

# ¿Se puede conseguir un entorno ciberseguro?



- Los principales riesgos para las empresas
- La nube, cada vez más segura
- La realidad del CISO

## Mejorar la colaboración entre equipos

## Las AA.PP. se apuntan a mejorar la relación con el ciudadano

# econocloud

WE   
YOU

**Backup &  
Disaster Recovery**  
para la continuidad  
de tu negocio

**¿Estás preparado para afrontar una  
caída de servicio o un ciberataque?**

Seguro que ya tienes tu Backup, pero  
ahora es posible recuperar en minutos  
lo que antes se tardaba días.

En **Econocloud**, la nube de confianza de Grupo Econocom, garantizamos la disponibilidad de su negocio. Tenemos **Disaster Recovery Services & Backup** para darte cobertura desde nuestros *data centers* en Madrid, Barcelona y Marsella, con la última tecnología y las máximas garantías.

**Descubre qué podemos hacer para ti desde Econocloud,  
la nube de confianza de Grupo Econocom:**

[hola@econocloud.es](mailto:hola@econocloud.es) | T. 900 800 297 | [www.econocloud.es](http://www.econocloud.es)

# econocom

# Las TIC como ejemplo sostenible



Manuel Navarro Ruiz  
Director de BYTE TI

**E**ste próximo sábado, 5 de Junio, se celebra el Día Mundial del Medio Ambiente. Al igual que ocurre con los antivacunas o los terraplanistas son ya muy pocos los que nieguen las consecuencias que vamos a sufrir por culpa del cambio climático y que todos ya estamos viendo. Incluso el Congreso de los Diputados, tan dado al choque de trenes, aprobó el pasado mes de Abril la Ley de Cambio Climático con el apoyo o la abstención de la totalidad de los grupos, salvo los negociacionistas de VOX a los que el verde sólo les gusta como logotipo.

El cambio climático es el mayor reto al que nos enfrentamos en la historia de la Humanidad. Sólo nosotros somos responsables del deterioro del Planeta y puede que lleguemos tarde para frenarlo, pero hay que intentarlo. Los países desarrollados tenemos la obligación de frenar este problema, aunque queda todavía mucho camino por recorrer.

Y en la posible resolución de este problema, el sector tecnológico juega el principal papel. La tecnología es un aliado que va a ayudar a poner algo más que un granito de arena en su compromiso por la sostenibilidad.

De hecho, este sector lleva años trabajando en pos de la mejora medioambiental. Las empresas que conforman este sector fueron de las primeras en incorporar la reducción de emisiones en sus políticas. También fueron unas de las que lideraron la que hoy se denomina como economía circular: muchas de ellas ya desarrollaron iniciativas para reciclar los componentes de sus equipos. En algunos casos, incluso pagando al usuario por ese reciclaje. Acuérdense de la política de sostenibilidad de Nokia hace ya 20 años.

Además, también han sido pioneras en el uso de materiales provenientes del reciclado para la fabricación de sus equipos, en reducir el plástico de sus embalajes y sustituirlos por materiales más sostenibles... La lista de iniciativas es larga y antigua.

Pero incluso en este sector TIC, todavía queda mucho por hacer. Algunos de los principales problemas tienen que ver con los minerales que han de ser extraídos en dudosas condiciones tanto humanas como medioambientales para poder fabricar equipos o dejar de prestar tanta atención a populistas corporativos como Elon Musk que se benefician de un pseudo activismo “verde” para incrementar los ceros de su cuenta corriente. Los CIOs, por su parte, han descubierto que además de mejorar el Planeta, la sostenibilidad les ofrece ahorros de costes y mejores ratios de productividad. Fomentar el teletrabajo o migrar a la nube es hoy, más necesario que nunca.

Por eso, les invito este próximo día 4 de junio a las 10:00, al webinar que sobre sostenibilidad organizamos en Byte TI y que mostrará qué están haciendo los CIOs en materia de sostenibilidad en sus empresas.

# SUMARIO



TEMA DE PORTADA

# Los retos de la ciberseguridad

44

N.º 294 • ÉPOCA IV

**MKM PUBLICACIONES**  
Managing Director

Ignacio Sáez (nachosaez@mkm-pi.com)

**BYTE TI**  
Director

Manuel Navarro (mnavarro@mkm-pi.com)

**Redacción**

Vanesa García (vgarcia@revistabyte.es)

**Coordinador Técnico**  
Javier Palazon

**Colaboradores**

S. Velasco, R.de Miguel, I. Pajuelo, O. González, M.López, F. Jofre, A. Moreno, MªJ. Recio, J.J. Flechoso, J. Hermoso, A. López, C. Hernández.

**Fotógrafos**

E. Fidalgo, S. Cogolludo,

**Ilustración de portada**  
Javier López Sáez

**Diseño y maquetación**

El Palíndromo Comunicación S.L.

**WebMaster**

NEXICA  
www.nexica.es

**REDACCIÓN**

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

**PUBLICIDAD**

Directora comercial: Isabel Gallego  
(igallego@mkm-pi.com)

Tel.: 91 632 38 27

Rocío de Castro (rdecastro@mkm-pi.com)

**DEPARTAMENTO DE SUSCRIPCIONES**

Tel. 91 632 38 27

Fax.: 91 633 25 64

e-mail: suscripciones@mkm-pi.com

Precio de este ejemplar: 5,75 euros

Precio para Canarias, Ceuta y Melilla:

5,75 euros (incluye transporte)

**Impresión**

Gráficas Monterreina

**Distribución**

DISPAÑA

Revista mensual de informática

ISSN: 1135-0407

**Depósito legal**

B-6875/95

© Reservados todos los derechos

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

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

JUNIO de 2021  
Printed in Spain



**EDITA**

Publicaciones Informáticas MKM

## ACTUALIDAD DEL MES

6



## COMPARATIVA

36



## TENDENCIAS

60



3 CARTA DEL DIRECTOR

6 ACTUALIDAD

18 WEBINARS BYTE TI

34 ANÁLISIS

36 COMPARATIVA

44 TEMA DE PORTADA

54 UN CIO EN 20 LÍNEAS

56 MUJERES TIC

58 LEGALIDAD TIC

60 TENDENCIAS

64 ENTREVISTA

66 CIBERCOTIZANTE

# La industria y los profesionales TIC se unen en ASLAN HYBRID



El Congreso ASLAN HYBRID 2021 ha superado la barrera de los 3.500 profesionales inscritos y se acerca al objetivo marcado para la 28ª edición del evento más importante del sector tecnológico profesional que se celebra en España.

Por Manuel Navarro

El acto de inauguración contará con la presencia de Miguel Ángel García Martín, Viceconsejero de Presidencia y Transformación Digital de la Comunidad de Madrid y Fernando de Pablo, Director General de la Oficina Digital del Ayuntamiento de Madrid. También será presencial con aforo limitado la tradicional ceremonia de entrega de los Galardones de los Premios @aslan a directivos y mejores casos de éxito de las AA.PP., a los que se han presentado cerca de un centenar de proyectos.

La Asociación @aslan, que agrupa y representa cerca de 140 empresas tecnológicas y aglutina un amplio ecosistema de innovación, ha conseguido sumar este año un 55% más de empresas patrocinadoras respecto a la edición anterior, demostrando el interés y apoyo que este evento suscita en el sector tecnológico. Una industria estratégica para la recuperación económica no solo en España, también en el resto del mundo.

Administraciones Públicas, Sectores Clave y PYME Este año ASLAN HYBRID congregará 114 ponentes en un amplio programa de conferencias donde destacan los

dos encuentros de expertos en Tecnologías, uno enfocado en la Administración Pública y otro en Sectores Clave.

## APERTURA

La sesión de apertura del IV Encuentro Anual Nacional de Expertos en Tecnologías en la Administración Pública correrá a cargo de Santiago Graña Domínguez, Subdirector General de Impulso de la Admón. Digital y Servicios al Ciudadano del Ministerio de Asuntos Económicos y Transformación Digital. En este foro participarán además los responsables de innovación, tecnología y digitalización de: Ministerio de Industria, Comercio y Turismo; Ministerio de la Presidencia; Ministerio del Interior; Seguridad Social; SEPE; Agencia para la Administración Digital de la Comunidad de Madrid; Centro Criptológico Nacional; los Ayuntamientos de Málaga, Madrid y Barcelona; la Sociedad Provincial de Informática; el Servicio Madrileño de Salud; Hospital 12 de Octubre; y Correos.

Por su parte, en el III Encuentro Anual Nacional de Expertos en Tecnologías en Sectores Clave destaca la Keynote de Miguel Ángel Ariño, Profesor del IESE Business School. Junto a él, los CIO y directores de TI de: AON; COFAS; Hospital Ribera Povisa; EVO Banco; Adecco Group; CELSA; Prisa; Editorial Santillana; Gilmar; Grupo IFA; Betapack; Faes Farma; y Nationale Nederlanden.

Además de estos encuentros, hay planificados dos foros dedicados a Cybersecurity&Data Management y a Cloud&Innovation, respectivamente; y conferencias dedicadas a cinco grandes áreas de innovación: Data Management, CyberSecurity, Cloud DataCenter, Digital Workspace e Intelligent Networks.

El cambio de paradigma al que ha obligado la pandemia ha demostrado la importancia de la tecnología para crear organizaciones más resilientes. ASLAN HYBRID quiere ofrecer este año una visión 360° de los avances en innovación tecnológica y ciberseguridad, incrementar el networking y acercarse a las necesidades de digitalización de las PYMES. Para ello, además del programa de conferencias, se han creado nuevos espacios digitales con los que superar las 3.000 interacciones de calidad entre profesionales y empresas participantes, como las reuniones de FastNetworking o los Business Spaces.

La edición de este año está patrocinada como Global Sponsors por AWS, Cambium Networks, Dell Technologies, ESET, HPE y NFON; como Event Sponsors hay que mencionar a Aruba, Citrix, Deutsche Telekom, Dynatrace, Fastly, Infinidat, Infoblox, Kaspersky, Micro Focus, Nutanix, OVHCloud, Qlik, Samsung, SAP, SonicWall, Sophos, Wildix, Winncom y Zaltor.

La Asociación @aslan cuenta con cerca de 140 empresas asociadas y un ecosistema de 73.500 profesionales con los que se impulsa un amplio Plan de Actividades anual. Además, forma parte del Consejo Nacional Consultivo para la Transformación Digital del Ministerio de Asuntos Económicos y Transformación Digital y a través de los Grupos de Expertos y Comisiones de Trabajo apoyará los distintos planes de Agenda Digital, infraestructuras, 5G, IA y PYMES puestos en marcha por el Gobierno de España.

# Sobresaliente

## ACOMTEC

Acaba de nacer ACOMTEC. Presidida por Fabián Gradolph, esta asociación desarrollará mecanismos de comunicación entre agencias, profesionales de empresas y periodistas, realizará eventos relacionales y facilitará la compartición de información a fin de analizar y promover las mejores prácticas en periodismo y comunicación tecnológica.

## LENOVO

Lenovo ha superado todos los registros. La multinacional china ha anunciado unos resultados de récord tanto para el cuarto trimestre como para el ejercicio fiscal, con un crecimiento extraordinario en todas las áreas del negocio. Durante este cuarto trimestre, los ingresos del Grupo aumentaron un 48% con respecto al ejercicio anterior, hasta los 15.600 millones de dólares.

# Suspense

## BITCOIN Y ELON MUSK

Bitcoin está sufriendo numerosos descensos y Elon Musk, al igual que tuvo culpa con sus apreciaciones, es bastante responsable de ello. No hay quien le acusa de lucrarse a costa de sus tuits en favor y en contra de la popular criptomoneda.

## ATAQUES DDOS

Según un estudio realizado por AKAMAI, los atacantes aceleran el ritmo y suben el listón en lo que se refiere a ciberataques DDOS. Solo en 2021, ya se han registrado más ataques de más de 50 Gbps (a fecha de 24 de marzo de 2021) que en todo 2019.

Además, los ataques DDoS son cada vez peores. Según el informe, tres de los seis peores ataques DDoS volumétricos que la compañía ha registrado y mitigado se han producido en los últimos dos meses, lo que da cuenta de su gravedad.

### LA OPINIÓN DE Fernando Jofre

## Seguridad avanzada

Aprovechando el lanzamiento de la iniciativa para reforzar la seguridad de dispositivos bajo la denominación HP Wolf Security, la compañía fabricante de hardware compartió detalles de un estudio titulado Blurred Lines & Blindspots, entre los que destaca que el volumen global de ciberataques ha aumentado un 238 % durante la Covid-19, de tal manera que los hackers se han centrado principalmente en atacar a los trabajadores remotos. ¿Alguien se sorprende? Me imagino que no...

El nivel de ataques dirigidos hacia dispositivos conectados a internet en todo el mundo ha sido tal, que se estiman en 1,5 ataques por minuto durante 2020. Y por esta razón, el 91% de los responsables de TI se han visto obligados a dedicarle más tiempo a asegurar los dispositivos que hace tan sólo dos años. Y ese mismo porcentaje señaló en el informe que la seguridad de los dispositivos se ha vuelto tan importante como la propia seguridad de la red. ¿Qué podemos hacer a este respecto? Pues la verdad es que iniciativas como la de HP están bastante bien orientadas. Porque incluyen funcionalidades y servicios tales como el firmware autorreparable, la detección de infracciones en memoria y la contención de amenazas a través de la virtualización... más concretamente la microvirtualización. Y cómo no, también aborda la inteligencia basada en la nube.

La cuestión básica es reducir lo que se conoce como la superficie de ataque, y con tecnologías que permitan recuperación en remoto de los dispositivos. Lo mejor de esta iniciativa de HP es que abarca tanto dispositivos de empresa como los de hogar. Porque no nos engañemos... Independientemente de que la empresa nos permita llevarnos el ordenador de la oficina a casa, es habitual utilizar también equipos domésticos para acceder a servicios online corporativos.

El nivel de ataques dirigidos hacia dispositivos conectados a internet en todo el mundo ha sido tal, que se estiman en 1,5 ataques por minuto durante 2020. Y por esta razón, el 91% de los responsables de TI se han visto obligados a dedicarle más tiempo a asegurar los dispositivos que hace tan sólo dos años. Y ese mismo porcentaje señaló en el informe que la seguridad de los dispositivos se ha vuelto tan importante como la propia seguridad de la red. ¿Qué podemos hacer a este respecto? Pues la verdad es que iniciativas como la de HP están bastante bien orientadas. Porque incluyen funcionalidades y servicios tales como el firmware autorreparable, la detección de infracciones en memoria y la contención de amenazas a través de la virtualización... más concretamente la microvirtualización. Y cómo no, también aborda la inteligencia basada en la nube.

## Globant premia a los líderes digitales



**G**lobant acaba de crear los Digital Disruptors Awards, un reconocimiento global para los profesionales que destacan y se esfuerzan en liderar el proceso de la digitalización a través de la innovación, aprovechando los datos, operando de manera ágil y adaptándose sin problemas a las nuevas realidades del mercado.

"Cada día son más las compañías que persiguen la transformación digital. De estas empresas, las que están lideradas por auténticos disruptores digitales son capaces de adaptarse al cambio más rápidamente. Con Digital Disruptors Awards, queremos reconocer a aquellos que han construido una cultura ágil, digital first, mezclando los mundos digitales y físicos para proporcionar una experiencia de usuario -consumidor o cliente-fluida", dijo Martín Migoya, CEO y cofundador de Globant.

"Para finales de 2021, Forrester espera que el 30% de las empresas del Global 2000 tengan una

cartera de productos digitales significativa", dijo Luis Ureta, Country General Manager de Globant en España "Aunque los datos muestran que estos cambios son muy necesarios, el 70% de los esfuerzos de transformación digital fracasan. Aquellas personas que lideran una transformación digital exitosa, y por lo tanto aportan crecimiento a sus negocios e industrias, merecen ser reconocidas y tener la oportunidad de destacar sus contribuciones".

El jurado global cuenta con líderes en la industria de la tecnología que han construido su carrera desafiando el statu quo, incluyendo a Donald Hicks, Vicepresidente de Políticas de Confianza y Programas de Airbnb; Linda Rottenberg, CEO y Co-fundadora de Endeavor; Diego Lerner, Presidente de Walt Disney Company Latin America; Europe & Asia; Sara Pastor, Sales Director de Twitch Spain; Manuel del Campo, CEO de Axel Springer & Business Insider España; Nuria Simo, CIO, Banco Interamericano de Desarrollo; y líderes del equipo directivo de Globant.

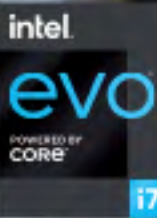




Smarter  
technology  
for all

Lenovo

Para los que nos  
gusta salirnos de lo convencional



Presentación de la plataforma Intel® Evo™  
Descubre más en [Lenovo.com/YOGA](https://www.lenovo.com/YOGA)

Una experiencia excepcional  
con tu portátil en cualquier lugar

Yoga Slim 9i  
Acabado en piel



 Windows 10

Basta con una simple mirada

YOGA  
for all of us

### LA OPINIÓN DE Manuel López

## TFO Are you ready?

Parece que por fin la vacunación masiva de la población conseguirá que vayamos hacia la normalidad en nuestras vidas.

Pero lo cierto es que como ocurre cuando hay grandes acontecimientos globales, nada será lo mismo. Nuestras vidas cambiarán probablemente para siempre.

Uno de los grandes cambios que nos ha traído la pandemia es el del modo de trabajar. La pandemia ha acelerado al máximo la digitalización de todo, pero en especial del modo de trabajo. A nadie se le escapa que el trabajo en la oficina tradicional no volverá a ser lo que era.

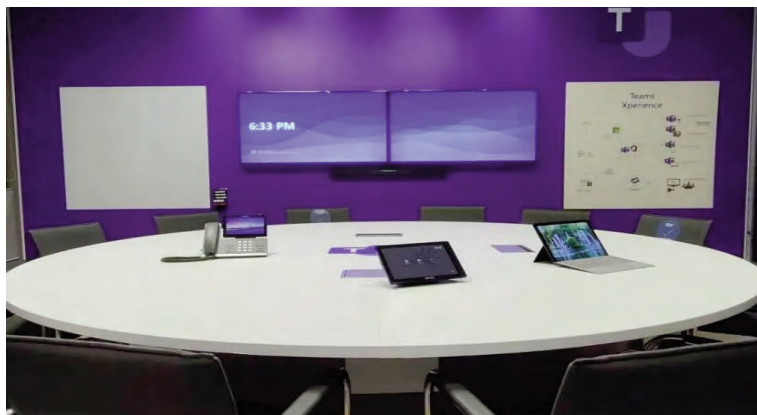
Lo hemos llamado de muchas formas, aunque la más habitual es “teletrabajo”, pero lo que sería más correcto es hablar de “trabajo fuera de la oficina” (TFO). No quiere esto decir que salgamos de la oficina para hacer cierto trabajo, sino que no volveremos a la oficina a trabajar o bien que el trabajo que antes hacíamos exclusivamente en la oficina, ahora lo haremos fuera de la oficina. Aunque parezca algo banal y sin más importancia que el uso masivo de la tecnología para trabajar, el cambio es mucho más profundo.

Con el TFO aparecerán nuevos modelos de negocio, se tambalearán otros tradicionales como el del mercado de espacios para oficina, será necesario definir nuevos modelos de gestión de recursos humanos y desde el punto de vista de los profesionales, tendremos primero que desaprender nuestros hábitos de trabajo, para reinventarnos en cuanto a la forma de crear valor, aprender, colaborar, debatir o aportar conocimiento.

Are you ready?



## Microsoft: el entorno laboral será híbrido



¿Qué ocurrirá tras el verano? ¿Seguiremos en un entorno laboral en el que el trabajo desde casa será permanente? ¿Volverán los trabajadores a las oficinas de forma permanente? En Microsoft creen que el futuro del entorno laboral será híbrido.

Microsoft quiere liderar también el entorno laboral de dentro de unos meses. Por eso, ha puesto a disposición de clientes y partners una completa experiencia inmersiva sobre las posibilidades que ofrece la plataforma Teams para la nueva forma de trabajar, que tiende hacia un modelo híbrido y colaborativo.

Los modelos tradicionales de trabajo se han tenido que transformar rápidamente. Hace tan solo un año, solo el 15% de las empresas contaba con una política de teletrabajo. En este contexto, a través de Teams Xperience, una innovadora sala, que Microsoft ha habilitado en sus oficinas de

Madrid y desde la que ofrece experiencias inmersivas y virtuales, con las que las organizaciones pueden explorar, tocar, vivir en primera persona, y en definitiva, descubrir todo el potencial del trabajo colaborativo y comprobar todas las posibilidades que la tecnología de comunicaciones unificadas de Microsoft y en concreto, Teams, les ofrece para tener éxito en este nuevo modelo de trabajo. Destacan las novedosas funcionalidades de reuniones avanzadas y de llamadas en Teams. Con Teams Xperience, se experimentan desde escenarios básicos de colaboración, comunicación a través de chat, compartición y edición de documentos, hasta capacidades de telefonía y audio conferencia, desde cualquier dispositivo dentro de Teams o funcionalidades de centralita en la nube. Además, se pueden explorar las capacidades que ofrece Teams para integrar todo tipo de aplicaciones dentro de la propia plataforma, desde aplicaciones de productividad.



# a3ERP

Solución integral de  
gestión para PYMES

## *La solución 360° que hace tu empresa más competitiva*

**a3ERP** te ofrece la visión global de todas las áreas de tu empresa de una forma ágil y sencilla, facilitando la toma de decisiones,  **aumentando la productividad** y contribuyendo así a  **hacer tu empresa más competitiva**.

**a3ERP**, la Solución integral de gestión que se adapta a las necesidades reales de tu empresa.

Infórmate  
y descubre  
como ser más  
competitivo



LA OPINIÓN DE  
José Joaquín Flechoso

### Internet de las personas

Actualmente no hay fenómeno más científico, cultural y político que Internet. La Agenda 2030 define que esta tecnología tiene “un gran potencial para acelerar el progreso humano” y una encuesta de la BBC confirma que el 87% de los usuarios consideran el acceso a Internet un derecho fundamental. Ciertamente no es un derecho humano como la libertad de expresión, pero para tutelar los derechos humanos, Internet es imprescindible.

A día de hoy y aunque sea inconcebible, en algunos países sigue habiendo censura en la Red. Aunque la mayoría de países permiten el uso de VPN, otros encuentran estos servicios indeseables e incluso ilegales. El 2019 fue el año con más bloqueos e interrupciones desde que existe la Red. Se produjeron un total de 122 cortes totales o parciales de Internet en más de 21 países, con una duración superior a las 18.000 horas.

Los gobiernos interrumpen o ralentizan Internet cuando se producen protestas continuadas para dificultar que los manifestantes se coordinen o convoquen nuevas acciones, a la vez que se evita la difusión de vídeos e imágenes que muestren la más que probable brutalidad policial. Para evitar estas situaciones, algunos gobiernos optan por impedir únicamente el acceso a las redes sociales y permitir la navegación normal en el resto de webs. Las plataformas más afectadas son WhatsApp, Facebook e Instagram, seguidas por Twitter y, en menor medida, YouTube.

En 2016, el Consejo de Derechos Humanos de las Naciones Unidas aprobó una resolución para la “promoción, protección y el disfrute de los derechos humanos en Internet” aprobando una resolución no vinculante, es decir, que ningún país está obligado a cumplir con esta resolución...



## Nueva edición del Foro Asesores



Wolters Kluwer ha anunciado que celebrará los próximos 9 y 10 de junio en formato online el Foro Asesores, el evento de referencia para el despacho profesional, donde analizarán la situación actual del sector y dará algunas claves para impulsar la recuperación económica.

El evento será inaugurado por la vicepresidenta tercera y ministra de Trabajo y Economía Social, Yolanda Díaz, el 9 de junio. Con la colaboración de Tomàs Font, Director General de Wolters Kluwer Tax & Accounting en España, y Claire Carter, EVP & Managing Director de Wolters Kluwer Tax & Accounting Europe.

Posteriormente intervendrán Oriol López, para dar a conocer los diferentes modelos de pricing que pueden ayudar al crecimiento de los despachos, y Félix Barrio, Gerente de Ciberseguridad para INCIBE, que explicará los puntos clave que

los despachos profesionales deben tener en cuenta en esta materia.

El primer día se cerrará con la parte más práctica centrada en la fiscalidad, con la participación de Valentí Pich, Presidente del Consejo General de Economistas, que hablará del papel de los economistas en los despachos profesionales.

Por su parte, Agustín Fernández, Presidente del REAF, analizará las más recientes novedades fiscales, y finalmente Jesús Gascón, Director de la Agencia Tributaria, que explicará los retos a los que se enfrenta la Administración Tributaria.

El jueves el Foro Asesores dedicará un primer bloque a abordar la actualidad económica y los fondos europeos, con Luis Socias, Jefe de la Oficina de Proyectos Europeos de la CEOE, que dará a conocer la oportunidad que estos suponen para los despachos profesionales.

Y se seguirá hablando de crecimiento del sector de la mano de Silvia Leal, experta en Innovación y, nuevas profesiones.

ThinkPad X1 NANO

# El ThinkPad más ligero. Menos de 1KG.

Lenovo



 Windows 10

Olvídate de las contraseñas. Usa Windows Hello.

# Las empresas sufrieron de media dos ciberataques en el último año



Los ciberataques se incrementan en todo el mundo y afecta a usuarios empresas y organismos oficiales. Los datos son claros.

**A**nte el incremento de los ciberataques a nivel mundial —según la ONU cada 39 segundos se produce uno—, la ciberseguridad se ha convertido en la principal preocupación de las organizaciones, un interés que se ha acentuado con la crisis de la Covid-19 y la agilidad de los procesos de digitalización. El sector demanda una mayor madurez para hacer frente a los desafíos que presenta, y está experimentando un notorio crecimiento —se prevé que este año el mercado de la ciberseguridad crezca un 8,1% respecto al 2020—.

En este sentido, la compañía Barracuda Networks ha elaborado el informe The State of Application Security (El estado de la seguridad de las aplicaciones), donde evidencia la necesidad de innovar en nuevos sistemas de protección para fortalecer la seguridad y la confianza de las organizaciones. El estudio analiza las opiniones de 750 profesionales de la seguridad acerca de las filtraciones de datos, las de-

bilidades más comunes de los sistemas de seguridad y las capacidades necesarias de un producto para defenderse con éxito de los ciberataques. Según el informe, las organizaciones sufrieron ciberataques de media dos veces en los últimos doce meses a causa de la vulnerabilidad de sus sistemas. En este sentido, el 72% de los encuestados afirmaron que su organización sufrió al menos un ataque debido a este motivo. La situación es aún más preocupante si se tiene en cuenta que más de una cuarta parte de los encuestados (28%) afirma que los errores de los empleados han sido un factor determinante en las infracciones producidas recientemente.

Además, identificaron como principales desafíos de la seguridad de las empresas los bots maliciosos (43%), los ataques a las cadenas de suministro de software (39%), la detección de vulnerabilidades y debilidades de los sistemas (38%), y la seguridad de APIs (37%). Se aprecian diferencias notables entre distintas regiones. Por ejemplo, en Estados Unidos, la detección de vulnerabilidades no figura entre los cinco desafíos más importantes. Sí, en cambio, el desarrollo continuo y la implementación de la seguridad en los procesos de integración. Por otro lado, los europeos están menos preocupados en los ataques a las cadenas de suministro y la disminución de la innovación en favor de la seguridad de las aplicaciones. La corrección de las amenazas supone un reto mayor para el continente. Por último, en Asia-Pacífico, hay una mayor preocupación por la ralentización del desarrollo de aplicaciones a causa de la adición de más seguridad.

### SOLUCIÓN

Asimismo, Barracuda ha lanzado la Cloud Application Protection 2.0 con el objetivo de proteger aplicaciones web de posibles ciberataques. En concreto, la compañía busca combatir los denominados “vectores de ataque”, acciones que llevan a cabo los ciberdelincuentes para identificar las vulnerabilidades de un sistema y atacar a fin de obtener, generalmente, un beneficio económico.

# Los retos que afronta la ciberseguridad



La ciberseguridad se ha convertido en una de las principales prioridades de las empresas. Un elemento, cuya preocupación ha crecido entre CIOs, CISOs y responsables de TI desde que comenzó la pandemia del coronavirus. Uno de los problemas es que los smartphones han sido los grandes olvidados de la estrategia de ciberseguridad.

## NO SÓLO ESTABLECER UNA ESTRATEGIA

Smartphones hay muchos. Pero para una organización no vale con cualquier terminal. Se necesitan aparatos específicos que garanticen esa seguridad. Samsung, por ejemplo, lleva años incidiendo en la importancia que tiene la implementación de medidas de seguridad en los smartphones. Lo hizo, incluso, antes de que ningún otro fabricante considerara el apartado de la ciberseguridad como prioritario.

Dentro de esa seguridad que incorporan los terminales de Samsung, destaca la plataforma Knox. Aparecida por primera vez en el año 2013, Samsung la ha ido incorporando paulatinamente a sus terminales pero, desde el año pasado, la evolución ha sido más que significativa con la aparición de Knox Suite. ¿Por qué aparece este nuevo desarrollo? En Samsung se dieron cuenta de que más del 30% de las empresas utilizan de forma simultánea dos herramientas de gestión movilidad empresarial (EMM). Esto hace que los departamentos de TI y de ciberseguridad de las empresas tengan que plantearse diferentes metodologías y procesos de administración.

La nueva evolución que se ha dado con Samsung Knox Suite se basa en la plataforma de seguridad multicapa Samsung Knox que da cobertura a la necesidad completa de una compañía en términos de seguridad y gestión del ciclo de vida del dispositivo. Con esta novedad se cubre la necesidad de las empresas en términos de seguridad y gestión de la movilidad. Knox Suite permite el registro masivo de terminales de manera

automática y desatendida, cada usuario registraría su terminal solo con encenderlo y conectarlo a internet, aplicando el perfil de configuración acordado en el departamento de seguridad de la empresa, podrían bloquear las actualizaciones del Sistema Operativo o instalar la versión necesaria para garantizar la compatibilidad con el resto de aplicaciones de la empresa. Además, se podría localizar un terminal en cualquier momento o monitorizar el uso del mismo para reemplazarlo si fuera necesario, por ejemplo, detectar si la batería está dañada o si es alguna aplicación concreta la que causa cierres inesperados del Smartphone. Todo ello ofreciendo al usuario una experiencia unificada y Single Sign On (SSO), lo que facilita al departamento de TI el uso de las soluciones Knox.

De esta forma, Samsung soluciona la problemática de utilizar varias herramientas de gestión y de seguridad ya que con Samsung Knox Suite se ofrece una única licencia para todos los servicios de ciberseguridad de Samsung y de esta forma todos los terminales que forman parte del parque de una organización se pueden aprovechar de todas las soluciones empresariales incluidas en la plataforma, a través de una gestión centralizada. Entre esos servicios se encuentran Knox Mobile Enrollment que permite el despliegue masivo y en remoto de la flota de terminales de una empresa, con un registro automático y obligatorio en el MDM. Asimismo, la solución EMM Knox Manage permite la gestión multiplataforma de terminales lo que permite que el equipo de TI aplique de forma remota las políticas de seguridad y gestión definidas para sus empleados. Finalmente, con Knox E-FOTA los administradores de TI pueden instalar la versión del Sistema operativo que funcionará en los terminales de su empresa lo que garantiza la compatibilidad con las aplicaciones internas y elimina la granularidad de las distintas versiones disponibles para un mismo terminal.

## LA ESTRELLA: SAMSUNG GALAXY S21

El último modelo de Samsung destaca por sus elevadas medidas de seguridad: incluye el elemento seguro integrado (eSE), un procesador seguro para proteger contra ataques físicos, lector de huellas ultrasónico integrado en pantalla y la solución Knox Vault, que agrega otra capa de seguridad. El terminal tiene una protección de extremo a extremo ya que Samsung es de los pocos fabricantes que diseña y desarrolla sus propios productos, software y servicios. Además se puede configurar de forma personalizada con Samsung Knox de manera remota y automática según los requisitos específicos de cada perfil de usuario. Además, todos los smartphones Galaxy, incluida la familia S21 reciben actualizaciones de seguridad regulares durante un mínimo de cuatro años.

# Cisco facilita una seguridad más sencilla, inteligente y ubicua



Cisco presenta las siguientes novedades anunciadas durante la reciente feria de seguridad RSA

Cisco ha desvelado las novedades anunciadas durante la reciente feria de seguridad RSA, diseñadas para simplificar la seguridad y ofrecer protección de principio a fin a través de usuarios, dispositivos, redes, aplicaciones y datos.

Y es que, el trabajo híbrido ha llegado para quedarse. Los usuarios demandan conectarse desde cualquier lugar y dispositivo, mientras los equipos de Seguridad cuentan con las mismas soluciones complejas, poco ágiles y apenas integradas.

“Con la migración acelerada al trabajo remoto y los servicios Cloud, las organizaciones necesitan visibilidad a través de los usuarios, aplicaciones y terminales, además de blindar los accesos con una autenticación continua y sin contraseñas”, afirma Ángel Ortiz, Director de Ciber-Seguridad en Cisco España.

Cisco SecureX

Aprovechando la plataforma Cisco SecureX, los anuncios mejoran la visibilidad y la protección de los terminales, amplían la visión de SASE con detección optimizada de amenazas en la nube y redefinen la seguridad de red. Las organizaciones demandan soluciones para extender la visibilidad y la protección a los terminales. Y es que, más del 40% de las organizaciones a escala global han sufrido una brecha de seguridad importante en los últimos dos años.

Sin embargo, aquellas compañías con soluciones integradas tienen la mitad de probabilidades de sufrir un incidente. Como respuesta, la compañía amplía las capacidades XDR integrando múltiples puntos de control de seguridad, analítica y automatización.

### NOVEDADES DE CISCO

Las novedades incluyen:

- **SecureX Device Insights.** Los clientes pueden consolidar rápidamente su inventario de dispositivos desde múltiples fuentes dentro de la plataforma SecureX para proporcionar mayor visibilidad y contexto para las operaciones de TI (ITOps) y las operaciones de seguridad (SecOps), así como una respuesta automatizada frente a las amenazas.

- **Migración simplificada desde EDR a XDR.** Como única plataforma de seguridad de terminales integrada, SecureX ayuda a simplificar la evolución de EDR a XDR, con más de 30 flujos de trabajo pre-construidos, 40 integraciones llave en mano y nuevas capacidades de orquestación. Además, Secure Client -el nuevo conector integrado que abarca usuarios, nube y terminales-, facilita una migración más rápida a XDR y reduce las horas dedicadas a operar con múltiples agentes.

- **Investigación ampliada y respuesta más rápida.** La tecnología de búsqueda avanzada de Secure Endpoint refuerza ahora el valor de XDR, ofreciendo más de 200 consultas de terminales ya preparadas para obtener respuestas en tiempo real y facilitar las investigaciones, threat hunting y otros casos de uso de las operaciones de TI.



# Por qué la confianza de los gobiernos en la seguridad cloud tiene muchos matices



Por José Battat,  
director general de Trend Micro  
Iberia

organizaciones del sector público, aunque parecen estar seguros de su estrategia de seguridad, hay conceptos erróneos preocupantes sobre los principios clave que pueden llevar a implementaciones no óptimas. Ahora, con el tercer aniversario del GDPR, es importante recordar el impacto potencial de estos problemas.

## CONFIANZA EN LA SEGURIDAD DE LA NUBE

La gran mayoría (84%) de los jefes de TI del sector público afirmó que la pandemia había acelerado "considerablemente" o "algo" la adopción de la nube. Además, la ciberseguridad parece haber sido una consideración clave, ya que el 74% ha implementado formación en esta materia y el 54% nuevas políticas sobre el manejo de la información personal para mitigar los nuevos riesgos. Casi la mitad (45%) señaló que el aumento de la adopción de la nube había incrementado su atención a las mejores prácticas de seguridad.

Así, no es extraño que el 82% se sienta totalmente o en gran medida en control de la seguridad de sus entornos de trabajo remotos, y el 79% confía en que puede asegurar el nuevo lugar de trabajo híbrido emergente después de la pandemia.

Pero los responsables de TI de las administraciones públicas tienen menos confianza de la que parece, y muchos pueden estar trabajando bajo falsas suposiciones y conceptos erróneos.

Con la pandemia muchos gobiernos, casi de la noche a la mañana, tuvieron que enfrentarse al doble reto de apoyar el teletrabajo masivo de los funcionarios y dar una respuesta rápida para apuntalar la economía. Las tecnologías en la nube fueron indispensables para este esfuerzo, aunque también ampliaron la superficie de ataque y el perfil de riesgo de una organización.

Según un estudio mundial de Trend Micro entre los responsables de la toma de decisiones de TI de orga-

Por ejemplo, la mitad de los encuestados admitió que la seguridad es un obstáculo importante para la adopción de la nube. Solo el 11% pensaba lo contrario. Los retos cotidianos abundan: los tres principales problemas operativos destacados en este estudio fueron la seguridad de los flujos de tráfico, la falta de integración con las herramientas de seguridad locales y la implantación.

Quizá lo más preocupante sea la escasa concienciación sobre el modelo de responsabilidad compartida, que delimita lo que es responsabilidad del cliente en términos de ciberseguridad y lo que ofrece el proveedor de la nube. Si se equivocan, las organizaciones podrían acabar con grandes lagunas de protección o gastando excesivamente en sistemas duplicados.

Alrededor del 86% de los encuestados dijeron que estaban "muy" o "algo" seguros de que entendían su parte del modelo. Pero casi todos (99%) también consideraron que los controles de su CSP eran "más que suficientes" o "suficientes" para proteger sus datos en la nube, cuando en realidad la responsabilidad es solo del cliente en los entornos IaaS y PaaS.

## UN 2021 MÁS SEGURO

Ahí no acaba todo. Casi la mitad (45%) de los responsables de TI del sector público afirmó que la introducción de herramientas de seguridad en la nube ha hecho que la seguridad general de TI sea más costosa, mientras que el 28% dijo que había creado más silos. De hecho, la plataforma de seguridad en la nube adecuada debería facilitar la seguridad, integrarla y hacerla más eficiente, además de respaldar los enfoques de DevSecOps que pueden unir a equipos dispares.

La clave está en encontrar la oferta adecuada: una que pueda ofrecer una serie de capacidades desde una única plataforma. La atención debe centrarse en la racionalización y automatización de la seguridad en los contenedores, las cargas de trabajo, aplicaciones, redes, etc., sin comprometer la protección. Los productos que ofrecen integraciones abiertas con herramientas de terceros también pueden ayudar a los gobiernos a maximizar el valor de las inversiones existentes en seguridad TI.

La revolución digital desencadenada por la pandemia durará mucho más que la crisis. Para que los proyectos futuros sean un éxito, los gobiernos deberán consolidarse y apoyarse en proveedores de seguridad en los que confíen.

# Optimización de costes en la nube pública

**OPTIMIZACIÓN DE COSTES EN NUBE PÚBLICA**

**Marc Niubó**  
Sales Expert Cloud Infrastructure  
**T-Systems Iberia**

**Alfons Ruiz**  
Public Cloud Leader  
**T-Systems Iberia**

**José Casado**  
Technical Solution Architect  
**CISCO**

**ENCUENTROS byte 20 años**  
En colaboración con:  
**T-Systems**

Trabajar de manera más eficiente gracias a un entorno Cloud se está convirtiendo más en una elección que en una mera necesidad. En el contexto actual, empresas de diversos sectores han tenido que tomar decisiones apresuradas para mantener la oferta de servicios y proteger a sus empleados y clientes. Para hablar sobre ello, Byte TI organizó ayer, junto a T-Systems y Cisco, un encuentro virtual en el que se dieron las claves de cómo optimizar los costes en la nube pública.

La digitalización es una realidad para muchas compañías que se han tenido que enfrentar a repensar operaciones, procesos, procedimientos, aplicaciones, datos...y se han tenido que transformar digitalmente, han tenido que innovar. Con el objetivo de garantizar la resistencia de sus compañías, una de las muchas determinaciones adoptadas ha sido usar la nube pública. Sin tiempo para crear infraestructuras –que no se tenían– ni presupuestos para mantenerlas ni a corto plazo, la nube pública se ha convertido en la verdadera tabla de salvación. Gracias a ella se ha conseguido salvar la productividad de muchas de las empresas que han

podido seguir operando en un entorno tremendamente complejo. La migración hacia entornos de nube pública se hizo por necesidad de supervivencia. Pero la apuesta por esos entornos se ha demostrado como acertada: menos costes, mayor agilidad o mucha más flexibilidad son sólo algunas de las ventajas que los departamentos de TI descubrieron en la migración hacia la nube pública. Así que, lo que eran proyectos concretos destinados a salvar un problema específico, ha ido creciendo y las empresas han ido incorporando nuevos elementos que tienen como pilar la nube pública y por tanto trabajan en un entorno híbrido.

## LOS PARTICIPANTES

Muchos departamentos han incorporado nuevas soluciones y servicios basados en la nube pública demostrando que ésta proporciona flexibilidad, agilidad, resiliencia y sostenibilidad.

Pero en el momento de ir a la nube pública, las empresas deben gestionar los servicios, optimizarlos y, sobre todo, gestionar los costes para que éstos no se disparen. Tal y como expuso Marc Niubó, Sales Expert Cloud Infrastructure de T-Systems, “la optimización y gestión de costes es uno de los elementos clave para que la adopción a nube pública tenga éxito. Hemos visto que la digitalización ya no es una opción y que las empresas que han tenido mayores crecimientos han sido aquellas que han apostado por la digitalización. En este sentido, la adopción del cloud es básico para el futuro. Cloud y modernización de infraestructuras son elementos clave para empresas de cualquier tamaño”. Y es que, para Niubó, “la nube debe ser un componente integral y básico de las organizaciones. Las empresas necesitan agilidad porque se requieren tiempos de reacción mucho más rápidos y estamos viendo que las empresas que han implementado el cloud han mejorado su efectividad. Necesitamos plataformas ágiles para poder desplegar nuevos entornos y creemos que al final más del 90% de la innovación del negocio estará dentro de un entorno de nube pública”.

Tal y como expuso este portavoz de T-Systems, todo ello implica grandes retos en los que la gestión y la optimización de los costes son algunos de los más importantes aspectos a tener en cuenta. Ya que ninguna empresa se puede permitir que la migración al cloud no se haga con una optimización y transparencia de la gestión de los costes.

### LAS CLAVES

Pero ¿Cómo se puede hacer de forma correcta esa optimización de los costes? Alfons Ruiz, Public Cloud Leader de T-Systems, centró su ponencia en cómo conseguirlo. En su opinión “los clientes, cuando empiezan a adoptar cloud, tienen una serie de retos a afrontar y uno de ellos es el control del coste porque ven que, de repente, aparecen problemas nuevos. Por ejemplo, llega una factura que no se entiende o que tiene unos cargos con los que no se contaba. El problema aquí es que muchos clientes han desistido en el apartado de las previsiones y se produce una lucha entre el gestor y el responsable de llevar el presupuesto, porque han perdido el control. Surgen dudas de a quién se le asigna un determinado gasto, o si se está optimizando o comprando lo que se tiene que comprar”. Tal y como señaló el portavoz de T-Systems, otro de los problemas con los que se encuentran las empresas son los modelos de compra disgregados, donde cada departamento realiza una compra de un determinado servicio cloud. “Por tanto, en T-Systems aconsejamos que se haga un control y una optimización continua. El control de lo que se tiene contratado es algo que no se va a acabar nunca. En este caso, nuestra propuesta pasa por llevar desde el desconocimiento, donde no sabemos lo que está pasando, a hacer un mejor control del coste y tener una mayor transparencia. Se trata de que haya una figura que sea el responsable del control del coste, alguien que informe a quién repercutir ese coste o que informe de si surge algún problema. Por tanto, al final del proceso, queremos llegar a la capacidad de gestión y tener todos los recursos asignados. No puede haber ningún recurso en cloud que no esté asignado a su departamento correspondiente”, afirma Ruiz.

Como quedó claro durante su intervención, el problema es que, en gene-



Marc Niubó, Sales Expert  
Cloud Infrastructure de T-  
Systems



Alfons Ruiz, Public Cloud  
Leader de T-Systems

ral, las organizaciones se centran sólo en el gasto, pero olvidan que en el montante de las facturas también está detallado el consumo de los recursos. Por eso, el Public Cloud Leader de T-Systems cree que “dependiendo del propósito, dependiendo del reporte que hay que llevar a cabo, o de quién es el destinatario, o el filtro de la categoría que me está llegando, hay que desarrollar un modelo de información que acompañe a ese control del coste. Prevención, detección y corrección son los factores determinantes en la gestión del coste”. Una vez resuelto el problema de la gestión del coste, se pasa a la parte de la optimización. En T-Systems lo dividen en seis áreas con el objetivo de gastar el mínimo posible:

**Eliminación:** es el gran olvidado. Según se puso de manifiesto en el encuentro, en ocasiones, hay hasta un 15% de recursos que no se utiliza, lo

### LOS PARTICIPANTES



José Casado, Technical Solution Architect de Cisco

que supone un gasto importante. Por tanto, hay que analizar qué es lo que no se usa y eliminarlo para que la factura no suba.

**Rightsizing:** es importante elegir el tamaño de lo que se consume porque, por ejemplo, el pasar de una talla de máquina a una talla inmediatamente superior puede suponer el doble de dinero. Para Alfons Ruiz, “no hay que provisionar más de lo que se necesita. Se trata de reevaluar de forma constante y además hay que automatizar para que cuando se necesitan más recursos se obtengan y viceversa”

**Modelo de compra:** es importante fijarse en las opciones que ofrecen los proveedores. Por ejemplo, para una talla de una máquina virtual se puede llegar a pagar hasta un 90% menos. Además, se puede utilizar software para mover la carga de trabajo entre diferentes regiones y aprovechar estos modelos de compra (spot instances). Otro detalle importante y que, en ocasiones pasa desapercibido, es que “en la nube pública se pueden buscar descuentos empresariales o subcontratar a terceros. En T-Systems ofrecemos los descuentos más importantes que la mayoría de los usuarios pueden conseguir”.

**Características del servicio:** otro detalle importante es fijarse en qué ofrece el servicio que se contrata: “Al final, cuando se mueve una carga a la nube pública, lo que se hace es consumir servicios de cloud pública en los que cada uno tiene diferentes precios. Por eso es importante estudiar qué características tiene ese

servicio del hyperscaler”, aseguró Alfons Ruiz.

**Arquitectura de la aplicación:** Hay que utilizar modelos de computación nuevos, pero lo que hay que interiorizar es que, por ejemplo, un contenedor o la tecnología serverless puede hacer lo mismo que una máquina virtual, pero con menos recursos.

**Patrones del servicio:** Hay que mirar qué es lo que ocurre y saber cuándo se produce un pico inesperado y cuándo no lo hay. Hay que estar atento a las tendencias y conocer cuándo se produce un comportamiento anormal.

### LA HERRAMIENTA

Para llevar a cabo todas esas pautas que apuntaba el portavoz de T-Systems es necesario contar con una herramienta adecuada y esta es la que proporciona Cisco con Workload Optimization Manager (WOM). José Casado, Technical Solution Architect de Cisco, afirmó que “optimizar los costes es un conjunto de procesos y dentro de esos procesos está la parte de la optimización. Se trata de uno de los retos más importantes a los que se enfrentan las empresas. El coste va asociado a muchos elementos y en Cisco creemos que el punto de la optimización es esencial. Si queremos hacer un ahorro de costes, desde Cisco, entendemos que para poder hacer una transición exitosa a la cloud y explotar la elasticidad que nos da la nube pública hay que entender cuáles son los recursos que realmente necesitan las aplicaciones. Es necesario saber cuáles son las dependencias de las aplicaciones, de las bases de datos o de los contenedores para de esta forma optimizar los recursos necesarios y que se usen en el momento en el que se necesitan”.

Es aquí donde WOM juega su papel. Esta solución se basa en tres pilares: la visibilidad, la analítica y la automatización. Tal y como expuso Casado, “la visibilidad vía API nos permite ver qué están demandando las diferentes aplicaciones. Por su parte, la analítica en tiempo real con Inteligencia Artificial nos enseña el mapa de a qué aplicación se le tienen que otorgar más recursos de los que necesita o viceversa. Finalmente, con la automatización se persigue que todas estas mejoras se puedan realizar de forma automática”.

Tal y como quedó señalado la herramienta sirve tanto para entornos de nube pública como para aquellos de nube híbrida. Una de sus ventajas es que WOM, en solo 45 minutos ofrece una visibilidad completa de todas las aplicaciones y proporciona recomendaciones sobre cómo actuar y todo ello sin tener que parametrizar nada. Pero como señaló el Technical Solution Architect de Cisco, “además hay otra parte fundamental y es saber qué pasaría si, por ejemplo, hay que provisionar más instancias. En este caso, la ventaja es que no hay que adivinar este tipo de escenarios ya que WOM nos permite saber, gracias a su motor de simulación, lo que puede pasar y qué acciones son las indicadas para poder tener una optimización no solo de recursos, sino cómo va a afectar ello al ahorro de costes. En general cualquier cliente, después de utilizar todas las herramientas, obtienen unos resultados muy importantes sin poner en peligro el negocio o las aplicaciones. El motor de IA de WOM nos permite dar ese paso de forma segura”.

# Gestión de parches: paso fundamental para lograr una seguridad TI eficaz



**Jose Luis Paletti,**  
sales Engineer Cytomic, a  
WatchGuard brand

Diseñados para tapan los agujeros de rendimiento, añadir funciones adicionales y mejorar la seguridad, los parches siguen formando parte del día a día de los equipos de TI. Sin embargo, la necesidad constante de aplicarlos a un elevado número de dispositivos puede suponer más de un quebradero de cabeza.

Además, es importante recordar que los ciberdelincuentes tienen acceso a exploits públicos para llevar a cabo sus ataques, que no dudan en utilizar pues saben

que muchas organizaciones no parchean sus sistemas. De hecho, el 80% de los ataques exitosos aprovechan vulnerabilidades que tienen parches conocidos que no se han aplicado.

Puede parecer sencillo, pero la mayoría de las organizaciones tiene dificultades para identificar qué actualizaciones de parches críticos deben instalar primero. Por tanto, priorizar el despliegue de parches es una parte clave del proceso de gestión. Los dos parches más comunes que hay que gestionar son los de seguridad y los de paquetes de servicios o funciones.

## UN CICLO DE VIDA EFICAZ PARA LA GESTIÓN DE PARCHES

Disponer de una estrategia eficaz de gestión de parches puede ser la herramienta más efectiva para proteger contra vulnerabilidades y ciberataques. La clave: establecer una rutina de gestión de parches e integrarla en las operaciones estándar.

En este ciclo hay 6 fases:

**1. Identificación de activos:** identificar con precisión todos los activos de TI y el software instalado en ellos, así como su estado de parches existente, es una tarea compleja. Sin embargo, el establecimiento de esta línea de base permite a un equipo de TI realizar cambios en el sistema sin riesgos y posibilita volver a un estado funcional anterior conocido en caso de problema.

**2. Disponibilidad de parches:** se debe revisar la lista actual de parches disponibles, basándose en la información obtenida del proceso de identificación de activos. Acto seguido, se pueden desplegar nuevos parches a medida que se vayan publicando.

**3. Aplicabilidad:** Por eso, es importante comprobar si una actualización específica es válida y adecuada para todos los dispositivos en los que se ha desplegado.

**4. Adquisición:** obtener el archivo del parche de actualización de una fuente oficial y comprobar que el parche es legítimo, lo que no siempre es fácil. El uso de hashtags no es habitual en los parches relacionados con los sistemas de control.

**5. Validación:** este paso garantiza que la actualización del parche no tenga un impacto negativo en la infraestructura de TI existente. Para validar el parche o actualización, hay que utilizar activos de prueba y seguir las fases de despliegue. La validación tiene por objeto comprobar qué implicaciones podría tener la actualización, que podría incluir cambios en las políticas del firewall y en la configuración de los usuarios.

**6. Despliegue:** el último paso de un proceso eficaz de gestión de parches es el despliegue de los parches validados en cada dispositivo apropiado. El proceso debe utilizar archivos de actualización, así como instrucciones de instalación para que los equipos de TI garanticen que el proceso se lleva a cabo con eficacia y de acuerdo con los requisitos del fabricante.

Al tener un enfoque tan estructurado de la gestión de parches, una organización puede estar segura de que su infraestructura de TI funciona al máximo rendimiento estando protegida. De ahí que sea crítico contar con un proceso eficaz de esta tarea para garantizar que todos los parches críticos se despliegan en todos los dispositivos tan pronto como estén disponibles.

Apoyarse en tecnologías como Cytomic Patch de WatchGuard-Cytomic ayuda a gestionar esta tarea haciéndolo en tiempo real y en todos los dispositivos de la compañía manteniendo bajo control todos los puestos de trabajo y servidores de Windows para reducir la superficie de ataque e impedir que las amenazas lleguen al endpoint.

Haga de la revisión completa de su proceso de gestión de parches su próxima prioridad.

# Open Networking para las Administraciones Públicas



Las redes, aunque no tienen tanto glamour cómo otras tendencias TIC, son fundamentales para la digitalización tanto de empresas como de las Administraciones. Las AA.PP. tienen unas necesidades específicas por lo que Byte TI, junto a Adjudicaciones TIC, organizaron un evento que contó con la presencia de Gonçal Badenes, ICT Director de la UAB y Gonzalo de Antonio, Networking Sales Specialist de Dell Technologies que contaron casos prácticos y explicaron el concepto de Open Networking.

Carlos Canitrot, director de consultoría de Adjudicaciones TIC fue el encargado de dar algunos datos acerca de cómo se encuentra el mundo de las redes en la Administración Pública española. En su opinión, “con la pandemia se ha puesto foco en las redes y conectividad. La conectividad es un factor fundamental para la digitalización de la AAPP según el Plan España 2025. Las AAPP invirtieron en networking casi el 3% del total de la inversión TIC. Toda la

parte de infraestructuras creció mucho si se compara con otros apartados en lo que se redujo la inversión. En licitaciones se incremento un 91% y en contratación centralizada un 71%. En la parte de Open Networking, está creciendo con respecto a soluciones más antiguas ya que produce ahorro en CAPEX y en OPEX, agilidad de los servicios y ahorros de energía lo que acelera el ROI”.

Gonzalo de Antonio, Networking Sales Specialist de

## LOS PARTICIPANTES

Dell Technologies hizo hincapié en lo que es el Open Networking así como en el concepto de las SDN o redes definidas por software. Tal y como expuso es esencial entender qué son estos dos conceptos para poder valorar cuáles son las ventajas que ambos pueden ofrecer a las Administraciones Públicas. Tal y como expuso, “el concepto de SDN es muy sencillo. Podemos ver que todos los switches tienen un plano de datos y otro de control. Además, hay otro plano de gestión con el que se configura la parte del control. Lo que propone SDN es que el plano de control, en lugar de estar asociado a cada uno de los elementos que componen la red, lo llevamos a un entorno centralizado y desde él, podemos ser capaces de configurar los elementos que componen una red”. De Antonio explicó que también es importante comprender qué son los conceptos de red underlay y overlay. Tal y como se puso de manifiesto, la primera es la red física que proporciona la conectividad mientras que la segunda es donde realmente nos encontramos el concepto de redes definidas por software ya que son un conjunto de redes virtuales que emplean la red underlay y que gracias a ella podemos establecer los servicios, aplicar la seguridad, etc.

En general las redes definidas por software ofrecen varias ventajas en un entorno de red moderno. Para de Antonio esas son: “La primera es la automatización, de tal forma que ya no tenemos que estar configurando de forma manual ya que esto es responsabilidad del plano de control. Además agiliza la forma de trabajar en toda la red, permite una gran flexibilidad y proporciona una alta escalabilidad. Asimismo, las SDN permiten un aislamiento del tráfico de diferentes servicios y de diferentes aplicaciones en la misma red física, con lo que, por ejemplo, se le pueden dar unas pautas de seguridad diferentes a cada uno de ellos. También permite implementar políticas de continuidad de negocio y además tendremos una visibilidad completa del tráfico que circula por la red de una organización, de tal forma que podremos establecer analíticas para resolver problemas y mejorar el servicio. Todo ello hace que se reduzcan los gastos operativos, no en la inversión de la nueva infraestructura pero sí en el trabajo posterior ya que vamos a poder dedicarnos a aquellas tareas que son más importantes para el negocio”.

### OPEN NETWORKING

A continuación se detalló en qué consiste el denominado como Open Networking. El portavoz de Dell Technologies señaló que, “tradicionalmente, los switches eran equipos monolíticos en los que tanto el hardware como el software los proporcionaba un único fabricante. Pero en Dell Technologies, en 2014, apostamos por cambiar el modelo, al que denominamos Open Networking. Básicamente proporciona una disgregación del hardware y el software, de tal forma que ambos pueden ser de diferentes fabricantes. La ventaja de ello es que, trabajando sobre una plataforma abierta permite que sobre un hardware abierto se pueden ejecutar diferentes alternativas de sistemas operativos lo que se traduce en una protección de la inversión ya que puedes cambiar de fabricante de hardware o de software, sin tener que renovar absolutamente todo”.



Gonçal Badenes, ICT Director  
de la Universidad Autónoma  
de Barcelona

Por otra parte, hay que destacar que el Open Networking, el año pasado sufrió una evolución adicional ya que también se ha producido una disgregación en el software para introducir los contenedores dando lugar a lo que se denomina como NFV. De esta forma, se pueden aplicar diferentes funciones de software sobre el sistema operativo de base.

Gracias a todas estas ventajas, toda la propuesta de Dell Technologies está basada en el modelo de Open Networking de tal forma que las empresas y Administraciones Públicas sobre el hardware de la compañía pueden diseñar diferentes estrategias de sistema operativo. De hecho el sistema operativo de Dell, denominado SmartFabric OS 10, es especialmente interesante cuando va de la mano de infraestructura de la multinacional (servidores, almacenamiento, etc.) porque se consigue automatizar toda la parte de red asociada a todas las cargas de trabajo. El portavoz de Dell Technologies indicó, además, en una tercera alternativa de un partner estratégico: Pluribus Networks. En este caso nos encontramos ante un sistema operativo SDN que puede funcionar sobre los switches de Dell. La ventaja es que Dell es el encargado de propor-

### LOS PARTICIPANTES



Gonzalo de Antonio,  
Networking Sales Specialist  
Dell Technologies

cionar el soporte técnico, aunque no se trate de un producto de la compañía.

#### VISIÓN ESTRATÉGICA

Desde Dell Technologies se considera esencial que las Administraciones Públicas renueven su estrategia en torno a la red.

De la misma forma que se apuesta por la digitalización en otros elementos, la apuesta por la renovación de la red es fundamental. Tal y como expuso Gonzalo de Antonio, “creemos que las redes tienen que ser definidas por software y basadas en la intención. Es decir, hay que trabajar con la red, indicándole qué servicio queremos que proporcione y no tanto cómo tiene que configurarse. Se trata que la red se autoconfigure de forma autónoma. Además queremos que todo esto afecte lo menos posible a lo que hay en funcionamiento en la red. Por eso, nosotros apostamos por un modelo Fabric SDN que no está basado en un controlador o modelo distribuido de tal forma que el plano de control se encuentre en toda la red”.

Dell Technologies tiene que claro que su estrategia es la más beneficios proporciona a las Administraciones ya que, por ejemplo, aunque se tengan decenas de elementos en la red se trabaja como si fuera un único elemento lógico y, por tanto, se convierte en un único elemento de gestión. De hecho, gracias a ese úni-

co punto de gestión se reducen de forma sensible las tareas de operación y provisión de la red. Además se pueden establecer reglas de seguridad relacionadas a un determinado flujo de tráfico, sin necesidad de implementar un cortafuegos ya que es la red la que se encarga de bloquear ese tipo de tráfico que lo lleva a un firewall central que es el encargado si los datos que provienen a través de esa red es seguro o no. Otro apartado importante es que gracias a esta estrategia se consigue una telemetría y una analítica completa del tráfico que circula por la red lo que abre la puerta a la toma de decisiones.

#### EN LA PRÁCTICA

Para ver cómo el concepto de Open Networking funciona, Gonçal Badenes, ICT Director de la Universidad Autónoma de Barcelona, explicó el proyecto que desarrollaron en el campus universitario. Tal y como afirmó “es un proyecto que se definió hace alrededor de tres años y que estamos terminándolo de ejecutar en estos momentos. Lo que tenemos en la UAB es una red con un grado de redundancia razonable. Tenemos dos data centers en dos puntos diferentes del campus y teníamos el objetivo de renovar todo lo que interconecta los edificios del campus. Tenemos 14 nodos y cada uno de ellos está conectado a los CPDs. El problema es que las conexiones eran de 1+1 Gbps, además muchos de los equipos ya eran antiguos por lo que se producía una dificultad de atracción de recursos de cálculo al centro de datos. Además teníamos muy poca flexibilidad para la creación y gestión de servicios distribuidos y también con la arquitectura tradicional no teníamos una completa visión del tráfico”.

Tras analizar toda la problemática se decidió renovar toda la red del campus para lo que se convocó un concurso público con una serie de requerimientos. La solución por la que se apostó fue la de Dell con Pluribus, basada en el concepto spine-leaf y que permitió multiplicar el ancho de banda disponible en cada edificio por 50.

Asimismo, ampliar la conectividad en el edificio se puede realizar con un coste muy bajo. Badenes explicó que “en estos momentos estamos acabando las pruebas para poner en marcha un punto de presencia de RedIris que tendremos en el Campus y que también ira conectado a esta red, lo que también permitirá mejorar la red”.

En definitiva la apuesta por la propuesta de Dell y Pluribus, ha permitido a la UAB mejorar la red de todo el campus y tener una gran capacidad de crecimiento a futuro. También, como afirma Badenes, “gracias a Pluribus, nos ha permitido tener una gestión global y una visión unificada de toda la red, además de tener la posibilidad de crear redes experimentales sobre un entorno de producción, con la posibilidad de desplegar servicios especiales en cualquier punto del campus y todo ello a un precio muy competitivo”.





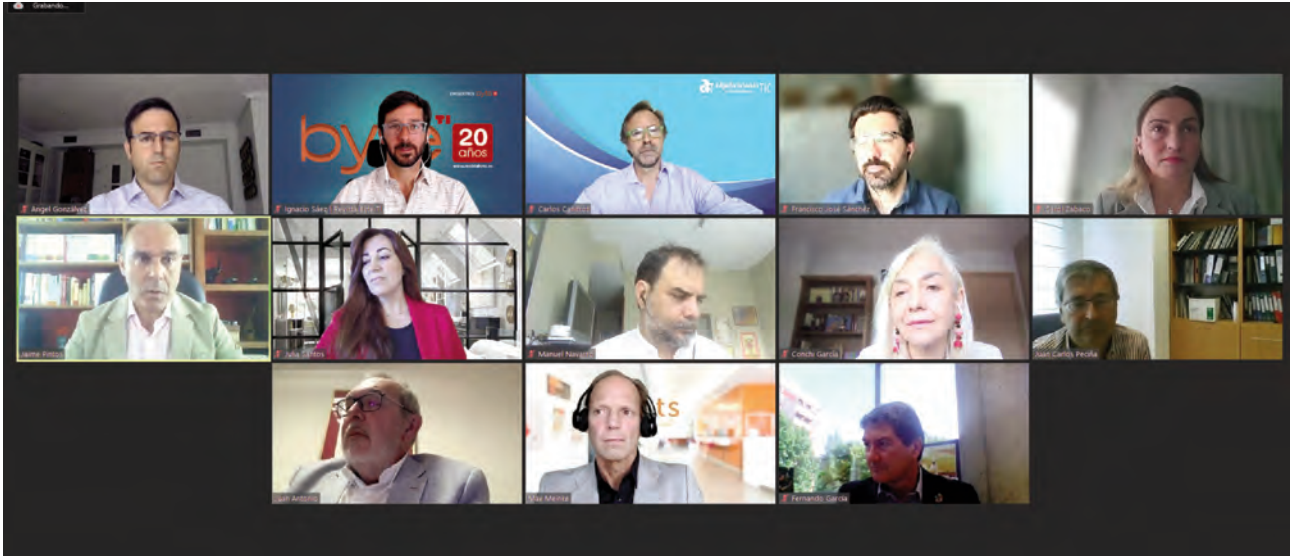
YOU'VE BEEN HACKED!

## SEGURO CIBERRIESGO

Cuando todo lo demás falla  
entra la última línea de defensa

Asistencia y servicio forense  
Responsabilidad civil  
Sanciones y multas administrativas  
Daños a los sistemas y costes de rectificación  
Gastos de interrupción del negocio  
Vulneración de los derechos de propiedad intelectual  
Gastos por difamación  
Indemnización por extorsión

# Experiencia Digital ciudadano-cliente



La experiencia del cliente o CX es una de las prioridades de las organizaciones. Pero ¿qué ocurre con la empresa que tiene el mayor número de clientes como es la Administración Pública? La prestación de servicios a la ciudadanía a través de las TIC ha ido mejorando de forma sensible en los últimos años, pero la pandemia ha acelerado la implementación de servicios.

Para conocer más sobre el estado de la AA.PP. así como de casos de usos, desde Byte TI y junto con Adjudicaciones TIC organizamos este encuentro, que contó con la participación de Conchi García, Directora de Capacitación Digital de Madrid Digital; Carol Zabaco, Coordinadora de TIC's y Transparencia para el Gobierno Abierto de Ayuntamiento de Barakaldo; Juan Carlos Peciña de Frutos, Jefe del Servicio de Tecnologías de la Información de Gerencia Regional de Salud de Castilla y León; Francisco José Sánchez Laguna, Jefe del Área de Sistemas Clínicos de Información, Subdirección General de Información Sanitaria; Fernando García, Subdirector General TIC de Comunidad de Madrid (Consejería de Educación y Juventud); Juan Antonio Gómez Palomeque, Subdirector TIC Servicio Andaluz de Salud; Jaime Pintos, Abogado y Consultor experto en contratación pública; Carlos Canitrot, Director de Consultoría de Adjudicaciones TIC; Max Meinke, Director General Iberia y Latam de TTS; Ángel González, Territory Manager Adobe y Julia Santos, Sales Manager de Dynatrace.

Jaime Pintos, Abogado y Consultor experto en contratación pública analizó la situación de la compra pública en la actualidad. En su opinión, “las AAPP necesitan de las TIC para funcionar. Además hay escasez de funcionarios de la escala superior TIC, que está altamente externalizada. Por eso la contratación de tecnologías es un factor crítico. A esto se le añade la necesaria profesionalización de estos funcionarios en la materia de la compra pública. Con todo ello, se produce un problema que es la dependencia de los proveedores y se da una situación en la que no nos podemos salir del proveedor. A falta de una ley y la necesidad de formación continua se necesitan órganos de compra pública de tecnología que algunas comunidades autónomas sí que tienen”.

Francisco José Sánchez Laguna, Jefe del Área de Sistemas Clínicos de Información, Subdirección General de Información Sanitaria trató el tema de la administración digital. Sánchez considera que “la administración digital es una realidad pero hay mucha desigualdad porque hay administraciones que han

## LOS PARTICIPANTES

avanzado mucho y hay otras que no tanto. El desconocimiento de que hay trámites que se pueden hacer de forma digital, no solo por la ciudadanía sino por los profesionales es uno de los problemas. Además está la brecha digital que no todos los ciudadanos tienen las habilidades o los medios para acceder al servicio. Luego está la complejidad que arrojamos al ciudadano. Muchas veces para quitarnos el problema se crea otro. Esto es algo en el que la empresa privada nos está superando ampliamente”.

Otro de los retos es el de pasar de un modelo presencial a otro virtual. Un caso paradigmático ha sido el de la educación. En este sentido, Fernando García, Subdirector General TIC de la Consejería de Educación y Juventud de la Comunidad de Madrid afirmó que “la pandemia para la educación ha sido una oportunidad. De forma radical tuvimos que pasar las clases desde el colegio al hogar. Ha sido un reto pero también una oportunidad y creo que hemos ganado cinco años en la digitalización de la educación lo que ha facilitado mucho la labor de todo el mundo. Hemos creado la plataforma educamadrid que emplean tanto profesores como alumnos. En la educación a distancia, su reto principal es que las herramientas que tenemos sean fáciles de usar para todo el mundo. Uno de los retos es que intentamos facilitar el uso de aulas virtuales pero te encuentras profesores a los que les cuesta usarlas, por eso la usabilidad es fundamental. Luego está la parte del equipamiento, hay un GAP del acceso a la tecnología ya que no todos los niños han podido acceder a ello por eso hemos intentado llegar a un 10% de los alumnos con estas dificultades dándoles equipamiento, pero te encuentras con limitaciones presupuestaria. Para llegar al 10% de los alumnos hemos tenido que gastar 30 millones de euros”.

### COMPETENCIAS DIGITALES

Otro de los problemas es el de la adquisición de competencias digitales. En este sentido, Max Meinke, Director General Iberia y Latam de TTS explicó que “España es el segundo país de la UE en ofrecer servicios digitales a sus ciudadanos, sólo por detrás de Estonia. Sin embargo, ocupamos el puesto 17 en el uso de estos servicios por parte de la ciudadanía. Esto es por una falta de cultura digital y porque tenemos un reducido nivel de competencias digitales básicas. La pandemia ha puesto de manifiesto esta realidad. La única forma que tenía la ciudadanía de relación con las AAPP era digital, por lo que mucha gente tuvo que dejar de relacionarse con la Administración. La crisis ha puesto de manifiesto la desigualdad entre la oferta y el deficiente uso de la ciudadanía. Los planes gubernamentales se van a centrar en reducir esa brecha digital”. Este directivo además, incidió en que el teletrabajo se ha impuesto entre los ciudadanos y también entre los funcionarios. “Vemos que los empleados públicos tienen que hacer uso más intensivo de las aplicaciones digitales y necesitan formación específica para su uso lo que es un reto importante. En mi opinión, lo que hay que hacer es humanizar la digitalización reduciendo la brecha digital de los funcionarios. Y este es el objetivo que tenemos en TTS. Tenemos varios proyectos de este tipo de los cuales, muchos son compatibles con las ayudas de los fondos Next Generation EU”.

Por otro lado, las Administraciones no han empezado a digitalizarse ahora. Tal y como opina Carol Zabaco, Coordinadora de TICs y Transparencia para el Gobierno Abierto de Ayuntamiento de Barakaldo, “las AAPP llevamos muchos años trabajando en la modernización de los servicios que prestamos a la ciudadanía. Ya estábamos en ello cuando llegó la pandemia, pero esto es un proceso de adaptación. No era fácil decirle a un funcionario que hiciera su trabajo de



Conchi García, Directora de Capacitación Digital de Madrid Dígita



Carol Zabaco, Coordinadora de TIC's y Transparencia para el Gobierno Abierto de Ayuntamiento de Barakaldo



Juan Carlos Peciña, Jefe del Servicio TIC de Gerencia Regional de Salud de Castilla y León



Fco José Sánchez, Jefe Área Sist Clínicos de Información,

### LOS PARTICIPANTES



Fernando García,  
Subdirector Gral TIC de C.  
Madrid (Consejería de  
Educación y Juventud)



Juan Antonio Gómez,  
Subdirector TIC Servicio  
Andaluz de Salud



Jaime Pintos, Abogado y  
Consultor experto en  
contratación pública

otra forma a como lo estaba haciendo y con unos medios digitales que no están capacitados para usar. Esto supone un cambio radical para ellos. La pandemia nos ha pillado en un momento bueno y ha incidido más en poner el foco en cómo nos relacionamos con la ciudadanía. Para mí esto es lo más relevante: cómo hemos sido capaces de poner proyectos en marcha y a capacitar a funcionarios y ciudadanía a cambiar la forma de trabajar y operar de forma radical. Nos ha pillado en un momento bueno porque para mí el tener la firma digital en la nube ha hecho que avancemos mucho. Nuestro objetivo es que si un ciudadano va a una atención presencial es porque lo ha decidido así aunque sepa que existe la sede electrónica. Esto se consigue con la facilidad de uso. Nosotros lo hemos logrado gracias a una herramienta de TTS que guía al ciudadano a hacer los trámites de forma fácil y sencilla y de forma guiada". Para Conchi García, Directora de Capacitación Digital de Madrid Digital, "en los últimos años nos hemos visto arrollados con dispositivos y aplicaciones que cambian de un mes para otro. No nos hemos dado cuenta, pero nos ha cambiado la vida. Con la pandemia se ha acelerado el ritmo de adopción de esa transformación digital y lo que vemos es que hay personas que se quedan atascadas y no avanzan como ya ocurrió en la revolución Industrial. Ahora estamos en un modo híbrido. Las personas necesitamos adquirir capacidades digitales y las Administraciones deben ser un elemento esencial en la reducción de la brecha digital y en formar a las ciudadanía en competencias digitales. Porque pueden y deben. El ciudadano debe saber que hay un cambio y debe incorporar esos cambios a su día a día y la Administración debe ser ayudarlo. El objetivo es viajar de la Administración Electrónica a la digital, que no es lo mismo".

#### SANIDAD: NO SÓLO MEDICINA

El sanitario, sin duda, ha sido el sector que más ha sufrido los efectos de la crisis provocada por el coronavirus. Pero no sólo a hospitales y médicos. Como aseguró Juan Carlos Pecifia de Frutos, Jefe del Servicio de Tecnologías de la Información de Gerencia Regional de Salud de Castilla y León, "también al departamento TIC ya que hemos tenido que implementar servicios nuevos porque estábamos con una ciudadanía muy acostumbrada a la presencia. Hemos salido adelante pero hay un GAP importante que cubrir, que no solo afecta a la capacitación digital de los ciudadanos sino que también hemos visto que en lo que se refiere a los profesionales el reto ha sido muy importante, ya que trámites que antes los hacían de forma presencial, ahora lo tienen que hacer de manera digital. Nosotros les hemos puesto herramientas para trabajar pero hemos visto que, aparte de la tradicional resistencia al cambio, nos hemos encontrado con que la edad también es muy elevada y aprender a utilizar ciertas tecnologías, cuesta. Hemos avanzado utilizando todos los medios a nuestra disposición con múltiples herramientas para intentar ampliar las capacidades digitales de los profesionales".

#### UNA ADMINISTRACIÓN PRÁCTICA

Como afirmó Ángel González, Territory Manager Adobe, uno de los objetivos es dirigirse hacia una nueva Administración Digital. En su opinión, "la pandemia ha puesto de manifiesto la necesidad que tienen las

## LOS PARTICIPANTES

AAPP, y deben entender la digitalización de una forma más práctica. Se han hecho apuestas muy importantes para prestar sus servicios de forma digital. Nosotros, aparte de las soluciones de creatividad trabajamos en torno a Adobe Experience Cloud para ayudar a las AAPP a afrontar los retos de la digitalización. Hablamos de herramientas como la analítica digital, la valoración, etc. El primero de esos retos que tienen que abordar es el de la agilidad. Necesitamos que las plataformas digitales den agilidad tanto a las áreas de negocio como a las áreas de soporte TIC. Otro reto es la reutilización. Hay que ir a modelos de arquitectura transversal que ofrezcan soporte a cada una de las necesidades. Otro apartado importante es la gobernabilidad: hay que tener un modelo de gobierno en el que cada área de negocio trabaje de forma independiente. No nos podemos quedar parados porque esto es un proceso en el que hay que incorporar estrategias de mejora continua dentro de la estrategia de canales digitales., Y por último hay que incorporar la personalización, se trata de dar una atención personalizada para cada perfil, porque no es lo mismo la persona que se relaciona de forma habitual con alguien que solo una vez”.

Y, ¿qué ocurre con la ciberseguridad. Tal y como expuso Juan Antonio Gómez Palomeque, Subdirector TIC Servicio Andaluz de Salud, “la seguridad es la gran olvidada de los sistemas y de las Administraciones porque es algo que no se ve. Cuando hablamos de AAPP lo que no se ve, no se vende. Son inversiones necesarias pero no tiene la trascendencia que tiene un portal, por ejemplo. Con los últimos ataques esta visión ha empezado a cambiar. Hemos de tener claro que la ciberseguridad es vital una vez que empezamos a dar servicios digitales a los ciudadanos. Hemos creado una dependencia, con herramientas que se utilizan cada vez más. Lo importante es tener en cuenta que una parte importante de las inversiones que se tengan que hacer tiene que incorporar la ciberseguridad porque cada vez hay un mayor número de ciberdelicuentes, bien porque quieren pedir un rescate o porque quieren obtener determinados datos”.

Finalmente, Julia Santos, Sales Manager de Dynatrace, afirmó que “la pandemia ha puesto de manifiesto determinadas carencias y tener una mala experiencia implica no tener acceso a unos servicios públicos que deberían ser universales. Y esto ha ocurrido. La buena noticia es que la digitalización está contemplada como una palanca para la recuperación y una parte de los fondos europeos van a ir a las AAPP para apoyar su digitalización. Entendemos que las AAPP van a tener foco y fondo para mejorar la relación que tienen los ciudadanos con ella. Si ya entramos en cómo mejorar la experiencia digital es necesario trasladar que el ciudadano tiene que estar en el centro. Hay que ofrecer servicios personalizados, que cuenten con la omnicanalidad y que sean proactivos. Además hay que simplificar los accesos. Se trata de facilitar capacitación, el acceso, la creación de chatbots, etc. Esto es algo muy importante. Desde Dynatrace nos preguntamos por qué las AAPP y organizaciones se obsesionan en medir cosas que no son importantes. Cuando hablamos de monitorización y observabilidad, por ejemplo, por qué se empeña en obtener unos datos que no son importantes cuando lo importante es saber cuál es la percepción que tiene el ciudadano del servicio que se le está ofreciendo. Es necesario monitorizar la experiencia real del ciudadano. Nosotros proponemos una observabilidad que vaya de fuera hacia adentro, que se monitorice de forma proactiva y que el ciudadano no se entere de que ha habido un problema”.



Ángel González, Territory  
Manager Adobe

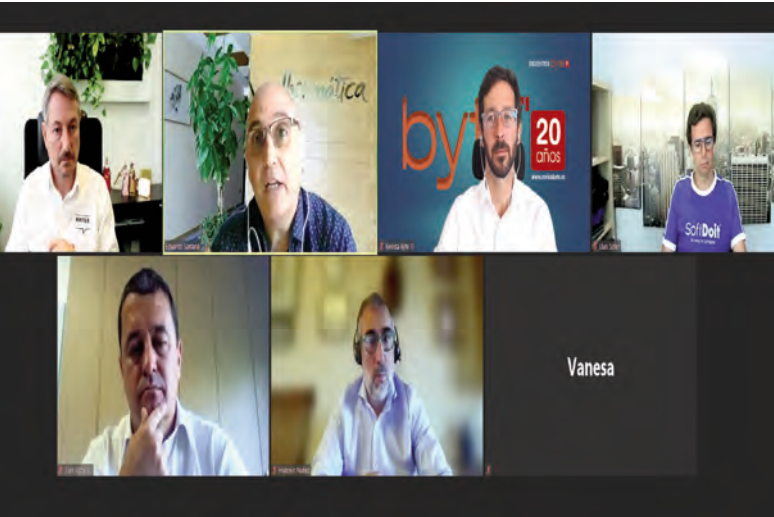


Julia Santos, Sales  
Manager de Dynatrace



Max Meinke, Director  
General Iberia y Latam de  
TTS

# La importancia del ERP y el CRM



Para hablar sobre el CRM y el ERP y su importancia en las empresas, Byte TI organizó un encuentro que contó con la presencia de Juan Valderas, Director de Desarrollo de Negocio de QAD; Eduardo Santana, Microsoft Business Cloud Advisor 365 en Ibermática; Joan Mora Bosch, CEO de Kriter y Francesc Nuñez, ERP y Gestión Product Manager de Wolters Kluwer. El encuentro fue moderado por Lluís Soler, Co-Founder y CEO, Softdoit.

Por Vanesa García

Este tipo de soluciones se han constituido como los pilares para sustentar la transformación digital de las compañías ya que permiten que un negocio lleve a cabo este proceso en esa dirección. Sin este elemento que ha favorecido la implementación de soluciones CRM y ERP ha sido la nube.

Pero, ¿cómo están estas soluciones en el mercado? Para Joan Mora Bosch, CEO de Kriter el mercado se encuentra efervescente, “la pandemia ha acelerado la transformación de la demanda, a pesar de ello, la oferta no ha avanzado a la misma velocidad. Las empresas tienen soluciones muy sofisticadas para satisfacer a los clientes, por lo que veo con optimismo este mercado que beneficiará a las empresas que quieran llevar a cabo una transformación digital al 100%”.

Por su parte, Eduardo Santana, Microsoft Business Cloud Advisor 365 en Ibermática opina que “paradójicamente, la pandemia ha servido como reactivo para determinadas prácticas, en ese sentido la nube es un elemento indispensable. Otro paradigma muy importante es el teletrabajo, que ha venido para quedarse. Esto no es llevarse el portátil a casa, necesitamos una plataforma que nos permita acceder a los datos de forma segura. El ERP y el CRM debemos entenderlo como un todo y racionalizarlo en términos económicos con el pago por uso”. En palabras de Juan Valderas, Director de Desarrollo de Negocio de QAD, “la situación global de mercado está en alza. Las oportunidades están ahí, es un momento interesante para los fabricantes, constructores y para las empresas, ya que se encuentran en un momento donde pueden dar un paso muy importante en su organización. Este es el inicio de un largo movimiento en esta materia”.

El comienzo del 2021 ha sido sorprendente a nivel mercado, como bien explica Francesc Nuñez, ERP y Gestión Product Manager de Wolters Kluwer, “durante los periodos más duros de la pandemia ha habido que gestionar muchos trámites, la respuesta desde Wolters ha sido excelente. Esta tendencia de efervescencia en la demanda muestra una búsqueda de soluciones de implementación mucho más rápidas. Se buscan soluciones más centradas en el usuario, una respuesta rápida y eficaz, con una acción-reacción”.

## EL PAPEL DE LA NUBE

Si hablamos del papel que está jugando la nube en el mercado del ERP y CRM, Francesc Nuñez lo tiene claro, “la nube ha dejado de tener el significado que tenía. La nube para nosotros, no es ni más ni menos, que una herramienta para los fabricantes, es una oportunidad de oro. Es la herra-

mienta que nos permite que articulemos nuevas herramientas. Las generaciones que vienen son puras digitales, por ello decir que eres cloud no es algo novedoso. La nube es la mejora entre el tiempo de concepción y la entrega al usuario de la solución”.

Desde QAD reitera que la nube no es nada nuevo, ellos mismos llevan casi 18 años distribuyendo software en la nube, “ya no es una novedad, es algo necesario. Lo que vemos en industria es que estamos en medio de una revolución tecnológica, lo que acelera el tiempo de creación de nuevas tecnologías, lo que hace que los mercados y los clientes sean mucho más exigentes. Estamos en un entorno muy variante, que requiere una actualización rápida, de ahí surge las tecnologías cloud como factor y facilitador”, explican.

Para Eduardo Santana el usuario digital busca si o si la nube, “lo más importante que ofrece la nube es que pone el foco en el negocio, es decir, en aquello que realmente es importante. Nos aporta una reducción de costes y mayor flexibilidad, pues nos permite reducir todo lo que tiene que ver con los sistemas y ajustarlos a lo que se necesita en cada momento, ya que estamos en un escenario muy cambiante. También nos ofrece accesibilidad, todo lo que tiene que ver con las integraciones se simplifica y se integran en la nube. Todo mejora la productividad de los usuarios”.

“Nosotros desde Kriter nos dedicamos, de laguna forma, a enmascarar la tecnología, para que el cliente simplemente vea las soluciones que hay detrás. Nos dedicamos a las pymes, el cliente medio es de 20 a 25 usuarios. Vemos que estas compañías se han transformado por completo, ya no buscan tener una atención al cliente telefónica, prefiero hacerlo de forma online. En este aspecto, la nube facilita este proceso. El cliente busca disponibilidad 24/7, integración y sistemas abiertos, inmediatez. La nube es una revolución evolutiva”, concluye Joan Mora.

## LA TRANSICIÓN AL CLOUD

Las empresas son personas, y cada una gestiona su compañía de una forma u otra en base a sus experiencias y expectativas, en este punto, como explica Eduardo Santana, “la reticencia inicial que había relacionada con la seguridad de la información que alojamos en la nube ya ha quedado atrás. Pues el mercado percibe la nube con un nivel de plataforma de seguridad certificada que sería muy complicada de conseguir en otro medio. La nube beneficia el desarrollo de IA, Big Data, IoT, la seguridad, desarrollo de aplicaciones... Para llevar a cabo una buena transición es necesario saber que es lo que nos ofrecen estas plataformas y establecer una estrategia que muestre los objetivos que planteamos para el negocio. Es una cuestión de estrategia”.

En opinión de Juan Valderas, la transición al cloud es un tema de estrategia, pero en contraposición con su compañero, afirma que no todos los sectores se han adaptado tan bien al cloud, pues en sectores como el de las manufacturas existe reticencia, “todavía tenemos que hacer un trabajo de evangelización para adaptar estas mejoras. Debemos tener más velocidad en la empoderación de los CIOs como elemento estratégico de la compañía y



Juan Valderas, Director de Desarrollo de Negocio de QAD

“La situación global de mercado está en alza”



Eduardo Santana, Microsoft Business Cloud Advisor 365 en Ibermática

“La pandemia ha servido como reactivo para determinadas prácticas”



Joan Mora Bosch, CEO y fundador de Kriter

“Las pymes ya no buscan tener una atención al cliente telefónica”



Francesc Nuñez, ERP y  
Gestión Product Manager de  
Wolters Kluwer

“La nube ha dejado de tener  
el significado que tenía”

enrocado con el control de gestión y los procesos de negocio. El principal paso que hay que dar es identificar la tecnología como una ventaja competitiva del sector, ese es el principal camino”.

Siguiendo esta misma línea, Francesc Nuñez explica que, “en Wolters hemos incitado la transición al cloud desde hace varios años, pero no hemos transformado la solución que teníamos al cloud, hemos construido nuevas soluciones. Nosotros vemos dos tipos de transformaciones a la web: la que viene ‘forzada’ y el mercado de despachos. Con la forzada vemos que tenemos demanda de servicios cloud”.

Por parte de Joan Mora desde Kriter la transición al cloud la están viendo de forma natural, “vendrá forzada por la propia tecnología, muchas compañías se están pasando a plataformas como Microsoft 365 y se van a la nube, pero sabemos que mantener una aplicación ex-changed para una empresa mediana es complicado, todo va a ser cloud. Nosotros lo que hacemos es acompañar al cliente con la mejor solución que necesita en cada momento. El cliente quiere alta disponibilidad, antes ofrecíamos esto on-premise, ahora podemos ofrecerlo en cloud. Nos van a ofrecer la nube de bolsillo”.

### INTELIGENCIA ARTIFICIAL Y BIG DATA

En los próximos años la IA y el Big Data tendrán un papel muy importante en el uso de estas herramientas de ERP y CRM. Dentro del sector manufacturing, empresas pequeñas, grandes de ámbito global, está todo muy enfocado a la gran digitalización en esta línea. “Van a jugar un papel fundamental dentro d un espectro completo, la industria 4.0 serán datos, recogerlos, procesarlos, almacenarlos y compartirlo, el Big Data está en este camino. El IoT nos ayudara a ser ágiles, la IA y el Machine Learning para el procesamiento de datos. Todo esto es fundmanetal para la digitalización”, comenta QAD.

Desde Wolters Kluwer afirman que, “El Big Data, la IA se pueden unificar creando un concepto, la nube. Por si mismo no va a ser relevante, es una herramienta más. Pero siempre con un filtro de aplicación, para que va a servir y que valor va a portar la negocio. Son dos ámbitos más que ya se están aplicando”.

Siguiendo esta línea, “la IA y el Big Data son una herramienta más para analizar los datos, son un valor extra que aportan a nuestro usuario final y al cliente del usuario final. Son soluciones que hospedemos aportar y que hasta hoy no se podía, bien por precio de infraestructuras. Hoy están al servicio de todos con pago por servicio”, explican desde Kriter.

Para finalizar este tema, “para nosotros son herramientas de transformación digital, la capacidad de poder recoger datos más allá de nuestros sistemas y analizarlos a través de IA es esencial para obtener información útil y tomar decisiones de una forma productiva. Esto ya es una realidad”, dicen desde Ibermática.

### INTEGRACIÓN ENTRE CRM Y ERP

A la pregunta de si existe la posibilidad de una integración total del CRM y el ERP Francesc Nuñez lo tiene claro, “definitivamente sí, no puede ser de otra manera. Conceptualmente muchos podemos pensar en el CRM como la preventa, pero este y el ERP deberían emanar. La relación con el cliente no acaba cuando compran. Ya hay bancos que te acompañan de una forma 360. La respuesta es un rotundo sí”.

En palabras de Eduardo Santana “deben funcionar como una sola pieza. Muchos sistemas ya esta integrados. No se trata solo de unir los procesos, si no que para el usuario sea transparente. El usuario quiere que las aplicaciones emergen cuando las necesitan. Rotundo sí, y ya es un hecho”.

Para Juan Valderas es sun sí y un no, “lo que realmente importa es el proceso, la necesidad de negocio, es la actividad que cada cliente tiene que resolver, no todas las empresas necesitan lo mismo. Las actividades propias de un CRM son muy diversas. Sí porque todos los ERP ampliamos las capacidades del CRM, pero siempre hay excepciones”.

Finalizando con el debate, Joan Mora explica que “tengo una respuesta afirmativa total ante esto, hace más de 10 años que hemos desarrollado el CRM dentro del ERP. Nosotros no concebimos que un comercial no entienda una llamada sin tener una alerta. Esta integración es ya una sola pieza”.



## EMPRESAS PARTICIPANTES

### WOLTERS KLUWER

a3ERP es la solución integral de gestión para pymes de Wolters Kluwer, que aporta una visión 360° de todos los procesos productivos y administrativos de la empresa, optimizando recursos, simplificando procesos y ayudando en la toma de decisiones para una gestión eficiente, con las máximas prestaciones de análisis y control y en un entorno de trabajo único.

### QAD

La próxima generación de ERP es más que un simple software, combina las mejores prácticas de la industria, una plataforma flexible y una experiencia de usuario adaptable (UX), con capacidades de tecnología avanzada para permitir la transformación digital. QAD ofrece el mejor ERP en nube de próxima generación del mercado, ayudando a los fabricantes a aprovechar la disrupción para obtener una ventaja competitiva.

### KRITER

Desarrollamos soluciones de confianza que facilitan el trabajo a la PYME. La SUITE KRITER ERP tiene todo lo que necesita para el mundo online (CRM, B2B/B2C, Apps móviles) con la libertad de elegir entre el modelo tradicional o en la nube y contar con la implicación de un fabricante, de proximidad, con más de 30 años de trayectoria y un propósito consciente: ayudar a nuestros clientes a ser aquello con lo que sueñan.

### IBERMÁTICA

Ayudamos a la transformación digital de las empresas para mejorar su competitividad mediante la aplicación de la tecnología basada en soluciones de Microsoft y el amplio conocimiento de los sectores en los que operamos. Más de 400 clientes nos confían sus proyectos de Implantación de ERP, optimización de procesos de negocio, optimización de procesos comerciales, reingeniería de procesos, y gestión del cambio. En el Centro de Excelencia de Microsoft juntamos valor añadido, tecnología, innovación y visión empresarial, generando el impulso necesario para abordar los proyectos más valiosos para nuestros clientes.

## Zyxel USG FLEX 100



Zyxel

Web:

[www.zyxel.com](http://www.zyxel.com)

Precio:

Desde 500 euros

Valoración Global



Zyxel Networks ha introducido la serie de switch USG FLEX. Con el lanzamiento del nuevo USG FLEX 100 la compañía quiere proporcionar una única plataforma de gestión en la nube que amplía la protección del firewall en los puntos de acceso. Analizamos algunas de sus principales características:

Zyxel USG FLEX 100 va fundamentalmente dirigido a los profesionales que teletrabajan y a los pequeños negocios que necesitan un acceso seguro y rápido a la red, si bien puede ser utilizado por otras organizaciones dadas las nuevas funcionalidades en seguridad que incorpora. Un aspecto clave es que minimiza el uso de energía informática y maximiza el rendimiento del firewall, a la vez que ofrece hasta 5 veces el rendimiento UTM con flexibilidad en cloud y un 125% más en el del firewall. Todo ello para proporcionar mejor conexión y seguridad de las pymes.

La nueva solución para Nebula de Zyxel cuenta con una política granular de seguridad Zero-Trust para facilitar autenticaciones de inicio de sesión y WiFi segura. Igualmente, su función de detección y res-

puesta colaborativas (CDR) puede utilizarse para identificar las amenazas y los riesgos que entraña los lugares de trabajo de las organizaciones, incluso las más complejas. El procedimiento se basa en que, si el firewall detecta una amenaza en cualquiera de los clientes conectados, se sincroniza directamente con el centro de control de Nebula.

El dispositivo incluye la nueva función Secure WiFi para crear un punto de acceso “drop-in” que se puede configurar para replicar el SSID de la oficina y crear un túnel seguro con el fin de acceder a la red corporativa desde el hogar u otras ubicaciones. Con ello lo que pretende la firma es simplificar la implementación al desplegar una opción “plug-n-play” manteniendo seguridad la hora de trabajar.

Por otro lado, USG FLEX 100 cuenta con filtrado de web a través de filtros basados en reputación y categoría. Además, el filtro DNS inspecciona el acceso a web, en especial cuando el sitio está implementando ESNI (indicación de nombre de servidor cifrado) donde el filtrado de URL tradicional no es aplicable al dominio del destino.

Asimismo, el dashboard presenta SecuReporter, un resumen de tráfico fácil de usar con estadísticas visuales de amenazas. Su misión es la de facilitar un análisis de amenazas con el diseño de funciones de correlación para un seguimiento proactivo del estado de la red y así evitar intrusiones.

En resumen, es un dispositivo expresamente indicado para dar la seguridad que las pymes y los pequeños negocios necesitan ante el teletrabajo. Además, USG FLEX 100 dispone de inteligencia sobre amenazas de las principales empresas de ciberseguridad para obtener la información precisa del estado de la seguridad.

# XXI TORNEO GOLF

byte 



AOC

servicenow



Lexmark

SOPHOS  
Cybersecurity evolved.



Wolters Kluwer



dynamabook



Compusof

# Los mejores ERPs

**N**o importa el tamaño que tenga una compañía o su actividad. Existe una herramienta de especial valor para que alcance sus objetivos y mantenga la productividad y la competitividad exigidas en el mercado.

Nos referimos a los programas de planificación de recursos empresariales o ERPs. Se trata de una serie de herramientas que cada vez son más necesarias para cualquier tipo de empresa. En ellos destaca la facilidad de uso. Ya no se requieren apenas conocimientos como en las soluciones de antaño. Sus características proporcionan un alto grado de flexibilidad y personalización, incluyendo varios módulos para cada una de las áreas de una organización. La siguiente selección reúne un total de seis de los mejores ERPs que se pueden adquirir en la actualidad, aunque en nuestra edición web podrán ver esta misma comparativa ampliada hasta a doce soluciones.

### LOS PARTICIPANTES

Por orden alfabético, Aqua eBS es una aplicación para la mediana y pequeña empresa que puede ser utilizada por personas y por cualquier software externo, desde soluciones web, apps y bots empresariales.

También participa Microsoft con su producto Dynamics 365, un conjunto de aplicaciones empresariales inteligentes que ayudan a gestionar todo el negocio para mejorar resultados a través de conocimientos predictivos generados mediante inteligencia artificial.

Otro de los programas destacados es Oracle Fusion Cloud ERP en el que encontramos los siguientes módulos: financieros, gestión de proyectos, compras, gestión de riesgo y compliance, EPM, SCM y fabricación y analítica.

Mientras, Sage 200 Advanced está disponible en tres versiones y Solmicro aterriza con su nuevo producto ERP 6. Cierra Wolters Kluvers a3ERP, la conocida solución de gestión que proporciona una visión 360° de la compañía.





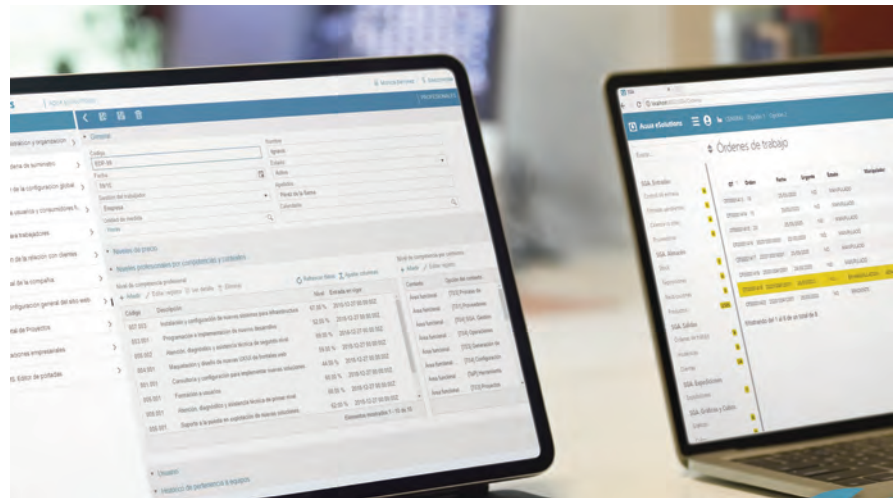
## Aqua eBS

Disponibile en diferentes modelos de implementación, sus características abarcan todas las funciones claves del negocio

La empresa española Aqua eSolutions ofrece Aqua eBS. Se trata de un ERP que destaca por su flexibilidad, alta capacidad de integración, escalabilidad y extensa funcionalidad estándar; una aplicación diseñada para la mediana y pequeña empresa que puede ser utilizada por personas (usuarios y programadores) y por cualquier software externo, desde soluciones web, apps y bots empresariales.

Facilita, además, la digitalización a través de la gestión de todas las áreas del negocio de forma integrada y la automatización de procesos a través de bots y apps, optimizando así los recursos de las organizaciones. En relación a este aspecto, cabe comentar que la herramienta facilita la integración de datos y la interoperabilidad a través de bots que programan y automatizan procesos y se integran con cualquier aplicación o web externa.

Si entramos en detalle, el ERP Aqua eBS abarca todas las funciones clave del negocio a través de una extensa funcionalidad estándar que incluye las siguientes opciones: contabilidad y finanzas, cadena de suministro, almacén, capital humano, gestión de clientes, producción, gestión de proyectos y operaciones, gestión de puntos de venta, informes y análisis del negocio, gestión de calidad, portal de proveedores y soluciones integradas de ecommerce b2b y b2c... Al tratarse de una herramienta flexible, modulable y personalizable, esto pone de mani-



fiesto su capacidad de adaptación. También permite que los usuarios extiendan y personalicen la solución por sí mismos a través de un potente entorno de desarrollo propio integrado.

Aqua eBS se distingue también por su especialización sectorial. En concreto, cuenta con hasta 17 soluciones sectoriales por industria y sector, Aqua Industry Solutions, que han sido desarrolladas a partir del conocimiento del negocio y el mercado que ha adquirido Aqua eSolutions, así como su experiencia de 32 años en multitud de proyectos. Algunas de estas soluciones son: distribución mayorista, servicios técnicos profesionales, sector de construcción y empresa auxiliar, sector de alimentación y bebidas, industria química y cosmética, alquiler de maquinaria y equipamiento, sector ferretería y suministro industrial y

sector de comunicación y telefonía móvil, entre otros.

Las funcionalidades de reporting y analítica se encuentran presentes para ofrecer una visión empresarial del negocio con informes y cuadros de mando integrados a través de una solución de business intelligence embebida en el ERP. La plataforma se actualiza periódicamente y se la dota de la última tecnología, funcionalidades y normativa. Por último, está disponible mediante estos tres modelos de implementación: on premise, en la nube o modelo híbrido.

**Aqua eSolutions**

**Tel:** :917 334 200

**Web:**

[www.aquaesolutions.com](http://www.aquaesolutions.com)

**Precio:** consultar

# Microsoft Dynamics 365

Desplegado en la nube Azure, dispone de Power Apps para que las organizaciones diseñen aplicaciones a medida, personalizadas y sin necesidad de saber programar.

Bajo el nombre de Dynamics 365, el gigante de Redmond propone un conjunto de aplicaciones empresariales inteligentes para que las compañías gestionen su negocio y mejoren sus resultados a través de conocimientos predictivos generados mediante inteligencia artificial. Esto le permite añadir valor a cada una de las capas de análisis de datos, permitiendo automatizar tareas específicas y mejorar las actividades relacionadas y el proceso general de apoyo a la decisión. Cuenta, para ello, con un amplio abanico de aplicaciones enfocadas a áreas relacionadas con ventas, finanzas, recursos humanos, operaciones, automatización y marketing, servicio al cliente...

Con un óptimo aprovechamiento de la información disponible, se integra, por un lado, con herramientas de productividad como Microsoft 365 y, por otro, funciona según un modelo de pago por uso en el que el cliente tiene lo que necesita sin compromiso de permanencia. Además, Microsoft Dynamics 365 ofrece una alta seguridad. Se despliega en la nube de Microsoft y, a las certificaciones ya existentes de los servicios en Azure frente al nivel más exigente del Esquema Nacional de Seguridad (ENS), se suma la publicación de guías técnicas y scripts de automatización de las configuraciones de seguridad cumplidoras con el nivel alto del ENS para ocho servi-



cios cloud de la compañía. También tiene integrado Microsoft Power Apps, un servicio para el desarrollo personalizado y a medida de todo tipo de aplicaciones cuyo objetivo es cubrir todas las necesidades de una organización con independencia de su sector de pertenencia. Con Power Apps cualquier empresa puede diseñar aplicaciones a medida, personalizadas y de manera autónoma sin la necesidad de saber programar.

Incluso, hay espacio para la realidad mixta. En este caso, HoloLens 2 proporciona una experiencia de realidad mixta cómoda e inmersiva, desarrollando un trabajo colaborativo que traslada virtualmente al experto al lugar donde debe desarrollarse la intervención para verlo mismo que el técnico desplazado e interactuar con él por medio de anotaciones e indicaciones ho-

lográficas. Todo ello, con un acceso completo a esquemas, documentos técnicos y a la información necesaria para realizar el diagnóstico o la intervención en remoto. De este modo, se reducen de manera importante los costes de servicio y se optimizan los tiempos de resolución de problemas. Esta tecnología, unida a la inteligencia artificial antes citada, pretende que las empresas aceleren el proceso de capacitación de trabajadores, automaticen los procesos de solicitud de reparación u optimicen la detección de anomalías.

**Microsoft**

**Teléfono:** 91 391 90 00

**Web:**

[www.microsoft.es](http://www.microsoft.es)

**Precio:** consultar

# Oracle Fusion Cloud ERP

La solución de Oracle incluye estos módulos: financieros, gestión de proyectos, compras, gestión de riesgo y compliance, EPM, SCM y fabricación, y analítica.

Se presenta como una única fuente de datos consolidada y con inteligencia y machine learning embebidos, lo que significa que las empresas no tienen que instalar después estas funcionalidades como adicionales. Con actualizaciones automáticas cada 90 días, facilita una rápida migración a la cloud, mejora la eficiencia operativa y minimiza el coste de propiedad. El ERP se compone de estos módulos: financieros, gestión de proyectos, compras, gestión de riesgo y compliance, EPM, SCM y fabricación, y analítica.

Oracle Financials brinda una visión completa de la situación financiera para que las empresas tomen en cada momento las mejores decisiones. Sus características incluyen: gestión de gastos, gestión de empresas conjuntas, cobros, cuentas por cobrar, gestión de ingresos, cuentas por pagar y activos, informes y analítica, y un centro de contabilidad. Por su parte, Oracle Project Management (gestión de proyectos) ayuda (entre otros) a planificar y realizar un seguimiento de estos proyectos, y aumentar o disminuir los recursos en función de las necesidades que haya que cubrir. En este módulo, hay espacio para las analíticas, el control de costes, contratos y facturación de proyectos, y labores de gestión relacionadas con tareas, costes o subvenciones.

Mientras, el módulo de compras se emplea para simplificar la gestión de proveedores, mejorar la rentabi-



lidad y reforzar el cumplimiento de los datos. El cuarto módulo es el de gestión de riesgos y compliance. Recurre a la ciencia de datos integrada para reforzar los controles financieros, detectar riesgos emergentes o frenar las pérdidas de liquidez, a la vez que se reduce el tiempo destinado a las tareas de seguridad y cumplimiento. Este módulo brinda a los negocios informes automatizados de cumplimiento de segregación de funciones, una supervisión continua de la seguridad de los usuarios y de los cambios de configuración, flujos de trabajo de gestión de riesgos empresariales, de SOX, auditoría y certificación...

En cuanto al módulo de gestión del rendimiento empresarial (EPM), sus características (informes fiscales y expositivos, planificación, conciliación de cuentas, o gestión

de costes y rentabilidad) sirven para modelar y planificar en las áreas de finanzas, recursos humanos, cadena de suministro y ventas. También optimizar el cierre financiero y obtener información para impulsar la toma de las mejores decisiones. Finalmente, estarían los módulos de cadena de suministro y fabricación, y analítica ERP. El primero garantiza la creación de una cadena de suministro resistente y el segundo provee de análisis predictivos e indicadores clave de rendimiento basándose en análisis de varianza.

**Oracle**

**Teléfono:** 902 302 302

**Web:**

[www.oracle.com/es](http://www.oracle.com/es)

**Precio:** consultar



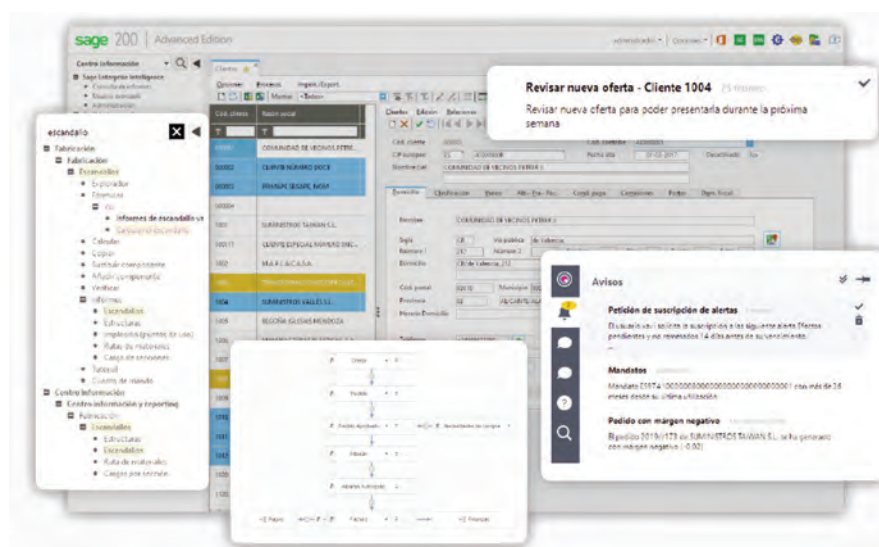


# Sage 200 Advanced

Permite acceder a funcionalidades de alta productividad y apoyo a la transformación digital como la firma digital o eCommerce

Sage 200 Advanced es una solución ERP de gestión empresarial integral, modular, personalizable, conectada a la nube y totalmente adaptable a las necesidades del negocio, independientemente del sector al que pertenezca. Ha sido diseñada especialmente para pymes de entre 20 a 200 empleados, aunque también está recomendada para aquellas empresas que necesitan entre 3 y 15 usuarios de ERP de forma simultánea y ampliable a los que sean necesarios. Esto facilita una gestión ágil e integrada de toda la organización. Sus principales clientes se encuentran entre las organizaciones centradas en el ámbito de la distribución, fabricación, servicios, retail y gestión de proyectos.

En lo que respecta a su funcionalidad, dispone de una gran variedad de tareas automatizadas que ayudan a ahorrar tiempo y costes. Además, gracias a la oferta modular y a la modalidad de pago por suscripción, los negocios pueden gestionar de forma adecuada y controlada la inversión que realizan en este tipo de soluciones. El producto de Sage tiene varias opciones de contratación disponibles a las que se pueden añadir nuevos servicios, y es posible elegir entre las siguientes versiones: Standard, Extra o Extent. Todos los planes cuentan con soporte técnico directo de Sage, ya sea online o por teléfono, lo que asegura que las incidencias sean resueltas con rapidez. Una vez elegida la plataforma, las



pymes pueden añadir distintos módulos de gestión y productividad, entre los que se incluyen: contabilidad y finanzas, gestión y fabricación. Tras la configuración, las compañías disponen asimismo de una serie de módulos de gestión avanzada que pueden sumar al servicio contratado a medida que la gestión de la organización lo requiera: gestión de clientes, atención al cliente y marketing, gestión de proyectos y post-venta, TPV, gestión laboral de recursos humanos, y Business Intelligence.

De igual forma, permite acceder a funcionalidades de alta productividad y apoyo a la transformación digital como la firma digital, gestión avanzada de almacenes, eCommerce, integración con Microsoft 365 y escaneo de facturas, entre otras. Es 100% compati-

ble con las últimas versiones de MS Windows, MS Office y MS SQL Server, e incluye RGPD Ready, un conjunto de funcionalidades avanzadas para el seguimiento y tratamiento del cumplimiento de la gestión, almacenamiento y custodia de documentación relacionada con los datos personales de los contactos que gestionan las empresas: lo que asegura el correcto cumplimiento de la normativa y la ley vigente. Con LiveUpdate, se mantiene actualizado de normativa vigente y de las últimas mejoras de producto.

**Sage**

**Teléfono:** 900 87 80 60

**Web:**

[www.sage.com](http://www.sage.com)

**Precio:** consultar

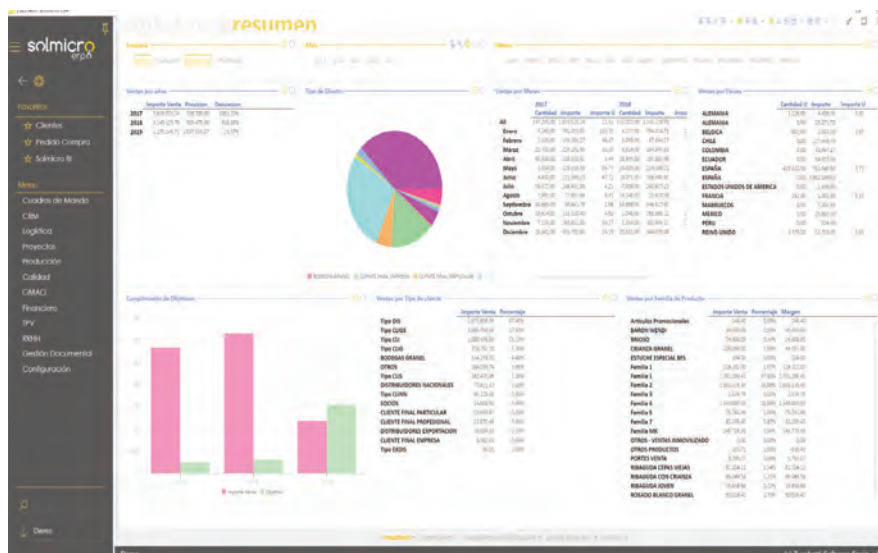
# Solmicro ERP 6



Tiene un sistema de extensibilidad para la máxima personalización funcional y visual, sin tocar el código estándar y evitando conflictos en evoluciones futuras.

Con el objetivo de cubrir las nuevas necesidades de gestión de las empresas en un mercado cada vez más cambiante, Zucchetti Spain ha lanzado Solmicro ERP 6, la nueva versión de su software de gestión. Totalmente renovado, sus claves residen en cuatro puntos clave. El primero es una nueva interfaz de usuario, ahora más visual, atractiva e intuitiva que brinda, entre otros, la configuración de elementos favoritos (programas, acciones, registros, informes...) y una nueva experiencia de búsqueda. Todo ello con el objetivo de potenciar su usabilidad y de reducir la curva de aprendizaje para potenciar la productividad de los usuarios. El segundo es una extensibilidad que permite la máxima personalización funcional y visual sin tocar el código estándar, evitando conflictos en evoluciones futuras del ERP.

El tercer aspecto a destacar es que Zuchetti Spain ha actualizado sustancialmente el 'look & feel' de su ERP con diferentes estilos y experiencias de usuario. Esto explica no sólo que la interfaz se haya simplificado, sino que se hayan eliminado clicks y esperas. Finalmente, sus desarrolladores han reducido de manera significativa los tiempos de desarrollo al eliminar labores de maquetación y estilizado haciéndolo más competitivo. En relación a este último apartado, se percibe un sistema layout de maquetación de pantalla automático donde la organización de los elementos que se muestran en pantalla adopta una estructura arborescente y con un único elemento contenedor, el panel dividido en filas y columnas (decidido el número de columnas, el sistema calcula las filas correspondientes). Junto a un menú centralizado en un único panel con búsquedas instantáneas y favoritos (entre otras características), se han introducido otra serie de mejoras notorias como las relacionadas con la gestión de los formularios (permite abrir el mismo formulario varias veces y en otra ventana), búsquedas avanzadas (por ejemplo, sugerencias al teclear) y gestión de tabs: es posible añadir nuevos tabs en la consola de administración, asignarles seguridad y mostrarlos de tres maneras distintas (flotante, acoplado y desacoplado), así como recordar la selección del usuario



mentos que se muestran en pantalla adopta una estructura arborescente y con un único elemento contenedor, el panel dividido en filas y columnas (decidido el número de columnas, el sistema calcula las filas correspondientes).

Junto a un menú centralizado en un único panel con búsquedas instantáneas y favoritos (entre otras características), se han introducido otra serie de mejoras notorias como las relacionadas con la gestión de los formularios (permite abrir el mismo formulario varias veces y en otra ventana), búsquedas avanzadas (por ejemplo, sugerencias al teclear) y gestión de tabs: es posible añadir nuevos tabs en la consola de administración, asignarles seguridad y mostrarlos de tres maneras distintas (flotante, acoplado y desacoplado), así como recordar la selección del usuario

para futuras sesiones. Cuenta, por otro lado, con campos multivalor configurable a nivel de diseño y contenido.

Con tiempos de implantación más reducidos y adaptaciones para garantizar la máxima rentabilidad de los negocios, su tecnología de última generación ayuda a ofrecer soluciones de inteligencia de negocio, Internet de las cosas, inteligencia artificial, realidad virtual y aumentada, big data... para que los clientes saquen el máximo partido a la información de su empresa.

**Zucchetti**

**Teléfono: 94 427 13 62**

**Web:**

**www.solmicro.com**

**Precio: consultar**

# Wolters Kluwer a3ERP

Existen cuatro versiones para adaptarse a las distintas empresas, y sus módulos se enfocan hacia áreas como facturación, contabilidad o CRM

Global, escalable, adaptable y preparado para ofrecer información en tiempo real en forma de estadísticas, informes y análisis. Sobre estos cuatro pilares se asienta a3ERP, un software de gestión para las pymes que unifica las distintas áreas de una compañía, automatiza tareas y optimiza recursos. Además, se adapta a diferentes tipos de compañías en función de su sector de actividad y necesidades. También destaca por integrarse con Office 365, contar con una diversidad de módulos y soluciones verticales especializadas, y por estar adaptado al Suministro Inmediato de Información (SII), lo que no requiere de plataformas externas al enviar la información solicitada por Hacienda. Asimismo, es posible trabajar con facturas electrónicas con los formatos que requiere la administración.

Para la gestión de todo el negocio, el ERP de Wolters Kluwer facilita que una organización disponga de su información en una misma base de datos, lo que evita errores y duplicidades en su gestión: nóminas, facturación, contabilidad, almacén o CRM son algunos ejemplos. De igual modo, provee de funcionalidades que agilizan la gestión diaria y prometen un mayor control y trazabilidad de los procesos. Esto incluye, por ejemplo, la generación automática de pedidos, albaranes y facturas, cuotas y los informes y documentos predefinidos.

Wolters Kluwer a3ERP está disponible en cuatro versiones. Para mi-



croempresas y autónomos se encuentra el producto base, mientras que la que tiene la 'etiqueta' profesional es idónea para los negocios (hasta cuatro usuarios) que necesitan gestionar el ciclo comercial completo de la compra-venta integrado con la contabilidad. Por su parte, a3ERP plus no tiene límite de usuarios y se dirige a las compañías que necesitan un ERP con todo tipo de funcionalidades para una gestión avanzada del ciclo comercial de compra-venta y financiero, con una amplia política de precios y descuentos, trazabilidad, herramientas para el análisis del negocio y contabilidad avanzada. Finalmente, la versión premium incluye módulos de CRM, TPV, expedientes, producción y herramientas de personalización.

Para que el usuario compruebe fácilmente el estado de su negocio,

brinda un cuadro de mando personalizable con los indicadores que más le interesen al trabajador. Algunos ejemplos son: listados con los principales clientes, representantes comerciales con mayor venta, artículos más vendidos y comparativas de ingresos y gastos o de ventas con el año anterior. Existe, por otro lado, un módulo de análisis de negocio que resulta útil para elaborar toda clase de informes, comparativas y estadísticas exportables a Excel con datos en tiempo real.

## Wolters Kluwer

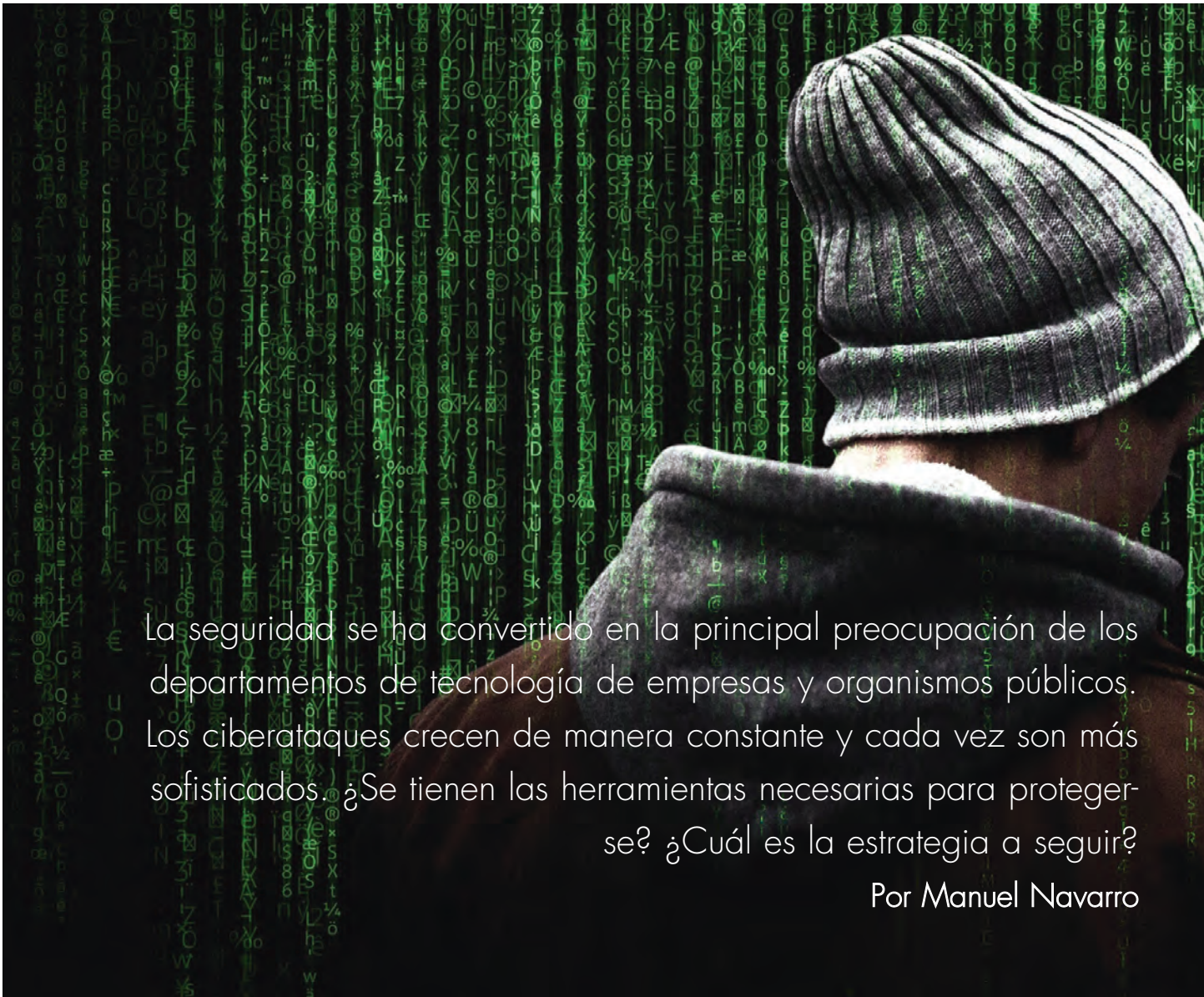
**Teléfono:** 902 330 083

**Web:**

[a3.wolterskluwer.es](http://a3.wolterskluwer.es)

**Precio:** consultar

# ¿Se puede tener un entorno ciberseguro?



La seguridad se ha convertido en la principal preocupación de los departamentos de tecnología de empresas y organismos públicos. Los ciberataques crecen de manera constante y cada vez son más sofisticados. ¿Se tienen las herramientas necesarias para protegerse? ¿Cuál es la estrategia a seguir?

Por Manuel Navarro



Lo que antes eran casos puntuales ahora se han vuelto cotidianos. Basta darse una vuelta por cualquier periódico no especializado de todo el mundo para descubrir que grandes empresas, multinacionales y organismos públicos supuestamente diseñados a prueba de cualquier ciberataque como el Pentágono, están sufriendo constantes amenazas. Según la ONU, cada 39 segundos se produce un ataque exitoso, lo que da cuenta del problema al que nos enfrentamos. Por eso no es de extrañar, que como se afirma en un estudio realizado por Byte TI, tres de cada cuatro responsables de tecnología y CIOs de grandes empresas consideren que las mayores inversiones que deben hacer sus empresas han de estar relacionadas con la ciberseguridad. Y no es para menos, los ataques son cada vez más sofisticados y peligrosos y como asegura Miguel López, director general de Barracuda Networks, “el riesgo es grave y evidente. Todos los días asistimos a ataques que se suceden tanto en el sector público como privado y en todo tipo y tamaño de organismos. Los ciberdelincuentes se rigen simplemente por un criterio de optimización del beneficio y atacan en todos aquellos sectores en los que les es posible hacerlo”.

La situación es preocupante, toda vez que además de los tradicionales



ciberdelincuentes, cada vez hay más grupos extorsionadores, bandas terroristas o incluso estados detrás de cada uno de esos ciberataques. La realidad es que las empresas, organismos públicos y la población en general están expuestas a más riesgos que hace unos años, pues la superficie de ataque se ha ampliado. A esto han contribuido avances tecnológicos como la nube o el IoT, así como prácticas tales como el teletrabajo, que han permitido que los límites del perímetro de la empresa se difuminen. Guillermo Fernández, Manager Sales Engineering de WatchGuard es tajante: “Por supuesto que los riesgos se han incrementado, ya que el trabajador tiene que hacer frente a más peligros y en muchos casos no cuenta con herramientas de defensa. Pensemos por ejemplo, en que algunos teletrabajadores se conectan desde sus ordenadores personales y la organización/administración pública no tiene forma de saber si ese equipo cuenta con una solución de protección del endpoint instalada. Puede darse el caso de que ese empleado se conecte a la red corporativa y su equipo esté infectado... las consecuencias pueden ser terribles para la empresa u organismo. Pensemos en los últimos casos de ataques de ransomware a entidades como el SEPE, la Universidad de Castilla La Mancha, empresas como The Phone House, etc.”.

El coronavirus que ha afectado a todo el mundo tiene su homólogo en el mundo virtual, aunque en este caso, el número de cepas, variantes y mutaciones es infinitamente mayor. Estamos en una situación en la que ni siquiera el Pentágono está seguro, con ciberdelincuentes que ya no sólo quieren obtener dinero, sino que atacan para hacer daño o noquear al enemigo, como en el caso de SolarWinds. Las empresas y organismos no tienen más remedio que incrementar su inversión en ciberseguridad, una inversión que, además, tiene que ser constante. Esto ya no va de comprar una determinada solución. Son necesarias la inversión, la formación continua y las actualizaciones constantes. Porque los ataques, además, ya no van al corazón. Pueden aparecer por cualquier parte, y sobre todo, desde los dispositivos móviles. “Debido a la creciente movilidad en las empresas, cada vez existe una mayor penetración de dispositivos móviles y, por tanto, mayores riesgos. Las compañías se encuentran ante el gran reto de proteger el hardware y software de sus terminales, y cada vez es más necesario tener una única solución integral que ofrezca la máxima seguridad: desde la etapa de producción con la implementación de la seguridad en el hardware, hasta la integridad del software y las aplicaciones. Por lo tanto, son necesarias soluciones de seguridad que realicen las comprobaciones necesarias desde que se inicia el sistema y durante su tiempo de ejecución”, señala Isabel Lopez, B2B Solutions&Services Manager de Samsung.

### LOS PRINCIPALES RIESGOS

Son muchos. La variedad de ataques es cada vez mayor. Las

técnicas también son múltiples y el número de ciberdelincuentes se incrementa. Ataques de denegación de servicio, phishing, ransomware, troyanos, suplantación de identidad... pueden añadir todos los que se le ocurran. Seguro que le salen más de diez. Los expertos, de hecho, no se ponen de acuerdo en dónde se encuentran los principales riesgos, lo que da una idea de la peligrosidad del momento. Por ejemplo, Aitor Jerez Director Comercial de Sarenet cree que “la mayor pesadilla sigue siendo el secuestro de datos, pero no son los únicos riesgos que afrontan. En un entorno en el que todo se conecta con todo, las superficies de ataque han crecido exponencialmente. Los últimos años se han desarrollado medidas para minimizar los riesgos a sufrir un ciberataque pero casi siempre atendiendo a entornos de IT. En la parte de OT aún hay mucho que hacer para alcanzar el mismo nivel. Las plantas de fabricación se han convertido en entornos muy críticos con la interconexión de sus activos y deben remodelarse para minimizar riesgos y permitir habilitar de forma segura nuevas tecnologías en su camino de la digitalización”.

En lo que coinciden la mayoría es que el mundo ha cambiado de tal forma que las técnicas defensivas de hace unos años ya no valen. El tradicional perímetro ha caído y las conexiones desde diferentes ubicaciones y desde distintos dispositivos hace que la ciberdefensa sea cada vez más compleja. En este sentido, Jose Luis Laguna, Director Systems Engineering de Fortinet afirma que al no existir un perímetro definido, la superficie del ataque se ha expandido, lo que complica la protección de todos los puntos de entrada a la red. En el último año, el teletrabajo ha supuesto una ventana de oportunidad para los ciberatacantes, al acceder a la red corporativa desde dispositivos que muchas veces no están contemplados dentro de las políticas de seguridad de las organizaciones, lo que les ha convertido en un blanco perfecto”.

Y es que, esta nueva forma de trabajar con la que nos ha obsequiado el coronavirus ha traído consigo un incremento de los riesgos. Sobre todo al inicio de la pandemia, cuando millones de trabajadores tuvieron que adoptar la fórmula del teletrabajo para que la productividad empresarial se viera lo menos afectada posible. En ese momento, las conexiones externas se dispararon y muchas de ellas, no contaban con las mínimas garantías de seguridad. ¿Que sucedía si un portátil particular, de los que se utilizaron muchos al principio del confinamiento, estaba infectado y accedía a la red empresarial? En realidad se puede asegurar que bastante poco ha sucedido, posiblemente porque a los ciberdelincuentes el Covid también les pilló con el paso cambiado porque los desastres podían haber sido muy numerosos, sobre todo si se tiene en cuenta que la mayoría del personal no ha sido debidamente formado para, al menos, detectar un correo malicioso. Para

Chester Wisniewski, investigador principal de Sophos, este es uno de los principales riesgos que están corriendo las empresas: “El mayor riesgo a la que se enfrentan las empresas en la mayoría de las ocasiones es la falta de preparación y previsión en cuanto a su seguridad. Cada vez se le está prestando más atención a la seguridad porque estamos viendo más ataques que son cada vez más dañinos también, pero sigue habiendo muchas compañías que tienen una protección precaria que nos les protege 100% en el caso de un ciberataque importante real. Contar con la tecnología y con equipos que la administran de forma generalizada desde las TI de las empresas ya no es suficiente, dado que el nivel de sofisticación y las herramientas que usan actualmente los ciberdelincuentes requieren que haya equipos y expertos en ciberseguridad rastreando las redes para identificar comportamientos sospechosos y evitar realmente un ataque”. Es casi la misma opinión de Antonio Martínez, Head of GRC and Cybersecurity de Audea para quien “la apertura de las redes y/o las aplicaciones, por ejemplo, para dar acceso a los empleados a los sistemas y servicios corporativos, o el desarrollo del trabajo en redes domésticas o inseguras, no controladas por la organización, son uno de los principales riesgos. El uso masivo de herramientas de colaboración y de reuniones también representa un hándicap respecto a la ciberseguridad. Adicionalmente, los ataques de ingeniería social y suplantación de identidad, principalmente Phishing (Correo), aunque existen otros por ejemplo Smishing (SMS) o Vishing (Llamada de voz) representan algunas de las mayores preocupaciones para una organización, por las peligrosas consecuencias en forma de fuga y/o cifrado de la información”.

## SOLARWINDS ROMPIÓ ESQUEMAS

Ataques como el de SolarWinds, han cambiado la forma en la que se entiende la ciberseguridad por el modus operandi. La técnica empleada en este caso ya era conocida, pero con Solarwinds se dio un paso más. Antes de Solarwinds ya existían ataques a la cadena de suministro. Lo que hace distinto a este ciberataque se encuentra en la sofisticación. Y es que, los ciberdelincuentes lograron entrar en la red interna de SolarWinds y alteraron varias versiones de su solución Orion para añadir el malware Sunburst. Ese malware se encontraba en todas las actualizaciones publicadas entre marzo y junio de 2020, y lo que es más grave, ningún cliente de SolarWinds se dio cuenta (o al menos no informó) de su existencia hasta que no transcurrieron nueve meses. De hecho, no fue hasta el 15 de diciembre cuando SolarWinds lanzó una nueva versión de Orion que pudiera hacer frente al ataque. El problema es que no sólo estaba Sunburst. Este malware no es complejo ni particularmente agresivo, pero fue el encargado de recopilar la información que permitía a los atacantes seleccionar los clientes objetivos que consideraban

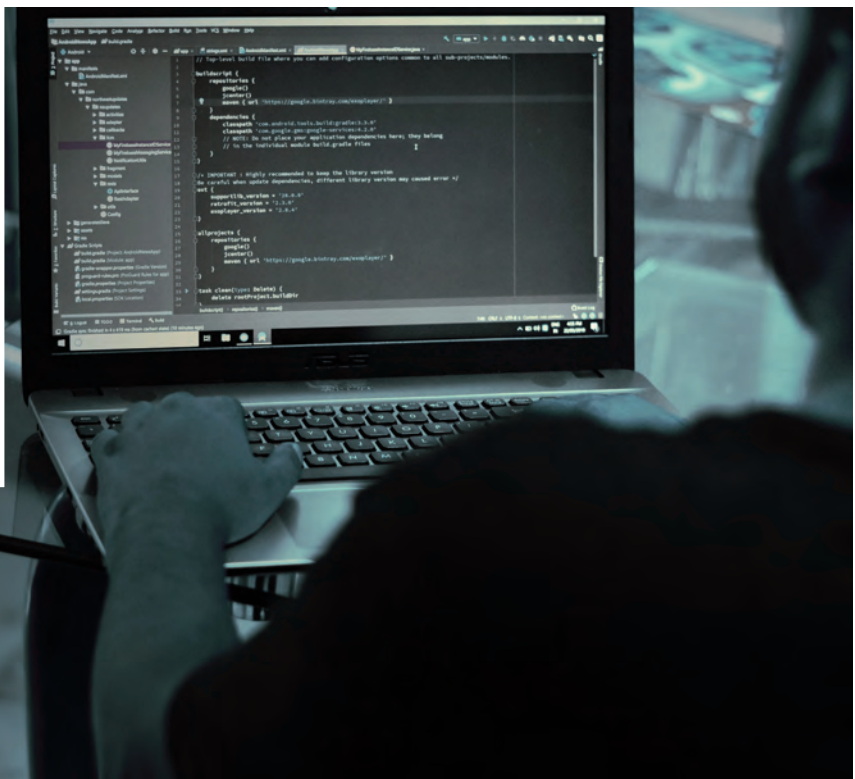
más interesantes: organismos gubernamentales norteamericanos y empresas como Microsoft o FireEye. La clave se encuentra en que Sunburst permitía escalar las infecciones a una segunda etapa, en la que se despliega otra cepa de malware llamada Teardrop que a su vez se emplea para desplegar balizas Cobalt Strike que permiten acceso remoto persistente a los dispositivos comprometidos y que pueden ser empleadas para implementar todo tipo de cargas útiles, como ransomware o keylogger, en la red comprometida. Este es el ataque y este ha cambiado la estrategia de seguridad de las compañías y de las AAPP. Pero lo que es más grave es que para lanzar un ataque de tal sofisticación se necesita algo: dinero, mucho dinero y personal, mucho personal. Así que todo apunta a que un estado está detrás de un ataque como éste. En este caso, la Rusia de Putin. Tal y como afirma uno de los mayores especialistas en ciberseguridad como Luis Corrons, Security Evangelist de Avast, “del mismo modo que las tecnologías de seguridad evolucionan, también lo hacen los ciberataques, especialmente en el caso de los ataques promovidos por un Estado, como el de Solarwinds. Estos atacantes tienen más recursos a su dis-

posición, lo que significa que sus métodos de ataque son mucho más avanzados, lo que crea nuevas olas de interrupción masiva”.

Este ciberataque representa el paradigma de lo que está por venir. Y no pinta nada bien: un ciberataque puede bastar para destruirnos a todos. Daniel González, Senior Sales Manager de Ivanti, cree que “es obligatorio tomar este caso como uno de los primeros por el modus operandi, pero, desde luego no será el último. De hecho, ha sido clasificado como “el mayor y más sofisticado de la historia”. Los ciberdelincuentes cada vez son mejores a la hora de encontrar la mejor vía para controlar cualquier sistema. En este caso, la actualización de un software muy utilizado, donde se “coló” el software atacante, que permite a los ciberdelincuentes tomar el control del sistema. Este tipo de ataque podría ocurrir a cualquier fabricante que no controle al más alto nivel sus procesos de producción, actualización o renovación de sus productos”.

## EN QUIÉN CONFIAR

En nadie. El malware se puede encontrar en cualquier lugar, incluso en aquellas actualizaciones que parecen confiables. Así que, mejor dudar de todo. Es lo que se pretende con la filosofía Zero Trust, un término de principios de la década pasada y que, establece que hay que dudar de cualquier intento de acceso a la red que se produce. Zero-Trust asume que los usuarios y los datos pueden estar ubicados en cualquier lugar, en el servidor empresarial o en la nube. Y todos ellos, tanto los que están dentro del perímetro como los que se encuentran fuera, son susceptibles de realizar un ataque y por tanto, no se puede confiar en ellos de una manera predeterminada. La ventaja de esta estrategia es que, en principio, el departamento de ciberseguridad tiene el control sobre los datos de la organización lo que hace que en el supuesto de que aparezca una brecha se puede detectar







con precisión cuándo se ha accedido a esos datos y saber si han sido manipulados. El portavoz de Ivanti considera que “esta filosofía se debería aplicar a todo el proceso de creación y actualización: desde el uso de micro-códigos, las API, los lenguajes de programación por objetos, etc. Nunca debemos confiar por defecto en nada. Siempre hay que comprobar todo, varias veces, por diferentes equipos. De esta forma, tendremos más garantías”.

En teoría debería solucionar el problema, pero Miguel López de Barracuda afirma además que, “a día de hoy, la única herramienta viable para sortear este tipo de ataques es la de implementar soluciones tecnológicas capaces de verificar la integridad y seguridad de la cadena de suministro de software de manera continua como las incorporadas en Barracuda WAF CAP 2.0. Las aplicaciones web son muy complejas y cada vez más requieren utilizar fragmentos o piezas de software externo para poder desarrollarse con las prestaciones y funcionalidades requeridas. Incluso si comprobamos la cadena de suministro de software en un día concreto, ello no implica que, en un momento dado, horas o días después esas piezas de software no puedan haber sido comprometidas. Así se hace ineludible establecer medidas de seguridad que comprueben la integridad y seguridad de nuestras aplicaciones web incluso en el lado cliente de forma exhaustiva, automática y continuada”.

### LA SEGURIDAD DE LA NUBE

Y este inicio de año ha puesto de manifiesto la mejor seguridad que proporciona la nube frente al modelo tradicional de tener los datos en el data center propio. El ataque a los servidores Exchange lo ha dejado claro. Microsoft, lleva años

insistiendo a sus clientes en las ventajas que proporciona la migración a la nube. También en materia de ciberseguridad. Pero todavía son muchas las compañías reticentes a mover sus cargas a un entorno cloud. Reticentes, claro, hasta que son atacados. En este caso, los atacantes comenzaron su labor el pasado mes de Enero y pasaron dos meses hasta que Microsoft se dio cuenta y empezó a parchear. Porque no fue un único ciberataque, sino que fueron cuatro que aprovecharon vulnerabilidades encontradas en Exchange Server 2013, Exchange Server 2016 y Exchange Server 2019. Alrededor de 30.000 clientes, entre los que se encontraban organismos gubernamentales, utilities o entidades bancarias se vieron afectados. Todos ellos con versiones on-premise. Nadie que trabajaba con Exchange en modo cloud fue atacado. Para Daniel Varela, experto en ciberseguridad de F5, con este ciberataque, lo que se pone de manifiesto es que “los servicios SaaS deben garantizar las mayores medidas de seguridad como parte del servicio. Los modelos on-premise no gestionados parten con desventaja en caso de que no se sigan las recomendaciones de seguridad. Por otro lado, modelos on-premise donde las empresas cuentan con equipos de seguridad con un alto expertise pueden proporcionar servicios similares a los que vemos en SaaS”.

Pero el ciberataque a Exchange no quiere decir que la nube sea 100% segura, aunque como afirma José de la Cruz, director técnico de Trend Micro, “lo cierto es que este ataque en un entorno cloud, habría sido más complicado de ejecutar (siempre y cuando el proveedor cloud haya tomado las precauciones necesarias). Cada entorno implica unos riesgos y estos deben ser identificados y protegidos adecuadamente siempre. Tenemos que concienciarnos de que la se-

guridad debe estar en la base de toda actividad, proyecto, aplicación, etc.". Para el portavoz de Sarenet, "en este caso varias vulnerabilidades del servidor de Exchange instalado en la red del usuario, si se explotaban de forma encadenada, podían poner en peligro la red del que lo albergaba posibilitando el robo de información, cifrado de datos o destrucción de los mismos. Si el Exchange está en la nube estará mejor actualizado y protegido por Microsoft pero hay que tener en cuenta que no son infalibles y además mañana puede ser cualquier servidor instalado en la red local con aplicaciones de todo tipo o una máquina virtual en la nube la que tenga vulnerabilidades susceptibles de ser explotadas".

Lo cierto es que las vulnerabilidades están en cualquier aplicación y entorno, aunque la nube empieza a ser mucho más segura que el modelo on-premise y consume menos recursos. En este sentido, Antonio Martínez de Audea considera que "las vulnerabilidades seguirán existiendo, ya sea en la nube o en modelos on-premise, porque el desarrollo del software no es perfecto, aunque en los últimos años se han incorporado nuevas técnicas y herramientas y una mejora sustancial de la concienciación de los fabricantes de software acerca de la ciberseguridad, que hacen que el software sea más seguro. Lo que ocurre es que en la actualidad existen más ciberdelincuentes y existe una mayor exposición de cualquier aplicación a los riesgos de redes abiertas como Internet, por lo que el mínimo fallo puede trans-

formarse en una brecha de seguridad grave". La clave del ataque a Exchange según Guillermo Fernández de Watchguard "es que los ciberdelincuentes se aprovechan de la explotación de vulnerabilidades a sistemas no parcheados debidamente. De hecho, la explotación de las vulnerabilidades de los programas informáticos es una de las principales causas de las violaciones de la seguridad informática, muchas de ellas son fallos que podrían haberse solucionado con un parche, pero que nunca se aplicó. Si una empresa actualiza su parque de software debidamente y lo mantiene al día, no tiene por qué ser inseguro. De la misma manera que si el proveedor de servicio en la nube no actualiza su software también es vulnerable en un momento dado. Lo importante aquí es que las empresas cuenten con herramientas capaces de automatizar todo el mantenimiento de lo que es la actualización de software y despliegue de parches. En caso de que esto no sea posible, lo lógico es delegar en un tercero todo este trabajo de mantenimiento para tener los sistemas al día. Aquí conviene subrayar que las dos alternativas son seguras, siempre y cuando se mantengan las actualizaciones y se se aplique un procedimiento que garantice la gestión y despliegue correcto de parches a todos los dispositivos pertinentes tan pronto como estén disponible".

### LA ESTRELLA

Ahora mismo la principal amenaza sigue siendo de la misma estrella que brilla en el mundo de la ciberdelincuencia. En este caso, el objetivo es sacar la máxima cantidad de dinero posible. La ciberextorsión tiene nombre y apellidos: Ransomware. Es evitable: sí. Normalmente viene adjunto en un correo, un whatsapp, un SMS,... Y lo que hace falta es, sobre todo, formación. Hay que enseñar al usuario a distinguir los mensajes que pueden tener contenido malicioso. El problema es que no todos saben hacerlo y en el momento que entra el Ransomware son muchas las empresas que optan por pagar el rescate, que casi nunca asegura la recuperación completa de todos los datos.

El portavoz de Trend Micro, José de la Cruz insiste en que la formación es la mejor prevención contra el ransomware, pero aún así cree que "dado que el ransomware no es un ataque en sí, sino un conjunto de ataques ejecutados de manera coordinada la estrategia más adecuada consiste en cubrir todos los vectores de ataque (correo, red, servidores, endpoint, etc); compartir inteligencia entre dichos vectores para que un ataque no consiga encontrar un punto débil de la cadena y proveer de herramientas que proporcionen visibilidad sobre lo acontecido en nuestra infraestructura".

Sophos es una compañía que lleva años insistiendo también en la formación de los usuarios como principal medida para combatir el ransomware. Según esta multinacional de la ciberseguridad el número de empresas que han sido víctimas de ataques de ransomware ha descendido a nivel global, sin embargo, la gravedad de estos ataques ha sido mayor, por lo que se convierte en una amenaza más preocupante si cabe. Según su estudio "El Estado del Ransomware 2021", un 37% de las empresas fueron atacadas por un ataque de ransomware importante en 2020, una cifra que se eleva al 44% en el caso de las empresas españolas. De estos ataques, en el 54% de los casos llegaron a cifrar los datos y las empresas pagaron de media un rescate de 170.000 dólares, a pesar de que solo en el 65% de los casos las empresas recuperaron sus datos aun habiendo pagado el rescate. Para Chester Wisniewski, investigador principal de la firma, "la mejor manera de defenderse de un ataque de ransomware es estar preparado y asumir que seremos atacados. Eso significa invertir en tec-

nologías de protección y establecer una cultura de seguridad. Es importante instrumentar el entorno de manera que los eventos aparentemente sin importancia y sin relación sean visibles, desde un malware en un servidor hasta un email de phishing denunciado por un usuario. Otras herramientas que pueden ser útiles es contar con backups para poder recuperar los datos en el caso de ser atacados, incluso realizar backups offline por métodos tradicionales, así como protegerse por capas. Por último, es necesario contar con un plan para cuando las cosas van mal. Tener un plan de recuperación significa que la empresa puede contener el problema, investigar la causa y recuperarse de un ataque mucho más rápido y con menos daños. En resumen, proteger, detectar y responder”.

Josep Albors, responsable de concienciación de ESET cree que “el ransomware es una de las principales preocupaciones debido al impacto directo que tiene en la continuidad del negocio. Las herramientas y conocimientos para detectar una intrusión en una red corporativa de un ransomware o cualquier otra amenaza existen y tan solo deben ser implementadas, empezando con una autenticación segura de





todos los usuarios, limitando sus permisos y accesos a sistemas o información crítica, segmentando redes para impedir que un atacante realice movimientos laterales buscando su objetivo, poniendo en marcha soluciones de seguridad y monitorización que permitan detectar acciones maliciosas aunque se estén utilizando herramientas legítimas y contando con un equipo de profesionales internos o externos que sea capaz de detectar este tipo de incidentes a tiempo y de revisar ataques anteriores para determinar cómo se produjeron y aplicar las medidas necesarias, entre otros puntos a tener en cuenta”.

### **LA MOVILIDAD**

Es otro de los puntos. Hace no mucho tiempo los dispositivos móviles no entraban dentro de la estrategia de ciberseguridad de una empresa. Ya no. Se trata de un vector muy importante desde el que cada vez se dan más



ciberataques. Samsung lleva años invirtiendo en ciberseguridad, un elemento que siempre ha considerado prioritario. Casi desde que desarrolló su primer smartphone. La firma surcoreana es de los pocos fabricante que apuesta por dispositivos seguros de principio a fin, que incluyen una solución de seguridad que permite la gestión de todo el ciclo de vida del equipo. Tal y como indica su portavoz, “nosotros comenzamos la protección del dispositivo y de la información en la etapa de producción del smartphone, con la implementación de la seguridad en el hardware, y continúa con una serie de comprobaciones que se activan desde que se inicia el sistema e incluso cuando el dispositivo está apagado, monitorizándolo tanto si se utiliza como si no. Todo ello gracias a tecnologías de vanguardia como el chip de seguridad más fuerte de la industria, el elemento seguro integrado (eSE), un procesador seguro para proteger contra ataques físicos; Samsung Knox -nuestra plataforma de se-

guridad de extremo a extremo- que encripta los datos y los aísla para evitar intromisiones en el caso de pérdida o robo del dispositivo, además de Knox Vault, que agrega otra capa de seguridad”.

Así que el hardware es importante. Un teléfono seguro en manos de un empleado tendrá menos posibilidades de ser atacado y éste es un factor en el que la mayoría de fabricantes de smartphones fallan de forma importante. En este aspecto, las empresas deben afrontar una serie de medidas para mitigar el riesgo en un mundo cada vez más hiperconectado, como poseer un hardware validado y comprobado, redes seguras y contar con una infraestructura para la gestión de la seguridad que soporte una gestión de parámetros unificados y la defensa ante cualquier tipo de amenaza. Por ello deben escoger dispositivos que ofrezcan la máxima productividad en todo tipo de escenarios y que también incluyan una plataforma para la gestión multidispositivo, la seguridad y la personalización de las aplicaciones de negocio.



# “Espero que el hotel sin recepción tarde todavía en llegar”

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

La mayor parte a las comunicaciones, al software y al personal.

### ¿En qué área se está invirtiendo más este año?

Si hablamos de 2020 pues como siempre es menos de lo que nos gus-

taría, pero en las circunstancias que estamos, que haya inversión es de agradecer. Hemos conseguido inversión en mejorar las comunicaciones habladas que nos permitirá uno bajar costes de cara al futuro y dos mejorar las opciones de comunicación con los clientes, hemos terminado algún proyecto en marcha de mejorar de la pla-

taforma WIFI para los clientes, hemos actualizado la web, un proyecto de BI y se ha aceptado la subida de la nube de una parte de nuestro ERP.

### ¿Qué proyecto es del que está más satisfecho?

Pues de todos, pero me alegra haber podido subir a la nube parte de nues-

tro software pues tiene ciertas implicaciones que nos permitirán mejorar nuestras gestiones internas.

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

No tendría manos para tanto proyecto. Pero si tuviera que escoger uno, gestión documental.

**¿La seguridad es un problema?**

Sí, cada vez más hay más ataques, para controlar los mismos, hay que dedicar recursos a la prevención del mismo, y a pesar de los mismos, uno nunca está exento de poder recibir un ataque y que este te afecte.

**¿Se puede trabajar desde casa?**

Poderse se puede. Evidentemente no en todos los puestos, en mi caso trabajamos para hoteles y los puestos de un recepcionista, de un camarero no se pueden llevar a casa por lo evidente.

**¿Qué tendencias principales observa en el mundo TIC?**

Si hablamos de una manera global, diría que la transformación digital. Todas las empresas, expertos de todos los sectores, están haciendo hincapié en la necesidad de esta transformación digital para estar preparados para lo que nos espera. Si hablamos de algo más particular, la inteligencia artificial.

**Bajo ningún concepto en su móvil puede faltar...**

Mi agenda de contactos.

**¿Cuál es la herramienta que realmente le cambió la vida?**

Más que la herramienta, diría que el dispositivo. El iPhone.

**¿Harto de solucionar los problemas tecnológicos de la familia y amigos?**

Harto tampoco. Me piden ayuda, y la verdad es que llevo tanto años como responsable que no puedo estar en el día a día de los equipos domésticos y hay veces que no sé ni de lo que me hablan.

**¿Tiene cuenta en redes sociales?**

Sí, en LinkedIn. La verdad es que me parecen muy útiles pero a día de hoy el uso que veo de ellas no me gusta mucho, por lo que prefiero mantenerme al margen en lo que se refiere a apartado personal.

**¿Qué es eso de la transformación digital? ¿Slogan o necesidad?**

Pues creo que es una idea. Para mí sería como pasar al siglo XXI de las empresas.

**¿Lo del I+D+i, es una leyenda urbana?**

No, otra cosa, es lo que creamos que son esas siglas.

**¿Cuánto tiempo queda para el hotel sin recepción?**

Espero que mucho tiempo, he sido botones y auxiliar de recepción y los valoro mucho. Y creo que su trabajo tanto en el back office como de cara al cliente es importante. Eso no quiere decir que no crea en soluciones que automaticen el proceso de check-in o de atención al cliente, pero espero que las personas siempre estén ahí.

Julián Castillo,

Responsable TIC de  
Hoteles Servigroup

**Fecha de nacimiento:**

21/8/1981

**Estado civil:** casado

**Hijos:** dos

**Deportes que practica:** Buceo, bici montaña, trekking

**Hobbies:** Leer, escuchar música, amigos, mi familia, mi perra

**Estudios:** Ingeniero técnico industrial en electrónica industrial e ingeniero técnico informático, especialidad sistemas

**Antigüedad en la empresa:**

14 años

**Personas a su cargo:**

Tres / Cuatro

# Victoria Zafra, Responsable de Sistemas en Hospital Quirón Salud Córdoba

**Hijos:** 1

**Hobbies:** running, bicicleta, montaña, cocina, mindfulness y jugar al pasapalabra con mi hijo

**Estudios:** Grado en Ingeniería Informática de Sistemas y FP Grado Superior de documentación sanitaria

### ¿Cómo llegó al sector TIC?

Comencé mi andadura profesional en Madrid antes siquiera de finalizar el proyecto de la carrera. Conseguí una beca en la empresa que me contrató y luego continué mi carrera profesional en Madrid en los dos siguientes años siguientes. Luego regresé a mi ciudad natal, Córdoba.

### ¿Qué es lo que más valora de su trabajo?

Lo que más valoro de mi trabajo es que me brinda la oportunidad de aportar conocimiento y valor para favorecer una mejor atención a los pacientes que nos visitan cada día en nuestro hospital; en definitiva, a mejorar la vida de esas personas. Asimismo, me posibilita a contribuir con estándares y buenas prácticas en la gestión de la TI a nivel de compañía junto a todo mi equipo. Desde la apertura del hospital, hace algo más de dos años, seguimos dándolo todo día a día e intentamos seguir superándonos. Trabajar desde el inicio en un proyecto como la apertura y consolidación de un hospital es apasionante. Lo vivimos con mucha ilusión, y entrega.

### ¿Qué es lo que falla para que las mujeres no apuesten más por el estudio de carreras STEM?

Creo que la limitación es la cultura que aún nos rodea, en cuanto a estereotipos de cuáles son las carreras que estudian las mujeres y cuáles los hombres. Nos queda mucho camino

por delante en ese sentido, desde los juguetes, los anuncios en televisión, la publicidad, la imagen... en ocasiones siguen existiendo esos detalles del pasado que aún están anclados en el presente.

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

No lo creo. Creo que la mayor parte de los CIO de empresas generalmente siguen siendo hombres por la falta de mujeres que hacen carreras técnicas. Entiendo que la solución pasa por que cada vez sean más las mujeres que acceden a esos determinados puestos, y para ello es clave la educación, la necesidad de que poco a poco vaya incrementándose ese porcentaje de mujeres que estudian carreras técnicas. Es fundamental que haya mayor equidad, la riqueza en cuanto a puntos de vista para tratar diversos problemas ... Es fundamental que la sociedad, tanto la educación como la familia vayan haciendo más partícipes a estas niñas o adolescentes de que la demanda es y será tal que pueden tener casi la total seguridad de tener un puesto de trabajo asegurado el día de mañana.

### ¿Una política de cuotas puede resolver el problema?

Podría ser parte de la solución, pero no la única.

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





Tengo que decir que, por ser mujer, ninguna. Nunca me he sentido discriminada en ese sentido. En la compañía a la que pertenezco hay un gran porcentaje de mujeres con puestos directivos, son excelentes profesionales con un nivel muy alto de compromiso y competencias.

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

Totalmente, es así, las estadísticas lo indican claramente. Es necesario ser más competitivos en oficios y trabajos que demanda la sociedad. Durante un tiempo se vendió la idea que con una carrera y un master ya no te iba a faltar el trabajo. La realidad es que hay muchos jóvenes muy bien preparados pero que tienen que emigrar para poder encontrar algo en su sector. Evidentemente algo no se está haciendo a nivel de políticas de empleo cuando dejamos escapar a jóvenes tan

bien preparados a otros países y con esto nuestro país se empobrece aún más.

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

Por supuesto. Nunca he dejado de formarme, para mí el conocimiento es mi pasión. Me harían falta varias vidas para aprender todo lo que deseo.

**Solucione el problema de la educación en España...**

Creo que como gran parte de la sociedad no es entendible que haya una continuidad en los planes de la educación, el gran pacto nacional, del que todos hablan en época de elecciones pero que se olvidan nada más llegar. Ese sería un buen punto de partida. Por otro lado, innovar en educación es fundamental, en instalaciones, en dotaciones, en ir capacitando mejor a los alumnos digitalmente, pero siempre con un equilibrio. Las bases del pensamiento y del conocimiento son universales, y eso se está di-

luyendo en cierta manera con las nuevas tecnologías. No se lee ni se escribe como antes, y eso, como todos sabemos es fundamental en cualquier puesto que luego se desempeñe.

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

Evidentemente lo orientaría hacia carreras tecnológicas, ingenierías o telecomunicaciones. Asimismo, todo lo relacionado con la ingeniería biomédica y bioinformática. Aunque también se está viendo cada vez más necesarios profesionales del ámbito de las letras como sociólogos o filósofos, que van a ser necesarios también en esta ola de la nueva revolución industrial que aporten la ética y lo necesario para delimitar hasta dónde se puede llegar con la técnica y la tecnología.

**¿Hacia dónde cree que va el sector TIC?**

Pienso que el PIB de cada país será directamente proporcional a lo evolucionado que esté su nivel de digitalización y automatización. Por tanto, pienso que es un sector clave y fundamental en el desarrollo de nuestras ciudades y países. En cuanto a las tendencias que están transformando la sociedad y lo seguirán haciendo son el IoT, la Inteligencia Artificial, la robótica, el Big Data, y el 5G como el gran precursor del gran cambio que viviremos en nuestras ciudades en cuanto a la movilidad se

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

Evidentemente. Si no, no estaría tan convencida que todas estas tecnologías vienen de la mano del hombre y que sin el hombre no existen por sí mismas. Se trata de delegar en las máquinas trabajos que no aportan valor en sí mismos, y poder dedicar el tiempo a lo verdaderamente importante.

# Responsabilidad de los hijos en RRSS



**S**e calcula que más del 65 % de los preadolescentes españoles menores de 12 años tienen su propio perfil en una o más redes sociales, siendo las más populares entre este sector de la población Instagram, YouTube, TikTok y Snapchat, además del omnipresente WhatsApp que, aunque es un sistema de mensajería instantánea, su capacidad de viralización de contenidos mediante el reenvío masivo provoca que se planteen problemáticas similares en lo que a los menores se refiere.

A estas es probable que se unan en breve YouNow, la red social de moda en Estados Unidos, el Messenger Kids de Facebook y la versión de Instagram para menores de 13 años que está proyectada, y que ya ha sido objeto de polémica tras la carta de oposición enviada recientemente a Mark Zuckerberg por la asociación “Campaña por una Infancia sin Comerciales” (CCFC, por sus siglas en inglés)

y 35 organizaciones más, denunciando que ello supone una explotación del síndrome FOMO (“fear of missing out”), especialmente sensible entre los jóvenes, y pidiendo que se valoren sus consecuencias negativas, en especial respecto al ciberacoso y el suicidio infantil.

El artículo 8-1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (GDPR), fija en 16 años la edad mínima del menor para considerar lícito el consentimiento para el tratamiento de sus datos personales. Y si fuera menor de 16 años, tal tratamiento únicamente se podría considerar lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.

Por lo que se refiere a la normativa nacional, el artículo 7 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, reduce a 14 años la edad para dar dicho consentimiento, y lo considera también lícito en el caso de los menores de 14 años si consta el consentimiento del titular de la patria potestad o tutela, con el alcance que determinen los titulares de la patria potestad o tutela. Por tanto, estas estadísticas sobre el acceso a redes sociales de los menores implicarían el conocimiento y consentimiento de sus padres o tutores. Sin embargo, no siempre es así, ya que muchas de estas aplicaciones pueden descargarse sin necesidad de acreditar la edad necesaria para ello.

En relación con la protección de los menores frente a agresiones de toda índole que pueden sufrir a través de las RRSS, una cuestión recurrente es la de los supuestos en que son los propios menores los que realizan actos que vulneran la legalidad, muchas veces contra otros menores, tales como el bullying, sexting, cyberstalking, trolls, haters, etc., o en retos virales como “la ballena azul”, los “ro-topper” o el “desk challenge”. En este sentido, recientemente se ha denunciado la agresión física y verbal producida en San Fernando (Cádiz) en abril de 2021, a una menor por otras tres adolescentes, que fue grabada por otra menor, para ser publicada en Instagram y difundida por Whatsapp. Pero, lamentablemente, no es un caso aislado.

En estos supuestos, ¿quién debe asumir las consecuencias de estos actos, tanto desde el punto de vista de la sanción que proceda, como de indemnización que hubiera que pagar para compensar los daños? Respecto a responsabilidad penal, cuando se trate de menores de 14 años no se les considera sujetos penalmente responsables por lo que sólo podría haber un resarcimiento en vía civil. Y cuando el autor sea mayor de 14 y menor de 18 años (momento en que adquiriría la mayoría de edad y, por tanto, la plena responsabilidad penal), le sería de aplicación la Ley Orgánica 5/2000, de 12 de enero, reguladora de la Responsabilidad Penal de los Menores, que prevé actividades formativas, educativas, laborales y de ocio para la reeducación, integración y reinserción del menor.

En cuanto a las indemnizaciones derivadas de la responsabilidad civil por los daños generados a terceros, el artículo 1903 del Código Civil establece que los padres y tutores son los responsables de los actos de los menores que se encuentren bajo su guarda, en virtud de la culpa in vigilando, in custodiando o in educando (STS de 10 de marzo de 1983), salvo que prueben actuaron diligentemente para prevenir el daño. Asimismo, también son responsa-

bles de los actos de los mayores de 18 años sujetos a su patria potestad o tutela y que vivan en su compañía, cuando haya por su parte culpa o negligencia (artículo 120-1 del Código Penal).

En aplicación de lo anterior, la Sentencia de la Audiencia Provincial de Murcia de 27 de abril de 2020 condenó al pago solidario de la cantidad de 12.000 € a los padres de unas menores de 12 y 13 años, que presionaron a una amiga para que publicase fotografías en las que aparecía desnuda en Tuenti, considerando irrelevante que se las hiciera la propia menor con su móvil y que las subiera ella misma a la red social, ya que ello fue debido a las amenazas y coacciones de sus amigas, que se valieron para ello de la situación de dependencia afectiva de la víctima; lo que generó una crisis de ansiedad que motivó su tratamiento psicológico, hasta el punto de tener que cambiar de instituto y sufrir miedo de salir a la calle sola, afectando a sus relaciones sociales.

Y, en ocasiones, son los propios progenitores los instigadores de estas conductas irresponsables, como supuesto el enjuiciado en la reciente sentencia del Tribunal Supremo de 15 de abril de 2021, que condenó a un padre de Gijón (Asturias) a pagar una multa de 2.160 € por grabar a su hijo de 8 años conduciendo en solitario un coche de alquiler en el que previamente le había puesto para realizar una grabación desde fuera sobre cómo conducía (previsiblemente para su posterior difusión en alguna red social o sistema de mensajería), cometiendo un delito contra la Seguridad Vial y poniendo en peligro la vida de terceros y del menor, incumpliendo con ello sus deberes parentales.

También dentro del ámbito de los deberes parentales, se encuentra la cuestión de hasta qué punto puede un progenitor limitar a un hijo el uso del WhatsApp dentro de su deber de educación y corrección del menor, o para evitarle potenciales situaciones perjudiciales, como, por ejemplo, comunicarse con el otro progenitor en el caso de controversias entre parejas separadas. En este sentido se pronunció la sentencia de 4 de febrero de 2020 de la Audiencia Provincial de Alicante, que estableció que, en este caso, la negativa del padre divorciado a que los hijos utilicen el móvil para relacionarse con la madre durante las estancias con él, no solo no resulta perjudicial, sino que es aconsejable, dada la actitud impositiva y manipuladora de la madre, que pretendía eliminar totalmente la figura paterna de la vida de sus hijos, habiendo generado en los mismos un conflicto de lealtades.

Javier López. Écija Abogados

# Mejorar la colaboración para impulsar una digitalización eficaz

Cuando el año pasado nos golpeó la pandemia se creó una necesidad urgente de que las organizaciones cambiaran sus estrategias de comercialización y aceleraran sus planes de transformación digital. A finales de 2019, IDC predijo que para 2023, más de la mitad de todo el PIB mundial estaría impulsado por productos y servicios de empresas transformadas digitalmente. Sin embargo, especialmente a la luz de lo ocurrido en 2020, parece seguro asumir que la realidad arrojará una proporción mayor. En la investigación publicada en el último trimestre del año, el 89% de los CIO aseguró que su transformación digital se había acelerado y el 58% predijo que continuaría acelerándose.

De la noche a la mañana, la capacidad de innovar más rápido y mejorar la experiencia digital se convirtió en clave para generar ingresos, mantener la productividad de los empleados y salvaguardar las operaciones comerciales. Sin embargo, también es cada vez más difícil para los equipos de TI mantenerse al día con esta creciente demanda de innovación más rápida y mejores experiencias digitales. El cambio a un modelo de trabajo remoto, el aumento de la demanda de servicios en la nube y el aumento del comercio electrónico han aumentado la presión y han agotado los recursos de TI más que nunca. Ante esta presión, los modelos operativos tradicionales con equipos en silos se están quedando cortos.

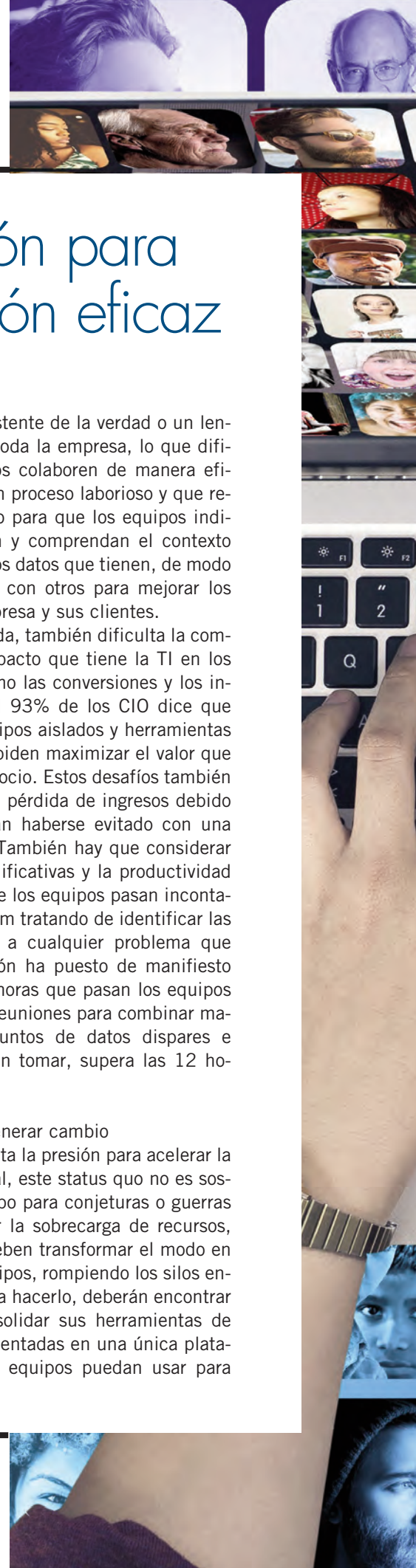
Una colaboración limitada frena el negocio. La mayoría de los departamentos de TI cuentan con varios equipos enfocados en diseñar, construir, implementar y ejecutar los servicios digitales en los que confía la empresa y sus clientes. Estos equipos suelen utilizar varias herramientas para supervisar y gestionar todo, desde el rendimiento de la infraestructura y las aplicaciones hasta la experiencia del usuario, las conversiones y los ingresos. Como resultado, no existe una

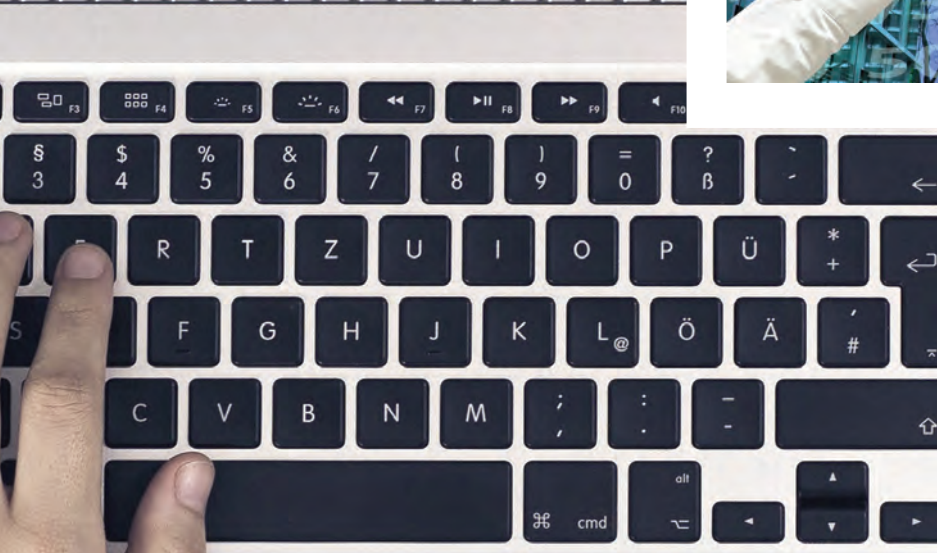
fuente única y consistente de la verdad o un lenguaje unificador en toda la empresa, lo que dificulta que los equipos colaboren de manera eficaz. A menudo, es un proceso laborioso y que requiere mucho tiempo para que los equipos individuales identifiquen y comprendan el contexto completo detrás de los datos que tienen, de modo que puedan trabajar con otros para mejorar los servicios para la empresa y sus clientes.

Esta visibilidad aislada, también dificulta la comprensión real del impacto que tiene la TI en los resultados clave, como las conversiones y los ingresos. De hecho, el 93% de los CIO dice que problemas como equipos aislados y herramientas fragmentadas les impiden maximizar el valor que la TI crea para el negocio. Estos desafíos también pueden provocar una pérdida de ingresos debido a errores que podrían haberse evitado con una mejor colaboración. También hay que considerar las ineficiencias significativas y la productividad desperdiciada, ya que los equipos pasan incontables horas en war room tratando de identificar las causas y soluciones a cualquier problema que surja. La investigación ha puesto de manifiesto que el promedio de horas que pasan los equipos de TI y negocios en reuniones para combinar manualmente sus conjuntos de datos dispares e identificar qué acción tomar, supera las 12 horas.

Romper silos para generar cambio

A medida que aumenta la presión para acelerar la transformación digital, este status quo no es sostenible. No hay tiempo para conjeturas o guerras internas. Para aliviar la sobrecarga de recursos, las organizaciones deben transformar el modo en que trabajan sus equipos, rompiendo los silos entre TI y empresa. Para hacerlo, deberán encontrar una manera de consolidar sus herramientas de monitorización fragmentadas en una única plataforma que todos los equipos puedan usar para





mantener la visibilidad en tiempo real de los KPI críticos del negocio. También deberán reunir todos sus conocimientos sobre el rendimiento de la infraestructura y las aplicaciones, la experiencia del usuario, las conversiones y los ingresos en un modelo de datos unificado. Entonces sus equipos tendrán la capacidad de comprender lo que significa todo en contexto. Este modelo operativo más unificado y colaborativo será esencial para la capacidad de las organizaciones de mantenerse al día con el ritmo acelerado de la transformación digital en los próximos años. Ya sea que se trate de desarrolladores que colaboran con operaciones, operaciones con equipos comerciales o la empresa con desarrolladores, equipar a los equipos con una fuente única y coherente de la verdad sobre los servicios digitales permite que todos estén alineados. Esto les brinda a todos un lenguaje único y unificador y respuestas precisas al alcance de la mano, para que los equipos digitales puedan comprender mejor el impacto que sus esfuerzos están teniendo en la empresa y sus clientes. Como resultado, pueden tomar más decisiones respaldadas por datos, por lo que pueden ofrecer continuamente mejores resultados comerciales digitales, lo que impulsa los ingresos y las conversiones, en todos los canales, de manera más eficiente.

Por Abdi Essa, RVP UK&I, Dynatrace

# 30 años en la historia de la impresión: ¿Qué ha cambiado?

**E**n los últimos 30 años, nuestra forma de trabajar se ha transformado: desde la irrupción de Internet a principios de la década de los 2000, hasta la expansión de la nube en la década de los 2010. Aunque las impresoras han existido durante todo este tiempo, su función y su tecnología interna ha sufrido tantas innovaciones como los ordenadores. Puede que las impresoras sigan teniendo un aspecto similar, pero sus usos y las tecnologías que las alimentan no son los mismos en absoluto. Si observamos con más detenimiento algunos de los principales aspectos que han cambiado en los últimos 30 años, resulta sorprendente lo lejos que hemos llegado.

### GESTIÓN DE DOCUMENTOS

Los días en los que sólo existía una función de impresión en un rincón, han pasado a mejor vida. Hoy en día disponemos de soluciones y dispositivos de gestión de documentos que pueden automatizar procesos que van desde el procesamiento de recibos hasta la gestión de stock en un almacén. Dado que el papel sigue siendo el motor de muchos procesos empresariales, la información de los documentos en papel, desde el momento en el que se crean, necesita ser recogida y gestionada como parte de la digitalización de los flujos de trabajo. Las impresoras multifunción inteligentes son capaces de capturar y escanear electrónicamente la información de los documentos y enviarla directamente a soluciones empresariales tan populares como SAP sin necesidad de un software de terceros, lo que permite activar automáticamente los flujos de trabajo digitales y ayuda a las empresas agilizar sus procesos.

### CLOUD

La llegada de la nube al sector de la impresión ha permitido evolucionar de los dispositivos conectados a la red por cable, que requerían un mantenimiento regular en persona, a soluciones conectadas a la nube que pueden gestionarse de forma remota. Las soluciones basadas en la nube, que aparecieron por primera vez

a mediados de la década de los 2010, permitieron descargar a los equipos de TI locales de gran parte de las tareas de seguridad, disponibilidad y rendimiento y trasladar su gestión a proveedores remotos. Los líderes en el sector de la impresión han desarrollado estos servicios para ofrecer la posibilidad de imprimir as-a-service en la nube, lo que significa que, en lugar de tener y gestionar una infraestructura de impresión física y asumir los costes que conlleva, los clientes simplemente pagan por lo que utilizan.

### SEGURIDAD

Hace treinta años, las impresoras eran tan seguras como la oficina en la que se encontraban. Por lo general, estaban conectadas por cable y muchas no tenían conexión a Internet, por lo que la única manera de vulnerarlas era entrar por la fuerza. Los dispositivos conectados han aportado beneficios considerables, permitiendo a las empresas imprimir a distancia y desde cualquier dispositivo. Sin embargo, a medida que ha crecido el acceso a Internet, también lo ha hecho, por desgracia, el panorama de amenazas. Hoy en día, invertir en mantener la seguridad de los clientes es esencial y los dispositivos de impresión deben contar con un espectro completo de capacidades de seguridad para restringir quién puede usar los dispositivos y qué puede hacer en ellos. Estas capacidades deben incluir funcionalidades de seguridad de red para proteger los dispositivos del acceso no autorizado a través de las interfaces de red, funcionalidades de seguridad de los documentos (como la liberación de la impresión) para evitar que los documentos caigan en las manos equivocadas, certificación automática de seguridad, seguridad del disco duro, firmware cifrado y firmado, tecnología de arranque seguro y verificación continua.

### SOSTENIBILIDAD

El concepto de la transición a una economía circular despegó en la década de los 90, poniendo un mayor énfasis en la longevidad de la tecnología. Más que re-



ciclar, ser circular significa partir de un lugar en el que se utilicen materias primas sostenibles, diseñar productos para el largo plazo y hacerlos fáciles de reparar, así como reciclarlos cuando realmente alcancen su verdadero punto de obsolescencia. También incluye la adopción de modelos de negocio basados en el intercambio y en el uso compartido de productos y servicios.

## HACIA EL FUTURO

En los últimos 12 meses se han producido nuevos cambios que determinarán nuestros entornos de trabajo de los próximos años. Una fuerza de trabajo repartida impulsará un mayor aumento en la adopción de tecnologías cloud e IoT, continuando la aceleración y la transición a la infraestructura digital. IDC ha detectado que el 43% de las empresas están invirtiendo en su infraestructura de impresión como parte de sus iniciativas generales de transformación digital. Este dato muestra que la impresión sigue siendo una función empresarial fundamental, y el papel sigue arraigado en la mayoría de los procesos empresariales. El 40% de los knowledge workers o trabajadores del conocimiento afirma que dedicar entre el 21 y el 30% de su semana laboral a tareas relacionadas con documentos (en papel y digitales) y crean 23 documentos en papel a la semana frente a 21 documentos electrónicos.

En los próximos años, la necesidad de imprimir no desaparecerá, pero las empresas empezarán a pensar de forma más estratégica en cómo incluir la impresión en sus proyectos globales de transformación digital, relacionados con la migración a la nube y las estrategias de procesos documentales. Las Print Infrastructure as-a-service de última generación jugarán un papel importante en la transformación digital. Como modelo de adquisición de impresión alojado en la nube, estas plataformas están diseñadas para simplificar la adquisición y gestión de la impresión, liberando así recursos de TI e impulsando un importante ahorro de costes, a la vez que se facilita el paso a un modelo de facturación más predecible y basado en la suscripción.

**Juan Leal Cárdenas,**  
Director General de Lexmark Ibérica

JOSÉ VELÁZQUEZ, DIRECTOR GENERAL DE INFOR



“Hemos hecho un gran esfuerzo por tener el mejor producto cloud del mercado”

La pandemia ha afectado a los clientes de Infor que han tenido que hacer un sobreesfuerzo para ayudar a sus clientes. Hablamos con José Velázquez, director general de la compañía que cuenta los retos que tienen por delante. **Por Manuel Navarro**



### **¿Cómo ha afectado a Infor la pandemia?**

Nos ha afectado como a todo el mundo. Es verdad que estábamos preparados para el teletrabajo, pero el hecho de no ver a las personas y trabajar de forma diferente requiere un esfuerzo para no perder la productividad. En lo que se refiere a negocio también nos ha afectado ya que somos una compañía que ofrece soluciones para el entorno industrial al que, sobre todo, durante la primera fase de confinamiento, le afectó mucho la situación ya que es un sector que estuvo prácticamente parado.

También hemos visto cómo a otros clientes les creció de manera desorbitada la demanda y aquí los retos estaban en la logística porque muchas cadenas de suministro tenían problemas, los productos que venían de fuera no llegaban... Infor ha intentado ayudar en ambos terrenos lo que hemos aprovechado para suplir los déficits que tenían todos estos sectores. En definitiva, el Covid ha sido dramático, pero también tiene sus aspectos positivos.

### **¿Cómo han afrontado el reto de la cadena de suministro? ¿Qué les ha faltado a los clientes?**

Ha habido varias cosas que les faltaban, pero sobre todo carecían de la capacidad de adaptarse al negocio físico. En este caso les hemos proporcionado soluciones específicas para afrontar la nueva realidad. También hemos visto que había clientes que tenían estructuras antiguas, que no han migrado a la nube y que les ha costado adaptarse al teletrabajo. Y por último, en todo aquello que se refiere a la gestión de la logística, la gran mayoría de clientes no estaban preparados para afrontar un reto tan grande. En este caso se requiere de sistemas mucho más flexibles y aquí se han podido aprovechar de nuestra gama de soluciones en la nube que lo que proponen son dos cosas fundamentales: digitalización y flexibilidad para que los clientes puedan adaptar de forma rápida sus diferentes escenarios a los retos que están por venir.

### **¿Se ha adaptado la cadena de suministro a esta nueva realidad que comenta?**

Estamos en ello, todavía. Se puede ayudar con algún parche puntual como se hizo al principio, pero la infraestructura tiene que ser totalmente nueva y eso

lleva más tiempo. En la segunda mitad del año pasado vimos cómo las empresas se lanzaron a adoptar la digitalización, a transformar de forma radical sus procesos y eso se aceleró muchísimo entonces y mantiene la misma velocidad en la actualidad.

### **¿Dónde está incidiendo más Infor en estos momentos? ¿Qué es lo que más se está demandando?**

Infor se enfoca en dos grandes tipos de soluciones: el ERP en cloud especializado en diferentes industrias y en soluciones de procesos específicos como la parte de logística, mantenimiento, gestión de la mano de obra, etc. Y estamos notando que clientes nuestros, que estaban en ERPs antiguos, están acelerando el cambio a nuestra cloud suite específica para su industria. Y lo hacen con proyección estratégica, con contratos transformadores.

Además hay clientes que buscan herramientas muy particulares departamentales que les ofrezcan las mejores soluciones para un proceso determinado. De esta forma estamos viendo un incremento muy importante de la demanda de nuestra solución de EAM. También en nuestras soluciones de analítica. Todo lo que es analizar datos en tiempo real para sacar conclusiones es una demanda muy importante por parte de las empresas.

### **¿Cómo va la migración de sus clientes a los entornos cloud? ¿Hay clientes que se niegan a moverse a la nube?**

Hemos hecho un esfuerzo enorme en tener el mejor producto cloud del mercado. Con la ventaja de que es un producto cloud nativo, que se ha construido desde cero y esto es algo que ven los clientes y que es fruto de una inversión en I+D de más de 5.000 millones de dólares.

Lo que estamos viendo, en general, es que las reticencias hacia los entornos cloud, sobre todo en este último año, han desaparecido casi totalmente. Hace un año, había muchas empresas que ponían en duda las ventajas de la nube. Así que, en estos momentos, estamos viendo una gran demanda por parte de los clientes. Es verdad que algunos tienen todavía dudas acerca de los beneficios que puede ofrecer, pero se van acercando poco a poco hacia la nube a través de pequeños proyectos, en vez de apostar de primeras por un gran proyecto transformador, y a partir de ahí empiezan a incorporar más servicios.

## Educación y digitalización



**Sebastián Reyna**

Miembro de la junta  
directiva de  
Cibercotizante

Tenemos que contrastar todos los cambios que la pandemia del Covid-19 va a producir en el futuro de la sociedad y en particular en el mercado laboral, sin embargo hay un consenso básico entre todos los agentes privados y públicos cuya primera consecuencia será la aceleración de todos los cambios que ya se venían perfilando en el proceso de digitalización de las empresas y de la actividad económica.

La revolución tecnológica y la aplicación de procesos de robotización en las empresas y en sus relaciones con proveedores y clientes, aconsejaba incluso con anterioridad, modificar la previsión de los perfiles profesionales demandados en el futuro. Para dar respuesta a este reto, resultaba imprescindible revisar en profundidad e incluso sustituir los sistemas de formación profesional, especialmente aquella formación vinculada al empleo y al necesario reciclaje de los trabajadores, a fin de que estos no lleguen a ser inempleables en el futuro.

Los confinamientos vividos y la restricción de la movilidad, ha obligado a las empresas a hacer un uso generalizado del teletrabajo, pero también a intentar poner al día, con desigual resultado, todos sus resortes tecnológicos y todas las posibilidades que las telecomunicaciones les facilitan para llegar con eficacia a sus clientes y facilitarles el servicio demandado. Pero, ¿sus trabajadores estaban preparados para ello? ¿los servicios de acompañamiento, información y soporte han funcionado correctamente?

Nada podemos añadir a los comentarios generalizados sobre los resultados positivos que la experiencia ha significado para superar la tradicional presencialidad de nuestras empresas y también el escepticismo ancestral de muchas de las más pequeñas en relación a las posibilidades que ofrece la tecnología, lo cual obliga a analizar los

déficits encontrados y actuar sobre ellos.

La principal dificultad ha venido de la escasa preparación de algunos empleados para afrontar esta nueva situación. Por desgracia los ciclos formativos en España terminan a edades cercanas a los cuarenta años, por lo cual muchos trabajadores mayores de esa edad, no han podido rendir adecuadamente al tener que afrontar retos tecnológicos que su formación no había contemplado. Por el contrario, entre los más jóvenes habituados al uso de herramientas tecnológicas, se ha puesto de manifiesto un alto nivel de desconocimiento y una falta de experiencia en determinadas capacidades y habilidades necesarias para la relación con clientes, habilidades con las que cuentan precisamente los trabajadores más veteranos. Urge un intercambio de conocimientos y experiencias entre generaciones, algo que nunca se había probado en nuestro país y que estaba fuera de cualquier programa formativo, que hemos echado en falta al comprobar que esa transferencia de conocimientos era casi imposible.

Contrastar esta realidad deberá servir al menos para realizar un diagnóstico más adecuado sobre cómo debe afrontarse la nueva formación tecnológica, que no implica tan solo el conocimiento de los equipos, sino también de las demandas formativas de personas en una sociedad más compleja y diversa. La formación dual práctica y el mentoring compartido entre personas con diversas experiencias y habilidades, deben formar parte de cualquier programa formativo futuro, pero es obligado superar la simplificación de estos conceptos. Los trabajadores de mayor edad deben pasar por nuevas etapas formativas y los más jóvenes tienen que profundizar su educación en el conocimiento y el control de una realidad que es más complicada que la que ofrece la pantalla del ordenador.

# Encuentros tecnológicos

# byte

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

TE ORGANIZAMOS UN ENCUENTRO AD HOC  
**INFÓRMATE**



- Sector Público
  - Banca
  - Sanidad
  - Seguros
  - Alimentación
  - Farmacéutico
- Y muchos más a tu alcance

Encuentros tecnológicos **byte **



¡EI ERP CON EL  
QUE TU EMPRESA  
ESTARÁ OK!

**solmicr**  
erp6

Tras una fuerte inversión en I+D+i, **Solmicro ERP 6** ve la luz. Un gran cambio tecnológico para la era digital. La máxima autonomía para tu negocio.

- ✓ **100% PERSONALIZABLE** a tus necesidades
- ✓ **RENTABLE.** Bajo coste inicial y de desarrollos.  
Máxima productividad
- ✓ **USABLE:** Interfaz moderna, intuitiva y fácil de usar. Rápida curva de aprendizaje
- ✓ **ESCALABLE:** Crece en rendimiento a la vez que en usuarios

## CON TECNOLOGÍA DE ÚLTIMA GENERACION

**TECNOLOGÍA VANGUARDISTA:** Pone a tu alcance soluciones de BI, IA, IoT, Realidad Virtual y Aumentada, Big Data...

**GARANTÍA DE EVOLUCIÓN FUTURA** manteniendo las personalizaciones.

**MIGRACIONES MÁS ÁGILES,** fáciles, transparentes y competitivas. Máxima compatibilidad con versiones futuras.

## ¡DI OK A LA ERA 4.0!

**INTERFAZ MÁS VISUAL,** sencilla e inteligente, que nunca se quedará obsoleta: usabilidad, rendimiento y conectividad.

**EXTENSIBILIDAD.** Personalizaciones funcionales y visuales que no alteran el estándar.

**MÁXIMA RENTABILIDAD.** Mayor productividad: reducimos los tiempos de las implantaciones y adaptaciones.

Desarrollado por **Zucchetti Spain**, el líder de los fabricantes de software ERP

30 años de experiencia  
2.300 implantaciones  
Centros propios de I+D+i

94 427 13 62



**ZUCCHETTI**