intel, éste “es el primer gran logro de la Ley de chips de la UE. Una inversión de 80.000 millones de euros durante la próxima década en toda la cadena de valor de los semiconductores. Desde la I+D hasta la fabricación y el embalaje avanzado. Con muchos socios locales fuertes”. ■

INTEL ANUNCIA UNA INVERSIÓN DE 80.000 MILLONES DE EUROS EN EUROPA

MÁS INFORMACIÓN

Comunicado de Úrsula Von der Leyen tras el anuncio de inversión de Intel en Europa

> “La Ley de Chips hará de Europa un lugar más atractivo para que las empresas tecnológicas inviertan en el desarrollo y la producción de chips de última generación”

Meta anuncia una fuerte inversión en España y la contratación de 2.000 personas en cinco años

La compañía de Zuckerberg acaba de anunciar una importante inversión en España, que incluye la contratación hasta 2.000 personas en los próximos cinco años y la creación del primer Meta Lab del mundo, con espacio para los emprendedores tecnológicos y startups locales. La compañía también está invirtiendo en la infraestructura digital del país con un nuevo cable transatlántico, e iniciando el proceso para la construcción de un nuevo centro de datos.

Meta, la matriz de Facebook, acaba de anunciar una significativa inversión en personal e infraestructuras en España, situándolo, dice la multinacional, "en el centro de nuestros planes" mediante la creación de nuevos puestos de trabajo altamente cualificados, el apoyo a los emprendedores y empresas tecnológicas locales y la inversión en infraestructuras digitales esenciales.

En sus planes figura la contratación de hasta 2.000 personas en los próximos cinco años y la generación del primer Meta Lab del mundo, un lugar de apoyo para los trabajadores en remoto de Meta en España, con espacio para los emprendedores tecnológicos y startups loca-

les. Además, tiene previsto duplicar el espacio de su oficinas en Madrid.

Dentro de estas inversiones la recientemente anunciada colaboración con Telefónica para establecer un Metaverse Innovation Hub en Madrid para ayudar a acelerar la preparación de la red y los dispositivos del metaverso.

En lo que respecta a infraestructura digital, la firma iniciando el proceso que nos permitirá construir un nuevo centro de datos, que estará situado en Castilla-La Mancha, y en un nuevo cable submarino transatlántico, que será el primero de medio petabit del mundo, uniéndose al cable Marea ya existente. De ambos subraya que beneficiarán a otras empresas tecnológicas, impulsando la innovación y el crecimiento en todo el sector. Según un estudio independiente, solo el cable Marea aporta unos 18.000 millones de dólares cada año a la economía europea desde 2019.

La compañía también quiere explorar posibles colaboraciones entre la industria, el sector académico y el Gobierno para trabajar en la construcción del metaverso de forma responsable, incluyendo la privacidad, la seguridad y la diversidad.

ESPERA "A LA VANGUARDIA EUROPEA"

Sobre la elección de España como país para invertir, señala que "está a la vanguardia de la tecnología europea", con dos fuertes centros tecnológicos, Madrid y Barcelona, a los que se han unido

CONTENIDOS↓

La Comisión Europea abre un investigación antimonopolio a Google y Meta

Google y Meta, matriz de Facebook, se enfrentan a una investigación antimonopolio en la Unión Europea, relacionada con un acuerdo que ambas compañías firmaron en septiembre de 2018 para la participación de la Audience Network de Meta en el programa Open Bidding de Google.

Google ofrece servicios de tecnología publicitaria que actúan como intermediarios entre los anunciantes y los editores mediante subastas en tiempo real de espacios publicitarios online en sitios web o aplicaciones móviles, incluso a través de su 'programa de licitación abierta'. Meta proporciona servicios de publicidad digital y, a través de su 'Meta Audience Network', participa en subastas de espacios publicitarios de editores externos utilizando los servicios de tecnología publicitaria de Google y sus rivales.

A la Comisión le preocupa que el acuerdo pueda haber perjudicado a otros servicios de tecnología publicitaria que compiten con el programa Open Bidding de Google y, por lo tanto, restringir o distorsionar la competencia en los mercados de publicidad display online, en detrimento de los editores y, en última instancia, de los consumidores.

Si se prueba, las prácticas investigadas pueden infringir las normas de competencia de la UE en materia de acuerdos anticompetitivos entre empresas y/o abuso de posición dominante.

Además, la Comisión cooperará con la Autoridad del Mercado de la Competencia del Reino Unido (CMA), que ha iniciado su propia investigación sobre el acuerdo entre Google y Meta.

No existe un plazo legal para completar una investigación, pero la Comisión ha dicho que la llevará a cabo en profundidad y con carácter prioritario.

Valencia y Andalucía. Además, se están registrando niveles récord de inversión en startups que resuelven todo tipo de problemas, desde la entrega de comida online hasta la neuroelectrónica.

En su comunicado, dice que espera que su Meta Lab "juegue un papel importante en la escena tecnológica española y ayude a sentar las bases para que España se beneficie del metaverso. Será un espacio para las alianzas, la colaboración y la innovación, del que destaca que es una nueva fase de Internet construida en torno a experiencias virtuales interconectadas. "El metaverso no pertenecerá a ninguna empresa y no surgirá de la noche a la mañana, pero tiene el potencial de ayudar a desbloquear el acceso a nuevas oportunidades creativas, sociales y económicas, y queremos que los españoles nos ayuden a darle forma desde el principio", asegura.

TELEFÓNICA COLABORARÁ CON META PARA AMPLIAR Y EXPLORAR LAS TECNOLOGÍAS DEL METAVERSO

El hub de innovación abierta de Telefónica, Wayra, ha abierto una convocatoria global en busca de startups del metaverso. Así lo anunció Chema Alonso, Chief Digital Officer de Telefónica, en su ponencia en Four Years from Now (4YFN).

Según ha informado, Open2metaverse es una convocatoria de ámbito global de búsqueda para apoyar a las empresas con las mejores tecnologías con aplicaciones para el metaverso a que crezcan y alcancen una escala global más rápidamente, conectándolas con Telefónica para generar oportunidades conjuntas. Los casos de uso en los que se centrará Wayra pondrá el foco en compañías que estén desarrollando estos casos de uso: conectividad, dispositivos, plataformas virtuales, herramientas de identidad, NFT y marketplaces, entre otros.

El hub de innovación abierta de Telefónica, Wayra, ha abierto una convocatoria global en busca de startups del metaverso

Open2metaverse es el primer proyecto conjunto de exploración y conocimiento que alcanza a las iniciativas de innovación Wayra X, Telefónica Ventures y los siete hubs que Wayra tiene en Latinoamérica y Europa.

Chema Alonso ha desvelado también una colaboración con Meta para ampliar y explorar conjuntamente nuevas formas de impulsar la innovación en conectividad y tecnológica en el campo del metaverso y desbloquear desarrollos de nuevos casos de uso.

Las dos compañías planean establecer un centro de innovación del metaverso para ayudar a acelerar la preparación de la red y los dispositivos metaversos a través de pruebas, casos de uso de experiencias metaversas y pruebas de dispositivos, entre otras cosas. A través de este Metaverse Innovation Hub, quieren proporcionar a las startups y desarrolladores locales acceso a un laboratorio 5G donde podrán utilizar un banco de pruebas metaverso de extremo a extremo en la infraestructura y equipos de red de Meta y Telefónica, así como beneficiarse del ecosistema de innovación abierta de Telefónica y de los recursos del Hub de Innovación y Talento de Telefónica, así como del apoyo, las herramientas y los recursos de ingeniería de Meta. Esta colaboración se dirigirá inicialmente a startups y desarrolladores seleccionados por Wayra. ■

MÁS INFORMACIÓN

- Metaverso, el espacio virtual que liderará la nueva revolución digital
- Metaverso, economía virtual de la Web 3.0
- Meta: inversiones para innovar en España

Despliegue la seguridad de ONE

Aumente su protección con ONE plataforma de seguridad unificada

Cohesiva

Administrada en la nube

Inteligente

WatchGuard Technologies | www.watchguard.com/es | sales-iberia@watchguard.com | +34 91 123 2196

Así es la Ley de Datos que propone la Comisión Europea

La Comisión Europea ha propuesto nuevas normas para regular quién puede utilizar los datos generados en la UE en todos los sectores económicos y acceder a ellos. Se agrupan en la Ley de Datos, que pondrá a disposición más datos para su reutilización y se prevé que generen 270.000 millones de euros de PIB adicional de aquí a 2028.

La nueva propuesta es el último componente horizontal de la estrategia de datos de la Comisión desempeñará un papel clave en la transformación digital, en consonancia con los objetivos digitales para 2030.

El volumen de datos aumenta constantemente y pasará de 33 zettabytes generados en 2018 a 175 zettabytes previstos para 2025. Se trata de un potencial sin explotar y el 80% de los datos industriales nunca se utiliza. La Ley de Datos aborda los problemas jurídicos, económicos y técnicos que se traducen en su infrautilización, y pondrá a disposición más datos para su reutilización que, según los cálculos, pueden llegar a generar 270.000 millones de euros de PIB adicional de aquí a 2028.

EXPLOTACIÓN DE LOS DATOS ACORDE A LAS NORMATIVAS EUROPEAS

En este sentido, según el organismo europeo, a través de Thierry Breton, comisario de Mercado Interior, "hasta ahora solo se ha utilizado una pequeña parte de los datos industriales y el potencial de crecimiento e innovación es enorme. La Ley de Datos garantizará que los datos industriales se intercambien, almacenen y traten respetando plenamente las normas europeas. Constituirá la piedra angular de una economía digital europea fuerte, innovadora y soberana".

La propuesta incluye medidas que permitan a los usuarios de dispositivos conectados acceder a los datos generados por ellos, que suelen recoger exclusivamente los fabricantes, e intercambiarlos con terceros para prestar servicios de postventa u otros servicios innovadores basados en datos. Mantiene incentivos para que los fabricantes sigan invirtiendo en la generación de datos de alta calidad al cubrir sus costes relacionados con la transferencia y excluir el uso de datos intercambiados en competencia directa con sus productos.

También incorpora pautas para reequilibrar el poder de negociación de las pymes mediante la prevención del abuso de los desequilibrios contractuales en los contratos de intercambio de datos. En este sentido, les protegerá de las cláusulas contractuales abusivas impuestas por una parte con una posición negociadora mucho más fuerte. La Comisión también formulará modelos de cláusulas para ayudar a estas empresas a redactar y negociar contratos equitativos de intercambio de datos.

Contempla, además, medios para que los organismos del sector público obtengan y usen datos en poder del sector privado que sean necesarios en circunstancias excepcionales, especialmente en caso de emergencias públicas como inundaciones e incendios forestales, si los datos no están disponibles de otro modo. La información sobre los datos es necesaria para responder con rapidez y seguridad, a la vez que se reduce al mínimo la carga para las empresas.

Asimismo, la Ley añade normas que permitan a los clientes cambiar efectivamente de proveedores de servicios de tratamiento de datos en la nube y establezcan salvaguardias contra la transferencia ilegal de datos.

Además, revisa determinados aspectos de la Directiva sobre bases de datos, que se formuló en la década de 1990 para proteger las inversiones en la presentación estructurada de los datos. En particular, aclara que las bases de datos que contienen información procedente de dispositivos y objetos de la internet de las cosas no deben estar sujetas a una protección jurídica independiente. Esto garantizará su acceso y utilización.

Tras la Ley de Gobernanza de Datos, ésta es la segunda gran iniciativa legislativa derivada de la estrategia europea de datos de febrero de 2020, cuyo objetivo es poner a la UE en la vanguardia de nuestra sociedad basada en la información. ■

Clica en la imagen para ver la infografía más grande

MÁS INFORMACIÓN

- Estrategia europea de datos
- Ley europea de Datos
- Comunicado de la Estrategia Europea de Datos

¿Qué esperar de la Web 3.0?

La Web 3.0 o la tercera generación de servicios de Internet promete un nuevo paradigma, marcado por la descentralización y la vuelta del control de los datos a manos del usuario. ¿Qué es y qué podemos esperar en los próximos años de esta evolución? Echamos una mirada al futuro de la mano de los expertos de IEBS Business School.

Hace ya años, el científico de la computación británico al que todos conocemos por ser el padre de la World Wide Web, Tim Berners-Lee, acuñó el término 'Web Semántica' para describir una red en la que las máquinas procesarían el contenido de forma similar a la humana y en la que todos los datos estarían conectados y se entenderían tanto contextual como conceptualmente. Hoy, en pleno desarrollo de la Web 2.0, ya se pueden atisbar lo que IEBS Business School llama "primeros brotes" que emergen del próximo cambio del paradigma en las aplicaciones de Internet denominadas Web 3.0 o Web3, que se centrará en el uso de una comprensión de datos basada en máquinas para proporcionar una Web semántica y datificada.

"El objetivo final de la Web 3.0 es crear sitios web más inteligentes, conectados y abiertos. Aunque todavía no está implementada, existen algunas tecnologías que definirán esta nueva web que ya se están desarrollando", explican desde esta escuela de negocios digital aludien-

¿QUÉ ES LA WEB 3.0 Y POR QUÉ PUEDE SER LA RED DEL FUTURO?

do, como ejemplo, a los electrodomésticos inteligentes que utilizan redes inalámbricas e IoT.

LO QUE PODRÍA ESTAR POR LLEGAR

Según su análisis, los principales beneficios que ponemos esperar de la próxima generación de Internet serán los siguientes:

❖ **Fiabilidad:** esta red dará a los creadores y usuarios más libertad en general. Garantizará que estos últimos siempre tengan control sobre sus datos online mediante la utilización de redes descentralizadas. También se espera que la próxima versión de Internet sea más fiable dada su naturaleza descentralizada, lo que elimina la posibilidad de un punto único de falla.

❖ **Para todos:** no necesita ser controlada por una sola entidad. Es posible que las empresas más grandes ya no tengan un control total sobre Internet. Como resultado, las aplicaciones descentralizadas o apps no se pueden censurar ni restringir de ninguna forma.

❖ **Personalización:** también se podrá personalizar la experiencia de navegación del internauta porque este tipo de web podrá entender sus preferencias. Esto también permitirá navegar de forma más productiva.

❖ **Vender mejor:** los vendedores entenderán mejor las necesidades de compra de sus clientes y les mostrarán aquellos productos y servicios que les interesa comprar con la ayuda de la inteligencia artificial. Esto permitirá ver mejores anuncios y más relevantes, que tendrán más probabilidades de conversión.

❖ **Menos interrupciones:** dado que los datos se almacenarán en bases distribuidas por la descentralización, los usuarios no tendrán que preocuparse por interrupciones del servicio o por suspensiones de cuentas por motivos técnicos.

❖ **Más segura:** la Web3 utiliza tecnología Blockchain, a diferencia de la Web 2.0, que aprovecha Internet para desarrollar aplicaciones. Es técnicamente más seguro almacenar datos de clientes en una cadena de bloques, ya que está descentralizado y su uso por parte de las empresas es transparente, por lo que los protege de los piratas informáticos.

❖ **Descentralizada:** la tecnología Blockchain, además, integra la descentralización. Esto permite a los usuarios dos cosas: por un lado, protege sus datos y, por otro lado, establece una interacción directa sin intermediarios.

Los próximos años van a ser decisivos para que se lleve a cabo esta evolución. ■

MÁS INFORMACIÓN

- Qué es la Web 3.0
- Web 3.0: la nueva revolución de Internet

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

Digital Security
Progress. Protected.

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

ENTREVISTA

JORGE GONZÁLEZ PÉREZ, CIO GLOBAL DE ADOLFO DOMÍNGUEZ

“La dimensión tecnológica en Adolfo Domínguez es una prioridad esencial para la compañía”

Foto: Punto GA / M. Riopa

Pablo García Reales

Uno de los sectores más castigados por la pandemia ha sido indudablemente el de la moda, ante la imposibilidad de abrir sus tiendas durante semanas, así como por las innumerables restricciones a las que se vio sometido durante los meses siguientes. Pero, como ha sucedido en otros verticales, ha sabido adaptarse en tiempo record a una situación mundial inimaginable y aflorar con un impresionante grado de resiliencia que le ha permitido mirar al presente y al futuro con un marcado optimismo.

La multinacional española Adolfo Domínguez es un ejemplo más que notable de esta nueva realidad, y por ello ha decidido poner en manos de su nuevo CIO Global su estrategia tecnológica redimensionada, que sea asienta en pilares como la ciberseguridad, los canales online o el conocimiento del cliente, a través de políticas orientadas al dato y a la información. Jorge González Pérez nos revela a continuación todos los detalles.

¿Cuáles son los principales rasgos que conforman la fotografía de la estrategia actual de Adolfo Domínguez en materia de Tecnologías de la Información y la Comunicación?

La dimensión tecnológica en Adolfo Domínguez es una prioridad esencial para la compañía. De hecho, aproximadamente el 53% de las iniciativas proyectadas que se llevarán a cabo en los próximos años desembocan en el ámbito digital y en su implementación.

En los últimos meses hemos llevado a cabo un gran ejercicio de análisis para conocer con exactitud los proyectos tecnológicos más demandados por la organización y, a partir de ahí, fijar en qué debemos mejorar. Hemos realizado entrevistas con todas las áreas de la compañía, de tal forma que hemos localizado objetivamente aquellos puntos que debemos reforzar o desarrollar. Estamos hablando de diferentes dimensiones tecnológicas, como la ciberseguridad, los canales online o el conocimiento del cliente, a través de estrategias orientadas al dato y a la información.

El objetivo es implantar una serie de acciones ajustadas en el tiempo y con un calendario de prioridades a lo largo de los próximos tres años, pero siempre desde una visión global de la compañía.

Foto: Punto GA / M. Riopa

¿Cómo ha afrontado Adolfo Domínguez estos dos años de pandemia tan complejos, especialmente para el sector retail, desde la perspectiva tecnológica?

Han sido dos años muy duros para todos, tanto en lo personal como en lo profesional. No debemos olvidarlo. La compañía, ante una situación inédita, adoptó de forma rápida acciones dirigidas, por un lado, para salvaguardar la salud de sus trabajadores y, por otro, para fortalecer todo aquello que pudiera permitirnos estar a flote, como el desarrollo del ecommerce, ante la imposibilidad de la venta física provocada por la obligación del cierre de todas las tiendas. Hubo momentos en los que más del 95% de nuestras tiendas estuvieron cerradas.

¿Cuáles han sido los principales focos y retos de la compañía, tanto a nivel interno como externo, en este ámbito durante este periodo?

El principal objetivo fue salvar la compañía en una situación, no solo desconocida, sino también cambiante. A partir de ahí, destacaría nuestra capacidad de adaptación y respuesta ante una realidad mundial desconocida e inimaginable. Evidentemente, nos hemos visto obligados a tomar muchas decisiones y de forma rápida, como la adopción de mecanismos de teletrabajo (dotación de PCs portátiles,

configuración de sistemas VPN, adecuación y refuerzo de sistemas de seguridad perimetrales y endpoints, herramientas de colaboración, etc.).

Por otra parte, el hecho de apostar por soluciones SaaS en cloud públicas, nos ha facilitado la elasticidad necesaria para adecuarnos a esta época tan difícil. Nos ha facilitado mucho su implementación y su adopción por parte de todos los usuarios de la compañía.

¿Cuál es la estrategia de Adolfo Domínguez en el ámbito de la ciberseguridad?

Los ciberataques se han convertido en un negocio que crece de forma exponencial. El hackeo se ha profesionalizado, transformándose en un negocio de secuestro y rescate. Los riesgos digitales son cada vez mayores y más sofisticados y hay que estar preparados para afrontarlos y gestionarlos de una forma correcta, rápida y sin que afecte al transcurso diario de la compañía. Ejemplos como la actual situación en Ucrania, no ha hecho más que enfatizar que la ciberseguridad es un arma capaz de paralizar las actividades de una empresa u organismo público.

En Adolfo Domínguez somos conscientes de ello y mantenemos una sensibilidad especial en estos temas. Incorporamos los riesgos cibernéticos a los riesgos operacionales de la organización, dedicándoles el mismo esfuerzo y dándoles la misma importancia.

Dentro de las iniciativas analizadas, hacemos un especial énfasis en el reforzamiento de toda nuestra área tecnológica en cuanto a la adecuación de nuevos procedimientos como planes de continuidad o de recuperación ante desastres, soluciones tecnológicas de última generación (haciendo especial hincapié en un Centro de Operaciones de Seguridad o SOC), y adopción de políticas y marcos internacionales estandarizados, como RGPD o ISO 27001, que nos permitan mantener un ecosistema digital seguro.

¿De qué manera está afrontando Adolfo Domínguez su estrategia de analítica e inteligencia del dato de cara a conocer mejor al cliente?

Vivimos en la era del dato, y cada vez somos más consciente de que es uno de nuestros activos más valiosos. Este recurso nos aporta valor al negocio y, sobre todo, ventajas competitivas en el ámbito de la actividad comercial. Dependemos, en gran medida, de un mejor conocimiento de nuestros clientes, y esto requiere utilizar inteligencia de negocio aplicada en todas las áreas, actuar en base a la información, y adecuar mejor nuestros productos y servicios, a las necesidades del cliente.

La estrategia del dato viene dada a través de varias acciones en las que estamos trabajando ahora mismo, como implementar un sistema de gobierno que garantice su control, privacidad y seguridad; democratizar el dato, de tal forma

Foto: Punto GA / M. Riopa

Biografía

Jorge González Pérez, nacido en Cáceres en 1980, es Ingeniero Informático por la Universidad Isabel I, Executive MBA por la EAE Business School y cuenta con el Máster por la OBS en Desarrollo de negocio y transformación digital. Jorge es un entusiasta digital con más de 20 años de experiencia en el ámbito de las tecnologías de la información, consultoría y proyectos de transformación digital, con un amplio bagaje en la relación con clientes y las estrategias TI. Durante su vida laboral ha desarrollado diferentes funciones en empresas nacionales e internacionales, demostrando un fuerte compromiso con la transformación digital de las organizaciones, asumiendo un papel clave en las fases de visión, diseño e implementación de nuevos servicios, y ayudando a empresas privadas y organismos públicos a desarrollar proyectos estratégicos tanto en tecnología como en nuevos modelos de negocio, con un gran impacto en las cuentas de resultados. En febrero de 2022 se incorporó a Adolfo Domínguez para el desarrollo de la implantación tecnológica de la multinacional.

que todas las áreas tengan acceso a una única fuente de información; y acelerar la adopción de datos no estructurados mediante plataformas de Big Data.

Nuestro objetivo final es conocer mejor al cliente para poder ofrecerle un mejor servicio y que crezca su satisfacción.

¿Cuál es la visión de Adolfo Domínguez con respecto al gran desafío que representa por el sector retail el empuje del e-commerce y la tensión que genera en la logística y la cadena de suministro al pasar de los grandes volúmenes a la venta al detalle, que supone que compañías como la suya tengan que competir con los nuevos marketplaces también en ese ámbito?

El crecimiento del comercio electrónico continuará siendo muy significativo durante los próximos años. Las ventas online se han incrementado un 36% en el tercer trimestre del ejercicio 2021/22 (septiembre-noviembre 2021) con respecto al 2019. Hemos pasado súbitamente de un modelo más tradicional a un escenario mucho más complejo. No solo tienes el desafío de enviar grandes volúmenes a tiendas o a áreas geográficas, sino que también cuentas con el desafío del servicio de venta unitaria hasta el domicilio.

El reto reside en cómo damos respuesta al cambio de un modelo en el cual se estaban gestionando envíos de manera rutinaria a tiendas o a zonas geográficas, con un procedimiento establecido, a un modelo más orientado al cliente final mediante envíos unitarios.

En Adolfo Domínguez seguimos invirtiendo en nuevas herramientas, por ejemplo, orientadas a una mejor gestión y control de los almacenes y de la logística, que nos permitan seguir de manera escrupulosa la trazabilidad de una prenda, por ejemplo, siendo lo más eficientes y ágiles posibles.

Foto: Punto GA / M. Riopa

"En Adolfo Domínguez somos conscientes de la ciberseguridad y mantenemos una sensibilidad especial en estos temas. Incorporamos los riesgos cibernéticos a los riesgos operacionales de la organización, dedicándoles el mismo esfuerzo y dándoles la misma importancia"

¿En qué otros proyectos futuros se está embarcando Adolfo Domínguez para salir reforzado de la actual coyuntura marcada por el COVID-19?

La verdad es que cada área de Adolfo Domínguez está sumergida en proyectos de futuro. Son iniciativas clave para los próximos 3 años, tanto a nivel de marketing, de logística, y, por supuesto, también de producto. También me gustaría destacar proyectos relacionados directamente y desde distintos ángulos con la sostenibilidad. En nuestro ADN está la sostenibilidad. Mantenemos un compromiso real para mejorar el medio ambiente en cada paso que damos.

De hecho, Adolfo Domínguez ha puesto en marcha un proyecto de I+D+i para reciclar las perchas de madera en desuso de su red comercial, en una investigación desarrollada con dos centros tecnológicos de Ourense y Braga. Ya hemos reciclado las 15.000 primeras perchas, que se comenzarán a reutilizar en sus 342 tiendas en 17 países.

También ya producimos prendas de vestir utilizando tejidos procedentes de madera de bosques sostenibles. El proyecto incluye prendas confeccionadas al 100% con este tipo de telas, así como mezclas con otros tejidos tradicionales de algodón, lino o lana. Bajo el lema `Vístete de árbol´, el grupo Adolfo Domínguez hace una nueva apuesta por la moda sostenible y responsable. ■

Adolfo Domínguez: más de 70 años haciendo historia

Estos son algunos de los principales hitos de la legendaria firma de moda española:

1950: ORIGEN: Nace la sastrería camisería 'El Faro' en un pequeño taller familiar de sastrería en Ourense (Galicia), origen del grupo Adolfo Domínguez como empresa textil, que abre su primera tienda en 1970.

1992: La internacionalización. Una vez consolidada en España, la firma se abre a otros mercados. Actualmente, cuenta con 349 puntos de venta en 18 países de los 5 continentes.

1997: Salida a bolsa. Los éxitos comerciales y el reconocimiento internacional de Adolfo Domínguez se reflejan en su salida a bolsa. Es la primera firma de moda de España en cotizar en el mercado continuo español. Todo un hito para la proyección y la estabilidad de la empresa.

ACTUALIDAD: Tras unos trimestres realmente complejos por la pandemia, al igual que el resto de compañías no solo de los sectores de la moda y el retail sino de prácticamente todos los mercados, Adolfo Domínguez cosecha unos notables resultados financieros en su tercer trimestre fiscal de 2021 (septiembre-noviembre 2021):

- ❖ EBITDA de 2,8 millones de euros, que supera en un 33% al del mismo período del ejercicio 2019/20.
- ❖ Las ventas crecen un 47% y alcanzan los 60,4 millones de euros en el acumulado del ejercicio (marzo-noviembre 2021).
- ❖ Se ha recuperado el 88% de las ventas respecto al mismo periodo del ejercicio 2019/20, antes de la crisis del coronavirus.
- ❖ Las ventas online crecen un 6,2% en los nueves primeros meses del ejercicio (marzo-noviembre 2021) y un 36,1% respecto al mismo periodo de 2019/20.

MÁS INFORMACIÓN

- Los CIO marcan sus prioridades tecnológicas para 2022
- Prioridades tecnológicas para los CIO en 2022

Bitdefender®

BUILT FOR RESILIENCE

Protegemos tu negocio
Protegemos a tus clientes

- eXtended Endpoint Detection and Response (XEDR)
- Managed Detection and Response (MDR)
- Cloud Workload Security (CWS)

www.bitdefender.es/business

Las empresas se enfrentan a problemas de retención del talento tecnológico

Los empleados de TI son los más propensos a dejar su puesto de trabajo si se compara con el resto de áreas de su empresa, según una encuesta de Gartner en la que han participado 18.000 empleados de 40 países, de los cuales 1.755 trabajaban en TI. Sus datos indican que solo el 29,1% de los trabajadores de TI tienen una intención firme de permanecer con su empleador actual. El problema es más intenso en regiones como Asia, donde el porcentaje baja al 19,6

En el corto plazo los CIO van a tener que hacer frente a un nuevo problema: la retención de su personal. Según un estudio de Gartner a nivel mundial, solo un 29% de los empleados de TI tiene la firme intención de permanecer en su actual empresa.

%, Australia y Nueva Zelanda (23,6 %) y América Latina (26,9 %), pero, incluso en Europa, la región con resultados más alentadores, solo cuatro de cada diez (38,8 %) tienen una gran intención de quedarse.

Por franjas de edad también se observan diferencias. El desafío es más intenso entre los empleados de TI menores de 30 años ya que, según la encuesta, solo el 19,9% de los trabajadores tienen una alta probabilidad de quedarse, en comparación con el 48,1% de los que tienen entre 50 y 70 años.

Los analistas de Gartner recomiendan a los CIO que adopten un enfoque basado en datos para identificar a los trabajadores que están en mayor riesgo y los más valiosos, y adaptar las políticas de trabajo híbridas para mantenerlos comprometidos y con un alto rendimiento.

Además, les aconseja que impulsen modelos de trabajo centrados en las personas impulsen políticas más flexibles para reducir el desgaste de los trabajadores, permitiendo a los equipos decidir cuando hacen mejor su trabajo o estableciendo nuevos horarios, como la jornada de cuatro días. En este grupo de medidas incluye también la adopción del trabajo híbrido, que reconoce que los empleados pueden ser completamente productivos de forma remota. Además, Gartner recuerda también que las reuniones presenciales para tomar decisiones ya no son necesarias como años atrás, ya que tecnología permite la colaboración y la creatividad distribuidas.

LOS SALARIOS DEL SECTOR TECNOLÓGICO SUBIRÁN EN 2022

Según la Guía del Mercado Laboral 2022, el pasado año los sueldos del sector se estabilizaron con una caída del 1%, lo que supuso un cambio de tendencia después de que los últimos tres años los salarios de esta área se incrementasen en un 9%. Durante este periodo, los profesionales de TI fueron de los que más vieron aumentar sus nóminas, junto con el sector legal, logístico y digital.

España es el quinto país de la UE con más desempleo femenino en el sector TI

Con motivo del Día Internacional de la Mujer, Esri España lanzó un mapa interactivo que permite explorar visualmente y por países la brecha de género en el terreno laboral del sector tecnológico en la Unión Europea, con datos de Eurostat.

Según Eurostat, España es uno de los países europeos que presentan mayor tasa de desempleo femenino en el sector científico y tecnológico. En España la tasa de desempleo en mujeres en el sector con formación superior es del 10,8%, porcentaje que en la Unión Europea solo superan Turquía, Grecia, Macedonia del Norte y Montenegro con una tasa de desempleo en mujeres con formación superior del 15,6%, 13,5%, 12,5% y un 10,8%, respectivamente. En cuanto a las mujeres sin formación superior, el ratio se sitúa a un 24,4%, solo superado por Grecia (25,2%) y Montenegro (24,8%).

Después de Grecia, España es el segundo país con más diferencias en el paro entre hombres y mujeres: de 3% y 6% entre hombres y mujeres con estudios y sin estudios superiores. República Checa, Alemania y Países Bajos son los países con menor tasa de desempleo en mujeres con formación superior: 1,1%, 1,4% y 2%, respectivamente; y en el caso de mujeres que no cuentan formación superior del 4,4%, 5,4% y 6,5%, respectivamente.

Según los datos del visor de Esri, los países vecinos de España, Portugal y Francia, tienen una tasa de desempleo en mujeres con formación superior del 4,6% y 4,30%, respectivamente; y del 9,1% y 12,6% en el caso de mujeres sin formación superior. Italia, presenta tasas similares con un 4,4% de desempleo en mujeres con formación superior y un 14,4% de desempleo en mujeres sin formación superior.

Ahora se prevé que vuelvan a crecer como años atrás. La realidad del sector durante la pandemia ha tenido varios momentos de montaña rusa, puesto que durante los inicios de la covid-19 cerraron algunas startups y se paralizaron grandes proyectos tecnológicos. "Si bien en abril de 2020 percibimos un estancamiento en la demanda de este tipo de profesionales, pocos meses después se revirtió la situación debido a una inflación salarial y de ofertas laborales", afirma Selena Sabiote, Manager en HAYS Technology.

El principal factor para anticipar una subida de salarios este año es la inflación, pero también que "hay muchas empresas que están instalando sus sedes de Data, e-Commerce y Cloud en España, sobre todo en Barcelona. Esto implica que el pool de candidatos sea el mismo y haya más demanda, lo que provoca que se fichen perfiles de una empresa a otra a golpe de talonario", asegura la experta.

Los perfiles más solicitados son los Data Engineer, con salarios que van desde los 30.000 euros hasta los 68.000 euros; Data Scientist, entre los 26.000 euros y los 65.000 euros, y Cloud Engineer/DevOps, cuyos sueldos se encuentran entre los 29.000 euros y los 65.000 euros.

También hay una fuerte demanda en los puestos de Front y Back End Developer, así como los Full Stack de varios lenguajes de programación, como Java, React, PHP, .Net y C++), con salarios anuales de entre los 30.000 euros a los 55.000 euros brutos anuales.

Por otro lado, también hay perfiles que han pasado a ser menos solicitados, como son de BI Consultant, System Administrator, Network Engineer y RoR Developer. ■

MÁS INFORMACIÓN

- La transformación del trabajo: el empleado conectado
- Gartner: Estrategia de retención de talento

Los analistas de Gartner recomiendan a los CIO que adopten un enfoque basado en datos para identificar a los trabajadores que están en mayor riesgo y los más valiosos, y adaptar las políticas de trabajo híbridas para mantenerlos comprometidos y con un alto rendimiento

¡AYÚDANOS A CONOCER LA REALIDAD TI DE LAS EMPRESAS!

Participa en nuestra encuesta **it RESEARCH**

¿Tu empresa va a invertir más en TI en 2022?
¿En qué áreas pondrá más foco?
¿Su inversión se dedica a innovar o a mantener su TI actual?

PARTICIPA

Las organizaciones tienen planes para aumentar sus presupuestos de protección de datos

El crecimiento de los datos, cuya explotación correcta aporta ventajas a las empresas, trae asociados una serie de retos, como su protección. Esto reviste cada vez una mayor complejidad. Un 89% de las organizaciones no están protegiendo los datos lo suficiente, aunque la mayoría tienen la intención de poner remedio a la situación, según un informe de Veeam.

El crecimiento de los datos en los últimos dos años se ha más que duplicado, en gran parte debido a la forma en que hemos adoptado el trabajo remoto y los servicios basados en la nube. Pues bien, según el Informe de Tendencias de Protección de Datos de Veeam 2022, el 89% de las organizaciones no están protegiendo los datos lo suficiente. El 88% de los líderes de TI esperan que los presupuestos de protección de datos aumenten a un ritmo más alto que el gasto de TI más amplio a medida que los datos se vuelven más críticos para el éxito empresarial y los desafíos de protegerlos crecen en complejidad. Más de dos tercios están recurriendo a servicios basados en la nube para proteger los datos esenciales.

Según Anand Eswaran, CEO de la compañía, a medida que los volúmenes de datos se han disparado, también lo han hecho los riesgos asociados con la protección de datos; ransomware es un buen ejemplo. “Esta investigación

muestra que las organizaciones reconocen estos desafíos y están invirtiendo fuertemente, a menudo debido a que se han quedado cortas en la entrega de la protección que los usuarios necesitan. Los volúmenes de datos y la diversidad de plataformas continuarán aumentando, y el panorama de amenazas cibernéticas se expandirá. Por lo tanto, los CXO deben invertir en una estrategia que cubra las brechas que ya tienen y se mantenga al día con las crecientes demandas de protección de datos", explica.

PROTEGER AL RITMO QUE NECESITA EL NEGOCIO

Los encuestados declararon que sus capacidades de protección de datos no pueden seguir el ritmo de las demandas del negocio, y el 89% informó de una brecha entre la cantidad de datos que pueden permitirse perder después de una interrupción y la frecuencia con la que se realiza una copia de seguridad de los datos. Esto ha aumentado en un 13% en los últimos doce meses, lo que indica que, si bien los datos continúan creciendo en volumen e importancia, también lo hacen los desafíos para protegerlos a un nivel satisfactorio.

El 76% de las organizaciones reportaron al menos un evento de ransomware en el último año. No solo la frecuencia de estos eventos es alarmante, también lo es su potencia. Por ataque, las organizaciones no pudieron recuperar el 36% de sus datos perdidos, lo que demuestra que las estrategias de protección de datos actualmente no ayudan a las empresas a prevenir, remediar y recuperarse de los ataques de ransomware.

El 76% de las organizaciones reportaron al menos un evento de ransomware en el último año. No solo la frecuencia de estos eventos es alarmante, también lo es su potencia

INCREMENTO DE LA INVERSIÓN

Para cerrar la brecha entre las capacidades de protección de datos y este creciente panorama de amenazas, las organizaciones gastarán alrededor de un 6% más anualmente en protección de datos que las inversiones de TI más amplias. A medida que la nube continúa su trayectoria para convertirse en la plataforma de datos dominante, el 67% de las organizaciones ya utiliza los servicios en la nube como parte de su estrategia de protección de datos, mientras que el 56% ahora ejecuta contenedores en producción o planea hacerlo en los próximos doce meses.

La diversidad de plataformas se expandirá durante 2022, y el equilibrio entre el centro de datos (52%) y los servidores en la nube (48%) continuará cerrándose. Esta es una de las razones por las que el 21% de las organizaciones califican la capacidad de proteger las cargas de trabajo alojadas en la nube como el factor de compra más importante para la protección de datos empresariales en 2022.

Para Danny Allan, CTO de la compañía, "a medida que los ciberataques se vuelven cada vez

Según IDC, se espera que los dispositivos de seguridad mantengan su relevancia dentro de las estrategias de seguridad diseñadas para proteger los ecosistemas de TI híbridos

más sofisticados y aún más difíciles de prevenir, las soluciones de backup y recuperación son fundamentos esenciales de la estrategia de protección de datos moderna de cualquier organización. Para su tranquilidad, las organizaciones necesitan 100% de certeza de que las copias de seguridad se están completando dentro de la ventana asignada y las restauraciones se entregan dentro de los SLA requeridos".

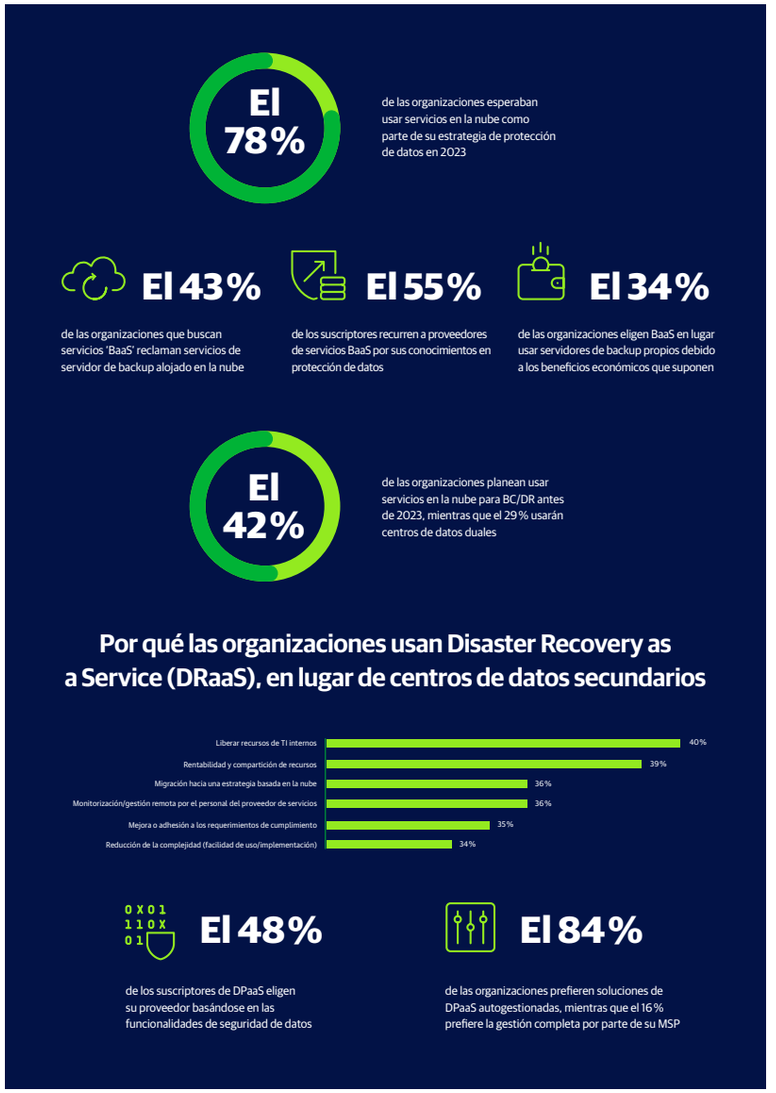
EL MERCADO MUNDIAL DE DISPOSITIVOS DE CIBERSEGURIDAD SIGUE CRECIENDO

Según el último rastreador mundial de dispositivos de seguridad de IDC, los ingresos de los proveedores crecieron un 9,7% anual en el cuarto trimestre de 2021, alcanzando un total de más de 5.800 millones de dólares, 515 millones más en comparación con al mismo trimestre de 2020. Las ventas de dispositivos de seguridad también aumentaron un 9,2% año tras año, llegando a más de 1,5 millones de unidades suministradas.

Cada una de las categorías de productos dentro del mercado de dispositivos de seguridad (Gestión unificada de amenazas (UTM), Gestión de contenido, Detección y prevención de intrusiones (IDP), Firewall tradicional y Red privada virtual (VPN)) arrojó resultados positivos en el cuarto trimestre. La categoría UTM tuvo el crecimiento interanual más rápido en el trimestre con un 12,3%.

"Aunque los problemas de la cadena de suministro tuvieron diversos grados de impacto entre los proveedores de dispositivos de seguridad, el mercado continuó con un desempeño saludable durante el último trimestre de 2021, y se espera que los dispositivos de seguridad mantengan su relevancia dentro de las estrategias de seguridad diseñadas para proteger los ecosistemas de TI híbridos", afirma Carlo Dávila, gerente de investigación de Worldwide Enterprise Trackers en IDC.

Al observar el desempeño regional en todo el mundo, la región de Europa, Medio Oriente y África (EMEA) lideró el camino con un crecimiento interanual del 13,7%, seguida por la región de Asia/Pacífico con un crecimiento del 10,4%. La región de América (EE. UU., Canadá y América Latina) representó el 40,7% de los ingresos del mercado mundial de dispositivos de seguridad, y América Latina mostró el crecimiento de



Clica en la imagen para ver la infografía más grande

ingresos más rápido, del 9,4 % en el trimestre.

Por fabricantes, Cisco se mantiene al frente del mercado por volumen de ingresos, con una cuota del 15,3%, seguido de cerca por Palo Alto Networks, con un 15,2% en su haber. A continuación, está Fortinet, que registró la subida más fuerte, cifrada en un 20,9%, lo que eleva su participación al 13,4%. Cierran el ranking Check Point y Huawei, con sendas cuotas de mercado del 8% y del 3,3%, respectivamente.

EL MERCADO DE CIBERSEGURIDAD INDUSTRIAL CRECERÁ A UN RITMO ANUAL DEL 7,3% HASTA 2026

Un nuevo estudio de mercado publicado por Global Industry Analysts (GIA) estima que el mercado global de ciberseguridad industrial generará un volumen de negocio de 17.000 millones de dólares en el año 2022, y seguirá creciendo a una tasa compuesta anual (CAGR) del 6,6% hasta 2026, cuando se espera alcance los 22.300 millones de dólares.

Se proyecta que los servicios crezcan a una tasa compuesta anual del 7,3% para alcanzar los 10.000 millones de dólares al final del período de análisis. Después de un análisis exhaustivo de las implicaciones comerciales de la pandemia y su crisis económica inducida, el crecimiento en el segmento de software se reajusta a una CAGR revisada del 6,3%, un segmento que representa actualmente el 36,1% del mercado global de ciberseguridad industrial.

La tendencia de "trabajar desde casa" impuesta por la pandemia requirió el establecimiento de una serie de procedimientos y herramientas de seguridad para garantizar que las instalaciones industriales y plantas de producción pudieran realizar operaciones remotas. Pero las oficinas domésticas carecen de protecciones sólidas de ciberseguridad, y el acceso remoto también proporcionó a los hackers una superficie más amplia para atacar.

Un nuevo estudio de mercado publicado por Global Industry Analysts (GIA) estima que el mercado global de ciberseguridad industrial generará un volumen de negocio de 17.000 millones de dólares en el año 2022

TENDENCIAS

Para los fabricantes, la importancia de la ciberseguridad ha crecido considerablemente, a medida que las empresas industriales conectan dispositivos y software a nivel de planta a sistemas empresariales conectados a Internet. El Internet Industrial de las Cosas (IIoT) ha fortalecido en gran medida las operaciones en la planta, pero también ha introducido muchos vectores novedosos para posibles ciberataques.

El aumento del movimiento de datos de las plantas podría aumentar la vulnerabilidad de las redes localizadas. Estas nuevas lagunas están siendo explotadas por delincuentes para robar información confidencial, como la propiedad intelectual, con fines de extorsión. Además, los atacantes también han explotado la sensación de incertidumbre y miedo a esta pandemia para llevar a cabo ataques de phishing, así como otros tipos de ingeniería social para engañar a los usuarios para que proporcionen acceso a diversa información y sistemas propietarios.

Ante los elevados niveles de ciberamenazas, las industrias están invirtiendo cada vez más en la implementación de una amplia gama de soluciones de seguridad como firewalls, antivirus y sistemas de detección de intrusos (IDS) para proteger los activos y evitar cualquier interrupción operativa debido a las brechas cibernéticas. El gasto también está aumentando en dispositivos de seguridad y soluciones de software para garantizar la seguridad de las redes de sistemas de control industrial, las instalaciones de infraestructura crítica y los centros de datos. El aumento de la financiación gubernamental y el aumento del gasto de las organizaciones para abordar el aumento de las amenazas cibernéticas continuarán presentando oportunidades de crecimiento favorables para el mercado de ciberseguridad industrial. ■

MÁS INFORMACIÓN

Trends Data Protection 2022

FORO it Digital Security

SASE

EL FUTURO DE LA SEGURIDAD DE LA RED

EVENTO ONLINE,
28 DE ABRIL DE 2022

Las pymes, ante el reto de gestionar los datos: claves para no quedarse atrás

En 2025 el volumen de datos anuales generados en todo el mundo superará los 180 zettabytes. Analizarlos para convertirlos en valor y tomar decisiones será una ventaja competitiva, pero solo un 10% de las pequeñas y medianas empresas hacen análisis de Big Data, según el INE. Será fundamental impulsar un cambio cultural y acelerar el uso de tecnología que les permita una gestión adecuada de los datos.

Los datos que se generan el mundo aumentan anualmente un 40%, de acuerdo con los datos de Statista, lo que significa que en 2025 se crearán más de 180 zettabytes. Estos grandes volúmenes tienen que ser gestionados mediante tecnología de Big Data, pero, hasta ahora, solo un 10% de las pymes tienen esa capacidad.

La consultora española atSistemas ha reunido las claves para que saquen provecho del análisis de toda esa información:

❖ **Acceso a herramientas digitales.** Una de las barreras más mencionadas a la hora de excusar la falta de digitalización de las pymes es la inversión necesaria para adquirir y formarse la tecnología necesaria. Con las ayudas del Kit Digital, las pymes podrán en 2022 acceder a estas herramientas tecnológicas que les ayuden a implementar la digitalización.

❖ **Consolidación y mantenimiento adecuado de los datos.** Para que los datos sean váli-

dos de cara a transformarlos en estrategias de marketing y ventas, el primer paso que debe dar la empresa es recopilarlos de la manera más adecuada en función de sus intereses. Esto implica tener la información actualizada de forma periódica, y así mantener los datos al día, pero también que deben ser ordenados, pues únicamente el 20% de la información es estructurada y eso puede provocar múltiples errores y afectar a su calidad, tal y como apunta Powerdata. La integración y consolidación de los datos independientemente de la fuente es esencial para obtener la mayor cantidad de información posible de los clientes. Conocer cómo se comportan en cada soporte e impactarles de la forma más efectiva, evitando la duplicidad de datos y encontrando relación entre ellos, hará que las empresas puedan sacar el máximo provecho de estos.

❖ **Personal especializado en el tratamiento de datos.** El talento humano es el valor más importante de una organización, por lo que es de vital importancia para las empresas retenerlo y apostar por la formación. En el actual contexto de escasez de talento tecnológico, son muchas las empresas que optan por subcontratar a estos profesionales especializados en el análisis de datos, pero esto supone un coste considerable para las empresas a largo plazo, ya que la evolución digital implica un aumento de su presencia digital. Por ello, resulta esencial para el crecimiento de las empresas apostar por empleados expertos en datos que sean capaces de conseguir y captar información relevante para la estrategia de la organización a partir de los mismos.

Los datos que se generan en el mundo aumentan anualmente un 40%, de acuerdo con los datos de Statista, y eso significa que en 2025 se crearán más de 180 zetabytes

❖ **Cambio cultural.** La digitalización no sólo tiene que ver con emplear soluciones digitales, sino que también exige un cambio de mentalidad y de cultura corporativa, una transformación de empresa con pensamiento analógico a una con pensamiento centrado en el dato. Existe cierta reticencia a lo tecnológico, una barrera cultural que hace que las pymes no se sumen al proceso de transformación digital y, si no ponen de su parte, acabarán perdiendo clientes. En línea con esta situación, tan solo un 5% de los líderes de las empresas españolas cree que su propia empresa tenga una cultura digital fuertemente asentada, según apunta Capgemini. Para conseguir sumarse al proceso de digitalización las empresas requieren de un cambio cultural a todos los niveles, para que la transición a los entornos digitales sea lo más eficiente posible. ■

MÁS INFORMACIÓN

Estrategias de datos para marcar la diferencia

TENDENCIAS TECNOLÓGICAS-DIGITALES 2022

¡Descárgatelo ahora!

Un informe de ADVICE Strategic Consultants

El gasto en soluciones de Inteligencia Artificial crecerá casi un 20% en 2022

El mercado mundial de Inteligencia Artificial moverá este año en torno a 432.800 millones de dólares, lo que supone un 19,6% si se compara con los datos de 2021. La previsión de la consultora IDC es que se supere la cifra de 500.000 millones en 2023.

El último informe de IDC sobre Inteligencia Artificial (IA) confirma la evolución de la adopción de esta tecnología y que se está convirtiendo en un impulsor de la inversión en TI. Según los datos de la firma, el gasto en hardware, software y servicios de IA se elevará a 432.800 millones de dólares en 2022, y a más de 500.000 millones en 2023. Para sus expertos, la IA está siendo la palanca de la próxima gran ola de innovación, y un elemento diferenciador para las empresas, a la hora de mejorar sus procesos, planificar y hacer previsiones, lo que les permite tomar mejores decisiones que tienen su reflejo en los resultados.

Entre las tres categorías de tecnología, el software verá disminuir levemente su peso en el gasto en 2022, mientras que el gasto en hardware y los servicios crecerán más rápidamente. A cinco años vista, el crecimiento anual compuesto que pronostica para el hardware es del 20,5%, mientras que, para los servicios,

del 22%. En la categoría de software de IA, las aplicaciones de representaron el 47% del gasto en la primera mitad de 2021, seguidas por el software de infraestructura de sistemas, que supusieron el 35%. En términos de crecimiento, se espera que las plataformas de IA registren una tasa de crecimiento anual compuesto del 34,5% en los próximos cinco años, mientras que el software de infraestructura de sistemas evolucionará más lento, a un ritmo del 14,1%.

En la primera mitad del año pasado, los servicios crecieron un 20,4% con respecto al mismo periodo de 2020, situando el gasto mundial en 18.400 millones de dólares. En 2022, el pronóstico de IDC es que crezcan un 22%, porcentaje que será constante en los próximos años.

El gasto en esta categoría alcanzará los 52.600 millones en 2025.

Las previsiones de la firma son que el gasto en hardware crezca interanualmente un 24,9% este año, y representará el 5% del total del mercado. Si en 2021, la categoría que más creció fue la de almacenamiento, en 2022 el gasto se concentrará en los servidores.

MADRID QUIERE SER UN REFERENTE INTERNACIONAL EN INTELIGENCIA ARTIFICIAL

El Alcalde de Madrid, José Luis Martínez-Almeida, ha calificado a Madrid Innovation Lab (MIL), el nuevo centro de innovación enfocado a la Inteligencia Artificial y nuevas tecnologías situado en el distrito de Chamberí, como "una oportunidad para los vecinos de Madrid y, especialmente, para

Así es ALIMENTE 21, un proyecto español para utilizar la IA en la producción alimentaria

Un consorcio de siete empresas, liderado por Raventós Codorníu, ha puesto en marcha un ambicioso proyecto para aplicar la Inteligencia Artificial a los procesos de producción de la industria alimentaria. Se llama ALIMENTE 21 – Industria alimentaria inteligente del siglo XXI, y tiene como principal objetivo incrementar la eficiencia de la gestión industrial en el sector alimentario, aumentar su calidad y seguridad y reducir su impacto ambiental (consumo energético e hídrico) aplicando nuevas tecnologías, principalmente la Inteligencia Artificial.

La iniciativa, que acaba de empezar y finaliza en 2024, cuenta con un presupuesto de 5,1 millones y con una ayuda de 3 millones. Está subvencionado por el Centro para el Desarrollo Tecnológico e Industrial (CDTI) con el apoyo del Ministerio de Ciencia e Innovación y cofinanciado por los Fondos Europeos Next Generation.

En el proyecto participan, además de Codorníu, las cárnicas Aldelís y Prolongo y cuatro ingenierías: Mapex, Omron Iberia, Cibernos y Agropixel. Además, cuenta con la colaboración y coordinación técnica del centro tecnológico Eurecat. Este último trabajará con las empresas en la investigación y desarrollo de soluciones punteras basadas en Inteligencia Artificial, Big Data, Edge Computing, Digital Twin y otras.

La idea es conseguir que la industria alimentaria avance hacia un modelo de gestión predictiva (se avanza a lo que sucederá), prescriptiva (sugiere qué hay que hacer), inteligente y con menor impacto ambiental, desde el punto de vista del uso del agua y la energía, principalmente.

los más jóvenes, para "darles la capacidad real de decisión sobre su futuro", que debe crearse "a partir de lo que es el conocimiento, la innovación y el fomento del emprendimiento y siempre con la mirada puesta en el conjunto de los madrileños".

Madrid Innovation Lab, impulsado por el Ayuntamiento de Madrid, tiene como objetivo convertirse en un espacio de referencia internacional en materia de Inteligencia Artificial (IA) y nuevas tecnologías (deep tech) y acogerá en sus instalaciones a emprendedores, startups y empresas del sector de la IA, así como a inversores, centros de investigación y organismos educativos y académicos. Además, estará abierto a los vecinos del distrito y todos los ciudadanos podrán participar en sus actividades y programación.

En la inauguración de este centro de innovación Almeida destacó que con estas iniciativas de las Administraciones Públicas se garantiza la igualdad de oportunidades de todos los madrileños en una ciudad cuyo éxito reside en "el talento, las personas, la capacidad que cada uno tenga para poder llevar a cabo sus sueños y oportunidades".

Ubicado en la calle Bravo Murillo, este centro tiene 400 metros cuadrados distribuidos en sala de conferencias, zonas de reunión, estancias de coworking y zonas de ocio con un estilo abierto que imita al del ágora griego, lo que supone un espacio flexible de trabajo para un aforo de 45 personas. En funcionamiento desde febrero, Madrid Innovation Lab ya cuenta con un calendario de programación: charlas con estudiantes de Altas Capacidades PEAC (Programa de Enriquecimiento Educativo para Alumnos con Altas Capacidades), formaciones con startups y eventos para visibilizar el emprendimiento femenino en IA, entre otras acciones.

Madrid Innovation Lab, gestionado por Accenture, apoyará las iniciativas que fomenten las tecnologías disruptivas, atrayendo y reteniendo talento e inversión y posicionando a Madrid a la vanguardia nacional y europea en IA.

El último informe de IDC sobre Inteligencia Artificial (IA) confirma la evolución de la adopción de esta tecnología y que se está convirtiendo en un impulsor de la inversión en TI

Con su Observatorio de Inteligencia Artificial, AMETIC tiene como objetivo el fortalecimiento del conocimiento que se tiene de la Inteligencia Artificial y de los retos de su aplicación en las empresas, las Administraciones Públicas y en la sociedad en su conjunto

Además, el centro pretende tener un efecto dinamizador en la vida económica y social del distrito, interaccionando con pymes y startups del entorno y con los vecinos para trabajar en procesos de digitalización y de capacitación en nuevas tecnologías, respectivamente. Asimismo, el centro colaborará con centros educativos para dirigir sesiones divulgativas a los estudiantes de educación primaria y secundaria. El trabajo de difusión y promoción de la IA también se concretará a través de eventos, reuniones, mesas redondas o charlas informativas.

AMETIC CREA UN OBSERVATORIO DE INTELIGENCIA ARTIFICIAL

La asociación de la industria digital, AMETIC, ha presentado su Observatorio de Inteligencia Artificial, que pone en marcha con cerca de 100 entidades españolas que actualmente investigan, desarrollan, aplican y consumen esta tecnología, y que reflejan la diversidad de la actividad nacional en Inteligencia Artificial (IA). La iniciativa, que cuenta con el apoyo de la empresa tecnológica Atos y está compuesto por grandes empresas de tecnología y consultoría, empresas de sectores clave de la economía, pymes y startups con un profundo conocimiento tecnológico y de nichos de mercado, Universidades, y centros de investigación.

Con este Observatorio, la asociación tiene como objetivo el fortalecimiento del conocimiento que se tiene de la Inteligencia Artificial y de los retos de su aplicación en las empresas, las administraciones públicas y en la sociedad en su conjunto.

Según explica AMETIC, nace con la vocación de fomentar el uso ético y sostenible de esta tecnología. Además, contribuirá a mostrar todo el potencial transformador de la IA, mostrando las últimas novedades tecnológicas y sus aplicaciones en nueve áreas de trabajo: tecnología, aplicaciones industriales, economía, finanzas y bolsa, regulación, investigación, sostenibilidad, educación y empleo.

El Observatorio estará presidido por Enrique Serrano, quien ha destacado que "supone el mayor exponente actualmente en nuestro país de convergencia público-privado en materia de IA. Sus funciones príncipes son observar (investigar y analizar) y compartir (divulgar, difundir y enseñar) desde una perspectiva totalmente neutra y tomando como ejes de aplicación la sociedad, las empresas y las administraciones públicas".

Entre sus actividades figura la publicación cuatrimestral de un Radar de IA que incluirá un análisis sobre el uso de esta herramienta por parte de la industria española, la evolución de roles en el mercado de trabajo o tendencias. ■

MÁS INFORMACIÓN

- El gasto en soluciones de IA en EEUU se duplicará en 2025
- Madrid Innovation Lab
- Observatorio de la IA de AMETIC
- Estudio sobre aplicación de la Inteligencia Artificial
- Guía empresarial sobre Inteligencia Artificial
- Indicadores de uso de la IA en las empresas españolas
- IA y su aplicación en los Servicios Públicos

La documentación TIC, a un solo clic

Nuevas reglas de seguridad para aplicaciones web y API

Es hora de poner al día las reglas de la seguridad para API y aplicaciones web para que correspondan a la manera en que se crean y gestionan las aplicaciones hoy en día. Al usar herramientas y procesos tradicionales, estarás siempre a la zaga de los adversarios y sus ataques. Con estas nuevas reglas, puedes tomar la delantera y conocer de primera mano el estado de la seguridad de tu empresa.

MTWO 6D BIM Construction Cloud Platform

MTWO es un software cloud de nivel empresarial para el sector de la construcción preparado para el futuro y que ayuda a gestionar todos los proyectos extremo a extremo con 6D BIM. Es capaz de conectar a todos los equipos en cualquier momento y en cualquier lugar a través de todos los dispositivos.

Los tres pilares de una Transformación Digital B2B exitosa

MTWO Complete Construction Cloud es una plataforma empresarial integrada de modelado de información de construcción en cinco dimensiones (BIM 5D) en la nube que permite a contratistas, propietarios de activos y desarrolladores acelerar su proceso de transformación digital.

Informe: Cloud, en busca de la agilidad

La nube se ha asentado en las organizaciones como un modelo de TI que permite ganar agilidad en las operaciones y en el despliegue de nuevos servicios. Este informe IT Trends apunta las principales tendencias en torno a la cloud en nuestro país.

Innovación cloud:
5 tendencias que hay que tener en cuenta

La creciente dependencia de las tecnologías cloud ha provocado también mayor presión y escrutinio sobre el sector. Tanto los actores ya presentes como los nuevos esperan que la industria cloud continúe avanzando rápidamente, tanto en el desarrollo de nuevas soluciones como en la respuesta a los retos de negocio. El crecimiento de multicloud, las arquitecturas cloud más modulares, los microservicios y el impulso del código abierto cobrarán relevancia en 2022.

La transformación digital de innumerables sectores ha tomado forma en 2021 a una velocidad y escala sin precedentes, con cloud consolidándose como el pilar central sobre el que se construye el mundo digital. Los expertos en tecnología cloud de Scaleway, proveedor europeo de infraestructura en la nube y centros de datos, analizan cinco tendencias en innovación cloud que empresas y proveedores deberán tener en cuenta en 2022:

❖ **Multicloud seguirá en auge.** La multicloud, o el uso de varios proveedores cloud en lugar de

depender de uno solo, ganará impulso en 2022, ya que los actores son cada vez más conscientes de los riesgos de poner todos los huevos en la misma cesta. De hecho, las caídas de los principales proveedores han causado muchos dolores de cabeza a los clientes, como se demostró con la gran interrupción de AWS, con consecuencias en todo el mundo. La tendencia a la multiplicidad de nubes permitirá mayor elección, arbitraje de precios y gestión de riesgos, tanto desde el punto de vista geopolítico como de la capacidad de recuperación. Además, la promesa de garantizar la continuidad del negocio a la vez que se reducen los costes hará también que la multicloud se consolide como el statu quo.

❖ **Los usuarios no quieren lidiar con servidores más de lo necesario.** La adopción de la abstracción de la arquitectura cloud moderna seguirá progresando rápidamente tanto en contenedores, con Kubernetes en particular, como en servicios serverless. Según Gartner, para 2025, el 85% de las empresas ejecutarán contenedores en su desempeños, frente a menos del 30% que lo hicieron en 2020. Este crecimiento en la adopción de contenedores apunta a la escalabilidad y flexibilidad de la arquitectura, cualidades cada vez más demandadas. La reducción de los costes y la complejidad no solo permitirá un uso más eficiente de los recursos, sino que también acelerará el trabajo eficiente, ya que se dedicará menos tiempo a la gestión de la tecnología.

❖ **La arquitectura cloud será cada vez más modular.** A medida que se desarrollen las necesidades tecnológicas y se requieran nuevas aplicaciones, la arquitectura cloud tendrá que ser cada vez más modular para soportar las aplicaciones aún desconocidas y que los ecosistemas de productos funcionen bien juntos. Conforme se afianzan las tecnologías emergentes, las previsiones apuntan a que el tamaño del mercado de microservicios cloud se triplicará entre 2020 y 2026. Además, se espera que la predicción de IDC de 2018 de que el 90% de las aplicaciones contarán con arquitectura de microservicios en 2022 se haga realidad. Para desarrollar arquitecturas modulares de contenedores o Serverless se aumentará el foco en la conexión de productos "pegamento", como la cola de mensajes o la observabilidad, que marcarán la diferencia.

❖ **La Inteligencia Artificial liberará un enorme potencial en la investigación médica.** La Inteligencia Artificial y la robótica están transformando la asistencia sanitaria, así como otros sectores. Sin embargo, para aprovechar este potencial será necesario recurrir a soluciones cloud centralizadas y Edge Computing, ya que el despliegue de servidores locales para la investigación de recursos intensivos supondrá un coste demasiado elevado. Los proveedores cloud tendrán que afrontar este reto ofreciendo soluciones cada vez más eficientes desde el punto de vista energético.

❖ **El código abierto como generador de equilibrio.** El código abierto se posicionará como la solución ideal para proporcionar un terreno de juego equilibrado. A medida que la comunidad del software se aleja cada vez más de los productos basados en la propiedad intelectual y las patentes, las barreras de entrada se reducen significativamente, abriendo así las puertas a personas y empresas con menos recursos, ya sean nuevas empresas, compañías en fase inicial, organizaciones sin ánimo de lucro u organizaciones de países en desarrollo.

SÓLO UN 27% DE LAS ORGANIZACIONES SANITARIAS UTILIZAN LA NUBE

Aunque los despliegues están aumentando, el sector sanitario está en las primeras fases de adopción de la nube. Según un estudio de Vanson Bourne para Nutanix, su uso pasará del 27% anual al 51% en los próximos tres años.

Esta nueva investigación muestra que las organizaciones sanitarias están en las primeras fases de la adopción de la nube y por detrás de la media global de encuestados del conjunto de los sectores. Sin embargo, se espera que la adopción pase del 27% al 51% en los próximos tres años.

La arquitectura de TI multicloud es la que predomina en todo el mundo; sin embargo, entre los encuestados de Enterprise Cloud Index del sector sanitario, el 30% afirma que la nube privada es su modelo de despliegue más común. De hecho, todas las organizaciones consultadas han trasladado una o más aplicaciones a un nuevo entorno de TI en los últimos doce meses, probablemente migrándolas de los entornos tradicionales a nubes privadas. La razón es porque la sanidad está muy regulada, lo que hace que se ralentice la adopción de la nube pública como un componente genuino de sus entornos de TI por razones de seguridad y privacidad.

Sin embargo, la adopción de la cloud pública se está viendo impulsada para establecer una infraestructura de TI complementaria a la que pueden recurrir para mejorar los niveles de continuidad del negocio y las configuraciones de recuperación ante desastres (BC/DR). De hecho, citaron BC/DR con mayor frecuencia como motivación de sus planes a tres años para aumentar el uso de multicloud (38%).

Aunque el uso de multicloud tiende a aumentar, la complejidad de la gestión a través de las fronteras de la nube sigue siendo un reto importante para las organizaciones sanitarias, ya que el 92% de los encuestados coinciden en que el éxito requiere una gestión más sencilla de las infraestructuras de nube múltiple. En este sentido, el 49% de ellas opina que el principal problema de este modelo cloud es la integración de los datos en todas las nubes, el 48% menciona la gestión de los costes (48%) y el 45% cita los problemas de rendimiento con las superposiciones de red.

PRIORIDADES DEL SECTOR

En el corto plazo, entre las prioridades de TI del sector destacan la adopción de 5G (47%) y servicios basados en inteligencia artificial y

machine learning (46%), así como la mejora de los sistemas de continuidad y recuperación (45%) y la gestión multicloud (44%). Además, la pandemia les ha impulsado a aumentar su gasto en TI en determinadas áreas, como la seguridad (62%), la tecnología de autoservicio basada en IA (60%) y la infraestructura de TI existente (48%).

ÉSTAS SON LAS CUESTIONES ESENCIALES PARA REALIZAR UNA MIGRACIÓN SEGURA A CLOUD

Según la encuesta sobre el uso de las TIC elaborada por el INE, el 28,2% de las compañías españolas recurre a algún servicio en la nube, unas cifras que aumentan a medida que lo hace el tamaño de los negocios. En el caso de empresas de más de 260 empleados, la cifra asciende al 64%. Un whitepaper más reciente de Penteo para Syntax, un 67% de las empresas españolas ya tienen más del 20% de sus cargas de trabajo en este modelo.

La transición a cloud debe realizarse con garantías de que la que la postura de seguridad de las compañías no se resiente, y es un tema preocupante para ellas. Por eso, los expertos de Serban Tech, referente en la implantación de soluciones innovadoras para la transformación de puesto de trabajo, biometrías e infraestructuras, han reunido un serie de cuestiones esenciales para que el traslado de los sistemas y aplicaciones a la nube se realice con eficiencia y seguridad. Son las siguientes:

- **Comprender el modelo de responsabilidad compartida.** Para llevar a cabo una migración a la cloud de forma fiable, hay que tener presente que la seguridad es una vía de doble sentido. La computación en la nube se basa en un modelo de responsabilidad compartida en el que el proveedor de servicios de Internet (ISP) es responsable de la seguridad de esta, pero eso no exime de ello al propio cliente. Todo dependerá del tipo de servicios en la nube que se decida usar. Aunque el proveedor del servicio de la cloud será responsable de aspectos básicos como, por ejemplo, el hardware, el almacenamiento o la red. El usuario, por su parte, debe proteger a conciencia sus endpoints, las aplicaciones conectadas a la red o sus propios datos añadidos a la cloud, entre otros.
- **Diseñar un plan a medida.** Las migraciones son bastante complejas y dependen de cada proyecto y sus requisitos. Para que toda la

Aunque el uso de multicloud tiende a aumentar, la complejidad de la gestión a través de las fronteras de la nube sigue siendo un reto importante para las organizaciones sanitarias

operación sea correcta, la planificación es esencial. Esto permitirá determinar qué aplicaciones y datos se trasladarán a la nube y cómo, qué estrategia de migración y qué tipo de cloud es la más adecuada para la empresa, de qué forma reducir los riesgos, quién participará en la migración... Además, la transferencia de datos en una migración se debe hacer por fases, así será más seguro y permitirá que los equipos se familiaricen con los sistemas en la nube. Se debe empezar con datos de baja prioridad, de esta manera se pueden descargar algunos de los recursos de almacenamiento con un riesgo controlado. Así, se podrá probar la configuración e identificar cualquier fallo o brecha de seguridad antes de transferir los datos de mayor prioridad o confidenciales.

✪ **Cifrar los datos y utilizar protocolos seguros.** Hay que asegurarse de que todos los datos están encriptados y utilizar protocolos seguros como HTTPS para la transferencia a los mismos. En realidad, hay que cifrar la información, tanto en reposo como en tránsito. Esto se aplica para garantizar la máxima seguridad, tanto en las propias infraestructuras, como en la nube.

✪ **Centralizar la supervisión.** La conectividad en la nube conlleva un aumento de las posibilidades de sufrir un mayor número ataques debido al incremento de la superficie disponible. Por ello, es necesario tener en cuenta la presencia de estas nuevas amenazas, así como seguir protegiendo los sistemas existentes. Durante la migración, y a menudo después, se necesitarán herramientas de seguridad que actúen, tanto en las instalaciones locales, como en el entorno de la nube. Centralizar la gestión y el uso de estas herramientas facilitará considerablemente la labor del equipo de seguridad. Esto permitirá la identificación y respuesta a las amenazas y vulnerabilidades de forma más rápida y coherente.

La adopción de la cloud pública se está viendo impulsada para establecer una infraestructura de TI complementaria a la que pueden recurrir para mejorar los niveles de continuidad del negocio y las configuraciones de recuperación ante desastres

LA GESTIÓN DE RENDIMIENTO DE ACTIVOS EN EL 60% DE LA GRAN INDUSTRIA ESPAÑOLA YA ESTÁ EN CLOUD

La gestión del rendimiento de los activos en la nube ha aumentado en la industria española a raíz de la pandemia por la posibilidad de acceso remoto a la solución, así como la escalabilidad o flexibilidad que supone para las empresas, de acuerdo con un estudio de IDC Research España para Infor. El resultado es que el 60% de las organizaciones españolas despliega sus sistemas APM en arquitecturas cloud.

Según el informe, que se ha realizado a partir de entrevistas a 100 responsables de operaciones de TI, esto es así porque los sistemas APM en la nube suponen una gran ventaja a la hora de incorporar nuevos procesos o líneas de producción, así como el rápido incremento en la capacidad productiva por un pico de demanda.

Para Ignacio Cobisa, autor del documento, "los avances en tecnologías como el Internet industrial de las cosas, la inteligencia artificial y el aprendizaje automático están transformando la forma en que los activos se supervisan, mantienen y optimizan. Las soluciones APM permiten a las organizaciones optimizar la mano de obra y los materiales, aumentar la seguridad y mejorar la precisión del proceso de presupuestación de capital".

UN 20% DEL MANTENIMIENTO ES REACTIVO EN EL 67% DE LAS EMPRESAS

El informe pone de relieve, sin embargo, que el recorrido que aún existe en cuanto a extensión del mantenimiento predictivo es importante, ya que el 67% del tejido industrial actual en España declara que más de un 20% de su mantenimiento es aún reactivo.

Respecto a las medidas implementadas por parte de los encuestados para digitalizar las operaciones de mantenimiento, destacan como primeros pasos del proceso la conexión remota y la sensorización, que han sido adoptados por el 74% y 67% de las compañías, respectivamente, seguidos de la aplicación de inteligencia (43%). "En ese punto es cuando podemos hablar propiamente de mantenimiento predictivo", explica Cobisa.

AUMENTA EL INTERÉS POR LA SOSTENIBILIDAD

IDC ha detectado también que existe un alto grado de sensibilización por parte del tejido industrial en cuanto a la importancia de la producción sostenible y la economía circular tanto en el impacto reputacional que supone como su impacto en la eficiencia de la organización.

Con la automatización, IoT, tecnologías emergentes como inteligencia artificial y machine learning, los sistemas APM hacen un seguimiento de toda la vida de un activo individual al tiempo que capitalizan y sintetiza grandes cantidades de información de cualquier sistema. ■

MÁS INFORMACIÓN

- Informe: Cloud, en busca de la agilidad
- 2022 CIO Report, Dynatrace
- Índice Enterprise Cloud Nutanix
- La utilización de infraestructuras en la nube en el sector público

it User
TECH & BUSINESS
ESPECIALES

CONTENIDOS↓

SCC

CISCO
Partner

CONECTANDO EL PUESTO DE TRABAJO DIGITAL

ENLAZANDO EL FUTURO DEL TRABAJO HÍBRIDO

EN LA ACTUAL ERA EN LA QUE NOS ENCONTRAMOS, DONDE EL TRABAJO HÍBRIDO JUEGA UN PAPEL DETERMINANTE, LO IMPORTANTE NO ES DÓNDE DESARROLLAMOS NUESTRA ACTIVIDAD DIARIA, SINO QUÉ Y CÓMO LA EJECUTAMOS. IMPULSADO POR LA CONVERGENCIA DE PERSONAS, TECNOLOGÍA Y LUGARES, ESTE CAMBIO HA REMODELADO DE FORMA PERMANENTE LAS EXPECTATIVAS QUE EXPERIMENTAN EMPLEADORES Y EMPLEADOS POR IGUAL. PARA NAVEGAR POR ESTE PANORAMA CAMBIANTE, AHORA MÁS QUE NUNCA LAS ORGANIZACIONES NECESITAN TRABAJADORES QUE PUEDAN TOMAR DECISIONES BIEN INFORMADAS.

Cisco acaba de hacer público el estudio Hybrid Work Index, basado en millones de datos globales que oscilan desde el usuario hasta la red, con objeto de facilitar a sus clientes los conocimientos más avanzados que les permitan alcanzar los siguientes retos: atraer y retener a los mejores talentos; aumentar su ventaja competitiva con mayor agilidad e innovación; y optimizar la seguridad en el trabajo desde cualquier lugar del mundo.

La experiencia de trabajo híbrido varía dependiendo del tamaño de las empresas y de los sectores en los que operan. Sin embargo, con el aumento del tráfico de Internet, está claro que las organizaciones están regresando a sus oficinas, particularmente en lo que

“HEMOS ASISTIDO A UN CAMBIO RADICAL EN LA CONCEPCIÓN DEL PUESTO DE TRABAJO”. ARTURO MONCADA (SCC)

concierne a las pequeñas empresas y al ámbito de la educación. Al mismo tiempo, se está produciendo un movimiento de grandes oficinas corporativas que posiblemente se trasladen a sucursales de menor tamaño, más cerca de donde los empleados quieran vivir y trabajar. Con un crecimiento acelerado en la implementación y el tráfico en los dispositivos de los teletrabajadores, los empleados que ejercen su labor fuera de la oficina continúan siendo productivos mediante el uso de aplicaciones como la colaboración.

Sin embargo, invertir y desplegar tecnología no es suficiente, ya que las organizaciones se enfrentan a retos determinantes:

>> Por un lado, brindar al empleado una experiencia consistente en materia de colaboración y del empleo de otras aplicaciones críticas a lo largo de toda la cadena de suministro digital, tanto dentro como fuera de su propio perímetro.

>> Además, han de mantener a la fuerza laboral en el centro de la toma de decisiones, asegurando que se prioricen todas las experiencias de los empleados, ya sea en casa, en la oficina o en cualquier otro lugar.

>> Y, por último, asegurar que los espacios de trabajo gocen de la conectividad, la monitorización ambiental y la automatización necesarios para mantener a los empleados productivos y seguros.

En el universo del trabajo híbrido, los empleados esperan una gran experiencia digital de sus aplicaciones, indistintamente del enclave en el que trabajen.

INNOVACIONES DE CISCO PARA HACER REALIDAD EL TRABAJO HÍBRIDO

Cisco ha anunciado recientemente innovaciones tecnológicas diseñadas para potenciar el trabajo híbrido con personas que trabajan desde su domicilio, oficina u otro lugar. Las empresas, independientemente de su tamaño, se están adaptando a las principales transiciones digitales que han venido a reformar los operativos tecnológicos en los últimos dos años, abarcando tanto la cloud híbrida para conectar nubes públicas y privadas, como la inteligencia artificial y el aprendizaje automático para la adopción, por ejemplo, del IoT. El éxito del trabajo híbrido no radica simplemente en la capacidad de apoyar a una fuerza laboral remota, si no en la capacidad de adaptación al cambio a medida que sucede. Todo funciona si existe conectividad de confianza y apta para situaciones de misión crítica.

La red es el impulsor esencial de la productividad en un mundo híbrido, ayudando a empresas, centros educativos y gobiernos a trabajar mejor. A medida que más personas requieren de flexibilidad para trabajar en sus propios puestos de trabajo, las organizaciones

se ven obligadas a escalar rápidamente sus operaciones digitales para habilitar las conexiones necesarias que faciliten el trabajo desde cualquier lugar.

Para que el trabajo híbrido funcione, se requiere un cambio fundamental en la forma en que las organizaciones usan y confían en la tecnología. Conectar a más personas y más dispositivos en más lugares requiere conexiones inalámbricas ubicuas, mayor resiliencia y resistencia de la red, así como seguridad de confianza cero para brindar la mejor experiencia en todo momento, sin interrupciones.

"El trabajo híbrido no funciona sin la red", ha afirmado Todd Nightingale, vicepresidente ejecutivo y gerente general de la división Enterprise Networking and Cloud en Cisco. "Las capacidades de la red fortalecen las aptitudes de la fuerza laboral. Estos lanzamientos, impulsados por el chip Silicon One, hacen posible el trabajo híbrido con una potencia y confiabilidad sin precedentes y, lo que es más importante, con la agilidad necesaria para continuar adaptándose y cambiando con nuestros equipos".

NETWORKING DE VANGUARDIA

En un evento reciente Cisco ha explicado cómo su última ola de innovación tecnológica resulta fundamental para que las organizaciones puedan brindar experiencias de usuario mejoradas, habilitar lugares de trabajo optimizados y sostenibles, y garantizar implementaciones de IoT a escala en toda la estructura de su empresa.

Las nuevas innovaciones de acceso y redes inalámbricas de Cisco son las siguientes:

- **Wi-Fi 6E (Catalyst 9136 y Meraki MR57):** la tecnología Wi-Fi 6E amplía la capacidad para superar el rendimiento gigabit. Los nuevos productos Cisco Wi-Fi 6E de Catalyst y Meraki son los primeros puntos de acceso 6E de gama alta de la industria que abordan los entornos empresariales híbridos más exigentes.
- **Cisco Private 5G:** el servicio administrado Private 5G de Cisco que se ofrece junto a proveedores de servicios globales y socios tecnológicos, proporciona una experiencia inalámbrica fácil de arrancar, intuitiva a la hora de operar y fiable para abordar las transiciones digitales hacia el trabajo híbrido y el IoT.
- **Switches Catalyst 9000X:** estos nuevos modelos amplían la familia de switches de Cisco, proporcionando la velocidad, la capacidad de ancho de banda y la escala necesarias para admitir el acceso a la red 100G/400G, aptas para las transiciones del trabajo híbrido en los campus y a la ampliación a las delegaciones con seguridad de confianza cero y eficiencia energética.
- **Introducción de Cisco Silicon One a la cartera de switches Catalyst:** Cisco Silicon One, originalmente implementado en escala web y para redes de proveedores de servicios, continúa demostrando su capacidad y flexibilidad de programación para respaldar la innovación en las redes empresariales. Los nuevos switches Catalyst 9500X y 9600X Series funcionan con Cisco Silicon One Q200.

"En los últimos años, las organizaciones han acelerado sus planes para respaldar los modelos de trabajo híbridos. Un componente fundamental de estos planes es una red segura y poderosa que pueda conectar a cualquier usuario en cualquier momento", ha señalado Brandon Butler, gerente de Investigación de Redes Empresariales en IDC. "Creemos que la red del futuro deberá abordar las crecientes demandas de rendimiento y confiabilidad de la red para, en última instancia, brindar una mayor agilidad y productividad comercial". ■

CONTENIDOS ↓

ROBERTO MORAL, DIRECTOR DE ARQUITECTURAS DE CISCO ESPAÑA

"LA RED ES LA QUE DICTAMINA QUE EL PUESTO DE TRABAJO HÍBRIDO FUNCIONE CORRECTAMENTE"

En los últimos dos años, las organizaciones han acelerado sus planes para respaldar los modelos de trabajo híbridos, que han revolucionado el mercado. Un componente fundamental de estos planes es una red segura y poderosa que pueda conectar a cualquier usuario en cualquier momento y desde cualquier lugar. Roberto Moral, Director de Arquitecturas de Cisco España, nos explica a continuación la visión y estrategia del fabricante en este contexto.

¿Cuál es la visión actual de Cisco con respecto al puesto de trabajo?

En Cisco siempre hemos considerado que el trabajo es una actividad, no un lugar. De hecho, según encuestas recientes, 9 de cada 10 trabajadores afirman querer moverse entre el trabajo remoto y el presencial. Pero el trabajo híbrido va más allá de la posibilidad de emplear ambos modelos, y pone de relieve la importancia de la experiencia de trabajo, que ha de ser inmejorable para que el usuario pueda ejercer

su trabajo por igual en cualquier entorno. Al margen de la experiencia y la conectividad, se deben incorporar otros elementos como sensores, robots y todo aquello que permita conectar esos dos mundos. Es decir, los componentes que residen en la red, a través de conexiones inalámbricas optimizadas, lugares de trabajo inteligentes, mejores herramientas de visibilidad de la red, y, sobre todo, seguridad de confianza cero.

Precisamente, ¿qué estrategia está siguiendo Cisco en el marco de la securización del puesto de trabajo híbrido?

Antes de adentrarnos en nuestra estrategia en este marco deberíamos recordar cómo ha evolucionado la seguridad en los últimos años. La seguridad de la empresa antes era perimetral, es decir, se consideraba seguro todo lo que estaba dentro de los perímetros de la empresa. Pero con el trabajo híbrido esos límites desaparecen, y se deben extender esas capacidades de seguridad a usuarios, dispositivos y aplicaciones, teniendo en cuenta que partes de estas últimas residen fuera de la empresa, por lo que se ha de garantizar que la seguridad se siga cumpliendo y que no afecta a la experiencia de usuario.

En este contexto Cisco combina dos ámbitos: la red y la seguridad. Con una arquitectura SASE y un enfoque de confianza cero hemos de conseguir que los usuarios se conecten de manera segura y transparente a todas las aplicaciones que utilizan. Y todo en base a la seguridad de los usuarios (asegurándonos que el usuario es quien es), la seguridad de los dispositivos (asegurándonos que los dispositivos cumplen con todos los requisitos para funcionar de forma segura) y la seguridad de las aplicaciones (empleando un enfoque de confianza cero extremo a extremo).

¿Qué papel ha de jugar la tecnología Wi-Fi 6 en este contexto?

El Wi-Fi 6 va a jugar un rol determinante, pero si atendemos a la expansión del trabajo híbrido, en el que se atiende no solo a personas, sino también a objetos, se extienden las capacidades del Wi-Fi 6, que son básicamente mejor ancho de banda, mayor resiliencia y menos interferencias. Si se combinan estas funcionalidades con las redes IoT y las conexiones 5G, se podrá obtener el potencial suficiente para modificar la industria y redefinir el futuro del trabajo híbrido.

¿Pero explotará por fin este año el Wi-Fi 6 o habrá que esperar todavía más?

Será una evolución gradual, como cualquier otra tecnología. Cuando se vaya quitando Wi-Fi 5 se irá instalando Wi-Fi 6 en las empresas, respetando los tiempos. Y hay que

ROBERTO MORAL

Roberto Moral es el Director de Arquitecturas en Cisco España. Con más de 25 años de experiencia en el mercado TI, Roberto lidera la iniciativa Green & Blue –políticas de sostenibilidad y eficiencia- del fabricante en nuestro país, comanda un equipo de especialistas técnicos y de ventas centrados en nuevas soluciones, y dirige el Grupo de Software de Infraestructura en la Nube (CISG) de Cisco en el sur de Europa. Roberto lideró anteriormente las ventas de la unidad CISG en España y también ejerció como arquitecto de la división de Soluciones Técnicas en EMEAR. Antes de unirse a Cisco en 2007, Roberto trabajó, entre otras compañías, en Novell como arquitecto de sistemas, tras graduarse en Ingeniería Informática por la Universidad Politécnica de Madrid.

EL TRABAJO HÍBRIDO PONE DE RELIEVE LA IMPORTANCIA DE LA EXPERIENCIA DE TRABAJO, QUE HA DE SER INMEJORABLE PARA QUE EL USUARIO PUEDA EJERCER SU TRABAJO POR IGUAL EN CUALQUIER ENTORNO

tener muy en cuenta que Wi-Fi 6 y 5G son tecnologías complementarias, dependiendo del caso de uso. Es muy improbable que una fagocite a la otra.

¿Cómo están evolucionando las soluciones de colaboración empresarial en este escenario?

En Cisco contamos con la plataforma Webex y sus distintos dispositivos de vídeo. En el último año hemos realizado cerca de 1.000 innovaciones, con 600 millones de usuarios mensuales, yendo más allá de las video-conferencias o las salas de conferencias tradicionales. Los productos de Webex han evolucionado para hacerlas mucho más productivas y mejorar la inclusión, independientemente de dónde se ubique el usuario, qué idioma hable o cómo de familiarizado se encuentre con la tecnología. Webex son conferencias, pero también reuniones, llamadas, mensajes, encuestas, eventos, hologramas, etc. Y

también hay que destacar para qué se aplica la inteligencia artificial en el ámbito de las comunicaciones unificadas, con ejemplos prácticos como el de la filtración del ruido de fondo, la traducción en tiempo real a más de 108 idiomas, el reconocimiento facial o el reconocimiento gestual.

¿Qué innovaciones tecnológicas acaba de presentar Cisco con objeto de ayudar a las organizaciones a acelerar la hibridación de sus puestos de trabajo?

Entre ellas, nuevos puntos de acceso Wi-Fi 6E, soluciones privadas de 5G en modo servicio gestionado a través de partners tecnológicos, nuevos switches con capacidades de 100G/400G tanto para acceso como para core, así como el nuevo chip Silicon One, tremendamente eficiente, que se incorpora a nuestros últimos equipos de switching.

¿Cómo está trabajando Cisco en este ámbito junto a sus socios tecnológicos y de canal?

Para asumir con garantías las oportunidades y desafíos de los que estamos hablando en torno al nuevo puesto de trabajo híbrido, el canal es fundamental.

¿Está el canal español preparado para atender estas demandas, también relativas al consumo de tecnología como servicio, en modo cloud?

El canal de Cisco está más que preparado y se ha esforzado por estar listo para dar servicio en la última milla, que es donde no llega el producto y es necesario que se adentre el partner. Su labor ahí pasa por generar el caso de uso en el cliente, acorde con el vertical específico del que se esté hablando, y poder ofrecer valor real trabajando, configurando, adaptando y generando desarrollos adiciones basados en nuestra tecnología para ser más relevantes entre sus clientes. ■

CONTENIDO RELACIONADO

Cisco adapta Webex a la era del trabajo híbrido

"Queremos acompañar a las organizaciones tanto en el proceso de digitalización como en la mejora de la experiencia de sus clientes"

LA PROPUESTA CONJUNTA MÁS INNOVADORA DEL MERCADO

GARANTIZAR LA MEJOR EXPERIENCIA AL TRABAJADOR, ESTÉ DONDE ESTÉ Y UTILIZANDO CUALQUIER DISPOSITIVO (PORTÁTIL, SOBREMESA, TABLETA Y/O SMARTPHONE), SIGNIFICA PROPORCIONAR EL MEJOR ACCESO A LAS APLICACIONES CORPORATIVAS, TANTO SI ESTÁN PROVISIONADAS ON-PREMISE O EN EL CLOUD PÚBLICO. ADEMÁS, ESTE ACCESO DEBE SER SEGURO, TANTO PARA EL EMPLEADO COMO PARA LA EMPRESA QUE LE PROPORCIONA DICHAS APLICACIONES.

Esta podría ser una de tantas definiciones de “trabajo híbrido”, pero podemos incluir otros requerimientos para esta definición como, por ejemplo, nuevas formas de interactuar entre nosotros, sin importar en qué lugar del mundo nos encontremos, o incluir a los dispositivos IoT/OT en esta nueva conectividad, para alcanzar esa transformación digital que está tan en boga.

También podemos pensar que, si el trabajo híbrido también ha de suponer la mejora de la experiencia del usuario, y no sólo radica en la conexión a las aplicaciones desde cualquier lugar, ¿por qué no utilizar la misma plataforma para monitorizar y gestionar de for-

ma automática las condiciones ambientales de la oficina? ¿O adaptar el consumo eléctrico de los dispositivos de la red inalámbrica o cableada, de acuerdo con la concurrencia física? La ergonomía y la sostenibilidad son cada vez más importantes en el mundo actual y lo serán más en el futuro.

Otros aspectos a tener en cuenta en ese puesto de trabajo ideal podrían ser el hecho de facilitar la reserva de una sala de reuniones, de planificar y realizar una videoconferencia o de realizar webinars en los que la interacción mediante tests, encuestas o sondeos mantenga la atención y proporcione información valiosa, independientemente del dispositivo que emplee el usuario.

EL PUESTO DE TRABAJO IDEAL PODRÍA SUPONER EL HECHO DE FACILITAR LA RESERVA DE UNA SALA DE REUNIONES, DE PLANIFICAR Y REALIZAR UNA VIDEOCONFERENCIA O DE REALIZAR WEBINARS EN LOS QUE LA INTERACCIÓN MEDIANTE TESTS, ENCUESTAS O SONDEOS MANTENGAN LA ATENCIÓN Y PROPORCIONEN INFORMACIÓN VALIOSA, INDEPENDIENTEMENTE DEL DISPOSITIVO QUE EMPLEE EL USUARIO

LA IMPORTANCIA DE LA SEGURIDAD

Es indiscutible que la seguridad es un aspecto clave para que se den las condiciones necesarias para el trabajo híbrido. Poner al alcance de los usuarios y proveedores externos las aplicaciones y datos corporativos en cualquier lugar y desde cualquier dispositivo, comporta incrementar la superficie de exposición a posibles ciberataques.

Implementar VPNs para proporcionar seguridad es insuficiente e ineficiente: muchas de las aplicaciones están en el cloud público. Por tanto, es imprescindible proteger los datos y aplicaciones corporativas, aplicando el concepto de Zero Trust Network Access (ZTNA). La aproximación de ZTNA consiste en denegar por defecto el acceso a los datos y aplicaciones corporativas, y permitiéndolo únicamente a aquellos usuarios/dispositivos que cumplan determinadas condiciones, teniendo en cuenta si está dentro o fuera del perímetro de seguridad y qué dispositivo está utilizando.

Una aserción muy común es la siguiente: "No puedes proteger lo que no ves". La solución ZTNA debe proporcionar esa necesaria visibilidad. Cisco Identity Services Engine (ISE) autentica, identifica, clasifica y rastrea continuamente los dispositivos que se conectan a la red.

Cisco proporciona ZTNA mediante su solución SASE Cisco Umbrella, que incluye seguridad para el protocolo DNS, un gateway de navegación seguro (SWG), Next Generation Firewall en la nube y CASB (Cloud Access Security Broker). La utilización de la solución de autenticación de múltiple factor (MFA: Multi-Factor Authentication) Cisco DUO es el complemento perfecto para la aproximación ZTNA de Cisco.

Parte importante de la aproximación ZTNA de Cisco es Cisco Identity Services Engine (Cisco ISE), una herramienta que autentica, identifica, clasifica y rastrea los dispositivos que se conectan a la red. Para poder aplicar Zero Trust es fundamental la capacidad de ver y conocer todo lo que está conectado a la red, ya sean smartphones, tabletas, PCs o dispositivos IoT/OT.

VISIBILIDAD Y GESTIÓN AVANZADAS

En un entorno cada vez más complejo, que incluye la infraestructura on-premise (data center y campus), aplicaciones e infraestructura en el cloud público, y empleados y proveedores externos accediendo remotamente, los departamentos de IT necesitan herramientas que les faciliten la detección, análisis y resolución de incidencias, y que les proporcionen información sobre la evolución de los recursos de la red.

Cisco DNA Center es la herramienta de Cisco que facilita la gestión, automatización, analítica basada en AI/ML e integración con Cisco ISE. Por su parte, Cisco Software-Defined Access (SD-Access), utiliza Cisco DNA Center y Cisco Identity Services Engine (ISE) para clasificar a los usuarios y dispositivos en grupos lógicos, definiendo cómo se comunican estos grupos y entre miembros de un mismo grupo. La infraestructura de red aplica estas reglas, segmentando la red, con todas las ventajas que esta segmentación conlleva en cuanto a seguridad y contención de amenazas y a través de una sencilla interfaz gráfica.

Por otro lado, Cisco DNA Spaces es una solución software que aprovecha la información que le proporcionan los equipos conectados a la red para dar visibilidad a la empresa de información vital sobre lo que está ocurriendo en sus edificios, ya sea una oficina, hospital, escuela, universidad, centro comercial, estadio, planta industrial u hotel. Las posibilidades de uso de esta tecnología son amplísimas y ayudan a tomar decisiones que afectan positivamente a la experiencia de los usuarios, así como a mejorar el servicio a clientes y empleados.

También cabe mencionar que la gestión de los equipos Cisco Meraki se realiza desde un cuadro de mando único, de fácil uso, ubicado en la nube para todos los dispositivos Meraki (switches, puntos de acceso, routers con firewalls, sensores y cámaras IoT). Las organizaciones pueden gestionar toda su infraestructura a través de un interfaz gráfico, independientemente de su dispersión geográfica. Todos los dispositivos se configuran, administran y monitorizan desde el cuadro de mando y las políticas se distribuyen desde ese punto único.

SCC Y CISCO: BINOMIO PERFECTO

Specialist Computer Centres (SCC) es Gold Partner de Cisco. Sendas compañías han desarrollado conjuntamente todo tipo de proyectos de redes campus, redes data center, seguridad, redes wireless y colaboración. Sus clientes conjuntos se encuentran en todo tipo de verticales, desde salud, distribución, industria, educación, hoteles, finanzas, seguros o service providers. Sus capacidades son transversales y abarcan desde virtualización (servidores y puesto de trabajo) hasta almacenamiento, pasando por protección y seguridad del dato.

El objetivo de SCC es asegurarse de que la tecnología que implantan sus clientes les ayuda a alcanzar sus objetivos de negocio. Para ello, han conseguido la especialización Cisco Customer Experience.

Además, los servicios gestionados de SCC garantizan una gestión eficiente de la infraestructura TIC de sus clientes, que a medio plazo les permite tomar decisiones de negocio basadas en información real de sus activos de IT. ■

NUEVOS EQUIPOS CISCO

Para garantizar las necesidades de los usuarios en el nuevo entorno del trabajo híbrido, Cisco ha anunciado nuevos equipos y soluciones en switching y redes inalámbricas:

➤ **En Wi-Fi 6E los puntos de acceso Catalyst 9136 y Meraki MR57:** los nuevos productos Cisco Wi-Fi 6E de Catalyst y Meraki son los primeros puntos de acceso 6E de gama alta del sector que abordan los entornos empresariales híbridos más exigentes.

➤ **Conmutadores Catalyst 9000X:** los nuevos modelos Catalyst 9000X amplían la familia de conmutación y ofrecen la red troncal que proporciona la velocidad, la capacidad de ancho de banda y la escalabilidad necesarias para soportar el acceso a la red 100G/400G para las transiciones al trabajo híbrido en el campus y la ampliación de la sucursal con seguridad de confianza cero y eficiencia energética. Los nuevos conmutadores Catalyst de las series 9500X y 9600X están equipados con el nuevo procesador Cisco Silicon One Q200.

➤ **Cisco Private 5G:** el servicio gestionado Private 5G de Cisco ofrece una experiencia inalámbrica sencilla de iniciar, intuitiva de operar y de confianza para las transiciones digitales al trabajo híbrido y al IoT.

Todas estas soluciones se encuentran enfocadas a dotar de adaptabilidad y escalabilidad a las redes que tienen que dar soporte al trabajo híbrido y a la futura utilización de aplicaciones como realidad virtual o realidad aumentada, que requieren mayor ancho de banda y calidad de servicio.

CISCO ENTERPRISE AGREEMENT PROGRAM GUIDE

ESTA INICIATIVA HA SIDO CREADA PARA SIMPLIFICAR LA GESTIÓN DE LICENCIAS Y CONSOLIDAR LAS MÚLTIPLES SUSCRIPCIONES Y FECHAS DE RENOVACIÓN QUE NORMALMENTE REQUIEREN LAS ORGANIZACIONES PARA ADMINISTRAR SUS CONTRATOS DE SOFTWARE.

La agilidad es esencial para las organizaciones de todas las industrias. Las prioridades comerciales cambian constantemente y mantener el ritmo en este entorno dinámico no es fácil, especialmente ante un panorama de software tan complejo como el actual. Los departamentos de tecnología se ven obligados a administrar múltiples contratos, lo que genera costes impredecibles, riesgos de incumplimiento y negociaciones constantes con los proveedores. Cisco entiende que los hábitos convencionales de administración de contratos tecnológicos ya no son aptos. Las organizaciones actuales requieren una mejor manera de administrar fácilmente todas sus soluciones de software a lo largo de sus distintos ciclos de vida, con objeto de poder responder a los cambios continuos del mer-

cado, mantener sus soluciones actualizadas y extraer el máximo retorno de sus inversiones.

A la vista de esta nueva realidad, y con el objetivo principal de minimizar la complejidad de los licenciamientos de software y conseguir que el software sea más flexible y fácil de gestionar, Cisco ha desarrollado Cisco Enterprise Agreement Program Guide. Estas son las principales características de esta herramienta:

- **Compromiso con toda la empresa.** Cisco Enterprise Agreement ha sido diseñado para cubrir a toda la estructura de cualquier organización.
- **Acceso a nuevas funcionalidades de software.** A través de este programa el cliente cuenta con acceso ilimitado a las nuevas funcionalidades de software que se agreguen a las suites adquiridas.
- **Growth Allowance.** Consumo flexible de hasta un 20% para las familias de producto de Colaboración (Flex y Perpetual) y las suites que forman parte de Security Choice. No se aplica a las inscripciones de Cisco DNA, Data Center o Meraki.
- **Precios fijos.** Todos los nuevos Cisco Enterprise Agreement incluyen precios fijos, lo que garantiza que el cliente pueda prever los precios de los productos comprados bajo este programa durante todo el plazo del acuerdo, independientemente de los incrementos de precios que se puedan producir.

- **True Forward.** True Forward es el proceso de ajuste periódico de facturación de Cisco para dar cuenta de cualquier consumo excesivo de productos y servicios durante el plazo de un Cisco Enterprise Agreement. A diferencia de otros acuerdos de licencia empresarial que requieren "ajustes" retroactivos cada año, éste concilia los pagos a través de un True Forward prospectivo. Es decir, si el consumo crece en demasía, el pago se revisa en el próximo período de facturación y continúa durante el resto del plazo de la suite.
- **Términos y Duración.** Los Términos y Duración del programa Cisco Enterprise Agreement han sido diseñados para cubrir todas las compras vía Enterprise Agreement Suite. El plazo estándar es de tres o cinco años.

BENEFICIOS

Cisco Enterprise Agreement simplifica la forma en que las empresas compran, consumen y administran la tecnología de Cisco, en todo su abanico de software, con objeto de alcanzar beneficios reales dentro de su organización.

Por un lado, facilita la compra de tecnología sacando partido de un enfoque simplificado y predecible, reduce el consumo eliminando los quebraderos de cabeza asociados a la adquisición e implementación de software y simplifica su gestión para acelerar la transformación digital.

Y, por otro, cabe reseñar que emplear este programa a lo largo y ancho de todas las arquitecturas tecnológicas con las que cuenta la organización simplifica la gestión de entornos complejos. En primer lugar, la co-terminación de las suscripciones permite ahorrar tiempo al administrar las renovaciones, incluso para soluciones que abarcan múltiples arquitecturas. Además, un espacio de trabajo simple e intuitivo proporciona visibilidad y control de todas las licencias adquiridas e implementadas, avisando del momento de la renovación. Y, por último, los términos y condiciones unificados eliminan complejidad a la hora de administrar múltiples contratos y negociaciones constantes.

PRODUCTOS INCLUIDOS

La iniciativa Cisco Enterprise Agreement Program Guide atiende a las siguientes familias de producto de Cisco:

- **Cisco DNA.** Esta solución ofrece automatización, garantía y seguridad integradas en la propuesta de switching, routing, SD-WAN y wireless de Cisco.
- **Centro de datos.** Este segmento incorpora las suites de software Cisco Data Center Networking, Hyperflex, Intersight, MDS, IWO y Container Platform. Y cuenta con dos complementos opcionales disponibles: Workload Optimization y AppDynamics.
- **Colaboración.** Cisco Collaboration Flex es la solución protagonista en este campo, idónea en todo lo relativo a reuniones y llamadas.
- **Security Choice.** Ofrece acceso personalizado a la gestión presupuestaria de un amplio abanico de soluciones de seguridad.
- **Services Enrollment.** Se trata de un complemento opcional para las soluciones de centro de datos y DNA de Cisco, e incluye Solution Support y la nueva Enterprise Agreement Management Support.
- **Meraki Pilot.** Brinda acceso a las licencias de Meraki, lo que le permite aprovisionar licencias directamente en el cuadro de mandos y eliminar la necesidad de reclamar claves de licencia.
- **AppDynamics Pilot.** Permite administrar todo el espectro tecnológico de Cisco, desde infraestructuras hasta aplicaciones, ofreciendo una experiencia unificada de licencias. ■

ESTAS SON LAS PRINCIPALES CARACTERÍSTICAS DE ESTA HERRAMIENTA: COMPROMISO CON TODA LA EMPRESA, ACCESO A NUEVAS FUNCIONALIDADES DE SOFTWARE, ASIGNACIÓN DE CRECIMIENTO, PRECIOS FIJOS, TRUE FORWARD Y TÉRMINOS

Descubre todas las Soluciones de
Cisco con las que podemos ayudarte

CONTENIDOS↓

Retos y soluciones para una Sanidad en cambio

Patrocinadores:

Retos y soluciones para una Sanidad en cambio

La pandemia del coronavirus ha puesto en evidencia la necesidad de acelerar la transformación digital de prácticamente todos los sectores. En España, al igual que en el resto del mundo, una de las áreas que más afectada se ha visto por su propia naturaleza ha sido la de la sanidad, que se ha enfrentado a una situación sin precedentes que ha obligado a buscar nuevos modelos de atención basados en la tecnología.

Durante estos últimos años, hemos sido testigos de un momento de gran aceleración en la adopción de nuevas tecnologías en todos los sectores. Uno de los más importantes ha sido el sanitario, donde la pandemia ocasionada por la COVID-19 ha puesto de manifiesto la necesidad acuciante de implantar soluciones tecnológicas que dieran respuesta a los grandes retos del presente y del futuro. En una crisis de salud pública como la que vivimos se ha evidenciado que las organizaciones sanitarias no estaban preparadas para atender de forma personalizada a pacientes que no llegaran a través de las vías habituales.

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

Desde la aparición de los primeros casos en febrero de 2020, son ya 11,3 millones de personas las que se han infectado con la Covid-19, y se contabilizan 101.703 fallecidos, a fecha de marzo de 2022. Con estas cifras, España ocupa la décima posición a nivel mundial en cuanto a número de casos confirmados de coronavirus.

Estas cifras han puesto de manifiesto una serie de nuevos retos que ha tenido que afrontar el sector de manera acuciante. Accenture señala en su informe Rapid Response seis retos principales: incremento de pacientes, sobrecarga de llamadas al servicio, monitorización y reporting, coordinación en la respuesta, peligros en la continuidad de la actividad y eficacia del personal.

Como indican las cifras de infectados, el primer reto al que tuvo que hacer frente el sector sanitario ha sido el del incremento de pacientes, que ha llegado casi a colapsar el sistema en momentos determinados. Es por ello que se necesitaron tomar medidas de urgencia, como la utilización de pabellones multiusos para las campañas de vacunación, plantas enteras de hospitales dedicadas a pacientes con Covid e incluso la construcción de nuevos centros hospitalarios para poder dar servicio a la población infectada. Esta sobrecarga de pacientes también se vio reflejada en las líneas telefónicas, con las centralitas de los centros sanitarios completamente colapsadas por las llamadas de los pacientes en busca de información.

Además, la necesidad de mantener una monitorización constante sobre toda la situación se convirtió en una prioridad, de manera que esa recogida de datos de lo que estaba sucediendo permitiera a las autoridades sanitarias tomar las mejores decisiones en función de cómo iban evolucionando las cifras de la pandemia. Otro de los retos más importantes que está encarando el sector es el de la coordinación en la respuesta, para ofrecer al ciudadano información precisa en cuanto a la situación y a las medidas necesarias que debiera tomar en función de su situación.

En España, al igual que en el resto del mundo, una de las áreas que más afectada se ha visto por su propia naturaleza ha sido la de la sanidad, que se ha enfrentado a una situación sin precedentes que ha obligado a buscar nuevos modelos de atención basados en la tecnología

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

Esta situación afectó directamente al colectivo de los profesionales de la salud, que al estar en primera línea, sufrieron directamente las consecuencias de la pandemia, llegando a contraer el virus hasta el 20% del colectivo en algunos casos, lo que suponía un problema a la hora de poder dar un servicio ya de por sí colapsado por el gran número de contagios que se estaban dando. Además, en muchas ocasiones este personal no contaba con los recursos necesarios para poder dar un servicio de calidad, ni a nivel de protección, ni a nivel tecnológico, en un sector que en la mayoría de los casos no había dado muchos pasos para afrontar su transformación digital.

LA HORA DE LA TELEMEDICINA

Para afrontar esta situación, en una pandemia cuya base ha sido la distancia social y el confinamiento de las personas infectadas, uno de los primeros campos que tuvo que revolucionar el sector sanitario fue el de la asistencia, apostando por un modelo remoto a través de la telemedicina, algo que hasta la fecha no era nada común. Un estudio de Capterra señala que un 62% de los españoles ha consultado al médico por medio de esta tecnología a raíz de la pandemia, e incluso para el 92% de las personas había sido su primera vez.

La implantación de este nuevo modelo ha sido todo un éxito, como demuestran datos como los de mediQuo, que señalan que las consultas de telemedicina habían aumentado un 153% en España a los pocos meses desde que se decretara el estado de alarma. Claramente se trata de un modelo que ha llegado para quedarse. Incluso la Organización para la Cooperación y el Desarrollo Económicos (OCDE) señalaba en un informe la necesidad de fortalecer los servicios de salud prestados de forma electrónica a través de internet.

El informe "Telemedicine: Emerging Technologies, Regional Readiness & Market Forecasts 2021-2025" de Juniper Research indica que gracias a la telemedicina el sector sanitario podrá ahorrar 21.000 millones de dólares en costes para el año 2025 y señala que para ese año ya se habrán realizado más de 765 millones de teleconsultas a nivel global.

Pero la velocidad a la que se ha impuesto este nuevo modelo hace que tanto profesionales sanitarios como pacientes se enfrenten a una serie de retos que tendrán que ir afrontando poco a poco. Uno de los más importantes es el de la reducción de la brecha digital, algo a lo que ayudaron mucho otros sectores como las compras online o las videollamadas con la familia durante el confinamiento, que pusieron sobre la mesa estas tecnologías para toda la población. Además, los profesionales sanitarios requieren de formación específica en el uso de esta nueva modalidad, de manera que sean capaces de ofrecer la mejor experiencia al paciente, ofreciéndole la mayor cercanía posible. Otro reto es el puramente tecnológico, con la necesidad de equipos

y conexiones de calidad que no entorpezcan la videoconsulta.

LOS DATOS Y SU CONFIDENCIALIDAD

Como en la mayoría de las industrias, la importancia del dato es primordial para ofrecer un servicio de calidad al paciente. En el caso del sector sanitario más si cabe, puesto que se trata de datos inherentes a las personas, con lo que la necesidad de mantener la confidencialidad médico-paciente se vuelve mucho más acuciante si cabe.

Por un lado, el sector utiliza todo el aglomerado de datos abiertos que puede obtener con el fin de optimizar su gestión y la organización de recursos, como indica el estudio "The Open Data Impact Map" de Open Data for Development Network (OD4D). Esto es muy importante en casos como el de la medicina preventiva, ya que permite el desarrollo de modelos predictivos capaces de diseñar patrones de comportamiento, que a través del análisis de los datos facilita una mejor atención del paciente, predecir su evolución e incluso adelantarse a sus necesidades.

El Big Data es un sector que está creciendo exponencialmente en todos los ámbitos, como demuestra el estudio de Technavio "Big Data Market by Type, Deployment, and Geography - Forecast and Analysis 2021-2025" que señala que para 2025 este mercado crecerá hasta los 247.300 millones de dólares con un CAGR del 18%. En concreto aplicado a la salud, el informe Big Data Analytics In Healthcare Market de Allied Market Research indica que su valor alcanzará los 67.820 millones de dólares para 2025.

En los proyectos estratégicos para la recuperación y transformación económica (PERTE), el Gobierno de España ha tenido muy en cuenta al sector sanitario, estableciendo un PERTE para la salud de vanguardia

En el sector sanitario se recaban una gran cantidad de datos que pueden provenir de diferentes fuentes: desde la información proporcionada por la maquinaria médica (pruebas de imagen y de laboratorio), hasta la información aportada por el propio paciente. La recogida, almacenamiento, tratamiento y posterior análisis de esos datos debe seguir un cuidadoso protocolo que permita facilitar la labor de los profesionales de la salud, para que puedan disponer de ellos siempre que los necesiten de una forma rápida y sencilla, pero teniendo en cuenta la importancia máxima de su seguridad, de manera que no haya brechas ni a la hora de almacenarlos ni en el momento de ser transferidos, sea por el medio que sea.

Para ello, la tecnología se pone al servicio del sector, por lo que es tarea de las organizaciones de salud implementar las soluciones adecuadas a la hora de velar por la privacidad de los datos, de contar con los dispositivos adecuados para su recogida y almacenamiento, y de preparar a los profesionales que están en contacto con ese dato, de manera que realicen un tratamiento y mantenimiento correcto.

EL GRAN RETO DE LA SEGURIDAD

Por si era poco la situación de pandemia que se desató a principios de 2020 con la aparición del coronavirus, el sector sanitario ha tenido que enfrentarse en este tiempo a un nuevo reto, el gran aumento de ciberataques que se ha producido con el punto de mira puesto en la industria de la salud. El pasado año, el Instituto Nacional de Ciberseguridad de España (INCIBE) señalaba que más de 500 instituciones sanitarias españolas habían notificado incidentes o reportes de vulnerabilidad, lo que suponía un 48% más con respecto al año anterior.

Uno de los principales riesgos a los que se enfrenta el sector sanitario es el de los ataques de ransomware, a través de los cuales el ciberdelincuente es capaz de cifrar toda la información del sistema para pedir un rescate a cambio de su liberación. Este tipo de ataques se han multiplicado en los últimos años. Según el informe "El estado del ransomware en la sanidad 2021" de Sophos, algo más de un tercio de las organizaciones sanitarias españolas (34%) recibieron algún tipo de ataque de ransomware el año pa-

sado. Para poder recuperar sus datos, el 34% decidió pagar el rescate, ya que no consiguieron hacerlo de otra forma, como demuestra que solo el 44% de las instituciones sanitarias consiguieron restaurar sus datos a través de copias de seguridad. Estos datos ponen de manifiesto el éxito que tiene este tipo de ataques para los ciberdelincuentes, lo que explica este aumento en los últimos años.

Pero el ransomware no es el único peligro que amenaza al sector sanitario. Las fugas de datos también están a la orden del día, como demuestran los datos de Bitglass, que indican que tan solo en Estados Unidos se produjeron 599 fugas de información en esta industria que afectaron en conjunto a más de 26 millones de personas. Sistemas desactualizados, tráfico de correo electrónico no cifrado, el Internet de las Cosas cada vez con mayor penetración en el sector sanitario, son muchos los riesgos que se presentan para un sector que ha tenido que afrontar una transformación digital de la noche a la mañana, para la que en muchas ocasiones se primó la necesidad de activar determinados servicios sin pararse a pensar en las capas de protección que serían necesarias para mantenerlos seguros.

Para ayudar a securizar los nuevos entornos digitales creados tras la pandemia, el Instituto Nacional de Ciberseguridad (INCIBE) ha publicado una serie de pliegos por sectores denominados Sectoriza2 con una serie de consejos y herramientas que ayudarán a las organizaciones a protegerse, incluyendo como no podía ser de otra manera también al sector sanitario.

PERTE PARA LA SALUD DE VANGUARDIA

Entre los proyectos estratégicos para la recuperación y transformación económica (PERTE), el Gobierno de España ha tenido muy en cuenta al sector sanitario, estableciendo un PERTE para la salud de vanguardia a finales del pasado año 2021. Su finalidad es la de apoyar la transformación digital de la industria sanitaria y prevé una inversión entre el sector público y el privado de 1.469 millones de euros en el periodo 2021 y 2023.

Los cuatro grandes objetivos que persigue este plan son posicionar a España como país líder en la innovación y desarrollo de terapias avanzadas, impulsar la puesta en marcha de medicina personalizada de precisión de forma equitativa, desarrollar un Sistema Nacional de

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

Salud digital y potenciar la atención sanitaria primaria a través de la transformación digital.

Como demuestras estos objetivos, el impulso de la transformación digital del sector es un hecho. Por un lado, el Componente 11 (Modernización de las administraciones públicas) está orientado al establecimiento de diferentes medidas para la modernización de los servicios digitales ofrecidos por el Ministerio de Sanidad en tres áreas principales de actuación: el desarrollo de servicios digitales e inteligentes, la interoperabilidad de la información sanitaria y el impulso a la analítica de datos.

Por otro lado, el Componente 18 hace mención de un Data Lake sanitario, que supone la creación de un repositorio de datos alimentado por los diferentes sistemas de información relevantes en Salud y que permitirá un análisis masivo e inteligente de los mismos, con capacidad de respuesta en tiempo real, orientado a la protección de la salud, la predicción sanitaria, así como para el incremento en la eficiencia del diagnóstico, tratamiento y rehabilitación de enfermedades, en las condiciones adecuadas de ciberseguridad.

Además, el Componente 19 hace mención a la necesidad de que los profesionales sanitarios también adquieran competencias digitales avanzadas dentro de los programas de formación, con menciones específicas a tecnologías disruptivas como la Inteligencia Artificial o la robótica, sin dejar de lado la ciberseguridad. ■

MÁS INFORMACIÓN

- Número acumulado de casos confirmados y muertes del coronavirus en España entre el 15 de febrero de 2020 y el 18 de marzo de 2022 de Statista
- Número de casos confirmados de coronavirus en el mundo a fecha de 18 de marzo de 2022, por país de Statista
- Informe Rapid Response de Accenture
- Diario Médico: profesionales sanitarios infectados por el coronavirus en España
- Capterra: Telemedicina en España: la irrupción tecnológica en la relación paciente-médico
- mediQuo: La razón por la que los médicos se deben adaptar a la nueva normalidad
- OECD Economic Surveys Spain
- Informe "Telemedicine: Emerging Technologies, Regional Readiness & Market Forecasts 2021-2025" De Juniper Research
- Estudio "The Open Data Impact Map" de Open Data for Development Network (OD4D)
- Estudio Technavio "Big Data Market by Type, Deployment, and Geography - Forecast and Analysis 2021-2025"
- Informe Allied Market Research Big Data Analytics In Healthcare Market
- Datos sobre aumento de ciberataques al sector sanitario del Instituto Nacional de Ciberseguridad de España (INCIBE)
- Informe "El estado del ransomware en la sanidad 2021" de Sophos
- Informe Bitglass sobre fugas de datos en el sector sanitario de Estados Unidos
- Sectoriza2 Salud, Instituto Nacional de Ciberseguridad de España (INCIBE)
- PERTE para la salud de vanguardia

logitech

SOLUCIONES LOGITECH PARA **ENTORNOS SANITARIOS**

Conéctese a través de vídeo de alta calidad cuando y donde sea más necesario.

Retos y Soluciones para una Sanidad en cambio

En el sector sanitario, la pandemia provocada por la Covid-19 ha puesto de manifiesto la necesidad acuciante de implantar nuevas soluciones tecnológicas que dieran respuesta a los grandes retos a los que se enfrenta el sector. Necesitamos una nueva forma de atención digital, una telemedicina que consiga conectar con los pacientes de forma preventiva y que los datos médicos sensibles y su análisis estén siempre disponibles y se pueda acceder a ellos de manera segura.

La llegada de la pandemia del coronavirus supuso una aceleración para la transformación digital de prácticamente todos los sectores, pero impactó a uno de ellos directamente: la sanidad. El sector sanitario se vio en la necesidad de realizar un cambio en sus procesos y aceleró su digitalización a pasos agigantados, tanto a la hora de hablar de teleasistencia como de los datos que manejan las organizaciones sanitarias, en muchos casos de una sensibilidad extrema. Esta rapidez a la hora de adoptar estos nuevos modelos no siempre se vio acompañada de un cuidado por la seguridad, lo que ha implicado grandes riesgos tanto para las propias instituciones sanitarias, como para el ciudadano. Por ello, el sector se enfrenta a una serie de importantes retos a los que debe dar solución de manera rápida y eficaz. Para hablar sobre cómo ha sido la transformación digital de la sanidad y cuáles son

MESA REDONDA IT: Retos y Soluciones para una Sanidad en cambio

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

"La visibilidad y el inventario de lo que tengas es la base para empezar a hacer políticas, segmentaciones de las redes, para intentar estar lo más seguro posible"

VESKU TURTIA

los principales retos a los que se enfrenta, hemos contado en esta Mesa Redonda IT con la participación de Vesku Turtia, Regional Director España y Portugal de Armis; David Marco, CEO de Iberlayer; Javier Rodríguez, Senior Key Account Manager de Logitech; Fernando Gutiérrez, Account Executive de MicroStrategy; Álvaro Fernández, Enterprise Account Executive de Sophos y Borja Pérez, Country Manager de Stormshield.

ESTADO ACTUAL DEL SECTOR SANITARIO

La mesa redonda comenzó agradeciendo a los profesionales sanitarios los esfuerzos que han realizado durante la pandemia, y que siguen realizando aún a día de hoy. En cuanto al estado actual del sector, para David Marco ha habido una evolución gigantesca. "Vemos una clara progresión hacia adelante, en cuanto a la integración de tecnologías dentro de la sanidad, ha mejorado en todos los sentidos, en lo personal, en lo tecnológico...". El portavoz señala que muchos aspectos han mejorado muchísimo, como por ejemplo la teleatención. A pesar de ello, cree que hay un pequeño desfase en cuanto a la responsabilidad que tienen estos profesionales y las capacidades que se les dan.

Javier Rodríguez señala que ha habido un cambio de paradigma que ha sucedido de forma muy acelerada, por lo que han surgido algunas carencias. Por ejemplo, en el área de la videocolaboración. "No se ha hecho teniendo en cuenta la tecnología adecuada de audio y video y al final hay mucho por mejorar en ese ámbito". Puede haber muchas vías de mejora para reducir colas en la atención primaria, para realizar algunas consultas que no requieran exploración de manera remota o para dar mejor calidad a los pacientes, que tengan que evitar desplazamientos y descongestionar un poco los centros de salud.

Por su parte, Fernando Gutiérrez cree que el estado de la sanidad en general en España en relación al dato ha salido reforzado. "Siempre se ha tenido el dato en cuenta, pero esta situación de necesidad tan brutal ha puesto de manifiesto la necesidad de apoyarse en el dato para tomar

"Si sigo construyendo la casa cogiendo piezas de la parte de abajo para crecer en altura cada vez más, pero usando materiales de abajo, llega un momento en que lo de arriba pesa tanto y lo de abajo es tan débil que no va a aguantar"

DAVID MARCO

decisiones y para la gestión". En esos momentos que se vivieron y que se siguen viviendo de estrés es donde se ponen a prueba todos los sistemas, las cosas que funcionan bien, las cosas que tienen área de mejora... Se ha visto que esa necesidad de analizar de manera inmediata la disponibilidad de camas, de material o de personal, ha hecho que el dato haya cobrado mayor importancia.

UNA ACELERACIÓN EN SU TRANSFORMACIÓN DIGITAL

Sin duda la pandemia creo una situación sin precedentes ante la que prácticamente nadie estaba preparado. ¿La situación vivida durante estos

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

"Ha habido un despliegue acelerado y masivo de las plataformas de colaboración, pero hay mucho campo de mejora en dotar de los dispositivos adecuados para que los equipos médicos puedan colaborar a distancia"

JAVIER RODRÍGUEZ

últimos años de pandemia ha supuesto una aceleración en los procesos de transformación digital de la sanidad?

Para Vesku Turtia es un rotundo sí. Durante la pandemia no solo el sector de la salud, sino que todos los sectores han acelerado su transformación digital. "Lo que veo ahora con muchísima alegría es también que en el uso de distintos aparatos médicos en los hospitales tanto del sector privado como del público, están poniendo foco para ver cómo se puede securizar el uso de los sistemas médicos, porque hoy en día los hospitales, tanto del sector público como del privado, están bastante digitalizados". Como vivimos en un mundo que no es perfecto, los ataques de ransomware pueden afectar a los sistemas de IT de un centro hospitalario, pero también ese mismo malware puede entrar en equipos médicos e incluso poner en peligro a los pacientes. "Vamos bien, pero todavía queda mucho que hacer".

En palabras de Fernando Gutiérrez, "la sanidad no podía estar fuera de esta transformación digital". La necesidad ha supuesto un acelerón de la digitalización, de eso no hay duda y pasa en general en todos los sectores, pero esta transformación digital ha venido muy propiciada también porque ha habido una digitalización del usuario. "La sanidad se ha encontrado con un ciudadano también más abierto, más preparado para utilizar canales digitales". En cuanto a las personas mayores, que conforman gran parte de los usuarios de los servicios médicos, ha sido la necesidad de otros sistemas, como las compras online o las videollamadas con la familia, lo que ha conseguido que se digitalizaran.

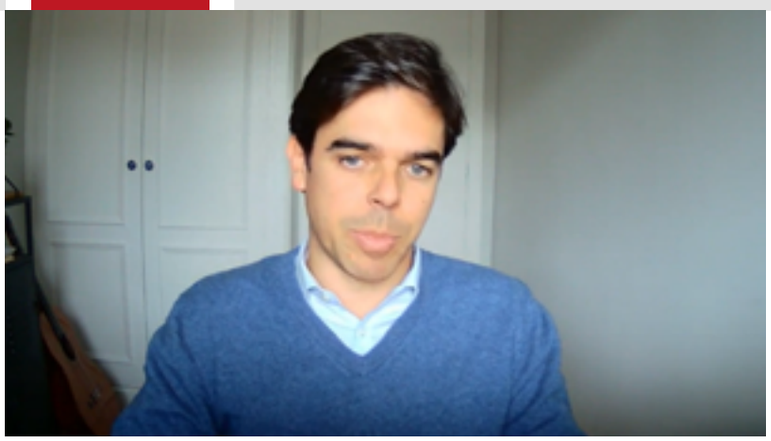
Según Álvaro Fernández, ha habido sectores que habían avanzado más en su transformación digital porque se había demandado por parte de los usuarios. En el sector de la sanidad, al igual que por ejemplo en el de la educación, quizá no hubo esa demanda, que surgió a raíz de la pandemia y se tuvo que hacer de forma precipitada. "Desde el punto de vista de la seguridad, las prisas son enemigas de la securización. Se han priorizado los servicios perjudicando de alguna forma el hacer esos servicios seguros". Además, añadía que "la pandemia hizo que todas las organizaciones de salud sin excepción pisasen el acelerador y fuesen a modelos más digitales para poder seguir dando un servicio". Estas organizaciones están trabajando ahora en terminar de securizar estos servicios y en consolidarlos.

"Siempre se ha tenido el dato en cuenta, pero esta situación de necesidad tan brutal ha puesto de manifiesto la necesidad de apoyarse en el dato para tomar decisiones y para la gestión"

FERNANDO GUTIÉRREZ

Borja Pérez es de la opinión que hay distintos ritmos de transformación digital según las organizaciones. Para explicar su afirmación, saca a colación el PERTE que se ha aprobado para sanidad, el cual está dotado con 1.500 millones de euros y en el que hay cuatro grandes áreas

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO



"Desde el punto de vista de la seguridad, las prisas son enemigas de la securización. Se han priorizado los servicios perjudicando de alguna forma el hacer esos servicios seguros"

ÁLVARO FERNÁNDEZ

de trabajo, una de ellas para la transformación digital en la atención primaria. "Las autoridades son conscientes de que hay que avanzar en ese sentido, pero hoy por hoy la atención primaria por ejemplo todavía adolece de falta de medios". Después hace referencia a que los envíos de datos no son siempre del todo seguros: "Hay un montón de transferencias de datos en otras áreas y en muchos casos todavía no están debidamente implementados los procesos más seguros y más adecuados".

¿ESTÁ PREPARADA LA SANIDAD?

La transformación digital de los entornos sanitarios ha supuesto la aceleración e implantación de nuevos modelos de asistencia, la telemedicina, la gestión y análisis de los datos y la securización de todos los sistemas. ¿Realmente está la sanidad preparada para todos estos avances?

En opinión de Vesku Turtia, lo más importante es que las organizaciones sepan lo que tienen en su infraestructura. "La visibilidad y el inventario de lo que tengas es la base para empezar a hacer políticas, segmentaciones de las redes, para intentar estar lo más seguro posible". Es importante ser consciente de todo lo que hay, para después poder hacer las estrategias e integraciones necesarias para proteger todos los sistemas. "Cuanto más avanzamos en integración tecnológica, más dependientes somos de ella", comenta David Marco, que añade hablando de la securización de los sistemas: "Rara vez se piensa en la seguridad antes que en el servicio". El portavoz señala hay pocos servicios sanitarios que tengan un departamento de seguridad, y subraya la importancia de proteger el correo electrónico: "9 de cada 10 ataques de ransomware empiezan por un email, sin embargo solo el 5% de los presupuestos de ciberseguridad se dedican a proteger el correo".

Álvaro Fernández también pone el punto de mira en la seguridad, cuando habla de la transformación digital acelerada que tuvo que emprender el sector a raíz de la pandemia: "Hay mucho espacio de mejora. Hemos podido salvar el escollo sabiendo que no ha sido todo lo seguro que debiera y hay muchas cosas que hacer". En su opinión hay diferentes escenarios en cuanto al estado de las organizaciones sanitarias se refiere: "hay algunas que están mejor, otras que están peor, pero por supuesto hay mucho que hacer".

"Hay concienciación sobre privacidad y confidencialidad de los datos del paciente, pero yo creo que no hay todavía los recursos dedicados a proteger la integridad y a proteger la disponibilidad de los datos"

BORJA PÉREZ

A Borja Pérez no le preocupan tanto estos nuevos servicios como el tema de los datos: "me preocupa más la gestión de datos internamente dentro de las distintas organizaciones". A la hora de hablar de Big Data, es importante que los datos vayan anonimizados para trabajar con ellos.

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

Por otra parte, también cree que en el sector hay luces y sombras. “Es un entorno muy heterogéneo e incluso dentro de un mismo hospital hay áreas que están a la última y áreas que están todavía muy atrasadas”.

DATOS Y TELEASISTENCIA

La nueva normalidad en la sanidad conlleva una securización del acceso a datos especialmente sensibles y del análisis de los mismos, así como de un nuevo modelo como es el de la teleasistencia, la virtualización o la movilidad que implica la asistencia remota.

Según Vesku Turtia “es muy importante proteger los datos de dentro del hospital con las segmentaciones”. Es de la opinión que se está mejorando muchísimo en ese aspecto, y las instituciones, tanto públicas como privadas, están esforzándose muchísimo para proteger nuestros datos aparte de nuestra salud. Sobre todo cree que hay que poner el foco en que la circulación de los datos sea segura.

Javier Rodríguez comenta que “Los centros sanitarios donde hemos hecho despliegues de soluciones de videocolaboración, en barras por ejemplo de última generación, estas barras vienen ya con computación integrada, con inteligencia artificial, y sí que veo a los responsables de los centros sanitarios concienciados con el tema de la seguridad”. Señala que hay cierta concienciación, pero está seguro que aún queda mucho por hacer.

En palabras de Fernando Gutiérrez, “en la parte del dato, hay velocidades distintas, no es lo mismo la sanidad pública que la sanidad privada y dentro de cada uno de ellas, hay hospitales y organizaciones en distintos rangos”. El objetivo es que también la sanidad siga el concepto de Data Driven Company. También señala que la población cada vez es más digital, pero sigue habiendo una brecha importante que hay que romper.

Para Borja Pérez “Hay concienciación sobre privacidad y confidencialidad de los datos del paciente, pero yo creo que no hay todavía los recursos dedicados a proteger la integridad y a proteger la disponibilidad de los datos”. El portavoz subraya que no se trata de un problema exclusivo de España, sino que es un problema a escala mundial. “No se están tratando de forma adecuada esos datos, no se están almacenando adecuadamente”.

ÁREAS DE MEJORA

Ante este panorama, ¿cuáles son las principales áreas de mejora que debe considerar la sanidad?

David Marco señala que descuidar la seguridad puede traer tres tipos de consecuencias: en el funcionamiento de la organización, consecuencias legales y para pacientes y empleados. “Si sigo construyendo la casa cogiendo piezas de la parte de abajo para crecer en altura cada vez más, pero usando materiales de abajo, llega un momento en que lo de arriba pesa tanto y lo de abajo es tan débil que no va a aguantar”. Hay que avanzar, pero de forma segura.

Donde pone el acento Javier Rodríguez es en la videocolaboración: “Ha habido un despliegue acelerado y masivo de las plataformas de colaboración, pero yo creo que hay mucho campo de mejora en dotar de los dispositivos adecuados para que los equipos médicos puedan colaborar a distancia y al final puedan llegar a diagnósticos entre varios especialistas remotamente, realizar por ejemplo ciertas terapias…”. A nivel de teleasistencia sí cree que se han dado pasos agigantados y los pacientes están más concienciados, pero tenemos que dar un salto en la calidad de la tecnología que se utiliza para dar esa asistencia.

Por su parte, Álvaro Fernández señala que las principales áreas de mejora en sanidad son cerrar la brecha que se ha producido entre servicios y seguridad por las prisas con las que se hizo la implementación y dotar a las organizaciones de más personal de IT. “Es uno de los ratios de los diferentes sectores donde menos personal de IT tiene más carga tecnológica para gestionar”. ■

MÁS INFORMACIÓN

Retos y Soluciones para una Sanidad en cambio

MAURICIO VALBUENA, RESPONSABLE DE INNOVACIÓN,
DIRECCIÓN DE PROYECTOS Y MEJORA CONTINUA DE LOS HOSPITALES
DEL T2 PÚBLICOS BCN-VALLÉS, QUIRÓN SALUD

“Esta situación vivida ha puesto a prueba la adaptabilidad de las organizaciones”

Tras dos años en el foco de la actualidad, directamente impactado por la pandemia, el sector de la Sanidad ha visto que los proyectos de Transformación Digital han tenido que acelerarse para poder estar a la altura de las demandas de profesionales y pacientes. De la situación actual que vive el sector, así como de los retos pendientes, hemos conversado con Mauricio Valbuena, responsable de innovación, Dirección de Proyectos y Mejora Continua de los hospitales del T2 Públicos BCN-Vallés, Quirón Salud.

¿Cómo valora la situación actual de la Sanidad después de estos dos últimos años de pandemia?

Escenarios como el surgido en Wuhan hace 2 años, que carecieron de un adecuado análisis predictivo integrado por parte de los sistemas de vigilancia epidemiológica a nivel mundial, ha puesto en el punto de mira la fragilidad y las grandes carencias de los ecosistemas sanitarios del siglo XXI. Es importante reconocer que nos queda mucho camino por recorrer no solo en materia de igualdad de derechos, sino también de accesibilidad, de igualdad de oportunidades y de mejorar las coberturas; hay que resaltar que la inversión es importante y que las organizaciones sanitarias deben asumir después de esta situación de emergencia no solo un compromiso, sino el reto de transformarse.

La realidad de los pacientes crónicos y los que se encontraban en listas de espera, el frenazo a la investigación científica al concentrarse fundamentalmente en el Covid-19, el impacto de la

pandemia y sus consecuencias en la salud mental, así como la situación que viven los profesionales sanitarios, ha creado una realidad muy compleja para asumir.

Se hace muy necesario no solo el conocimiento en materia de actualidad sino la capacidad de implementar medidas de cambio agiles y con visión holística, que permitan a los lideres de las organizaciones sanitarias agilizar la adaptación a este período de transición y anticiparse a lo que sucederá en los próximos años. Ha de quedar claro que no solo hablamos de avances en el área tecnológica, sino también en lo relacionado a la adopción de nuevos modelos organizacionales innovadores, más dinámicos y eficientes, centrados en las personas pero que utilizan la tecnología como palanca de aceleración, todos nacidos dentro de la filosofía de cambio implícita en la ola de la transformación digital y que indudablemente están cambiando la manera de funcionar y de gestionar la salud por parte de las organizaciones sanitarias.

¿Considera que esta situación pandémica ha provocado un cambio de paradigma en la Sanidad y, debido a esto, se han acelerado los procesos de Transformación Digital e Innovación en el sector?

La situación vivida ha roto de forma inesperada los esquemas en los que estábamos anclados, ha sido la palanca de cambio perfecta para la irrupción en pleno de este nuevo actor que es la transformación digital. Es tal vez por este motivo que la gestión organizacional de esta situación tan excepcional durante la pandemia ha supuesto una serie de desafíos para los distintos actores implicados, así como la necesidad de planificación de cambios adaptativos, a una velocidad sin precedentes dentro y fuera de los ecosistemas sanitarios. Sería difícil hablar de esta gestión sin resaltar el esfuerzo titánico que esto supuso para las áreas TIC, que han tenido que afrontar con urgencia el despliegue de infraestructuras y herramientas tecnológicas a una escala sin precedentes, para hacer frente a la situación generada por el nuevo escenario que planteo la crisis sanitaria. Cambios que han llevado a rediseñar por completo, no solo la manera de prestar servicios en salud, sino la visión de las organizaciones y sus procesos, para garantizar la continuidad de aquellos servicios que pasaron del formato clásico presencial en su gran mayoría, a ser atendidos por canales digitales de la noche a la mañana.

“La situación vivida ha roto de forma inesperada los esquemas en los que estábamos anclados, ha sido la palanca de cambio perfecta para la Transformación Digital”

Esta situación de cambio, derivada del afán de la implementación de estrategias de transformación digital, buscando minimizar el impacto de la pandemia en la salud de la población, ha puesto a prueba la adaptabilidad de las organizaciones, que a su vez han puesto el foco en la introducción de cambios tecnológicos, y pueden haber ignorado en algún momento el papel relevante de las personas que conforman los ecosistemas de salud. Las personas son una pieza clave, no solo en la fase de implementación, sino en la consolidación y la evolución del cambio cultural, que pueda garantizar el éxito de este nuevo paradigma que ha traído la transformación digital.

Desde las lecciones aprendidas, ¿cómo considera que deberá evolucionar el sistema sanitario para garantizar una asistencia efectiva y de calidad al paciente? ¿Cuáles deberían ser los pasos siguientes en el camino de digitalización del sector?

Los resultados y las lecciones aprendidas de la pandemia por Sars-Cov-2, en el contexto de su comportamiento impredecible y variable en las distintas olas vividas, muestran un camino claro; lo primero y muy importante es la necesidad de inversión. Y es que ahora es el momento para apostar por la innovación disruptiva, por investigar y desarrollar nuevas tecnologías en

“Asistimos a la era del Dato de calidad como herramienta útil no solo para la medición, sino en la planificación y en la predicción de escenarios fuera de lo común”

materia de atención sanitaria, implantarlas no solo como un eje de crecimiento económico, sino con un serio compromiso social de todos los actores que participan directa o indirectamente en el sector salud.

Un reciente artículo publicado en New Medical Economics comparte cinco recomendaciones que he considerado como líneas estratégicas sobre las cuales evolucionar. Estas líneas, deberían estar muy bien alineadas con las tecnológicas; con la sencilla idea de generar dinámicas que sean favorables y que permitan avanzar en este cambio cultural. Tenerlas en cuenta, garantizará la creación de modelos efectivos que sean capaces de satisfacer las necesidades de las personas integrantes de los sistemas sanitarios y que tengan a su vez un alto impacto positivo sobre el end-user que es el paciente: Formación, visión integral, inversión a largo plazo, políticas público-privadas y comunicación y compromiso.

Por otra parte, es muy necesario que se establezca un foro abierto público-privado, que permita la creación de políticas con líneas estratégicas comunes, bien definidas y que dibujen procesos con métricas claras, que nos permitan trazar dentro de las organizaciones sanitarias la situación real, su evolución y puntos de mejora. Un modelo uniforme y homogéneo que dibuje un engranaje dinámico, que permita la evolución exponencial de los todos los actores involucrados, la creación de alianzas estratégicas con actores tecnológicos que fortalezcan la sostenibilidad y adaptabilidad del modelo al entorno, y que faciliten el camino hacia la verdadera transformación digital que requieren los sistemas de salud hoy.

Es por este motivo que urge trabajar en la búsqueda de modelos innovadores de alto rendimiento, que sean capaces de conectar a todos los actores, que lideren una transformación del sistema con un “scope” holístico, donde se innove en procesos asistenciales, donde se integren nuevas tecnologías y se promueva la salud digital, que faciliten la incorporación de infraestructuras tecnológicas; no solo basados su capacidad de vigilancia y prevención en salud, sino con una alta capacidad para adaptarse y evolucionar según el entorno, que permitan la toma decisiones de alto impacto, en tiempo real, con datos fiables, recopilados de los mismos sistemas sanitarios; pero con una interoperabilidad e interconectividad de alcance global. Modelos que ofrezcan una atención sanitaria adecuada, personalizada, predecible, ágil, segura, y con un alto nivel de calidad tanto para el personal asistencial, como para el paciente.

¿Quieres saber más?

Este texto es un resumen de la entrevista con Mauricio Valbuena. Puedes leer la entrevista completa en este enlace

Desde su punto de vista, ¿cómo puede ayudar la tecnología en la evolución y medición de la calidad de la asistencia sanitaria? ¿Qué herramientas considera que son necesarias para ello?

La importancia que ha adquirido la tecnología en el mundo de la asistencia sanitaria es un hecho indudable; vemos con diferencia cómo este campo se está viendo beneficiado en gran medida por un alto nivel de inversión y por los nuevos avances tecnológicos-científicos. Podríamos decir, sin temor a equivocarnos, que asistimos a la era del Dato de calidad como herramienta útil no solo para la medición, sino en la planificación y en la predicción de escenarios fuera de lo común; sino como una nueva herramienta que juega un papel importantísimo para la

supervivencia y evolución de las organizaciones sanitarias.

Hasta hace muy poco la explotación de los datos se hacía de una forma meramente descriptiva buscando asociar factores de riesgo para plantear acciones preventivas, sobre bases observacionales aplicando estadísticas y probabilidades. Gracias a la irrupción de estas nuevas tecnologías y a su gran capacidad de análisis de grandes volúmenes de datos y prácticamente en tiempo real, es posible construir modelos con un perfil mucho más objetivo y dinámico, con un enfoque predictivo y personalizado, que nos permita abordajes más personalizados y de calidad en materia de diagnóstico, tratamiento y seguimiento de diferentes enfermedades. Los nuevos modelos de análisis predictivo permitirán una anticipación de un modo más real a situaciones como la que se vivió durante esta pandemia.

En este sentido, la aparición de la nueva cultura centrada en los datos, Data Driven, y con herramientas poderosas de análisis, Data Analytics, muestran una alta capacidad para recopilar, clasificar y analizar enormes cantidades de datos generados por dispositivos de todo tipo que son parte del día a día de las personas. El dato de calidad es el actual protagonista del nuevo modelo de atención y gestión de la salud. Gracias a herramientas tecnológicas como la inteligencia artificial y el Big Data, la interpretación y el análisis predictivo de datos está transformando la

> "La inversión es importante y las organizaciones sanitarias deben asumir después de esta situación de emergencia no solo un compromiso, sino el reto de transformarse"

forma de entender y prestar servicios dentro de los ecosistemas sanitarios.

Estamos viviendo un nuevo modelo de asistencia sanitaria... telemedicina, gestión y analítica de datos sensible, securización de infraestructura y accesos ... ¿está la sanidad preparada para soportar estos nuevos modelos? ¿Qué tipo de escenarios de atención al paciente podremos ver que se van a crear en los próximos meses/años?

Digitalmente hablando, la hiperconectividad se ha convertido en un aspecto clave de la transformación de los modelos de negocio y de las organizaciones sanitarias. La innovación y la irrupción en los entornos sanitarios de nuevas tecnologías, los grandes volúmenes de datos generados relativos a las personas plantean muchos interrogantes en materia de seguridad y desde la perspectiva de derechos y libertades. En concreto, en materia de derechos fundamentales como el de la intimidad y la protección de datos personales.

De ahí, que para que este proceso de transformación digital sea confiable y seguro, tiene que ir acompañado del cumplimiento de la normativa aplicable en protección de datos personales, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (no hay que olvidar que no estamos protegiendo datos sino derechos y libertades de las personas físicas) y por la implementación de políticas de seguridad realmente eficientes y que comprometan al conjunto de las organizaciones sanitarias de modo efectivo. En definitiva, cumplir con esta normativa en materia de privacidad y protección de datos, supondrá una mejora en los resultados y la competitividad de las organizaciones sanitarias; que, además, permitirá aportar seguridad y confianza, favoreciendo la transparencia de las organizaciones y fortaleciendo la relación con los usuarios.

Por otra parte, una de las grandes ventajas que aporta la transformación digital a las organizaciones, es precisamente el buen aprovechamiento de la información obtenida de los datos masivos generados gracias a la incorporación de las nuevas tecnologías a los ecosistemas sanitarios. Es así, como en los últimos años se ha visto un crecimiento en la tendencia de invertir en herramientas de inteligencia empresarial, y

analítica de datos; con la consiguiente mejora de resultados comerciales y el incremento directo de beneficios para las organizaciones.

Por último, y como conclusión, ¿cuáles son, desde el punto de vista de la tecnología y su transformación digital asociada, las principales áreas de mejora que debe abordar la Sanidad? ¿Qué tecnologías emergentes o ya consolidadas van a tener un mayor protagonismo en Sanidad en los próximos años?

En líneas generales, esta pandemia podríamos decir que se ha transformado en un catalizador de grandes avances en materia de salud; el cre-cimiento abrumador de tecnologías digitales; el acceso a datos y a su creciente capacidad de análisis, la cultura de empoderamiento del paciente, su autocuidado y su experiencia son factores que juegan un papel importante en los próximos años y aceleraran aún más la transformación de los ecosistemas sanitarios.

Son ya muchas las herramientas tecnológicas nacidas en los entornos digitales forzados por la pandemia, todo ello ha despertado una respuesta de creciente interés por parte actores externos, que buscan activamente incursionar en el mundo sanitario y establecer un nicho de mercado. Muchas de estas tecnologías en los próximos años, se harán cada vez más presentes, consolidando un nuevo modelo de relación médico-paciente. Modelos basados en servicios no presenciales como punta de lanza; veremos una notable mejora no solo en cuanto al alcance de oportunidades y de cobertura de la atención médica, sino también en la gestión de la salud de las personas. Hecho que por otra parte permitirá a los actores del sistema sanitario un cambio de visión, ya que serán más ágiles y/o eficientes en la prevención y detección de ciertas enfermedades o en el seguimiento mismo del enfermo crónico; todos ellos, aspectos que fueron relegados a un segundo plano debido a la situación de colapso de los servicios sanitarios generado durante la reciente pandemia.

Creo que todas las organizaciones sanitarias deberían tomar conciencia a nivel general, que deben seguir apostando por la transformación digital. Que no es cuestión de digitalizar los procesos para generar dinámicas de cambio. Que el mindset digital se logra con un profundo conocimiento de los procesos y de los circuitos a nivel funcional de la organización. Que también resulta imprescindible adoptar un marco adecuado para el proceso de la transformación digital que vincule a las personas. Marco que implica la adquisición de capacidades digitales adecuadas, sistemas de información interconectados e interoperables, la vinculación de tecnología disruptiva e integrable, además de una financiación que habrá de ser sostenida en el tiempo. Solo entonces se podrá desarrollar una planificación clara de cuáles son las posibilidades de la transformación digital y una visión acertada de cómo y dónde verdaderamente puede ayudar la tecnología.

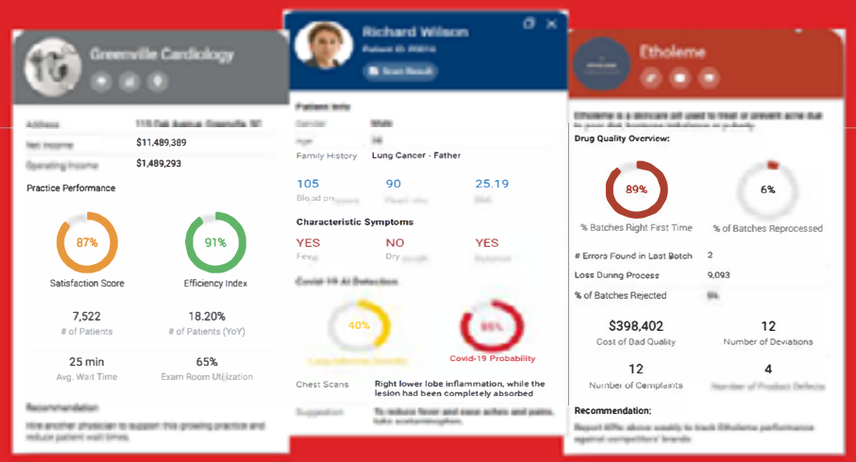
La Transformación Digital supone así, un paso fundamental para alcanzar una atención alineada con la ola de cambio tecnológico y científico que avanza vertiginosamente y que trae implícito un nuevo modelo de atención en salud. Con una mayor cobertura, atención de predominio virtual, el enfoque predictivo, alta capacidad diagnóstica ligada a un abordaje terapéutico en el marco de la medicina 5P, que serán, en definitiva, aspectos a tener en cuenta para que se contribuya de un modo realista y activo a mejorar la salud de las personas. ■

MAURICIO VALBUENA

Mauricio Valbuena es médico con Postgrado Ejecutivo en Transformación Digital por IEBS y en Inteligencia Artificial en Salud por la Universidad de Standford.
Actualmente, es responsable de innovación dentro de la Dirección de Proyectos y Mejora Continua de los hospitales del T2 Públicos BCN-Vallés Quiron Salud.

HYPERINTELLIGENCE®

Las respuestas le encontrarán



MicroStrategy

Intelligence Everywhere

eSalud, clave para la transformación del sector sanitario

JAVIER RODRÍGUEZ,
Senior Key Account Manager de Logitech

La situación de emergencia sanitaria que hemos vivido ha provocado un estado de metamorfosis continua y global, con una urgente necesidad de incluir nuevos modelos de trabajo, de comunicación, de relación o de acceso a servicios primarios, en cualquier momento y lugar.

Bajo estas premisas, la transformación digital se ha convertido en un objetivo inaplazable para cualquier organización y los centros de salud, hospitales y profesionales sanitarios no son ajenos a estos cambios. Y es que, durante la pandemia se han habilitado toda una serie de recursos y herramientas tecnológicas, así como servicios digitales para abordar la transformación digital del sector sanitario de forma acelerada, habilitando las reuniones entre equipos y centros, la discusión de diagnósticos, formaciones o convenciones. Todo ello, no solo internamente entre comunidad médica sino también con pacientes, incorporando la telemedicina para seguimientos, terapias o atención primaria, entre otros usos.

Actualmente estamos en la línea de salida del cambio en el ecosistema de salud que sitúe más cerca de la prevención de enfermedades, que sea más proactivo y que, al final, mejore la calidad de vida de los pacientes, facilitando su acceso y contacto con el sistema sanitario, y asegurando una intervención inmediata, en caso necesario, así como la desaturación de los centros de salud convencionales.

Las tecnologías para el sector salud suponen, además, la aportación de un valor añadido respecto a la cualificación de los sanitarios en el ámbito digital, una inversión a futuro que posiciona España como país referente. Según confirmamos en septiembre del año pasado en un análisis global realizado junto a Scalent sobre la opinión que merecía la atención sanitaria mediante vídeo, la mayoría de sanitarios exponían su preocupación por esta tendencia digital, pues solicitaban tecnologías intuitivas, conexión estable, aparatos de uso sencillo y con calidad de imagen y sonido comparable a lo que podría ser esa misma consulta si se realizara de forma presencial.

Entre 2020 y 2021, equipamos más de 700 centros sanitarios de la capital con sistemas de video colaboración de última generación y liderамos el proceso de digitalización de hasta 100 salas del Hospital Clínic de Barcelona con el fin de facilitar el trabajo colaborativo y el creciente servicio de telesalud al que ya se adscriben más del 57% de los pacientes en todo el mundo. En esta línea, también hemos llevado a cabo un proyecto de eConsulta para dermatología que permite captar imagen y vídeo de las lesiones de los pacientes en alta resolución desde los servicios de atención primaria para, posteriormente, compartir esos recursos gráficos con un especialista. Agilizando, de este modo, la derivación al especialista si éste lo considera oportuno.

Cada avance y cada proyecto que iniciamos comparten siempre un objetivo inamovible, que es el de proveer la mayor cantidad posible de facilidades a las personas para minimizar cualquier

obstáculo existente. Por eso, la digitalización en el sector sanitario debería dividir sus esfuerzos en cuatro ámbitos de igual relevancia: mejorar la calidad de vida de la sociedad, cuidar la experiencia del paciente, motivar la formación de los profesionales sanitarios en cuanto a lo digital y aumentar la eficiencia de los sistemas a través de su modernización.

En este sentido, la tecnología se ha posicionado como aliada indiscutible en el proceso. Propiciar la autonomía de los pacientes al implicarse en la gestión activa de su estado de salud, facilitar el acceso a historiales y datos médicos desde cualquier dispositivo, aumentar la rapidez y disponibilidad para las citas, agilizar los trámites administrativos, medir datos o celebrar formaciones y debates online son solo algunos de los servicios que ofrece la video colaboración.

Para ello es prioritaria la transformación del sistema sanitario, de forma progresiva, segura y efectiva, para habilitar experiencias personalizadas que contribuyan a la mejora de la salud de toda la población, con las innovadoras tecnologías de telemedicina que tenemos a nuestra disposición tanto para modernizar la relación médico-paciente como los métodos de comunicación entre centros o profesionales sanitarios. Es decir, una transformación a través de la tecnología que permita derribar fronteras y abrir puentes en la relación médico-paciente. ■

JAVIER RODRÍGUEZ, SENIOR KEY ACCOUNT MANAGER DE LOGITECH

Nuevos modelos de asistencia sanitaria

La pandemia ha transformado todos los sectores, incluido el sanitario, implicando la irrupción de nuevos modelos de asistencia sanitaria, entre los que destacan los entornos colaborativos y la telemedicina como tecnología emergente.

Según McKinsey, la utilización de la telesalud a diciembre de 2021 era 38 veces mayor que justo antes de la pandemia. Javier Rodríguez, Senior Key Account Manager de Logitech, cree que ha supuesto una aceleración de todos los procesos y ha provocado la creación de nuevos modelos de asistencia sanitaria remota, debido a los confinamientos y a la necesidad de evitar contagios. A pesar de ello, aún hay margen de mejora en cuanto a la calidad y la experiencia que se le ofrece al paciente. Estas soluciones deben contar con tres requisitos básicos: seguridad, integración y facilidad de uso.

Las soluciones Logitech se utilizan en todo tipo de áreas en el sector sanitario, desde la comunicación interna de los equipos de trabajo a la atención a distancia del paciente para tener nuevas vías de interacción. La compañía ofrece soluciones de audio, video y control que funcionan en cualquier plataforma de videocolaboración en la nube y ofrecen una buena experiencia tanto en el puesto de trabajo del personal médico como en las salas de reunión.

La sanidad y el mundo del dato

FERNANDO GUTIÉRREZ,
Account Executive de MicroStrategy

Hoy en día, la información es un activo fundamental de las empresas y la sanidad no es una excepción.

La sanidad maneja uno de los "productos" más preciados por todos, la salud.

El objetivo principal del sistema sanitario es mejorar la salud y por tanto la calidad de vida de la población. Existen también otros objetivos como facilitar el acceso a los servicios de salud, mejorar la calidad y satisfacción del ciudadano, incrementar la eficiencia y efectividad de la infraestructura hospitalaria/centros y un incremento eficiente de los presupuestos.

Como sucede en otras industrias, ese deseo de incremento en diferentes aspectos necesita de nuevas vías más allá de las vías tradicionales. El uso del dato junto con nuevas tecnologías puede permitir al sistema sanitario alcanzar los objetivos anteriormente mencionados.

Una mejora en la gestión del dato del paciente, de los centros de atención y de los procesos tiene una repercusión y un beneficio directo en la salud del ciudadano.

Por tanto, el dato se convierte en un activo fundamental que debe ser utilizado para la obtención de información y aportar ese valor diferencial al ciudadano.

No se trata exclusivamente de ver la información histórica del paciente en el momento de acudir a la consulta y ser reactivo, se trata de ser proactivo para obtener una sanidad preventiva. Las capacidades de inteligencia artificial y machine learning en la sanidad nos permiten poder ofertar una sanidad preventiva que evite problemas mayores en la salud de los pacientes, que permitan una mejor planificación y utilización de los recursos.

Otro de los aspectos que hacen que el dato sea crítico en el sistema sanitario, es el aspecto económico. Un análisis de la actividad operacional del sistema sanitario permitirá un incremento de la eficacia y de la eficiencia de los procesos, lo cual repercutirá directamente en un uso eficiente del presupuesto e indirectamente en la satisfacción del ciudadano al percibir una mejora en la calidad de los procesos, disponer de los medios necesarios y una organización más eficiente.

En los periodos de estrés se pone a prueba todo; los sistemas, los protocolos… se ve de manera clara que cosas son realmente necesarias, que cosas funcionan y que áreas son susceptibles de mejora.

Es por eso que el sistema sanitario se encuentra como muchas empresas y sectores en un proceso de transformación digital, muy encaminado a la calidad del dato y al gobierno del dato, pero también en la analítica y explotación del dato para la obtención de información.

Se podrían mencionar 3 áreas de mejora en lo que al mundo del dato respecta:

1. Uno de los objetivos que se busca con el gobierno y la calidad del dato es tener una visión del paciente 360º, necesidad incrementada con la incorporación de nuevos canales como la teleasistencia.

2. Incorporación de inteligencia artificial y machine learning para una sanidad preventiva y mejora de la operativa de los sistemas sanitarios.

3. Un área donde hay claro margen de mejora es en como facilitar el acceso a la informa-

ción para todo el personal involucrado en la operativa de un hospital o centro; ya personal sanitario, como personal de mantenimiento encargado de la gestión de las maquinas... para ayudarles en la toma de decisiones.

Hoy en día la gran mayoría de decisiones que se toman no van sustentadas en el dato. Existen 3 motivos principales, el dato se encuentra demasiado disperso y no hay tiempo, el segundo motivo es la falta de conocimiento en como acceder a todos esos sistemas y el tercer motivo es utilizar la experiencia

Es por tanto que el acceso a la información debe ser sencillo, rápido, intuitivo y multicanal. De esta manera se asegura que todo el personal dispone esté donde esté de la información relevante para la toma de decisiones. Como sucede en el resto de sectores, la sanidad no podría ser diferente, la tendencia actual es la de convertirse en un sector Data Driven con el menor coste y tiempo posible, es por ello que muchas compañías líderes han recurrido a HyperIntelligence como solución. ■

FERNANDO GUTIÉRREZ, ACCOUNT EXECUTIVE DE MICROSTRATEGY

El dato, fundamental en el sector sanitario

La situación pandémica ha implicado un nuevo modelo de la gestión del dato, tanto en su análisis como en su tratamiento, fundamentalmente dada la sensibilidad de muchos de ellos en un entorno tan específico como el sanitario.

El concepto data driven es completamente aplicable al sector sanitario. Para Fernando Gutiérrez, Account Executive de MicroStrategy, el poder disponer de datos para poder tomar decisiones y mejorar los tiempos de respuesta tiene un impacto en la sociedad brutal. El dato es fundamental para la salud del paciente, tanto en aspectos directamente relacionados con él, como en la gestión y la operación de los centros, que al final también recae en su bienestar. Además, la correcta gestión del dato ayuda a la medicina preventiva.

El objetivo de MicroStrategy es llevar de manera rápida y sencilla esa información recopilada a cualquier persona que en su trabajo requiera tomar una decisión y que pueda resultarle útil, pero de forma completamente segura. También trabaja en proyectos 360 y apuesta por una hiperpersonalización de la teleasistencia, ofreciendo una visión global de cada caso a través del dato. Además, tecnologías como la inteligencia artificial o el machine learning sirven para intentar detectar y ser proactivo ante posibles enfermedades.

El sector sanitario, protección crítica de sus datos

PEDRO DAVID MARCO,
CEO y Fundador de Iberlayer

El sector sanitario ha estado sometido a grandes tensiones durante los últimos dos años. Por las consecuencias de la pandemia de COVID 19, clínicas, centros de atención primaria, hospitales, farmacias y laboratorios farmacéuticos están jugando un papel crítico, y a esta presión se suma el hecho de que este sector, se ha convertido en un objetivo prioritario para los ciberdelincuentes.

La criticidad de los datos que manejan: hospitales y clínicas, con los registros médicos de cada paciente, y laboratorios farmacéuticos, con la documentación confidencial sobre vacunas o medicamentos; o la importancia de asegurar -en todo momento- la disponibilidad de los sistemas de información y la conexión ininterrumpida de los diferentes dispositivos y máquinas de salud, han actuado en su contra.

EL CORREO ELECTRÓNICO EN EL PUNTO DE MIRA

A esta situación se ha unido también el hecho de que el correo electrónico, uno de los servicios más antiguos de Internet y, en el caso del sector sanitario, herramienta crítica de los sistemas de información, se ha convertido en un arma de ataque para los ciberdelincuentes.

Cada vez más, entre todos los correos legítimos que circulan por Internet, se da un mayor número de mensajes SPAM, de correos con virus, troyanos, ransomware o de tipo phishing, en un intento por conseguir información sensible de carácter personal para realizar suplantación de identidad. Esta forma de comunicación no solicitada e ilícita está provocando serios problemas a las organizaciones y usuarios en cuanto a su seguridad y al consumo de recursos informáticos y ancho de banda de comunicaciones.

Las estadísticas de los tres últimos meses en el sector sanitario, al que Iberlayer proporciona su servicio de seguridad y anti-fraude para el correo electrónico en algunas compañías, muestran que en torno al 60% de los correos recibidos son SPAM. Aún más peligroso y preocupante es el hecho de que un 10% son campañas de phishing (en todas sus variantes, incluyendo intentos de fraude) mientras que otro 10% son correos con adjuntos con virus (que descargan ransomware en su mayoría).

El ransomware es un tipo de malware por el que un ciberdelincuente se lucra económicamente extorsionando a compañías a las que amenaza básicamente de dos modos posibles:

1. Cifrando todos sus datos y pidiendo un dinero de “rescate” a cambio de la clave de descifrado

2. Sacando fuera de la compañía enormes cantidades de datos internos y amenazando con hacerlos públicos si no se paga un “rescate”. A menudo, esta modalidad va acompañada de avisos a los propietarios de esos datos: pacientes, clientes, proveedores a los que se advierte que, de no efectuarse el pago, sus datos se harán públicos.

A este respecto aclarar que, en contra de lo que pueda parecer, no existe ninguna ga-

rantía de que, una vez ejecutado el pago, los datos perdidos sean recuperados o sigan permaneciendo secretos.

El sector sanitario es, por desgracia, uno de los objetivos del ransomware, y el correo electrónico es, sin lugar a dudas, el principal vector de entrada al ser los usuarios el eslabón de más débil de la cadena y el más fácil de engañar.

Otra de las amenazas más graves para el sector sanitario es el llamado Fraude del CEO, el cual es un tipo de engaño (y un posible delito a nivel legal) donde los cibercriminales crean cuentas de correo o dominios fraudulentos para hacerse pasar por ejecutivos de la organización, normalmente directores generales, o consejeros delegados, entre otros altos ejecutivos.

El fin último es intentar engañar a un empleado -con poderes para transferir dinero- para que lleve a cabo transferencias bancarias urgentes. Estos correos electrónicos no contienen malware malicioso, ni URL sospechosas; están completamente limpios desde el punto de vista de la seguridad. Por ello, es necesario utilizar una tecnología y un conocimiento especial de las técnicas empleadas por los ciberdelincuentes, para detectarlos y bloquearlos. Asimismo, es preciso poner una capa por encima de esta tecnología con un servicio de aviso personalizado, utilizando canales (para alertar a las posibles víctimas) distintos al del propio correo electrónico. ■

PEDRO DAVID MARCO, CEO DE IBERLAYER

Seguridad para el correo electrónico como servicio

La pandemia del coronavirus ha supuesto un verdadero reto para el sistema sanitario español, pero no solo a pie de campo, sino que sus sistemas informáticos también han visto cómo se han multiplicado los ciberataques amenazando la seguridad de datos muy sensibles, sobre todo a través del correo electrónico.

La forma más fácil de llegar al corazón de las empresas son los usuarios. Dado que la manera más directa de impactar al usuario es mediante el correo electrónico, se ha convertido en uno de los principales vectores de ataque. Pedro David Marco, CEO de Iberlayer, señala que no muchos directivos son conscientes del daño que le puede ocasionar a su compañía un ciberataque, sobre todo en sectores como el sanitario que no cuentan con departamentos específicos dedicados a ello.

Por esta razón Iberlayer ofrece la seguridad del correo como un servicio, lo que permite al cliente abstraerse de esa capa y tener la mayor protección que existe en el mercado sin necesidad de contar con especialistas in house. Además, sus soluciones de seguridad para el correo electrónico realizan un cifrado por defecto, de tal manera que todo el tráfico del cliente pasa a estar protegido.

El sector sanitario tiene graves problemas para detener el ransomware.

El 65% de los ciberataques consiguieron cifrar datos

Sophos Managed Threat Response

Tome medidas contra las ciberamenazas
Un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

www.sophos.com/es-es/

SOPHOS
Cybersecurity delivered.

Los atacantes tienen una mayor tasa de éxito en el cifrado de datos sanitarios

JAVIER DONOSO,
Sales Engineer, Sophos

Según El estado del ransomware en la sanidad 2021 de Sophos, entre las organizaciones sanitarias afectadas por el ransomware, el 65% afirmó que sus datos estaban cifrados, en comparación con la media intersectorial del 54%. A nivel mundial, el 39% de las organizaciones fueron capaces de detener el ataque antes de que se cifraran los datos, pero sólo el 28% en el sector sanitario. Esta menor capacidad para detener un ataque puede ser un reflejo de los retos financieros y de recursos a los que se enfrenta el sector sanitario, en parte debido a la reticencia a desviar fondos a la ciberseguridad que podrían utilizarse para la atención de primera línea a los pacientes.

Para que los organismos sanitarios ganen terreno a las nuevas y evolucionadas ciberamenazas, deben seguir ciertas estrategias clave de seguridad para protegerse:

1. Adoptar el modelo de seguridad de confianza cero o Zero Trust. Un informe, 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 elimina la oportunidad de que los atacantes y los usuarios deshonestos realicen acciones malintencionadas y obtengan acceso a información personal confidencial de salud mientras permanecen fuera de todas sospecha.

2. Mejorar la ciberseguridad contra los ataques de ransomware. Más de un tercio de las organizaciones sanitarias (34%) fueron atacadas por ransomware el año pasado. Podemos afirmar, que el ransomware es un arma devastadora en manos de los ciberdelincuentes que tienen como objetivo el sector sanitario.

Estos ataques han detenido operaciones sanitarias, han paralizado los dispositivos y sistemas médicos conectados y han cifrado los registros para que el personal sanitario no pueda acceder a ellos. Sophos ofrece una seguridad líder en ransomware con Intercept X Advanced with XDR, la única solución XDR del sector que sincroniza la protección nativa de endpoints, servidores, firewalls, correo electrónico, infraestructura en la nube y M365.

3. Superar la escasez de mano de obra cualificada. La falta de personal con los conocimientos y la experiencia adecuados en materia de ciberseguridad es uno de los principales desafíos para los proveedores de servicios de salud.

Para las organizaciones sanitarias que carecen de recursos en ciberseguridad, Sophos ofrece el servicio de Managed Threat Response (MTR). Este servicio brinda una supervisión eficaz y una evaluación continua de los riesgos gracias al equipo de expertos dedicado las 24 horas del día, los 7 días de la semana. Nuestra solución va más allá de las simples alertas, ya que proporciona una respuesta contra las amenazas, asegurando que el riesgo se identifica, se contiene.

4. Cubrir los puntos ciegos en sus esfuerzos de transformación digital. Las transacciones de información entre los pacientes, los cuidadores, las agencias de seguros y otras partes interesadas deben ser fluidas y seguras. Las redes SD-WAN, con su arquitectura flexible, ha surgido como una muy buena alternativa entre las organizaciones de salud para cumplir con estos requisitos.

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 Sophos Firewall y SD-RED, hace posible conseguir una conectividad SD-WAN en línea con sus objetivos de seguridad y continuidad.

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.

Es importante tener una cultura de ciberseguridad adecuada para ayudar a reducir la alta susceptibilidad de la sanidad a una amplia gama de sofisticados ciberataques.

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

ÁLVARO FERNÁNDEZ, ENTERPRISE ACCOUNT EXECUTIVE DE SOPHOS

Prevención, detección y respuesta

En los últimos dos años los ciberataques hacia el entorno sanitario se han visto multiplicados como consecuencia de la pandemia, con infraestructuras, accesos y datos como principales objetivos. El ransomware es el más notorio, pero detrás de esos ataques hay mucho más.

Muchas veces se entiende el ransomware como un ataque aislado, pero realmente se trata de la última fase de un ataque, antes de aflorar han pasado muchas otras cosas. Como explica Álvaro Fernández, Enterprise Account Executive de Sophos, una vez dentro el atacante va a intentar pasar inadvertido y filtrar información, lo que supone un gran riesgo para un sector como el sanitario, y será después cuando preparará el entorno eliminando las copias de seguridad existentes para poder liberar el ransomware sin problemas y salir a la luz.

Para hacer frente a estos problemas es necesario contar con un plan de respuesta ante este tipo de incidentes. Sophos Rapid response es un servicio específicamente diseñado para este tipo de eventos que cuenta con una fase de neutralización del atacante y otra de monitorización para solucionar cualquier tipo de incidente. La seguridad del entorno sanitario se debe basar en 3 claves: prevención, detección y respuesta.

El impacto de TLStorm

en la seguridad de las organizaciones médicas y sanitarias

OSCAR MIRANDA,
CTO for Healthcare, Armis

TLStorm son un grupo de tres vulnerabilidades críticas, descubiertas por Armis, que afectan a los Smart-UPS de APC. Dos de ellas son vulnerabilidades de ejecución remota de código (RCE) en el código que maneja la conexión a la nube, lo que hace que estas vulnerabilidades sean explotables a través de Internet. La tercera vulnerabilidad es un fallo de diseño, en el que las actualizaciones de firmware de la mayoría de los dispositivos Smart-UPS no están correctamente firmadas o validadas, lo que permite a un atacante cargar firmware malicioso de forma remota y sin validación. Un ataque a estos dispositivos podría llegar a traer consecuencias catastróficas, ya que los Smart-UPS de APC se encuentran en infraestructuras críticas como hospitales, centros de datos e instalaciones industriales.

Estas tres vulnerabilidades de día cero, acuñadas como TLStorm, exponen a más de 20 millones de dispositivos en todo el mundo y podrían permitir a atacantes eludir las funciones de seguridad y controlar o dañar remotamente dispositivos médicos, industriales y enterprise críticos para el funcionamiento de cualquier organización. Datos obtenidos por el equipo de investigadores de Armis, muestran que 8 de cada 10 organizaciones podrían ser vulnerables a TLStorm.

En el sector de la sanidad, esta amenaza pone de manifiesto los riesgos que entrañan los dispositivos médicos conectados y la importancia de la seguridad de los mismos. Con activos como los dispositivos SAI convirtiéndose en un objetivo para los actores maliciosos, es más importante que nunca tener una visibilidad completa de todos los dispositivos conectados a la red, junto con la capacidad de supervisar su comportamiento e identificar los intentos de explotación de cualquier fallo de seguridad, como TLStorm.

Alrededor del 91% de los clientes de Armis del sector sanitario y médico de todo el mundo utilizan algún tipo de SAI, y de ellos el 76% tienen modelos de SAI identificados como vulnerables a TLStorm. Los clientes de la compañía pueden ver inmediatamente los dispositivos vulnerables y parchearlos, pero el alto número de posibles afectados destaca los riesgos potenciales para aquellos que no pueden hacerlo.

El ecosistema de dispositivos en empresas sanitarias va más allá de los dispositivos médicos. Los SAI se utilizan no sólo en los centros de datos sino dentro de los hospitales y clínicas, por lo que un ataque podría afectar significativamente los cuidados y el trato con los pacientes. En resumen, cualquier evento de seguridad que afecte a los dispositivos médicos conectados puede causar una interrupción considerable en la prestación de servicios sanitarios y afectar a la seguridad de los pacientes.

Los hospitales deben identificar qué dispositivos ayudan al flujo de trabajo clínico, aparte de los dispositivos médicos clásicos, y cuáles están conectados a sistemas SAI vulnerables. Solo a través de la identificación y monitoreo continuo de los dispositivos un hospital puede mitigar o remediar el riesgo creado por estos sistemas SAI rápidamente.

Aunque las ventajas de las nuevas tecnologías son evidentes, cada dispositivo médico conecta-

do crea un nuevo objetivo para los malos actores y debe utilizarse en un entorno seguro, con supervisión continua de su actividad.

El descubrimiento de las vulnerabilidades TLStorm subraya la importancia de tener un inventario de dispositivos en entornos como el médico, y de controlar la actividad de todos aquellos dispositivos responsables de mantener la energía y las operaciones críticas en funcionamiento. El uso de dispositivos médicos conectados supone una gran oportunidad para mejorar la atención al paciente en centros hospitalarios y sanitarios, pero los profesionales de la salud deben entender que también crea oportunidades de entrada para actores maliciosos.

Contar con un plan de ciberseguridad para los dispositivos médicos, es fundamental para cualquier organización que utilice el Internet de las cosas médicas, o IoMT. La Agencia de Ciberseguridad de la Unión Europea (ENISA) y la FDA ofrecen directrices para ayudar a los equipos informáticos (TI) a gestionar la seguridad de los dispositivos médicos. Ambas son un buen punto de partida para garantizar la seguridad del IoMT.

La visibilidad es fundamental para que las organizaciones sanitarias se aseguren de que todos los dispositivos están supervisados y protegidos. En la realidad hiperconectada en la que vivimos, tener visibilidad completa y a tiempo real garantiza una protección holística. ■

VESKU TURTIA, REGIONAL DIRECTOR ESPAÑA Y PORTUGAL DE ARMIS

Monitorización continua sin agentes y de forma pasiva

La situación de pandemia vivida en los últimos años ha implicado un nuevo paradigma para sectores como el sanitario, así como la aceleración de nuevos modelos tecnológicos, donde el componente de la ciberseguridad de los diferentes assets juega un papel muy importante.

La aceleración de la digitalización en el sector sanitario es un hecho desde el inicio de la pandemia, lo que ha implicado ciertos retos para los players del sector. Para Vesku Turtia, Regional Director España y Portugal de Armis, el principal reto es que las empresas logren entender qué es todo lo que tienen integrado en su red, para poder hacer políticas de ciberseguridad y proteger los assets de cada centro hospitalario. Además, es muy importante hacer una monitorización continua, sin agentes y de una forma pasiva, para no interferir en posibles procesos hospitalarios importantes.

Armis ha traído al mercado una plataforma que engloba precisamente todas estas cuestiones: inventario, visibilidad, monitorización continua, sin agentes y de forma pasiva, que se integra de forma perfecta con los sistemas del cliente. Además, cuentan con una base de datos en la nube de más de 2 billones de dispositivos distintos perfilados en 20 millones de perfiles, que permite compartir información para estar a la última en protección.

El riesgo de las infraestructuras sanitarias frente a diversos vectores de ataque

BORJA PÉREZ,
Country Manager
Stormshield Iberia

Cada vez más digital e interconectado, el sector sanitario, con los hospitales al frente, lleva tiempo siendo objetivo de ciberataques. La sensibilidad que encierra, lo han convertido en un blanco codiciado para los ciberdelincuentes, quienes lanzan sus amenazas contra estas entidades. No en vano, el sanitario fue, según la Agencia de la Unión Europea para la Ciberseguridad, ENISA, el cuarto sector más atacado durante 2020, registrando 143 incidentes , lo que supone un 47% más que el año anterior. Se trata por tanto de un sector expuesto en el que, además, y a diferencia de lo que ocurría en el pasado, no se enfrenta a un factor de riesgo uniforme, sino que los peligros, cada vez más, proceden de diferentes vectores: redes, software, físicos y humanos.

EN EL CORAZÓN DEL SISTEMA

El rendimiento y la disponibilidad de las redes informáticas de los sistemas de salud son muy importantes, dado que la vida de los pacientes a menudo depende de la información que permiten intercambiar.

Por tanto, salvaguardar esa información confidencial y vital es un tema prioritario, igual que garantizar la disponibilidad de los servicios. La salud vive al ritmo de las emergencias. Por lo tanto, requiere una reacción rápida en caso de incidente, en relación con equipos biomédicos, Gestión Técnica de Edificios (BMS) o Gestión Técnica Centralizada (CTM) del hospital. Estas intervenciones se pueden facilitar proporcionando acceso remoto seguro a técnicos o proveedores externos a través de VPN nómadas, SSL o IPSec y autenticando a los usuarios a través de flujos de red. Dos medidas que también son útiles para fortalecer el mantenimiento a distancia y el desarrollo de la telemedicina.

UN ATAQUE CONTRA EL CEREBRO

Los programas informáticos prestan innumerables servicios en los hospitales, tanto para la gestión interna como externa de la organización. Sin embargo, por su propia naturaleza, también pueden presentar puntos débiles, como lagunas o una obsolescencia, que pueden ser aprovechados por los ciberdelincuentes para acceder a los equipos médicos, informáticos o, incluso a los datos de los pacientes o a las instalaciones sensibles.

Para prevenir los ciberataques de software, es esencial la concienciación de los equipos humanos, así como el cumplimiento de las mejores prácticas en este ámbito: limitar el acceso a la red de las aplicaciones al mínimo, realizar una auditoría del sistema, endurecer las configuraciones y realizar copias de seguridad sin conexión.

TRABAJANDO SOBRE EL TERRENO

Lejos del cliché del ciberdelincuente, aislado tras su pantalla a kilómetros de su víctima, algunos se acercan lo más posible a su objetivo. Su técnica consiste en atacar directamente los equipos hospitalarios, ya sean informáticos, médicos u operativos, y explotar sus vulnerabilidades. Para ello el ciberdelincuente accede físicamente al equipo en cuestión, y se conecta a él para interrumpir su funcionamiento. Tras ello, su impacto puede ser múltiple, desde el sabotaje de la máquina hasta la

alteración -o incluso el robo- de datos sanitarios.

Para protegerse de estos ataques, es necesario salvaguardar las máquinas, como las estaciones de trabajo. Por lo tanto, se recomienda el control de acceso, la gestión de los dispositivos externos e incluso el análisis del comportamiento. Esto puede lograrse con la creación de estaciones blancas que actúan como una descontaminación de llaves USB. Como último recurso, la segmentación de la red para limitar la propagación de la infección, en caso de que esta se produjera.

RIESGO HUMANO, PRINCIPAL PREOCUPACIÓN

Además de los riesgos tecnológicos es importante tener en cuenta los asociados al ser humano, sobre todo con el uso todavía muy extendido de las memorias USB en entornos TI y OT. Por ello, es importante endurecer los puestos de control y supervisión mediante el establecimiento de soluciones de listas blancas o de análisis de dispositivos de almacenamiento, para rechazar cualquier uso de un perfil no autorizado, pero también concienciar a los trabajadores sanitarios de todos los riesgos cibernéticos para evitar cualquier error o acción involuntaria que pueda poner en peligro los datos o la infraestructura.

Adicionalmente, y además de trabajar en esta concienciación, dado que los ataques son cada vez más dirigidos y sofisticados, es fundamental ofrecer soluciones que no dependan del conocimiento que el usuario pueda tener en ciberseguridad. ■

BORJA PÉREZ, COUNTRY MANAGER DE STORMSHIELD

El cifrado de datos, imprescindible

La seguridad del sector sanitario se ha cuestionado a raíz de la pandemia, dado que se ha convertido en uno de los entornos más amenazados por los ciberdelincuentes.

El intercambio de datos sensibles entre distintas áreas del sistema sanitario, como laboratorios, hospitales, clínicas, es continuo, pero no está debidamente securizado. Así lo pone de manifiesto Borja Pérez, Country Manager de Stormshield, señalando que los datos no se están almacenando adecuadamente y el intercambio muchas veces no se hace con las medidas de seguridad suficientes. A pesar de ello, en su opinión los CISOs son conscientes del problema, pero les faltan recursos.

Para Stormshield es fundamental tener todos los datos cifrados y salvaguardados de manera segura, de manera que si se produce una filtración de datos, no se pueda sacar ninguna información útil de esos documentos filtrados. La compañía basa su propuesta en tres principios:

Securización de los datos mediante cifrado de documentos y correo, protección del puesto de trabajo; y segmentación de las redes y securización de cada uno de los servicios que se estén dando en el entorno sanitario.

STORMSHIELD

La opción europea en ciberseguridad

Su socio de confianza para proteger **infraestructuras hospitalarias**

www.stormshield.com

Visibilidad, clave de la seguridad en el entorno sanitario

En el sector sanitario, Armis permite a las organizaciones utilizar la visibilidad en su ecosistema de dispositivos médicos e informáticos, para identificar, evaluar y asegurarse ante riesgos cibernéticos, a la vez que realizar mejoras operativas significativas.

Esta aproximación ofrece un valor clínico y un valor operacional. En el caso del primero, destaca el manejo y seguimiento de inventario; identificar y localizar dispositivos médicos no conectados a la red; alertar sobre dispositivos médicos que abandonen el recinto hospitalario y monitorización del comportamiento de dispositivos en busca de indicadores de mal funcionamiento. Asimismo, sobresale la utilización dirigida hacia la eficacia clínica (tiempos de espera y satisfacción del paciente); mejorar la monitorización de dispositivos de alto valor para controlar tiempos de inactividad y problemas operacionales; identificar tiempos óptimos para el mantenimiento de los dispositivos y alertar de anomalías o usos incorrectos de dispositivos para el cuidado de pacientes. Por último, mejoras de seguridad y calidad, y realizar informes trimestrales con seguimiento de medidas de los órganos reguladores.

Desde el punto de vista operacional, destaca el coste de gestión; asistir a operaciones para realizar previsiones financieras; mostrar dispositivos perdidos para prevenir la compra excesiva; y ayudar a a tomar decisiones de compra informadas al adquirir inventario adicional. Igualmente, ahorro en contratos de mantenimiento, al mostrar datos de utilización y riesgo para optimizar los Acuerdos de Nivel de Servicio (SLA) y los contratos de mantenimiento relacionados con dispositivos médicos y sistema de gestión de edificios. Finalmente, integración con inversiones existentes en TI y Seguridad de la Información como ServiceNow, Biomed CMMS o CMDB, para una mayor visibilidad y precisión de los activos; realización de informes en tiempo real sobre los usos de li-

cencias; simplificación de la implementación de soluciones de Control de Acceso a Red (NAC) (Cisco ISE); aumento de las capacidades de otras soluciones y de administración de vulnerabilidades para dispositivos no gestionados y puntos ciegos de redes; mejora de la visibilidad y alerta en la Gestión de Información y Eventos de Seguridad (SIEM); e identificación de dispositivos perdidos durante proyectos de migración de tecnología – proyectos de migración de servidores y proyectos de renovación de infraestructuras inalámbricas.

CIBERSEGURIDAD Y CONTINUIDAD DE LAS OPERACIONES

Con la Auditoría y Cumplimiento de normativas se crean informes cuatrimestrales de requerimientos regulatorios; cuadros de mando dinámicos en tiempo real para identificar dispositivos que incumplen la normativa; fuentes de información absoluta para la identificación y orquestación de dispositivos; e identificación de riesgos de terceras partes relacionados con el comportamiento de los dispositivos.

Mientras, con la Protección de la Privacidad de los Clientes, se informa de transmisiones de Información de Salud Protegida (PHI) no encriptada a destinaciones internas o externas no autorizadas; se identifican cámaras IP transmitiendo en la red; se alerta de dispositivos afectados con potencial de grabar o impactar la privacidad del paciente; y se crean normativas de seguridad para prevenir la exfiltración de datos.

Por último, con las Políticas de Seguridad y control de Regulaciones (Análisis de Brechas de Seguridad), se crean informes para la identificación de dispositivos sin los controles de seguridad enterprise necesarios como: agentes de protección endpoint, parches/asset management agent (SCCM). Ayuda a fortalecer la seguridad y protección ante ciberataques; y se identifica y ayuda a la remediación de dispositivos personales (BYOD).

ARQUITECTURA DE SEGURIDAD Y OPERACIONES

Con las Operaciones de Seguridad de la Información, se mejora la detección y respuesta del SOC ante ciberataques y detección de ransomware (reduce el tiempo de inactividad del hospital); se aplican políticas de seguridad automáticas para contener y mitigar incidentes (menor tiempo de respuesta y resolución); y se alerta ante comportamientos anómalos como exfiltración de datos, comunicación con IPs internacionales, y conexiones de red no autorizadas.

Con la Gestión de vulnerabilidades y amenazas, se manejan las vulnerabilidades en dispositivos médicos; se realizan y expanden políticas de escaneo de vulnerabilidades para dispositivos nuevos y ya existentes; se asesora sobre riesgos en tiempo real y contextualiza, según tipo de dispositivos, función, comportamiento, y vulnerabilidades; se crean informes y monitorizan en tiempo real los intentos de explotación de vulnerabilidades de día cero en dispositivos médicos y Enterprise; y se crean cuadros de mando de seguimiento de los esfuerzos de remediación.

Por último, con la Capacidad de Respuesta de Incidentes Automatizada, se integra con mallas de ciberseguridad existentes para automatizar respuestas de seguridad; se identifican comportamientos malignos y ejecuta políticas estrictas de firewall para remediarlos; se integra con soluciones NAC para segmentar la red y poner en cuarentena dispositivos; y genera tickets de forma automática para alertas, investigación y seguimiento. ■

MÁS INFORMACIÓN

- Security Operational efficiency
- Securing the patient journey
- Medical device vulnerabilities

La protección de correo electrónico, clave en el sector sanitario

Iberlayer, como compañía centrada exclusivamente en la protección del correo electrónico desde la nube, ofrece una solución en la que han confiado compañías de casi toda Europa, Reino Unido, Estados Unidos y América Latina: Iberlayer Email Guardian.

El correo electrónico es la principal vía y puerta de entrada de aproximadamente 9 de cada 10 incidentes de ciberseguridad, porque el email es la forma más sencilla de llegar al interior de las compañías y a su eslabón más débil: el usuario final. Con solo un 8% del correo electrónico considerado como limpio, todo el resto es correo no deseado, incluyendo correos spam, scam, phishing, fraudes, estafas, y correos con malware, que además de consumir recursos corporativos, como ancho de banda, carga en sistemas, espacio en disco, entre otros, puede suponer un gran riesgo en la seguridad de las propias compañías hasta límites críticos.

Hoy día, las compañías se enfrentan a la necesidad de contar con cuatro elementos fundamentales para mantenerse protegidos:

- Tecnología con años de experiencia con un alto nivel de sofisticación, automatización, disponibilidad, y capacidad de detección de los algoritmos empleados en las campañas de correo no deseado.
- Personal experto en ciber-seguridad que esté constantemente actualizado y constan-

Al tratarse de un servicio y no de un producto, Email Guardian ofrece a las compañías una capa de seguridad completa con una fuerte protección frente a las amenazas que a diario se reciben por email

temente pendiente de todas las amenazas nuevas que a diario van apareciendo...

- Personal experto en el correo electrónico y en el uso y administración de las herramientas de filtrado de correo para su correcto funcionamiento, continuos ajustes y parametrizaciones...
- Personal que esté pendiente de los paneles de control, estado de los sistemas, logs, posibles alertas... y con el nivel de entrenamiento adecuado para distinguir cuando es necesario tomar medidas drásticas.

EMAIL GUARDIAN DE IBERLAYER

Al tratarse de un servicio y no de un producto, ofrece a las compañías una capa de seguridad completa con una fuerte protección frente a las amenazas que a diario se reciben por email y sin necesidad de gestionar todas las anteriores necesidades mencionadas. Como servicio completo de protección del correo electrónico desde la nube, impide que posibles amenazas a través de este vector, lleguen hasta los usuarios, protegiéndolos contra ransomware y malware de todo tipo, Spam, Scam, Phishing, Fraudes, Estafas, y un largo etcétera.

IBERLAYER DOMAIN GUARDIAN

Uno de los principales métodos utilizados para ataques de Phishing es la suplantación de identidad. Resulta sencillo y económico registrar un dominio similar al de la víctima para hacernos pasar por un alto cargo y realizar un fraude de CEO. En muchos casos se suplantan dominios de reconocidas marcas para que resulte mucho más creíble el origen del correo. De este modo, el usuario confía en el emisor y no sospecha de un posible ataque.

El sistema de vigilancia de dominios, incluido en el servicio Iberlayer Email Guardian, monitoriza la creación de nuevos dominios similares. De este modo, se puede anticipar a una posible suplantación de identidad permitiendo tomar las medidas necesarias en un tiempo mínimo.

El laboratorio de Iberlayer vigila, monitoriza, estudia y analiza constantemente la actividad mundial relativa al email, incluyendo un servicio de vigilancia de dominios, para, no solo bloquear todo tipo de amenazas, sino también tratar de adelantarse a ellas lo antes posible. Dada la inmediatez del peligro, a través de Domain Guardian, Iberlayer es capaz de monitorizar posibles abusos, avisando al cliente de manera directa, incluso vía telefónica en casos urgentes, de aquellas actividades sospechosas de posibles fraudes o ataques dirigidos. ■

MÁS INFORMACIÓN

Iberlayer

Email Guardian

Soluciones para una telesalud de calidad

Logitech está promoviendo la adopción y eficacia de la telesalud trabajando para crear una atención médica innovadora que mejore la calidad de vida y la interacción entre pacientes, proveedores y profesionales sanitarios. Logitech permite a las organizaciones de atención médica brindar atención de alta calidad independientemente de su ubicación a través de un conjunto de soluciones de videocolaboración fundamentales y fáciles de administrar.

A medida que la telesalud continúa transformándose e innovándose, Logitech busca desarrollar soluciones que se integren fácilmente en la sanidad con el objetivo de ofrecer experiencias excepcionales a todas las personas involucradas en los servicios sanitarios a través de atención vanguardista y centrada en el paciente.

Para los profesionales, sus pacientes y los equipos de TI, las soluciones de videocolaboración de Logitech proporcionan experiencias de telesalud de alta calidad para repensar las posibilidades y necesidades de todos ellos. Logitech ayuda a las organizaciones de atención médica de todo el mundo a brindar atención de alta calidad de forma remota, mejorando los resultados, reduciendo los costes y elevando la experiencia de atención sanitaria para todos los involucrados.

De cara al paciente, las soluciones de Logitech le conectan con su especialista médico al instante y le permiten evitar desplazamientos innecesarios, porque su examen y control se realizan en modo remoto, a través de vídeo y evitando cualquier riesgo de contagio potencial.

En el día a día de los profesionales sanitarios, estas soluciones modernizan las salas de reuniones, los despachos y demás ubicaciones de los diferentes equipos multidisciplinares (MDT). Asimismo, permiten equipar las salas de los centros favoreciendo la consulta entre el personal médico y potenciar la formación a distancia, habilitando a los médicos y enferme-

Para los profesionales, sus pacientes y los equipos de TI, las soluciones de videocolaboración de Logitech proporcionan experiencias de telesalud de alta calidad para repensar las posibilidades y necesidades de todos ellos

ras la observación de cirugías y procedimientos en remoto de otros hospitales o centros de investigación.

Herramientas como webcams, auriculares y otras soluciones profesionales para equipar el espacio de trabajo personal sanitario, como es el caso de Logitech Brio, una webcam que permite habilitar cualquier espacio en una sala de consulta remota para conectar al personal médico con los pacientes, y estos con sus familiares en casos de ingreso prolongado. La implementación de auriculares con micrófono como los Logitech Zone con cancelación de ruido con el objetivo de mejorar la experiencia de los pacientes y los médicos con un audio claro y de alta calidad. O, el uso de Logi dock para simplificar la organización del espacio de trabajo del especialista, reducir la acumulación de cosas en el escritorio y contribuir a su productividad.

Además de la apuesta por avanzadas soluciones de videocolaboración para consultas o salas de formación, como es el caso de Rally Bar, una barra de video todo en uno, que facilita el acercamiento de equipos que están en diferentes centros, con el fin de reducir el número de viajes para el seguimiento de los pacientes o la puesta en común de casos prácticos. Todo ello a partir de un sistema de doble cámara y tecnología de encuadre automático RightSight 2, que además permite elegir la vista para resaltar al orador activo, la vista de grupo para capturar a todos los presentes en la sala o combinar las dos vistas para una experiencia inmersiva y atractiva; y, Tap Scheduler, un panel de programación enfocado a gestionar de forma más eficiente los espacios de reunión. Esta solución se ha diseñado para facilitar su visualización y uso, con una instalación sencilla y una experiencia de usuario intuitiva que impulsan una rápida implantación y adopción.

En resumen, todo tipo de soluciones para impulsar la digitalización del sector sanitario, compatibles con todas las plataformas de vídeo en la nube del mercado, que permitan tender los puentes necesarios de cara a mantener unidos a todos los profesionales del ámbito sanitario y apostar por una nueva relación entre médico-paciente. ■

MÁS INFORMACIÓN

- El futuro de la atención virtual conectada
- Lecciones del COVID 19

ARMIS®

Fortalece la seguridad de tus pacientes obteniendo visibilidad completa de todos tus dispositivos

Armis ofrece visibilidad completa e información precisa sobre todos los dispositivos administrados y no autorizados de tu red.

Descubre nuestra solución en
www.armis.com/medical-device-security/

Soluciones para convertir a las sanitarias en compañías Data Driven

MicroStrategy es una empresa con foco en el sector analítico, siendo una arquitectura orientada a objetos su mayor diferenciador con el resto de soluciones analíticas, una arquitectura que le permite el gobierno de la información y ofrecer una visión única de la verdad a lo largo de la toda la compañía.

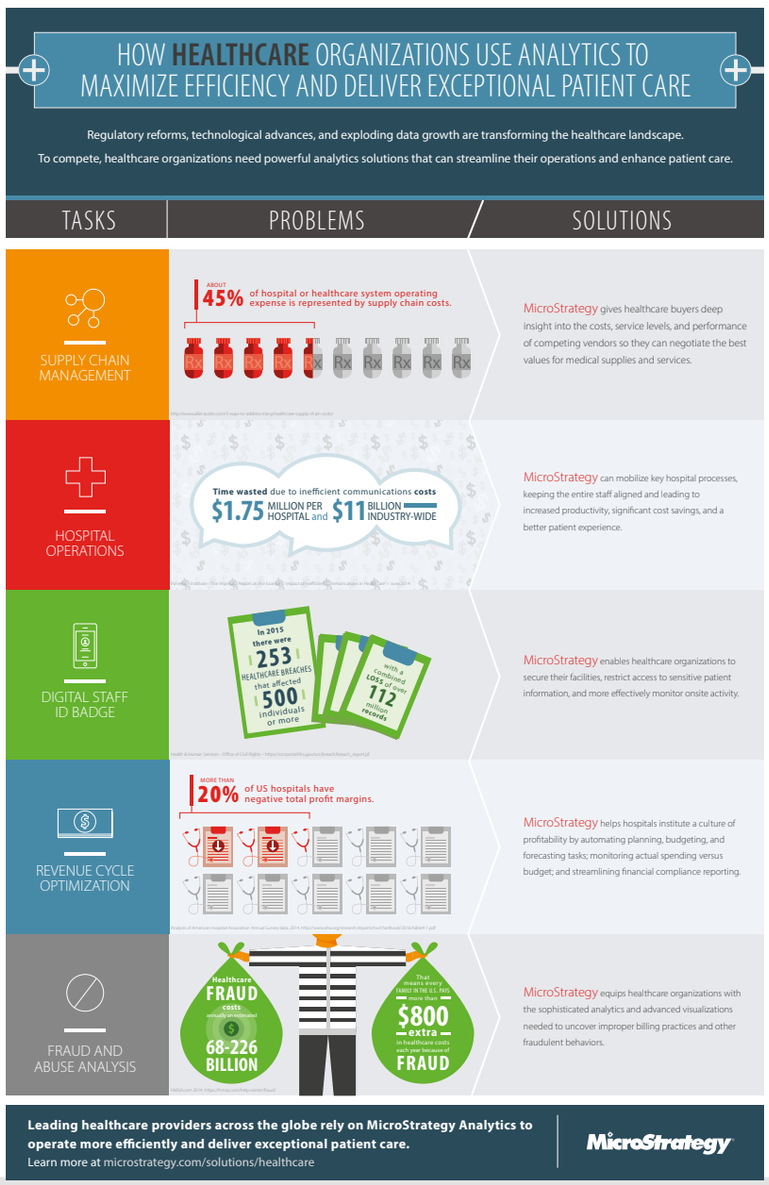
Se trata de una plataforma escalable, tanto en usuarios como en datos, que cubre cualquier caso de uso que planteen los consumidores de información sin necesidad de añadir más herramientas y por tanto pudiendo reaprovechar los desarrollos en cualquiera de los canales por los que el usuario consume la información, dando una sensación de omnicanalidad y reduciendo los costes de gestión.

Otro de los diferenciales principales de MicroStrategy es su dedicación plena a la analítica, esto hace que sea una empresa cercana con sus clientes, lo que le permite dar una atención y escucha diaria de las necesidades y tendencias. Es por eso que, desde hace unos años MicroStrategy ha trabajado en 3 áreas principalmente:

❖ **Área Corporativa.** Esto es, seguir trabajando en las capacidades para dar un servicio empresa-

rial, es decir, capacidades de gobierno del dato, de una visión única, de escalabilidad de datos y usuarios y de una seguridad centralizada.

❖ **Una arquitectura abierta.** MicroStrategy ha apificado prácticamente toda la plataforma, ha incluido un motor RestAPI para no solo poder consumir de cualquier sitio, si no para poder inyectar datos en cualquier sitio.



❖ **Modernizar la plataforma** para dar respuesta a esas necesidades de negocio modernas, como son autoservicio, pero un autoservicio gobernado, intuitivo y sin líneas de código. Dentro de la modernización, dispone de una tecnología que permite el acceso rápido, sencillo e intuitivo a la información, que se conoce con el nombre de HyperIntelligence.

Hyperintelligence es una tecnología que permite romper la brecha digital con los usuarios consumidores, y ayuda a acelerar el proceso de ser una compañía Data Driven.

El objetivo principal de Hyperintelligence es facilitar de manera rápida, sencilla e intuitiva la información a los usuarios con cero clics. Esto es, permite que los usuarios sin realizar clics con tan solo situarse sobre las palabras, conceptos de negocio que son importante para él, le abra una tarjeta que trae los datos relevantes de 1 o varias fuentes. De esta manera, la tarjeta permite consolidar los datos más importantes de múltiples sistemas, lo que acelera enormemente la productividad y permite que las decisiones estén apoyadas en los datos.

La otra gran característica de Hyperintelligence es su tiempo de despliegue, en tan solo unos días es posible tener las tarjetas disponibles, las cuales aparecerán sobre cualquier solución de mercado o aplicación desarrollada internamente que corra sobre navegador o móvil principalmente. ■

Hyperintelligence es una tecnología que permite romper la brecha digital con los usuarios consumidores, y ayuda a acelerar el proceso de ser una compañía Data Driven

MÁS INFORMACIÓN

- Healthcare Pharmaceuticals
- The Hyperintellicenge Pilot
- Health Solution Map
- Caso de éxito: Derbyshire NHS
- Caso de éxito: AllScripts
- HyperIntelligence

Seguridad Sophos para Sanidad

Sophos cuenta en su oferta tecnológica con soluciones de seguridad que aplican en el mundo de la Sanidad. Conozcamos algunas de ellas.

❖ **Sophos Intercept X EDR/XDR.** Es un sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti exploit, análisis de 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 sus firewalls, su servicio de correo, su UEM para la gestión de los dispositivos móviles y los 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 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 posibles amenazas 24/7. Formado por un equipo de detección de amenazas y profesionales expertos en investigaciones avanzadas dando respuesta a los ciberataques y tomando medidas para neutralizar incluso las amenazas más sofisticadas. Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y la mitigación de la amenaza. Cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response, que es capaz de realizar un despliegue rápido del producto y su equipo de expertos en ciberseguridad son capaces de ver cuál es la situación dentro de la compañía, detener el ataque y, si es posible, detectar por dónde ha venido, a quién ha afectado y limpiar todo lo que haya sido dañado para que pueda volver a la normalidad lo antes posible.

❖ **Sophos Firewall.** La seguridad de red desde la compra de Astaro en 2008 por Sophos ha seguido evolucionando hasta llegar a los nuevos Sophos Firewall, que son gestionados de forma centralizada desde Sophos Central, se integran con el Endpoint y con el servicio MTR. Además, son capaces de hidratar el lago de datos, englobándose dentro de su estrategia XDR. La arquitectura de Xstream de Sophos Firewall protege la red de las amenazas más recientes, al tiempo que acelera el tráfico importante de SaaS, SD-WAN y aplicaciones en la nube.

❖ **Sophos Zero Trust:** Sophos ZTNA se basa en los principios de Zero Trust: no confiar en nada y verificarlo todo. Los usuarios y dispositivos se convierten en su propio perímetro microsegmentado, con lo que se validan y verifican constantemente. Con Zero Trust,

los usuarios ya no se encuentran “en la red” con la confianza y el acceso implícito que habitualmente conlleva. Sophos ZTNA es la única solución Zero Trust Network Access que se integra perfectamente con un producto para endpoints next-gen: Sophos Intercept X.

❖ **Sophos Email.** Seguridad del correo electrónico más inteligente con IA. Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email, es decir, que combata las amenazas de hoy día sin perder de vista el mañana.

❖ **Sophos Cloud Optix.** Conscientes de que cada vez más la infraestructura de TI está migrando a la nube, Sophos lleva tiempo hablando de CSWP y CSPM gracias al agente para servidores y a Cloud Optix, el cual audita los recursos que se tengan sobre proveedores de nube pública como AWS, Azure o Google Cloud. Además, se integra con XDR y con servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el lago de datos. ■

MÁS INFORMACIÓN

- Ramsonware in Healthcare
- Adaptative Security
- Guía para la adquisición de servicios de detección

Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email

Seguridad de Stormshield para el sector sanitario

Stormshield cuenta con una serie de soluciones diseñadas para ayudar a las empresas del entorno sanitario a enfrentarse a los retos de ciberseguridad que tienen por delante.

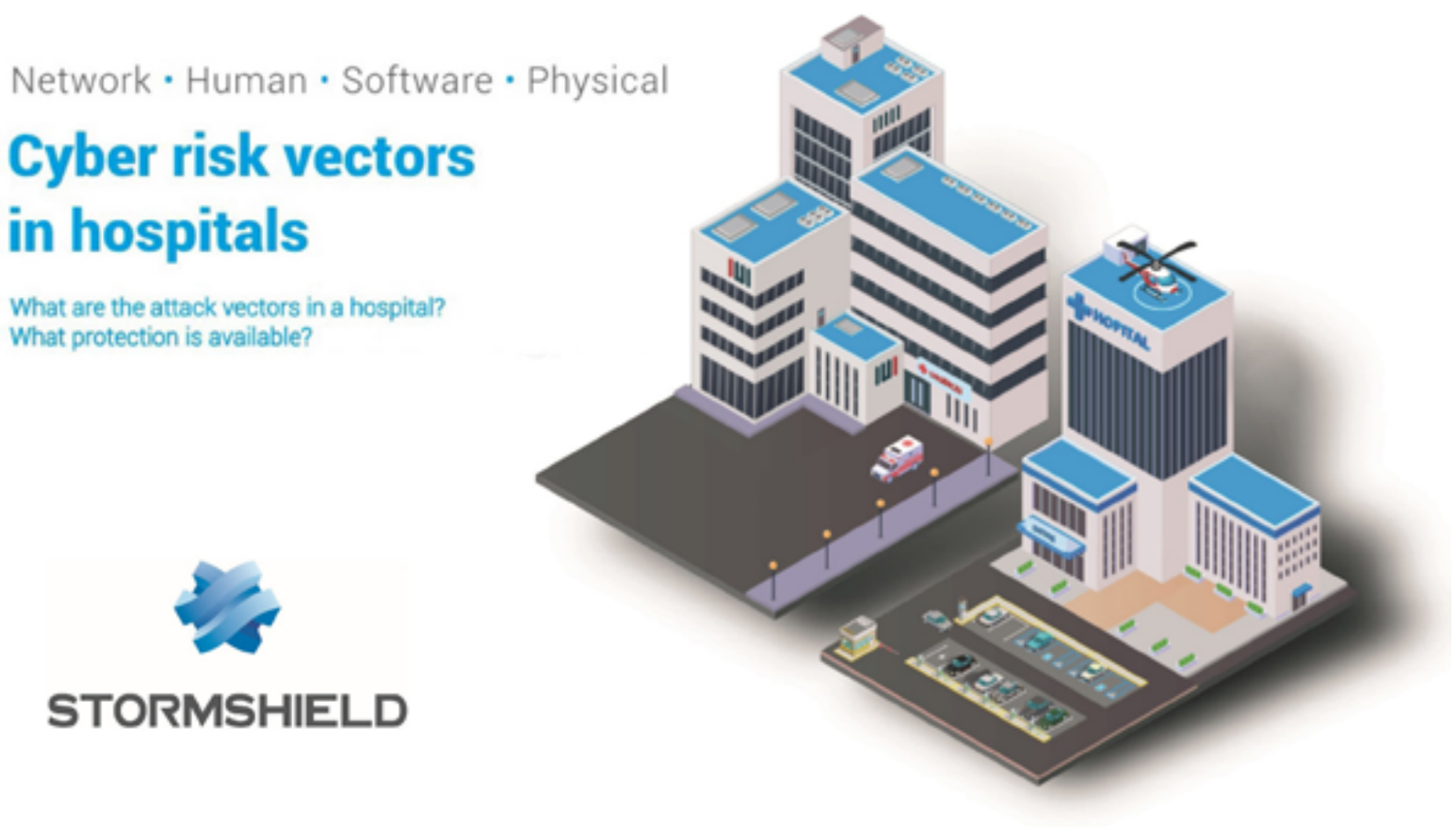
SNI20. FIREWALL A MEDIDA PARA ENTORNOS SANITARIOS

El firewall industrial SNi20 ofrece una integración de red única y completa (enrutamiento y NAT) y seguridad avanzada. Asimismo, proporciona una inspección profunda de paquetes (análisis basado en el contexto), permitiéndole proteger protocolos de comunicación de telemedicina, BMS (Building Management Systems) y CTM (Centralized Technical Management). El firewall garantiza la confiabilidad operativa de su infraestructura y una continuidad de negocio óptima en todo momento, incluso en caso de avería, gracias al sistema de alta disponibilidad y modo de seguridad de la red operativa.

El cortafuegos SNi20 ha sido diseñado para cumplir con los estándares de certificación más estrictos del mercado.

SNI40. FIREWALL PARA SISTEMAS SANITARIOS

El cortafuegos SNi40 está especialmente diseñado para proteger equipamiento médico (respiradores, imágenes médicas...) y equipamiento técnico como reguladores de presión, temperatura o gases y ofrece una amplia gama de funciones: segmentación de red, control de acceso por filtrado de direcciones IP o MAC, análisis contextual de paquetes, control de mensajes operativos y cumplimiento de protocolos (IPS) y comunicaciones seguras de mantenimiento remoto (VPN). Además, este equipo se puede integrar fácilmen-



te en su entorno, especialmente en sus armarios de control (sobre rieles DIN), gracias a un sencillo procedimiento de puesta en marcha.

El SNi40 garantiza la continuidad de la actividad gracias, en particular, a su sistema de alta disponibilidad y al modo de seguridad de la red operativa, que mantiene sus sistemas de producción funcionando sin interrupción, incluso en caso de fallo.

El SNi40 es un cortafuegos certificado al más alto nivel europeo. Ha recibido la certificación y calificación CSPN a nivel elemental, emitida por ANSSI. Por ello, si elige esta solución de Stormshield Network Security, puede estar seguro de que su infraestructura industrial estará cubierta por la mejor protección posible.

STORMSHIELD ENDPOINT SOLUTION (SES)

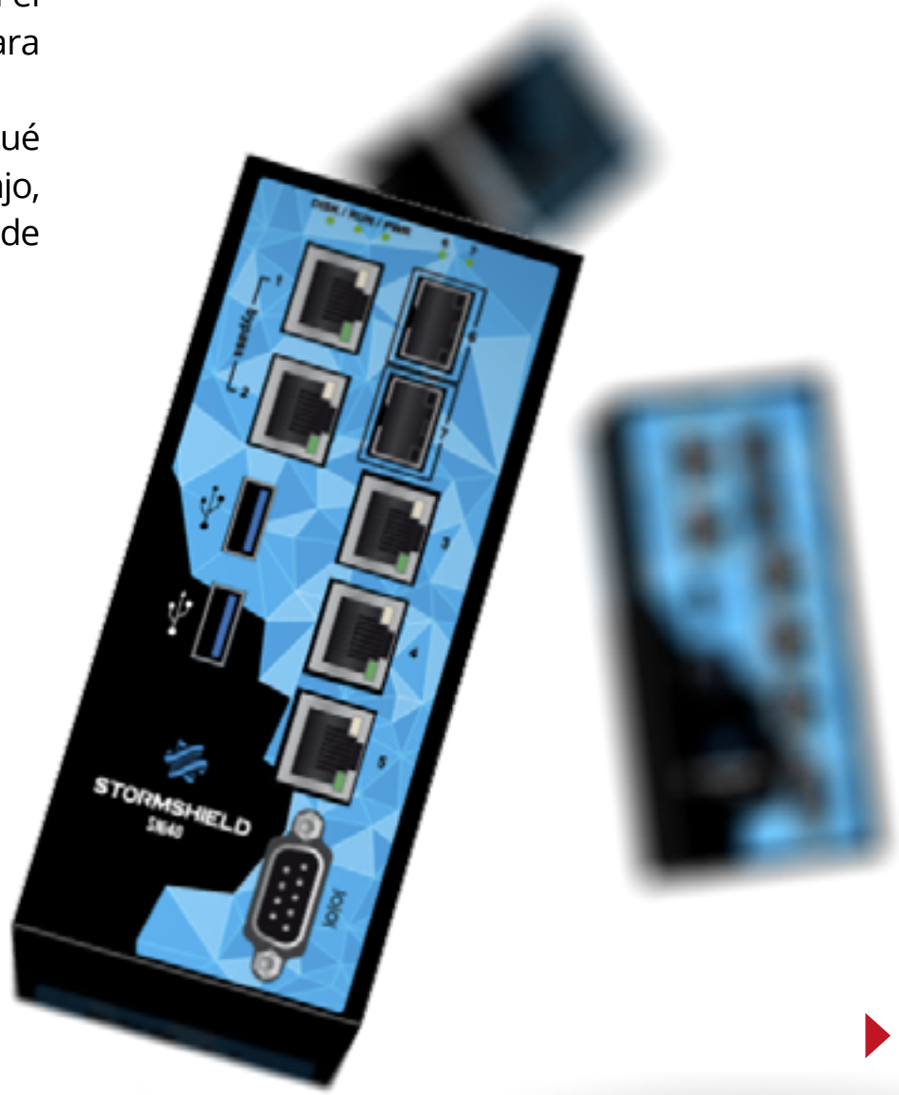
A menudo considerados como los eslabones más débiles en la seguridad de TI, los terminales incluyen todos los dispositivos que se conectan a la red central de una organización sanitaria: ordenadores de escritorio y portátiles, tabletas, teléfonos inteligentes, impresoras y todos los demás dispositivos (inteligentes o no) que se nos requiera conectar a la red interna. Sin embargo, todos estos terminales podrían ser secuestrados y utilizados por los ciberdelincuentes como un punto de entrada para penetrar en su sistema informático con el fin de instalar malware u obtener acceso a sus datos. Desde ellos, pueden saltar a la red hospitalaria provocando graves daños.

SES tiene características que lo hacen especialmente adecuado para el entorno sanitario: protege sistemas operativos obsoletos que siguen operando en redes de imágenes médicas, por ejemplo, como puede ser Windows XP. Por otra parte, SES no está basado en firmas ni necesita conexiones al exterior para su correcto funcionamiento. Por último, hay que destacar sus capacidades de creación de listas blancas, que no son manejables en el mundo IT pero sí en el sanitario, donde las aplicaciones necesarias para los puestos son mínimas y estables.

SES también controla qué dispositivos y a qué redes puede conectarse cada puesto de trabajo, bloqueando, por ejemplo, el uso no deseado de dispositivos USB. ■

MÁS INFORMACIÓN

- Telemedicina y ciber-riesgos
- Cómo prevenir ataques de ransomware
- Vulnerabilidades en la infraestructura de un hospital
- DPI Systems Network Security
- Context/Behavior-aware Endpoint Protection and response to meet digital and hybrid workforce requirement



IBERLAYER

Cloud Email Security

9 de cada 10 incidentes de
ciberseguridad empiezan por email

¿Cuánto le preocupa la seguridad del suyo?

WWW.IBERLAYER.COM

Protección total contra Spam, Phishing, Ransomware, Malware,
APTs, Scam, Fraudes de CEO, Fraudes Bancarios ...

España, ¿hub de centros de datos?

Los centros de datos, espacios dedicados a mantener servidores de datos para almacenar y procesar datos, han crecido rápidamente a medida que la demanda de datos ha aumentado exponencialmente. Estados Unidos, sede de muchas de las principales empresas productoras y consumidoras de datos del mundo (incluidas Facebook, Amazon, Microsoft y Google), históricamente ha tenido muchos más centros de datos que cualquier otro país.

Se trata de un mercado en plena expansión. En 2010, IDC calculaba que se habían creado 1,2 zettabytes (1,2 billones de gigabytes) de nuevos datos en todo el mundo, un aumento del 50 % con respecto al año anterior. Ese año, también estimó que la cantidad anual de datos producidos crecería a 35 zettabytes para 2020, un nivel que se alcanzó en 2018. En 2020, la creación de datos fue de aproximadamente 59 zettabytes.

Ahora, esta misma consultora ahora señala que, para 2025, los datos recién creados serán de 175 zettabytes. Si se alcanza esta cifra, equivaldría a un aumento de 146 veces en el período de 15 años entre 2010 y 2025. Es decir, que entre 2018 y 2020 se crearon más datos que en toda la historia humana antes de 2018.3

¿Dónde residen todos estos datos? Efectivamente, muchas veces están situados en estos CPD. Por eso, en términos de valoración, el procesamiento y almacenamiento de datos se estima que crecerá de 56.000 millones de dólares en 2020 a 90.000 millones para 2025.

REPARTO MUNDIAL

El aumento significativo de la generación y el uso de datos en una variedad de industrias ha llevado a un aumento en la demanda de servidores y centros de datos. Según los datos de CloudScene, que ha recopilado la información disponible de 110 países, en enero de 2021 había cerca de 8000 centros de datos en todo el mundo. Entre estos países, seis albergan la mayoría de los centros de datos: Estados Unidos (33 % del total), Reino Unido (5,7 %), Alemania (5,5 %), China (5,2 %), Canadá (3,3 %) y Países Bajos (3,4 por ciento). Además, el 77 por ciento se encuentra en los estados miembros de la OCDE y aproximadamente el 64 por ciento en los países de la OTAN.

La demanda de centros de datos difiere según el país. En este sentido entran en juego muchas variables: legislación sobre soberanía de datos, espacios disponibles, infraestructuras eléctricas apropiadas, mercado y masa crítica, situación geopolítica…. El Reino Unido, por ejemplo, tiene la segunda mayor participación de centros de datos y es uno de los centros financieros más grandes del mundo. Estados Unidos y China (primero y cuarto, respectivamente) tienen demandas sustanciales de datos en una variedad de sectores, mientras que Alemania (tercero) tiene una capacidad industrial y de fabricación significativa con grandes demandas de datos.

ESPAÑA, EN AUGE

Lo que está claro es que, en este juego de tener cada vez más centros de datos, tanto de los jugadores de la industria tecnológica como de las propias empresas de cualquier sector de actividad, España vive un momento dulce.

De hecho, hace meses que las consultoras especializadas en el terreno (incluyendo aquellas que se dedican a buscar las mejores localizaciones para este tipo de infraestructuras), señalan que la Península Ibérica está ganando enteros y atrayendo la inversión de muchas compañías internacionales, quienes están decidiendo abrir en nuestro país sus centros de datos.

El reciente anuncio de Meta de situar en Talavera de la Reina (Toledo) uno de sus CPD no hace sino reforzar esta tendencia.

Además, el hecho de que España también esté siendo puerto de destino de cables submarinos para conectar diferentes continentes también ayuda a consolidar esta tendencia.

De hecho, la actividad de desarrollo de centros de datos de colocación en España durante 2020 alcanzó cuotas históricas. Los anuncios de nue-

> “España se está convirtiendo en el destino mundial del datacenter, con un mercado en ebullición que va a duplicar su capacidad en los próximos dos años, lo que ayudará a crear muchos puestos de trabajo especializados y a convertirnos en un verdadero motor de la industria cloud”
>
> ADOLFO CRESPO, HEAD OF DATA CENTER OPERATIONS EN ARSYS

vos proyectos en Madrid y Barcelona supusieron añadir una capacidad informática estimada de 70MW, lo que implica duplicar la capacidad de colocación existente.

Son datos de la consultora CBRE que, en un informe a nivel mundial sobre el mercado de centros de datos, destaca que España tiene un mercado de centros de datos muy maduro. Madrid vuelve a ser el eje central de este movimiento, aunque Barcelona y Bilbao también están experimentando un importante crecimiento, debido en parte a la conexión de esos cables submarinos como 2Africa, respaldado por un consorcio de empresas que incluye a Facebook, o Grace Hopper, impulsado por Google.

LO MEJOR ESTÁ POR VENIR

Pero, además, este informe de Cebre asegura que los proyectos de cable submarino Marea & 2Africa, que se completarán en este 2022, harán que España se sitúe, aún más, como un destino clave de centros de datos para la prestación de servicios y transporte de tráfico de datos entre Europa y América.

“Se espera una aceleración del despliegue de la red 5G y, según DE-CIX, el uso de la red en España se disparó un 50% entre 2020 y 2021. Este escenario hace suponer un crecimiento de la inversión en este tipo de infraestructuras”

JAVIER RAMÍREZ, SENIOR DEVELOPER ADVOCATE DE AWS IBERIA

LA IMPORTANCIA DEL CENTRO DE DATOS EN 2022, A DEBATE

Nuestra posición geográfica también jugará un papel determinante al ser una puerta natural hacia África.

Sin embargo, este buen momento no está exento de ciertos desafíos. Por un lado, disponer de parcelas que puedan albergar estos grandes centros de datos y que, además, la infraestructura eléctrica sea lo suficientemente potente como para dar suministro a estas instalaciones.

Además, España también tiene que "pelear" con la competencia europea. Aunque el mercado de centros de datos europeo sigue atrayendo el interés de la comunidad inversora, debido sobre todo a la creciente demanda de los operadores de la nube a hiperescala, los grandes nombres de la industria siguen optando, en muchas ocasiones, por los mercados tradicionales de CPD. Los conocidos como FLAP: Frankfurt, Londres, Ámsterdam y París. En el primer trimestre de 2021, estas cuatro ciudades representaban casi 2.000 MW de oferta de centros de datos, el doble que en 2016.

Lo que no cabe duda es que estas grandes instalaciones también conllevan mucha inversión alrededor de la misma.

POR QUÉ ESPAÑA ATRAE LA INVERSIÓN

Ante la situación que vive España en el mercado de los CPD, hemos querido preguntar sobre las razones y, más importante aún, por las repercusiones que estas inversiones van a suponer para el panorama tecnológico y empresarial.

Como avanza Adolfo Crespo, head of data center operations en Arsys, se dan varias circunstancias. "Por un lado, la importancia creciente y el peso específico que tecnologías como el Cloud, el 5G y el Edge Computing están adquiriendo para el funcionamiento de nuestras sociedades hace que esté creciendo considerablemente la demanda global de estas infraestructuras y convirtiendo los centros de datos de proximidad en el centro neurálgico de la economía digital. Además, en nuestro país cada vez hay más empresas dispuestas a mover sus operaciones a la nube y, por último, conviene señalar que nuestra ubicación geográfica para montar un centro de datos es privilegiada.", declara.

Javier Ramírez, senior developer advocate de AWS Iberia, asegura que, en el caso de AWS, el anuncio de la apertura de una región cloud en España (en Aragón) ha sido "fruto de la demanda de nuestros clientes y una evolución natural de las inversiones que AWS lleva haciendo en España desde 2012 y que incluyen oficinas corporativas en Madrid y Barcelona, 2 Edge Locations y 2 AWS Direct Connect". Este responsable asegura que, en estos momentos, AWS cuenta con "decenas de miles de clientes en la Península Ibérica que, en el momento de la apertura de la nueva Región AWS en España, podrán satisfacer a sus usuarios finales con una latencia aún más baja". Frente a otras empresas que han apostado por Madrid para situar sus CPD, AWS asegura que Aragón es una localización

"Se estima que, para los próximos cuatro años, solo en infraestructuras físicas, las inversiones en el sector del data center en España podría alcanzar la cifra de 3.000 millones de euros"

IGNACIO VELILLA, MANAGING DIRECTOR DE EQUINIX EN ESPAÑA

"estratégica ya que nos permitirá cubrir necesidades de baja latencia para nuestros clientes en España y Portugal, en el sur de Francia y en otras zonas del sur de Europa".

Por su parte, Ignacio Velilla, managing director de Equinix en España, cree que, al encontrarnos en un "boom de la economía digital", es muy probable que "haya empresas que piensen que el mejor momento para invertir es este. La digitalización de la economía en España, con acceso a servicios cloud, IoT o 5G también requieren una mayor proximidad de la infraestructura con el usuario final, lo que da pie a que muchas compañías estén interesadas en aprovechar las oportunidades que abre nuestro mercado". Además, asegura que otro gran motivo para que España esté acaparando tanta inversión en el sector de los data centers es "porque se ha consolidado como el hub de interconexión global del sur de Europa".

Javier Martínez, sales engineering manager de Google Cloud, expone que almacenar y gestionar los datos que se generan "está llevando a que las empresas inviertan cada vez más en centros de datos y en la gestión de estos y España representa un punto clave en el mapa. En primer lugar, por su ubicación geográfica, que además de su cercanía con África, la convierte en una de las puertas principales de entrada para que las comunicaciones entren a Europa desde zonas como Estados Unidos. La experiencia de España, que la hace ser un hub de interconexión fundamental en este sentido. La reciente llegada del cable submarino 'Grace Hopper', diseñado para aumentar la fiabilidad del servicio y ofrecer altos niveles de velocidad y flexibilidad de la red y que harán que mejore aún más la infraestructura general de las telecomunicaciones en esta área, así como la llegada a las costas de Portugal de cable submarino Equiano que une las costas de Portugal y Sudáfrica y que también beneficiará la conectividad de la región y beneficiará al territorio español, son solo algunas de las ventajas que España ofrece a los inversionistas en materia de CPD".

Como añade Daniel Boluda, director general de Huawei Digital Power España, hay diferentes motivos por los que nuestro país está siendo foco de atracción de inversiones en el ámbito de los CPD. "Entre otros aspectos, España destaca por encontrarse en un enclave geográfico estratégico, al que llegan fibras submarinas provenientes de tres continentes. Hay que tener en cuenta que alrededor del 90% de las comunicaciones globales circulan por cables submarinos, que permiten la transferencia de grandes cantidades de datos con la mínima latencia posible. Por esta razón, y de cara a minimizar retrasos en las comunica-

"Los centros de datos son uno de los actuales impulsores de la economía digital para un país. La inversión en infraestructuras provoca un efecto multiplicador en otras industrias y, por supuesto, la creación de nuevos puestos de trabajo, repercutiendo de manera muy positiva en la sociedad en la que se opere"

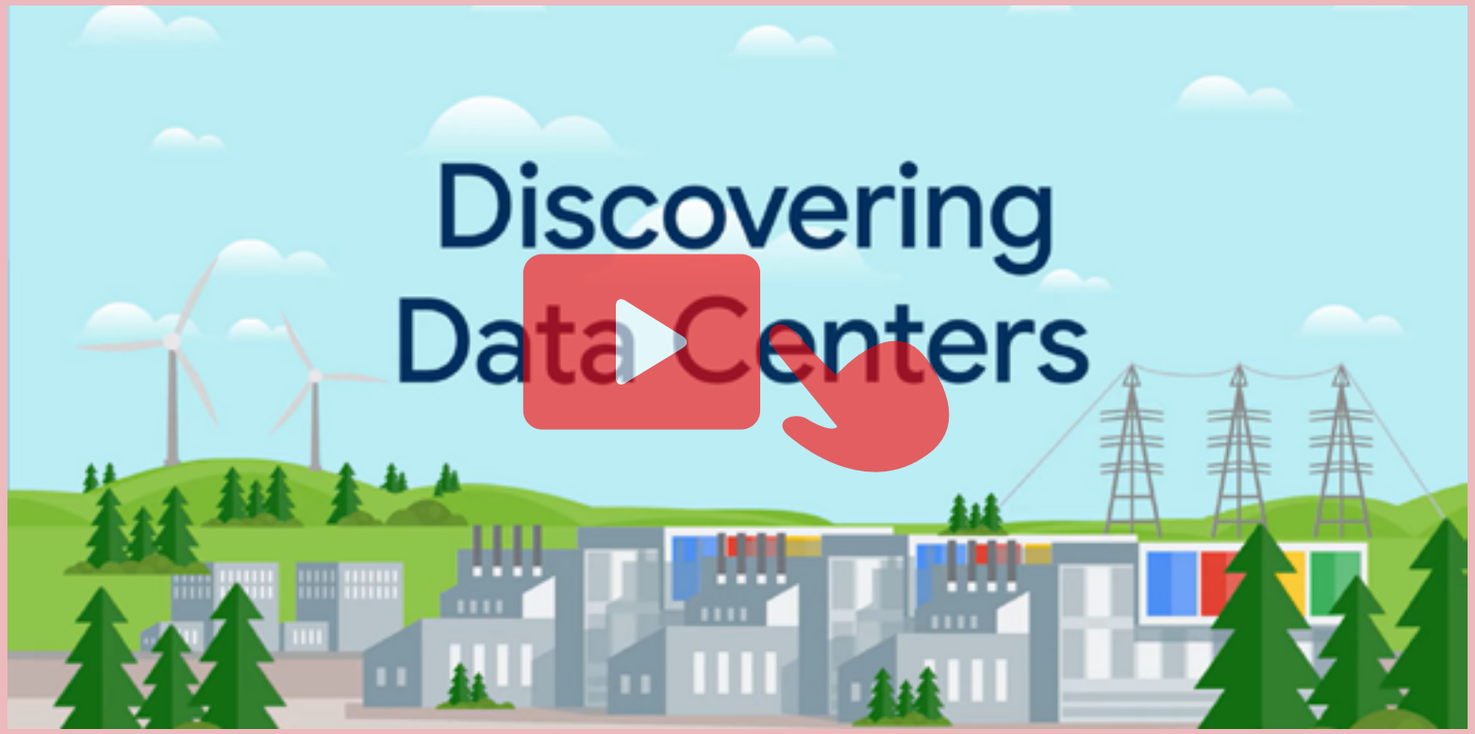
JAVIER MARTÍNEZ, SALES ENGINEERING MANAGER DE GOOGLE CLOUD

ciones, se considera primordial construir los data centers lo más cerca posible de estas fibras, y España se encuentra en una localización privilegiada para ello", relata. Pero, además, este responsable que también tenemos que tener en cuenta la "enorme capacidad energética con la que cuenta el país, y muy especialmente en el ámbito de las energías renovables, que hoy en día es un área estratégica para Huawei, ya que propicia una actividad más sostenible y eficiente, aportando un factor de competitividad claro. Igualmente, otro aspecto que favorece las inversiones es la disponibilidad de suelo para la construcción de centros de datos en nuestro territorio".

Mientras, Robert Assink, director general de Interxion España, alude también al crecimiento acelerado de la economía digital que ha experimentado nuestro país en los últimos años. "Actualmente se dan además cuatro condiciones que contribuyen a la expansión en inversiones programadas en centros de datos para los próximos años", explica. Por un lado, "una red de telecomunicaciones de gran calidad y capilaridad". En segundo lugar, los cables submarinos intercontinentales que llegan a la costa española y que "se conectan en centros de datos especializados para distribuir y entregar contenido". En tercer lugar, "la presencia en la península

"Al factor geográfico hay que sumar también la enorme capacidad energética con la que cuenta el país, y muy especialmente en el ámbito de las energías renovables"

DANIEL BOLUDA, DIRECTOR GENERAL DE HUAWEI DIGITAL POWER ESPAÑA



¿QUÉ ES UN CENTRO DE DATOS?

ibérica de los nodos locales de proveedores cloud hiperescalares". Y, por último, "el aumento del volumen de datos corporativos, que genera un efecto de fuerza de atracción entre datos y aplicaciones, exigiendo una mayor capacidad para alojar y conectar dicha información".

QUÉ SUPONE QUE ESTÉN EN ESPAÑA

El hecho de que los CPD se sitúen en nuestro país conlleva ciertas consecuencias. Jaime Balañá, director técnico de NetApp España, subraya que, antes de decidir apostar por un determinado país, además de lo mencionado anteriormente, como puede ser la conectividad, influyen otros factores como las regulaciones en relación con la privacidad de los datos o las propias medidas de seguridad implementadas en los CPD. "La legislación vigente de la ley de privacidad de datos ofrece mayor seguridad. Los inversores buscan la situación de seguridad jurídica que se desarrolla en Madrid, por ello, apuestan por invertir aquí. A esto se le suma a la situación geográfica de la ciudad", explica. Además, cree que otro punto clave de nuestro país, es que somos la vía de entrada de Latinoamérica y poseemos una gran proximidad con África. "En general, estamos centralizando las gestiones, desarrollando un interlocutor que conecte la Administraciones pública con las organizaciones privadas lo que facilita los procedimientos/trámites. Y supone el lanzamiento del país a la vanguardia de los CPD".

Para Sergio Sáez, director del negocio cloud de Oracle en España y Portugal, la decisión de traer una Región Cloud a España por parte de su compañía "ha venido dada por las necesidades de nuestros clientes y partners", ya que "nuestro objetivo es presentar servicios cloud en entornos de misión crítica y para ello es fundamental poder acercar los CPDs a nuestros clientes. Esta misma estrategia se está siguiendo en otros países del sur de Europa, como Francia o Italia, por ejemplo, donde también tenemos Regiones Cloud de Oracle de reciente apertura. En todos estos casos, estamos siendo capaces de desplegar los CPD más rápido que nuestros competidores por los altos niveles de automatización".

Luis Casero, field marketing manager de Vertiv para España y Portugal, detalla que "todos los grandes proveedores de Colocation han establecido o ampliado presencia en España en los últimos años, lo que demuestra las grandes ventajas que tiene nuestro país para este tipo de instalaciones".

EL PELIGRO ESTÁ AHÍ FUERA

En cuanto a los principales inconvenientes, Luis Casero explica que los centros de datos "no están contemplados como grandes consumidores en la planificación de expansión de la red

"La inversión depende de las características de cada proyecto. Los factores que influyen principalmente son la potencia eléctrica requerida y la capacidad de espacio técnico del centro de datos"

ROBERT ASSINK, DIRECTOR GENERAL DE INTERXION ESPAÑA

eléctrica, lo que ralentiza la obtención de permisos y la ejecución de las infraestructuras necesarias". Además, este responsable considera que "las administraciones públicas podrían jugar un papel más facilitador para la atracción de empresas e inversiones".

Sin embargo, más que hablar de inconvenientes, Sergio Sáez que estamos ante un reto: "el de encontrar al partner local adecuado para la co-locación de nuestra infraestructura". En este punto, asegura que, "tras un proceso de análisis muy detallado, Oracle ha elegido a Telefónica España para nuestra Región Cloud local, esto nos va a permitir, además de los beneficios anteriormente detallados, contar con un partner con una amplia experiencia y presencia en España que facilitará los procesos de adopción del cloud por parte de nuestros clientes".

Mientras, desde NetApp se alude a que, pese a que "las condiciones que se dan y el auge que están teniendo, no hay suficientes Data Centers para la gran cantidad de datos que se generan diariamente". Es más, Balañá sentencia que el volumen de datos que se genera actualmente "excede el espacio de almacenamiento que hay destinados para ellos. Por ello, la inversión que estamos experimentando en cuanto a CPD resulta beneficiosa".

Por eso, más que de inconvenientes, Rober Assink cree que podríamos hablar de aspectos a mejorar. "Hay que trabajar en la planificación y asignación de recursos energéticos, fomentando las renovables e incluyendo a los centros de datos existentes y en construcción en la planificación energética; potenciar el talento cualificado y el emprendimiento; y agilizar la concesión de licencias y simplificar procesos burocráticos", detalla.

Como concluye Adolfo Crespo, "no hay muchos inconvenientes, quizás uno de los más reseñables, especialmente en Madrid y Barcelona, puede ser la falta de suelo libre en las condiciones que exige la instalación de un centro de datos, es decir, cerca de alimentadores de energía de alta tensión y rutas de fibra".

LA INVERSIÓN DE UN CPD

Dentro del sector de los CPD, los hay de todos los tamaños y tipologías. Desde los que apenas tienen un par de racks a los que se extienden por varios metros cuadrados de terreno.

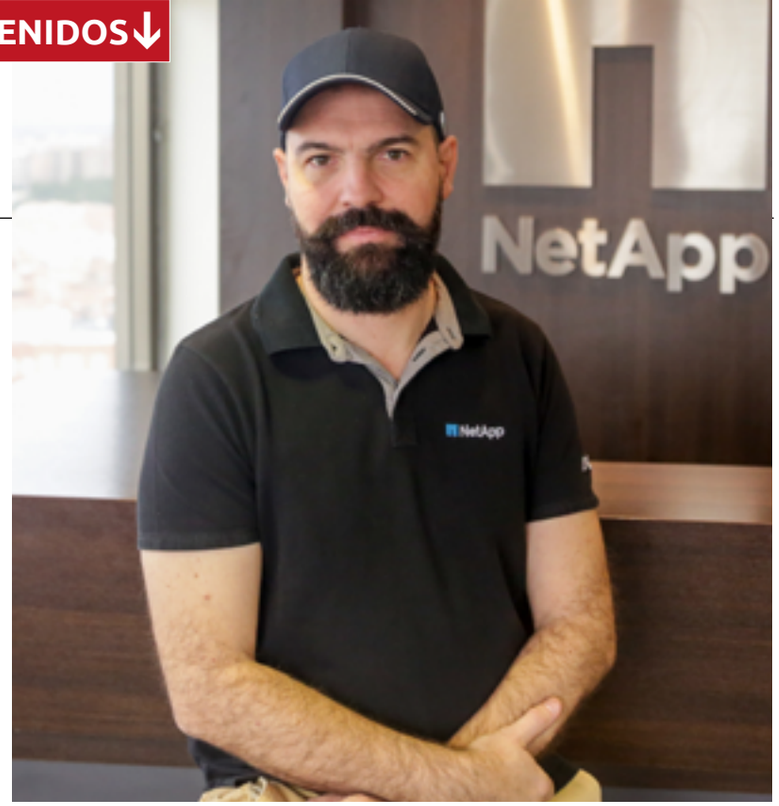
En cualquier caso, invertir en un CPD supone una partida importante. ¿Cuánto? "No hay un precio promedio, dependerá de las condiciones de cada CPD que contribuyen a que el precio final varíe en mayor o menor medida. Como norma general, a mayor inversión mejor eficiencia", incide Jaime Balañá, director técnico de NetApp España, quien asegura que muchas empresas "optan por firmar alianzas y colaboraciones con empresas proveedoras de servicios de centro de datos en la nube o co-localización" para con-

CENTRO DE PROCESO DE DATOS DE LA UNIVERSIDAD DE BURGOS

trolar el gasto mientras se garantiza la escalabilidad y la seguridad".

Y es que resulta muy difícil dar una cifra al respecto. "Influye la superficie total de la instalación y el precio del suelo, que varía considerablemente de un sitio a otro. También son importantes en el coste final la potencia energética contratada, la complejidad de las instalaciones eléctricas, la alta disponibilidad que queramos que nos ofrezca (a mayor disponibilidad mayor nivel de redundancia de los elementos críticos) y los costes de mantenimiento", detalla el head of data center operations en Arsys, añadiendo la climatología del lugar, que "es importante porque está directamente relacionada con la eficiencia energética del centro de datos, condiciona la elección de los sistemas de refrigeración y climatización e influye directamente en el consumo energético".

Sin embargo, el director general de Interxion España aclara que, aunque la inversión depende de las características de cada proyecto, para hacernos una idea podemos poner en una balanza diferentes factores. Los que más influyen son, en su opinión, "la potencia eléctrica requerida y la capacidad de espacio técnico del centro de datos". En este punto, considera que la tendencia es ir hacia "centros de datos más grandes y eficientes para soportar la demanda de la economía digital". Como muestra, un botón: cuando Interxion construyó MAD3, operativo desde 2019, el proyecto



"A pesar de las condiciones que se dan y el auge que están teniendo, no hay suficientes Data Centers para la gran cantidad de datos que se generan diariamente. El volumen de datos que se genera actualmente excede el espacio de almacenamiento que hay destinados para ellos"

JAIME BALAÑÁ,
DIRECTOR TÉCNICO DE NETAPP ESPAÑA

incluía 6MW de carga IT con una inversión de 44 millones de euros. Hoy, el cuarto centro de datos (MAD4), cuya inauguración está prevista para este año, contará con 30MW de potencia eléctrica, será cinco veces más grande que MAD3 y su inversión alcanzará los 230 millones de euros. "En cuanto a cómo repercuten estas inversiones en otros datos económicos, destaca el impacto positivo en el PIB y en la creación de empleo. El estudio Madrid Hub DigitalTM muestra que, por cada euro invertido en centros de datos, el retorno se puede llegar a multiplicar por 12", asegura Assink.

Javier Martínez coincide en que cada apertura es única y conlleva numerosos aspectos a considerar que impactan directamente sobre la cifra final. Pero subraya que los centros de datos son "uno de los actuales impulsores de la economía digital para un país. Si hablamos de los datos económicos que se generan alrededor de estas instalaciones podemos destacar la inversión en infraestructuras, la cual provoca un efecto multiplicador en otras industrias y, por supuesto, la creación de nuevos puestos de trabajo, repercutiendo de manera muy positiva en la sociedad en la que se opere. La atracción de talento es también otro punto importante, puesto que centros como estos generan un efecto llamada para muchos profesionales".

Es decir, que tal y como corrobora el director del negocio cloud de Oracle para España y Portugal, más que la inversión en sí es el impacto que tuene para todo el ecosistema de "clientes y partner, facilitando los procesos de innovación y puesta en marcha nuevos proyectos que supondrán atracción de talento, empleabilidad, generación de riqueza local. Queremos que nuestra próxima Región Cloud ayude al tejido empresarial a acelerar su transformación digital y a nuestras Administraciones públicas a avanzar con decisión en sus procesos de digitalización".

LO QUE MUEVE UN CPD

Independientemente de quién apueste por co-locar un CPD en nuestro país, esto supone una tracción para el resto de empresas. En este sentido, el director general de Huawei Digital Power España, manifiesta que la consolidación de los data centers en España "aporta un importante impulso no solo para las empresas directamente involucradas en su construcción y mantenimiento, sino también de otras empresas auxiliares". Según su visión, esto se pone de manifiesto, por ejemplo, en "la atracción del empleo cualificado por parte de este tipo de centros lo que, dada la falta de especialistas en este sector, significa una importante aportación de valor en las zonas geográficas en las que se encuentran ubicados". Además, añade que el propósito de que los centros se desarrollen "no solo en grandes extensio-

"Más que un inconveniente, invertir en un CPD es un reto. Y es el de encontrar al partner local adecuado para la co-locación de nuestra infraestructura. Tras un proceso de análisis muy detallado, Oracle ha elegido a Telefónica España para nuestra Región Cloud"

SERGIO SÁEZ, DIRECTOR DEL NEGOCIO CLOUD DE ORACLE EN ESPAÑA Y PORTUGAL

nes como campus multipropósito, sino también en otras ubicaciones en forma de pequeños edge data centers, contribuye a que muchos sectores, como el energético, el transporte o la educación, entre otros, se desarrollen de forma paralela".

De la misma forma, Ignacio Velilla enumera que, entre otros beneficios, "aquellas empresas que quieran desplegar servicios en España y estén conectados a los data centers de Equinix dispondrán de una gran capacidad de interconexión internacional y podrán ofrecer bajas latencias a sus usuarios". Además, "tendrán acceso a los principales proveedores de servicios cloud y contarán con la posibilidad de habilitar conexiones directas y privadas con miles de partners para adaptarse a un ecosistema dinámico de negocio al mismo tiempo que mejoran su rendimiento y mantienen la seguridad".

Javier Ramírez, mientras tanto, explica que AWS tiene el concepto de una región, que es una ubicación física donde agrupa los centros de datos. "Cada región de AWS consta de varias "zonas de disponibilidad" aisladas y separadas físicamente dentro de un área geográfica. Una zona de disponibilidad es uno o más centros de datos discretos con alimentación, redes y conectividad redundantes en una región de AWS. Los clientes de AWS centrados en la alta disponibilidad pueden diseñar sus aplicaciones para que se ejecuten en múltiples zonas de disponibilidad y lograr una mayor tolerancia a errores", detalla.

En este sentido, la nueva Región AWS Europa (España) permitirá, según este responsable, a las empresas y organizaciones "que tengan requisitos de residencia de datos almacenar de manera segura su contenido en España, con la garantía de que mantendrán control total sobre la localización de sus datos. La nueva región también asegura que los clientes que desarrollan aplicaciones en cumplimiento con el Reglamento General de Protección de Datos (RGPD) tendrán acceso a otra región de infraestructura segura de AWS en Europa -además de las regiones existentes en Dublín, Frankfurt, Londres, París, Estocolmo y Milán - respetando los más altos estándares de seguridad, cumplimiento normativo y protección de datos. AWS también cuenta con la certificación del Esquema Nacional de Seguridad (ENS) Nivel Alto, lo cual significa que su infraestructura cumple con los más altos niveles de seguridad y cumplimiento para agencias estatales y organizaciones públicas en España". Y, por si fuera poco, esta infraestructura ofrecerá a los usuarios finales con una latencia aún menor.

Es decir, que como resume, con una nueva región, "las organizaciones españolas podrán acceder a tecnologías avanzadas de AWS, la nube más ampliamente adoptada en el mundo. El completo conjunto de servicios cloud de AWS -incluyendo computación, almacenamiento, re-

des, bases de datos, análisis, aprendizaje automático, Internet de las cosas (IoT), dispositivos móviles, y mucho más – puede ayudar a impulsar la innovación y la transformación digital que impulsarán aún más el desarrollo económico de España".

EL LUGAR ENTRE LOS FLAP

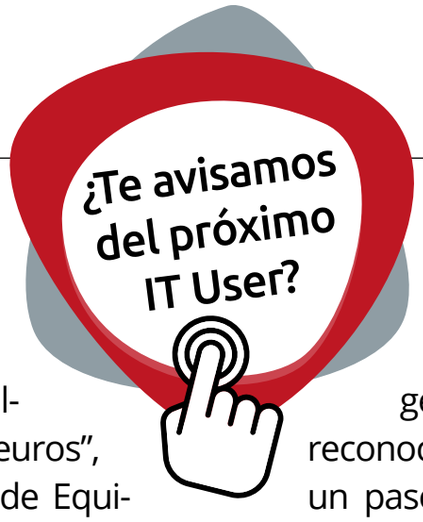
Pese a este buen momento que vive España en el terreno de las inversiones en CPD. Lo cierto es que seguimos lejos de los números que atesoran los FLAP. ¿Llega tarde España a la carrera de los CPD o, por el contrario, nuca es tarde si la dicha es buena?

El sales engineering manager de Google Cloud descarta que nuestro país llegue tarde. "España tiene las condiciones necesarias para estar a la altura del resto de países. Además, el mercado de las telecomunicaciones y los datos no va a hacer más que aumentar. España juega un papel fundamental en el sur de Europa y por esta razón Google Cloud tiene ese firme compromiso en lo que a inversión se refiere. Nuestro compromiso por apostar e invertir en una región como España está más presente que nunca, y un claro ejemplo de ello es lo que hemos estado comentando anteriormente y por supuesto el plan de Google anunciado el año pasado de invertir más de 650 millones de dólares en cinco años en España para impulsar iniciativas que contribuyan a la transformación digital y la recuperación económica del país", enfatiza.

CENTRO DE PROCESO DE DATOS DE ENAGAS EN ZARAGOZA

"España todavía está un paso por detrás de los FLAP, pero es la ubicación con mayor crecimiento proyectado. No se trata de llegar pronto o tarde, sino de maximizar las oportunidades cuando se dan las circunstancias para el crecimiento"

LUIS CASERO, FIELD MARKETING MANAGER DE VERTIV PARA ESPAÑA Y PORTUGAL



"Se estima que, para los próximos cuatro años, solo en infraestructuras físicas, las inversiones en el sector del data center en España podría alcanzar la cifra de 3.000 millones de euros", contextualiza el managing director de Equinix España. "De esta manera, la infraestructura digital de nuestro país alcanzaría el mismo tamaño de los principales mercados europeos. Por tanto, España, y Madrid en concreto, se encuentran en un momento de inversión clave para ponerse al mismo nivel que los países que tradicionalmente han liderado el mercado de los data centers: Frankfurt, Londres, Ámsterdam y París. Si se mantiene la tendencia, Madrid podría pasar en poco tiempo a ser considerada una de las grandes capitales europeas de la conectividad", sentencia.

Mientras, el field marketing manager de Vertiv para España y Portugal, reconoce que, aunque España "todavía está un paso por detrás de los FLAP", asegura que es "la ubicación con mayor crecimiento proyectado" por lo que, en su opinión, "no se trata de llegar pronto o tarde, sino de maximizar las oportunidades cuando se dan las circunstancias para el crecimiento".

Por eso, y aunque los FLAP son "una región muy consolidada", Adolfo Crespo subraya que en estos momentos "hay un interés evidente en nuestro país como mercado emergente. Primero porque se dan todas las condiciones para ello, como hemos visto anteriormente, pero también porque las empresas lo demandan y los proveedores cloud buscan prestar servicios a los mercados locales desde el propio país, en lugar de hacerlo en la región". El director técnico de NetApp España concluye que "estamos progresando para mejorar nuestro posicionamiento". Aunque puede que a España "todavía le queda cierto recorrido para alcanzar a los FLAP", considera que esto no implica "que no podamos alcanzar su mismo nivel y llegar a igualar la cantidad de instalaciones de CPD con respecto a países como Alemania que actualmente cuenta con 453 CPD".

APROVECHAR EL MOMENTO

Por tanto, la clave está en saber aprovechar el buen momento que vive el sector de los CPD en España. Y, en este sentido, Daniel Boluda cree que es "fundamental que estos centros estén ligados a las energías renovables y a ecosistemas más completos". En su opinión, "las energías renovables son clave para que los data centers se conviertan en una industria verde y sostenible". Añade que, ya "sea por PPA (Power Purchase Agreement, por sus siglas en inglés) o por autoconsumo (tanto solar como hidrógeno) los centros de datos desempeñan un papel clave en el plano energético, que irá aumentando a medida que vaya creciendo su contribución en este ámbito. También hay que considerar que los modelos de data center están evolucionando en los últimos años y lo seguirán haciendo en los venideros. Por

ejemplo, hay conceptos de modernos mega-data centers (más de 100MW) que implican la construcción de un nuevo y completo ecosistema a su alrededor en materia educativa, de generación energética (proporcionando energías renovables a los vecindarios próximos al centro) e industrial (fábricas inteligentes en estos mega-capus), entre otros". Igualmente, considera que "ya es posible ver cómo el 5G y las próximas redes de telefonía móvil de nueva generación van a contribuir a que los micro-data centers (Edge) tengan un gran futuro en el largo plazo, con el objetivo de minimizar latencia y maximizar la capacidad de proceso lo más cerca posible del usuario final".

Como sentencia el senior developer advocate de AWS Iberia, "la nube ya está impulsando la innovación en las empresas, instituciones educativas, administraciones públicas y agencias estatales en toda España" y la llegada de estos CPD supone una ayuda para "acelerar dicha transformación, permitiendo a organizaciones de todos los sectores reducir sus costes, mejorar su agilidad y competitividad y aumentar la seguridad". "La creación de la región permite a las organizaciones proporcionar una latencia más baja a sus usuarios finales en todo el país al tiempo que funcionará como un gran impulsor de la innovación entre las empresas españolas, ya que podrán aprovechar tecnologías avanzadas como la inteligencia artificial, el aprendizaje automático (ML), Internet de las cosas (IoT), o servicios móviles, entre otras muchas, desde esta región", asegura. ■

Cómo se presenta el futuro

No dormirse en los laureles y seguir trabajando para que este buen momento no se quede en una anécdota y España siga siendo un hub importante en el negocio de los CPD. ¿Cómo ven el futuro nuestros interlocutores?

En general, de forma muy positiva. Algunos, como Sergio Sáez, director del negocio cloud de Oracle en España y Portugal, lo lleva a su terreno al avanzar que "nuestra Región Cloud España se pondrá en funcionamiento en Madrid en los próximos meses".

Un anuncio que podría coincidir con el de Google Cloud puesto que, dos años después de que comunicara la apertura de la región en España, la compañía se prepara para "su puesta en servicio en las próximas semanas". Esta infraestructura "permitirá a las empresas y administraciones públicas españolas acelerar su transformación a escala y desplegar el potencial de los servicios en la nube con baja latencia y alto rendimiento.

La aceleración de la transformación digital en España y la proliferación de las tecnologías 5G son motores clave para el crecimiento de la economía. España necesita que las empresas y las organizaciones públicas de todos los tamaños estén preparadas para afrontar los desafíos digitales presentes y futuros y, para hacerlo, deben contar con una infraestructura ágil, escalable, segura y resistente. Este sólido eje tecnológico facilitará el acceso a innovaciones que permitirán acelerar el desarrollo empresarial", señala Javier Martínez.

"La tendencia sigue siendo de gran crecimiento, con llegadas de nuevas empresas y expansión de la presencia de las ya existentes", asegura Luis Casero, field marketing manager de Vertiv para España y Portugal.

Una visión con la que coincide Jaime Balañá, director técnico de NetApp España, para quien el futuro es "positivo en cuanto a CPD", ya que "se seguirá apostando por la calidad en la gestión y sobre todo la seguridad de los datos". Además, entiende que la administración pública "va a jugar un papel importante en referencia al futuro en la inversión de CPD" y que "esto ayudará al desarrollo de los CPD en nuestro país".

mejorando el posicionamiento actual. Las previsiones de inversión han aumentado, en los próximos años se espera inaugurar más de diez CPD seguidos.

Mientras, Robert Assink, director general de Interxion España, asegura que "se prevé la puesta en marcha de nuevos centros de datos especializados además de las instalaciones planificadas por los grandes proveedores cloud en distintos puntos del país para inaugurar sus regiones locales", por lo que parece que el sol seguirá brillando.

Algo parecido a lo que manifiesta Adolfo Crespo, head of data center operations en Arsys, quien cree que España "se está >>

MÁS INFORMACIÓN

- Soluciones de conmutación para el centro de datos
- Migración de datacenters en caliente
- Centros de datos y la red eléctrica
- Soria, el lugar perfecto para construir centros de datos sostenibles
- Mesa Redonda IT - La transformación del Centro de Datos
- La importancia del centro de datos en 2022, a debate
- Microsoft Reimagina España con su nueva Región Cloud de Centro de datos

>> convirtiendo en el destino mundial del datacenter, con un mercado en ebullición que va a duplicar su capacidad en los próximos dos años, ayudará a crear muchos puestos de trabajo especializados y a convertirnos en un verdadero motor de la industria cloud. El potencial de nuestro país para ubicar nuevos centros de datos en unas condiciones excelentes está situándolos en el punto de mira de las inversiones".

Mientras, Daniel Boluda, director general de Huawei Digital Power España, manifiesta que la industria de los data centers "va a experimentar un gran crecimiento en España. En la actualidad, hay muchos más proyectos en desarrollo que en años anteriores. En este sentido, para 2022 se espera crecimientos de dos cifras que podría extenderse al menos durante los próximos 3 años", sostiene.

Es decir, que las previsiones son muy positivas y van en consonancia con la tendencia de crecimiento del sector. "Son muchas las empresas interesadas en desarrollar infraestructura en España, pero uno de los principales hitos que están previstos para este año es la apertura en Madrid de dos nuevos data centers xScale de Equinix. Esto va a permitir reforzar la posición como hub del sur de Europa y convertirnos en una referencia europea en el despliegue e interconexión de los grandes proveedores de servicios cloud a nivel mundial. Y, por supuesto, estos proyectos van a contribuir a seguir impulsando la atracción de inversiones a nuestro país", adelanta Ignacio Velilla, managing director de Equinix en España.

Así pues, como concluye Javier Ramírez, senior developer advocate de AWS Iberia, si en España se ha experimentado un "incremento de la penetración del comercio electrónico, y un aumento del uso de tecnologías como Cloud Computing, Big Data, Machine Learning o Blockchain", se espera una "aceleración del despliegue de la red 5G y, según DE-CIX, el uso de la red en España se disparó un 50% entre 2020 y 2021. Este escenario hace suponer un crecimiento de la inversión en este tipo de infraestructuras".

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!!!

Avanzando en la digitalización de la pyme española

La pandemia ha acelerado la transformación digital que se demandaba a la empresa española, especialmente entre la pyme y la micropyme, en lo que se ha venido a denominar como 'super digitalización'. Hay muchas esperanzas puestas al respecto en torno a los Fondos Next Generation UE. ¿Están las distintas Administraciones haciendo todo lo necesario para conseguir que el tejido empresarial español acelere su digitalización en estos momentos? ¿Cuál está siendo el papel de fabricantes y partners como facilitadores durante este proceso de transformación digital?

De éstas y otras cuestiones debatimos junto a Susana Juan, head of SMB Sales & Partners en Arsys España; Karina Miguel, national channel manager en Bitdefender España; Carlos Tortosa, director de grandes cuentas de ESET España; Aitor Jerez, director comercial de Sarenet; Fernando Casares, distribution manager para Sophos Iberia; Guillermo Fernández, manager sales engineering Iberia en WatchGuard Technologies; y Francesc Núñez, ERP product manager de Wolters Kluwer Tax & Accounting España. Y, en primer lugar, quisimos saber cuál es la realidad de la digitalización de las pequeñas y medianas empresas. En palabras de Susana Juan, "la tecnología avanza a una velocidad increíble y, dado que está cambiando a las personas y sus ámbitos de consumo, a las empresas no les queda otra que transformarse.

LA DIGITALIZACIÓN DE LA PYME ESPAÑOLA, A DEBATE

Esto no es nuevo, y las empresas con más recursos llevan más tiempo y otros quizá menos, pero con la llegada de la pandemia, los hábitos de consumo se desplazaron radicalmente hacia lo digital, y miles de pymes y micropymes se han visto abocadas a vender por internet para sobrevivir. En pocos meses, la transformación ha dejado ser cosa de otros, y cada negocio ha encontrado su punto de partida, y lo que parecía que no era para ellos, ahora lo es. Falta mucho por hacer, pero los pasos han sido gigantes en los últimos dos años".

Para Karina Miguel, "la crisis ha puesto en evidencia las carencias existentes entre las pymes y las micropymes. Quizá la pyme ha estado más preparada que la micropyme, que se ha tenido que adaptar a cambios no previstos. Estamos en un momento incierto, por la velocidad creciente en la innovación y en la tecnología, y hemos visto mayores inversiones de las empresas en el último año que en el resto de la década anterior. Las pymes españolas han mejorado mucho en ciberseguridad, y los fondos europeos ayudarán mucho en este proceso".

Discrepa de ella Carlos Tortosa, que apunta que "la pandemia provocó que muchas empresas tuvieran que sobrevivir, y eso paralizó proyectos de digitalización que habían comenzado, porque había que diversificar la inversión para mantener la actividad. Ha habido empresas que sí se lo han tomado en serio, porque

"Estamos muy lejos de la situación ideal: solo el 20% de las pymes tiene página web y el 60% se decanta por invertir las ayudas en la creación de una"

SUSANA JUAN, HEAD OF SMB SALES & PARTNERS EN ARSYS ESPAÑA

o vendían por internet o tenían que cerrar. Todavía, en todo caso, queda mucho por hacer, sobre todo en ciberseguridad. A principios de 2020 se vio un gran interés en buscar soluciones de servicios que poder aprovechar en las

pymes, y ahora el segmento pyme sigue creciendo en torno a un 15% en soluciones que nos permitan protegerlas".

Desde la perspectiva de Aitor Jerez, "el 98% de nuestros clientes son pymes o micropymes, y, para ellos, la pandemia ha sido un catalizador, sobre todo, del teletrabajo. Han tenido que aprender a utilizar herramientas colaborativas, se han llevado la extensión de voz en sus portátiles a casa, ha habido un gran esfuerzo en hacer seguro el acceso a los datos que se quedaron en la oficina... tecnología que ya estaba y que es parte de los procesos de digitalización. También es cierto que algunas empresas, para sobrevivir, han tenido que emplear nuevos canales de venta, cuando antes no soñaban con vender en internet. Pero esto solo es parte del camino. Las empresas más grandes han emprendido un camino más complejo, pero se inició hace años, aunque ahora se ha visto algo frenado por la pandemia. De todas formas, nos encontramos con un mayor nivel y número de usuarios digitales y eso va a acelerar el proceso de transformación en las empresas".

Coincide con él Fernando Casares, que añade que "la pandemia ha obligado a muchas empresas a adecuarse a su mercado. Había que poner a las empresas toda la infraestructura necesaria para que no murieran. Ha habido mucho marketing, pero hemos tenido que estar al lado de los clientes para ayudar-

"El canal se está especializando con servicios para el usuario, y éste necesita confiar en el partner, porque no tiene claro cómo solicitar los fondos, y el socio debe ofrecerles lo que ellos necesitan"

KARINA MIGUEL, NATIONAL CHANNEL MANAGER EN BITDEFENDER ESPAÑA

GRAVITYZONE, agente y consola únicos de protección

Bitdefender
BUILT FOR RESILIENCE

Aunque muchas pymes son conscientes de la importancia de la digitalización de sus negocios para crecer y afianzarse en el mercado, la realidad es lo contrario. La gran mayoría de las pymes, sobre todo las pequeñas, no cuentan con personal cualificado en tecnologías y mucho menos, con una estrategia que les permita abordar el proceso de digitalización que requieren. El partner TI se convierte en un aliado para estas empresas que necesitan el apoyo constante de una figura especializada que las acompañe en el proceso de digitalización.

En lo que a ciberseguridad se refiere, muchos ataques afectan a pymes, poniendo en riesgo la continuidad de sus negocios, el dinero, los datos y el equipamiento informático. Los piratas informáticos se centran en ellas porque suelen carecer de un plan de respuesta ante ataques informáticos y dependen para su protección del antivirus y del firewall.

Las grandes empresas normalmente se pueden recuperar de un ataque de ransomware, aunque acaben pagando, pero las pequeñas, en cambio tras un ataque de este tipo, acaban sufriendo un prolongado período de cese de actividad.

En Bitdefender con nuestra filosofía de agente y consola únicos de GravityZone contribuimos a reducir los costes y le proporcionar toda la visibilidad y el control necesarios. Para proteger su empresa contra las amenazas más recientes sin salirse del presupuesto, ha de buscar soluciones para endpoints que superen sistemáticamente la seguridad convencional, como software antivirus, antimalware o firewall. Bitdefender propone estos productos para la protección de la PYME.

les en un cambio durante una situación que, financieramente, era muy complicada".

En opinión de Guillermo Fernández, "comparto las opiniones de mis compañeros, pero, si ponemos el foco en el área de seguridad, lo cierto es que al principio de la pandemia las empresas apostaron mucho por continuidad de negocio, pero lejos de decaer, ahora que ven que el negocio va a sobrevivir a la pandemia, han decidido, ante esta situación de entornos híbridos, extender la seguridad, adoptando medidas para proteger el puesto de trabajo. El ritmo depende de la concienciación de cada empresa o del sector en el que se mueve, pero, en líneas generales, la tendencia es al alza".

Finaliza la primera ronda de valoraciones Francesc Núñez, que señala que "al inicio de la pandemia, las empresas de este tamaño sufrieron, y muchas no han sobrevivido. Había empresas que aceleraron la transformación por la necesidad de sobrevivir. Además, hubo muchos cambios legales a los que se adaptaron mejor los despachos más digitalizados. Nuestra actividad subió mucho. En esta segunda etapa, las empresas han visto que necesitan este empuje, tanto las que necesitaron hacerlo para sobrevivir como aquellas que lo ven en su sector. Todo lo que se ha hecho es necesario, y la adhesión a esta tendencia de las AAPP, está obligando que muchas empresas deban digitalizarse a su vez. La demanda ha subido mucho en esta línea, y las empresas tienen clara esta necesidad de transformación".

"Hay un cambio de paradigma en la ciberseguridad. Lo que se consideraba gasto ahora se ve como inversión"

CARLOS TORTOSA, DIRECTOR DE GRANDES CUENTAS DE ESET ESPAÑA

EL PESO DE LA PYME EN EL GASTO TI

Es interesante que, pese a que la pyme representa un porcentaje muy elevado de las empresas españolas, algunos hablan de un 98%, solo aportan el 15% al gasto de TI. Con este paso adelante en la digitalización, ¿cambiará

este dato? Para Aitor Jerez, "quizá la coyuntura actual no es la mejor, porque muchas empresas se están tambaleando, pero a lo largo de los próximos años vamos a ver una inversión mayor. La digitalización tiene muchas más ventajas que riesgos. Por ejemplo, el ciberseguridad, las empresas ven el gasto ya con otros ojos, porque saben que las ventajas con mayores. La inversión de la pyme va a crecer, pero hay que salir de la situación actual, que está retrayendo el gasto. Nosotros trabajamos en ello, y lo tenemos muy interiorizado, con crecimientos importantes esperados en áreas como cloud o seguridad".

Coincide con él Susana Juan, que indica que, "hablando, sobre todo, de las empresas más pequeñas, muchas han dado un primer paso haciéndose visibles en internet, pero son conscientes de que tener una cuenta en redes sociales no es suficiente. Es cierto que, lo que nosotros llamamos digitalización, no es un camino fácil para una pyme que, en el 99% de los casos, necesita aliados tecnológicos y de inversiones que, en la situación actual, son complejas. Por tanto, esta aceleración de la digitalización va a depender de cómo funcionen las ayudas, tanto de los fondos europeos como del Kit Digital, poque ahí va a estar la clave. Si todo va bien, estas ayudas van a ayudar mucho".

Para Karina Miguel, "la economía española está en un proceso de recuperación, y el negocio TI está creciendo rápidamente. Las pymes

"Quizá la coyuntura actual no es la mejor, porque muchas empresas se están tambaleando, pero a lo largo de los próximos años vamos a ver una inversión mayor, ya que la digitalización tiene muchas más ventajas que riesgos"

AITOR JEREZ, DIRECTOR COMERCIAL DE SARENET

ya se han adaptado al trabajo en remoto, los entornos híbridos, e invertir en la seguridad del perímetro y en los datos es un punto clave para minimizar el riesgo y asegurar la continuidad de sus negocios, porque el foco del malware está ahora en la pyme. Es un buen momento para recuperar presupuestos antiguos o aprovechar las ayudas para invertir en seguridad".

Apuesta por ciberseguridad, cloud, IoT y Big Data

sarenet

La necesidad de adaptarnos a nuevas fórmulas durante la pandemia nos ha convertido en algo más expertos digitales a todos, usuarios y empresas. Esta situación, junto con otros factores que apuntan en la misma dirección como las ayudas económicas por parte de las administraciones van a acelerar todo el proceso de la digitalización en las empresas. La ciberseguridad y los servicios cloud, IoT y Big Data van a ser los negocios que esperamos que tengan más crecimiento durante los próximos años. Por nuestra parte, estamos trabajando para poder ayudar a las empresas en este proceso con el foco puesto en estas áreas.

VARIACIONES EN LA DEMANDA DE TECNOLOGÍA

Si bien con el inicio de la pandemia las inversiones se centraron en áreas concretas de la tecnología, otras están tomando el relevo ahora. Desde la óptica de Guillermo Fernández, "cuando una empresa se encuentra entre la espada y la pared, busca otras opciones y sale de su zona de confort. Y la tecnología es una de estas vías. En los medios vemos noticias de ataques a grandes compañías y algunas pequeñas pueden sentir que para ellas no es tan necesaria la inversión en este terreno, pero la realidad es otra. Son tan o más lucrativas para los cibercriminales por esas menores medidas

de seguridad. Esta percepción va cambiando ligeramente, porque ven que el riesgo real es el cierre, y esto les impulsa". En palabras de Fernando Casares, "las ayudas europeas y el Kit Digital van a potenciar las inversiones. De hecho, ha leído que son más de 10.000 empresas las que ya han solicitado esos fondos. Cada una lo destinará donde más lo necesite, ya sea mejorar la web o la ciberseguridad, pero el gasto va a crecer, porque tienen los medios para, por lo menos, planteárselo".

Carlos Tortosa apunta que "hay un cambio de paradigma en la ciberseguridad. Lo que se consideraba gasto ahora se ve como inversión. Pero algunas empresas todavía están en un momento en que no pueden abordar según qué proyectos. Pensamos que, a futuro, hay que apoyar a la pyme, porque no se trata solo de herramientas, sino de apoyo profesional basado en el servicio para que una pyme pueda acometer proyectos que no se plantea ahora mismo".

Añade Susana Juana que estas ayudas europeas y el Kit Digital son muy positivos, pero "todavía hay confusión, incredulidad y frustración, porque los clientes ven demasiada información y no todas las ayudas están todavía disponibles. Además, me preocupa que hay muchas solicitudes para ser agente digitalizador, donde hay más de 4.500 empresas y todavía no se han aprobado muchas de ellas. Por eso, nos preocupa que surjan falsos expertos que se aprovechen de la situación y del desconocimiento de las empresas".

"Las ayudas europeas y el Kit Digital van a potenciar las inversiones. Cada empresa lo destinará a lo que más necesite, ya sea mejorar la web o la ciberseguridad, pero el gasto va a crecer porque tienen los medios para planteárselo"

FERNANDO CASARES, DISTRIBUTION MANAGER PARA SOPHOS IBERIA

Coincide con ella Francesc Núñez, que recuerda que el esfuerzo de su compañía "no ha estado solo en convertirnos en agentes digitalizadores, sino en explicar los pasos a las pymes y acompañarlas, porque hay mucho ruido alrededor. Es fundamental ayudarles a que tengan todo claro. El esfuerzo debe ser ese: comunicar y aclarar. Para el cliente es un poco confuso, aunque estamos en la primera fase, y todavía queda mucho por desarrollar. Seguimos atentos a cambios o modificaciones, para ayudar a las pymes y micropymes, porque realmente lo necesitan. Estas empresas van a incrementar la inversión, pero estas iniciativas van a ayudarles mucho y son muy necesarias, porque, además de la presión del negocio, es-

tán las obligaciones legales y de relación con la Administración".

Apunta Guillermo Fernández que esperamos que "los clientes aprovechen la confianza que ya tienen con los partners para no necesitar buscar otros agentes digitalizadores, pero lo cierto es que para ellos es un reto".

RETOS Y OPORTUNIDADES

Es en este aspecto, comenta Carlos Tortosa, "donde tenemos que hacer esfuerzos. Primero, clarificar qué podemos aportar, como fabricantes, a la propuesta del Kit Digital, y, después, formar al canal para que puedan asumir esta labor de agente digitalizador para que las pymes los vean como alguien de confianza que les ayude en todo el proceso. No se trata solo de nuestro producto, sino de formarles para que puedan ayudar a sus clientes".

Para Karina Miguel, "el canal se está especializando con servicios para el usuario, y éste necesita confiar en el partner, porque no tiene claro cómo solicitar los fondos, dado que hay demasiada información, y el socio debe ofrecerles lo que ellos necesitan".

En palabras de Aitor Jerez, "las pequeñas empresas están apostando por áreas como el e-commerce o la seguridad, pero nosotros nos dirigimos a una pyme algo diferente, con unos servicios que tienen un encaje complicado en estas ayudas. Nos obliga mucho en nuestra forma de vender convertirnos en agentes digi-

"El incremento de inversión en ciberseguridad depende de la concienciación de cada empresa o del sector en el que se mueve, pero, en líneas generales, la tendencia es al alza"

GUILLERMO FERNÁNDEZ, MANAGER SALES ENGINEERING IBERIA EN WATCHGUARD TECHNOLOGIES

Seguridad inteligente, de forma fácil

WatchGuard

La seguridad y la complejidad son enemigas, y ahora los ataques son más complejos. Esto requiere de más herramientas y deriva en confusión para los clientes, incapacidad para conocerlo todo y en errores de configuración. La propuesta de WatchGuard es seguir ofreciendo un portfolio de seguridad integral y simplificado a través de una plataforma centralizada, a la que denominamos Unified Security Platform (USP). Esta plataforma resume nuestro lema: "Seguridad inteligente, de forma fácil": entregamos una plataforma unificada focalizada en los proveedores de ciberseguridad gestionada (MSP/MSSP) para simplificar, centralizar y automatizar la entrega de estos servicios de seguridad. Se trata de una propuesta disruptiva para ofrecer seguridad de última generación, pero de forma fácil y sencilla.

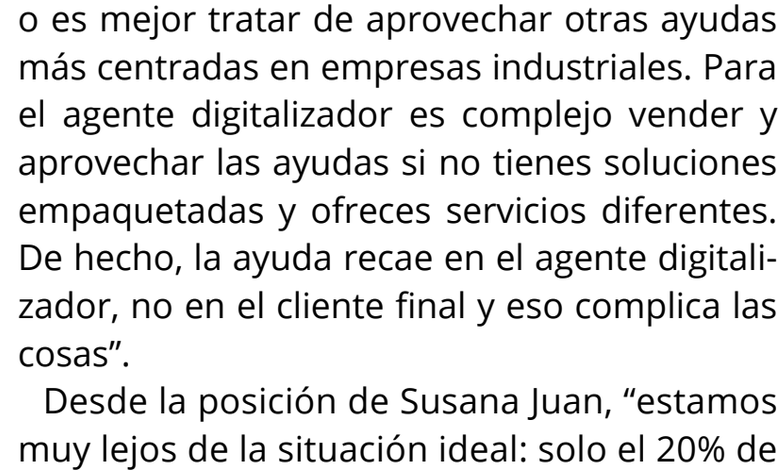
Así, ayudamos a las empresas a elevar y ampliar su seguridad al tiempo que hacemos que la gestión sea más eficiente y la mitigación de riesgos más simple, gracias a la amplitud de nuestro portafolio, a la correlación entre las tecnologías y al enfoque de seguridad centrado en el usuario.

Unified Security Platform nos afianza como una compañía con un completo portafolio que se vertebra en torno a 4 líneas de negocio sólidas e integradas entre sí: seguridad de red, seguridad Wi-Fi, seguridad endpoint avanzada y seguridad para la protección de la identidad de los usuarios (autenticación multifactor -MFA-).

Con Unified Security Platform el resultado es una postura de seguridad más fuerte, escalable y fácil de manejar.

talizadores, y no tenemos claro si tiene sentido o es mejor tratar de aprovechar otras ayudas más centradas en empresas industriales. Para el agente digitalizador es complejo vender y aprovechar las ayudas si no tienes soluciones empaquetadas y ofreces servicios diferentes. De hecho, la ayuda recae en el agente digitalizador, no en el cliente final y eso complica las cosas".

Desde la posición de Susana Juan, "estamos muy lejos de la situación ideal: solo el 20% de las pymes tiene página web, y el 60% se decanta por invertir las ayudas en la creación de una. Lo mismo pasa con la ciberseguridad, porque tenemos casi 40.000 ataques diarios en España, la mayoría contra pymes, y prevenir estas situaciones es esencial para la supervivencia del negocio. De ahí que creamos que el grueso de la demanda va a estar en crear páginas web, sistemas de e-commerce y ciberseguridad". ■



"Las empresas van a incrementar la inversión, pero las ayudas son muy necesarias porque, además de la presión del negocio, están las obligaciones legales y de relación con la Administración"

FRANCESC NÚÑEZ, ERP PRODUCT MANAGER DE WOLTERS KLUWER TAX & ACCOUNTING ESPAÑA

MÁS INFORMACIÓN

La digitalización de la pyme española, a debate

Wolters Kluwer, soluciones expertas para el profesional

Wolters Kluwer

Wolters Kluwer es la compañía líder mundial con más de 180 años de historia en el desarrollo de soluciones para los profesionales de despachos y empresas. Son soluciones expertas y especializadas en los ámbitos fiscal, contable, laboral y de gestión que mejoran la productividad y competitividad de los negocios.

Con unos ingresos anuales de 4.771 millones de euros (2021), Wolters Kluwer atiende a clientes en más de 180 países, mantiene operaciones en más de 40 países y emplea aproximadamente a 19.800 personas en todo el mundo.

En España, desde hace más de 35 años, Wolters Kluwer es la única compañía que ofrece soluciones integrales de software de gestión, información y servicios a despachos profesionales, pymes y departamentos de Recursos Humanos.

El liderazgo local y global de la División Tax & Accounting nos permite acompañar a nuestros clientes en la transformación de sus negocios para hacerlos más eficientes y competitivos a través de soluciones que combinan el conocimiento más especializado, la tecnología más innovadora y los servicios más avanzados.

Nuestras soluciones favorecen el trabajo colaborativo entre el despacho profesional y las empresas para mejorar sus relaciones y la gestión de sus negocios. a3innuva es la máxima expresión de este modelo: nuestra suite de soluciones online para despachos profesionales y empresas que proporciona un entorno de trabajo colaborativo a los asesores y sus clientes con el objetivo de mejorar la eficiencia de sus negocios con todas las ventajas y la seguridad de la nube.

NO SOLO it

PANEL DE EXPERTOS

MARKETING Y CONSUMO

Protección de derechos personales y neurotecnología

José Manuel Navarro,
CMO MOMO Group

CIBERSEGURIDAD 4.0

El Amanecer de la Humanidad Digital VIII: cómo los Ciudadanos Digitales superaron la oscura década de los 20

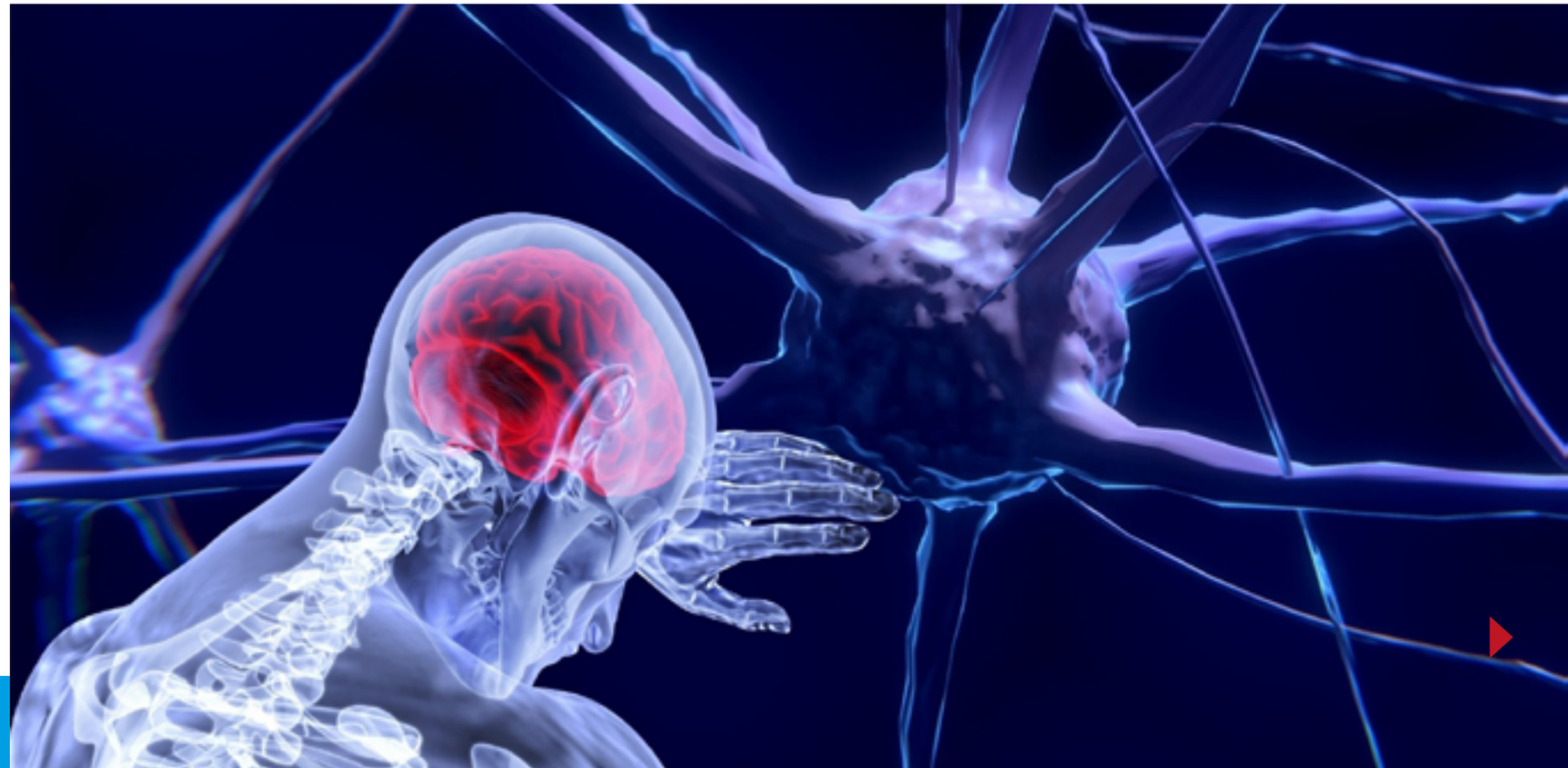
Mario Velarde Bleichner,
Gurú en CiberSeguridad

Protección de derechos personales y neurotecnología

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).

Mientras escribo estas líneas, la revista Nature Communications publica el estudio clínico llevado a cabo por investigadores del Centro Wyss de Bioingeniería y Neuroingeniería, en colaboración con la Universidad de Tubinga (Alemania), con el que han conseguido que una persona de 30 años con parálisis completa, derivada de una esclerosis lateral amiotrófica (ELA) avanzada, se comunique gracias a la implantación de 64 microelectrodos en su corteza motora primaria y a una interfaz cerebro-ordenador (BCI). El paciente moduló las tasas de activación neuronal en función de la retroalimentación auditiva y usó esta estrategia para seleccionar letras una a una que le permitieron formar palabras y frases para comunicar sus necesidades y experiencias. Estos resultados dan esperanza a las personas que están completamente aisladas a causa de



enfermedades neurodegenerativas progresivas para crear un canal de comunicación que les devuelva la facultad de expresarse.

Pero también, como manifiesta el equipo de investigadores que ha llevado a cabo el experimento clínico, éste avala las bases para avanzar en la decodificación del lenguaje directamente desde el cerebro de una persona durante el proceso de habla imaginada. Esto no solo permitiría tener una comunicación más fluida con pacientes que sufran un bloqueo total o síndrome de enclaustramiento completo (CLIS), una parálisis motora general empero con capacidades cognitivas y emocionales intactas, sino que además podría suponer el principio para poder acceder a otras funciones cerebrales más complejas como son el pensamiento, los sentimientos o la anticipación de la toma de decisiones.

Este tipo progresos tecnológicos realizados en centros científicos, públicos o privados, y bajo la premisa de ayudar a mejorar las condiciones de vida de pacientes con ciertos trastornos neurológicos que se traducen en discapacidades motoras o cognitivas, merecen todo el reconocimiento y el apoyo necesario para culminar con éxito el objetivo de integrar sistemas electrónicos en la red neuronal mediante BCI que asuman el papel de las funciones o las regiones lesionadas o deterioradas. Que una persona con ELA pueda comunicarse, un paciente con Parkinson pueda controlar los episodios de temblores y la disfunción de sus movimientos o un parapléjico pueda volver a caminar, son algunos de los ejemplos que han sido fruto del interés científico por cumplir con sus principios deontológicos de combatir la enfermedad, procurar el bien del paciente, evitar dañar y actuar con generosidad aún a riesgo de su vida o de sus intereses personales.

Pero ¿qué puede suceder cuando esta tecnología no se desarrolla en el ámbito sanitario sino en el de empresas privadas con socios que exigen reparto de beneficios cada ejercicio? Tomemos como ejemplo Neuralink, la compañía de Elon Musk creada para desarrollar BCI que conecten nuestros cerebros a sistemas inteligentes para, en principio, ayudar a personas con discapacidad para que puedan recuperar algunas de las habilidades o funciones perdidas a través del control mental de ordenadores y dispositivos móviles. La aspiración de conectar la inteligencia biológica con la artificial, de lograrse satisfactoriamente, permitirá no solo restaurar disfunciones motrices y sensoriales, sino que será el paso para expandir nuestras capacidades cognitivas y aventurar un nuevo mundo de múltiples interacciones interpersonales (brainet) y persona-má-

No se trata de obtener datos e información de comportamiento de compra, de preferencias, de respuestas emocionales o de tendencias ideológicas, sino de acceder a la identidad personal más íntima, que es la integridad psicológica, el pensamiento y la conciencia

quina, y de oportunidades para mejorar la raza humana. Estos avances, a cargo de una empresa privada que deba responder a las compañías y fondos de inversión que aportaron el capital privado para llevarlos a cabo, ¿tendrían que ser vigilados para no caer en el riesgo de servir para otros propósitos más allá de los sanitarios?

Avances tecnológicos como por ejemplo los teléfonos inteligentes, las redes sociales o las plataformas de comercio electrónico, han pasado de ser instrumentos para comunicarse o hacer más fácil la vida de sus usuarios a ser fuente inagotable de datos para que grandes corporaciones puedan predecir y condicionar la conducta de miles de millones de personas. De manera análoga, neurocientíficos de todo el mundo ya han advertido de la posibilidad de que, en un plazo de dos décadas, los desarrollos descritos en los párrafos precedentes puedan convertirse en sistemas inteligentes para poder manipular los circuitos cerebrales, por lo que gobiernos y juristas deberían empezar a pensar en la legislación básica que proteja a los ciudadanos de esos avances enmascarados en soluciones médicas.

No se trata de obtener datos e información de comportamiento de compra, de preferencias, de respuestas emocionales o de tendencias ideológicas, sino de acceder a la identidad personal más íntima, que es la integridad psicológica, el pensamiento y la conciencia. Si contamos con una legislación sobre protección de datos personales, habrá que avanzar en los derechos de las personas para que, por un lado, no se pueda manipular su "yo" cuando se le implanten electrodos con cualquier finalidad médica ni queden registros de su actividad cerebral para monitorizar cómo se organizan las respuestas neuronales frente a estímulos externos e internos. E igualmente, no se debería aplicar esa tecnología para mejorar substancialmente las capacidades cognitivas de personas sanas para crear diferentes clases de humanos.

Aunque hay neurocientíficos, como M. Nicolelis, pioneros en la codificación de poblaciones neuronales , BCI y neuroprótesis, que también son defensores de la imposibilidad de poder acceder a los complejos e intrincados mecanismos que son ejecutados por grupos de cientos de millones de neuronas, de miles de millones de interconexiones entre ellas y de millones de células gliales encargadas de darles soporte y también de realizar algunas funciones conectoras, ya que los procesos que regulan no son codificados por estructuras estáticas sino enormemente variables. Esta propiedad, denominada plasticidad, eleva a un número tan extremadamente alto de posibles combinaciones de conexiones que supera a las que pueda realizar cualquier máquina actual, y con un consumo de energía que no llega al que tiene una bombilla de 20 vatios.

No obstante existan estas cautelas, recordemos el conocido dilema de Collindridge: siempre que nos enfrentamos a la implantación de

un nuevo avance tecnológico, no somos capaces de evaluar las consecuencias sociales que puede llegar a tener; y cuando detectamos posibles efectos negativos, su uso está tan arraigado que es complejo controlarlo o impedirlo. Es decir, nadie elucubró que un teléfono móvil pudiera convertirse en un dispositivo que generase tal adicción en su uso, que las redes sociales pudieran servir de fuente de datos para personalizar ofertas comerciales y argumentos ideológicos, que la biometría como método para securizar operaciones garantizando la identidad del usuario se transformara en mecanismo de control ciudadano...

Frente a este dilema, está quien contrapone el principio de precaución, ampliamente aplicado en el derecho internacional medioambiental, que (extrapolándolo) defiende que hasta que no se demuestre fehacientemente que ciertos avances tecnológicos no causan perjuicio alguno a individuos o colectivos, debe limitarse o prohibirse su aplicación. Llegar a ese extremo, seguramente limitaría la capacidad innovadora de muchos desarrolladores, por lo que los defensores del desarrollismo tecnológico pedirían un período de carencia para legislar mientras se encuentra una prueba de seguridad consistente o evidencia irrefutable de perjuicio.

Realmente es una situación compleja de afrontar, aunque la experiencia corrobora que las leyes han ido siempre detrás de las innovaciones y tendencias sociales, culturales, tecnológicas, etc. Sin embargo, en el ámbito de la neurociencia, por ejemplo, no se debería esperar a evidenciar malas praxis para proteger el derecho de los ciudadanos a decidir el acceso a su "intimidad cognitiva", con independencia de que acepten el implante de "neurochips" para cuestiones médicas. Abordar la protección de esos derechos no es solo una cuestión jurídica, sino también ética que debe afrontarse con urgencia. En España, algo se ha avanzado en el apartado XXIV de la Carta de Derechos Digitales redactada el año pasado tomando como base las propuestas de la plataforma Neuro Right Initiative, en la que se ha recogido:

- **(I)** el derecho a la privacidad mental para garantizar que la actividad del cerebro no sea descifrada sin consentimiento expreso:
- **(II)** el derecho a la identidad psicológica para evitar que la personalidad sea manipulada;
- **(III)** el derecho al libre albedrío para no influir en los procesos de toma de decisiones;
- **(IV)** derecho a la igualdad de oportunidades para evitar le mejora cognitiva de determinadas personas en detrimento de otras;
- **(V)** el derecho a ser consciente de los efectos que puede tener la implantación de neurotecnologías y la aplicación de programas o

Es necesario promover también la ampliación del juramento hipocrático que realizan los médicos a los científicos especializados en neurotecnologia, para asegurar la finalidad de los ensayos clínicos bajo el paraguas de unos principios deontológicos comunes

algoritmos que pudieran llevar incorporados sesgos cognitivos.

Siendo estos principios bienvenidos para, al menos, definir el marco legal sobre el que trabajar, dado que la neurociencia lleva más de tres lustros investigando soluciones tecnológicas para, con métodos invasivos o no invasivos, encontrar soluciones a problemas neurodegenerativos o importantes lesiones, lo que ya es apremiante es la regulación jurídica y ética con naturaleza de ley que bloquee las pretensiones de cualquier empresa de aprovechar la neurotecnología para obtener beneficios a partir de la explotación de información inherente a la actividad cerebral de los pacientes. En primera instancia, porque no olvidemos el futurible de conectar a personas con máquinas para elevar sus capacidades intelectuales, motoras o sensoriales. En segundo lugar, habrá que prever igualmente cómo prevenir el uso de tecnologías no invasivas que puedan extraer esa información de manera coercitiva o no consentida, que puedan ejercer el llamado neurohacking o la manipulación de la percepción o de la memoria.

Tranquiliza saber que, además del gobierno de España, la OCDE lanzó en 2019 una recomendación sobre innovación responsable en neurotecnología, que el Consejo de Europa ha creado el Plan de Acción Estratégica centrado en derechos humanos y nuevas tecnologías biomédicas y que la ONU pretende promover en 2023 una modificación de la Declaración de los Derechos Humanos que recoja estas inquietudes. No obstante, es necesario promover también la ampliación del juramento hipocrático que realizan los médicos a los científicos especializados en neurotecnologia, para asegurar la finalidad de los ensayos clínicos bajo el paraguas de unos principios deontológicos comunes que limiten el espacio de investigación de lo que será la cuarta revolución industrial (4.0), en la que convergirán tecnologías digitales, físicas y neurobiológicas.

Legislación, normativa ética, compromiso científico, voluntad política y conciencia social serán las claves para que los derechos de los ciudadanos, en materia de protección de la información de su actividad neuronal, no sean vulnerados, y para que los desarrollos tecnológicos no se vean abocados a cumplir el principio de Skolnikoff, es decir, que terminen siendo utilizados para otros propósitos diferentes para los que originalmente fueron creados. ■

MÁS INFORMACIÓN

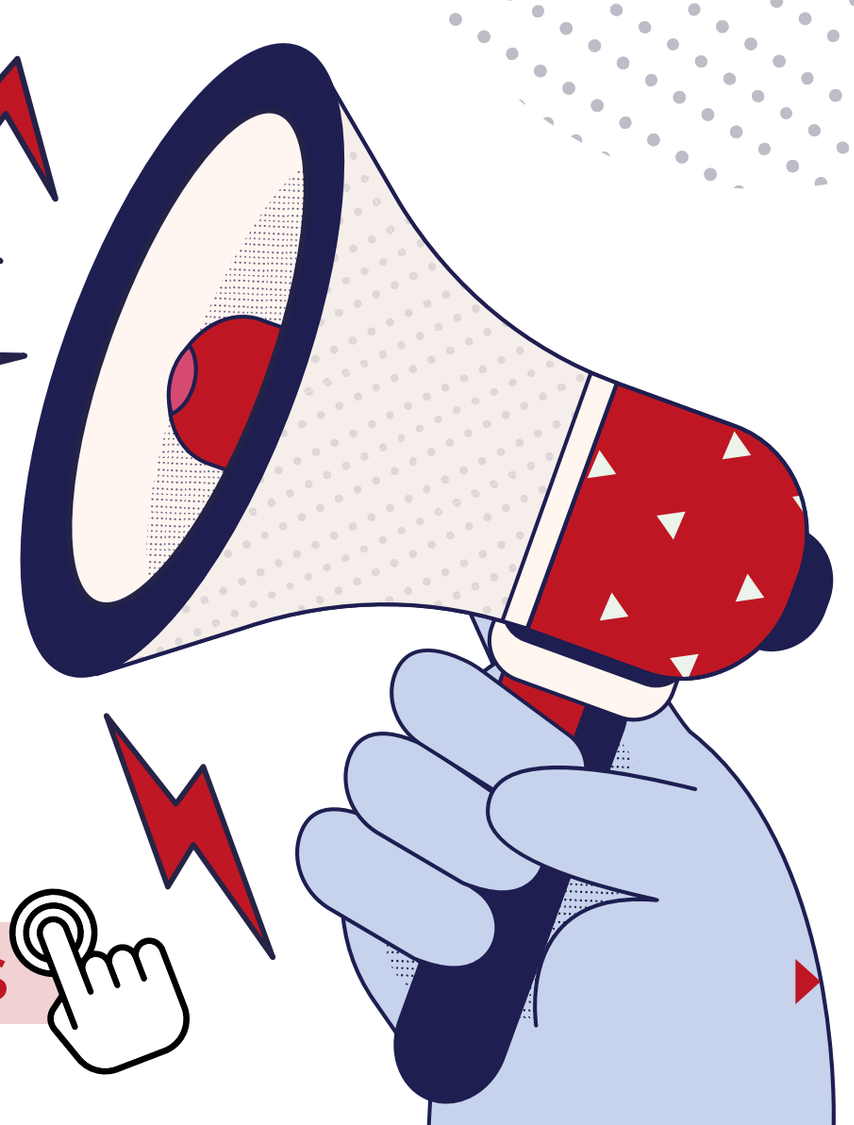
- Derechos de los ciudadanos
- Estudio clínico revista Nature Communications
- El principio de precaución
- Carta de Derechos Digitales
- Plataforma Neuro Right Initiative

Administración Pública Digital

NUEVA WEB

¡VISÍTANOS!

www.administracionpublicadigital.es



El Amanecer de la Humanidad Digital VIII: cómo los Ciudadanos Digitales superaron la oscura década de los 20

En los primeros días del siglo XXII, el Gobierno Digital del Paneta Tierra puso en marcha los actos de reconocimiento a los primeros ciudadanos digitales que durante los difíciles años de la década de los años 20 mantuvieron vivos los avances de las tecnologías digitales a pesar de los acontecimientos que pusieron en peligro el avance de la incipiente Humanidad Digital.

Está ya en la historia la primera pandemia de la era digital, Covid19, que afectó al vibrante avance de la Globalización Digital de las dos primeras décadas del siglo XXI de una manera brutal e inesperada, y que en los tres primeros meses del año 2020 produjo una prácticamente total paralización de la economía en todo el planeta y a toda la humanidad.

Curiosamente, en los más de dos años que duró la pandemia, con fortísimos aislamientos entre las naciones, la práctica desaparición de la movilidad de los primeros ciudadanos digitales confinados durante largos meses, ya no solamente dentro de sus países sino incluso dentro

Mario Velarde Bleichner

Gurú en CiberSeguridad

Con más de 20 años en el sector de la Ciberseguridad, Mario Velarde Bleichner, Licenciado en Ciencias Físicas con especialidad en Calculo Automático y PDG por el IESE, ha participado en el desarrollo de esta industria desde la época del antivirus y el firewall como paradigma de la Seguridad IT, dirigiendo empresas como Trend Micro, Ironport, Websense, la división de Seguridad de Cisco Sur de Europa y la división Internacional de Panda Software.

de las ciudades o barrios de ciudades, tuvo lugar uno de los períodos de mayor y más rápido desarrollo de los fundamentos de las nuevas sociedades digitales.

En esta situación de confinamientos, donde la comunicación prácticamente de casi todos los tipos, social, laboral, política... pasó a ser virtual (digital), fueron los sistemas digitales los que permitieron la continuidad de la sociedad y la economía; se produjo un cambio en los hábitos de los Ciudadanos que tuvo un impacto en el futuro desarrollo de las nuevas sociedades digitales en décadas posteriores.

La combinación del desarrollo rapidísimo de vacunas que, por su propia génesis de urgencia no fueron tan eficaces como hubiera sido de desear, y la también rápida mutación del virus a una mayor capacidad de contagio, pero a la vez a una menor virulencia, hicieron que esta pandemia quedara limitada en el tiempo y, aunque produjo graves daños a la economía global, no llego a producir efectos los catastróficos en la economía mundial que se pronosticaban si la pandemia hubiera durado 5 o más años.

El estado del avance de las tecnologías digitales de comunicación en 2020 permitió que muchos segmentos de la sociedad pudieran continuar funcionando a pesar de los durísimos confinamientos; así, por ejemplo, la educación se demostró que podría realizarse de forma remota completamente, el teletrabajo alcanzo sus máximos niveles, la telemedicina masiva dio sus primeros pasos, las finanzas siguieron funcionando de manera remota, y las Administraciones Publicas descubrieron, por fin, que podrían funcionar online y, mejorando los procesos con tecnologías digitales, dar servicio a los ciudadanos digitales sin pasar por ventanillas ni hacer grandes colas. Creo que no quedó casi nada sin recibir el beneficio de los modelos digitales como respuesta a una situación de emergencia mundial.

Pero la década de los 20, que en sus dos primeros años había avanzado tanto en el desarrollo de la Sociedad Digital con el sacrificio y dolor que produjo la pandemia, se encontró con una situación inesperada de conflicto entre ideologías caducas del siglo XX que seguían activas, en especial los nacionalismos trasnochados que desataron una guerra en el corazón de Europa que produjo graves perturbaciones en el nacimiento de la Humanidad Digital.

La disponibilidad de sistemas digitales, especialmente móviles, para la mayoría de la población mundial empezaba a igualar a los ciudadanos digitalizados independientemente de las diferencias geográficas, regionales, nacionales, idiomáticas, políticas, económicas; se había iniciado la disrupción digital más importante del avance hacia la humanidad digital: por primera vez en la historia de la humanidad la información disponible a todos los ciudadanos del planeta tierra era la misma y la participación en los avances digitales estaba a disposición de toda la humanidad.

Lamentablemente, el agrietamiento de la globalización producido por la guerra en Europa dio lugar al fenómeno de la aparición de islas separadas de información en el modelo de Dictaduras Digitales que aislaban a sus respectivas poblaciones para que solo pudieran recibir información dictada por los líderes de los diferentes países o grupos de países implicados en este conflicto.

Pero, felizmente, el avance de las comunicaciones globales había ya superado las limitaciones nacionales de comunicación física y entrabamos ya en el incipiente establecimiento de redes de comunicaciones digitales personales directamente desde satélites que escapaban al control de los líderes de los países y que, a finales esta década de los años 20, estableció por fin unos de los derechos primordiales de la nueva Humanidad Digital que es el derecho al acceso libre para todos y cada uno de los ciudadanos digitales.

Por supuesto, siempre puede haber una excepción, y en este caso fue Corea del Norte que, no solo actuaba como Dictadura Digital, sino que había sumido a su población en tal grado de eliminación de derechos individuales que fue ya en la década de los 30 el último país donde consiguie-

ron la libertad y fueron recibidos con júbilo en la nueva Humanidad Digital.

La Guerra de 2022, además de las explicaciones políticas que se transmitieron a la población mundial, tenía una profunda motivación en los procesos de transición energética que apoyados en las tecnologías digitales daban sus primeros pasos hacia el abandono de los combustibles fósiles y su sustitución por energías renovables con la consecuente mejora de la ecología y bienestar de los ciudadanos digitales del futuro.

Los combustibles fósiles aun necesarios en esos momentos, sufrieron una especulación brutal multiplicando sus precios de manera artificial en un último esfuerzo de enriquecimiento con energías obsoletas y dañinas, claramente rechazadas ya por la población mundial.

La parte buena de esta crisis energética artificial, en absoluto producida por una demanda excesiva o una oferta insuficiente, puesto que se había determinado que las reservas de petróleo y gas mundiales no serían necesarias, es que la transición energética se aceleró y llego a buen puerto muchos años antes de las predicciones más optimistas. Fue cuando todos los ciudadanos digitales comprendieron que la transición a energías renovables era buena para el planeta, independientemente de dónde quedaran las reservas inutilizadas de los combustibles fósiles haciendo cierta esa frase premonitoria cuando aún se temía el fin de la civilización por haber consumido todos los combustibles fósiles del planeta. "La Humanidad no dejara de usar combustibles fósiles porque se acaben, lo hará porque ya no serán necesarios y permanecerán para siempre en las entrañas de la tierra".

Solamente estos dos eventos graves del inicio de la década de los 20, la Pandemia y la Guerra provocaron una gran convulsión en el desarrollo de la Humanidad que en épocas previas al Desarrollo Digital alcanzado en estas fecha hubieran causado un retroceso que hubiera requerido varias décadas para recuperar solamente el nivel previo a estos eventos.

Sin embargo, la aceleración en los avances tecnológicos sobre la base de la digitalización en todos los ámbitos de la actividad humana no solamente no se ralentizo, sino que se incrementó más aun al mismo ritmo que el porcentaje de que los Humanos Digitales Nativos iba creciendo de forma natural hasta ser una mayoría solo tres décadas más adelante.

Por eso en la realidad digital del principio del siglo XXII, donde toda la Humanidad ya es Digital Nativa, se recuerdan aquellas situaciones que parecía que ponían en peligro el futuro de la especie Humana Digital y que, sin embargo, gracias a la resiliencia de esas generaciones pasadas, como la de la década de los 20, hicieron posible esa nueva Sociedad Digital fuera un paso más en la gran aventura de la Evolución Humana. ■

En esta situación de confinamientos, donde la comunicación prácticamente de casi todos los tipos, social, laboral, política... pasó a ser virtual (digital), fueron los sistemas digitales los que permitieron la continuidad de la sociedad y la economía

MÁS INFORMACIÓN

- Cómo afecta la invasión rusa de Ucrania al sector TI
- La pandemia ha provocado cambios tecnológicos en el 47,2% de las empresas
- 2020, el año de la normalización de la digitalización en la sociedad española

it Reseller
TECH&CONSULTING

Cada mes en la revista,
cada día en la web.