COMPARATIVA - - - >

Los últimos smartphones

www.revistabyte.es

Marzo 2019 • Nº 269 • 5,75 euros

byte TI

Síguenos en twitter: (@BYTE_TI)

ANÁLISIS

Samsung Galaxy S10+

Ciberseguridad: cada vez más necesaria

- Nuevos retos
- Establecer políticas de seguridad
- Soluciones novedosas

Hacia un nuevo Centro de Datos

Razones para apostar por la nube

mkm PUBLICACIONES

Javier López Sáez

Barracuda Total Email Protection

Proteja el email de su negocio de todos los ataques con un solo bundle de las más avanzadas soluciones.

Barracuda Essentials Protección de correo y archivado
Proteja su negocio de los ataques dirigidos al correo electrónico.

Barracuda Sentinel
Prevenga la usurpación de cuentas y los ataques de ingeniería social.

Barracuda PhishLine
Transforme la vulnerabilidad de los usuarios en una capa de defensa sólida.

Barracuda Essentials Cloud to Cloud Backup
Fomente la resistencia y mitigue los riesgos de incumplimiento.

Más información:
iberia_team@barracuda.com | barracuda.com

Barracuda.
Your journey, secured.

Estuve en el Mobile World Congress de Barcelona. Ha vuelto a ser un éxito de convocatoria, de buen hacer de la organización y del conjunto de autoridades. A ver si somos los suficientemente listos como para conservarlo, mejorarlo, si cabe, y disfrutar del mundo de la tecnología, que está en estado puro.

Me rindo

Siempre he sostenido que la marcha de nuestro sector, como no podía ser de otra manera, está vinculado a la salud económica del país y muy sensible a los cambios normativos bruscos. Por eso, cuando dependemos de políticos como Pedro Sánchez, me asusto sobremanera.

Tras nueve meses de su gobierno, el crecimiento ha empezado a bajar y el ritmo de crecimiento del empleo se ha estancado. La exhumación del dictador Franco (o inhumación, como dice la ministra encargada), me da que no ha servido para vender más soluciones tecnológicas, que es lo que nos viene bien a nosotros. En todo ese tiempo, los periodistas del sector sólo hemos recibido una convocatoria del Gobierno (para presentar un estudio de los hábitos de Internet). Un desastre auténtico de abandono.

Con todos los años que acumulo de ver, conocer, aguantar, soportar, padecer, y poco disfrutar, de políticos de todo tipo, con nuestro último presidente del Gobierno, he experimentado una sensación que no me había ocurrido con un personaje público: el menosprecio de mi pobre inteligencia con mensajes que nadie en su sano juicio puede creerse. Cada vez que le veo, o le escucho, me debe reventar alguna neurona que me hace padecer un dolor intestinal que solo remite con buscapina o similares.

Es una mezcla de rabia e impotencia: la primera por constatar cómo miente de forma compulsiva y la impotencia de no poder subvertir la idea de que nos va a volver a gobernar: somos lo suficientemente memos como para votar a un tío que, como decía un periódico madrileño, no miente más porque no tiene más tiempo. Estoy convencido de que en un país con un nivel cultural medio (lamentablemente en España no lo tenemos), tipo Suecia o Dinamarca, un personaje como Sánchez no sacaría cuatro votos.

Como, además, las alternativas que tenemos tampoco son para tirar cohetes (Casado compitiendo con VOX, ¡madre mía!), yo me rindo: como sé que todos vais a ir a votar (principio básico del sistema democrático, en el que creo), yo me voy a aprovechar y me daré un paseo divino por mi monte de Boadilla.

Como he dicho en otras ocasiones, tenemos que hacer abstracción de toda esta fauna y dedicarnos de lleno a trabajar, innovar e invertir en tecnología, que es el futuro para todos.

SUMARIO

TEMA DE PORTADA

La seguridad se abre paso en la empresa

42

N.º 269 • ÉPOCA III

Director
Juan Manuel Sáez
(juanmsaez@mkm-pi.com)

Redactor Jefe
Manuel Navarro
(mnavarro@mkm-pi.com)

Coordinador Técnico
Javier Palazon

Colaboradores
S. Velasco, R.de Miguel, I. Pajuelo, O. González, D. Rodríguez, F. Jofre, JL. Valbuena, MªJ. Recio, MA. Gombáu, J. Hermoso, JC. Hernández, C. Hernández, M. Barceló, A.Barba.

Fotógrafos
E. Fidalgo, S. Cogolludo, Vilma Tonda

Ilustración de portada
Javier López Sáez

Diseño y maquetación
El Palíndromo Comunicación S.L.

WebMaster
NEXICA
www.nexica.es

REDACCIÓN
Avda. del Generalísimo, 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
Ignacio Sáez (nachosaez@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 autorizació expresa por escrito del titular del Copyright. La cabecera de esta revista es Copyright 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.

MARZO de 2019
Printed in Spain

EDITA
Publicaciones Informáticas MKM

ACTUALIDAD DEL MES

COMPARATIVA

TENDENCIAS

3 CARTA DEL DIRECTOR

6 ACTUALIDAD

22 DESAYUNO Centro de Datos

26 COMPARATIVA

42 TEMA DE PORTADA

56 UN CIO EN 20 LÍNEAS

58 APLICACIÓN PRÁCTICA

60 TENDENCIAS

64 ENTREVISTA

66 TEMPORAL Por Miquel Barceló

Smartphones plegables y 5G, triunfadores del MWC 19

El Mobile World Congress celebrado esta semana en Barcelona ha destacado por dos elementos: los smartphones plegables y la tecnología 5G.

Por Redacción Byte TI

En el primero de los casos, no se sabe el éxito que puedan tener estos smartphones plegables toda vez que sobre ellos penden dos espadas de Damocles: cómo afectará la apertura constante de los smartphones a la durabilidad de los mismos y, por supuesto el precio. Fue Samsung, una semana antes del inicio de la fera la que dio el pistoletazo de salida a este tipo de equipops pero a continuación, y ya durante la feria, Huawei sorprendió con su nuevo smartphone. Ambos equipos rondan los 2.000 euros, por lo que, en principio, se puede afirmar que son simples prototipos para ver si el público los asume. Es cierto que algo hay que destacar: por primera vez en los últimos años, los fabricantes han arriesgado y han sacado un modelo disruptivo, lejos de ampliar el almacenamiento o incorporar más cámaras.

En cuanto al 5G, ha sido una de las principales protagonistas. Se han podido probar las bondades de esta tecnología y se han presentado los primeros terminales. La operadoras también se han esforzado en mostrar su desarrollo, pero una

cosa está clara: al menos hasta el año que viene no se podrá disfrutar de 5G por parte de una mayoría de usuarios. Fuera de estos dos elementos, estos han sido algunas de las novedades más relevantes de la feria:

HOLOLENS 2

Microsoft presentó las HoloLens 2 que incluyen un sistema de visualización que hace que los hologramas sean más realistas. La compañía ha duplicado el campo de visión en HoloLens 2, mientras mantiene la densidad holográfica de 47 píxeles por grado de visión. HoloLens 2 contiene un nuevo sistema de visualización que permite alcanzar grandes avances de rendimiento con baja potencia. Aprovechando un nuevo sensor de profundidad, combinado con la comprensión semántica y de Inteligencia Artificial integrada, HoloLens 2 permite manipular los hologramas directamente con los mismos gestos intuitivos que se emplean para interactuar con los objetos físicos.

HPE

HPE y Continental han anunciado una nueva plataforma para compartir los datos generados por los vehículos con el fin de ofrecer nuevos servicios digitales que mejoren la seguridad y comodidad de los conductores. Al mismo tiempo, la plataforma ayudará a los fabricantes de automóviles a rentabilizar sus datos y a diferenciar sus marcas. Esperando que esté disponible a lo largo de 2019, la plataforma proporciona control al usuario, seguridad, transparencia y eficiencia de los datos para superar las barreras al compartir la información generada.

CONEXIONES 5G

Orange y Ericsson han llevado a cabo la primera conexión de datos 5G a través de equipos Radio NR de Ericsson totalmente compatibles con 3GPP conectados a la red comercial de Orange en España. Orange y Ericsson han demostrado este hito, retransmitiendo una Haka, la danza tribal maorí, a través de una red comercial 5G y conectando en directo tres nodos New Radio (NR) situados en tres localizaciones diferentes.
Por su parte, Huawei y Vodafone han desarrollado en conjunto una experience zone durante el Mobile World Congress 2019 (MWC). En esta zona, Vodafone ha implementado sites 5G con espectro comercial 5G con el fin de construir una red 5G de alto rendimiento con productos y soluciones end-to-end de Huawei. A través de esta red, se proporcionan varios servicios de banda ancha móvil mejorada (eMBB, por sus siglas en inglés) utilizando el teléfono plegable 5G, Huawei MateX, y equipos locales del cliente (CPE, por sus siglas en inglés) para ofrecer la mejor experiencia de servicio 5G.

Sobresaliente

CONEXIÓN A INTERNET

Según el informe de la ONTSI, siete de cada diez personas se conectan diariamente a Internet en España y destaca el incremento de población internauta entre la franja de edad de 65 a 74 años, con una conexión semanal del 42% frente al 38% del año 2017. La conexión a Internet entre las personas de 16 a 34 años, los estudiantes y las personas con estudios superiores supera el 95%.

KASPERSKY

Los ingresos de Kaspersky Lab han alcanzado los 726 millones de dólares, con un incremento del 4% en sus cifras interanuales. Durante 2018, y a pesar de la evolución de las condiciones del mercado la compañía ha cerrado el año con éxito gracias a la confianza de clientes y partners y al desarrollo de soluciones y servicios de ciberseguridad líderes.

Suspenso

SEGURIDAD EN CLOUD

Según Check Point, el 30% de los profesionales TI todavía piensa que la seguridad cloud es responsabilidad del proveedor: este dato tan preocupante va en contra de las recomendaciones de que la seguridad cloud debe basarse en un modelo de responsabilidad mutua, en el que tanto el proveedor y el cliente comparten la toma de decisiones en torno a la seguridad.

SUPLANTACIÓN DE IDENTIDAD

La firma de Proofpoint ha realizado un análisis para conocer los riesgos de suplantación de identidad en Europa, en el que destaca la baja tasa de adopción de mecanismos de defensa frente a ciberdelincuentes de empresas del Ibex 35. Según el citado estudio, un 69% de estas compañías están expuestas al fraude por correo electrónico y a la suplantación de dominio

LA OPINIÓN DE
Fernando Jofre

DaaS: el nuevo concepto cloud

Si las predicciones de los analistas se cumplen, en los próximos dos años el mercado de DaaS (Device as a Service) va a experimentar un notable crecimiento. En el 2016 tan sólo un 1% de los dispositivos empresariales se suministraban bajo esta novedosa fórmula (novedosa en TI, porque otros sectores como el automovilístico la tienen bien asimilada), y según IDC se espera que en 2020 alcance entre un 12 y un 15%.

Ese tránsito del gasto de Capex a Opex es realmente atractivo los para los presupuestos de los CIO, así como para los departamentos financieros de cualquier organización. Y gran parte del ecosistema de proveedores de TI centrados en el mantenimiento tanto de PCs/portátiles como de dispositivos móviles va a tener que ponerse las pilas. Teniendo en cuenta además que no afectará sólo a los dispositivos, sino también al software instalado en ellos. Hardware, software y servicios bajo un mismo contrato.

El concepto es sencillo: conocidos ya los beneficios del cloud, se trata de aplicar los mismos principios a la infraestructura que utilizarán mis empleados. Que dispongan de la última tecnología, con las herramientas óptimas para trabajar. Y así el departamento de TI externaliza otra pieza más del puzle, cediendo la administración de equipos a un tercero. ¿Beneficios? Reducción de costes, más flexibilidad financiera, reducción de la carga de trabajo para los departamentos de TI, se acortan los ciclos de actualización de equipos/software y también más seguridad: además de proporcionar software de seguridad en el dispositivo, DaaS va a liberar recursos de TI que se podrán centrar en nuevas iniciativas de seguridad. ¿Qué más se puede pedir?

HPE ayuda a los CSP

HPE ha presentado la plataforma HPE Edgeline EL8000 Converged Edge System con la que pretende ayudar a los Proveedores de Servicios de Comunicaciones (CSP) en el despliegue rápido de servicios que requieran un uso intensivo de datos y baja latencia en los extremos de la red de acceso. Por ello, la plataforma es ideal, entre otros casos de uso, para servicios de difusión de contenidos multimedia, movilidad conectada y ciudades inteligentes. Asimismo, HPE también ha anunciado un acuerdo con Samsung y Tech Mahindra para acelerar la implantación de redes 5G, permitiendo la transformación hacia redes basadas en estándares abiertos con HPE Edgeline EL8000 Converged Edge System.

Para poder respaldar el rápido crecimiento en la demanda de procesamiento datos y despliegue de servicios digitales en tiempo real, los CSPs están tendiendo a transformar el extremo de su red de telecomunicaciones hacia sistemas estándar TI y arquitecturas definidas por software. Para dar soporte a dicha transformación, los HPE Edgeline EL8000 Converged Edge System basados en estándares abiertos, han sido desarrollados para poder reemplazar a sistemas propietarios de los CSP, ofreciendo alto rendimiento y baja latencia para los casos de uso más demandados. Por ello, son plataformas utilizadas para la virtualización de los servicios de la red de acceso radio (vRAN) y Sistemas de Terminación de Cable módems (vCMTS), siendo también ideales para la transmisión multimedia (media streaming), IoT, inteligencia artificial y analíticas de vídeo, por su compacto y robusto factor de forma, capacidad funcional, así como sistemas de gestión remota.

El crecimiento masivo del volumen de datos requiere que los CSP desplieguen sistemas de gran rendimiento y que puedan garantizar una alta calidad en el servicio en las celdas de comunicaciones. La solución de HPE ofrece varias características de diseño único para hacer frente a estos desafíos.

ESET BUSINESS SOLUTIONS

BLINDA TU EMPRESA CON LA COMODIDAD DE LA NUBE

Gestiona toda la ciberseguridad de tu empresa estés donde estés.

PREDICCIÓN

ESET Threat Intelligence
ESET Virus Radar
WeLive Security

PREVENCIÓN

Endpoint Protection Platform
ESET Mail Security
ESET Gateway Security
ESET SharePoint Security
ESET Secure Authentication
ESET Endpoint Encryption
ESET Security Management Center
ESET Cloud Administrator

RESPUESTA

ESET Enterprise Inspector
ESET Dynamic Threat Defense
ESET Security Management Center
ESET Cloud Administrator

DETECCIÓN

Endpoint Protection Platform
ESET Dynamic Threat Defense
ESET Enterprise Inspector
ESET Mail Security
ESET Gateway Security
ESET SharePoint Security
ESET Secure Authentication
ESET Endpoint Encryption
ESET Security Management Center
ESET Cloud Administrator

CYBERSECURITY
EXPERTS ON
YOUR SIDE

PROVEEDOR Nº 1 DE LA UNIÓN EUROPEA EN CIBERSEGURIDAD EMPRESARIAL

MADE IN EU

go.eset.es/byte

LA OPINIÓN DE
Manuel Navarro

Trabajar en Google o en Amazon

En mi época de universitario el objetivo de muchos de mis compañeros era encontrar un puesto en Telefónica, Repsol o Endesa en el que estuvieran el resto de sus días hasta que llegase el día de la jubilación. Hoy, eso ha cambiado. Partamos del hecho de que nno me creo esas estadísticas que dicen que los jóvenes quieren ser emprendedores y tener sus propios negocios. Esa afirmación está bien para vender humo y poco más. La realidad es que son muy poquitos los que tienen esa capacidad, básicamente porque la imaginación (elemento indispensable para imaginar el futuro negocio) no es algo que sea habitual entre la totalidad de la población. No, los jóvenes actuales saben que, lo normal es que no ingresen en una empresa y acaben sus días laborales en ella. Saben que van a ir cambiando de empleo el resto de sus días. Pero sí que tienen muy claro que lo que quieren es trabajar en determinadas empresas (y no ser emprendedores).

Pues bien, Merco y PeopleMatters han dado a conocer los resultados de la 2ª Edición de Merco Talento Universitario en España, que recoge las 100 empresas más atractivas para trabajar según los universitarios. En esta segunda edición del ranking de las mejores empresas españolas para trabajar según los universitarios la encabezan Google, Amazon, Inditex, Mercedes Benz, Apple, Mercadona, Santander, Coca-Cola, Microsoft y BBVA. Los jóvenes consideran como los factores más importantes a la hora de elegir una empresa como lugar para trabajar, una buena retribución y beneficios, la calidad de vida, la formación y el desarrollo profesional que ofrecen, así como un buen ambiente de trabajo. Vamos, nada que ver con crear startups por doquier.

Reconocimiento facial en el cajero

CaixaBank se ha convertido en el primer bancodel mundo que ofrecerá a sus clientes la posibilidad de sacar dinero de sus cajeros automáticos mediante reconocimiento facial y sin necesidad de introducir su PIN. La entidad, ha presentado el sistema en un acto que supone el lanzamiento comercial del servicio para todos los clientes que quieran utilizarlo en los cajeros que dispongan de la nueva tecnología.

El objetivo de la implantación de la tecnología de reconocimiento facial en cajeros es ofrecer una mejor experiencia de usuario y una mayor seguridad en las operaciones, ya que agiliza el proceso de identificación del cliente y facilita la realización de reintegros sin memorizar múltiples contraseñas. CaixaBank ya tiene en funcionamiento este sistema de verificación en los cajeros de cuatro oficinas Store de Barcelona, con un total de 20 terminales. La entidad prevé realizar progresivamente la expansión del reconocimiento facial en sus oficinas Store a partir del segundo semestre de 2019.

El sistema es totalmente pionero a nivel mundial al permitir extraer dinero del cajero simplemente reconociendo al usuario a través de la imagen captada por la cámara del terminal. El cajero dispone del hardware y el software necesario para validar hasta 16.000 puntos de la imagen del rostro del usuario, lo que garantiza una identificación totalmente segura.

Sin embargo, el cliente podrá elegir en cada momento la tecnología de identificación personal más conveniente, pues en los cajeros de CaixaBank coexistirán ambas posibilidades: identificación mediante reconocimiento facial o identificación por PIN.

El lanzamiento de este nuevo servicio para cajeros se enmarca dentro de los objetivos del Plan Estratégico 2019-2021 de CaixaBank, en el cual los proyectos de innovación tienen una importancia clave.

a3ERP

Solución integral de gestión para PYMES

La visión 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 AHORA Y DESCUBRE CÓMO SER MÁS COMPETITIVO CON **a3ERP**.

Wolters Kluwer

902 330 083
www.wolterskluwer.es

LA OPINIÓN DE
Óscar González

SecDevOps

Durante los últimos años, el término "DevOps" ha pasado de ser un término de "hype" a ser una realidad en cualquier empresa que desarrolle software de forma seria. Trata de la organización del ciclo de vida de desarrollo y explotación de productos o servicios basados en software, e intenta atajar los problemas derivados tanto de un desarrollo ágil y cambiante, como de una explotación de sistemas que tiene que ser sólida y segura. Ambos mundos nunca se han llevado bien, y "DevOps" es un conjunto de técnicas y herramientas para intentar que se lleven mejor. Últimamente también hay que lidiar con la seguridad. Seguridad del código fuente, de los procesos de compilado y empaquetado, procesos de distribución y despliegue. Un aspecto que a día de hoy está siendo infravalorado en muchas empresas, pero que tiene importantes consecuencias en el mundo real. Pasado el "hype" de Devops, entramos ahora en el de "SecDevOps".

Fabricantes de hardware de seguridad, grupos de gurús y desarrollos de herramientas privativas y de opensource aparecen de forma tímida para abordar los importantes retos que surgen. Y es que en este mundo de startups, desarrollo ultra-ágil y entrega continua "extrema", son muchísimas las organizaciones que sin saberlo están poniendo software en producción de manera poco segura, confiando en la seguridad perimetral tradicional. Queda todavía pendiente una importante tarea de envangelización del tema, ya que de forma habitual muchas empresas no quieren asumir el coste de incorporar técnicas de seguridad a su ciclo de desarrollo, simplemente porque no se visualiza como una mejora inmediata. Actualmente se vé más como un coste innecesario que como una inversión necesaria, y es una visión que en el corto plazo debe de cambiar de manera drástica.

Dell y sus soluciones de almacenamiento

Dell EMC anuncia capacidades nuevas y mejoradas para el portafolio de soluciones de almacenamiento de Dell EMC Data Domain e Integrated Data Protection Appliance (IDPA), diseñados para ofrecer a las organizaciones flexibilidad y valor con capacidades ampliadas de múltiples nubes y un rendimiento optimizado. Las mejoras en la soluciones de almacenamiento de Dell EMC también brindan a las organizaciones medianas y a las oficinas remotas de organizaciones grandes más posibilidades y opciones para obtener protección de datos a nivel empresarial.

El software Data Domain OS 6.2 e IDPA 2.3 ofrece a los clientes más opciones para extender su protección de datos a nubes públicas con soporte ampliado de Cloud Tier a Google Cloud Platform y Alibaba Cloud, permitiendo así una mayor flexibilidad para la retención a largo plazo. Además, una nueva herramienta de estimación de espacio libre para el nivel de nube facilita una administración de capacidad más eficiente para ayudar a reducir los costes de almacenamiento en la nube y en las instalaciones.

Dell EMC también ha ampliado su ecosistema de proveedores de nube pública compatibles para Data Domain Virtual Edition (DD VE), que proporciona protección de datos definida por software en las nubes locales y públicas, a AWS GovCloud, Azure Government Cloud y Google Cloud Platform. Esto se suma a las plataformas ya compatibles AWS S3 y Azure Hot Blob. El ecosistema de nube ampliado y combinado con la capacidad previamente anunciada de DD VE, hasta 96TB por instancia, garantiza que los clientes recibirán el mismo nivel de protección dentro de sus entornos de nube que reciben de sus dispositivos locales de Dell EMC.

Además, la recuperación de desastres en la nube nativa está ahora disponible para toda la familia IDPA.

Panda Adaptive Defense 36C

Visibilidad sin Límites, Control Absoluto

SIN SECUESTRO, NO HAY RE$CATE

En los últimos años el Ransomware ha provocado pérdidas millonarias. Durante el 2017 provocó costes en torno a los cinco mil millones de dólares, lo que lo ha convertido en el tipo de ciberataque con más impacto y sofisticación, con un aumento de 350% respecto al año anterior.

Pero cuando tu negocio está protegido por **Panda Adaptive Defense 360**, no tienes que temer al secuestro, porque para la plataforma de ciberseguridad más avanzada, el malware no es un problema en absoluto.

Y es que **ningún malware ha afectado nunca a ningún dispositivo con Panda Adaptive Defense 360** en modo lock.

panda

pandasecurity.com/business/adaptive-defense/

OVH se consolida en el mercado español

OVH acaba de celebrar su 20 aniversario con España como uno de los mercados clave a nivel mundial. En la actualidad, OVH ya cuenta con 28 datacenters ubicados en 12 localizaciones

El grupo continúa su plan de expansión, apoyado por la innovación y fruto de la fase de inversión de 1500 millones de euros que inició en 2016 y que continuará hasta el 2020. «España es un país fundamental en la estrategia global de OVH y ha conseguido establecerse como un mercado clave para el desarrollo de nuestro negocio en Europa. Prueba de ello es el crecimiento de dos dígitos de la división española en el 2018, que va en sincronía con la tendencia de aumento del mercado cloud en nuestro país. Por otra parte, estamos orgullosos de contribuir a que las empresas locales puedan impulsar un crecimiento rápido de sus recursos digitales, consolidando su infraestructura informática y con un modelo interoperable y reversible», afirma Romain Coplo, Sales Director Cloud de OVH.

El año 2018 ha sido especialmente significativo para OVH. Entre los diversos avances destaca la apertura de una nueva fábrica de 14 000 m2 ubicada en Croix, Francia, que incorpora las últimas tecnologías y que permite cuadriplicar la capacidad de producción de la compañía, pasando de 120 000 a 400 000 servidores al año. Las migraciones en caliente entre datacenters también ocupan un punto de referencia entre los logros del pasado año. La idea de migración de workloads entre datacenters sin tiempos de inactividad era algo impensable hasta hace poco tiempo, pero durante el año pasado OVH consiguió migrar las cargas de trabajo de sus clientes de vClour Air de todo el mundo, gracias a la tecnología Hybrid Cloud Extension (HCX), lo que ha supuesto mover unos 500 entornos y casi 9000 máquinas virtuales, con un volumen total de datos de 3 petabytes.

INNOVACIÓN PERMANENTE

La fortaleza de OVH como proveedor mundial de cloud hiperescalable también se ha visto revalidada en los últimos meses con el relanzamiento de su solución Private Cloud: una oferta de Software-Defined Datacenter (SDDC) que integra la innovadora tecnología vSAN de VMware y la tecnología HCX para permitir la hiperconvergencia y garantizar un rendimiento extraordinario.

El nuevo año vendrá marcado asimismo por el crecimiento y la diversificación de servicios adaptados a cada tipo de cliente. Por ese motivo OVH anuncia la llegada de un amplio abanico de infraestructuras de datos listas para usar, así como la inminente actualización de su gama de servidores dedicados. Una gama que se completará también en este año con los nuevos servidores de Alta Gama 2019, basados en los procesadores escalables Intel Xeon y especialmente dimensionados para el calculo intensivo.

Deje que fluya su creatividad. Y aleje las ciberamenazas

Kaspersky Endpoint Security Cloud.
La seguridad que necesita con la flexibilidad que desea

El 40 % de las empresas afirma que el aumento de la complejidad de su infraestructura está llevando sus presupuestos al límite. Kaspersky Endpoint Security Cloud ayuda a las pequeñas y medianas empresas a simplificar la gestión de la seguridad, sin tener que invertir en recursos o hardware adicional. Gestione la seguridad de endpoints, dispositivos móviles y servidores de archivos Mac y Windows de forma remota, desde cualquier lugar, con nuestra consola basada en la nube.

cloud.kaspersky.com

© 2017 Kaspersky Lab Ibería, España. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.

Ibermática potencia la Industria 4.0

Ibermática participa en el desarrollo del proyecto europeo iDev40 (Integrated Development 4.0). La iniciativa cuenta con un presupuesto de 47 millones de euros

Liderado por la filial austriaca de la firma Infineon Technologies AG, líder en el mercado de semiconductores, iDev40 cuenta con la colaboración de 38 compañías, procedentes de 6 países que investigarán durante tres años en materia de redes inteligentes de procesos de desarrollo y producción para componentes y sistemas electrónicos. El programa se centrará en tres líneas de investigación principales: seguridad de los datos y gestión del conocimiento a lo largo del ciclo de vida del producto, flujo de información digital e innovación aplicada a la cadena de suministro.

La Industria 4.0 trae un nuevo modelo en el que la administración segura e inteligente de grandes cantidades de datos permitirá analizar cada vez más información a mayor velocidad, tanto del funcionamiento de dispositivos y sistemas tecnológicos, como de los trabajadores y usuarios. Los equipos de desarrollo y producción del tejido industrial se interconectarán entre sí, independientemente de su ubicación, y se comunicarán en tiempo real a lo largo de toda la cadena de valor. Los procesos podrán monitorizarse virtualmente en tiempo real y replicarse rápidamente en un contexto de fábrica digital en el que la Inteligencia Artificial y el aprendizaje automático desempeñan un papel central.

Un aspecto al que la investigación de iDev40 prestará especial atención es al de los nuevos perfiles profesionales que traerá consigo la Industria 4.0 y a las habilidades que se necesitarán para interactuar con sistemas altamente automatizados y complejos.

A través de este proyecto, más de 15.000 empleos quedarán asegurados a medio-largo plazo en las compañías involucradas. Si se suma a toda la comunidad de partners de estas compañías a lo largo de toda la cadena de valor de componentes y sistemas electrónicos, las cifras aumentan hasta los 50.000 empleados en todo el mundo.

EL PAPEL DE IBERMÁTICA

Una de las principales áreas en las que colaborará Ibermática entronca con el desarrollo de un caso práctico de Digital Tween (gemelo digital), replicando virtualmente un tren de impulsión para una aplicación de trabajo pesado en una factoría. El objetivo es desarrollar un sistema basado en cloud que reciba y procese todos los datos recopilados de diferentes fuentes, como sensores de vehículos o bancos de pruebas, entre otras, para predecir cómo se comportará ese vehículo, encontrar anomalías en los datos, hacer recomendaciones predictivo-proactivas de mantenimiento, etcétera, mediante el uso de herramientas de Inteligencia Artificial.

LAB SEC
Blockchain

PRIMER LABORATORIO DE EXPERIENCIAS DE NEGOCIO BLOCKCHAIN, EN INTELIGENCIA ARTIFICIAL Y SMART CONTRACT

Unimos los conceptos de Ciberseguridad y Blockchain para securizar las transacciones de las compañías, además de crear contextos y redes Blockchain, consolidando al máximo la seguridad de las organizaciones.

labsec-blockchain.com

LAB SEC BLOCKCHAIN, UN LABORATORIO CREADO POR:

OneseQ by alhambraoidos

enki.blue.

Metro de Madrid se apunta a la inteligencia artificial

Accenture ha ayudado a Metro de Madrid a desarrollar un sistema de ventilación autodidacta basado en Inteligencia Artificial (IA) que minimiza los costes de energía

Este sistema basado en IA ha permitido que Metro de Madrid reduzca su consumo de energía por ventilación un 25% y 1.800 toneladas anuales de sus emisiones de CO2. Accenture presentará este sistema en el MWC (anteriormente conocido como Mobile World Congress) de este año en Barcelona, durante el 25 y el 28 de febrero.

Cada día, una media de 2,3 millones de viajeros utiliza los 294 kilómetros de vía y las 301 estaciones de Metro de Madrid. Para ayudar a los pasajeros a estar cómodos dentro de las estaciones, sobre todo en los calurosos meses de verano, el Metro tiene instalados 891 ventiladores que consumen hasta 80 gigavatios de energía anuales. En el MWC de Barcelona, Accenture contará con una demo del sistema de ventilación basado en Inteligencia Artificial del Metro de Madrid, capaz de reducir 1.800 toneladas anuales de emisiones de CO2

Los expertos de ventilación de Metro de Madrid trabajaron junto al Accenture Applied Intelligence para desarrollar un sistema basado en una fuente de inspiración insólita: el comportamiento coordinado de una colonia de abejas en búsqueda de alimento. Así, el sistema utiliza un algoritmo de optimización capaz de movilizar grandes cantidades de datos para obtener todas las combinaciones posibles en cuanto a temperatura del aire, arquitectura de la estación, frecuencia de trenes, carga de pasajeros y precio de la electricidad a lo largo del día. El algoritmo utiliza datos tanto históricos como simulados, y tiene en cuenta la temperatura externa y la del subsuelo durante las siguientes 72 horas. Además, como utiliza machine learning, el sistema va mejorando a la hora de predecir el balance óptimo para cada estación de la red a lo largo del tiempo.

NUEVO SISTEMA DE VENTILACIÓN

El sistema también incluye un motor de simulación y un módulo de mantenimiento que permite, entre otras cosas, detectar los fallos de operación de los ventiladores. De esta manera, Metro de Madrid puede monitorizar y gestionar fácilmente el consumo de energía, identificar y responder a las deficiencias del sistema y llevar a cabo de manera proactiva el mantenimiento de los equipos.

"Gracias a la ayuda de Accenture y a este innovador sistema de ventilación, hemos conseguido una dualidad de beneficios: la disminución de los costes de energía y la reducción del impacto medioambiental", según Isaac Centellas, director de Ingeniería y Mantenimiento del Metro de Madrid.

LA MEJOR PROTECCIÓN ENDPOINT

¿CUÁNDO NOS HAN ATACADO?
¿POR DÓNDE HAN ENTRADO?
¿QUÉ DAÑOS HAN CAUSADO?

Obtenga la capacidad de detectar, investigar y responder a posibles amenazas de seguridad con Sophos Intercept X ahora con EDR

Más información
www.sophos.com/es-es/intercept-x.aspx

SOPHOS

Huawei sorprende en el MWC 19 con su smartphone plegable

Huawei fue de las primeros en convocar a la prensa en el MWC 19 para deleitar a los más de 1.500 convocados con una batería de nuevos productos

Por Juan Manuel Sáez (Barcelona)

Entre los productos destaca el smartphone plegable 5G que, a juzgar por los comentarios compartidos con redactores que también pudieron ver la semana pasada el modelo de Samsung, y lo que se sabe del de Apple, (y a la espera de un análisis más específico), los supera ampliamente en prestaciones.

Para la firma china el Mate X supone un viaje a un territorio desconocido: "combina 5G, pantalla plegable, IA y un nuevo modo de interfaz para proporcionar a los consumidores una experiencia de usuario sin precedentes y ofrecer una nueva generación de teléfonos inteligentes. Como resultado de la experimentación audaz por parte de Huawei con los novedosos factores de forma de los smartphones, el teléfono inteligente y tablet "2 en 1" Huawei Mate X cuenta con un panel OLED flexible y una bisagra mecánica Falcon Wing que combina estilo con tecnología. El smartphone lanzado en el MWC 19 es ligero y plegable y se presenta en nuevo tono de color "Azul Interestelar" que personifica la belleza de la tecnología y establece un listón más alto para los futuros smartphones".

Huawei Mate X es más que un smartphone plegable o una tablet, es mayor que la suma de sus partes. La flexible pantalla OLED plegable FullView y el chipset de módem 5G más rápido del mundo, Balong 5000, se combinan para ofrecer un nuevo modo de interfaz, en el que la experiencia de gran pantalla y la portabilidad coexisten en armonía. Los usuarios pueden aprovechar dos pantallas simultáneamente en este smartphone plegable para llevar a cabo múltiples actividades y disfrutar de una experiencia similar a la de sobremesa.

Los smartphones buques insignia de Huawei siempre incorporan cámaras potentes y, como se ha visto en el MWC 19 el smartphone plegable Huawei Mate X no es una excepción. Huawei Mate X dispone de una batería de alta capacidad de 4.500 mAh compatible con Huawei SuperCharge, lo que satisface la demanda de mayor rendimiento de la batería en la era 5G.Huawei MateBook X Pro actualizado.

NO SÓLO MÓVILES

La multinacional china también ha presentado en el MWC 19, los nuevos Huawei MateBook de 13" y 14" llevan la última tecnología a los consumidores tradicionales. Combinan pantallas FullView con alto rendimiento, portabilidad extrema, una estructura de excelente calidad y un diseño elegante para realizar actividades de próxima generación. Aunque están dirigidos a todo tipo de consumidores en general, estos portátiles revolucionarios permiten la interconexión inteligente entre dispositivos inteligentes y el PC, redefiniendo cómo los dispositivos pueden interactuar y conectarse entre sí.

Cloud, ¿un reto de seguridad para los CISOs?

Los CISOs juegan un papel fundamental en las organizaciones para mantener la infraestructura corporativa a salvo de las ciberamenazas. Se enfrentan a numerosos retos, no solo de justificación de presupuestos de TI, sino de nuevas infraestructuras y formas de trabajar de las empresas. Por ejemplo, el cloud computing, una parte clave en el viaje estratégico de la transformación digital.

La adopción de la nube es imparable, y es que cada vez más empresas tienen al menos una aplicación o una parte de su infraestructura TI alojada. Este cambio se está produciendo a ritmos imparables, pero los riesgos también lo hacen. ¿Están prepradas las empresas para este salto? ¿Y los CISOs?

Según el informe "What It Takes to Be a CISO: Success and Leadership in Corporate IT Security" de Kaspersky Lab, cerca del 60% de los CISOs europeos ve que la expansión sin control de la nube en las organizaciones es un tema de gran preocupación en materia de sgueridad.

Si bien es cierto que la nube híbrida facilita a las empresas entregar sus productos y servicios más rápidamente, optimizar su rendimiento y mejorar la fiabilidad de los servicios, la nube puede presentar retos adicionales de ciberseguridad, sobre todo cuando la infraestructura está alojada en un tercero.

De hecho, una filtración media de datos en un incidente en la nube pública, puede suponer a la empresa casi 1,5 millones de euros. Así, mientras que la infraestructura TI de una organización se vuelve heterogénea con la nube, los CISOs se enfrentan a nuevos quebradores de cabeza para mantener sus datos seguros, proteger las finanzas y la reputación de la empresa.

Además, la adopción de la cloud híbrida requiere especialistas con conocimientos necesarios para configurar y administrar la seguridad de las partes de la infraestructura TI. Aquí los retos se incrementan para los CISOs. De hecho, un 38% considera que es difícil encontrar especialistas que puedan trabajar en esta infraestructura cada vez más compleja.

Ante este panorama, los CISOs necesitan una solución que no solo les ofrezca un alto nivel de seguridad, sino que también garantice que la capa de ciberseguridad de la empresa sea visible y pueda ser administrada en toda la infraestructura de la nube, incluso por un equipo de seguridad cloud limitado.

Asimismo, y ante el rápido crecimiento, las empresas no van a detener la adopción por la falta de problemas de seguridad. En este sentido, es vital que la seguridad resiliente también se implemente de forma rápida y efectiva.

Por ello, es crucial proteger los datos y las cargas de trabajo en la nube. Asimismo, las capas de protección deben incluir la capacidad de monitorizar el comportamiento de la aplicación y prohibir cualquier actividad sospechosa; evitar las brechas mediante el uso de la última inteligencia de amenazas y encontrar y parchear automáticamente las vulnerabilidades, para proteger de las amenazas los datos y las cargas de trabajo que transitan a través de la infraestructura de la nube.

El CISO tiene un rol fundamental en la transformación digital y en la adaptación a la nube de las organizaciones. Gestionar la nube y tener un control de los presupuestos de TI ayudarán a la empresa a iniciarse en la senda de una estrategia de seguridad 100% efectiva.

Alfonso Ramírez,
director general de Kaspersky Lab Iberia

Hacia un nuevo centro de datos

El centro de datos está evolucionando a grandes velocidades. Para hablar sobre ello, BYTE TI organizó un desayuno al que asistieron Ramón Rodríguez, Data Centers Solution Architect de Schneider Electric; Luis Colino, Director de Preventa Sur de Europa de Microfocus; Manuel Lendinez, Business Unit Outsourcing Systems and Cloud Datacenter de IECISA; Miguel Rebodero, Alliances Manager de Econocom e Ignacio Arrieta, Commercial Account System Engineer Manager for Iberia de Dell EMC.

Por Manuel Navarro Ruiz

El encuentro comenzó con el análisis de la situación del mercado. Ramón Rodríguez, Data Centers Solution Architect de Schneider Electric fue el encargado de abrir el debate afirmando que "actualmente, la situación es buena. La irrupción de nuevas tendencias hace que el centro de datos se encuentre en auge. Además, la mejora de la conectividad va a permitir que en España y Madrid se postule como posible hub europeo en el futuro ". Para Luis Colino, Director de Preventa Sur de Europa de Microfocus, el principal cambio radica en que "el data center ya no son cuatro paredes como antaño. Esta es la principal diferencia. Cloud ha desmitificado el data center clásico y ahora mismo hay un mix de todo: híbrido, tradicional, etc. Estamos en un momento muy importante para los centros de datos".

Cloud estuvo presente durante todo el encuentro y, en este sentido, Manuel Lendinez, Business Unit Outsourcing Systems and Cloud Datacenter de IECISA afirmó que "lejos de pensar que el cloud iba a acabar con el data center, lo cierto es que los clientes están solicitando más soluciones de centros de datos que nunca. Lo que ha cambiado es la concepción y se ha transformado en un elemento básico para acceder a la hibridación". Por su parte Miguel Rebodero, Alliances Manager de Econocom, consideró que "ahora hay una explosión en cuanto a tecnología, innovación etc. Los CIO tienen una inquietud y es que hay conceptos que se empiezan a cruzar como Cloud, IoT, etc. de tal forma que se empieza a pensar en ahorro de costes y se empiezan a llevar cargas a la nube pero sin mucho sentido. Se empiezan con cargas tipo Office 365 y se empieza a pensar en llevar cada vez más cosas. Los CIO cuando tienen que evolucionar el data center se encuentran con mucha falta de argumento para convencer a los directivos de las compañías de que no todo se puede llevar a la nube". Finalmente, Ignacio Arrieta, Commercial Account System Engineer Manager for Iberia de Dell EMC aseguró que "la tecnología para la hibridación del data center está ahí. Ahora es algo que es viable a pesar de que llevamos hablando del cloud desde hace 10 años. Todas las organizaciones de IT se tienen que plantear dónde está la línea de evaluación para focalizar los recursos de IT, en mejorar el engadgement con los clientes y ser más ágil,que es lo que propone el mundo multicloud".

TENDENCIAS

El siguiente apartado pasó por analizar cuáles serían las tendencias en la evolución del data center del futuro. En este

sentido, el portavoz de Dell-EMC cree que "claramente las tendencias van a pasar por el multicloud. Ni siquiera el mundo híbrido. Se trata de cómo alinear la estrategia al multicloud con las personas y los procesos y ahí nos vamos a focalizar las empresas TIC". Para Miguel Rebodero, "existe una labor importante de reeducación a fin de tratar de que las nuevas tecnologías se puedan incorporar con éxito. Otro tema importante es el de las subidas de cargas a la nube, temas concretos de seguridad de algunas compañías, etc. Al final hay que hacer estudios pormenorizados de cada empresa a la hora de subir datos a la nube".

El portavoz de IECISA, por su parte, hizo especial hincapié en los retos que va a afrontar el centro de datos del futuro. En su opinión, "el reto principal de un data center es el de reducir las latencias y el de establecer el consumo energético del data center. También influye la competencia con el mundo cloud y hay que tener en cuenta las diferencias de un cloud público con uno que tu quieras instalar en tus oficinas. No todo es democracia en las TIC. Hay que valorar lo que se sube a la nube porque no todo se puede subir ahí".

En definitiva se trata de tener el control de los datos y, en este aspecto, el centro de datos juega un papel importante. En esta línea argumentativa se posicionó Luis Colino de Microfucus para quien "estamos viendo como el uso masivo de cloud publica está disparando los costes sobre todo porque no se sabe controlar lo que se contrata y si realmente es necesario utilizar determinados servicios. Agilidad, automatización y control son los principales retos que afronta el data center". Finalmente el portavoz de Schneider Electric aseguró que "es cierto que las tendencias nos llevan a situaciones híbridas cada vez más complejas. Todo esto hace que la gestión del data center sea un reto complicado. Al final, hay que focalizar en como se gestiona la parte de software que te ayude a gestionar esa complejidad.

SEGURIDAD

Como en casi toda aplicación, hardware o tendencia tecnológica, la seguridad cobra un papel fundamental en el correcto desarrollo de las TIC. Fue éste, otro de los apartados tratados durante la celebración del desayuno y fue Ramón Rodríguez el encargado de señalar que el de la seguridad "es una de las principales preocupaciones de las empresas en la actualidad. Se trata de establecer estándares, protocolos, etc para garantizar la seguridad. Nosotros enfocamos el problema de la ciberseguridad como un proceso de mejora continua porque creo que una empresa no se tiene que preguntar si va a sufrir un ataque, sino cuándo lo va a sufrir". Para Luis Colina, "en realidad, la seguridad es un conjunto de distintas estrategias. Nosotros estamos intentando ver esa visión holística. Ya no vale el firewall de turno. Hay que tener una política correcta para poder remediar posibles ataques". En la misma línea se situó Manuel Lendinez que afirmó que "tenemos que avanzar en la continuidad del dato. No sólo tiene que estar todo seguro sino que independientemente de donde estés, puedas tener acceso al dato en cualquier momento. No hay que pensar solo en la

Ignacio Arrieta, Commercial Account System Engineer Manager for Iberia de Dell EMC

"Las tendencias van a pasar claramente por multicloud"

Miguel Rebodero, Alliances Manager de Econocom

"Hay que hacer estudios pormenorizados de cada empresa a la hora de subir datos a la nube"

Manuel Lendinez, Business Unit Outsourcing Systems and Cloud Datacenter de IECISA

"Los clientes solicitan más tecnología de centro de datos que nunca"

Luis Colino, Director de Preventa Sur de Europa de Microfocus

"La gestión dinámica del data center es una prioridad para los clientes"

Ramón Rodríguez, Data Centers Solution Architect de Schneider Electric

"Hay muchas tecnologías que se pueden utilizar para mejorar la optimización"

seguridad sino en la continuidad de ese dato, porque ¿qué ocurre si cae un data center?". En opinión de Miguel Rebodero de Econocom, "cuando se habla de ciberataque todo el mundo se piensa en un ataque externo y no piensa en los ataques desde dentro. Por ejemplo: ¿Cómo gestionar el data center para que ciclo de vida lo tenga perfectamente controlado cuando elimino un dato? Hay que establecer mecanismos para tener un control perfecto del data center para saber si tengo vulnerabilidades". Finalmente, el portavoz de Dell-EMC puso el énfasis en que es necesario "detectar y reforzar la ciberseguridad interna. Además en las aplicaciones modernas hay que crear plataformas en las que la seguridad está embebida dentro de las mismas aplicaciones. La gobernanza del dato es fundamental también".

OPTIMIZACIÓN DEL CONSUMO

Es otra de las piedras angulares sobre las que se sustentan los centros de datos modernos. Gozar de un consumo ajustado es una de las necesidades y exigencias de las empresas. En este sentido, Ignacio Arrieta aseguró que "invertimos mucho en I+D para mejorar todos los elementos que van en un data center. Ahora estamos yendo hacia modelos all-flash, que suponen unos ahorros de consumo muy importantes". Por su parte el portavoz de Econocom consideró que "para optimizar hay que conocer muy bien cuál es el uso de las cargas que hace el cliente. De esta forma, analizamos costes, vemos hasta dónde se necesita automatizar, se ofrece formación al personal para que sepa gestionar una cloud privada o un workflow de un entorno virtualizado, etc. Si la gente que lo tiene que explotar no está educada en este nuevo entorno es complicado optimizar el data center". Por su parte, el portavoz de IECISA consideró que la optimización "hay que verla desde el punto de vista físico y desde el punto de vista lógico. Del primero, la tendencia es que en centros de datos más pequeños que son antiguos es complicado optimizarlos pero si empiezas de cero, tienes que ver qué datos o aplicaciones vas a meter dentro a fin de optimizar el espacio, el consumo, etc.".Para Luis Colino de Microfocus, "en el mundo del software se trata de dar al cliente la solución que necesita para que pueda automatizar y orquestar sus datos. Estamos viendo que la gestión dinámica del data center, que antes no se hacía, es una prioridad para los clientes".

NUBE

Finalmente, la nube cobró su protagonismo. Hubo un tiempo que incluso se llegó a afirmar que cloud acabaría con los centros de datos instalados en las empresas. En este sentido, Ramón Rodríguez aseguró que la nube "no acabará con el data center de la empresa. Es más la sensibilidad del dato y la gestión la que nos dirá qué se debe llevar a la nube". El portavoz de Econocom señaló que el data center no desaparecerá "por temas de seguridad y de normativa. Hay otros aspectos importantes que hace que esto no sea posible. Hay una cosa de la que nos olvidamos y es que hay cargas de trabajo que se pueden pasar a la nube y que antes no se planteaba". Finalmente desde Dell-EMC se afirmó que "ya empieza a haber soluciones que permiten tener lo que se encuentra en la nube en el data center del cliente. El mundo va a ser multicloud e híbrido. Hay que hacer una categorización de las cargas que quieres en la nube. El cloud hay que utilizarlo con conciencia sabiendo qué es lo que se lleva".

ECONOCOM

El reto de muchos clientes es afrontar el futuro del data center desde el punto de vista de los cambios tecnológicos, tendencias y necesidades del negocio. Por esta razón, Grupo Econocom ha ido adaptando sus soluciones para ir cubriendo todo el ciclo de vida del data center garantizando su alta disponibilidad, seguridad, actualizaciones automáticas, reducción de tiempo y costes de administración. El objetivo de Econocom es acompañar a los clientes en la transformación y adaptación de su centro de datos para dar respuestas a las demandas de su negocio de forma transparente y no intrusiva.

DELL-EMC

El Data Center se ha convertido en el centro de la transformación digital. Por este motivo, las soluciones integrales para centros de datos de Dell EMC están diseñadas para ayudar a las empresas a responder de forma dinámica al cambio. En 2018 Dell Technologies se ha consolidado como líder mundial en servidores, almacenamiento e infraestructuras hiperconvergentes como soluciones idóneas para el data center del futuro.

MICROFOCUS

Micro Focus le ayuda a gestionar su negocio y transformarlo. Nuestro software proporciona las herramientas críticas que necesita para construir, operar, asegurar y analizar su empresa en un mundo en constante cambio. En este momento, eso significa potenciar su transformación digital con soluciones que abarcan cuatro áreas clave:

· Enterprise DevOps: crear y entregar mejor software más rápido.
· Gestión de TI híbrida: operar con agilidad.
· Seguridad, riesgo y gobierno: asegurar lo que más importa.
· Análisis predictivo: analizar para actuar en tiempo real.

Por diseño, estas soluciones cierran la brecha entre las tecnologías existentes y las emergentes, lo que significa que puede innovar más rápido, con menos riesgo, en la carrera hacia la transformación digital.

SCHNEIDER ELECTRIC

Las nuevas tecnologías y la digitalización están impactando drásticamente en el panorama empresarial a nivel global. El sector Datacenter está directamente implicado en esta transformación, teniendo que adaptarse a este nuevo entorno. La aparición del Edge, sustentado por tecnologías como la inteligencia artificial, realidad aumentada, el blockchain, el IoT y sus aplicaciones va a requerir soluciones de infraestructura distribuida distintas a las que conocemos hasta ahora y perfiles especializados para su operación. Es por ello que cobra especial importancia la utilización de herramientas de gestión capaces de ayudar en la toma de decisiones del día a día e incluso actuar de manera predictiva, anticipándonos al fallo y optimizando los recursos, permitiendo hacer planificación y selección de distintos escenarios participando en la estrategia de negocio. A nivel de eficiencia energética, a través de la propia digitalización de los Datacenters y del análisis de los datos podemos obtener criterios de mejora e incluso comparativas con infraestructuras similares a través de "data lakes" o datos estructurados, obteniendo una ventaja competitiva al reducir el consumo energético. Las tendencias en freecooling, incremento de temperaturas, consolidación IT, hiperconvergencia, alta densidad, nuevos refrigerantes y

IECISA

Informática El Corte Inglés es la consultora tecnológica del Grupo El Corte Inglés. Está especializada en la provisión de soluciones digitales y servicios de valor añadido para la transformación digital de empresas y Administraciones Públicas. Por su trayectoria y amplio conocimiento sectorial, aporta a las organizaciones propuestas integrales de valor con base tecnológica, necesarias para adaptarse a los nuevos modelos de negocio propiciados por la Nube, la movilidad, el Big Data, Internet de las cosas y la seguridad. Su compromiso con la innovación y la calidad han impulsado su proceso de internacionalización, potenciando la actividad global de la compañía.

Los últimos smartphones

El negocio de la telefonía móvil no se detiene y los cambios se suceden a pasos agigantados. Uno de los mejores escaparates para que los fabricantes presenten sus nuevos desarrollos es el Mobile World Congress que recientemente ha cerrado sus puertas y donde este año, entre otros muchos asuntos, se ha hablado de telefonía 5G. Fabricantes como LG de la mano de su V50 ThinQ 5G (que, por cierto, puede adquirirse con una pantalla secundaria como accesorio) y ZTE con su dispositivo Axon10 Pro 5G son una prueba de ello. Quien acudió también a esta cita fue la finlandesa Nokia que ha creado para su nuevo buque insignia, el 9 PureView, un sistema de cinco cámaras de 12 megapíxeles cada una. Asimismo, Xiaomi desveló su última apuesta, el terminal Mi 9. También asistió Sony: a la espera de que aterrice en el mercado el Xperia 1 hemos incluido en este artículo su teléfono Xperia XZ3 que, entre otras bondades, saca el máximo provecho de la tecnología de inteligencia artificial, una tendencia que cada vez tienen más en cuenta los fabricantes.
Como el abanico de precios se ha diversificado bastante, el usuario tiene acceso a una oferta que se adapta a toda clase de bolsillos, con la ventaja añadida de no tener que renunciar a la calidad y el rendimiento que espera cuando adquiere uno de estos terminales. Los más sofisticados y avanzados son el iPhone Xs, el Huawei Mate 20 Pro y el Samsung Galaxy S10, pero el resto de propuestas incluidas en este artículo dejan sensaciones y experiencias de uso muy favorables y a precios más accesibles como es el caso del Asus ZenFone Max Pro (M2), el BQ Aquaris X2 Pro y la nueva familia Motorola moto G7. Entre medias de ambos extremos se sitúa el Honor View20 que propone una cámara frontal incrustada de 25 megapíxeles, otra trasera de 48 megapíxeles y una 3D con inteligencia artificial que ayuda a convertir el terminal en una consola de juegos.

Apple iPhone Xs

En dos tamaños de pantalla, 5,8 y 6,5 pulgadas, integra el primer chip móvil con tecnología de siete nanómetros que destaca por su inteligencia y potencia.

El último lanzamiento de la firma de la manzana está disponible en dos tamaños de pantalla OLED: uno de 5,8 pulgadas y 2.436 x 1.125 de píxeles de resolución para el modelo XS y otro de 6,5 pulgadas y 2.688 x 1.242 píxeles para la versión XS Max, que se convierte en el iPhone con la pantalla más grande comercializada hasta la fecha. Además, ambas son pantallas Super Retina HD compatibles con HDR10 y Dolby Vision, y disponen de un sistema de gestión del color en iOS que ofrece una elevada precisión cromática. La otra diferencia importante entre ambos dispositivos inteligentes es que en el caso del teléfono Xs Max la duración de la batería es algo superior.

La joya tecnológica de Apple incorpora una importante novedad en su procesador A12 Bionic. ¿Cuál es? Se trata del primer procesador móvil con tecnología de siete nanómetros: esto le convierte en la propuesta tecnológica altamente potente e inteligente con un consumo eficiente y un rendimiento sobresaliente. Asimismo, funciona muy rápido y de manera fluida con cada una de las acciones que debe completar; este chip se compone de seis núcleos: dos de alta potencia que se destinan a aquellas situaciones en las que el usuario necesita el máximo rendimiento posible y cuatro para las actividades menos intensivas con un 50% más de eficiencia.

En cuanto a la GPU, lo más sobresaliente es que tiene la capacidad de ir aprendiendo del uso diario que una persona haga del teléfono.

Con Face ID como tecnología de reconocimiento del rostro para iniciar sesión o pagar las compras que se realizan, es resistente al polvo, el agua y las salpicaduras, y su estructura está bañada en acero inoxidable. Funciona con iOS 12 y su parte trasera que es de vidrío facilita una carga inalámbrica más rápida. El soporte doble para tarjetas SIM sólo incluye una ranura para tarjetas física porque el usuario necesita configurar la otra a través de eSIM, una versión virtual, en la línea secundaria del teléfono.

El apartado dedicado a la fotografía deja también importantes mejoras y sensaciones gracias al desarrollo de un motor neural y el procesador ya mencionado. Por ejemplo, se ha conservado el doble sensor de 12 megapíxeles de resolución pero como su tamaño es mayor así puede entrar más luz. De otro lado, el angular es un poco más amplio y posee una apertura de f/1,8). Se ofrece control de la profundidad.

Apple

Teléfono: 900 812 703
Web: www.apple.es
Precio: desde 1.159 €

Asus ZenFone Max Pro (M2)

Toma el testigo del terminal M1 de la firma, ofreciendo un mayor rendimiento, duración de la batería y diseño resistente que mejora su usabilidad.

La taiwanesa Asus ha propuesto para este artículo al sucesor de su teléfono inteligente M1, un modelo completamente renovado que se convierte en el tope de gama de la serie ZenFone Max. Con una pantalla 6,3 pulgadas y 2.280 x 1.080 píxeles de resolución protegida por una capa Corning Gorilla Glass 6 en el frontal –este nivel de resistencia se duplica con respecto a la norma anterior- está decorado con un acabado 'Wave': se trata de un patrón de ondas que cambia al visualizarlo desde el ángulo que se haga. A este respecto, la pantalla brinda una relación de aspecto de 19:9 que sirve para pronunciar la sensación de inmersión en los contenidos visualizados.

Sus creadores le han equipado con un procesador modelo Qualcomm Snapdragon de 14 nanómetros con inteligencia artificial. De hecho, la CPU es hasta un 11 % más rápida que la versión anterior y ofrece hasta un 33 % más de rendimiento gráfico –según indica el fabricante-, lo que significa un mayor grado de realismo y unas capacidades 3D notablemente superiores. La memoria RAM tiene un tamaño de 6 Gb.

La batería también ha sido mejorada y su capacidad escala hasta los 5.000 mAh para que el usuario lo pueda utilizar hasta dos días de forma continuada. Por otro lado, este ZenFone Max Pro (M2) cuenta con un sensor de cámara doble de Sony avanzado y de alta resolución (IMX486) que incluye tecnología de Detección de Escenas por Inteligencia Artificial para proporcionar resultados sensacionales tanto en situaciones de día como de noche.

Mientras tanto, su sistema de autoenfoque por detección de fase (PDAF) y la estabilización electrónica de imagen (EIS) elimina las secuencias movidas y enfocan al instante cualquier tipo de sujeto. La cámara secundaria consigue el efecto bokeh en retratos y realzar al sujeto de forma artística. Es posible elegir entre 13 tipos de escenas diferentes.

También llama la atención la presencia de una bandeja triple que combina dos ranuras SIM (dual SIM/dual standby) con una ranura microSD que permite ampliar el espacio de almacenamiento hasta llegar a los 2 Terabytes de capacidad.

No falta tampoco el soporte para pagos a través de NFC, una opción que poco a poco se va extendiendo cada vez más. Desde el punto de vista del sonido, su altavoz de cinco imanes y amplificador NXP inteligente dejan sensaciones muy buenas por la potencia y el nivel de detalle ofrecidos. Por último, comentar que incluye sensor de huella dactilar y sistema de reconocimiento facial.

Asus

Teléfono: 932 938 154
Web: www.asus.es
Precio: 299 euros

Honor View20

Cuenta con una cámara frontal de 25 megapíxeles, otra trasera de 48 megapíxeles y una 3D con inteligencia artificial para convertirlo una consola de juegos.

El buque insignia de Honor fue presentado recientemente en París, y el usuario puede elegir entre cuatro colores diferentes y dos configuraciones posibles: una que incluye una memoria RAM de 6 Gb y 128 Gb de almacenamiento, y otra de 8 Gb y 256 Gb. Además, viene con el último procesador Kirin 980 IA de 7 nanómetros y NPU Dual con notables mejoras en términos de rendimiento y eficiencia energética. El teléfono View20 cuenta, por otro lado, con una batería de 4.000 mAh de capacidad y un sistema de enfriado líquido que se encarga de disipar el calor para un mejor funcionamiento.

El diseño destaca por una pantalla sin marcos de 6,4 pulgadas y 2.310 x 1.080 píxeles de resolución que integra una cámara frontal de 25 megapíxeles perforada en la propia pantalla. Los ingenieros del teléfono han recurrido, para ello, a un soporte con diseño de amortiguador ya que la cámara se ha dispuesto de tal manera que se encuentra debajo de un agujero transparente de 4,5 mm de grosor elaborado a partir de un proceso de litografía. Hay que destacar, asimismo, la utilización de una tecnología avanzada de nanolitografía para crear una nanotextura invisible en el cuerpo del dispositivo que luce una curvatura 3D con un elegante diseño de arco de 8,1mm de grosor. La combinación de metal y cristal no pasa desapercibida.

La cámara principal del View20 funciona con el sensor Sony IMX586 de 48 pulgadas y gracias a las características ofrecidas por el procesador Kirin 980 -antes mencionado- sus posibilidades se ven favorecidas. Así, por ejemplo, la cámara toma simultáneamente fotos de 48 megapíxeles y superpone los mejores detalles de cada una de ellas para crear la mejor imagen posible; en este caso, el chip Kirin 980 procesa la instantánea aplicando un algoritmo potenciado por inteligencia artificial. El resultado es una captura detallada, detalles en negro optimizados y colores que al ajustarse parecen más vivos.

El fabricante ha apostado, de igual forma, por una cámara 3D que recopila información de las formas de los objetos gracias a señales time-of-flight (TOF) que potencian la sensación de profundidad. Además, es capaz de detectar el cuerpo y capturar el movimiento por lo que el teléfono puede convertirse en un sistema de control de movimiento para consolas de juego. Dicha cámara 3D y su inteligencia artificial llega incluso a identificar hasta 100 tipos de comida y facilitar información calórica de la misma.

Honor

Teléfono: 902 012 420
Web: www.hihonor.es
Precio: desde 549 €

ASLAN 2019 CONGRESS & EXPO

3 & 4 ABRIL MADRID

ENABLING DIGITAL TRANSFORMATION

Líderes en **Innovación IT** para acelerar la Transformación Digital

Security · Cloud · Mobility · Collaboration · Networks

IoT · DataCenter · Analytics · Artificial Intelligence · Big Data

Impulsar la tecnología para acelerar la Transformación de empresas y administraciones: IT managers, partners, service providers y startups tienen la oportunidad de liderar la Transformación Digital aportando su talento y experiencia. Conocer las últimas innovaciones tecnológicas, y cómo transformar las organizaciones, es su gran reto en la nueva era digital y el foco principal del Congreso ASLAN2019.

PALACIO MUNICIPAL DE CONGRESOS MADRID
+2.500 m² +10 Espacios y Salas de Conferencias

+6.000 asistentes procedentes de...

+3.000 ...empresas de toda España

+100 compañías líderes en tecnologías y servicios IT

+150 speakers

GLOBAL SPONSORS

DELL EMC · econocom · eset ENJOY SAFER TECHNOLOGY · Hewlett Packard Enterprise

EVENT SPONSORS

axians · CenturyLink · COMMVAULT · Danysoft · Extreme · KASPERSKY · MICRO FOCUS · SOPHOS · Symantec · INTRACOM · vmware

Inscripción gratuita en **www.congreso.aslan.es**

CELEBRACIÓN SIMULTÁNEA

smart energy CONGRESS

ORGANIZA

@asLAN

Creamos espacios de encuentro y divulgación tecnológica gracias al apoyo de más de 120 empresas asociadas

ZTE Axon10 Pro 5G

El primer teléfono 5G de ZTE integra una pantalla de 6,47 pulgadas, inteligencia artificial y un sistema de triple cámara posterior con gran angular de 125º.

Está previsto que a lo largo del primer semestre de este año desembarque en el mercado europeo el primer smartphone 5G de ZTE. En este sentido, el fabricante ha explicado que sus ingenieros tuvieron que afrontar los retos técnicos inherentes a las innovaciones de esta tecnología como es el caso de la compatibilidad electromagnética, el diseño de la antena, el consumo de energía y la disipación de calor en el proceso de desarrollo del dispositivo. Así, por ejemplo, se empleó un modelo de consumo total de energía mejorado con éxito, lo que supuso la disipación de calor mediante la aplicación de una tecnología de refrigeración líquida y materiales térmicos compuestos de cambio de fase.

Estas características se completan con una solución de arquitectura ajustable para mejorar la señal RF y una solución llamada Smart SAR que reduce la radiación electromagnética de estos dispositivos minimizando el daño en los usuarios.

Desde el punto de vista técnico, sus desarrolladores combinan el procesador Qualcomm Snapdragon 855 y el módem Snapdragon X50 5G para que el usuario disfrute de las bondades de contar con una velocidad más rápida, un alto ancho de banda y una latencia baja. Asimismo, el fabricante hace uso de la tecnología de inteligencia artificial para una experiencia de uso diferente gracias al empleo de una triple cámara trasera, captura de movimiento, reconocimiento facial, ajuste de iluminación de retrato, y aprendizaje del comportamiento del usuario. En relación al apartado de las cámaras, indicar que la frontal ha sido equipada con un sensor de 20 megapíxeles de resolución y la posterior con un triple sensor de 48, 20 y 8 megapíxeles, gran angular de 125º, teleobjetivo y apertura de f/1.8

ZTE Axon10 Pro 5G cuenta, por otro lado, con una memoria RAM de 6 Gb, almacenamiento de 128 Gb ampliable con una tarjeta microSD, y batería de 4.000 mAh de capacidad. Como sistema operativo, funciona a las órdenes de la última versión disponible de Google Android, la 9.0.

En cuanto al diseño, se suma a la tendencia ya generalizada de las pantallas infinitas y perfil de fino grosor (en este caso, ofrece unas dimensiones de 159,2 x 73,4 x 7,9 mm). El tamaño de su pantalla AMOLED alcanza las 6,47 pulgadas y una resolución FHD+ de 2.340 x 1.080 píxeles de resolución. Como sistema de autenticación del terminal, el usuario lo desbloquea con su huella dactilar.

ZTE

Teléfono: 900 828 288
Web: www.zte.com.cn
Precio: no disponible

BQ Aquaris X2 Pro

El terminal más avanzado de BQ incorpora el sistema de carga Quick Charge 4+ y un sistema de doble cámara compatible con Google Lens.

Con 54 modelos acreditados y nueve fabricantes, Android Enterprise Recommended es un programa que Google ha puesto en marcha para reconocer a los mejores smartphones para el ámbito corporativo. A este grupo pertenece el Aquaris X2 Pro, el modelo más avanzado de BQ que ha sido sometido a unos requisitos en cuanto a hardware, software y seguridad. Asimismo, es compatible con Zero Touch, la nueva API de Google que permite a los equipos de IT configurar, desplegar y gestionar los dispositivos en bloque y de forma remota desde una plataforma que se integra con las soluciones de los principales proveedores de EMM (Enterprise Mobility Management). Asimismo, forma parte del programa Google Android One que apuesta por una política de actualizaciones muy estricta dentro del ecosistema Android (se tienen garantizados dos años de actualizaciones y tres años de actualizaciones de seguridad).

A nivel de diseño, este BQ Aquaris X2 Pro combina cristal y metal, y ofrece también una alta resistencia en los desplazamientos gracias a su protección Gorilla Glass. Mientras, su pantalla posee un tamaño de 5,65 pulgadas, resolución FHD+ y Quantum Color, una tecnología para emitir luz de mejor calidad y que logra que los rojos y los verdes resulten más puros. ¿Y a nivel de fotografía? Descubrimos una cámara dual dotada de Google Lens. Se trata de un sistema de reconocimiento basado en los avances de la inteligencia y visión artificial en tiempo real que, por ejemplo, es útil para consultar información sobre aquello que está siendo fotografiado.

En su centro neurálgico, sus desarrolladores han colocado un procesador Qualcomm Snapdragon 660 octa-core con hasta 2,2 GHz y tecnología de 14 nanómetros. Asimismo, hay espacio para una tecnología conocida como Kryo que mejora el rendimiento (más de un 67%) y minimiza el consumo de energía del teléfono (30%). Estos datos porcentuales han sido facilitados por la marca. La batería, que tiene una capacidad de 3.100 mAh, soporta el sistema de carga Quick Charge 4+; así, el usuario puede llegar a cargar su terminal al 50% de su carga en apenas media hora.

Es posible, por otro lado, vivir una experiencia sonora más inmersiva con la reproducción en estéreo que brinda la solución Qualcomm Aqstic y sus dos altavoces. Otros datos de interés son: protección frente al polvo y las salpicaduras, lector de huellas dactilares, tecnología NFC, USB tipo-C DisplayPort, ranura dual nano-SIM y soporte para tarjetas microSD de hasta 256 Gb.

BQ

Teléfono: 91 111 87 00
Web: www.bq.com
Precio: 379,90 euros

Huawei Mate 20 Pro

Las cualidades más destacadas son: una batería de gran capacidad, carga reversible, modo escritorio y triple cámara Leica con inteligencia artificial.

Se trata de un dispositivo tope de gama que aloja una batería grande y de alta densidad de 4.200 mAh, y es compatible con el Huawei SuperCharge de 40 vatios que permite cargar el 70% del teléfono en sólo media hora; en este sentido, la seguridad de dicha tecnología de carga está certificada por TÜV Rheinland. Además, soporta el sistema de carga rápida inalámbrica de 15 vatios de la firma y carga inalámbrica reversible, que hace que el terminal funcione como un banco de energía para los dispositivos que admiten esta clase de carga.

Huawei Mate 20 Pro admite el 4.5G LTE Cat. Estándar 21, pudiendo experimentar velocidades de descarga de hasta 1.4 Gbps. También es compatible con velocidades de conexión Wi-Fi muy rápidas: por ejemplo, y según apunta el fabricantes, imágenes de 2 Gb de tamaño sólo requieren 10 segundos para su descarga. Compatible con el posicionamiento GPS de banda dual (L1 + L5), la tecnología AI GPS Satellite Selection mejora la precisión de posicionamiento en una amplia gama de escenarios.

El dispositivo está basado en el sistema de chip más denso y de mayor rendimiento que ha comercializado Huawei hasta la fecha: el chipset Kirin 980. Fabricado con un proceso avanzado de 7 nanómetros que incorpora una avanzada CPU basada en Cortex-A76 y una GPU Mali-G76, arroja un rendimiento mejorado y una experiencia fluida de usuario.

Mientras, y tomando como referencia los cimientos del sistema de cámara de la serie Huawei P20, el fabricante ha mejorado la serie Huawei Mate 20 añadiendo un importante complemento: una lente ultra gran angular Leica de 16 mm. Esta perspectiva más amplia crea una sensación de amplitud y dota de un efecto tridimensional a las imágenes. Mientras, el nuevo sistema de cámara también admite la distancia macro, que produce imágenes nítidas de objetos situados a tan solo 2,5 cm del objetivo. La lente agregada de ángulo ultra-amplio y la compatibilidad con macros completan el conjunto de funciones de la cámara.

Por último, la funcionalidad Huawei Share 3.0 ofrece una mejora en la interconexión de dispositivos, lo que resulta útil para transferir archivos entre teléfonos inteligentes y ordenadores. Esta solución, propiedad de Huawei, quiere revolucionar la forma en que los usuarios pueden transferir imágenes y vídeos: todo lo que necesitan es un toque para establecer una conexión entre el teléfono inteligente y ordenador para compartir archivos de manera fácil y rápida.

Huawei

Teléfono: 900 483 303
Web: ww.huawei.com/es
Precio: desde 1.049 €

CLOUD
by
arsys

¡SEGUIMOS DANDO LA VUELTA AL CLOUD!

CLOUD HIBRIDO

SERVIDORES DEDICADOS Y CLOUD EN UN ÚNICO PANEL

©2019 Arsys Internet S.L.U. Promoción vigente del 1 de mayo 2019 al 31 de mayo 2019. Consulte condiciones en www.arsys.es/legal

CLOUD

30 DÍAS GRATIS

PRUÉBALO

- PAGO POR USO, SIN INVERSIÓN INICIAL
- FÁCIL Y RÁPIDO, DESPLIEGUE EN MINUTOS
- PROCESADOR INTEL DE ÚLTIMA GENERACIÓN
- ALTO RENDIMIENTO, DISPONIBILIDAD Y FIABILIDAD
- CENTROS DE DATOS EN ESPAÑA, EUROPA Y EEUU
- INNOVACIÓN Y ALTA TECNOLOGÍA A TU ALCANCE

EL MEJOR SERVICIO AL CLIENTE | INNOVACIÓN TECNOLÓGICA | MÁS DE 20 AÑOS DE EXPERIENCIA

www.arsys.es/cloudhibrido | 902115530

arsys

LG V50 ThinQ 5G

El primer smartphone de la coreana LG preparado para la llegada de la telefonía 5G permite contar con una segunda pantalla en forma de funda opcional.

Disfrutar de todo el potencial de la tecnología 5G -tan pronto como esté disponible- es uno de los propósitos que ha llevado a LG a incorporar esta propuesta a su catálogo para 2019. Este LG V50 ThinQ 5G quiere ofrecer al consumidor una experiencia de uso completamente renovada y para ello ha desarrollado una doble pantalla (Dual Screen) como elemento opcional y adicional.

Esta doble pantalla es un accesorio o complemento con el formato de una carcasa que tiene un tamaño de 6,2 pulgadas y tecnología OLED. Idónea para tareas laborales y momentos de ocio, se combina con la pantalla principal del terminal (6,4 pulgadas y 3.120 x 1.440 píxeles de resolución). En este caso, ambas funcionan de forma independiente pero coordinada, de tal manera que, por ejemplo, el usuario puede utilizar una para ver una película mientras que usa la otra para realizar una búsqueda en Internet.

¿Cómo funciona? Al añadir la Dual Screen, aparece en la pantalla de este terminal avanzado una pestañita que, al presionarse, enciende la segunda pantalla o incluso es posible intercambiar el contenido entre ambas. Cuenta además con una funcionalidad de multi-window que divide cada una de ellas a su vez en dos, de tal manera que es posible usar hasta cuatro aplicaciones simultáneamente. De la misma forma, puede colocarse en dos ángulos (uno de 104º y otro de 180º) y no es necesario cargarla aparte del teléfono. En otro orden de cosas, el apartado de audio incluye tecnología DTS:X y Qualcomm aptX y aptX HD para un sonido de mayor calidad con matices más claros y profundos.

El primer dispositivo 5G de LG ha sido equipado con la plataforma Qualcomm Snapdragon 855 que, combinada con el software optimizado de la coreana, le permite brindar una capacidad de procesamiento avanzada. A ello contribuyen su batería de 4.000 mAh y un nuevo sistema de disipación del calor llamado Vapor Chamber. La memoria RAM tiene un tamaño de 6 Gb y la capacidad de almacenamiento (128 Gb) puede ampliarse hasta los 2 Terabytes con una tarjeta microSD.

Entre las funcionalidades disponibles para tomar fotografías y vídeos, destaca 'Video Depth Control' que se ha implementado tanto en la cámara principal como secundaria. Mientras, la tecnología Dual FOV analiza la distancia y profundidad del entorno. Un último detalle de interés: ha superado los estándares militares (MIL-STD 810G) y posee resistencia IP68.

LG

Teléfono: 963 05 05 00
Web: www.lg.com
Precio: no disponible

Nokia 9 PureView

En el apartado fotográfico se desmarca de la competencia apostando por un sistema formado por cinco cámaras de 12 megapíxeles de resolución cada una.

El último teléfono inteligente que se ha sumado al portafolio de Nokia se convierte en el primer dispositivo móvil de su categoría en integrar un sistema de cinco cámaras (está formado por dos sensores de color y tres monocromático) con tecnología ZEISS Optics y 12 megapíxeles de resolución. En concreto, estas cinco cámaras funcionan de manera conjunta para obtener hasta 10 veces la cantidad de luz precisa en comparación con un único sensor de color del mismo tipo, explica el fabricante: de esta manera, puede garantizar instantáneas con rangos dinámicos superiores y con texturas que sobresalen. Para ello, y una vez que cada una de estas cinco cámaras se ajusta automáticamente a las distintas partes de la escena – y son sincronizadas con algoritmos de inteligencia artificial- el disparo se produce a la vez. El resultado es una imagen HDR con un mayor nivel de color, detalle y contraste. Nokia 9 PureView lleva instalado el sistema operativo Android 9, que combina potencia y eficiencia, y como emplea tecnología de inteligencia artificial puede adaptarse a la experiencia que realiza el consumidor de su teléfono para entender sus preferencias y mejorar con el paso del tiempo. En cuanto a la batería, hablamos de una capacidad de 3.320 mAh compatibilidad con el sistema de carga inalámbrica Qi. También provee de una función de carga rápida.

En otro orden de cosas, señalar que el fabricante ha apostado por una configuración técnica que viene encabezada por el chipset Qualcomm Snapdragon 845, una memoria RAM de 6 Gb y una capacidad de almacenamiento de 128 Gb ampliable. ¿Y la pantalla? No tiene marco, emplea tecnología pOLED QHD, cuenta con un tamaño de 5,99 pulgadas y alcanza una resolución 2K. Mientras tanto, y gracias a la tecnología PureDisplay, los colores resultarán más precisos y la legibilidad bajo la luz del sol ve me mejorada. Debajo de esta pantalla, se ha situado el sensor de huellas dactilar como método de autenticación. La estructura del terminal está bañada por una capa de aluminio mecanizado y el cristal Corning Gorilla Glass 5 en la parte frontal y trasera garantiza una mayor resistencia y durabilidad. Cabe destacar, de igual forma, que el smartphone ha sido provisto de una función bautizada con el nombre de 'App Actions': está basada en las rutinas del usuario y le ayuda a hacer las cosas mediante atajos. Su certificación Qualcomm aptX augura una alta calidad del audio al utilizarlo con auriculares y altavoces bluetooth.

Nokia

Teléfono: 91 330 40 00
Web: www.nokia.es
Precio: 599 euros

Samsung Galaxy S10+

Sistema de triple cámara trasera, certificación HDR10+ para la pantalla, sensor de huellas ultrasónico, inteligencia artificial… Así es la última generación Galaxy S.

La multinacional coreana conmemora el lanzamiento de su primer teléfono Galaxy S (hace ahora 10 años) presentando uns nueva línea de terminales premium: la familia Galaxy S10. Está formada por diferentes modelos, uno de ellos su primer smartphone 5G.

Vamos a comenzar por su pantalla Dynamic AMOLED, que tiene una relación de 19:9. Ha recibido las certificaciones HDR10+ y VDE contribuyendo a la calidad de las imágenes que muestra. Además, y justo debajo de esta pantalla, la firma sitúa el primer sensor digital de huellas dactilares ultrasónico. Lo que le hace especial es que no lee una imagen en 2D sino los controles tridimensionales de la propia huella para mejorar la protección del dispositivo ante una suplantación. Existe, asimismo, la posibilidad de utilizar un sistema de autenticación basado en el reconocimiento facial.

El apartado dedicado a la fotografía deja, igualmente, buenas sensaciones. Así, y gracias a su cámara con inteligencia artificial el optimizador de escenas –por ejemplo- reconoce y procesa de forma más precisa un mayor número de escenas gracias a su unidad de procesamiento neural (NPU); mientras, la función 'Sugerencias de composición' realiza recomendaciones automáticas de los encuadres. También es novedad que tanto las cámaras traseras como frontales graban en calidad UHD y que, por primera vez, la trasera da la alternativa de grabar en HDR10+. La lente angular arroja un campo de visión de 123º, similar al ojo humano por lo que para grandes panorámicas es perfecta.

Con soporte para Wi-Fi 6, es compatible con un sistema de carga rápida disponible no sólo por cable, también de forma inalámbrica. Samsung Galaxy S10+ cuenta, por otro lado, con un nuevo software basado en la inteligencia artificial que optimiza automáticamente no sólo la batería, también la CPU, la memoria RAM e incluso la temperatura de acuerdo a cómo se utiliza el teléfono mientras continúa aprendiendo de los hábitos del consumidor. La capacidad de almacenamiento tampoco es un problema. El teléfono que nos han dejado para prueba incluye 128 Gb más una ranura para tarjetas microSD de hasta 512 Mbytes, asunque que sus capacidades oscilan entre los 128 Gb y el terabyte, añadiendo asimismo una ranura microSD de hasta 512 Gb.

A nivel de seguridad, integra el sistema Samsung Knox y almacenamiento seguro mediante hardware que guarda las claves privadas para los servicios móviles con tecnología blockchain.

Samsung

Teléfono: 902 811 030
Web: www.samsung.es
Precio: 1.009 euros

Xiaomi Mi 9

Con un cuerpo de cristal holográfico, posee un sensor de imagen de Sony de 8 megapíxeles y triple cámara con ultra gran angular e inteligencia artificial.

La familia de dispositivos inteligentes Mi de Xiaomi continúa creciendo y el último modelo en incorporarse es el dispositivo Mi 9 con un cuerpo trasero de cristal y formato 'all-curved' para una mayor adaptación en la mano. Como dato curioso, señalar que su diseño está inspirado en el estilo del arquitecto Antonio Gaudí, de ahí que la cubierta cuente con una amplia gama de colores que hace que parezca distinto en cada momento.

En lo que respecta a la pantalla, el fabricante apuesta por un panel Samsung AMOLED de 6,39 pulgadas, 2.340 x 1.080 píxeles de resolución y protección Corning Gorilla Glass 6 para una seguridad superior. Asimismo, la cubierta de la cámara hecha con cristal de zafiro de una sola pieza refuerza la durabilidad y resistencia del dispositivo sobre todo en los desplazamientos. El sensor de huella dactilar está situado debajo de esta pantalla y reduce en un 25% el tiempo de desbloqueo con respecto a la generación anterior.

Xiaomi Mi9 cuenta, en otro orden de cosas, con un procesador Snapdragon 855 fabricado con tecnología de siete nanómetros para brindar un mayor rendimiento y rapidez en las tareas que ejecuta el usuario. Además, su doble tecnología Turbo le permite duplicar la aceleración. ¿Y la batería? Integra un modelo de 3.300 mAh de capacidad, y apuesta por una solución de carga rápida tanto de manera inalámbrica, como por cable. En el caso del cargador por cable de 27 vatios- admite el estándar QC4 + de Qualcomm- es posible que el terminal se cargue al 70% en solo 30 minutos y la autonomía completa en una hora. Mientras, si se emplea la nueva versión de 20 vatios de potencia del cargador inalámbrico Mi Wireless Charging Pad, el Mi 9 estará cargado completamente en una hora y media.

Mi 9 destaca también por su triple cámara con inteligencia artificial, incorporando el último sensor de 48 megapíxeles Sony IMX586 1/2" que combina cuatro píxeles en uno. Hay que añadir, asimismo, una cámara de gran angular de 16 megapíxeles y otra con teleobjetivo de 12 megapíxeles. El gran angular es de 117º. Por su parte, la cámara frontal con modo retrato e inteligencia artificial está provista de un sensor de 20 megapíxeles. Hablando de inteligencia artificial, se ha previsto un botón específico completamente personalizable. Otros datos de interés son: GPS de doble frecuencia y método de pago NFC compatible con Android Pay.

Xiaomi

E-mail: service.es@xiaomi.com
Web: www.mi.com/es
Precio: 449 euros

Sony Xperia XZ3

Luce un diseño de cristal curvado elegante a la par que resistente. Algunas de sus funcionalidades se benefician de las bondades de la inteligencia artificial.

Con un 'diseño infinito' en 3D de cristal curvado, este modelo quiere ofrecer al usuario una experiencia inmersiva. Para ello, ha sido provisto de una pantalla de 6 pulgadas QHD+ HDR OLED que destaca por integrar la tecnología Bravia OLED que el fabricante japonés concede a sus televisores. Esto significa que los negros son más profundos, las tonalidades más brillantes y los niveles de claridad y contraste superiores.

Además, esta pantalla, que alcanza un formato 18:9, proyecta un fino marco de aluminio de 3 mm de grosor mientras que el material Corning Gorilla Glass 5 que se ha empleado proporciona una durabilidad mayor. Su certificación IP65/IP68 corrobora su resistencia al agua y el polvo.

Entre sus funcionalidades, descubrimos una opción llamada 'Side Sense' que destaca por utilizar tecnología de inteligencia artificial y proporcionar un uso más sencillo a las aplicaciones favoritas del usuario. ¿Cómo funciona? Presionando dos veces en cualquier lugar en cualquiera de los dos bordes del terminal, se abre un desplegable con las aplicaciones que más se usan y que se colocan de forma más fácil.

Dicha inteligencia artificial está presente también en la funcionalidad 'Smart launch' que activa la cámara cuando se sujeta el smartphone de forma horizontal para no perder detalle alguno. Además, hay que destacar la tecnología de cámara Sony Motion Eye para grabar vídeos en 4K HDR, así como Super slow motion en Full HD a 960fps.

Xperia XZ3 cuenta con una cámara trasera de 19 megapíxeles y una delantera de 13 megapíxeles, y con la aplicación 3D Creator es posible añadir expresiones faciales como tristeza o felicidad a los escaneos. Desde el punto de vista del rendimiento, incorpora el procesador para móviles Qualcomm Snapdragon 845 y brinda una velocidad máxima de conexión a Internet con 1.2 Gbps. Sus aplicaciones inteligentes de batería como el modo Smart Stamina, STAMINA, Battery Care y la tecnología de carga adaptativa inteligente de Qnovo ayudan a garantizar la vida útil de su batería de 3.300 mAh; esta carga controla el estado de la batería cuando está conectada y ajusta los niveles de rendimiento para garantizar que no se utilice más de lo necesario.

En lo que respecta al audio, Sony quiere que el usuario escuche y disfrute de la música como la creó el artista. Así, ha recurrido a tecnologías de mejora como Hi-Res Audio, DSEE HX y LDAC. Sus altavoces frontales estéreo emplean tecnología S-Force Front Surround y son un 20% más potentes.

Sony

Teléfono: 910 507 396
Web: www.sony.es
Precio: 799 euros

Motorola moto G7 Plus

El fabricante actualiza su serie moto G7, ahora con un rendimiento superior y pantallas de mayor calidad. Hay cuatro modelos, el más avanzado la versión Plus.

Motorola ha lanzado cuatro versiones del teléfono móvil que más ha vendido en su historia, y lo hace adaptándose a las tendencias del momento al incluir mejores cámaras, pantallas de mayor tamaño, velocidades de procesador más rápidas y una capacidad de la batería superior adaptándose, así, a los distintos perfiles de usuario.

El modelo tope de gama es el Moto G7 Plus, que cuenta con una cámara dual de 16 megapíxeles de resolución y estabilización óptica de imagen –reduce el desenfoque a consecuencia de movimientos accidentales o manos temblorosas- e inteligencia artificial (IA). En este sentido, y gracias al software basado en IA, la composición inteligente reconoce posibles mejoras en el marco y genera automáticamente una segunda imagen optimizada. Además, incluye Google Lens.

El fabricante ha rediseñado, por otro lado, su pantalla Max Vision para brindar un rendimiento optimizado. Con un tamaño de 6,2 pulgadas y resolución Full HD+, se suma a la moda del diseño 'noch'. Además, el terminal ha sido protegido con un cristal Corning Gorilla contorneado en 3D y una capa que lo preserva contra el sudor, los derrames accidentales y la lluvia ligera. La batería posee una capacidad de 3.000 mAh y con el cargador TurboPowe de 27 vatios de potencia se puede disfrutar con una carga de 15 minutos de hasta 12 horas de energía, explica la firma.

Otros datos de interés relaciones con el dispositivo son: altavoces estéreo mejorados con tecnología Dolby Audio, lector de huellas dactilares y opción de utilizarlo como dispositivo de pago. El Moto G7 Plus, al igual que la nueva generación de smartphones moto g, viene equipado con Experiencia Moto que hacen más fácil su uso; por ejemplo, el botón de navegación rediseñado reemplaza a los botones de navegación con una sencilla barra en la pantalla.

Por su parte, el terminal moto G7 comparte con la versión Plus algunas características como la pantalla Max Vision Full HD+ de 6,2 con notch de gota, cámara dual de 12 megapíxeles con captura automática de detección de sonrisas y Google Lens. Funciona a las órdenes del procesador de ocho núcleos Qualcomm Snapdragon 632. En el caso del motoG7 Power su batería de 5.000 mAh amplía la autonomía a 60 horas de duración con una única carga. Finalmente, se encuentra el moto G7 play que a pesar de su diseño compacto no renuncia al rendimiento.

Motorola

Teléfono: 91 275 71 64
Web: www.motorola.es
Precio: 299 euros

La **seguridad** se abre paso en la **empresa**

Ciberespionaje, Ransomware, suplantación de identidad,... cada día, los usuarios y las organizaciones han ido viendo cómo los ciberataques han ido en aumento.

Por Manuel Navarro

Paradójicamente, este incremento de los ciberataques ha supuesto una ventaja para la seguridad. Y es que, usuarios y empresas, a base de ataques, han ido tomando conciencia de la necesidad de tomar medidas para proteger equipos, datos y aplicaciones. Faltan todavía muchas cosas en las que avanzar: formación de los usuarios, desmontar falsas creencias o considerar la ciberseguridad como una inversión y no un gasto son sólo algunos de los elementos a mejorar, pero lo cierto es que la política de seguridad por parte de las empresas es algo que está mejorando. A pesar de esta mejoría, la ciberseguridad es uno de los principales elementos para poder llevar a cabo la transformación digital y son múltiples los retos que tiene por delante. Vamos a analizar algunos. En opinión de José María Ochoa, Área Manager de OneseQ (by Alhambra-Eidos) y Co-Director de LAB SEC Blockchain, "el principal reto de seguridad de cualquier compañía es siempre eliminar o minimizar al máximo cualquier brecha de seguridad que pueda afectar a su ecosistema. En muchas organizaciones, a la hora de afrontar la transformación digital, no cuentan con un plan de seguridad que garantice la estabilidad de la compañía, por lo que las consecuencias acaban siendo en algunos casos desastrosas. De ahí que la concienciación en materia de ciberseguridad sea un pilar fundamental en las compañías.

Resulta fundamental que, las compañías que no se encuentren capacitadas para mantener sus infraestructuras seguras, se dejen auditar y asesorar por expertos que puedan hacer un estudio del que, entre otras cuestiones, puedan extraer, como punto de partida, un mapa de riesgos e impacto junto con los activos más valiosos a proteger".

Pero en la era del Big Data, la nube o el IoT, hay un elemento que es clave en lo que se refiere a la ciberseguridad. Ese no es otro que la protección del dato por lo que es cada vez más importante su protección frente a accesos no autorizados o del uso indebido que, de forma inconsciente, puedan hacer los propios empleados de la compañía. En este sentido, Rafael Del Cerro Flores, Presales Security Systems Engineer para el Sur de Europa de Aruba cree que "los principales retos son analizar como se están comportando los propios usuarios en la red para detectar anomalías y posibles usos indebidos, y es necesaria la gestión de la amenaza interna". Por su parte, Daniel Madero, country manager de MobileIron considera que los principales retos del sector de la ciberseguridad se encuentran en "la desaparición del perímetro de la red corporativa. El puesto de trabajo es móvil y los servicios se van a la nube. Ya no existe la visibilidad y el control sobre la red". En definitiva, los principales retos que marcarán las prioridades en ciberseguridad durante los próximos meses son variados. María Campos, VP sales worldwide key account, MSSP y Telcos de Panda Security cree que "por una parte, el incremento de la ingeniería social será uno de los puntos donde hacer foco, dado el elevado número de ataques de phishing que hemos visto durante 2018. Otro reto importante seguirá siendo las contraseñas débiles, con las que aumentan las posibilidades de robos de credenciales. El auge de los dispositivos IoT también cobrarán importancia, ya que la seguridad de estos dispositivos es muy débil y los usuarios no son completamente conscientes de las amenazas que presentan". La portavoz de Panda Security cree además que, la seguridad del Cloud es otro de los grandes retos, ya que la mayoría de las empresas que utilizan estos servicios, confían en que los proveedores de servicios son los responsables únicos de la seguridad, cuando en realidad es responsabilidad de todas las partes implicadas. Esta directiva, con una larga experiencia en el sector añade que también hay que estar atentos a "las amenazas de Inteligencia Artificial, ya que los hackers podrían utilizar esta tecnología para encontrar vulnerabilidades en los sistemas para poder atacarlos e, incluso, podrían llegar a habilitar malwares con IA para que aprendan cómo atacar un ordenador en red".

RIESGOS INNECESARIOS

Una de las características del mundo de la ciberseguridad es que en numerosas ocasiones y, fruto del desconocimiento,

las empresas toman riesgos que son innecesarios. Existen males endémicos, no solo relacionados con riesgos o malas praxis, más bien en relación a la falta de concienciación de la Seguridad a los propios empleados. La compartición de password, accesos no controlados, falta de segmentación en la red y sobre todo visibilidad de todo lo que hay conectado es el principal problema. El problema es que las empresas no pueden defenderse de algo que no conocen, por lo que se vuelve a un punto inicial de dar visibilidad de lo que se tiene para poder aportar las medidas correspondientes. El problema se agrava porque esta visibilidad muchas veces no la puede ofrecer un sistema aislado por sí solo, sino que se deben contar con herramientas abiertas que fomenten la compartición de contexto entre ellas. Para Miguel López, country manager de Barracuda, "uno de los mayores riesgos es considerar que una herramienta de antispam y antimalware perimetral tradicional es una protección suficiente. A día de hoy estas barreras no pueden frenar ataques basados en ingeniería social y robo de credenciales como los ya mencionados BEC y ATO". Pero hay más. Así por ejemplo, Josep Albors, responsable de concienciación e investigación en ESET, afirma que entre los riesgos innecesarios que se toman por parte de las empresas destacan "la conexión de dispositivos IoT que no son monitorizados ni cuentan con unas medidas de seguridad básicas a redes corporativas suponen una puerta de entrada a los atacantes. Asimismo, las malas políticas

Machine Learning frente a amenazas

Aunque los algoritmos de machine learning han existido durante años, constantemente se están descubriendo y aplicando casos de uso adicionales, especialmente cuando se trata de la seguridad de la red y de los datos. Con el paso de los años, la sofisticación de las habilidades y enfoques utilizados por los hackers ha aumentado tanto en severidad como en frecuencia, y los white hats, así como los responsables de TI y seguridad en las empresas, deben emplear todas las herramientas a su alcance para detener la marea de amenazas.

Recientemente, el machine learning ha pasado a formar parte de la vanguardia de los esfuerzos en seguridad de TI, y los investigadores han identificado varias formas exitosas en las que las herramientas de machine learning pueden contribuir a la protección general de las TI.

El machine learning se está aplicando en todos los sectores industriales, permitiendo a las partes interesadas aprender de los datos procesados y utilizar estos resultados de manera que respalde su misión. Un ejemplo lo encontramos en Netflix, que ha utilizado el machine learning durante años para hacer recomendaciones más personalizadas de entretenimiento en tiempo real a los usuarios. Con la ayuda del machine learning, este precioso tiempo se puede recuperar y aprovechar.

Machine learning para la identificación de amenazas: clasificación del tráfico de red

No obstante, uno de los campos más importantes para las herramientas de machine learning está dentro de la seguridad de TI, lo que incluye respaldar los esfuerzos para identificar y detectar las amenazas de red y los datos confidenciales que contiene y a los que se accede a través de ellas.

Como se indica en la definición anterior, el machine learning es capaz de procesar cantidades considerables de datos, destacar patrones dentro de esta información y aprovecharlos para hacer predicciones y comprender.

Machine learning supervisado

Tal y como se indicara en la investigación "Anticipación a la curva: comprensión en profundidad de las amenazas de red a través del machine learning", este nivel de clasificación del tráfico de red aprovecha el machine learning supervisado. En otras palabras, mientras que la herramienta de machine learning es capaz de procesar y extraer información clave de los datos por sí misma, también es guiada en el sentido de que los usuarios humanos la "entrenan" para que sepa cómo procesar los datos que se introducen en el sistema. Este tipo de modelo de machine learning se mejora a través de datos etiquetados por el hombre para una mayor precisión.

Machine learning no supervisado

El machine learning no supervisado también se puede utilizar para ejecutar la detección de amenazas. En este tipo de proceso, los datos sin etiquetar se introducen en la plataforma de machine learning, para luego ser analizados y clasificados mediante la agrupación de datos. El beneficio de este tipo de actividad de machine learning es que necesita menos tiempo y orientación por parte de los usuarios humanos, ya que los datos no necesitan ser etiquetados antes de ser procesados.

Identificación de las características

Nuestros investigadores de seguridad han aprovechado una combinación de machine learning supervisado y no supervisado, o semisupervisado, para demostrar cómo se puede aplicar el proceso a la identificación de amenazas dentro del tráfico de red. El objetivo es procesar cantidades significativas de datos de red no etiquetados para identificar las características clave de las muestras de malware actuales y las posibles relaciones entre ellas.

Los resultados de este estudio han sido esclarecedores. Con el uso de machine learning no solo se ha separado el tráfico legítimo de la red de los flujos de datos maliciosos, sino que también se han podido identificar las amenazas en función de sus características analizadas. Por tanto, el machine learning juega un papel clave en el proceso de agrupar con éxito las amenazas de red. Utilizarlo en las labores de análisis mejora la velocidad con la que se organizan los datos y se obtienen las conclusiones.

José de la Cruz, director técnico de Trend Micro Iberia

El CISO demuestra la importancia que las empresas están empezando a dar a las estrategias de ciberseguridad

de actualización de software y la pobre segmentación de las redes permiten que muchas amenazas sigan afectando a nuestras empresas con gran facilidad".

Pero, probablemente uno de los principales riesgos que corren las empresas españolas sea precisamente la falta de estrategias de seguridad integrales en el contexto de transformación digital que vivimos. Ya no basta con poner una solución puntual frente a un problema o riesgo puntual. Por lo que el desafío de las empresas es aumentar y mejorar el control de todos los endpoints de su red. En este sentido, el director general de Sophos, Rucardo Maté, considera que "la mayoría de los movimientos laterales que realizan los cibercriminales en sus ataques se producen en los endpoints y recurren a técnica antimalware para avanzar por el sistema y aumentar sus privilegios. Es importante contar con medidas de seguridad como la seguridad sincronizada que promovemos desde Sophos que permite compartir la información entre los endpoints y los firewalls para poder detectar y automáticamente aislar un sistema que sea vulnerable a una posible infección antes de que se extienda por todo el sistema".

EL COSTE

Este es otro de los problemas a los que se enfrentan las empresas a la hora de proteger sus datos. Sobre esto, hay que señalar dos factores: el primero de ellos, tiene que ver con que, todavía, muchas compañías consideran la seguridad como un gasto y no como una inversión por lo que en muchas ocasiones se dejan de tomar las medidas necesarias. Y luego está el coste propiamente dicho y éste, si se quiere tener todo realmente protegido, es elevado.

En realidad no debería considerarse el coste de la seguridad ya que es un elemento necesario en la infraestructura tecnológica de una empresa. Ciertamente, cubrir cada ángulo, cada dimensión tecnológica puede no resultar económico... pero ¿cuál es la alternativa?, ¿no hacerlo? Desde Symantec, Ramsés Gallego, Strategist & Evangelist de la compañía, considera "es importante apostar por la priorización, por definir un mapa de inversiones que, lógicamente, protejan primero las superficies mayores de ataque (el puesto de trabajo, la red, la nube, la movilidad) y posteriormente entornos menos habituales, que supongan un riesgo menor. Pero disponer de una protección de principio a fin, holística, completa, sólida, etc. nos parece instrumental para el éxito. Vivimos tiempos de profundidad y expansión tecnológica, con muchos sistemas, muchos entornos, muchas nubes, sí. Pero, a la vez, vivimos tiempos en los que una aproximación de seguridad que comparta servicios comunes, con una visión 'de plataforma', que permita a más de un servicio/producto nutrirse de la inteligencia de amenazas vista en otro entorno es fundamental. Por último, no creo que deba res-

ponder si es caro o barato porque, en nuestra opinión, depende del apetito de riesgo de cada organización".

Ángel Ortiz, Director Regional de McAfee en España cree que "no se trata tanto de una cuestión económica, sino de necesidad. Las inversiones en ciberseguridad deberían estar contempladas en los presupuestos de las organizaciones y nadie mejor que ellas mismas conoce sus necesidades. La realidad es que el panorama de ciberamenazas está en constante evolución y protegerse ya no es una opción. No hacerlo puede exponer gravemente a las empresas a exposición de datos confidenciales, robo de información personal e incluso acceso a sus cuentas bancarias". No obstante, invertir en ciberseguridad no es algo que tenga que ser necesariamente claro. En este sentido, la portavoz de Panda Security considera que "contar con una infraestructura de ciberseguridad no tiene por qué ser necesariamente tan caro como para no poder invertir en ello. Es un error considerar la ciberseguridad de una empresa como un gasto adicional". Por su parte, el portavoz de OneseQ de Alhambra-Eidos, cree que "más que si es caro o barato, yo hablaría en términos de rentabilidad. Es obvio que el volumen de la inversión se determinará por las características de cada organización. No obstante, y, en cualquier caso, es mucho más caro recuperarse de un ciberataque que prevenirlo. Es tan sencillo como preguntarse: ¿cuánto me costaría el parón total de mi compañía durante horas, días, semanas…? Y es que, aunque a veces caemos en el error de creer que una pyme no necesita invertir en este tipo de cuestiones, podríamos decir que es, más bien, al contrario. Su capacidad de recuperación tras un ataque suele ser menor que la de una gran empresa. Es normal y habitual que las compañías no se encuentren capacitadas para mantener sus estructuras seguras, debido a

que la ciberseguridad se encuentra en constante cambio y resulta difícil estar al día y tener capacidad de respuesta. Es por lo que muchas entidades deciden ponerse en manos de compañías proveedoras que puedan ofrecerles soluciones escalables y gestionadas adecuadas a su situación".

Aunque a priori parezca caro, lo cierto es que contar con una infraestructura de seguridad fuerte y robusta puede, a largo plazo, ser la mejor opción para las empresas. Y es que el coste medio de una brecha de seguridad alcanzó los 102.000€ en 2018, que es un 36% superior a la cifra de 2017 según los datos del informe "El estado de la economía de la seguridad TI corporativa en 2018" de Kaspersky Lab. Por ello, Alfonso Ramírez, director general de la compañía asegura que "estos crecientes costes son una preocupación para las empresas inmersas en la transformación digital actual. Por ello, y ante este panorama, las organizaciones se están dando cuenta que deben priorizar el gasto en ciberseguridad para que los proyectos de transformación digital funcionen sin problemas y de forma segura. Esto se puede ver en el crecimiento que los presupuestos de seguridad TI han tenido en 2018. De acuerdo con este mismo informe se prevé que las empresas grandes dediquen casi un tercio de su presupuesto TI (7,5 millones €) a la ciberseguridad. Curiosamente, a pesar de que tradicionalmente se consideraba que las empresas más pequeñas eran las que menos gastaban en seguridad, en los últimos doce meses su presupuesto ha pasado desde los 2 mil € hasta los 3,3 mil €".

En definitiva, el coste puede ser muy elevado si se pretende tener todo controlado, pero lo normal es que éste no sea alto si se establecen los parámetros necesarios. No tomar medidas, sí que supone un coste y es que, como afirma el portavoz de MobileIron, "incumplir la GDPR puede resultar mucho más caro".

> Con el avance de la IA, seremos capaces de automatizar ciertas labores de ciberseguridad sin comprometer el nivel de protección

LA NUBE

Uno de los elementos que están cambiando el mundo de la seguridad es la nube. Ya no se trata de proteger los datos y la infraestructura situada en la propia empresa porque muchos datos ya no se encuentran allí sino en el cloud. En este sentido, aparece uno de los errores más comunes por parte de las empresas a la hora de afrontar su política de seguridad y es que muchas de ellas creen, erróneamente, que la seguridad corre por cuenta del proveedor cuando es el cliente el que es responsable de lo que ocurre con sus datos. Para Sergi de la Torre, CTO de Econocloud de Econocom, "cualquier aplicación requiere que se apliquen políticas de seguridad a múltiples niveles y es necesario conocer de antemano quien será responsable a cada uno de los niveles. Por norma general nuestro proveedor cloud, ya sea Econocloud de Econocom o cualquier otro, gestionará la seguridad física así como la continuidad del servicio, mientras que la gestión de la seguridad a nivel de aplicación, la configuración segura de las comunicaciones, el almacenado seguro de los datos, etc. serán responsabilidad del administrador de la aplicación. Conviene siempre asegurarse y realizar auditorias periódicas para garantizar el correcto cumplimiento".

Cloud, sin embargo, también mejora la seguridad. Y es que, son muchas las aplicaciones de seguridad que corren bajo cloud. En este sentido, Miguel López de Barracuda asegura que "cloud es imprescindible ya que permite dedicar recursos a tareas con mucha mayor efectividad que un planteamiento de seguridad basado en procesamiento local. Un buen ejemplo de ello son los entornos antimalware con Sandbox en los que vemos que el cloud mejora de forma sustancial tanto el nivel de detección y seguridad como la velocidad y escalabilidad de los análisis". Por su parte, Ignacio Franzoni, SME en Fortinet afirma que "Cloud es sinónimo de automatización y de pago por uso (entre otras), por lo que para los desarrolladores de soluciones de seguridad como nosotros cloud es uno de los pilares estratégicos de desarrollo y crecimiento, invertimos en I+D para

adaptar los productos a estos modelos, consiguiendo los mismos beneficios que el cloud proporciona".

En cuanto a cambiar la mentalidad de empresas y usuarios con respecto a quién es el responsable de la seguridad del dato, si el proveedor o el propio usuario, José María Ochoa, de OneseQ de Alhambra-Eidos, considera que "la seguridad es cosa de todos, de la propia organización y de los proveedores con los que cuente la misma. Por tanto, debemos ser conscientes de que este equipo debe existir, debe trabajar conjuntamente y la elección de los miembros externos de este equipo debe de ser la adecuada. Haciendo una buena elección del proveedor Cloud, la organización mejorará la seguridad y la protección de datos, le ayudará al cumplimiento normativo tan importante a día de hoy, contará con planes de recuperación ante desastres y dispondrá de manera continuada de una total flexibilidad ante las necesidades del negocio, evidentemente también en seguridad. Un proveedor Cloud de garantía, dispondrá de servicios acreditados por certificaciones que aseguren la calidad del servicio y permitan al cliente adecuarse a procesos de seguridad de la información y cumplimiento normativo sólo con el hecho de acceder a su nube. Proveedores Cloud con certificaciones como la ISO 27018, ISO 27000, ISO 22301 o ISO 20000 son proveedores con servicios Cloud GDPR

Compliance que van a hacer que sus clientes estén al día en lo relativo a la protección del dato, la seguridad, el cumplimiento normativo y, además, en eficiencia energética". El director técnico de Trend Micro, José de la Cruz también considera de suma importancia conocer quién es el responsable de la seguridad de los datos y aplicaciones alojados en el cloud. En su opinión, "al trabajar con entornos cloud debemos comprender que la responsabilidad de la seguridad es compartida: el proveedor se encarga de la infraestructura y el cliente de proteger sus aplicaciones y datos. En este sentido debemos acotar dicha responsabilidad en el momento de la firma del contrato con el correspondiente proveedor cloud. Asimismo, debemos exigir información acerca de las medidas de seguridad que dicho proveedor tiene implementadas en su infraestructura.Una vez acotada la responsabilidad, deberemos implementar mecanismos para proteger la parte que nos corresponde (la no protegida por el proveedor cloud) de idéntica manera que haríamos en nuestra infraestructura local".

ACTUACIONES A TOMAR

Para enfrentarse de la mejor forma posible al complejo panorama de la seguridad, las empresas deben contar con una solución que resuelva la ecuación de manera sencilla, innovadora y altamente efectiva. Un sistema de seguridad por capas que cubra los diferentes componentes de sus sistemas de TI: correo, red, navegación web, puestos de trabajo, wifi, dispositivos móviles y aplicaciones. Pero no solo eso, sino que debido a la complejidad de los ataques de hoy en día es más que conveniente que estas soluciones sean capaces de hablar entre sí, compartiendo información sobre cualquier incidente de seguridad, para conseguir que su fiabilidad aumente. En este sentido, Ricardo Maté de Sophos considera que "el puesto de trabajo seguirá siendo siempre atractivo para el cibercrimen y, con una solución como Intercept X de Sophos, capaz de detener el malware de día cero, los ataques sigilosos y las variantes exploit desconocidas, e incluye funcionalidades avanzadas antiransomware que permiten detectar ataques desconocidos previos en cuestión de segundos, minimizaremos los riesgos. Y otro factor importante y que más vale no perder de vista es el correcto cumplimiento con el GDPR. En cuestión de seguridad, los datos son un riesgo, no un activo y no solo hay que tener cuidado con lo que almacenamos y dónde lo almacenamos, sino también hemos de poner medidas para que, en caso de que nuestra información se pierda o sea sustraída, no pueda ser utilizada".

Por otra parte, en estos momentos existe un incremento de los datos críticos en servicios SaaS e IaaS, es decir, que están situados fuera del perímetro de la empre-

sa. Ha cambiado totalmente la forma de trabajar, el lugar de residencia de los datos y la forma de acceder a los mismos. Y, sin embargo, los presupuestos de seguridad continúan enfocados en soluciones de seguridad Perimetral principalmente, las cuales son inefectivas en este nuevo entorno en el que nos movemos. Por todo ello, se debe buscar un nuevo paradigma de protección de la información. Se debe de apostar por soluciones que redefinan un nuevo perímetro de seguridad alrededor de los datos que tenemos hoy, alrededor de la nube. Por ello, Samuel Bonete, country manager de Netskope cree que "esas soluciones pueden ir orientadas en dos líneas. Por un lado el Gobierno de los datos en SaaS, ya sea este SaaS regulado (O365, G-Suite, Salesforce, etc) o no regulado (aplicaciones cloud que los empleados utilizan sin estar aprobadas ni gobernadas por los departamentos de IT). Por otro lado, es también importante el gobierno de la información y revisión continúa de configuraciones en IaaS. Estamos hablando monitorizar de forma continua la postura de seguridad de nuestra infraestructura IaaS (Cloud Security Posture Manage-ment) así como de tener control sobre los datos que tenemos albergados en IaaS y como éstos son trasegados entre los diferentes proveedores de cloud pública. Por tanto, podemos hablar de la importancia creciente de controlar tanto los entornos SaaS, bien sea aplicaciones reguladas como

Prevenir ataques

Todas aquellas acciones que ayuden a minimizar los riesgos de sufrir ataques cibernéticos son esenciales en las organizaciones. Existen multitud de medidas que pueden emplearse por parte de las empresas. A continuación, enumeramos algunas de las medidas de las cuales no debería prescindir ninguna empresa:

Contraseñas

Cambiar siempre las contraseñas predeterminadas, crear contraseñas sólidas y únicas para cada una de las cuentas de los empleados y renovarlas al menos una vez al año para mantener segura la información personal.

Protección avanzada en los puestos de usuario

Los antivirus tradicionales no son efectivos frente a nuevos ataques y/o desconocidos. Se deben implantar nuevas medidas basadas en contexto y comportamiento.

Autentificación Multifactorial

Utilizar la autenticación multifactorial siempre que sea posible, además de contraseñas seguras, para confirmar la identidad al iniciar sesión en las cuentas.

Cortafuegos

Utilizar un cortafuegos para bloquear el acceso no autorizado a equipos y dispositivos

Actualizaciones

Asegurarse de actualizar los sistemas operativos, navegador y demás software con parches de seguridad para minimizar las amenazas de virus y malware.

VPN

Limitar la actividad a través del Wi-Fi público y utilizar software que crean conexiones seguras a través de Internet, como una Red Privada Virtual (VPN), para conectarse de forma segura desde cualquier lugar.

Navegación segura

Practicar la navegación y las compras de forma segura, comprobando que la dirección del sitio comienza con "https" en lugar de solo "http".

Privacidad

Habilitar la configuración de privacidad y aumentar la configuración de seguridad predeterminada del software que se utiliza.

Discreción

Ser selectivos con la información personal que se comparte, ya que de no hacerlo podría ser utilizada por los hackers para adivinar contraseñas e inicios de sesión.

Software pirata

No descargar software pirata, ya que no solo es ilegal, sino que casi siempre incluye algún tipo de malware.

Copia de seguridad

Realizar una copia de seguridad de los datos, ya sea en un disco duro externo o en la nube, ya que es la forma más fácil de recuperarse de un ataque

María Campos,
VP sales worldwide key account, MSSP y Telcos de Panda Security

Office 365 o AWS, bien sea aplicaciones no autorizadas por el departamento de TI, como los entornos IaaS (AWS, Azure, GCP)".

EL PAPEL DE LA IA

Una de las herramientas que parece que en los próximos años va a tener una especial relevancia en el mundo de la ciberseguridad es el de la inteligencia artificial. Gracias a ella, es de prever que se puedan atajar numerosos ataques antes de que incluso lleguen a producirse. Como afirma el country manager de MobileIron, "la inteligencia artificial lo que va a proporcionar es añadir capacidad contextual a los sistemas de seguridad, lo que redunda en una mejora de la seguridad implementada".

La inteligencia artificial ha llegado para quedarse y la realidad es que los fabricantes ya tienen en el mercado soluciones que empiezan a explorar las ventajas de esta tecnología. Los sistemas más innovadores están implantando ya en la actualidad sistemas basados en IA/ML para detectar los patrones de conducta de las infraestructuras y poder así alertar/adaptar cuando se identifican patrones de comportamiento anómalos. Estos sistemas nos permitirán identificar rápidamente los puntos que merecen de nuestra atención para así corregir de manera ágil y segura. En este aspecto, Sergi de la Torre, CTO de Econocloud de Econocom asegura que "la inteligencia artificial es más fiable cuanta más información dispone. Es por este motivo por el que el campo de la seguridad es uno de los entornos más aptos para este tipo de tecnologías, debido a la ingente cantidad de información que recolectan los sistemas SIEM y todos los sensores desplegados. Estas tecnologías son un gran valor de futuro para la seguridad". Por su parte, María Campos de Panda Security cree que "la IA puede ayudar a detectar, así como analizar ciberamenazas rápidamente de cara a evitar incidentes. En esta línea, la IA ayudará a localizar más rápidamente aquellos parámetros que sobresalgan los patrones normales, aquellos que pueden ocultar un potencial ataque. Además, el aprendizaje automático posibilitará la identificación de posibles vulnerabilidades del ecosistema tecnológico de una organización, especialmente aquellos más sensibles como el correo o los dispositivos móviles. Con el avance de la IA, seremos capaces de automatizar ciertas labores de ciberseguridad sin comprometer el nivel de protección, de tal manera que los activos humanos puedan dedicarse a tareas más complejas".

EL ROL DEL CISO

El CISO demuestra la importancia que las empresas están empezando a dar a las estrategias de ciberseguridad. Buena prueba de ello es que se trata de un cargo de reciente crea-

ción. Las empresas, sobre todo las grandes cuentas, empezaron a priorizar la necesidad de tener a una persona que se encargará de forma exclusiva de la ciberseguridad. Asi que, ¿cuál es el papel que debe jugar esta figira en el engranaje de las organizaciones? Para José María Ochoa, Área Manager de OneseQ de Alhambra-Eidos, "el CISO es una figura que cada vez tiene más fuerza en las medianas y grandes organizaciones (quizá en estas últimas). Seamos realistas, el papel que el CISO hace en una gran corporación, es el papel que hace el responsable IT en una pequeña organización. Lo que pasa que la dedicación, la puesta en marcha y el conocimiento de la seguridad a aplicar en su compañía va a ser menor que la que puede aportar un CISO. Sea como fuere, ambos deben mantener la seguridad de la compañía y es básico que estén alineados con la estrategia de la compañía y que la Dirección de la empresa le dote de las herramientas necesarias para llevar a cabo su plan de seguridad. Uno de los primeros pasos que se está dando es la formación del personal dedicado a la ciberseguridad, sea o no el CISO. Programas formativos que ayudan a dar grandes pasos hacia un plan de garantías que permita minimizar las amenazas, conocer cómo se suceden los ataques y saber dónde están las brechas". Por su parte, Antonio Martínez Algora, responsable técnico de Stormshield afirma que "el CISO es un actor clave para garantizar la continuidad de negocio ya que no sólo conoce la tecnología sino también el negocio, igual que otros directivos de máximo nivel".

LOS RIESGOS DE IOT

IoT es una realidad, pero todavía va a tener mucha más importancia cuando la tecnología 5G y el Edge Computing estén funcionando a pleno rendimiento. Entonces, posiblemente se oirá "Houston, tenemos un problema" y es que, muchos de los dispositivos y sensores que se fabricaron hace años, se hicieron sin tener en cuenta la seguridad. Tal es así que en la mayoría de los casos no tienen ninguna medida de seguridad. Esto es algo que no ocurre con los nuevos dispositivos, pero ¿qué sucede con los antiguos? El portavoz de ESET no tiene ninguna duda: "La inseguridad de los dispositivos IoT es una de las principales amenazas debido a que se están conectando a redes corporativas y sirven como puerta de entrada a los ataques de los ciberdelincuentes. Se deben segmentar adecuadamente las redes e instalar medidas eficientes para, en caso de que se vean afectados estos dispositivos, aislarlos del resto de la red".

Ya existen varios ejemplos de los últimos años de que algunos ataques han sido originados por dispositivos de este tipo. En muchos casos estos equipos no han sido concebidos con el mantra "security-by-design" y por tanto pueden representar un problema. Por eso el portavoz de Aruba cree que, "es importante que las soluciones de tipo NAC permitan aportar solución a dicha conexión. No se puede negar ni vetar que existen en la red, por lo que se deben aportar las medidas necesarias para garantizar la conexión, primero identificando qué se está conectando a la red mediante el perfilado; y luego asignándole roles de acceso según dicho perfilado. Estas políticas de seguridad deben ser adaptadas al tipo de dispositivo IoT conectado: ¿Tiene sentido que un sensor de Temperatura envíe varios gigabits de tráfico cada hora? Ahí está la importancia de la segmentación y perfilado".

Finalmente, Ramsés Gallego de Symantec considera que "cuando, como sociedad, decidimos que conectar sistemas industriales a la red Ethernet de las compañías y, de allí, a Internet, no consideramos los problemas que puede acarrear tener sistemas complejos en la misma topología que por donde viajan nuestros datos. Además, esos sistemas industriales, que fueron diseñados de manera que fueran funcionales pero con nulas medidas de seguridad, suponen la superficie de ataque más extensa que hayamos conocido hasta ahora. Por ello, desde Symantec pensamos que considerar el entorno industrial, esa 'Internet de TODAS las Cosas' como un elemento más es fundamental. A veces no se puede desplegar nada 'tradicional' en ese sistema pero sí se puede reforzar la seguridad para garantizar que la plataforma únicamente hace aquello para lo que fue diseñada, con tráfico entrante o saliente pero controlado".

La entrevista al experto

Daniel Madero,
country manager de MobileIron

¿Qué objetivos se ha marcado MobileIron para lo que resta de año?
Ayudar a nuestros clientes a seguir innovando en todo lo relativo al puesto de trabajo móvil, y aprovechar nuevos servicios Cloud sin poner en riesgo la seguridad de la información.

Los últimos resultados de la compañía a nivel global (4Q) han sido excelentes. ¿Cuál es la situación en España de la compañía?
Muy buena; toda la región de EMEA, España inclusive, ha cerrado un año con buenos resultados.

¿Qué es lo que más le solicitan los clientes?
Gestión y seguridad para el puesto de trabajo móvil y servicios en la nube. Hay mucho interés por las nuevas posibilidades que ofrece Google con Android 8 para el puesto de trabajo. Por otra parte, para los servicios en la nube se requiere un control de acceso seguro y eficaz desde el móvil, sin uso de contraseñas. Existe además una creciente toma de conciencia de los riesgos asociados con posibles ataques al dispositivo móvil por parte de ciber-delincuentes, para lo que se necesita una solución de detección integrada con remediación local.

La seguridad móvil se está convirtiendo en un mercado en el que cada vez hay un mayor número de propuestas, ¿qué le hace a MobileIron diferente de su competencia?
MobileIron está dedicado íntegramente a la gestión y seguridad del puesto de trabajo móvil y servicios en la nube. Este enfoque nos permite un nivel de especialización importante y resulta especialmente relevante, dado que los mecanismos de seguridad del puesto de trabajo móvil son diferentes a los tradicionales del puesto de trabajo fijo en redes corporativas. MobileIron ofrece una plataforma completa para dar seguridad al nuevo entorno del puesto de trabajo sin la existencia del perímetro tradicional. Este modelo se fundamenta en tres pilares: 1) Gestión Unificada del Puesto de Trabajo (UEM), 2) Control Contextual de Acceso a los Servicios Cloud y 3) Protección a la Información en el Dispositivo, con una única aplicación integrada de MDM y MTD

La movilidad empresarial es una realidad. ¿Prestan las empresas suficiente atención a la seguridad en dispositivos móviles?
Las empresas han avanzado de forma poco homogénea en su trayectoria de transformación del puesto de trabajo. Existe todavía una curva de aprendizaje; algunos clientes han hecho importantes avances y aprovechan al máximo las posibilidades de innovación y productividad que ofrece el puesto de trabajo moderno. Por el contrario, otros tienen aún la asignatura pendiente de iniciar este proceso, incumpliendo directamente con la nueva regulación de protección de datos, GDPR. En

cuanto un dispositivo móvil tiene acceso a un recurso corporativo como el directorio activo o el correo electrónico, resulta imprescindible gestionar ese dispositivo con EMM/UEM para cumplir con los requerimientos de control de información de contactos personales que exige GDPR.

Los ataques a entornos móviles crecen exponencialmente, ¿cómo puede gestionar una empresa el binomio movilidad-seguridad móvil?

Lo puede gestionar con una solución integrada MDM+MTD, es decir, la gestión del dispositivo móvil reforzado con una solución de detección y prevención de ataques. MobileIron ofrece la única solución realmente integrada del mercado, que: 1) no requiere la instalación ni la activación de una aplicación de MTD independiente y 2) la aplicación única MDM+MTD puede remediar en local, sin depender de conexión a la red, ante cualquier ataque detectado.

Los entornos multicloud, poco a poco, se van imponiendo. ¿Qué riesgos amenazan a las compañías? ¿Qué propone MobileIron en este sentido?

El mayor riesgo es que la empresa pierda el control de la información en la nube. Los móviles acceden a través de APP's, que a su vez guardan los datos en el dispositivo. La solución pasa por un control contextual de acceso a las Cloud, es decir, que no solo verifique la identidad del usuario sino que también tenga en cuenta la postura del dispositivo. MobileIron no solo ofrece este control de acceso contextual a la nube, sino que además proporciona una experiencia de Seamless Single Sign-On (SSSO) al usuario, aprovechando los mecanismos de seguridad del propio móvil gestionado para eliminar el uso de contraseñas.

En muchos casos, las empresas (sobre todo pymes) consideran que la seguridad Cloud es labor exclusiva del proveedor, ¿cómo se convence a una empresa de que no es así?

Se les explica que las App's sincronizan la información de la Cloud en el dispositivo, y que si este no es seguro la información está en riesgo. Esto es así porque una app no gestionada puede copiar la información a otras apps y/o nubes sin que la empresa tenga visibilidad y/o control alguno al respecto.

Por ejemplo, Office 365 es susceptible de ser atacada y, en general, las compañías no ponen medidas para securizarlo, ¿qué proponen desde MobileIron?

Los proveedores de servicios Cloud invierten mucho dinero en la seguridad de sus instalaciones. Es responsabilidad de la empresa controlar el acceso de sus usuarios a sus servicios, para que únicamente los usuarios autorizados con dispositivos gestionados y aplicaciones seguras puedan acceder sin que se pierda la información. Llevamos el móvil a todas partes; si está gestionado por la empresa, podrá utilizarse como método seguro de autentificación a los servicios. Eliminamos de esta forma el uso de incómodas contraseñas que, por otra parte, representan el eslabón más débil en la cadena de seguridad.

¿Es el usuario el principal factor de riesgo de una compañía?

Lo es si la empresa no ha puesto una capa de gestión que imponga políticas de seguridad a los dispositivos que el propio usuario dispone para acceder a la información de la empresa.

¿Cuáles cree que van a ser las tendencias en seguridad en el corto-medio plazo?

Pienso que en el corto-medio plazo la tendencia será implantar seguridad en un entorno sin perímetro. Esto pasa por mover la seguridad al dispositivo y el control de acceso a la Cloud, dando por hecho que el usuario estará conectado a redes no seguras y necesitará verificar con mayor intensidad en todo momento la ubicación de su terminal.

"Estudiar en las praderas con buen tiempo no tiene precio"

¿A qué se dedica la parte principal del presupuesto de TI de la empresa?
La parte más importante de nuestro presupuesto se destina a servicios contratados.

¿En qué área se está invirtiendo más?
La inversión más importante del 2018 se ha dedicado a la actualización del equipamiento de seguridad, en concreto, a los firewalls.

¿Qué proyecto es del que está más satisfecha?
La reestructuración del equipo de TI. Cuando llegué a la UAM, la distribución de los puestos de trabajo de Tecnologías estaba muy desordenada. Tras dos años recabando expectativas y, acto seguido, de negociaciones, conseguí que se aprobara el organigrama actual con el que funcionamos ahora.

Si le pusieran todos los beneficios de la empresa a cargo del departamento de TI, ¿qué le gustaría implementar?
Difícil cuestión pues siempre hay puntos que se pueden mejorar. Desde mi punto de vista, un deseo que no requeriría grandes presupuestos, pero sí mucha dedicación por parte de la comunidad, sería el reenfoque hacia la tecnología en la forma de hacer las cosas, el cambio cultural.

¿La seguridad es un problema?
La seguridad no la considero un problema, sino más bien un proceso que requiere constante atención. Mantener actualizadas las políticas y evaluar periódicamente los riesgos, es una labor constante que no se puede descuidar.

¿Se puede trabajar desde casa?
En lo que se refiere a medios tecnológicos, si se puede. Pero no es habitual asistir virtualmente a las reuniones. La presencia física, salvo causas de fuerza mayor, sigue siendo imprescindible.

Bajo ningún concepto en su móvil puede faltar….
La agenda de contactos.

¿Cuál es la herramienta que realmente le cambió la vida?
El smartphone.

¿Harto de solucionar los problemas tecnológicos de la familia y amigos? ¿Qué le suelen pedir?
La mayor parte de mis amigos proceden del ámbito tecnológico, así que no necesitan ayuda en este campo. Y respecto a la familia, intento que mis hijos busquen las soluciones por sus propios medios. Al fin y al cabo, para ellos la informática es algo básico.

¿Qué es eso de la transformación digital? ¿Slogan o necesidad?
Una tendencia de la sociedad que nos hace la vida más cómoda.

¿Lo del I+D+i, es una leyenda urbana?
En absoluto, de hecho, es una obligación para la universidad.

¿En la nube u on-premise?
Ambos bien encajados.

¿Las ingenierías son el futuro?
Sí, pero compartiendo espacio con otras disciplinas. Las ingenierías siempre han de estar buscando como mejorar la sociedad.

¿Dan más problemas los alumnos o los sistemas tecnológicos de la Universidad?
Bueno, digamos que los problemas de los sistemas tecnológicos, antes o después se acaban resolviendo. Podemos dejarlo ahí.

¿Campus virtual o campus real?
Pues al igual que los entornos, cada cosa tiene sus ventajas. El campus virtual facilita enormemente la comunicación entre docentes y estudiantes en cualquier momento, pero visto la demanda en primavera, estudiar en las praderas cuando hace buen tiempo, no tiene precio. Más ahora que disponen de cobertura WiFi.

María José García Rodríguez

Directora de Tecnologías de la Información. UAM.

Fecha de nacimiento: 11 de marzo de 1967
Estado Civil: Casada
Hijos: 2
Deportes que practica: Pilates
Hobbies: Me encanta la jardinería, en especial los bonsáis
Estudios: Licenciada en C.C. Físicas por la UCM y Executive Master en Sistemas de Información por el IE
Personas a su cargo: 64
Antigüedad en la empresa: desde junio del 2012
Trabajos anteriores: Directora de soporte en Unitronics, y anteriormente, formé parte como socia de una pequeña consultora

Pirelli se apunta al Low-Code de la mano de Appian

Pirelli es una compañía líder en fabricación de neumáticos de alta gama y rendimiento que, gracias a su larga experiencia en el sector, su compromiso con la excelencia durante el desarrollo y su gran red de ventas, ha sido capaz de alcanzar una posición de liderazgo mundial.

La compañía concibe calidad y rendimiento como dos máximas ineludibles en la creación de negocio y esto es algo que extrapola también a su departamento de IT. Por eso, durante años ha reivindicado el uso de las tecnologías más sofisticadas para garantizar la eficiencia y eficacia en la organización y la calidad y fiabilidad superior de todos sus productos.

Como ejemplo de esta tradición de innovación, Pirelli fue la primera empresa en Italia en implementar el software de planificación de recursos empresariales (ERP) SAP R / 3 en 1994, y ha dedicado desde entonces una gran cantidad de presupuesto al Business Intelligence. Con esta misma filosofía de renovación, Pirelli puso en marcha una ambiciosa revisión de la infraestructura IT de la compañía para garantizar que los sistemas que respaldan el negocio fueran lo más proactivos y modernos posible. El objetivo era evolucionar sus sistemas IT para crear una arquitectura segura y fiable que facilitara el acceso a la información por parte de los trabajadores, en lugar de una arquitectura tradicional, mucho menos accesible, que podía generar brechas de información y costosos retrasos en materia de tiempo.

LOW-CODE: LA SOLUCIÓN PERSONALIZABLE

La revisión tecnológica de Pirelli llevó a la compañía a concluir que lo que necesitaba era una plataforma de software de Gestión Avanzada de Procesos de Negocios. Es decir, en palabras de los profanos, una solución que facilitara la gestión de datos empresariales, la movilidad y la colaboración. No se trataba por tanto de reinventarse desde cero, si no de adaptar su esencia. La compañía evaluó a muchos de los principales proveedores de este tipo de tecnología, y finalmente eligió a Appian como la plataforma más avanzada y fácil de usar del mercado. Además de por funciones como la capacidad de arrastrar y soltar elementos, el diseño Low-Code de Appian contaba a su favor con un sistema de procesamiento integrado, la posibilidad de acceder a análisis, informes, eventos, y otras tantas capacidades de gestión de contenido. Sin olvidar la simplificación en materia de tiempo y de codificación que ofrece su intuitiva interfaz.

Como resultado de su colaboración mutua, Pirelli cuenta ya con una extensa lista de desarrollos basados en la plataforma de Appian, que tocan diversos aspectos de los procesos de negocio de la organización. Estas creaciones abarcan desde procesos de ventas y diseño de productos hasta facturación, administración de sistemas, compras, control de calidad, seguridad e impacto ambiental.

La aportación más importante para Pirelli ha sido una aplicación para mejorar el proceso de gestión de moldes. La solución de Appian (Mold Management) aceleró la administración y ejecución de las solicitudes de fabricantes de automóviles de nuevos tipos de llantas, o cambios en los modelos de llantas existentes. Además, Appian ha asumido la entrada y enrutamiento de estas solicitudes y garantiza la finalización y la entrega de las tareas de trabajo relacionadas.

La segunda implementación más destacada tiene en su origen la integración con el sistema SAP ERP de la compañía. Bajo el nombre de "Decomplexity", esta solución se encarga de vincular las especificaciones del proyecto en el sistema ERP con los procesos comerciales que se llevan a cabo en varios departamentos de la empresa. De este modo, al facilitarse que los proceso transcurran de forma más fluida y transparente, Appian consigue optimizar el flujo del proceso, las colaboraciones, las aprobaciones,

etc., y garantiza la precisión y la coherencia de los datos subyacentes. Y lo que es más importante, cuando surgen excepciones a los procesos estándar, Appian puede afrontarlas, activando alertas para las partes involucradas y permitiendo una rápida colaboración para resolver los problemas que surjan. Entre las aplicaciones implementadas destacan las de Gestión de desarrollo y producción para analizar averías relacionadas con la maquinaria de fábrica, la gestión y seguimiento de nuevos materiales y su rentabilidad, o el monitoreo y gestión de la homologación de neumáticos nuevos. También destacan las de Gestión de proveedores y facturación al cliente:o las de Gestión de seguridad y garantía de calidad con soluciones en salud, seguridad y medio ambiente, recopilando datos y analizando tanto incidentes como datos sobre la práctica de Responsabilidad Social Corporativa, para eliminar condiciones de riesgo.

Como resultado de todo este proceso de modernización, Pirelli ha experimentado mejoras significativas en materia de eficiencia y eficacia. La aplicación Mold Management, por ejemplo, ha acelerado la velocidad de respuesta de la compañía a los cambios solicitados por el cliente, mejorando así la experiencia de atención al cliente y la calidad de los productos finales, al mismo tiempo que ha reducido el trabajo previo requerido, debido a la inconsistencia de datos, procesos y comunicación del cliente. Tanto las aplicaciones Mold Management como Decomplexity han incrementado la estructura y la visibilidad de la administración y supuesto una mejora significativa en comparación con lo que anteriormente eran procesos humanos ad-hoc.

Miguel A. González Serrano,
Director en Appian Spain

Tres razones para apostar por la nube

Fue en 2011 cuando las ventas de música digital superaron a las ventas de discos físicos por primera vez. Actualmente, los ingresos derivados de la venta de iPhones y el iPads representan el 72% de los ingresos totales de Apple y, sin embargo, ninguno de los artículos podía adquirirse hace apenas diez años. O, por poner otro ejemplo, cada 4 minutos se descargan ilegalmente unas 694.000 canciones. La nube (la llamada tecnología cloud) se ha convertido en una realidad tanto para las personas como para las empresas de todo el mundo. Tanto es así, que es difícil creer que solo exista desde el año 2000.

Cuando se trata de tecnología, dudo que otra palabra haya creado tanta confusión y controversia como esta.Como sabemos, estamos viviendo momentos en los que los tiempos van a una velocidad exponencial. Con 31 billones de búsquedas en Google cada mes, 600 tweets por segundo y un estimado de 4 exabytes (4.0×10^19) de información única generada este año, no podemos permitirnos no adoptar y abrazar la nube.¿Por qué es importante la administración de la red en la nube?

Hay que tener en cuenta que la administración de la red en el cloud es simplemente eso, una red informática que se administra en la nube. Por lo tanto, es dependiente de Internet y es especialmente beneficioso para las empresas con múltiples ubicaciones y que buscan expandirse con el tiempo. Después de haber dedicado un tiempo a investigar la administración de la red en la nube, los beneficios son obvios. Estas son las áreas que creo que proporcionan más valor:

FACILIDAD DE IMPLEMENTACIÓN

Las redes diseñadas en la nube facilitan la gestión. Con los diseños administrados en la nube no hay necesidad de implementar controladores en cada sitio. La nube proporciona acceso remoto para controlar toda la red, independientemente de dónde se encuentre el personal de TI.

Las implementaciones sin contacto permiten que el personal no técnico ni especialista conecte el dispositivo a la red de una manera sencilla, el cual se instalará y se configurará automáticamente. En mi opinión, esto es uno de los mayores beneficios de las redes en la nube; que es especialmente importante para las empresas con pocos recursos humanos especializados en TI.

Otro beneficio de las WLAN basadas en la nube es la cantidad de puntos de acceso (AP) que la nube puede manejar. Cuando se trata de expandir la infraestructura de red o de configurar una nueva ubicación, las soluciones administradas en la nube pueden respaldar a la empresa con un punto de acceso único, en una sola ubicación, pero también admite manejar múltiples accesos desde cientos de AP. La cantidad de puntos de acceso es ilimitada. Esto significa que las re-

des en la nube brindan una escalabilidad superior sin la necesidad de comprar controladores de hardware adicionales.

CENTRALIZADO

La WLAN gestionada en la nube se adapta fácilmente a cada organización, desde una pequeña empresa en una única sede pero con expectativas de expandirse, a un negocio más grande ubicada en lugares geográficamente dispersos.

Como los puntos de acceso administrados por la nube pueden autoconfigurarse a través de la misma, los empleados que no son del departamento de TI solo necesitan conectarlos y encenderlos para que los administradores puedan realizar provisión, monitoreo y diagnóstico desde una ubicación remota.

COSTE TOTAL DE PROPIEDAD

Tanto si se trata de una empresa grande o pequeña con personal mínimo en los departamentos de TI, los sistemas basados en la nube permiten que todos utilicen las mismas funcionalidades y herramientas.

En una arquitectura WLAN gestionada en la nube, las organizaciones no tienen que comprar controladores físicos e implementarlos en cada sitio. La "nube" mencionada aquí funciona como un controlador virtual y todos los puntos de acceso inalámbricos distribuidos se conectan a ella a través de Internet. La nube ofrece aprovisionamiento remoto, monitoreo y resolución de problemas en cada punto de acceso. Es por ello que los servicios WLAN administrados en la nube, como Zyxel Nebula, son soluciones eficientes que brindan más flexibilidad y accesibilidad para cumplir con los presupuestos más ajustados y maximizan el retorno de la inversión. Además, no hay que olvidar que gracias a la nube se pueden manejar otros asuntos de manera sencilla, como las copias de seguridad de datos, el almacenamiento, o los sistemas de redundancia, entre otros.

Gonzalo Echeverría, Country Manager Iberia en ZYXEL Communications

La digitalización de las empresas: el futuro de las redes

La multitud de puntos de contacto con el cliente, actualmente, obliga a las empresas a prestar una asistencia extra. ¿Cómo se desarrolla un entorno integrado, que no solo asiste a los clientes sino que también revierte ahorros en costes, mejoras en la eficiencia y que esté preparado para los cambios del futuro?

Son muchas las empresas que han ido impulsando sus iniciativas digitales para no perder competitividad.

El papel de estos avances ha sido vital para hacer frente a la demanda cada vez más diversificada que consumidores y partners imponen a las empresas. La agilidad de éstas es vital para adaptarse al cambio y para acelerar el desarrollo de nuevos servicios o productos. La relación entre las compañías con sus clientes y partners, que cambia constantemente, está actuando como impulsor del desarrollo de nuevas tecnologías. A medida que la demanda se extiende hacia la omnicanalidad, cada punto de contacto debe contar de una atención al cliente con redes integradas, robustas y flexibles.

La forma en que los consumidores utilizan la tecnología y las redes que la sostienen también ha cambiado. El espacio móvil ha copado, por supuesto, la mayor y más fascinante evolución. La penetración de estos dispositivos no ha dejado de crecer año tras año, aumentando también el número de usuarios cuyo foco de contacto con la red es su dispositivo móvil. La explosión de los servicios de entretenimiento online ha traído, también, la necesidad de mejorar el rendimiento de la red de forma continua. El consumo de vídeos no ha dejado de subir exponencialmente. Según un estudio de Fetch, hasta un tercio de los consumidores ven contenidos en vídeos todos los días. De todas formas, las empresas no pueden desatender la necesidad de crear un mayor rango de contenido.

Es fundamental que la integración de las redes permita a estos consumidores moverse ágilmente de dispositivo a dispositivo y de red a red.

Sin lugar a duda, las empresas que impulsen esta movilidad ganarán en fidelidad y, consecuentemente, en ventas, ya que el uso de sus redes se convierte en una experiencia menos dificultosa.

REDES MÁS ÁGILES

El cambio profundo que están sufriendo los hábitos de consumo, y cómo éste se manifiesta en el acceso a las redes digitales, subirán un peldaño más con la transición al 5G. La red 5G, no sólo será más rápida, sino que sobre todo cambiará en profundidad el desarrollo de las infraestructuras de red y el uso de éstas para proveer servicios al usuario.

Los contenidos y experiencias relevantes y personalizados son actualmente el pilar de las relaciones entre marcas y consumidores. El trasfondo de esta relación son unas redes rápidas y flexibles. Buscando transformar la forma de proveer servicios a través del móvil al consumidor, las empresas están invirtiendo en infraestructuras de red descentralizadas que se apoyarán en la incipiente red 5G.

Ampliar el ancho de banda móvil y el consumo de vídeo son dos vectores claves de la transición al 5G. Sumados al Internet de las Cosas y sus altísimos requisitos de rendimiento a la red, forman la trinidad de factores que impulsarán los beneficios del 5G para las empresas, cuando comience su despliegue.

En el estudio La Digitalización de Todo, EY explora lo que traerá esta nueva situación para las empresas: "Es fundamental que las compañías se centren en proveer un modelo de gestión omnicanal ágil y suave. Esto requerirá una estrategia que incorpore constantemente la última tecnología y una filosofía de ensayo y error. Es fundamental una estrategia de mejora, lanzar nuevos canales digitales e iteraciones y cambios basados en el feedback del cliente." Pasar de una red centralizada y jerárquica a una descentralizada, buscando poder ofrecer servicios de datos on-demand localizados, es uno de los pilares de lo que hará el 5G. Cada vez más empresas virtualizarán sus

redes para poder entregar los servicios rápidos y localizados que sus clientes demandarán.

MADUREZ DIGITAL

La reacción de las empresas a este enorme cambio en la forma de crear servicios y productos digitales consiste en fijar la madurez digital como meta estratégica.

Su hoja de ruta incluye una mayor agilidad en las infraestructuras de red, así como la estrategia para expandir y mejorar las mismas. Unas redes optimizadas, integradas y adaptadas al cambio disfrutarán de la base sólida sobre la que construir su cartera de servicios y productos.

La naturaleza móvil de los consumidores y partners de hoy en día también implica que las redes deben flexibilizarse, hasta el punto en que puedan ofrecer servicios y productos personalizados.

El 5G trae consigo la promesa de un nuevo escalón del rendimiento de la red, que facilitará un nivel inédito de innovación del que todas las empresas pueden tomar parte, si su red está a la altura de sus ambiciones.

Key takeaways:

- Las redes tienen que evolucionar rápidamente hacia la virtualización y la descentralización para ofrecer productos y servicios ricos en datos.
- 5G transformará la forma en que se distribuye la red a cada cliente y partner.
- Con más velocidad y accesos descentralizados, podrán crearse servicios personalizados.
- La expansión continua del acceso a datos móviles hará que las redes se centren en el acceso primario desde el móvil.
- La digitalización de las empresas no frena su ritmo, y los negocios pueden aprovechar las nuevas redes que este cambio traerá como un activo de desarrollo de servicios.

Miquel Rodrigo, Director de Ventas y Jefe del Service Management de Claranet

IRENE ACEDO – DCG SALES EXECUTIVE DIRECTOR, LENOVO EMEA

"Queremos ser el líder en supercomputación"

La apuesta por convertirse en la empresa que lidere el centro de datos es esencial para la estrategia de Lenovo. Para hablar de ello, entrevistamos a Irene Acedo

¿Cuáles son los objetivos de Lenovo en el área de DCG (Data Center Group) para este año?
Nuestro objetivo de cara a 2020 es estar en el top 3 de fabricantes de centros de datos, y convertirnos en el número 1 a nivel mundial en supercomputación, acelerando así el ritmo de innovación de nuestro negocio de data center para nuestros clientes. Ya hemos conseguido la tercera posición en España y Europa, y obviamente nuestro objetivo a largo plazo es liderar el mercado y convertirnos en el proveedor más fiable del mercado. Llevamos creciendo siete trimestres seguidos, y queremos seguir en esa línea, hasta alcanzar el liderazgo como lo hemos conseguido en el área de PC y en la de supercomputación.

¿En qué tecnologías se van a enfocar?
Queremos liderar el mercado, tanto en servidores como en almacenamiento y networking. Estamos haciendo foco en el mercado de HPC, en el de almacenamiento con nuestro nuevo acuerdo con Netapp y en el de hiperconvergencia, a través de alianzas con partners como Nutanix, VMware y Microsoft. Además, estamos poniendo mucho foco en SAP Hana, e impulsando soluciones cloud a través de acuerdos con arquitecturas certificadas de Suse o Red Hat, Microsoft yVMWare.

Una compañía tradicionalmente de hardware, ¿qué elementos añadidos ofrecen a las empresas?
Nuestro objetivo es ofrecer a nuestros clientes las soluciones más fiables del mercado. Consideramos esencial ofrecer las soluciones que más tranquilidad ofrezcan al cliente, no ofrecer las soluciones más económicas, porque un fallo en estos sistemas sale mucho más caro que la propia infraestructura. En Lenovo ofrecemos soluciones innovadoras cada vez más eficientes y con un mayor control sobre la operación de la cadena de suministro. Estamos continuamente invirtiendo en personas y tecnología por lo que hemos logrado crear un portfolio de data center muy amplio, que abarca desde servidores, almacenamiento, networking hasta soluciones de infraestructura definidas por software, soluciones de hiperconvergencia y soluciones de HPC. Además, ofrecemos productos y servicios completamente paquetizados gracias a nuestras alianzas con partners a nivel mundial.

Están poniendo especial énfasis en la IA, ¿cuál es su propuesta?
Con nuestro negocio existente de Data Center, estamos en una transición: de la tecnología tradicional a tecnología basada en la nube y soluciones equipadas que están definidas por software o por Inteligencia Artificial. En un futuro cercano nuestro objetivo es crear productos que ofrezcan servicios específicos compatibles con la nube, como por ejemplo nuestro asistente inteligente. Estos dispositivos se diseñarán para resolver los puntos débiles de nuestros clientes, y les facilitarán a su vez la gestión y mantenimiento de sus infraestructuras de almacenamiento y servidores. Llevamos tiempo inmersos en la construcción de un modelo de futuro donde todos los dispositivos inteligentes podrán conectarse a la nube y ponerse en marcha a través de la inteligencia artificial. Gracias al nuevo portfolio de productos y a nuestra estructura organizacional revitalizada, el negocio de Data Center Group de Lenovo tiene las piezas adecuadas en cuanto a rentabilidad por su inversión en el centro de datos software-defined, Inteligencia Artificial y HPC.

Otra de sus grandes apuestas pasa por el Centro de Datos, ¿cómo ve este mercado? ¿qué papel están jugando?
El mercado de data center en la actualidad está liderado por las infraestructuras hiperconvergentes, que han mejorado enormemente nuestras operaciones de centro de datos en términos de rentabilidad, protección de datos, escalabilidad y eficiencia de datos. Nuestras soluciones de hiperconvergencia integran el cómputo, el almacenamiento, las comunicaciones y el software necesario para ayudar a nuestros clientes a implantar de una manera simple y rápida este tipo de soluciones. Tenemos appliances para todos los segmentos y sectores, ofreciendo una arquitectura innovadora y escalable con respecto a otras alternativas del mercado.

¿Qué aporta Lenovo al cloud?
El modelo híbrido, que ofrece lo mejor del mundo de las nubes pública y privada, es la mejor solución para alcanzar y superar sus objetivos empresariales. Quizá el beneficio más importante que obtengan sean las tecnologías innovadoras integradoras del "cómo y cuándo quieras", una capacidad clave en el panorama cambiante de las tecnologías emergentes y capacidades digitales. El modelo híbrido también permite a los negocios elegir las cargas de trabajo adecuadas para su entorno, así como las que dependen de las necesidades de las empresas y las nuevas tecnologías. También ayuda a las empresas a lograr éxitos digitales y abre las puertas hacia una hiperescalabilidad, la cual es crucial para cumplir con las demandas del mundo digital en el que vivimos. Desde Lenovo llevamos apostando por este modelo varios años.

Firmaron un acuerdo con NetApp, ¿cómo valoran ese acuerdo?
El acuerdo con Netapp nos ha permitido seguir creciendo, como avalan los resultados que estamos obteniendo, y por tanto ha sido muy positivo. Esta alianza nos va a dar muchas más oportunidades y nos va a permitir ofrecer a nuestros clientes un servicio mejorado acompañado de soluciones líderes en el mercado.

Los viejos luditas nunca mueren

Por Miquel Barceló

Ha sido terrible. He presenciado un fenómeno desesperante y trágico, una amenaza directa al futuro de la humanidad: una máquina ha vencido a un ser humano.

Ocurrió el otro día cuando un atlético joven no logró llegar a tiempo a la parada del autobús. El vehículo rodado, la máquina, corrió más que el humano...

Recordé apesadumbrado cuando, hace ya unos 22 años, Deep Blue ganó a Garry Kasparov en su enfrentamiento a seis partidas de ajedrez. Los viejos luditas nunca mueren, y de nuevo se temió que "la máquina venza o sustituya al hombre", resucitando viejos esquemas de la más tradicional ciencia ficción.

No hay para tanto.

Sabemos hace tiempo que las máquinas pueden ser más fuertes o más rápidas que los seres humanos, que el más sencillo de los coches (o un simple patinete eléctrico...) es capaz de correr mucho más deprisa que el mismísimo Usain Bolt. Que la calculadora de nuestro smartphone hace los cálculos con mayor rapidez, seguridad y exactitud que nosotros mismos usando las tradicionales herramientas asociadas al lápiz y al papel... Eso ya no nos quita el sueño. ¿Por qué debería preocuparnos que, desde hace ya décadas, las máquinas también nos venzan jugando al ajedrez, que la calculadora digital sea mejor que nosotros al hacer cálculos o que un vehículo a motor nos venza en cualquier carrera?

Se supone (sólo se supone...) que el ajedrez tiene algo que ver con la inteligencia. Entrados ya en el siglo XXI, nos preocupa que las máquinas, que sabemos más rápidas y fuertes, también puedan ser (o parecer) más inteligentes que nosotros.

En los últimos años, a pesar de las viejas referencias como Deep Blue, se habla (y mucho, tal vez demasiado...) de la inteligencia artificial. Parece la gran panacea para todo y, me temo, se están asociando con "inteligencia artificial" muchas actividades de la más simple informática o, si quieren, algorítmica clásica. A veces me convenzo que "inteligencia artificial" se usa como un elemento más de marketing en la sociedad de consumo que hemos creado.

Es cierto que John McCarthy, en la conferencia de Darmouth, reunida en Hannover (New Hampshire, EEUU) en verano de 1956, creó uno de los nombres con más marketing de la tecnología: "Inteligencia artificial". Y eso era en un momento en que poco se sospechaba de la inteligencia de chimpancés o delfines y del altísimo nivel de compartición de nuestro ADN humano con el de dichos animales. La única inteligencia de referencia en 1956 parecía ser la de los seres humanos. Inteligencia artificial no era más que un reto: las máquinas nos llegarán a superar.

¿Y qué? En realidad las máquinas, Deep Blue y cualquier ordenador o smartphone incluidos, suelen servir sólo para pocas cosas. Son, al menos hasta hoy, muy poco versátiles. Carecen de la maravillosa adaptabilidad del ser humano quién, por cierto, si de verdad es inteligente, nunca se pone en el trance de competir con las máquinas. Simplemente las fabrica como un elemento que le puede resultar de ayuda en determinados casos.

Yo mismo, que no soy Kasparov, perdería al ajedrez con Deep Blue al igual que pierdo con Fritz 8. Pero ya me gustaría a mí ver a Deep Blue conduciendo un coche o, simplemente, haciendo una tortilla de patatas. El ya desaparecido Marvin Minsky, otro de los padres fundadores del proyecto de investigación en "inteligencia artificial", se defendía, a finales de los años ochenta, del ataque de Roger Penrose (La nueva mente del emperador, 1989) con las ideas expuestas en su La sociedad de la mente (1986) centrada en la interacción de diversos agentes inteligentes. Tal vez esa colaboración de diversos (una verdadera infinidad...) agentes inteligentes especializados logre construir en su conjunto una inteligencia artificial a imagen de la humana pero estoy seguro de que falta mucho (siglos tal vez) para ello.

Incluso a pesar de los cantos de sirena del consumismo rampante y su uso de la etiqueta "inteligencia artificial" como si ya tuviéramos ese resultado al alcance de la mano.

Aunque, los viejos luditas lo saben, todo llegará... Hoy, jugar al ajedrez contra una máquina es condenarse a una derrota segura...

¿Cómo serán tus experiencias en Nexica?

The Cloud Experience:

Cloud pública, privada o híbrida,
en tu CPD o en el nuestro

NEXICA
C/ Cardenal Marcelo Spínola, 4, 2ª planta, 28016 Madrid
C/ Acer, 30-32, 1º 4ª, 08038 Barcelona
Contacta con nosotros: www.nexica.com | **902 202 223**

nexica | econocom