COMPARATIVA - - - >

Portátiles híbridos

www.revistabyte.es Marzo 2017 • Nº 247 • 5,75 euros

byte TI

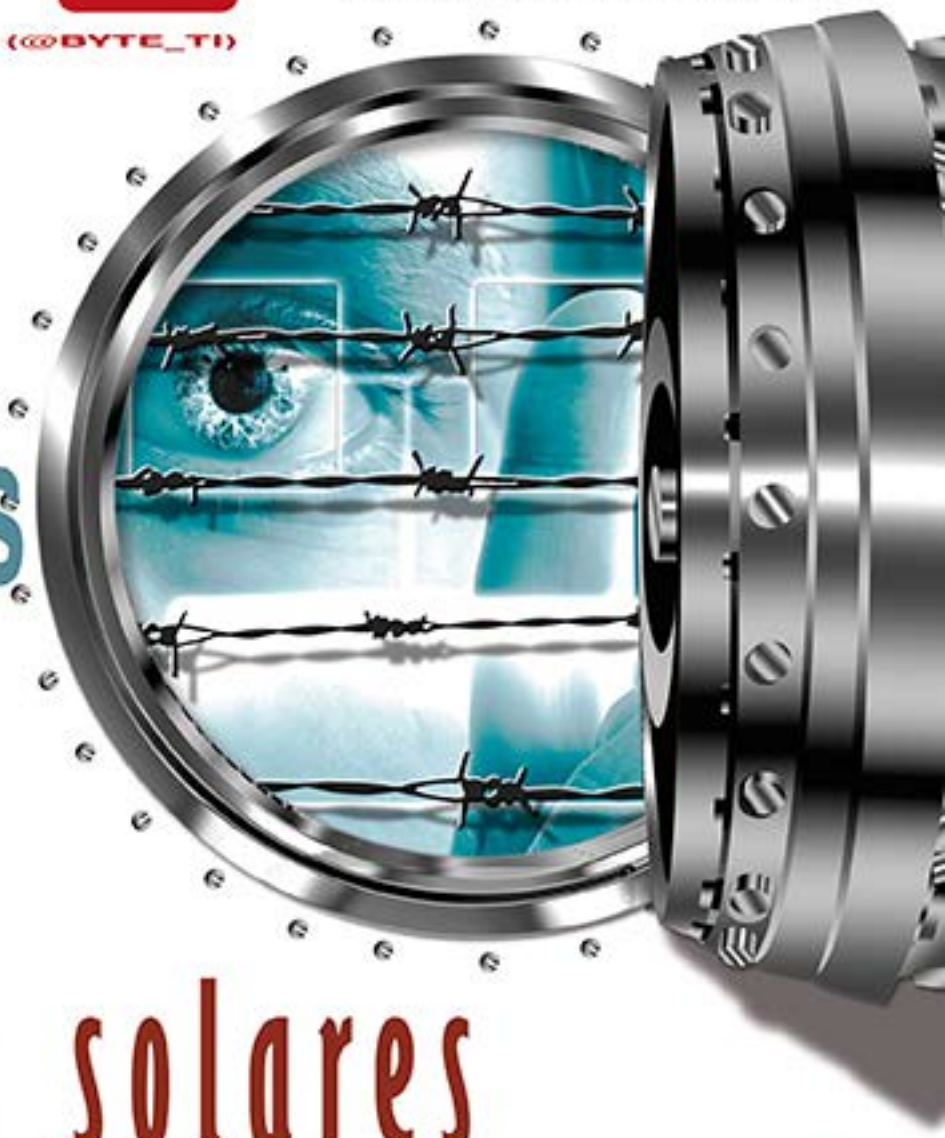
Síguenos en twitter: (@BYTE_TI)

ANÁLISIS

- Sophos Intercept X
- Schneider Electric Galaxy VX

Defenderse de los ciberataques

- Retos de la ciberseguridad
- Las mayores brechas
- Riesgos empresariales



Tormentas solares y continuidad de negocio

Todo sobre los datalakes

m k m PUBLICACIONES

Javier López Sáez

Disfrute de todo el placer de la velocidad

FUJITSU

Almacenamiento ETERNUS AF de FUJITSU

Flash es sinónimo de velocidad: aproximadamente 500 veces mejor tiempo de respuesta que el disco duro tradicional, con una gestión más eficiente del espacio, y una drástica reducción del consumo energético. Proporciona mayor densidad y es, además, una tecnología respetuosa con el medioambiente.

Descubra más en: www.fujitsu.com/es

shaping tomorrow with you

Basado en tecnología Intel®

intel XEON inside

El nuevo GPRD (Regulación General de Protección de Datos), que entrará en vigor a principios de 2018 en toda Europa, ayudará a las empresas a hacer frente al ciberdelito. El nuevo GPRD establece importantes multas y sanciones (que pueden alcanzar hasta el 4% de los ingresos totales de una compañía) con un claro efecto disuasorio para el ciberdelincuente.

La ciberseguridad, el reto de este siglo

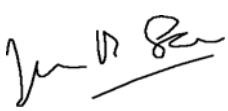
La seguridad es el común denominador imprescindible para aplicar con éxito la tecnología, cualquier producto, aplicación o desarrollo que resuelva una problemática, si no garantiza la seguridad, no es recomendable de ser utilizado.

El 70% de las grandes corporaciones de EE. UU y Europa se enfrentarán a ataques cibernéticos en 2019. En 2016, las instituciones comunitarias experimentaron en sus servidores un aumento del 20 % en ciberataques respecto año anterior. En el último Estudio sobre la Cibercriminalidad en España, elaborado por la Secretaría de Estado de Seguridad, se destaca que, sólo durante el año pasado, se realizaron un total de 60.154 hechos delictivos en Internet, de los cuales el 67,9% se corresponde a fraudes informáticos (estafas) y el 16,8% a amenazas y coacciones. Este tipo de delitos dejó en 2015 un total de 46.860 víctimas de la ciberdelicuencia en nuestro país.

Las cifras causan escalofríos. Pero el problema no ha hecho más que empezar. Ya todo está en Internet. El peligro, -que lo es- no solo está en que nos ataquen y manipulen los datos, sino que se bloqueen y, sobre todo, que se hagan desaparecer. ¿Se imagina alguien que no se pueda recuperar la información, por ejemplo, que almacena en sus servidores un gran banco? ¿Qué ocurriría si, por un ataque, se paraliza el sistema informático que regula todos los vuelos en Europa o Estados Unidos? ¿Y si nos dejan sin comunicaciones (tanto de voz como de datos) durante una semana? ¿Y si concurren estos tres escenarios descritos a la vez?

Porque esto, no nos engañemos, puede pasar, y con menos dificultades de las que podamos imaginar. Por mucho que digan, no estamos preparados para un desastre como el descrito. Según expertos en la materia, las sospechas de manipulación en los resultados de las elecciones norteamericanas y holandesas, no son descabelladas.

O lo prevenimos, o podemos llegar a caer en un caos de consecuencias imprevisibles.



Juan Manuel Sáez. **Director**

Sumario

MARZO 2017

EN PORTADA

Ciberseguridad contra el cibercrimen

34

N.º 247 • 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, JR. Jofre, 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
ERLON

WebMaster
NEXICA
www.nexica.es

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

PUBLICIDAD
Directora comercial: Isabel Gallego
(igallego@mkm-pi.com)
Tel.: 91 632 38 27
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

MARZO de 2017
Printed in Spain

EDITA
Publicaciones Informáticas MKM

8 NOVEDADES

44 COMPARATIVA

TENDENCIAS 60

ESTE MES
RECOMENDAMOS

HPE amplía su portfolio NFV

HPE ha anunciado actualizaciones de su portfolio de virtualización de funciones de red NFV, ofreciendo a los proveedores de telecomunicación (CSPs) acceso a nuevas soluciones y herramientas para acelerar su implantación, así como nuevas soluciones virtualizadas para ofrecer servicios novedosos y personalizados. Estos incluyen:

- **HPE NFV System 1.4 –** una actualización del paquete de soluciones preintegradas NFV de HPE, que soporta y permite elegir entre Red Hat OpenStack Platform y HPE Helion OpenStack Carrier Grade 4.0, integrando el controlador de HPE OpenSDN basado en OpenDaylight.
- **HPE VNF Onboarding Factory Service –** un nuevo programa que permite a CSPs acelerar el proceso de instalación e integración de funciones de red virtualizadas (NFV).
- **HPE Virtual Headend Manager –** una nueva solución de virtualización para gestionar el despliegue de contenido IPTV para mejorar la experiencia del cliente y abrir potenciales nuevas oportunidades de ingresos.

- **HPE Virtualized NonStop para la gestión de datos de los suscriptores –** una nueva solución para gestionar datos de suscriptores (SDM), optimizada para tener una alta sensibilidad a los fallos, disponibilidad y escalabilidad para crear nuevos servicios personalizados que sean más rápidos y económicos.

"A medida que las operadoras de telecomunicaciones se transforman en Proveedores de Servicios Digitales, una de nuestras mayores prioridades es establecer una red sólida y plataformas de servicios flexibles," comenta David Sliter, Vicepresidente y General Manager de Soluciones para Empresas de Comunicación en HPE.

Canon revoluciona la impresión de papel continuo

Canon ha presentado la nueva Océ ProStream, la siguiente generación en tecnologías de impresión en color sobre papel continuo. ProStream combina las mejores características de la tecnología Canon de alto rendimiento con las últimas innovaciones para conseguir que la inyección de tinta en alta velocidad llegue a nuevas cotas de calidad de color y versatilidad de soportes. Así creamos nuevas oportunidades de negocio para los proveedores de servicios de impresión (PSPs) al mejorar sus posibilidades para entregar trabajos de gran valor añadido como campañas de correo directo, materiales de marketing variados, catálogos personalizados, especificaciones y libros.

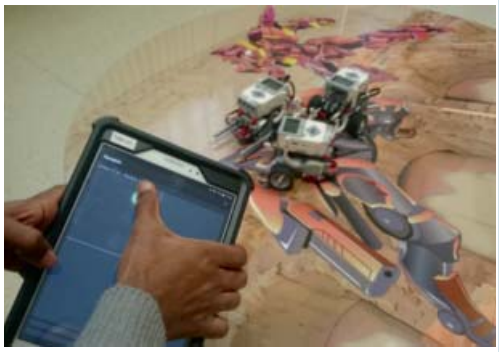
Christian Unterberger, Chief Marketing Officer y Executive Vice President Production Printing Products de Océ comentó: "ProStream constituye la pieza lógica a añadir a la gama existente de soluciones de inyección de tinta sobre papel continuo de Canon".

Gracias a un ancho de impresión de 540 mm y a una velocidad máxima de 80 metros por minuto, Océ ProStream ofrece una productividad líder en su segmento de hasta 35 millones de páginas A4 al mes. Su gran calidad de impresión se consigue al incorporar unos nuevos cabezales de alta definición de 1200 ppp (Océ DigiDot) que son capaces de producir imágenes muy definidas.

MotivaTICs

El Programa MotivaTICs, de Informática El Corte Inglés, Samsung y Ayuntamiento de Barcelona, liderado por la Plataforma de Educación social Martí-Codolar (Salesians Sant Jordi), consigue que de los 30 alumnos participantes, 69% hayan retornado al sistema reglado de educación y el 19% se incorporen al mercado laboral. MotivaTICs ha conseguido desarrollar un proyecto de acción social con dos objetivos: analizar el impacto de las TIC como eje motivador para la adquisición de competencias en jóvenes en situación de riesgo social y analizar el impacto que las competencias digitales tienen en la facilitación de la inserción laboral.

Precisamente para dar a conocer esta iniciativa Salesians Sant Jordi estará presente en The Youth Mobile Festival dentro del stand de Yomo en Fira de Montjuïc, el festival del móvil para la juventud en el marco del Mobile World Congress que se celebrará del 27 de febrero al 2 de marzo. Los visitantes del stand podrán realizar batallas de robots y experimentos domóticos durante la jornada y los ganadores recibirán un premio fabricado por una impresora 3D.



Además explicarán las diferentes disciplinas STEM (science, technology, engineering y mathematics) que trabajan en la plataforma social a través de las vertientes domótica y robótica.

La evolución del proyecto "MotivaTICs" para el presente curso ha dado paso a un formato educativo reglado dentro de los Programas de Formación e Inserción (PFI), consiguiendo así que sean unos cursos que permitan obtener una titulación académica a estos jóvenes. La nueva edición del curso tiene una duración de 1000 horas, 180 de ellas de prácticas en empresas y cuenta con un nuevo financiador público, la Fundació BCN Formació Profesional.

Chatbot financiero

CaixaBank, a través de su banco para dispositivos móviles, imagingBank, acaba de desarrollar el primer chatbot del sector financiero en España. Los chatbots son una tecnología basada en inteligencia artificial, gracias a la cual las máquinas pueden interactuar con las personas utilizando el lenguaje natural. Actualmente, se calcula que existen unos 30.000 chatbots en funcionamiento en distintos sectores en todo el mundo, aunque en el ámbito financiero las experiencias son puntuales. La integración del chatbot supone una apuesta por seguir aplicando las últimas tendencias en innovación a imaginBank, el banco mobile only de CaixaBank, que ofrece servicios financieros avanzados basados en la tecnología. Los clientes pueden acceder a ellos para gestionar todas sus finanzas personales a través de la aplicación móvil y de aplicaciones para redes sociales. En el caso del chatbot, el nuevo servicio está disponible a través de Facebook Messenger. Los clientes pueden acceder a él tanto desde la propia aplicación de Facebook Messenger –buscando "imaginBank"-, como mediante la página de Facebook de imaginBank, donde deben seleccionar la opción "Enviar mensaje". Al clicar en "Empezar", el chatbot les da la bienvenida y les guía por las distintas opciones.

El chatbot está especializado en proporcionar información y asistencia sobre el uso de ofertas y promociones.

CABINAS FLASH DE NETAPP

NetApp ha presentado la cabina de almacenamiento all flash de mayor rendimiento del mercado, y una garantía de eficiencia que brindará a sus clientes un rendimiento sin concesiones que cumplirá con las exigencias de esta era digital en la que los datos son el motor de la empresa.

Las nuevas cabinas All Flash FAS (AFF) A700 de NetApp ofrecen un gran rendimiento en un formato compacto que permite modernizar las infraestructuras tecnológicas para las aplicaciones empresariales más exigentes, las cargas de trabajo de análisis de datos y la integración con el cloud. La densidad extrema del flash y las eficiencias punteras que ofrecen en almacenamiento permiten a los clientes reducir drásticamente el espacio físico que ocupan sus centros de datos, así como sus gastos energéticos tanto por funcionamiento como por refrigeración. NetApp también ha anunciado su nuevo programa all flash Guarantee, que garantiza un ahorro en el almacenamiento de hasta el 80%, en función de la carga de trabajo, dando así a los clientes la confianza de que podrán contar con la capacidad y eficiencia que NetApp les promete.

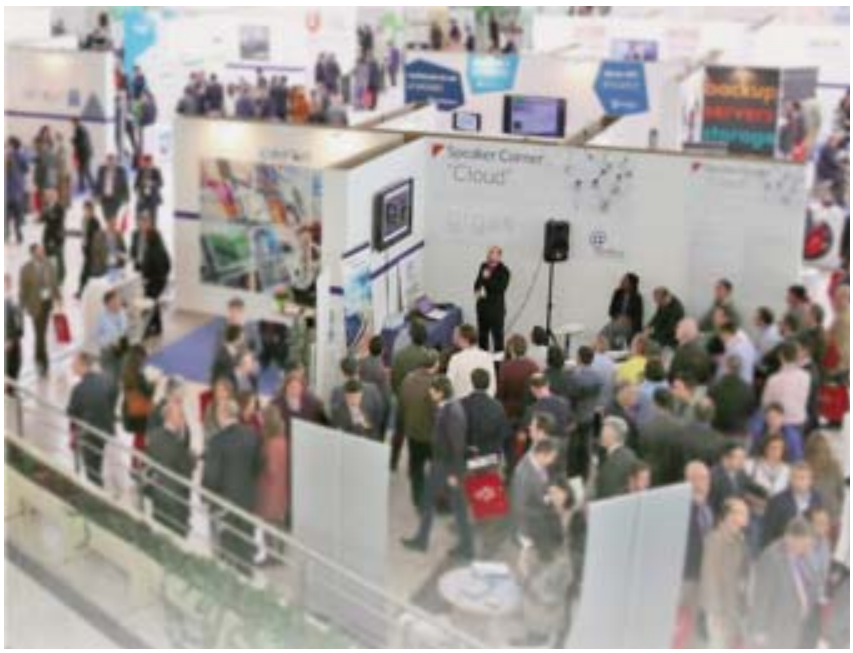
El congreso @asLAN 2017 incrementará su exposición un 20%

Más de 100 expositores en 3.000 metros cuadrados son las cifras de @asLAN 2017 lo que supone un aumento del 20% en el área de exposición con respecto a la registrada el pasado año.

Después de cumplir los 24 años, la asociación @asLAN ha conseguido superar el centenar de asociados y prepara el congreso de este año con una presencia de 100 expositores para un total de 3.000 metros cuadrados de ocupación, lo que supone un incremento del 20 % en relación al año pasado; se espera la asistencia de 5.500 visitantes. Así lo reveló en rueda de prensa Francisco Verderas, máximo directivo de la asociación, que estuvo acompañado de Félix García, Vicepresidente, y de otros componentes de su junta directiva.

"El papel de la tecnología y el de los expertos IT cambiará más en 2017 que en los últimos diez años. Nos encontramos en el punto de inflexión impuesto por el fenómeno de la Digitalización. Responsables IT, Partners tecnológicos, service providers y startups tienen ante sí la oportunidad de liderar la Transformación Digital aportando su valor y talento, experiencia así como su conocimiento tecnológico", argumenta la Asociación ante el Congreso que tendrá lugar los días 15 y 16 de Marzo en el Palacio de Congresos de Madrid.

"La principal ventaja de este Congreso", en palabras de Félix García, "es que el visitante se va a encontrar un ecosistema de partners para ayudarle con sus clientes en cómo transformar digitalmente su empresa. Va a encontrar soluciones mucho más en la realidad que en otros grandes congresos, donde están grandes operadores, grandes consultoras, pero que trabajan a otro nivel. Aquí estamos hablando de un ecosistema de partners que estamos liderando la transformación digital con la pyme, con la mediana y gran empresa, pero que cubrimos todos los aspectos. Somos partners más terrenales".



@asLAN cuenta actualmente con una sólida base de empresas asociadas comprometidas con la promoción y difusión de nuevas tecnologías en España

"En la Asociación @asLAN, que desde

1989 agrupa a empresas punteras en innovación tecnológica en torno a la red; vemos la coyuntura actual como una gran oportunidad para todos y el mercado en general. Ahora más que nunca la tecnología es un elemento clave en la generación de valor y ventajas competitivas para las empresas".

@asLAN cuenta actualmente con una sólida base de empresas asociadas comprometidas con la promoción y difusión de nuevas tecnologías en España; en el momento actual, en el que el fenómeno de la Transformación Digital está marcando el cambio de la economía y generando un incremento excepcional en el interés por nuevas inversiones en infraestructuras, tecnologías como el cloud computing, Internet of Things, redes inalámbricas, seguridad informática y la capacidad de analítica de la información, así como el control y monitorización de la red, están en constante innovación y son pieza elemental de la Transformación Digital." En la Asociación nos reunimos directivos de centros de datos, proveedores de servicios cloud, fabricantes especializados, operadores de telecomunicaciones, integradores, para poner en marcha iniciativas que permitan que toda esta innovación tecnológica se conozca y se difunde lo más rápidamente en España y se aplique en ámbitos estratégicos para nuestra sociedad así como en las SmartCities, lndustry 4.0 o eHealth.

Con el apoyo de 104 empresas asociadas, organizan un amplio Plan de Actividades anual que tiene como máximo exponente el Congreso & EXPO anual ASLAN2017, en el que durante dos jornadas intervienen cerca de 150 speakers presentando sus soluciones tecnológicas a los principales proveedores del sector. En esta vigesimocuarta edición habrá tres polos de innovación tecnológica: 1. Network & loT & DataCenter, 2. Cloud & Mobility & Collaboration, 3. Security & Analytics & Digitalldentity, además de dos Foros sobre Tendencias Tecnológicas, en los que intervendrán reconocidos fabricantes líderes y visionarios de la industria IT internacional. Habrá una Sala específica para Coloquios sobre Cómo liderar la Transformación Digital, dirigida tanto hacia responsables IT como empresas tecnológicas.

Además de organizar grandes eventos como ASLAN2017, en el que se espera la asistencia de más de 5.000 profesionales interesados en conocer las últimas tendencias tecnológicas y como aplicarlas en su negocio, en estos últimos años, la asociación se ha consolidado como un ecosistema de socios tecnológicos en el que grandes y pequeñas compañías puedan encontrar a sus aliados en este proceso de Transformación Digital. La colaboración entre empresas IT es clave para satisfacer la creciente demanda de tecnología.

"La Transformación Digital está cambiando el escenario, todos debemos evolucionar para adaptarnos a estos nuevos tiempos. Los proveedores debemos ofrecer servicios IT cada vez más especializados y competitivos, los responsables de IT rodearse en un ecosistema de socios tecnológicos que le permita centrarse en aplicar la tecnología al negocio, y las empresas desarrollar nuevos modelos de negocio y servicios a sus clientes soportados en estas nuevas tecnologías".

Conocer las últimas innovaciones tecnológicas, y ver cómo alinearlas al negocio, es el gran reto en la nueva era digital y el foco principal del Congreso ASLAN2017. Esta XXIV edición se celebrará bajo el título Tecnologías en red para impulsar la Transformación Digital y podrán verse soluciones tecnológicas presentadas por más de un centenar de proveedores especializados.

Sobresaliente

GOOGLE

La nueva creación de Google, junto con Jigsaw, pretende acabar con los comentarios tóxicos en los medios. Se llama Perspective y se basa en una tecnología y que utiliza el Machine Learning para identificar esos comentarios tóxicos y eliminarlos. A través de una API, editores (incluyendo los miembros Europeos de la Digital News Initiative) y desarrolladores, pueden acceder a esta tecnología y utilizarla en sus sitios web.

TELEFÓNICA

La operadora ha presentado un beneficio neto subyacente de 4.038 millones de euros (+4,8% interanual). Considerando los impactos no recurrentes registrados en el ejercicio – fundamentalmente gastos de reestructuración, plusvalías y bajas de fondo de comercio-, el beneficio reportado anual se sitúa en 2.369 millones de euros.

Muy deficiente

BIG DATA

A pesar de que el volumen de datos es cada vez mayor, las compañías aún no extraen el valor del Big Data para su negocio. Así lo confirma un reciente estudio de SAS que señala que, si bien para el 83% de las empresas encuestadas la inversión en gestión de datos es cada vez más significativa, sólo el 33% afirma obtener valor de los datos, mientras que un 49% considera que aún es pronto para confirmar la aportación de valor.

TESTING

Según el informe anual de SOGETI sobre el mercado de calidad y testing de aplicaciones, la situación política vivida en 2016 pudo haber ralentizado el ritmo de crecimiento que la Administración Pública venía manteniendo de contratación de proyectos para asegurar la calidad de sus aplicaciones. La Administración acaparó el 12% de los proyectos de este mercado en 2016, decreciendo 5 puntos con respecto a 2015 y situándose a niveles de 2014.

Watson IoT impulsa la innovación en IoT

IBM ha inaugurado en Múnich (Alemania) su sede mundial Watson IoT (Internet de las Cosas). Este nuevo centro ha supuesto una inversión de 200 millones de dólares, la mayor de la compañía en Europa en más de dos décadas.

El año 2017 será clave en la evolución del IoT, un fenómeno que cambia la forma de interactuar con el mundo y que se ha convertido en una pieza clave de la transformación digital. Según estimaciones de IHS, en 2020 habrá cerca de 30.700 millones de dispositivos conectados, prácticamente el doble de los que había en 2015 (15.400 millones). En este sentido, IBM anunció el año pasado que destinaría más de 3.000 millones de dólares hasta 2020 para llevar todas las ventajas de la tecnología cognitiva Watson al Internet de las Cosas (IoT).

El nuevo Centro Watson IoT de Múnich cuenta con 15.000 metros cuadrados y albergará a más de 1.000 investigadores, diseñadores y desarrolladores en el primer entorno profesional cognitivo de IoT. Este ecosistema de colaboración arranca con compañías de diferentes sectores que cuentan con equipos humanos in situ: Avnet, BNP Paribas, CapGemini y Tech Mahindra.

En el caso del distribuidor global de soluciones tecnológicas Avnet, su trabajo consiste en desarrollar conjuntamente con IBM soluciones basadas en IBM Watson destinadas a múltiples sectores: desde edificios inteligentes a industria, transporte, atención médica y consumo. Por su parte, la consultora CapGemini quiere utilizar el área de "Experiencia de Clientes" de la nueva sede Watson IoT para mostrar las posibilidades del Internet de las Cosas a sus clientes, entre ellos Faurecia, uno de los principales fabricantes de piezas para el sector de la automoción.

Por otro lado, la compañía india de tecnología Tech Mahindra tiene un equipo de seis desarrolladores e ingenieros trabajando en esta sede con el objetivo de desarrollar nuevas soluciones y tecnologías IoT antes de 2020. Asimismo, el banco francés BNP Paribas dispone de un equipo de desarrolladores en esta nueva sede de Watson IoT para investigar cómo las tecnologías cognitivas pueden transformar el sector financiero y ayudarles a diseñar productos y servicios más personalizados.

IBM ha anunciado también una alianza con EEBus, la principal iniciativa europea de IoT. Como parte del acuerdo, la compañía cede un espacio de innovación en su sede Watson IoT de Múnich para que los miembros de EEBus puedan colaborar en el diseño de estándares.

Por Fernando Jofre

ASISTENTES Y APPS DE MENSAJERÍA

Hoy en día las aplicaciones vinculadas a las redes sociales son sin duda las más populares, pero según un estudio reciente realizado por Gartner, serán eclipsadas por las de mensajería en tan sólo un par de años. A finales de Febrero, la consultora y analista del mercado publicó los resultados de un estudio sobre el uso de las aplicaciones móviles en Estados Unidos, Reino Unido y China, en el que se reflejaba que el número de consumidores que emplean apps de mensajería y asistentes personales virtuales sigue creciendo, como era de esperar. De tal forma que el colectivo de usuarios de éstas últimas ha pasado del 31% en el 2015 al 35% en el 2016. Mientras que los usuarios de apps de mensajería fueron un 71%, lo que supone un incremento de tres puntos con respecto al año anterior. Por el contrario, en lo que respecta a aplicaciones de redes sociales, su cifra ha bajado dos puntos con respecto al 2015. También bajaron las de video y mapas, quedándose en un más que honroso 71%. Terminamos la batería de cifras comentando que las de comercio electrónico crecieron cuatro puntos, para situarse en el 60%.

Los VPAs están creciendo, utilizándose principalmente para saber el pronóstico del tiempo, localizar sitios cercanos, o conocer las últimas noticias. El uso de estos asistentes es por ahora residual, aunque todavía queda por explotar todo su potencial. De hecho, no nos debería sorprender en breve que reemplacen a otras apps tradicionales, de tal forma que los usuarios tendrán estos "atajos", para disponer de información de una forma más consolidada. Facebook Messenger, WhatsApp o WeChat irán acaparando a los usuarios para retenerles con todo tipo de experiencias, como el eCommerce social, por ejemplo. En cuanto los desarrolladores y empresas integren bots en plataformas sociales se eliminará la necesidad de ir cambiando entre aplicaciones, y con ellos se atenderán tareas tales como atención al cliente o potenciar las ventas de productos y servicios. Por el momento, de la encuesta de Gartner se desprende que, a finales del 2016, sólo el 33 % de los entrevistados usaba de 6 a 10 apps.


Kaspersky®
Anti Targeted Attack
Detecta ataques dirigidos y amenazas avanzadas que el software de seguridad tradicional no puede reconocer
• Identifica rápidamente ataques dirigidos contra redes corporativas
• Combina análisis de objetos y de actividades para ofrecer detección avanzada
• Proporciona una visibilidad mejorada tanto a nivel de red como de endpoint
• Investigación de incidentes efectiva usando la inteligencia más avanzada
• Fácil escalado para cubrir redes de IT complejas y en crecimiento
Saber que eres el objetivo y reaccionar antes de que sea demasiado tarde
kaspersky.es
KASPERSKY lab
THE POWER OF INTELLIGENCE
© 2016 Kaspersky Lab. Todos los derechos reservados.
Las marcas registradas y logos son propiedad de sus respectivos dueños.

La tecnología 5G será protagonista en Cebit 2017

Parece algo de ensueño: una velocidad de transmisión de datos 1.000 veces mayor que la de la red LTE. El futuro estándar de la tecnología 5G de telefonía móvil lo hará posible. Vendrá a ser la columna vertebral para la interconexión de robots de fabricación, equipos operativos en quirófanos o farolas LED de alumbrado público. La telefonía móvil de la quinta generación será la base tecnológica de los desarrollos IoT (Internet de las Cosas) y su estrecha conexión de movilidad, Logística, energía y servicios de comunicación de todo tipo. Con tecnologías de red actualmente disponibles pueden operarse ya algunos escenarios. Pero la tecnología 5G amplía significantemente las posibilidades de interconectar miles de millones de equipos. Para realizar conceptos y modelos de negocios gracias en alta medida a esta tecnología.

Altos ejecutivos de la investigación, la industria o el comercio y todos los interesados por la Informática pueden informarse de primera mano en Cebit 2017 sobre las infinitas posibilidades de la conectividad en tiempo real. Así por ejemplo, Telefónica Deutschland coloca su presencia en el pabellón 12 bajo el lema "Mundo Interconectado en 360 grados" y ya ha anunciado escaparates como el sistema de respuesta en tiempo real "FeedbackNow" en forma de una "Smiley-Box" o caja de rostro sonriente que anuncia la Suela Inteligente GTX – una suela de zapato con función de seguimiento, que gracias a su tarjeta SIM de alcance global puede ser usada en todo el mundo. Expositores tales como Deutsche Telekom, Vodafone o Huawei hacen de la tecnología 5G también su tema central. Otros impresionantes casos de uso de conceptos pioneros de telefonía móvil se muestran en los sectores feriales "Internet de las Cosas" y "Comunicación & Redes", pabellón 12, y "Sistemas & Soluciones no Tripulados", pabellón 17. Aquí todo gira en torno al pujante negocio con los drones. Este ancho de banda tanto tecnológico como temático de cara a la digitalización no es ofrecido por ningún otro evento más que por CeBIT Hannover.

Por Manuel Navarro

Reutilice su smartphone

Ya se han quedado atrás esos tiempos en lo que los usuarios, cada año, pretendían cambiar de smartphone. Sí, ahora el móvil nos dura más tiempo. Ello es debido a que el salto entre un nuevo modelo y el de la generación anterior no tiene, para un usuario común, grandes diferencias. Sí, el procesador es más rápido o la pantalla presenta mejores definiciones pero el usuario ve que con su modelo antiguo va a realizar las mismas tareas que con el nuevo. Así que la gama alta se va a quedar para unos pocos.

Ya no queremos el terminal más caro, sino uno que nos sirva. Y casi todos sirven para lo que la gente realmente lo utiliza: enviar un whatsapp, consultar una red social, navegar por la Web o ver un correo. De tal forma que crece más la gama media que la alta. Y no sólo eso: son muchos los usuarios los que apuestan por el mercado de segunda mano para comprar un nuevo terminal.

Gracias a ese reciclaje, España se sitúa a la cabeza de los países en reciclado de terminales. Esto no sólo tiene un impacto positivo para el bolsillo de los consumidores sino también para el medioambiente. De acuerdo con las estimaciones de Back Market, la reutilización de estos terminales en nuestro país, evita la emisión de 60.000 toneladas de CO2 a la atmósfera y supone un ahorro de 24 millones de litros de agua cada año.

Esta plataforma, la primera especializada en tecnología reacondicionada en nuestro país, ha calculado tanto la cantidad de dióxido de carbono que deja de emitirse a la atmósfera como el ahorro de un recurso natural tan limitado como el agua, gracias a la reutilización que se hace de los teléfonos móviles en España. Este mercado se ha incrementado un 25% en los últimos tres años y los españoles reutilizan ya más de dos millones de dispositivos, lo que supone el 10% de todos los smartphones que se utilizan en nuestro país, según las últimas cifras publicadas por las consultoras Gartner y Deloitte. Por su parte, desde Back Market estiman que con la reutilización de cada aparato se evita una emisión media de 30 kg de CO2 a la atmósfera y se ahorran unos 12 litros de agua limpia.

YOGA 910

Lenovo

UN DISEÑO SUPERIOR

UNA PANTALLA INFINITA

- Procesador Intel® Core™ i7
- 14.3mm de grosor
- 1.38 kgs de peso

Windows

Usa tu portátil como una tableta.

Azure IP Advantage protege la innovación de los clientes de Microsoft

Microsoft ha presentado Azure IP Advantage, un nuevo programa diseñado para ayudar a las compañías a protegerse frente al riesgo de pleitos por infracción de IP en la nube.

El programa Azure IP Advantage ya ha sido valorado por distintas empresas, como Toyota, Mattel o Itron, que se han manifestado positivamente acerca de los beneficios

El programa Azure IP Advantage dota a los clientes de Azure de una protección líder en la industria, ofreciendo los siguientes beneficios:

· Protección frente a demandas por infracción de IP, con indemnidad sin límite de cuantía, que a partir de ahora también cubrirá cualquier tecnología de open source que Microsoft haya incorporado a Microsoft Azure, como por ejemplo la tecnología Hadoop que se emplea para el servicio Azure HD Insight.

· 10.000 patentes de Microsoft estarán a disposición de los clientes que utilicen Azure con la única finalidad de permitirles defenderse mejor frente a pliegos por infracción de patente que se dirijan contra los servicios que estos clientes ejecuten sobre Azure.

· Licencia de patente para que, si en el futuro Microsoft transfiriese una patente a una entidad no practicante, dicha patente nunca pueda ser ejercitada frente a nuestros clientes de Azure. Microsoft no tiene la práctica de realizar este tipo de transferencias, pero somos conscientes de que se trata de una protección adicional que aprecian numerosos clientes.

El programa Azure IP Advantage ya ha sido valorado por distintas empresas, como Toyota, Mattel o Itron, que se han manifestado positivamente acerca de los beneficios que les ofrece para centrar sus esfuerzos en desarrollar nuevos proyectos contando con la tranquilidad de saber que se encuentran seguros gracias al programa Azure IP Advantage de Microsoft.

Por Óscar González

RetroMadrid 2017

Que la nostalgia vende es más que una noticia actual. Nos encontramos ante un hecho más que contrastado. Son miles las personas, entre cuarenta y cincuenta años, que escanean día a día Ebay, Wallapop y similares en busca de chollos y ofertas de aquél juego de 8 bits que tenía de niño. Consolas de 16 bits, ordenadores tipo Spectrum, Amstrad y Amiga, y toda suerte de revistas, libros, casettes, disquettes y periféricos cambian de mano todos los días, a menudo a precios que superan las tres y cuatro cifras.

´Para todos aquellos nostágicos ansiosos por encontrar el desfasado producto de sus vidas hay lugares concretos y específicos. Uno de ellos es RetroMadrid. Se trata de una de las ferias más importantes de nuestro pais en lo que a nostalgia retroinformática se refiere, y este año finalmente sí que vamos a tener una edición como Dios manda. Las expectativas crecen año a año y aunque en el pasado se han producido pequeños (y comprensibles) errores de organización y capacidad, se espera que este año sea lo que todos esperamos. Servidor al menos estará por allí “frikiteando” y compartiendo esta pasión por lo retro.

A este respecto, resulta curioso hacer una sencilla estadística de los precios de este tipo de artículos en la red.

Juegos como los conocidos Game&Watch se han revalorizado cerca de un 300% en menos de ocho años. Se nota que los niños de los ochenta ahora ganan dinero y rebosan nostalgia. El sufrido consumidor de este tipo de artículos, debe bucear casi a diario en busca de ese vendedor incauto que “no sabe lo que tiene” e intentar arrebatárselo de sus manos todavía temblorosas. Y es que una copia de un Rocky, un Saimazoom o un Babaliba todo lo valen...

RetroMadrid 2017 tendrá lugar en el Espacio Cultural Daoíz y Velarde de la capital de España, durante el fin de semana de los días 29 y 30 de Abril.

MUCHO MÁS

Tanto si eres el gerente de tu empresa o supervisas los sistemas informáticos, los productos de seguridad ESET son rápidos, fáciles de usar y proporcionan un nivel de detección líder del mercado. Te ofrecemos una protección que te permite hacer MUCHO MÁS. Más información en **ESET.ES/EMPRESAS**

CON TUS SISTEMAS INFORMÁTICOS PROTEGIDOS POR ESET

ESET ENJOY SAFER TECHNOLOGY™

Sophos incorpora el aprendizaje automático avanzado a su porfolio

El aprendizaje automático de detección de malware y tecnología de prevención de Invincea estarán totalmente integrados en el porfolio de protección endpoint de Sophos

Sophos ha anunciado la firma de un acuerdo para adquirir Invincea, un proveedor de protección de malware de última generación. El porfolio de protección de endpoints de Invincea está diseñado para detectar y prevenir malware desconocido y ataques sofisticados a través de sus algoritmos patentados de redes neuronales de aprendizaje automático profundo. Además, ha sido valorada por expertos del sector como una de las mejores empresas en el desempeño de aprendizaje automático, tecnología endpoint de última generación sin firmas para las pruebas de terceros y posicionada en un alto nivel tanto por las altas tasas de detección, como por los falsos positivos.

Fundada en Fairfax, Virginia, Invincea fue creada por el chief executive officer Anup Ghosh para hacer frente al aumento de amenazas de seguridad de día cero, a los ciberdelincuentes y a los defraudadores. X by Invincea, la solución insignia de Invincea, utiliza redes neuronales de aprendizaje profundo y supervisa el comportamiento para identificar malware difícil de detectar y detener los ciberataques antes de que estos puedan tener consecuencias.

Enfocando su trabajo en soluciones para el gobierno de Estados Unidos, así como en sectores como la sanidad y los servicios financieros, Invincea se ha implementado en alguna de las redes más atacadas del mundo.

"Al incorporar a Invincea a nuestro porfolio, Sophos cumple con su visión de reunir tecnologías superiores para ofrecer las mejores y más avanzadas defensas a nuestros clientes", señala Kris Hagerman, chief executive officer de Sophos. "Invincea lidera el mercado de la detección de amenazas basándose en el aprendizaje automático con la combinación de altas tasas de detección y mínimas de falsos positivos. De esta manera, Invincea reforzará el liderazgo de protección endpoint de última generación con defensas predictivas complementarias que creemos que serán cada vez más importantes para el futuro de la protección de endpoints, y nos permitirá aprovechar al máximo esta significativa oportunidad de crecimiento. Estamos encantados de dar la bienvenida al equipo de Invincea y esperamos poder presentar los beneficios de esta tecnología avanzada para los consumidores y partners de todo el mundo", añade.

Sophos es reconocido como líder en protección endpoint por sus tecnologías de última generación en expansión como tecnologías anti-malware sin firmas, anti-exploit, anti-ransomware que se agrupan en Intercept X y analíticas basadas en el comportamiento, detección de tráfico malicioso y aplicación de reputación en la protección de endpoints de Sophos. El aprendizaje automático de detección de malware y tecnología de prevención de Invincea estarán totalmente integrados en el porfolio de protección endpoint de Sophos, reforzando aún más el liderazgo de Sophos en este mercado de rápido crecimiento. La disponibilidad de la tecnología de Invincea a través de Sophos Central, la plataforma de gestión de seguridad, mejorará aún más el porfolio de seguridad sincronizada de Sophos y el intercambio de inteligencia en tiempo real.

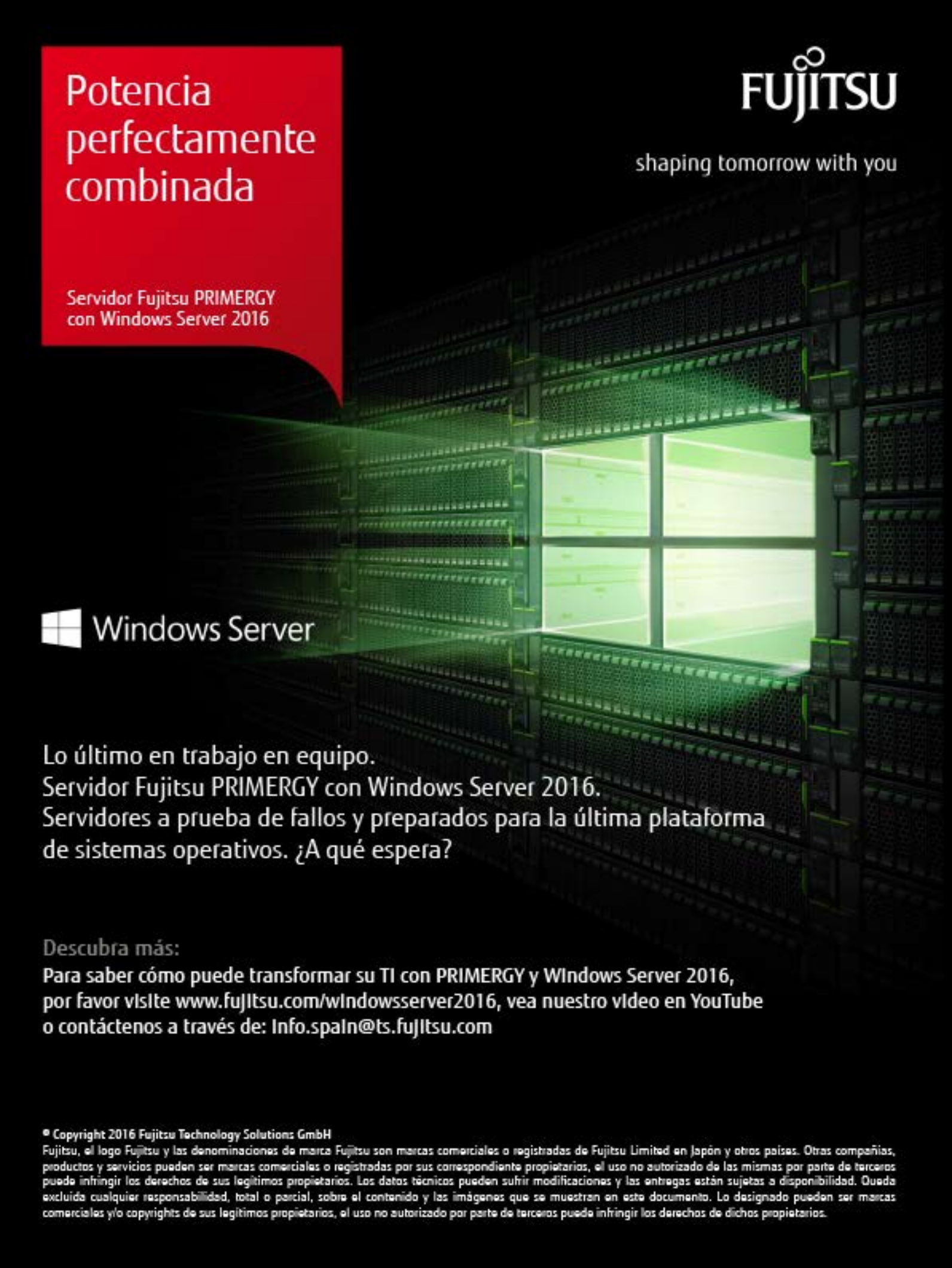
"Fundamos Invincea con el objetivo de usar tecnologías que no estuvieran basadas en firmas, combinando el aprendizaje automático, con formas innovadoras de protección de las organizaciones para luchar contra las más avanzadas técnicas de ciberataque" afirma Anup Ghosh, fundador y chief executive officer de Invincea.

Potencia perfectamente combinada

FUJITSU

shaping tomorrow with you

Servidor Fujitsu PRIMERGY
con Windows Server 2016



Windows Server

Lo último en trabajo en equipo.
Servidor Fujitsu PRIMERGY con Windows Server 2016.
Servidores a prueba de fallos y preparados para la última plataforma de sistemas operativos. ¿A qué espera?

Descubra más:

Para saber cómo puede transformar su TI con PRIMERGY y WIndows Server 2016, por favor vIsIte www.fujItsu.com/wIndowsserver2016, vea nuestro vIdeo en YouTube o contáctenos a través de: Info.spaIn@ts.fujItsu.com

Amazon Chime: la apuesta de Amazon por las comunicaciones unificadas

AWS ha anunciado Amazon Chime, un nuevo servicio unificado de comunicaciones que, según afirman desde la multinacional, hace las reuniones más fáciles y eficientes que nunca.

Amazon Chime permite iniciar reuniones con audio y video de alta calidad con un solo clic, liderar o unirse a una reunión fácilmente, una experiencia sincronizada y sin fisuras a la hora de compartir contenido y pantalla en dispositivos de escritorio, iOS y Android.

En un mundo donde los asistentes a reuniones a menudo no están en la misma ciudad, y mucho menos en el mismo edificio, las comunicaciones unificadas se han vuelto cada vez más importantes. La mayoría de los servicios y soluciones para reuniones son difíciles de usar, el video es granulado y se desconecta con frecuencia, la calidad de audio es pobre, hay ruido de fondo constante y es imposible saber quién lo está causando, requieren PINs largos para entrar y unirse a una llamada, y no están totalmente preparadas para móvil. Además, la mayoría son sólo buenos en una cosa (por ejemplo, llamadas de voz, videoconferencia, compartir pantalla o mensajería instantánea), por lo que los usuarios a menudo tienen que alternar entre varias herramientas diferentes, ninguna de ellas resuelve totalmente el problema.

Amazon Chime elimina la frustración en las reuniones ofreciendo video, voz, chat y pantalla compartida de gran calidad

Amazon Chime elimina la frustración en las reuniones ofreciendo video, voz, chat y pantalla compartida de gran calidad. Amazon Chime llama a todos los participantes cuando empieza la reunión para que se unan y basta un clic para unirse, no requiere PIN. En el panel visual de participantes de Amazon Chime es fácil ver quién se une o se cae. Además, es fácil acabar con el ruido en la reunión silenciando la línea que lo provoca.

Amazon Chime ofrece una potente aplicación tanto para móvil como para escritorio y es compatible con Android, iOS, Mac, y Windows. Además, puede integrarse con los directorios corporativos existentes y proporciona a los administradores de TI la capacidad de administrar identidades y controlar el acceso desde la organización. Amazon Chime no requiere inversión inicial, ni complicados despliegues o mantenimientos, basta con descargar la aplicación y empezar a usarla. Además, su coste es tres veces menor que el de otras soluciones tradicionales.

El directo de IT de la empresa Brooks Brothers ha declarado al respecto: "Normalmente tenemos que impulsar proactivamente la adopción de nuevas herramientas entre los empleados, pero después de iniciar un piloto de Amazon Chime, rápidamente vimos crecer el interés, llegando a una adopción del 90% entre nuestro personal sin ningún lanzamiento formal o formación. Con Amazon Chime, nuestros usuarios usan una sola aplicación para sus necesidades de comunicación desde todos sus dispositivos. Ahora que está disponible, planeamos comenzar a retirar las múltiples aplicaciones heredadas que hemos estado utilizando".

Amazon Chime elimina la frustración en las reuniones ofreciendo video, voz, chat y pantalla compartida de gran calidad

SECUESTRO DE DATOS CORPORATIVOS EN AUGE

¿Cómo proteger tu empresa del ransomware?

Alfonso Ramírez,
director general de Kaspersky Lab Iberia

Las cifras no mienten: el ransomware se ha convertido en una de las ciberamenazas más conocidas en los últimos años. Una vez que un troyano de este tipo se filtra, cifra los archivos, incluyendo documentos valiosos, vídeos y fotos. El proceso completo se ejecuta en un segundo plano dentro del ordenador, por lo tanto la víctima no se da cuenta del problema hasta que es demasiado tarde.

Según el Boletín de Seguridad de Kaspersky Lab, entre enero y septiembre de 2016, los ataques de ransomware a empresas se multiplicaron por tres, pasando de un ataque cada 2 minutos a uno cada 40 segundos en el último trimestre. Algunos sectores de la industria recibieron más ataques que otros, pero el análisis muestra que no existe un sector de bajo riesgo: con el índice más alto, alrededor del 23%, Educación y con el 16%, el más bajo, Comercio y Ocio.

España no se queda al margen de esta tendencia. De acuerdo con la investigación de Kaspersky Lab, una de cada cinco empresas en España sufrió un incidente de seguridad TI como resultado de un ataque de ransomware y una de cada cinco pequeñas empresas no recuperó sus archivos, incluso después de pagar

Además, el pasado año quedó demostrado hasta qué punto el modelo de negocio de Ransomware-as-a-Service atrae a los cibercriminales que carecen de las habilidades y los recursos necesarios. Los creadores de código ofrecen su producto malicioso 'bajo demanda', vendiendo versiones modificadas de manera exclusiva a clientes que luego distribuyen a través de spam y sitios web, pagándoles una comisión. El clásico modelo de negocio de 'afiliación' parece estar funcionando de forma muy eficaz para el ransomware. Las víctimas suelen pagar, así que el dinero sigue fluyendo. Inevitablemente, esto nos ha llevado a que aparezcan nuevos cryptors casi todos los días.

¿CÓMO PROTEGER LA EMPRESA?

Para que la protección corporativa sea total es necesario tener en cuenta: todos los dispositivos, redes, trabajadores concienciados, prevención e inteligencia, siempre con un servicio personalizado y adaptado a cada una de las necesidades empresariales que presenta cada cliente.

Las compañías deben contar con varias capas de protección, implementar el cifrado en las comunicaciones de datos sensibles, proteger todos los elementos de la infraestructura (gateways, correo electrónico, etc.) y parchear las vulnerabilidades de forma rápida y automatizar el proceso. También conviene implementar seguridad contra exploits y garantizar que las soluciones de seguridad incluyen los métodos de detección de comportamiento.

La tecnología es clave, pero también es recomendable que las empresas tomen otro tipo de medidas para reducir el riesgo y aumentar su conocimiento de las amenazas más recientes. Teniendo en cuenta que el 80% de los ciberincidentes se deben a errores humanos y que un porcentaje similar de CISOs admite que están insatisfechos con la eficiencia de sus programas de formación, es evidente la necesidad de encontrar un modelo que forme e informe de forma amena pero eficaz en materia de ciberseguridad. Desarrollar una cultura de ciberseguridad podría ayudar a reducir el número de incidentes en un 90% y disminuir el volumen monetario del riesgo entre un 50 y un 60%.

En este sentido, desde Kaspersky Lab recomendamos definir el plan de formación y concienciación sobre seguridad a todos los empleados para así reducir los incidentes.

KASPERSKY lab

Dell EMC renueva sus soluciones de infraestructura hiperconvergente

Dell EMC renueva sus soluciones de infraestructura hiperconvergente y anuncia que su plataforma de nube híbrida llave en mano, Dell EMC Enterprise Hybrid Cloud (EHC), estará disponible por primera vez con Dell EMC VxRail Appliances.

"Está claro que las empresas están adoptando modelos de nube híbrida y acuden a nosotros para que les ayudemos a simplificar la gestión de estos entornos, que inevitablemente incluye múltiples nubes, tecnologías entre nubes y una combinación de varias nubes dentro y fuera de las instalaciones", afirmó Chad Sakac, presidente de la división de Soluciones y Plataformas Convergentes de Dell EMC. "La infraestructura de hiperconvergencia ha demostrado ser eficaz para las cargas de trabajo más importantes del centro de datos y se está convirtiendo en la solución para la parte on-premise de la nube híbrida. La incorporación de Appliances VxRail de Dell EMC como una opción de infraestructura de Dell EMC Enterprise Hybrid Cloud nos ayuda a simplificar la nube híbrida para pequeñas empresas y para un mayor número de clientes".

La gama de Appliances VxRail HCI de Dell EMC totalmente integrados, preconfigurados y probados, son los únicos appliances HCI del mercado equipados con VMware vSAN y diseñados conjuntamente con VMware. Desde que se lanzaron los Appliances VxRail hace un año, Dell EMC ha vendido más de 8.000 nodos VxRail – más de 65 petabytes de almacenamiento y 100.000 núcleos – a más de 1.000 clientes en docenas de industrias en 78 países.

Según un estudio de IDC, los ingresos del portfolio HCI de Dell Technologies,

entre ellos VxRail Appliances, VxRack Systems y XC Series, superaron el mercado total de HCI, uno de los mercados TI de más rápido crecimiento- y representan el 28 por ciento de los sistemas hiperconvergentes vendidos en el tercer trimestre de 2016. 1

DELL EMC ENTERPRISE HYBRID CLOUD CON APPLIANCES DELL EMC VXRAIL

Dell EMC EHC es una solución de ingeniería totalmente diseñada, integrada y probada, lo que permite a una organización de TI aportar valor al negocio bastante más rápido que mediante la construcción de su propia infraestructura de nube híbrida. EHC con Appliances VxRail ofrece a los clientes una nube híbrida llave en mano optimizada para implementaciones que van de 200 a 1000 máquinas virtuales y:

- **Una plataforma optimizada para despliegues más reducidos** que ofrece una superficie más rentable y más reducida, con la flexibilidad para empezar a crecer a medida que los requisitos van cambiando.
- **Instalaciones simplificadas y automatizadas** en la pila de software Enterprise Hybrid Cloud con Appliances VxRail, que reducenel tiempo de implementación, los costes y el riesgo.
- **Soporte basado en suscripción con servicios profesionales**, que permite a las organizaciones sacar el máximo partido de las últimas mejoras de EHC.

Un estudio de Evaluator Group publicado recientemente demuestra por qué la nube híbrida es el verdadero modelo de nube. La rentabilidad de la nube pública (incluyendo Amazon Web Services, Azure, Google Cloud Engine y otros) la convierte en una excelente solución para cargas de trabajo que escalarán de formas desconocidas o transitorias. Como señala el informe, las plataformas HCI sencillas y rentables pueden ofrecer, para cargas de trabajo que se mantendrán durante años, un TCO mejor para la parte on-premise del modelo de nube híbrida.

Synology RT2600ac: seguridad y alta velocidad

Conjugar la mejor seguridad con una alta velocidad son las dos características de este router de Synology: el RT2600ac. Se trata de una solución perfecta para los hogares y oficinas de hoy en día que viene equipado con potentes paquetes de soluciones en una interfaz de usuario intuitiva.

Una de las grandes ventajas del Synology RT2600ac es que ofrece un gran rendimiento con conexión estable e ininterrumpida por cable e inalámbrica para varios usuarios. Asimismo, el router junto con VPN Plus permite a los usuarios de los routers de Synology configurar una solución VPN local potente.

REDES INTELIGENTES

Para maximizar la experiencia de usuario y el rendimiento de la red, el RT2600ac incorpora un procesador de doble núcleo de 1,7 GHz y es compatible con el estándar 802.11ac Wave 2 y con MU-MIMO, lo que garantiza que puedan conectarse más dispositivos a velocidades mayores. Con la ayuda de la función Conexión Inteligente, el RT2600ac puede optimizar de manera inteligente la calidad de la conexión y equilibrar dispositivos en frecuencias de 2,4 GHz y 5 GHz para obtener la máxima velocidad y alcance inalámbrico. El doble WAN con ancho de banda combinado de 2 Gbps permite a los usuarios aprovechar las ventajas de dos conexiones a Internet de fibra óptica de alta velocidad para el equilibro de carga y la conmutación por error.

Nos encontramos ante un router de alto rendimiento con el que los usuarios pueden gestionar de manera fiable un número cada vez mayor de dispositivos. Con el Synology Router Manager (SRM), el intuitivo sistema operativo para gestionar este dispositivo, y su colección de paquetes de soluciones disponibles, los usuarios pueden convertir sus RT2600ac en un VPN versátil, un RADIUS y un servidor de archivos con transmisión de alto ancho de banda. La capa de aplicación QoS (Quality of Service) permite monitorizar y controlar el consumo de ancho de banda, no solo de los dispositivos, sino también de las aplicaciones individuales. Incluso con el control de tráfico avanzado y la detección de aplicaciones habilitados, el motor de aceleración de hardware posibilita mantener un alto rendimiento y procesamiento en todos los dispositivos conectados. El RT2600ac cuenta con certificación Wi-Fi y DLNA.

POTENTE E INTUITIVA SOLUCIÓN VPN

La incorporación de VPN Plus en el router ofrece a los usuarios de oficinas en casa y pequeñas empresas una renovada experiencia de oficina virtual. WebVPN proporciona acceso sin cliente a servicios internos basados en web, lo que hace que el trabajo remoto sea tan fácil como abrir un explorador. Para aquellos usuarios que necesitan conectarse a un servidor de archivos o realizar mantenimiento remoto, Synology SSL VPN ofrece un rendimiento excelente y la seguridad del cifrado SSL, así como una configuración sencilla. Además, VPN Plus ofrece a los administradores una amplia gama de herramientas de gestión del tráfico y permisos para visualizar y optimizar su red. La compatibilidad con otros protocolos, como SSTP, OpenVPN, PPTP y L2TP por IPSec, también asegura que VPN Plus se integre a la perfección en todos los entornos. VPN Plus ofrece una única cuenta simultánea gratuita con acceso a WebVPN, Synology SSL VPN y SSTP. Para permitir más accesos simultáneos, se pondrá a la venta una licencia más adelante.

SEGURIDAD

Además de las herramientas de seguridad de serie, como protección de denegación de servicio y gestión de firewall, SRM ofrece herramientas innovadoras para ayudar a proteger su red de ataques externos:

- **Detección de intrusos:** El sistema de detección de intrusiones analiza el tráfico de red y registra todos los intentos de intrusión, para que pueda ajustar sus reglas de firewall sin que casi afecte al rendimiento. El sistema de prevención de intrusiones bloquea además el tráfico sospechoso en base a reglas personalizables.

- **Security Advisor y QualysGuard:** El usuario podrá supervisar y verificar los ajustes y los archivos del sistema en busca de problemas de seguridad y aplicar automáticamente las correcciones recomendadas.

- **Actualizaciones:** Como cada día se descubren nuevas vulnerabilidades, Synology se compromete a suministrar actualizaciones rápidas para mantener la seguridad del dispositivo y ofrecer máxima protección.

Microsoft, Epson, Toshiba, Eset y Unit4 explican al canal las ventajas de sus productos

Microsoft, Epson, Toshiba, Eset y Unit4 han sido esta vez los fabricantes que ha reunido Byte TI, en su Reseller Forum celebrado en Barcelona, para, en una jornada matinal, explicar a representantes de una veintena de compañías punteras del canal de distribución barcelonés las ventajas de contar con ofertas concretas de sus respectivas compañías.

Carlos Tortosa Responsable de Grandes Cuentas de ESET Espana.

Ignacio Sáez, director comercial de Byte TI, organizadora de este III Reseller Forums, dio la bienvenida a los asistentes para recordar el fin primordial de estos eventos, que no es otro que crear un vínculo estable de negocio entre el fabricante y el canal de distribución. Resaltó el éxito que están teniendo estos encuentros y desveló que la Comunidad Valenciana, Málaga y Galicia serán las próximas citas del Byte TI Reseller Forums.

UNIT 4

Joan Marc Llesuy, Partner Manager de ekon en Unit4, detalló cuatro principales ventajas de ser partner de ekon: exclusivo y limitado número de partners, eficiente plan de activación en 100 días, asignación de un Partner Manager con experiencia en la venta directa y cercanía del fabricante, acompañadas de otras cuatro más específicas para impulsar la rentabilidad del negocio con sus soluciones: tecnología de última generación (el secreto está en la plataforma), formación y tutoría del fabricante, soporte de servicios de consultoría con amplia experiencia en implantación y un programa de generación de leads. Llesuy avaló la calidad de sus productos en base al importante gastos en I+D y en su fabricación en España.

TOSHIBA

Moises Cuerva, Dealer Manager de Toshiba, presumió de ser el único fabricante de su especialidad que vende cien por cien por el canal. Centró su exposición en el novedoso portátil Toshiba Portégé X20-D y la solución Toshiba Mobile Zero Client. Al primero lo calificó de revolucionario, con disponibilidad de 23 chasis diferentes y 16 horas y media de duración de la batería. Puo de relieve que “en 2017 esperamos un impulso importante de dos elementos de

seguridad :Windows Hello e Intel authenticate“. Ambos sistemas se basan en la autentificación multifactor y, por esta razón,“implementamos secure pad con lector de huella dactilar en A30, A40 y Z40“. Se espera mucho interés, agregó, en la autentificación por reconocimiento facial. Cámaras IR.

Sobre el primer Zero Client en ordenador portátil, aclaró que sólo TMZC ofrece movilidad a los clientes VDI, que cualquier Portátil Profesional Toshiba puede usarse como Zero Client, que no se requiere almacenamiento en el Portátil y que el S.O., Aplicaciones e información se encuentran en la Granja de Servidores VDI.

Moises Cuerva, Dealer Manager de Toshiba

David Aibar, Account Manager Hosting Solutions de Insight de Microsoft

EPSON

Néstor Giner, Manage Print Services Sales Specialist de EPSON, habló sobre Print 365, la oferta de Servicios de Impresión gestionados de la compañía japonesa. Una oferta que reveló se presenta en el momento adecuado. Lo justificó

Alrededor de veinte distribuidores se dieron cita en Barcelona para conocer de primera mano lo que los fabricantes pueden ofrecer al canal de distribución especializado

en que el mercado Impresión Oficina crecerá 5%, el Business Inkjet lo hará en un 12% anual, un 20% de instalaciones Business Inkjet, crece el Inkjet vs. decrece/estanca el laser y la penetración BIJ oficinas en 2019 será 34,5%. Con estos mimbres justificó la propuesta de Epson. Un Print 365 diseñada para entorno PYME, paquetización del servicio con tarificación fija, servicio auditoría impresión, sin costes ocultos, proyección del coste de impresión, alta disponibilidad de servicio, y sin riesgo de cobertura. Y enumeró a sus potenciales partners, por qué les podría convenir vender la solución: cotización sencilla en paquetes cerrados; Plataforma Web gestión integral evaluación/gestión; diseñado especificamente para el entorno Pyme; herramienta de Evaluación y cotización de fácil uso; y, pago adelantado sin riesgo para el Reseller.

ESET

Carlos Tortosa, Responsable de Grandes Cuentas de ESET España, presentó el modelo de canal de su compañía, basado en la confianza y unos altos márgenes de beneficios para sus distribuidores. Recordó que ESET es un proveedor global de software de seguridad para empresas y consumidores, líder de la industria en detección proactiva de malware y que ESET NOD32 Antivirus, posee el récord mundial en número de premios VB100 de Virus Bulletin.

Empezó poniendo de manifiesto los principales puntos que les diferencian de sus competidores. A saber: poco uso de recursos del sistema; lideres en detección pro-activa; inicio del sistema mejorado; mayor productividad para usuarios y empresas; actualizaciones gratuitas a nuevas versiones de producto; productos situado entre los 5 mejor considerados a

Joan Marc Llesuy Partner Manager de ekon en Unit4

nivel mundial; y, certificaciones internacionales. Pero, la pregunta clave era ¿por qué distribuir sus productos. Y aquí ponemos la respuesta que dio: elevados márgenes (entre el 25 y el 35 % (Según segmento); protección de la cartera de clientes, incluso renovaciones; comisiones sobre las renovaciones; sin cuotas ni facturación mínimas; licencias OEM a precios reducidos para equipos nuevos; demos asociadas a su cartera que generan comisiones al convertirse en ventas; trato preferencial en operaciones especiales, y, soporte técnico preferencial y gratuito.

MICROSOFT

Finalmente, por parte de Microsoft intervino David Aibar, Account Manager Hosting Solutions de Insight, quien mostró las Soluciones Cloud de Microsoft. Dio detalles de lo que es un CSP. Básicamente un nuevo modelo de negocio, una nueva tipología de partners y una nueva relación con usuarios Cloud

CSP es un nuevo modelo para partners. Coexiste y no sustituye al resto de los acuerdos : Open, EA, Select, SPLA, etc. Convive y añade ventajas sobre ellos tanto para clientes finales como para los partners. Se licencia al usuario final de los productos Pay as you Go : verdadero pago por uso mensual a mes vencido. Los partners CSP gestionan una oferta integrada con varias capas de soluciones. Estas soluciones pueden ser de Microsoft, del partner o de terceros en cualquier proporción. La ventaja para el Cliente es evitar tener que contactar con los diferentes proveedores de cada pieza de la solución teniendo a un único proveedor. La ventaja para el partner es la fidelización completa del cliente final alrededor de todas las piezas de la solución. Esto además implica ampliar la oferta de soluciones a cada cliente lo que supone más facturación, mayor proporción de servicios y mejores márgenes.

Manuel Montaner, Gerente de Mayoristas Informática, coorganizadora del evento, cerró el acto dando las gracias a las empresas que se dieron cita.

Nestor Giner Manage Print Services Sales Specialist de EPSON

Durante los próximos meses el Byte TI Reseller Forum llegará a la Comunidad Valenciana, Málaga y Galicia

La ciberseguridad en el centro de la transformación digital: llega el RGPD

Cuando se habla de transformación digital y de la gran cantidad de datos personales y confidenciales que manejan en las empresas, hay que tener en cuenta la responsabilidad y los retos que éstas afrontan ante posibles ataques y brechas de seguridad. Hay un factor especialmente relevante que condicionará a las empresas en 2017 en la gestión de todos los datos que manejan: este año habrá que tomar todas las medidas para adaptarse a la entrada en vigor del Reglamento Europeo de Protección de Datos (RGPD) y la NISS. Todas las compañías tendrán nuevas obligaciones que afectan al almacenamiento y tratamiento de datos para proteger la privacidad de las personas.

El RGPD, aunque entró en vigor en 2016, será de obligado cumplimiento en mayo de 2018 y hay que tomarse muy en serio los cambios que introduce, porque son muchos, y no dejar los deberes para última hora. En su vertiente hacia los ciudadanos de la UE, el Reglamento viene a reforzar la definición de datos personales, que será más amplia e incluirá identificadores como identidad genética, cultural, económica y social. Y no sólo eso, la obtención del consentimiento para procesar los datos personales debe ser expresa y requerirá una respuesta afirmativa.

En cuanto a las empresas, desde PYMES hasta grandes corporaciones, este nuevo Reglamento, introduce el principio de 'Accountability', término inglés que implica responsabilidad y, además, la obligación de rendir cuentas. Las empresas estarán obligadas a realizar el análisis de riesgo y establecer los controles y medidas que pondrá en marcha para cumplir la normativa. Para ello, las sociedades españolas que cumplan unos determinados requisitos -fundamentalmente que realicen monitorizaciones periódicas y sistemáticas de datos a gran escala o gestionen datos considerados sensibles- tendrán que nombrar o contratar a un delegado de protección de datos (DPO). Además de establecer los procesos necesarios para captar y almacenar la información, también se han de tomar las medidas para protegerlos.

Los nuevos retos de protección y detección de brechas que exige el Reglamento y las ciberamenazas cada vez más sofisticadas y dirigidas, exigen soluciones de ciberseguridad más avanzadas. Panda Security ha cambiado el modelo de la ciberseguridad desarrollando Adaptive Defense 360, una plataforma de investigación, análisis, categorización y correlación de las ciberamenazas, que conecta en tiempo real a varias fuentes de información para revelar patrones de comportamiento malicioso y para generar acciones de ciberdefensa avanzada. Su modelo de seguridad integra una completa infraestructura con capacidades de Prevención, Detección, Respuesta y Remediación contra amenazas conocidas y desconocidas.

Adaptive Defense 360, es la primera solución cloud de ciberseguridad formada por un conjunto de servicios que conectan la inteligencia predictiva con las soluciones que ejecutan las acciones de remediación en el endpoint. Registra, correlaciona, analiza y categoriza diariamente más de 1TB de información sobre todo tipo de ciberamenazas. A partir de todos estos datos, genera patrones de conducta, que son utilizados para revelar comportamientos extraños, automatizar procesos de detección y para desarrollar acciones de protección y remediación.

En resumen, 2017 llega con un reto importante, el nuevo Reglamento, y las empresas deben de establecer los procesos necesarios y dotarse de las herramientas adecuadas para proteger uno de sus más importantes activos, la información, y –en segundo lugar- su reputación. Además, evitarán sanciones, que se volverán mucho más cuantiosas.

panda

Movilidad: mucho más que un smartphone

La situación del mundo de la movilidad fue el motivo de este encuentro organizado por Byte TI y que contó con la presencia de Ángel Luna, Director Centro Excelencia Movilidad de IECISA; Sales Channel Manager en Wolters Kluwer; Business Development Manager, Mobility de Red Hat; Bosco Espinosa de los Monteros, Ingeniero Pre-venta de Kaspersky Lab; Eva Sánchez, Business Development Manager de Canon España; José Antonio García, Iberia Mobility Sales specialist de HP Inc.; Genaro Escudero, EMEA Principal Consultant de Dell EMC y David Sanz, EMEA Endpoint and Mobile Competency Lead de Commvault.

El encuentro comenzó con el análisis de si el mercado de la movilidad está ya maduro o si todavía le queda mucho por avanzar. Ángel Luna, Director Centro Excelencia Movilidad de IECISA aseguró que hay que partir del punto de que "la movilidad no es solo el dispositivo móvil sino otro tipo de dispositivos y también realidad aumentada y virtual. Cabe la innovación tanto en consumo como en empresa". Para Jesús González, Sales Channel Manager en Wolters Kluwer, "la movilidad es vital y todavía se puede mejorar. Como desarrolladores de aplicaciones intentamos que haya una mayor productividad entre los usuarios y por tanto la movilidad ha venido impuesta porque ha permitido que la empresa gane eficacia". Por su parte, Javier Naranjo, Business Development Manager, Mobility de Red Hat consideró que hay un error en lo que normalmente se acepta como movilidad. En su opinión, "la movilidad se ha planteado como un pilar de la transformación digital y en realidad es innovación. La movilidad no solo es el dispositivo y desde ahí se puede innovar. Nos encontramos ante un entorno muy grande. Bajo mi punto de vista, no hay que quedarse solo en el desarrollo de la aplicación sino que hay que industrializar el desarrollo de aplicaciones".

Bosco Espinosa de los Monteros, Ingeniero Pre-venta de Kaspersky Lab, cree que "en movilidad se va a seguir innovando. Tenemos un problema que es que siempre vamos con el go-to market. Hay que poner unos estándares de seguridad. HP, por ejemplo, ha dado un gran paso en esta materia que es por donde tendrían que ir todos los fabricantes". Por su parte, Eva Sánchez, Business Development Manager de Canon España, consideró que "siempre se puede innovar y mejorar las soluciones y equipos que hay. En el ámbito empresarial, por ejemplo, esta innovación pasa por el documento, que es de vital importancia para las organizaciones. Por ejemplo, para poder capturar cualquier documento que tengamos en papel". En opinión de José Antonio García, Iberia Mobility Sales specialist de HP Inc., en el mercado de la movilidad sí se está produciendo innovación de forma constante: "hay innovación a nivel hardware. Nosotros apostamos por reducir equipamiento y debe haber una mejora en las aplicaciones, en las comunicaciones y en la conectividad. La tendencia del mercado va en esa dirección y es un compendio de cosas". Por su parte, Genaro Escudero, EMEA Principal Consultant de Dell EMC cree que "estamos al principio de la movilidad. Queda mucho por avanzar. Por ejemplo, yo entiendo la movilidad como la capacidad de acceder a los datos desde cualquier sitio y a nivel de comunicaciones estamos al principio. Los dispositivos surgen y evolucionan pero el paradigma de la movilidad está muy al principio". Finalmente, David Sanz, EMEA Endpoint and Mobile Competency Lead de Commvault, afirmó que "la movilidad no deja de innovar. Lo que había hace cinco

años no tiene nada que ver con lo que hay ahora, La gestión de riesgos es un punto en el que hay que avanzar. Lo que es móvil es la información no los dispositivos y esto es lo que las compañías están empezando a entender".

ÚNICO DISPOSITIVO

Una de las tendencias del mercado parece ser la travesía de ir hacia un único terminal que sirva para todo. Sin embargo, no todos los asistentes estaban de acuerdo con esta posibilidad. Así, el portavoz de Commvault afirmó: "Yo no me aventuraría a decir que esa es la tendencia. Lo que importa es la información y acceder a ella desde cualquier lugar. Si lo hacemos con uno o con dos dispositivos, es secundario". El portavoz de Dell se manifestó en el mismo sentido y aseguró que "la ventaja de la movilidad es que puedas usar un dispositivo según las necesidades. La movilidad rompe con el elemento tradicional de usar un solo equipo".

HP Inc. es una de las empresas que más está apostando por el desarrollo de un único dispositivo que valga para todo. Según afirmó José Antonio García, "a nivel profesional vamos a tender hacia un único dispositivo. Está claro que la experiencia será diferente según el dispositivo y hay que conseguir que esa experiencia sea la misma independientemente del dispositivo. El ir con una tableta, un smartphone y un portátil es algo que se va a quedar obsoleto. Nosotros creemos que el mercado ya ha visto una clara tendencia a unificar portátil y tableta. Ahora falta meter también el teléfono". En la misma línea se sitúo Eva Sánchez de Canon: "la tendencia acabará dirigiéndose a trabajar con un único dispositivo. Las compañías buscamos que la experiencia del usuario sea más cómoda. Al final con un único dispositivo se consigue esto".

Otros, como el portavoz de Kaspersky, aunque sí creen que la tendencia del único dispositivo va en aumento, no se arriesgan a valorar si esa situación será definitiva. En su opinión, "es una tendencia pero a nivel de usuario es complicado porque tenemos muchos perfiles y porque hay determinados trabajos que requieren unas características específicas. Es ideal para la empresa, seguro. Pero por desgracia los perfiles de usuario son diferentes y habrá gente que necesite otro tipo de dispositivo". También el portavoz de Red Hat cree que "puede ser lo mejor pero el perfilado de usuario se hace para que pueda trabajar desde cualquier sitio. Cada vez salen más wearables y creo que sería un error irse hacia un solo dispositivo. Creo que la tendencia es un entorno de movilidad más que un dispositivo móvil".

PROCESOS DE NEGOCIO

Alinear la movilidad con los procesos de negocio es uno de los retos a los que se enfrentan las empresas y no siempre se consigue. Tal y como aseguró el portavoz de IECISA, "queda mucho trabajo para que la movilidad se ensamble en los procesos de negocio empresariales. Se trata de optimizar el procesamiento gracias a la movilidad. En nuestro caso, tratamos de acompañar a los clientes en esa optimización que pasa por definir con ellos el caso real de uso y ayudarles a optimizar ese proceso". Para Jesús González de Wolters Kluwer, "hay mucho por hacer. A nosotros nos cuesta horrores explicar a los empresarios la importancia de la movilidad. El trasfondo es que todo lo que es físico, está cuestionado. A medida que vaya trasformándose ese pensamiento iremos mejorando".

Javier Naranjo de Red Hat cree que en la base se encuentran los problemas de alinear la movilidad con los procesos de negocio. En su opinión, "el error de la movilidad fue utilizar la capilaridad del móvil y olvidarse de la parte del backend y los empleados. El objetivo debe ser el de tratar de dotar de movilidad a los empleados". Para el portavoz de Red Hat el error radica en que en "mucha empresa, el concepto es dar el dispositivo al empleado. No se ha pensado en el negocio y lo que tenía que haber hecho es darle un dispositivo para que sea autónomo. Pero no es movilidad si va a ver al cliente y luego tiene que ir a la oficina para volcar los datos. Este es el mayor problema y queda mucho por desarrollar sobre todo en la concienciación de las empresas". Para la portavoz de Canon, "uno de los pilares de la transformación digital es el análisis de procesos y como la movilidad puede mejorar esos procesos. Si hablamos de gestionar el documento, hablamos de gestionar la información… La integración de la movilidad está empezando. Hay que hacer análisis y destinar recursos para ello.

Finalmente el portavoz de Commvault aseguró que "lo que las compañías buscan, es el equilibrio entre la información y la seguridad. En estos extremos muchas organizaciones priman la seguridad y son restrictivas y otras priman la productividad.

Al final hay que buscar el equilibrio entre ambas".

ESTRATEGIA

Cuál es la estrategia que deben seguir las empresas fue otro de los asuntos tratados durante el encuentro. El portavoz de Commvault afrimó que "lo que estamos viendo es que las organizaciones se centran en los dispositivos y eso es un error. Las soluciones de MDM no cubren todo. Lo importante es la información y el dispositivo es un mero medio de acceso". Para el portavoz de Dell, "en las empresas más conservadoras, que no se dan cuenta de que esto está cambiando, es donde se encuentra el fallo. Los que ni siquiera se preocupan, tienen que comenzar a planteárselo". Por su parte el directivo de HP Inc. afirmó que "lo que falla es que no hay una estrategia como tal. La estrategia hay que definirla. Pasó algo similar en las redes sociales. Hay que pensar que si se van a movilizar procesos, por qué se van a movilizar. Ahora corremos todos para sacar una app porque lo ha sacado un competidor… y claro se comenten errores de bulto. Falta estrategia". Para Eva Sánchez, "cualquier proceso de evolución requiere que el usuario final sepa lo que tiene y cómo lo tiene que utilizar. Puede haber proyectos magníficos pero si el usuario no lo conoce, el proyecto acabará fracasando". Por su parte, Bosco Espinosa de los Monteros cree que "falla el no hacer un plan de movilidad integral. El problema es que estamos poniendo puertas al campo. Imitamos lo que hace un competidor sin saber porqué tenemos que hacerlo. Hay que ver porqué voy a hacer una plan de movilidad, qué socio elegir para implantarlo, ver si es interesante para la compañía, ver los costes y dar visibilidad y formación a los usuarios. Puedes tener el mejor producto pero si no le ofreces formación al usuario, no vale para nada".

El portavoz de Red Hat cree que "no se hace un análisis correcto del ROI y no se piensa que si vas a una tendencia de movilidad vas a tener que desarrollar múltiples aplicaciones. Hay que pensar cuál es el entorno que hay que montar para industrializar ese desarrollo de aplicaciones". Finalmente desde Wolters Kluwer se aseguró que "es importante el tema de análisis de los procesos. A nosotros nos cuesta mucho meter la movilidad entre los clientes. Si acaso lo consigues en el departamento comercial. Muchas veces tenemos que insistir al cliente para que también lo haga en otros departamentos de la empresa".

SEGURIDAD

Finalmente se trató el apartado de la seguridad. Para el portavoz de IECISA, "se exagera y se protegen demasiado la información que dispone el empleado o el cliente con lo que el negocio no evoluciona a una gran rapidez. La seguridad es importante pero no puede poner freno a la evolución". Sin embargo desde Red Hat se aseguró que "es necesaria la seguridad. No vale de nada colocar la mayor medida de seguridad si luego la información no es accesible al usuario. Hay que buscar medidas de seguridad suficientes tanto en el dispositivo como en los flujos de información. Hay que buscar proveedores que te ofrezcan seguridad. Si un proveedor te ofrece lo mismo a un precio más barato algo hay. La seguridad no consiste sólo en poner candados. En seguridad hay que estar vigilando e innovando".

LOS PROTAGONISTAS

Ángel Luna, Director Centro Excelencia Movilidad de IECISA

Jesús González, Sales Channel Manager en Wolters Kluwer

Javier Naranjo, Business Development Manager, Mobility de Red Hat

Bosco Espinosa de los Monteros, Ingeniero Pre-venta de Kaspersky Lab

Eva Sánchez, Business Development Manager de Canon España

José Antonio García, Iberia Mobility Sales specialist de HP Inc.

Genaro Escudero, EMEA Principal Consultant de Dell EMC

David Sanz, EMEA Endpoint and Mobile Competency Lead de Commvault

KASPERSKY LAB: es una empresa de ciberseguridad fundada en 1997. El profundo conocimiento de las amenazas y la experiencia en seguridad de Kaspersky Lab se está continuamente transformando en soluciones de seguridad y servicios para proteger a empresas, infraestructuras críticas, gobiernos y consumidores en todo el mundo. El extenso portfolio de seguridad incluye su reputada solución de protección de dispositivos finales junto con un número de soluciones de seguridad y servicios para combatir sofisticadas amenazas digitales en constante evolución. La visión de Kaspersky Lab se basa en 4 pilares fundamentales que incluyen prevención, detección, predicción y respuesta a los incidentes de ciberseguridad. Más de 400 millones de usuarios son protegidos por las tecnologías de Kaspersky Lab y ayudamos a 270.000 clientes corporativos a proteger lo que más les importa.

COMMVAULT: permite gestionar los datos corporativos globalmente, estén donde estén, habilitándolos para su uso productivo de forma segura y en modo autoservicio para el usuario. Asimismo, la compañía garantiza la protección y visibilidad de la información accedida, almacenada o compartida en el entorno móvil, con el fin de analizar riesgos ante posibles pérdidas o normativas legales. La completa solución para puestos de trabajo de Commvault gestiona los datos corporativos almacenados en ordenadores portátiles, dispositivos móviles, ordenadores de escritorio o en servicios de compartición de archivos en la nube. Una solución que hace sencillo el backup y la búsqueda para recobrar el control de los datos en movilidad y gestionar de forma efectiva los archivos y carpetas que viven fuera del centro de datos, que pueden ser accedidos desde aplicaciones móviles o navegador web.

WOLTERS KLUWER: a3ERP | sales mobility es una aplicación móvil de Wolters Kluwer diseñada a la medida de las necesidades del equipo comercial, que, desde una tablet o un smartphone, puede llevar a cabo todas las gestiones de autoventa y preventa en cualquier momento y desde cualquier lugar. La app, disponible tanto para iOS como para Android, aumenta la productividad comercial de la empresa, garantiza el ahorro de tiempo y de costes, y lo hace con información actualizada, gracias a su integración y sincronización automática con a3ERP, la solución integral de gestión para la pyme.

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.

HP INC.: El HP Elite x3 es la apuesta principal de HP por la movilidad profesional, es el primer dispositivo empresarial 3 en 1 que combina la potencia de un ordenador de sobremesa para el día a día, junto con la versatilidad de un portátil para adaptarse a distintos entornos de trabajo y la movilidad total de un Smartphone. Gracias a la función de Windows Continuun ofrece una experiencia completa de trabajo en todos los ámbitos, por lo que constituye un verdadero puesto de trabajo móvil para los profesionales más exigentes. Este dispositivo cuenta con Windows 10, procesador Qualcomm Snapdragon 820 y 4Gb de RAM; además de una capacidad de almacenamiento de 64GB ampliables hasta 2TB gracias a una micro SD.

DELL EMC: El puesto de trabajo informático ha sufrido una de las mayores transformaciones en los últimos años. Los usuarios han tomado la iniciativa en el tipo de dispositivo y aplicaciones que quieren usar, y cómo o desde dónde quieren trabajar. Este hecho ha provocado que las empresas se estén planteando cómo afrontar la transformación digital y en particular la del lugar de trabajo. En la visión de Dell EMC este cambio debe ser disruptivo, entendiendo que ya no se gestiona el ciclo de vida del equipo, sino el del usuario y que además requiere entender las TI como un servicio, más que simplemente aplicaciones. Dell EMC aplica esta visión holística en todas las áreas (Movilidad, Operatividad, Productividad y Seguridad) aportando soluciones concretas y tecnologías que permiten realizar la transformación de un extremo al otro, desde el Centro de Datos hasta el usuario.

CANON: Hoy en día las empresas buscan una forma flexible y escalable de gestionar la impresión y el escaneo de forma eficiente, segura y con la máxima rentabilidad. Los usuarios demandan soluciones integradas de gestión de impresión y escaneo para poder hacer frente a los retos que supone la movilidad. La posibilidad de gestionar el documento end-to-end desde los dispositivos móviles está cambiando el concepto de oficina móvil.

RED HAT MOBILE APPLICATION PLATFORM: permite acelerar el desarrollo, integración y despliegue de aplicaciones móviles de nivel empresarial - tanto nativas, híbridas, o en la web, satisfaciendo flujos de usuario y de negocio a la par. Red Hat Mobile Application Platform, dota a los desarrolladores de la capacidad de trabajar de modo colaborativo y alineado con el concepto de "Ideation". Metodología que permite a los equipos de desarrollo de sistemas, de parte cliente y de integración, diseñar de modo independiente, y a su vez alineado con el concepto de "DevOps", metodología de desarrollo continuo y ágil. La integración con los sistemas empresariales tiende a ser la pieza fundamental, y a ese respecto el modelo "MBaaS"es clave, ya que permite la abstracción para poder utilizar cualquier entorno de desarrollo, e integrarse, en cualquiera de los sistemas empresariales. Adicionalmente, Red Hat Mobile permite la gestión de las fuerzas de trabajo de las compañías, con su módulo de "Workforce Management (WFM)".

Sophos Intercept X

Ransomware se ha convertido en una pesadilla tanto para empresas como para usuarios. La nueva herramienta de Sophos promete acabar con él.

Sophos

Calle de Orense, 81,
28020 Madrid

Precio
000 euros

Teléfono
913 75 67 56

WEB
www.sophos.com

EXCELENTE
MUY BUENO
BUENO
ACEPTABLE
POBRE

TECNOLOGÍA

IMPLEMENTACIÓN

RENDIMIENTO

A FAVOR:
Bloquea ransomware

EN CONTRA:
Ransomware tiene que empezar a actuar para ser bloqueado

La principal característica de Sophos Intercept X es que se trata de un producto de seguridad enpoint de última generación que detiene el malware de día cero, los ataques sigilosos y las variantes exploit desconocidas, e incluye una funcionalidad avanzada antiransomware que permite detectar ataques desconocidos previos en cuestión de segundos. Sophos Intercept X se instala junto al software de seguridad endpoint ya existente de cualquier fabricante, y al instante impulsa la protección endpoint eliminando el código malicioso antes de que este se ejecute.

Para poder eliminar el código malicioso que pudiera encontrarse en el equipo, Intercept X combina cuatro componentes de seguridad esenciales que cualquier administrador de TI debería esperar de los productos de protección next-gen endpoint:

1. Detección de amenazas y exploit sin firmas. En este caso se trata de una defensa antimalware y antihacker que bloquea las amenazas de día cero, los ataques residentes de memoria y amenazas desconocidas sin necesidad de escanear los documentos.

2. CryptoGuard. Este segundo componente es el que promete acabar c9on el temido ransomware-ya que identifica e intercepta la actividad de encriptación maliciosa. Esto significa que la solución de Sophos es capaz de bloquear el ransomware antes de que el virus bloquee los sistemas. Gracias a ello puede hacer que los documentos encriptados vuelvan a su estado original.

3. Analítcas de Causa Raíz. En este caso, se trata de análisis visuales en 360º de los ataques que permite ver de dónde proviene la amenaza, qué infectó, hasta dónde infectó y proporciona recomendaciones para prevenir ataques similares futuros.

4. Sophos Clean. Muy útil para cazar y eliminar cualquier rastro de spyware y malware persistente e incrustado.

Desarrollado como un componente clave en la estrategia sincronizada de seguridad de Sophos, Intercept X está equipado con Security Heartbeat para compartir la inteligencia ante amenazas con las soluciones de última generación Firewall XG y Safeguard Encryption, para una respuesta coordinada y automatizada frente a los ataques. El producto puede ser instalado y controlado de forma remota a través de la consola de gestión cloud Sophos Central, que permite a los administradores controlar y ajustar la configuración, distribuir licencias, añadir nuevos endpoints y realizar seguimiento de toda la actividad. Además, su panel de control exclusivo diseñado por los partners de Sophos muestra todos los servicios disponibles de Sophos Central para aportar niveles de protección más elevados para el cliente a la vez que ofrece a los partners oportunidades extra de ingresos recurrentes.

Pero sin duda alguna, lo que más llama la atención del producto es que permite acabar con la pesadilla ransomware. El ransomware constituye el ataque de malware que más afecta a las organizaciones en la actualidad. Cifra sus archivos y los secuestra hasta que se paga el rescate, lo que provoca graves interrupciones en la productividad del negocio. Sophos Intercept X incluye CryptoGuard, que impide el cifrado malicioso espontáneo de datos por parte de ransomware, incluso archivos o procesos de confianza que hayan sido secuestrados. Y una vez que se ha interceptado el ransomware, CryptoGuard revierte sus archivos a su estado seguro.

Las empresas deben concebir los riesgos como un conjunto

Jaime Guevara
Director General
Alhambra-Eidos

Es mucha la información publicada sobre casos de hacking, phising y otros ciber-delitos, lo que es muy positivo, así como las diferentes herramientas para combatirlos. Pero a pesar de esa abundancia de información, la mayoría de los dirigentes de empresas no tecnológicas difícilmente pueden imaginar cómo esto se aplica a sus negocios.

Y en efecto, no es tan fácil imaginar la diversidad de amenazas específicas que pueden vulnerar los datos que maneja una empresa y sus diversos procesos, ni la forma en que los ciber-delincuentes pueden sacar provecho de estos delitos a costa de la empresa, ni tampoco el impacto que estos actos pueden llegar a tener en el negocio.

Imagine el esfuerzo de analizar todos estos escenarios y de tener una visión clara de cómo se desarrollaría en la práctica cada uno de ellos: su detección, la reacción del equipo de TI, las operaciones de defensa ante la amenaza detectada, las consecuencias de este combate sobre las operaciones en curso, las reacciones del personal y de los clientes, proveedores y otros interlocutores, las medidas paliativas a tomar, los remedios a aplicar, las acciones judiciales para intentar recuperar lo perdido, las pruebas de que se dispondrá para llevarlas a cabo, etc.

Un proceso muy complejo que requiere de la ayuda de profesionales que se hayan enfrentado a muchos de estos casos para hacernos ver cómo sería si sucediera en casa. Y más aún si deseamos llegar a conclusiones sobre qué hacer HOY para evitar algunos de esos riesgos, limitar sus efectos y estar mejor preparados para enfrentarlos si se producen.

Este tipo de riesgos se suman a otros de los que ahora se habla mucho menos: cada vez son mayores los riesgos de origen no delictivo que corren las empresas al hacer un mayor uso de la nube, de la movilidad y de las transacciones directas con clientes y proveedores.

Por nuestra experiencia podemos decir que, para poder ayudar a una empresa, es necesario tener una visión completa de sus actividades IT y una buena comprensión de su negocio. Saber analizar los verdaderos riesgos de una empresa e intervenir sobre una gran cantidad de elementos y procesos para ir mejorándolos. Aportar soluciones realistas en términos de impacto sobre el trabajo y sobre los costes de cada uno de estos puntos. Y evidentemente, establecer una relación de verdadero partner tecnológico que acompañe a largo plazo a la empresa. No se puede actuar sólo como especialista, ni estar urgido por vender las soluciones y servicios de la cartera.

En nuestro caso en OneseQ, nuestra área de Ciberseguridad, concentramos las competencias y las unidades especializadas para dar servicios de seguridad, pero su acción se inscribe dentro de una colaboración estrecha con el resto de nuestras divisiones, y tiene el mismo enfoque de asesoramiento y servicio a nuestros clientes, para acompañarles hacia su éxito.

Concebir los riesgos como un conjunto y los dispositivos y medidas de protección frente a todos ellos, sean delictivos o no, como un todo, nos permite optimizar recursos y costes.

Y es así como se puede, por ejemplo, diseñar un servicio SIEM o un SOC que funcione en coherencia con la supervisión proactiva de los procesos, o asegurar una ubicación del DRP adecuado para tomar a cargo la operación en caso de ataque, etc. Si se hace bien, la gestión de las redes puede asegurar la conectividad de los sitios tanto en caso de fallo técnico como de bloqueo malicioso, y proteger la integridad de los datos frente a la corrupción de uno de los soportes, sea accidental o malintencionado.

Dado que además como proveedor de servicios tomamos a cargo los servicios gestionados de las redes, la telefonía y las nubes (privadas, públicas o híbridas) de nuestros clientes, tenemos la responsabilidad de estudiar con él los riesgos de todo tipo que implica su arquitectura. OneseQ hace estos estudios y propone diversos complementos y modificaciones de diseño para llegar al nivel de seguridad adecuado al valor que cada elemento tiene para nuestro cliente.

Nuestra preocupación con los objetivos del cliente, su reputación y su sostenibilidad, nos han llevado a diseñar en OneseQ una serie de soluciones y servicios gestionados que permiten llevar a la mediana y pequeña empresa niveles de seguridad que antes sólo estaban al alcance de las muy grandes.

Combinando estas capacidades en ciberseguridad de OneseQ con las competencias de Alhambra-Eidos en materia de backup gestionado y de DRP, tanto en contextos en que somos los que alojamos, como en configuraciones de nubes híbridas, damos una protección total a las infraestructuras de datos y procesos.

Completamos esa protección del cliente, asegurando la continuidad y confidencialidad de sus comunicaciones, tanto a nivel de sus redes como de sus servicios de telefonía y mensajería convergentes. Nuestros servicios en estas áreas están certificados para poder tratar datos confidenciales médicos y financieros.

Además, nuestros clientes más sensibles se benefician de nuestras competencias en desarrollo de software seguro, y de nuestras soluciones para asegurar el cumplimiento de procesos de validación internos y el respeto de las políticas de adquisiciones y contratos, que utilizan en particular las administraciones públicas.

Por eso nos consideramos un Grupo enfocado totalmente en dar seguridad y protección a nuestros clientes para asegurarles un desarrollo sostenible.

OneseQ
by alhambraeidos

Schneider Electric Galaxy VX

Este equipo proporciona un modo de operación flexible con la tecnología ECOnversion para grandes instalaciones, Data Centers y aplicaciones críticas.

Schneider Electric

C/ Bac de Roda, 52, 08019 Barcelona

Precio
consultar

Teléfono
934 84 31 00

WEB
www.schneider-electric.es

EXCELENTE
MUY BUENO
BUENO
ACEPTABLE
POBRE

TECNOLOGÍA

IMPLEMENTACIÓN

RENDIMIENTO

A FAVOR:
Alto rango de energía

Galaxy VX es un sistema de alimentación ininterrumpida (SAI) trifásico, compacto, altamente eficiente y fácil de instalar, con un modo de operación flexible, pensado para grandes instalaciones, data centers y aplicaciones críticas.

Una de las grandes características del nuevo SAI presentado por Schneider Electric es que el Galaxy VX está diseñado para ofrecer un rango de energía desde entre 1000KW y 1500KW en configuración unitaria y es capaz de ofrecer incluso más capacidad en configuración en paralelo. Destaca de entre sus cualidades el innovador modo ECOnversion y la tecnología de inversores a cuatro niveles que ayudan a las empresas en su transición hacia los Data Centers de hiperescala y les permite aprovechar mejor sus instalaciones implementaciones TIC ofreciendo eficiencia, sin comprometer la fiabilidad.

Cloud computing y los modelos de colocation continúan su proceso de expansión en las compañías, y se está dando la circunstancia de que cada vez hay un mayor interés en la eficiencia energética en la transición hacia los Data Centers de hiperescala. Lo que Galaxy VX proporciona son menores costes de propiedad, gracias a que ofrece una gran disponibilidad, consistencia y escalabilidad a través de un modelo de inversión según crecimiento.

La apuesta de la multinacional norteamericana con este nuevo SAI es la de proporcionar a sus clientes una gran variedad de opciones de almacenamiento de energía para ofrecer el mejor servicio para su negocio en la actualidad, mientras que a la vez puedan prepararse para las necesidades de almacenamiento de energía que puedan tener en el futuro.

Galaxy VX está totalmente integrado con las soluciones de gestión de la energía de Schneider Electric y presenta modos flexibles de funcionamiento para optimizar la eficiencia de los entornos TIC, incluyendo:

- Modo de doble conversión: Gracias a la tecnología de inversores a 4 niveles, en modo doble conversión, el SAI es capaz de ofrecer la eficiencia más alta a bajos niveles de carga. Esta tecnología ofrece una mayor fiabilidad gracias a sus menores tensiones de conmutación y reduce la tasa de fallos.
- Modo Eco: Galaxy VX ofrece el modo ECO tradicional que proporciona hasta el 99% de eficiencia.
- Modo ECOnversión: con este nuevo modo de operación, Galaxy VX ofrece un híbrido entre el Modo Eco y el Modo de Doble Conversión. ECOnversión proporciona unas prestaciones dinámicas equivalentes a la doble conversión con una eficiencia de hasta el 99%.

El sistema Galaxy VX está disponible desde el mes de enero a través de Schneider Electric y sus partners. El nuevo miembro de la gama de soluciones Galaxy V para la protección de cargas críticas se integra fácilmente en los entornos eléctricos, físicos y de monitorización de clientes en los que operan los Data Centers o aplicaciones para infraestructuras industriales.

CeBIT 2017

Information for Visitors

Global Event for
Digital Business

20 – 24 March 2017
Hannover • Germany

cebit.com

Japan
CeBIT Partner Country 2017

Consigue tu entrada en
http://www.cebit.de/promo?qkumt

Deutsche Messe

CeBIT

Delegación Deutsche Messe en España
Teléfono: 0034 91 562 0584
Email: info@messe.es

Ciberseguridad contra el cibercrimen

No hay día que pase en el que no aparezca una noticia relacionada con el cibercrimen. Robo de datos, de identidades, Ransomware,… El abanico es amplio y crecerá. En este reportaje intentaremos dar las claves de lo que está sucediendo en un mundo cada vez más peligroso. **Por Manuel Navarro**

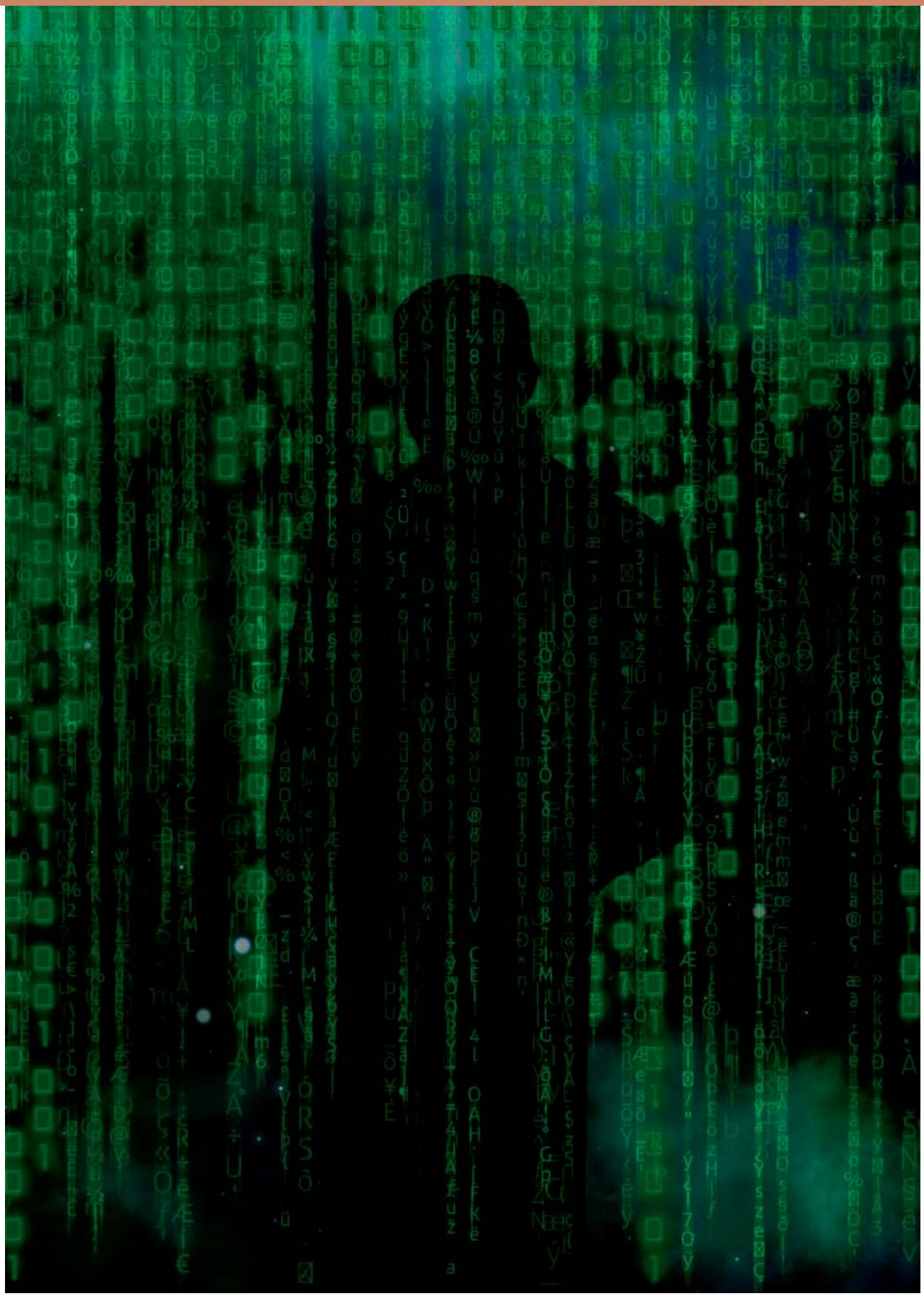
Los ataques afectan a todo el mundo: usuarios, empresas, administraciones y hasta Gobiernos y estados que hasta ahora parecían invulnerables. Nos hemos acostumbrado a convivir con una permanente batería de ataques y que no parece tener fin. Algunos, incluso graves. La victoria de Donald Trump en EE.UU. está en entredicho por suspuestos ataques informáticos. Países como Francia, cuyas elecciones se celebrarán el mes que viene, han decidido volver al recuento manual, toda vez que no están seguros de que un ataque informático pueda hacer variar el resultado electoral. Ransomware, cada vez afecta a un mayor número de usuario y los robos de información y datos a empresas están a la orden del día. Lejos de disminuir, los ataques seguirán en aumento. Para el año 2019 se espera que un 80% de las organizaciones reciba algún tipo de ataque. Lo peor es que nos enfrentamos ante un escenario desconocido, puesto que, por ejemplo, en el auge que está experimentando IoT, no se han tenido en cuenta las medidas de seguridad necesarias… hasta ahora.

La ciberdelincuencia es la principal preocupación de los responsables de TI (riesgo de infección de un equipo aumenta +40% al año):

- Más de un millón de usuarios son víctimas cada día de un ciberdelito
- 51% de las compañías que han tenido una brecha de seguridad en hardware o software, también han tenido como consecuencia una parada en sus operaciones
- Cada día, 2000 ordenadores son robados o perdidos en el mundo

Si bien el posicionamiento tradicional consistía en crear un perímetro de seguridad que impidiese el acceso, para 2016 (IDC), el 70% de las organizaciones TI pondrá el foco en aumentar el control y la visibilidad que tienen de la infraestructura y las soluciones tecnológicas, para poder detectar las amenazas y prevenir los posibles daños incluso antes de que se produzcan.

Nos encontramos, por tanto, ante un panorama con innumerables retos. Unos más importantes que otros, pero todos ellos deben ser tenidos en cuenta. ¿Cuáles son esos retos? Florian Malecki, International Product Marketing Director, SonicWall afirma que "podríamos destacar cuatro retos principales: los ataques al punto de venta (o Point of Sale), el ransomware, los ataques DDoS y la proliferación del tráfico SSL/TLS. En cuanto a los ataques en el



punto de venta, la Global Response Intelligence Defense (GRID) Threat Network de SonicWall ha visto que el número de nuevas familias de malware relacionadas con POS caerá de las 14 que existían en 2014, a sólo una en 2016. A pesar de esta prueba de la eficacia de los sistemas chip, muchos comercios todavía no han activado la tecnología chip. Esto significa que los comercios tendrán que activar sus escáneres de chips de forma consistente para mantener la tendencia de malware POS en la decadencia".

Las amenazas avanzadas, incluyendo el ransomware, se están convirtiendo rápidamente en el crimen cibernético más popular, ya que son más fáciles de diseñar y distribuir que el malware POS y pueden dirigirse a individuos, empresas y minoristas por igual. El ransomware suele obtener acceso a una red cuando un empleado visita un sitio comprometido o descarga un archivo comprometido por correo electrónico. Una vez conseguid el acceso, bloquea el sitio web del minorista y lo mantiene "secuestrado" hasta que se pague un rescate. La mayoría de los ciberdelincuentes utilizan sistemas de encriptación de grado militar, por lo que incluso las grandes organizaciones pueden ser susceptibles a estos ataques. Pero para estos delincuentes es más sencillo atacar a pequeñas y medianas empresas, por lo que podemos esperar que estos grupos sean atacados de manera más frecuente en el próximo año.

Además, desde SonicWall se prevé un aumento ataques distribuidos de denegación de servicio. Dichos ataques DDoS (por sus siglas en inglés) han existido durante años, principalmente dirigidos a instituciones financieras y gubernamentales. Sin embargo, estos ataques están evolucionando para apuntar a la infraestructura de la propia Internet, más recientemente aprovechando las brechas de seguridad presentes en los dispositivos IoT. Por ejemplo, el crecimiento del número de dispositivos IoT sin seguridad, provocó numerosos ataques botnet del malware Mirai en octubre. Estos ataques DDoS se infiltraron en los sistemas IoT para bloquear sitios tan importantes como Reddit, Amazon o PayPal. Este tipo de ataque puede ser especialmente costoso para las empresas que tienen una cantidad significativa de negocio online. Los ciber-ladrones pueden acompañar el ataque con una nota de rescate, lo que implica que la motivación es un pago. Pero esto también puede ser una distracción mientras los ladrones cibernéticos lanzan ataques menos obvios, como la exfiltración de datos.

Por último el tráfico SSL / TLS dentro de la red empresarial está aumentando, al igual que la amenaza para las empresas. Las empresas están viendo cada vez más tráfico cifrado pasando por sus redes, debido a la creciente proliferación de los dispositivos móviles dentro del ecosistema de las empresas. El informe de amenazas 2016 de SonicWall reveló que casi dos tercios del tráfico de la red de las empresas estaba cifrado y esta cifra sigue subiendo. Sin la capacidad de inspeccionar los paquetes cifrados, como los correos electrónicos personales, las empresas corren el riesgo de sufrir ataques de malware, específicamente ransomware, que se está convirtiendo en una de las amenazas número uno para la empresa. Las empresas que bus-

can asegurar sus datos deben emplear soluciones que ofrecen inspección profunda de paquetes (DPI) y análisis en la nube para archivos sospechosos.

Sin embargo, muchos piensan que el reto se encuentra en el propio usuario. Se trata del elemento más débil de la cadena y por ello se producen casos como el del Ransomware. Para Jordi Gascón, EMEA Security Presales Lead de CA, "el eslabón más débil en la cadena de seguridad suelen ser los propios usuarios/empleados. Típicamente, los ataques y brechas de seguridad se producen con credenciales válidas de usuarios existentes y, una vez dentro de los sistemas, se llevan a cabo mediante diferentes técnicas los intentos de elevación de privilegios para conseguir acceso de administrador (usuarios privilegiados).

Por este motivo, en seguridad se debe aplicar los conceptos de defensa en profundidad (defense in-depth) y mínimo privilegio (least privilege) aplicando diferentes capas de protección. En el primer nivel o capa se sitúa una correcta gestión de los usuarios y sus accesos y es aquí donde soluciones como CA Identity Suite ayudan a asegurar que los usuarios tienen los accesos pertinentes y que no existen cuentas "huérfanas" susceptibles de ser usadas como puerta de entrada. Por otra parte, las soluciones como CA Privileged Access Management (CA PAM) y CA PAM for Server Control, aseguran una correcta gestión de los usuarios administradores, manteniendo control de quién hace qué en todo momento e, incluso evitar que usuarios como "root" o "administrator" tengan el poder y control completo de los servidores. Por último, soluciones como CA PAM for SC permiten realizar un bastionado de los servidores críticos".

Pero los retos continúan. En el punto de mira una tecnología emergente, aunque ya no tanto: IoT. Rodrigo Chávez Rivas, IT Security Services & Solutions de Unisys afirma que "desde una perspectiva de amenazas, los retos están enfocados hacia la seguridad en los móviles, servicios en la nube e IoT. Desde una perspectiva de cumplimiento, uno de los principales retos en el corto plazo será la protección de datos (GDPR)". También desde Symantec se pone el foco en IoT. Para Carlos Ferro, Symantec Enterprise Country Manager, "Nuestros expertos en seguridad han examinado de cerca las tendencias a las que se enfrenta el mercado de la ciberseguridad y las resumimos en tres grandes bloques: la necesidad de asegurar el Internet de las Cosas en un mundo donde cada vez es mayor el número de dispositivos conectados que utilizan tanto consumidores como empresas; el uso cada vez mayor de la nube en las rutinas de trabajo, que hará imprescindible apostar por la protección para asegurar que proteger el Big Data compartido en la nube empresarial no sea objetivo de ataques; y, por último pero no menos importante, la necesidad de trabajar cada día para que nuestras tecnologías estén preparadas para luchar contra las últimas amenazas del cibercrimen".

En definitiva, los retos son múltiples y es que como señala Eva Cuadrado Díaz, responsable del centro de competencia de seguridad en Connectis, "los retos a los que se enfrenta el mercado de la ciberseguridad son múltiples, pero quizá uno de los principales retos sea conseguir soluciones inteligentes que ayuden a interconectar los diferentes productos de seguridad existentes dentro del cliente, consiguiendo una protección más eficiente".

ATAQUES

Como hemos visto, los retos son numerosos. Pero, actualmente, ¿cuáles son los principales ataques que se está produciendo? La amenaza de los ataques cibernéticos seguirá incrementándose a medida que los datos globales se multipliquen y aumente la cantidad de dispositivos conectados/puntos de entrada. De hecho, en 2014, y según Forbes, las empresas notificaron un incremento anual del 48 % en los ataques cibernéticos realizados en sus redes. No obstante, las infracciones de seguridad o las pérdidas de datos también pueden ser producto de amenazas internas a impresoras inseguras. Por ejemplo, el robo de documentos confidenciales de las bandejas de salida, o la recogida accidental de los mismos por parte de las personas equivocadas. Desde la vcompañía Barracuda, su máximo responsable, Miguel López afirma que "el ingenio de los ciberdelincuentes no conoce límites y los ataques pueden dirigirse a casi cualquier entorno". Para este directivo, cabe destacar tanto por el volumen de ataques producidos como por el impacto y daños generados las siguientes superficies de ataque:

- Correo Electrónico: es la principal vía de comunicación y de entrada y salida la organización y por tanto el más explotado. Spam y Ramsomware no dejan tregua a este elemento. Es necesario contar con filtros avanzados de Antispam, antimalware (incluyendo Ramsomware, por supuesto) y protección frente a links maliciosos y Amenazas Avanzadas. La formación a los empleados es también un elemento crítico en este entorno.

- Navegación web de los empleados: Otra ventana al exterior en la que es necesario establecer medidas de protección de última generación que permitan la inspección no sólo del tráfico http tradicional sino del creciente trafico https, mensajería, redes sociales… Es necesario contar aquí con herramientas que incluyan filtros antimalware y frente a Amenazas Persistentes ya que los contenidos dañinos pueden encontrarse hoy día en páginas legítimas en las que normalmente se confiaría.

- Servidores Web corporativos: esta es una de las vías de ataque más utilizadas en los últimos años y, sin embargo, sigue estando en muchos casos totalmente desprotegida. La falsa creencia de que los cortafuegos de nueva generación son capaces de proteger nuestros servidores web le ha costado a muchas empresas enormes daños por robo de información, caídas de servicio, desfiguraciones de su página y caída en su reputación.

Sin embargo, "Más que hablar de dónde se están produciendo los ataques, deberíamos hablar de los métodos para conseguir dinero a través del cibercrimen. No olvidemos que, el principal objetivo de los ataques, es conseguir un beneficio económico por parte de quien los acomete. En este sentido, es común pensar que para obtener mucho dinero has de atacar a grandes organizaciones (banca, seguros, sector industrial…) pero la realidad es que, en muchas ocasiones, es más sencillo atacar a pymes que superan en

número a las grandes empresas y, por regla general, están más desprotegidas, lo que les reporta mejores resultados. Y así lo demuestra el auge del ransonware del tipo cryptolocker, entre otros", afirma Ricardo Maté, director general de Sophos.

COSTE

Visto lo visto, cada vez es más imprescindible establecer una política de seguridad. El problema es que, sobre todo en los entornos de las pequeñas y medianas empresas, la seguridad no se ve todavía como un problema y por tanto, no se invierte en seguridad, sino que se gasta en seguridad. Es cuando se sufre un ataque cuando, las compañías comienzan a plantearse el establecimiento de estas políticas.

Lo que está claro es que establecer políticas de seguridad tienen un coste y esa inversión puede hacer que para una determinada empresa sea elevada con lo que determinados proyectos no saldrán adelante. Josep Albors, director del laboratorio de ESET, no cree que el coste sea un elemento disuasorio a la hora de elaborar un proyecto. En su opinión, "si se hace de forma planificada y pensando en esta implantación como una medida que garantice la continuidad de proyectos presentes y futuros, el coste pasa a un segundo plano cuando se comprueban los beneficios que aporta una política de seguridad eficiente". En la misma línea se sitúan en HP Inc. Desde la multinacional norteamericana consideran que "ni mucho menos el coste puede ser un elemento que influya. Además, si se tiene en cuenta las pérdidas económicas que podría sufrir la empresa si le robasen información confidencial, ese presupuesto inicial para implantar la política de seguridad quedad totalmente seguro". Finalmente, Raúl Núñez, experto en Ciberseguridad y Network Defense de Trend Micro cree que "por lo general, en el mercado de la seguridad siempre se ha invertido de manera reactiva, es decir, cuando se ha sufrido el problema es cuando se valora la inversión en seguridad que debe hacer una empresa. Tenemos que tener en cuenta que no es solo la adquisición de las protecciones, sino también el coste asociado a la implementación y puesta en marcha de dicha política. Sin embargo, esta visión es cortoplacista y supone que la seguridad se ve como un gasto. Afortunadamente, y debido a los ataques que se están produciendo en la actualidad y a las pérdidas económicas y de reputación para las empresas, se está empezando a percibir un cambio de mentalidad, es decir, ahora cada vez más la seguridad se percibe como parte estratégica para el buen funcionamiento de un negocio y por tanto, se tiene en cuenta en los planes iniciales. En definitiva, se está empezando a percibir la seguridad como una inversión. Tengamos en cuenta que nunca empezaríamos una casa por el tejado… lo mismo debe ocurrir con la seguridad en las empresas, debe estar en la base del negocio integrada con el resto de estrategias".

CONCIENCIA DE LOS RIESGOS

Tal y como se señala desde SonicWall y según el informe de de Osterman Research sobre las mejores prácticas de 2016 de para tratar el phishing y el ransomware, sólo el 27% de las organizaciones encuestadas no habían experimentado un incidente de ciberseguridad en los últimos 12 meses y muchos habían sufrido múltiples ataques de diferentes tipos en ese período. El mismo informe también estimó un aumento de más del 10 por ciento en los presupuestos de seguridad cibernética para las empresas en 2017 en comparación con el año anterior, ya que los ejecutivos y miembros de la c-suite se preocupan más por amenazas cibernéticas avanzadas y vectores de ataque. A medida que el coste de caer víctima de un ciberataque logre una mayor visibilidad en la comunidad internacional, esperamos que las empresas adopten un enfoque aún más proactivo para asegurar sus infraestructuras TI.

Desde HP Inc. se señala que "durante los últimos meses hemos sido testigos de cómo varios ciberataques masivos han inutilizado las páginas webs de grandes compañías, considerándolos como los más graves de la última década al afectar a más de mil millones de clientes en todo el mundo. Hay que añadir que en los últimos años, Estados Unidos ha sufrido varios ataques informáticos significativos. El departamento de Seguridad Nacional de Estados Unidos ha informado de que los hackers están utilizando un nuevo sistema para infectar routers, impresoras, televisiones inteligentes y todo tipo de objetos conectados con un malware que los convierte en una especie de "ejército robot". Con todo ello, podemos afirmar que la ciberseguridad se ha convertido en una de las prioridades tanto para los organismos gubernamentales como para las compañías". Por su parte, Alejandro Solana, EMEA Networking and Security Practice Manager de VMware, afirma que "ninguna compañía quiere aparecer en los titulares después de un gran escándalo de seguridad, por lo que sería lógico que las estrategias de ciberseguridad de las empresas funcionen como máquinas bien engrasadas. Pero parece que no es así según las conclusiones de un estudio realizado por The Economist Intelligence Unit (EIU) y patrocinado por VMware. El estudio ha descubierto que una desconexión sistemática entre los ejecutivos de nivel C y los responsables de tecnología de las empresas… una división que puede poner en peligro la seguridad de la organización. Este ciberabismo debe ser resuelto por ambas partes. Los ejecutivos necesitan entender mejor la vulnerabilidad de sus negocios, y en particular como las amenazas pueden crecer. El equipo de TI necesita alinearse con los ejecutivos para tener una mejor panorámica de la estrategia de seguridad. Finalmente, la función de la seguridad debe gestionar las expectativas sobre el presupuesto destinado a la ciberdefensa o adoptar soluciones más flexibles y de menor coste".

LA CLAVE ESTÁ EN EL USUARIO

La mayor brecha se encuentra en el usuario. Como afirman desde CA, "el eslabón más débil en la cadena de seguridad suelen ser los propios usuarios/empleados. Típicamente, los ataques y brechas de seguridad se producen con credenciales válidas de usuarios existentes y, una vez dentro de los sistemas, se llevan a cabo mediante diferentes técnicas los intentos de elevación de privilegios para conseguir acceso de administrador (usuarios privilegiados).

Por este motivo, en seguridad se debe aplicar los conceptos de

defensa en profundidad (defense in-depth) y mínimo privilegio (least privilege) aplicando diferentes capas de protección. En el primer nivel o capa se sitúa una correcta gestión de los usuarios y sus accesos".

El eslabón más débil de la cadena debe empezar a convertirse en el elemnto sobre el que las brechas se reduzcan y para ello es fundamental la formación para que esta circunstancia cambie. En este sentido, Manuel Cubero, Director Técnico de Exclusive Networks, "la educación y concienciación de los usuarios es una asignatura que aún está pendiente en muchas empresas y que claramente no se está abordando con el suficiente éxito. Además de este primer paso, se deben mejorar los sistemas de protección de los puestos de trabajo y apostar por las nuevas soluciones que abordan las problemáticas actuales con eficacia. Al igual que las amenazas evolucionan las defensas también deben hacerlo y proporcionar herramientas que interfieran lo menos posible en el trabajo de los usuarios, que nos garanticen tasas de éxito más elevadas frente a ataques nuevos y que aporten estrategias de contingencia y remediación rápida en el caso de que alguno de los puestos de trabajo se hubiera visto afectado por el ataque.

RANSOMWARE CIFRADO DESDE RUSIA

El ransomware cifrado, un tipo de malware que cifra los archivos de sus víctimas y solicita un rescate a cambio de recuperarlos, es uno de los tipos de malware más peligrosos en la actualidad. De acuerdo con la telemetría de Kaspersky Lab, en 2016 más de 1.445.000 usuarios (incluidas empresas) de todo el mundo fueron víctimas de este tipo de malware. Para entender mejor la naturaleza de estos ataques, los analistas de Kaspersky Lab han examinado el mercado sumergido de cibercriminales de habla rusa. Una de las principales conclusiones es que el incremento observado en estos últimos años en el ransomware cifrado es el resultado de un ecosistema clandestino muy flexible y atractivo, que permite a los criminales lanzar sus campañas sin necesidad de grandes conocimientos informáticos ni recursos financieros.

Los analistas de Kaspersky Lab han identificado tres niveles de participación delictiva en el negocio del ransomware:

- Creación y puesta al día de nuevas familias de ransomware.

- Desarrollo y soporte de un programa de afiliados de distribución de ransomware.

- Participación como asociado en un programa de afiliados.

El primer nivel exige que un participante tenga conocimientos informáticos avanzados para escribir los códigos. Los cibercriminales que crean los primeros renglones del nuevo ransomware se colocan a la cabeza de este mundo clandestino, ya que son los creadores de los elementos clave del ecosistema.

En el segundo peldaño se sitúan los desarrolladores de los programas de afiliados, integrado por las comunidades de cibercriminales que, con la ayuda de diferentes herramientas, como el spam malicioso o los exploit kits, distribuyen el ransomware recibido de sus creadores.

Los socios del programa de afiliados se sitúan en el nivel más bajo del sistema. Utilizando diferentes técnicas, ayudan a los programas de afiliados a distribuir el malware a cambio de un porcentaje de los rescates pagados. Sólo con mostrar interés, voluntad de llevar a cabo acciones ilegales y el pago de un par de bitcoins, es suficiente para participar en un programa de afiliados.

De acuerdo a las estimaciones de Kaspersky Lab, los ingresos diarios de un programa de afiliados pueden llegar a alcanzar decenas, cientos o miles de dólares, de los cuales el 60% es el beneficio neto que se queda en los bolsillos de los cibercriminales.

Durante su análisis del ecosistema clandestino y de las múltiples operaciones de respuesta a incidentes, los analistas de Kaspersky Lab identificaron varios grupos de cibercriminales de habla rusa especializados en el desarrollo y distribución de ransomware cifrado. Estos grupos pueden llegar a agrupar decenas de participantes, cada uno con su propio programa de afiliados, y la lista de sus objetivos incluye no sólo a usuarios de internet, sino también pequeñas y medianas compañías, e incluso alguna de gran tamaño. Inicialmente con el objetivo puesto en usuarios y entidades rusas y de la Comunidad de Estados Independientes (CIS), estos grupos están virando su interés hacia compañías ubicadas en otras partes del planeta.

"Es difícil explicar por qué muchas de las familias de ransomware tienen un origen ruso, pero sí estamos observando que se está evolucionando desde grupos pequeños, con recursos y capacidades limitadas, a grandes empresas cibercriminales capaces de atacar objetivos más allá de Rusia. No es algo nuevo. Ya hemos visto el mismo recorrido en grupos de malware financiero, como Lurk. Primero empezaron con ataques masivos a usuarios de banca online para luego evolucionar a grupos sofisticados capaces de atacar y robar a organizaciones mucho más grandes. Por eso hemos creado esta sinopsis: las bandas de ransomware se están convirtiendo en unos enemigos peligrosos, y para el público y la comunidad de seguridad es realmente importante que lleguemos a aprender lo máximo posible", dice Anton Ivanov, analista de seguridad de Kaspersky Lab y autor de este resumen.

Remediación que permita volver al estado anterior de la máquina y que permita que el usuario pueda seguir trabajando en pocos minutos después del incidente". En la misma línea de impulso de la formación se sitúa Ángel Victoria, country manager de G DATA para quien "una formación básica y regular, que no necesariamente tiene que suponer una gran inversión de tiempo, puede convertir al empleado en la mejor barrera contra el malware. Algunos fabricantes ya estamos intentando concienciar en este sentido y colaborar con nuestros clientes en estos procesos, si es necesario".

Para Ricardo Maté de Sophos, "la formación y concienciación en materia de seguridad ha de ser continua, pero quizá estemos equivocándonos en la forma de educar, más que en el fondo. Si logramos que el usuario o empleado comprenda las consecuencias de un fallo de seguridad, obtendremos mucho mejor resultado que si únicamente le hacemos leer interminables manuales sobre buenas prácticas en seguridad".

LA NUBE

Hemos visto el creciente uso de aplicaciones de almacenamiento en la nube desde 2015, con el tráfico total aumentando de 88.000 billones a 126.000 billones en 2016. Dado que el cifrado SSL / TLS abarca todas las interacciones de servicio en la nube, podemos decir que esto contribuye significativamente al riesgo de que amenazas cifradas se infiltren en el entorno TI de la empresa. Sin embargo, existen ventajas y desventajas para las opciones de almacenamiento interno y en la nube. La información almacenada internamente no requiere conexiones de tráfico a través de Internet y, por lo tanto, reduce los posibles vectores que los hackers pueden utilizar para acceder al sistema. Sin embargo, las empresas en general no tienen presupuestos significativos para gastar en la gama alta de servicios de seguridad de la red y como tal, sus datos son más vulnerables debido a un menor nivel de protección. Los servicios en la nube, por otro lado, tienen los recursos para asegurar que los datos se mantengan seguros con los mejores y más recientes productos y protocolos de seguridad, pero el uso de transmisiones cifradas de Internet, junto con la mayor visibilidad del centro de datos desde la perspectiva de atacantes externos, da lugar a ataques e intentos más frecuentes de infiltrarse en el mainframe. Como los ciberdelincuentes a menudo trabajan con el objetivo de atacar a los objetivos más fáciles y más rentables, las empresas deben asegurarse de que sus datos se almacenan detrás de firewalls fuertes y actualizados, así como de sistemas de monitoring en instalaciones anóni-

mas para proporcionar la máxima protección.

La nube y los servicios basados en ella aportan muchos beneficios que son difícilmente replicables fuera de la misma, pero no hay que olvidar que esta nueva tendencia también conlleva que la superficie de exposición de una empresa aumente exponencialmente. Es por ello que se debe poner especial foco en la seguridad y sobre todo adoptar medidas específicas y orientadas a este nuevo entorno. Además del control y visibilidad que aportan las nuevas herramientas de CASB (Cloud Access Security Broker) no debemos olvidar que lo que realmente importa son los datos e información que subimos a la nube. Por esta razón, estrategias centradas en el control del dato, su identificación, clasificación y el cifrado de los mismos, son las soluciones más eficientes ante un robo de datos en infraestructuras de cloud. Manuel Cubero, Director Técnico de Exclusive

¿SERÁ ESTE EL AÑO EN QUE LAS CIBERAMENAZAS A IOT SE CONVERTIRÁN ALGO GENERALIZADO?

Ed Cabrera, Chief Cybersecurity Officer, Trend Micro

Hay un antes y un después en la forma en que vivimos y trabajamos, y este punto está marcado por Internet de las Cosas (IoT). Nos hace más productivos, saludables y felices, y permite a las empresas trabajar de manera más inteligente, eficiente y con mayor agilidad. Solo hay un problema: desde la perspectiva de ciberseguridad, los dispositivos IoT son básicamente defectuosos. Y los chicos malos están consiguiendo bastantes buenos resultados explotándolos.

Ante el boom del IoT, este año podríamos ver una avalancha de nuevos ataques dirigidos no solo a los dispositivos inteligentes de consumo, sino a los entornos IoT industriales. Estos sistemas pueden pertenecer a mundos diferentes, pero el efecto que los compromisos pueden tener en las empresas objetivo podría ser igualmente devastador.

Si 2016 fue el año en que las botnets impulsadas por IoT se convirtieron en una gran noticia, entonces, lo lógico, sería que en los próximos doce meses fuéramos testigos de cómo esta tendencia finalmente se generaliza y se convierte en algo predominante. Después de que el código fuente del perverso malware Mirai se hiciera público el año pasado, no pasó mucho tiempo antes de que los black hats lo utilizaran para probarlo en dispositivos domésticos inteligentes, optando por aquellos con nombres de usuario y contraseñas predeterminados. Entonces lograron comprometer tales dispositivos en decenas de miles de unidades para crear botnets capaces de lanzar algunos de los mayores ataques DDoS jamás vistos. Uno supuestamente dejó fuera de línea durante un breve espacio de tiempo a la nación africana de Liberia. El más notable se dirigió a la firma de DNS, Dyn, que tuvo un efecto llamada devastador, arrastrando a sus clientes –entre algunos de ellos se encontraban los más grandes y conocidos de la web. Twitter, Reddit, Spotify y SoundCloud estaban entre los afectados.

Los ciberdelincuentes seguirán aprovechando este año las vulnerabilidades básicas de seguridad en los dispositivos de consumo como cámaras web y DVR para crear botnets DDoS. Después de todo, la reacción tibia e indiferente ante Mirai entre la comunidad de proveedores ha demostrado que siempre habrá dispositivos vulnerables que se puedan explotar. Los sitios políticos, los basados en servicios, noticias y los corporativos estarán en el punto de mira de los hacktivistas y los atacantes que tengan motivaciones económicas y que se valen de botnets DDoS.

En el otro extremo del espectro, la probabilidad de que aumenten los ataques altamente dirigidos para comprometer sistemas IoT industriales (IIoT), como los que ya se han registrado en compañías del ámbito de la fabricación y energía, es muy grande. Una vez más, el precedente ya se ha establecido. Las centrales eléctricas ucranianas vieron interrumpida su actividad en diciembre de 2015 y en 2016 tras ser víctimas de ataques relativamente sofisticados, dejando con ello a mucha gente sin electricidad.

El riesgo aquí no radica necesariamente en la pérdida de datos, sino en un daño físico muy real, porque el IIoT se encuentra en la intersección del mundo físico y el virtual. Hackea un coche conectado y podrías causar un problema nunca visto en una autopista. Corta con éxito el suministro de una central eléctrica en medio del invierno y quién sabe qué podría sucederles a los ciudadanos que no puedan calentar sus hogares.

Desafortunadamente, también en este plano los productos en sí mismos son terriblemente vulnerables a un ataque. De hecho, las vulnerabilidades en los sistemas de control y adquisición de datos (SCADA) comprendieron casi un tercio (30%) del número total de vulnerabilidades encontradas en 2016.

Entonces, ¿qué podemos hacer? Podemos tratar de aumentar la concienciación en materia de seguridad entre los consumidores y fabricantes, con el fin de no ponérselo tan fácil a los cibercriminales y reducir sus posibilidades. Mientras que desde el punto de vista industrial, los responsables de seguridad siempre deben tratar de mantener los sistemas de misión crítica parcheados y actualizados, y donde sea posible, dejar los menores huecos posibles a una circulación de Internet más amplia. Además, conviene asegurarse de tener un IPS de red en las instalaciones para detectar y bloquear paquetes de red maliciosos.

Y mientras el año transcurre, una cosa sí es segura. todos vamos a tener que arrimar el hombro para mitigar la creciente amenaza de la seguridad IoT.

PROTEGER LA RED: UN IMPERATIVO

Jose Tormo, regional managing director de Aruba, una compañía de Hewlett Pakard Entreprise

Benjamin Franklin decía: 'Cuando hayas acabado de cambiar, estarás acabado'. Ésta es una buena enseñanza para la vida, pero también válida para la forma en la que abordas la seguridad de los datos corporativos y cómo cumplir con las expectativas de los trabajadores en la era de la conectividad en cualquier momento y lugar.

Si echamos un vistazo al pasado reciente, los empleados tenían que cambiar la manera en que trabajaban para adaptarse a la tecnología que les aportaba su departamento de TI corporativo. Ya no es así.

La tecnología de los negocios ahora se mueve al son de un nuevo tambor: el de la "siempre-conectada" generación #GenMobile. Los empleados más jóvenes hoy, nativos digitales, siguen cambiando el modo en que operan las compañías, comportándose de una manera que tiene un amplio alcance en la seguridad de la red corporativa. En paralelo a esta situación, es conveniente saber que igual que ha cambiado el perfil del empleado móvil también lo ha hecho el perfil del ciberdelincuente que, lejos del saboteador o hacktivista que perseguía llamar la atención, ataca a compañías y organizaciones a través de una estructura empresarial propia muy organizada, contando con potentes infraestructuras, y con planes estudiados. Hoy los ciberdelincuentes son adversarios racionales, con objetivos muy específicos.

En un contexto como el actual, en el que los ciberdelincuentes tienen más fácil atacar a una sociedad cada vez más conectada, en la que existe un gap entre la innovación y la preparación eficiente para dar respuesta a los ataques, se impone la necesidad de apostar por soluciones creativas basadas en la última tecnología.

Agitemos la coctelera en la que tenemos una #GenMobile, que exige altos niveles de conectividad en su entorno profesional, con el fenómeno del BYOD, añadamos un poco de IoT y tendremos un escenario potencialmente peligroso para la protección eficaz de los datos corporativos de las empresas. Y todo ello en un contexto en el que los máximos niveles de conectividad, la movilidad y la colaboración, se imponen en aras de la eficiencia, la competitividad, la felicidad de los empleados y de la retención del talento.

Según Gartner, en 2016 hubo unos 6.400 millones de aparatos conectados en el mundo, un 30% más que en 2015 y la consultora prevé que haya más de 300 millones de terminales de automatización de edificios y más de 400 millones de dispositivos para la gestión energética en edificios en 2020.

Las cifras pueden ser abrumadoras si tenemos en cuenta que, aunque los ataques de DNS pudieran parecen algo del pasado, para un ciberdelincuente lanzar un ataque de 650 gigabytes por segundo, tiene un coste aproximado de 5 dólares a la hora, en tanto que para una empresa, defenderse de un ataque de ese tipo tiene un coste aproximado de 40.000 dólares. Ante tal asimetría entre los gastos de ataque y los costes derivados de la defensa de las organizaciones, están proliferando los ataques a empresas que son chantajeadas reiteradamente. Con una ciberdelincuencia organizada y ante la explosión de los dispositivos de IoT que ya se están conectando a las redes empresariales es crítico -a través de tecnologías que garanticen la seguridad y mantengan a raya las amenazas- identificar, conectar y proteger de manera óptima todos los dispositivos móviles y de IoT desconocidos, algo a tener muy en cuenta al idear respuestas de seguridad eficientes. Para hacer frente al desafío, es clave poner en marcha estrategias que satisfagan los requisitos de las empresas a la hora de identificar, conectar y proteger todos los dispositivos del IoT. La tendencia pasa por adoptar soluciones mixtas de software y hardware, y por ser capaces de integrar a las líneas de defensa las soluciones de un ecosistema de partners que contribuya a adoptar y mantener a salvo las iniciativas de movilidad, de incorporación de dispositivos de IoT, sin comprometer las crecientes demandas del personal #GenMobile. Por eso, estamos convencidos de que la mejor estrategia para la ciberseguridad de las empresas pasa por incorporar soluciones que permitan el descubrimiento y el reconocimiento automático de todos los dispositivos IP (gestionados, no gestionados y de IoT) conectados a través de redes inalámbricas o cableadas y con múltiples proveedores.

Contar con este tipo de soluciones permite a las organizaciones ver claramente cuántos dispositivos en total y de qué categorías están conectados en cualquier momento. Además, el departamento de TI ya no tendrá que "adivinar" o utilizar herramientas dispares para ver qué dispositivos se están conectando a sus redes.

Las compañías necesitan incluir entre sus activos para la defensa de sus redes, soluciones que les proporcionen información completa sobre el tipo de dispositivo, el sistema operativo, el estado y la ubicación, que ha de mostrarse en una interfaz gráfica fácil de leer. Esta información se puede utilizar para optimizar el rendimiento y la seguridad de los componentes de infraestructura y, a continuación, compartirla para proporcionar un análisis de comportamiento del usuario, contrainteligencia y seguridad de firewall. De este modo, los dispositivos que exhiban un comportamiento no deseado pueden ser puestos en cuarentena de forma automática para minimizar el riesgo para la red. Por todo, la ciberseguridad no es un tema menor, y es algo que no ha tenido hasta ahora un crecimiento acorde con la complejidad y el tamaño que ya ha adquirido la presencia de dispositivos de IoT. A partir de ahora, será necesario reflexionar profundamente sobre este particular, y dejar de considerar que un dispositivo es seguro tan sólo porque está funcionando para empezar a considerar que necesita un control más allá del simple mantenimiento como aparato.

Networks afirma que, “no es fácil resistirse a todos los beneficios que aporta la nube o tener centros de datos distribuidos. Si bien es cierto que la superficie de exposición aumenta, también lo hacen nuestras capacidades y flexibilidad en la movilidad y compartición de datos. En cualquiera de los casos, a día de hoy no debería ser un problema poder convivir con infraestructuras tradicionales y de cloud. De hecho, han surgido muchos y buenos productos de seguridad que centran sus esfuerzos en combatir las amenazas especialmente diseñadas para atacar el cloud”.

INTERNET DE LAS COSAS

Se trata de un elemento clave de la seguridad actual, pero sobre todo de la seguridad futura. El hecho de que muchos dispositivos, ya instalados, se heyan desarrollado sin introducirles ninguna medida de seguridad es un riesgo que está alarmando a los principales actores de este mercado. Para el portavoz de SonicWall, “para evitar que los dispositivos IoT sean víctimas de un ataque DDoS, hay que asegurarse de que sus dispositivos estén detrás de un firewall de nueva generación que escanea el malware específico de IoT, como Mirai. También es fundamental separar todos los dispositivos IoT en una zona propia del resto de la red en caso de que el dispositivo se vea comprometido”. Por su parte, desde Trend Micro, se afirma que “”Vivimos en un mundo que está hiperconetado y tenemos que tener en cuenta que los sistemas se crean inicialmente para dar facilidades y no pensando en la seguridad. Debemos de ser conscientes de que cualquier servicio que esté expuesto a Internet se debe proteger. En Trend Micro somos conscientes de esto y trabajamos por cubrir todas y cada una de las superficies de ataque”.

El responsable de Exclusive Networks considera que IoT supone un serio riesgo. En su opinión, “la carencia de seguridad en los dispositivos IoT cada vez se está haciendo más evidente. La primera recomendación es hacer un análisis de riesgos para determinar los posibles problemas derivados de una brecha de seguridad en ellos y su impacto. Su aislamiento no es una solución, porque podría dejar de tener sentido tenerlos en producción. Por suerte ya hay soluciones comerciales que han centrado sus esfuerzos de desarrollo en la protección de este escenario y ofrecen al mercado productos que aportan la capa de seguridad necesaria a este segmento de dispositivos. A grandes rasgos, lo primero que estas herramientas deben ofrecer es visibilidad para poder inventariar e identificar los dispositivos, de manera eficaz, ofrecer métodos de conexión segura entre dispositivos y con otras redes y, para terminar, una capa de gestión optimizada para un gran número de elementos y con capacidades de automatización y orquestación con otras herramientas”. Por su parte, el portavoz de Sophos asegura que “en el mundo actual en que todo está conectado las amenazas se han multiplicado y ampliado su espectro. No solamente hablamos de IoT, sino de cualquier dispositivo que hoy en día conectamos tanto en casa como en el trabajo, es susceptible de ser atacado con mayor o menor facilidad y con mayor o menor riesgo para usuario y sus datos. La seguridad empieza en casa, más del 90% del spam emitido a nivel mundial se envía a través de nuestros dispositivos domésticos, una gran mayoría de los ataques DDoS también se realizan a través de estas redes bots de usuarios domésticos. Por eso Sophos pone a disposición del público general Sophos Home, nuestra herramienta gratuita para casa, el mismo motor de protección para grandes empresas puesto a disposición de los usuarios domésticos. Respecto a los dispositivos IoT, como cualquier otro dispositivo conectado a Internet, desde Sophos queremos que los usuarios entiendan los riesgos. No consiste en estar en contra de su uso, ni mucho menos, pero una buena práctica cuando vas a adquirir alguno de estos dispositivos, sería tomar un tiempo en revisar la configuración de seguridad de los mismo”.

Finalmente desde GData se asegura que en el terreno de IoT se asegura que en este terreno, “entra en juego la seguridad by design. Esto significa que la seguridad debió valorarse en el momento en que la cosa era tan solo una idea, un proyecto, un borrador y que es tan importante como la función que da sentido al propio dispositivo. Respecto a las cosas inseguras que hoy en día se conectan a Internet se puede hacer poco. Actualizarlas con parches de seguridad, en la medida en que sea posible. Y si no lo es, hay que sustituirlas por una nueva generación que corrija sus deficiencias”.

Equipos híbridos para el ámbito de los negocios

A continuación te ofrecemos una selección de once dispositivos móviles híbridos y a la última, que combinan lo mejor de los ordenadores portátiles y las tabletas.

Si existe una categoría de producto que ha protagonizado una importante evolución, esa es la de los ordenadores portátiles, máquinas que despiertan un interés especial en el mundo de los negocios ya que permiten a los trabajadores 'llevarse la oficina' en sus desplazamientos. Dentro de la misma, cada vez están adquiriendo un mayor protagonismo los llamados híbridos, equipos que integran en una sola propuesta las características más atractivas e interesantes de los portátiles y las tabletas.

La siguiente selección arroja una radiografía bastante completa acerca de las últimas tendencias en este campo, pues no todos los híbridos presentan el mismo diseño o estructura. Es cierto que la tendencia refleja que es posible combinar ligereza a la par que resistencia, ahora bien ¿qué diferencias encontramos? Algunos fabricantes como HP, Lenovo, Dell o Toshiba apuestan por pantallas de 360º capaces de adoptar distintas posiciones o modos de uso. Otros, en cambio, lo que hacen es acoplar un teclado magnético a la pantalla para que el usuario lo mantenga o lo quite según sus necesidades. Este es el caso, por ejemplo, de Acer, Fujitsu, Samsung y Asus. Los casos de Apple y Microsoft son especiales porque ambas firmas han desarrollado para sus tabletas (iPad Pro y Surface Pro 4 respectivamente) diferentes accesorios entre los que se encuentran las llamadas fundas-teclado y que hay que adquirir por separado. Panasonic, con su Toughbook CF-20, también admite varias posiciones y queremos tratarlo de manera independiente ya que se trata de un híbrido marcadamente profesional para actividades al aire libre y que quizás se aleja un poco de la imagen que estamos habituados a ver en las grandes superficies comerciales, sobre todo en lo que a estética se refiere pues es una auténtica máquina todoterreno.

Cada una de estas once propuestas, dadas sus características, satisface las necesidades de los usuarios móviles y quizá el precio sea el factor que determine una u otra elección. Procesadores a la última, unidades de estado sólido, avanzadas pantallas, puertos de carga más veloces, autonomías cada vez superiores y opciones de seguridad mejoradas son algunos de sus atractivos más interesantes.

Acer Switch Alpha 12

La clásica ranura de ventilación se ha sustituido por un sistema de refrigeración eficiente que mejora su comportamiento, prometiendo una autonomía de ocho horas. El teclado se separa de manera fácil de la pantalla que, además, cuenta con soporte estable y ajustable.

De la mano de Acer, llega este modelo convertible pensado para diferentes usos: educación, hogar y trabajadores también gracias a características como TPM (Trusted Platform Module), lo que garantiza un uso mucho más seguro. Pantalla y teclado juntos alcanzan un peso de 1,250 kg, pero si separamos este último elemento para manejarlo como tablet entonces el peso de sitúa en 900 gr, cifras que en ambos casos facilitan su cómodo transporte en cualquier situación. A este respecto, el teclado se conecta y desconecta mediante unas bisagras magnéticas que se ajustan ergonómicamente, disponiendo de un trackpad que por dimensiones es cómodo. La firma sugiere dos posibles opciones: una estándar y otra con retroiluminación para situaciones con escasa luminosidad.

Entrando en detalle en sus prestaciones, el equipo de desarrolladores de Acer ha integrado LiquiqLoop. Se trata de un sistema de refrigeración que prescinde del ventilador y libera a la máquina de los problemas derivados de la acumulación de polvo, flujo de aire o ruido generado. Este mismo sistema es el que va a permitir permite que funcione de manera más eficiente y que alcance una temperatura estable.

Switch Alpha 12 emplea la interfaz gráfica Continuum para utilizarse como un portátil con Windows 10 y como tableta con las funciones plenas de un ordenador, virtualmente en cualquier sitio. En este caso, se ha recurrido a un soporte en forma de 'U' y un diseño antideslizante que mantiene la pantalla boca arriba cuando se toca o se escribe sobre ella, pudiéndose ajustar hasta un ángulo de 165º. Dicha pantalla tiene un tamaño de 12 pulgadas, tecnología IPS, 2.160 x 1.440 píxeles de resolución y admite hasta 10 puntos táctiles de control. Sin embargo, y de manera opcional, es posible adquirir un lápiz activo que mejora el rendimiento y la escritura que resultará más fluida y precisa a la hora de plasmar un boceto o redactar notas.

En este caso, el usuario elige entre diferentes configuraciones técnicas. El procesador, por ejemplo, pertenece a la sexta generación de la serie Intel Core y puede ser un i3, un i5 o un i7 si se requiere de la máxima potencia.

Por su parte, la memoria RAM posee un tamaño de 4 u 8 Gb y la capacidad de almacenamiento SSD oscila entre los 128 y los 512 Gb. Otras características de interés son: webcam Full HD para videoconferencias, sistema de dos altavoces, tecnología Bluetooth 4.0, HDMI, DisplayPort, puerto USB 3.1 reversible de clase C capaz de alcanzar transferencias de datos de hasta 5 Gbps desde los periféricos conectados…

Su aspecto es el de un equipo moderno y a la última con una carcasa de aluminio anodizado y textura de superficie pulida. La batería llega a las ocho horas de uso.

Acer Computer Ibérica
Calle Disseny, número 3
08850 Gavà (Barcelona)
Teléfono: 934 92 24 00
Web: www.acer.es
Precio: Desde 999 euros

Toshiba X20W-D-10P

Su bisagra permite girar su pantalla táctil 360º, pudiéndose utilizar no sólo como portátil sino también como tableta o cuaderno de notas. Alcanza una autonomía de hasta 16 horas y con una carga de media hora disfrutamos de cuatro horas de uso ininterrumpido.

Hace tan sólo unas semanas que aterrizó en el mercado español el miembro más reciente de la familia Portégé de Toshiba. Se trata del convertible dos en uno X20W-D-10P, un dispositivo que puede utilizarse como portátil, tableta o cuaderno gracias a un lápiz óptico Wacom con soporte para la escritura manual y encriptación bajo la norma AES (del inglés Advanced Encryption Standard). Con un peso de 1,1 kg, posee una cubierta de magnesio en color azul ónice que combina con unas bisagras color oro que destacan por su alta resistencia. El teclado es retroiluminado y sus desarrolladores han apostado por una tecnología que detecta si un usuario apoya la mano en la pantalla, evitando que interactúe con ella al utilizarla como cuaderno de notas.

Su hoja de características técnicas revela la presencia de la séptima generación de procesadores Intel Core (serie U) para una potencia de procesamiento y rendimiento superior, una memoria RAM de 8 Gb y una unidad de almacenamiento de estado sólido de 256 Gb de capacidad. Mientras, la pantalla –que es antirreflectante- posee un tamaño de 12,5 pulgadas con una resolución de 1.920 x 1.080 píxeles. La presencia de la tecnología Corning Gorilla Glass 4 brinda un revestimiento anti golpes y caídas.

La seguridad cobra especial protagonismo en esta propuesta. Así, incluye un dispositivo SecurePad para que el usuario se identifique con su huella dactilar y una cámara IR para un reconocimiento facial, ambas opciones con soporte para los sistemas Intel Authenticate (protección de identidad por hardware) y Windows Hello, característica que comparte con otros modelos recogidos en este artículo. Pero, además, la BIOS de este Toshiba

X20W-D-10P, que ha sido diseñada y fabricada por la propia firma, arroja una capa adicional de seguridad que elimina los riesgos de interferencias de terceros. La presencia, por otro lado, de un módulo TPM 2.0 se enfoca a la encriptación de las comunicaciones y opciones de inicio de sesión más seguras.

La batería está preparada para aguantar cómodamente uno o incluso dos días de trabajo si tenemos en cuenta que la japonesa promete una autonomía de hasta 16 horas de uso. A este respecto, y gracias a su sistema de carga escalonada, con una carga de sólo media hora es posible disfrutar de cuatro horas de autonomía. El empleo de un sistema de refrigeración híbrida por aire le permite proporcionar un rendimiento pleno incluso en las condiciones más exigentes. ¿Cómo funciona este sistema? Mientras que la refrigeración trasera enfría el chasis y otros componentes de la máquina, la inferior sólo se encarga de la CPU.

Desde el punto de vista del audio, destacan sus altavoces estéreo Harman Kardon, capaces de adaptarse a la rotación de la pantalla y los diferentes usos que haga el usuario del equipo. Incluye un puerto USB 3.0 compatible con Sleep-and-Charge, cámara de infrarrojos con micrófonos duales para Windows Hello e Intel Authentica, y un puerto USB 3.1 de clase C con Thunderbolt.

Toshiba España
Parque Empresarial San Fernando
Edificio Múnich, 3ª Planta, Oficina A
Av. de Castilla, número 2
28830 San Fernando de Henares (Madrid)
Teléfono: 91 660 67 00
Web: www.toshiba.es
Precio: Desde 1813,79 euros

Apple iPad Pro

La aclamada tableta de Apple se convierte en ordenador portátil con la ayuda del teclado Smart Keyboard, a la venta en dos tamaños: uno para modelos de 9,7 y otro para los de 12,9 pulgadas.

En esta selección de portátiles híbridos hemos querido reservar un espacio a la tableta de la firma de la manzana, disponible en dos versiones: una con pantalla de 9,7 pulgadas y otra de 12,9 pulgadas. Estas dos mismas versiones son las que nos vamos a encontrar en el teclado Smart Keyboard, el complemento que sugiere Apple para convertir a su tablet en un ordenador portátil. Sin cables y sin interruptores, descubrimos un teclado completo y ligero de peso que acopla a través de la conexión Smart Connector para empezar a trabajar o disfrutar del ocio y el entretenimiento de manera mucho más cómoda. El accesorio Smart Keyboard también puede utilizarse como una funda de fino grosor.

El usuario tiene a su disposición -dentro de cada una de estas dos versiones- diferentes posibilidades y combinaciones. Así, por ejemplo, la capacidad oscila entre los 32 y los 256 Gb. Además, y junto a los modelos Wi-Fi, están los que combinan Wi-Fi + Cellular para hacer llamadas de teléfono y FaceTime con el plan de datos que se tenga contratado, o compartir la conexión.

La potencia y el rendimiento que proporciona el dispositivo de Cupertino se debe, en gran parte, a su chip A9X de 64 bits. Según datos facilitados por la propia firma, éste multiplica hasta por 1,8 el rendimiento de la CPU de su iPad Air 2. De igual forma, la potencia gráfica se duplica para disfrutar de efectos más reales, animaciones más fluidas, gráficos con mayor detalle… Mientras que el modelo de 12,9 pulgadas brinda la resolución más alta de un dispositivo iOS (2.732 x 2.048 ppp), el de 9,7 pulgadas deja sensaciones igual de buenas. Su panel Retina de 2.048 x 1.536 píxeles de resolución minimiza los reflejos y muestra un alto brillo. Asimismo, y como utiliza el mismo espacio de color que la industria del cine digital, exhibe una gama cromática más amplia y hasta un 25% más de saturación con respecto a versiones pasadas. Por otro lado, la presencia de la opción True Tone explica que los sensores de luz ambiental de cuatro canales -integrados en el propio dispositivo- ajusten de manera automática tanto los valores referidos al color como a la intensidad de la pantalla en función de la luz que haya.

Con una autonomía de hasta 10 horas, tampoco falta la tecnología Touch ID para utilizar la huella dactilar como contraseña y desbloquearlo, o realizar compras ya sea a través de la App Store, en iTunes o en iBooks. Desde el punto de vista del sonido, localizamos cuatro altavoces de alta fidelidad situados en cada una de sus esquinas. Como nota adicional, señalar que la tablet puede detectar cómo se sujeta para ajustar la orientación de las frecuencias altas a los altavoces de la parte superior.

En el apartado multimedia, las cámaras de ambas versiones resultan muy completas. Quizá, una de las prestaciones más interesantes sea la posibilidad de grabar vídeo en 4K con el modelo de 9,7 pulgadas.

Apple España
Teléfono: 900 812 703
Web: www.apple.es
Precio:
Modelo de 9,7 pulgadas: desde 679 euros; versión de 12,9 pulgadas: desde 899 euros
Smart Keyboard: modelo de 9,7 pulgadas 169 euros y para el de 12 pulgadas 179 euros

Asus Transformer 3 Pro T303UA

Este híbrido de 800 gr destaca por su diseño duradero, sistema de carga rápida y pantalla de 12,6 pulgadas y 2.880 x 1.920 píxeles de resolución. De manera opcional, es posible adquirir una base gráfica externa o un altavoz con sonido envolvente para sacarle mayor partido.

Nos encontramos ante un equipo fabricado de manera artesanal y cuya estructura -a pesar de ser ligera- ofrece resistencia, rigidez y solidez frente a los arañazos y las rozaduras. Para ello, sus creadores se han decantado por una aleación de magnesio y aluminio. Con un grosor de 8,5 mm y un peso inferior a los 800 gr, se comercializa en distintas combinaciones de color y dispone de un soporte integrado con bisagra mecánica que (por sus características) permite colocar la máquina en prácticamente cualquier ángulo. Además, contamos con una cómoda y práctica funda-teclado retroiluminada y panel táctil revestido de vidrio agradable al tacto.

A la cabeza de tus específicas técnicas se encuentran los procesadores pertenecientes a la sexta generación Intel Core, una memoria RAM de 16 Gb de tamaño y almacenamiento escalable hasta 1 Tb. La gráfica es integrada y la pantalla, con un tamaño de 12,6 pulgadas, brinda retroiluminación LED y una resolución de 2.880 x 1.920 píxeles, prestaciones que contribuyen a su calidad de visionado, nivel de detalle y representación de los colores. Precisamente, y para mejorar la experiencia visual, los ingenieros de la taiwanesa han introducido el modo 'Eye Care': gracias a él, la cantidad de luz azul dañina que emite la pantalla se reduce hasta un 30% por lo que los ojos quedan más protegidos y se evita su cansancio en espacios con poca luz. Otra de las tecnologías a mencionar es TruViVid que ha sido desarrollada por la propia Asus para incrementar la claridad y disminuir los reflejos hasta un 67%.

Asus Transformer 3 Pro T303UA proporciona una interfaz Thunderbolt 3 con tasas de transferencia de datos capaces de alcanzar los 40 Gbps a través de la interfaz USB-C, lo que permitiría utilizar dos pantallas 4K UHD externas.

Por otro lado, comentar que integra una tecnología de carga rápida que logra una carga hasta del 60% en una hora y una cámara frontal por infrarrojos que reconoce el rostro del usuario para un inicio de sesión seguro. Es posible controlar, de igual forma, el asistente digital Cortan con la voz. A este respecto, un micrófono de matriz reduce el ruido de fondo para captar la voz de la manera más clara posible, desde cualquier dirección y logrando el reconocimiento de voz y grabaciones con total precisión. ¿Y el sonido? Posee dos altavoces frontales a los que se suma una tecnología de amplificación y otra llamada SonicMaster Premium –a su vez con tecnología de Harman Kardon-que aprovecha la potencia resultante para arrojar un audio sin distorsiones a cualquier volumen

Como características complementarias, señalar que existe la opción de conectar una base gráfica externa (ROG XG Station 2) a través de la interfaz Thumderbolt 3 en el caso de añadir una tarjeta gráfica de sobremesa si, por ejemplo, se van a utilizar aplicaciones de realidad virtual o juegos de última generación. De igual forma, tenemos a nuestra disposición un dock universal con toda clase de puertos (LAN, VGA, HDMI, USB 3.0, USB-C y un lector de tarjetas); el altavoz bluetooth Audio Pod para un sonido envolvente virtual de 5.1; y el lápiz Asus Pen para tomar notas y trazar dibujos.

Integra una tecnología de carga rápida que logra una carga hasta del 60% en una hora y una cámara frontal por infrarrojos

Asus Ibérica
Carrer del Plom, número 5
08038 Barcelona
Teléfono: 932 93 81 54
Web: www.asus.es
Precio: Desde 999 euros

Dell XPS 13 2 en 1

Su principal reclamo está en la pantalla. De 13,3 pulgadas y 3.200 x 1.800 píxeles de resolución, prácticamente no tiene bordes. La bisagra de 360º de este equipo admite hasta cuatro posibles modos de uso.

Para el mundo de los negocios, Dell sugiere a sus clientes este convertible de 13 pulgadas con una pantalla amplia y de extremo a extremo, prácticamente sin bordes y a la que el fabricante se refiere como InfinityEdge. De esta manera, y en cuanto a características de diseño y estructura, ha logrado un dispositivo compacto, ligero y resistente al estar fabricado con aluminio mecanizado; fibra de carbono; revestimiento de cristal Corning Gorilla Glass NBT; y bisagras de que ayudan a potenciar su solidez y durabilidad.

Dell XPS 13 2 en 1 comparte con algunos equipos de su categoría la ya clásica bisagra de 360º de apertura que maximiza la productividad y las opciones de visionado gracias al uso de Continuum. A este respecto, el equipo admite hasta cuatro posiciones para adaptarse a las necesidades del usuario en cada momento. El modo Portátil está enfocado a la productividad y a la eficiencia en el trabajo, la utilización del correo electrónico, hojas de cálculo… En cambio, si queremos realizar una búsqueda rápida, una compra on line o desplazarnos a través de una lista de reproducción, la opción más acertada es el modo Tablet. El modo Atril, por otro lado, es la tercera posibilidad y permite colocarlo en posición vertical para, por ejemplo, mostrar una presentación. Finalmente, estaría el modo Plegado, con el que este portátil-tableta adopta la posición de un caballete.

Incorpora un diseño sin ventilador, lo que contribuye a un factor de forma más delgado (8 -13,3 mm) y al hecho de que se limita el exceso de calor y ruido para apostar por procesos más eficientes. Este producto se comercializa con la séptima generación de procesadores Intel (versión Core i5 o i7), procesadores que vienen equipados con un modo de energía dinámica y unidades de disco de estado sólido que permiten un arranque rápido. Otra novedad es que este equipo se lanza con Windows Inking (es el nombre de soporte para lápiz de Microsoft) y es compatible con Windows Hello, opción que proporciona diferentes maneras para la autenticación como pudiera ser el rostro o la huella dactilar.

Es el turno de la autonomía. En este caso, su duración varía en función de cómo se esté utilizando. Por ejemplo, con programas como Excel y Word se garantizan hasta 15 horas de uso, tiempo que en el caso de contenidos en streaming se rebaja a las 13 horas, lo que tampoco está nada mal. De manera opcional, es posible adquirir un adaptador híbrido y batería externa para disponer de un tiempo de ejecución extra de 11 horas.

En otro orden de cosas, señalar que ha sido provisto de un modo de energía dinámico que arroja una potencia de procesamiento extra en ráfagas cortas para las tareas más exigentes. El portátil XPS 13 2 en 1 incluye dos puertos USB tipo C, ambos compatibles con la funcionalidad de carga y visualización (de ellos, uno también soporta Thunderbolt 3).

Se comercializa con la séptima generación de procesadores Intel (versión Core i5 o i7), procesadores que vienen equipados con un modo de energía dinámica

Dell Computer
Calle de Basauri, número 17
28023 Madrid
Teléfono: 91 722 92 00
Web: www.dell.es
Precio: Desde 1.399 euros

Samsung Galaxy TabPro S

Con una pantalla de 12 pulgadas, 2.160 x 1.440 píxeles de resolución y tecnología Super AMOLED, incluye una funda con teclado.

Equipado con el sistema operativo Windows 10 y preparado para aunar las esferas del mundo personal y laboral, este dos en uno es un dispositivo de 693 gr de peso y 6,3 mm de grosor que cuenta con una práctica funda-teclado. A este respecto, hay que señalar que la bisagra incluida en el teclado ofrece dos posiciones entre las que elegir para que la visualización y la utilización del equipo resulte lo más cómoda posible. Ese teclado, además, incorpora un touchpad de generosas dimensiones y una clavija llamada Pogo que suprime la necesidad de emparejar o cargar por separado.

Samsung Galaxy TabPro S posee una pantalla de 12 pulgadas y 2.160 x 1.440 píxeles de resolución. Sensible al tacto, utiliza la tecnología Super AMOLED para ofrecer al usuario una experiencia de visualización mejorada gracias a dos puntos clave: un contraste más profundo y tonos más naturales que contribuyen a que la paleta de colores se represente con mayor viveza y con detalles más precisos.

Si atendemos a su hoja de especificaciones técnicas, encontramos que soporta el estándar de comunicaciones LTE Cat 6 para una conexión más rápida y que su centro neurálgico opera a las órdenes de la sexta generación de procesadores Intel Core M (Dual Core a 2,2 GHz), los cuales son capaces de alcanzar un consumo de sólo 4,5 vatios eliminando el ruido y aumentado a la vez la eficiencia en cada una de las tareas que hay que completar. En otro orden de cosas, Samsung ha perfeccionado la función referida a la carga de la batería (5200 mAh), la cual logra una autonomía de hasta 10,5 horas de uso con una carga de dos horas y media.

Con una memoria RAM de 4 Gb y una capacidad de almacenamiento de 128 Gb, incluye otras características de interés como Wi-Fi, Wi-Fi Direct, USB 3.1, NFC y tecnología Bluetooth 4.1. En lo que respecta al apartado multimedia, tanto la cámara frontal como principal tienen un sensor CMOS de 5 megapíxeles de resolución; esta última, de igual forma, dispone de autofocus. Los vídeos que se registran (admite los formatos MP4 y WMV) tienen calidad Full HD. Para audio, los archivos compatibles son: MP3, M4A, AAC, WAV, WMA y FLAC.

Aquellos usuarios interesados en mejorar la productividad de este equipo híbrido pueden adquirir de manera independiente dos complementos. Uno es un lápiz bluetooth y el otro es un adaptador multipuerto con soporte para HDMI y USB tipo A y C para unos tiempos de carga y de transferencia de la información ganen en agilidad.

Samsung Electronics Iberia
Parque Empresarial Omega
Avda. de Barajas, número 32
28109 Alcobendas (Madrid)
Teléfono: 91 714 36 00
Web: www.samsung.es
Precio: 999 euros

Soporta el estándar de comunicaciones LTE Cat 6 para una conexión más rápida y que su centro neurálgico opera a las órdenes de la sexta generación de procesadores Intel Core M

Fujitsu Stylistic R727

Con soporte integrado en su parte posterior, esta pantalla se transforma en un portátil para los negocios gracias al teclado magnético con el que se comercializa.

La compañía japonesa ha seleccionado para este artículo el dispositivo Stylistic R727. Se trata de una pantalla antirreflectante de 12,5 pulgadas y 1.920 x 1.080 píxeles de resolución que tiene la capacidad de transformarse-al igual que el resto de modelos partícipes-en un portátil que ofrece a los usuarios el rendimiento y la productividad que demandan. ¿Cómo pasar de un modo a otro? Conectando un teclado magnético que posee unas dimensiones compactas y proyecta una estructura sólida. Este miembro de la serie Stylistic se caracteriza, en otro orden de cosas, por los materiales elegidos para su fabricación y que aportan la durabilidad necesaria para el día a día: hablamos, una vez más, del aluminio y el magnesio. Con ellos se logran equipos que a pesar de ser ligeros no renuncian a la resistencia que se requiere y se pide.

Por otro lado, su conectividad a nivel empresarial (como 4G/LTE), su capacidad de gestión y las funciones de seguridad facilitadas (como las unidades cifradas y la autenticación mediante NFC) contribuyen a que el trabajador pueda desempeñar cómodamente sus tareas aun no estando en su puesto habitual en la oficina. Incluso, es posible utilizar un lápiz táctil sobre su pantalla de 12,5 pulgadas para, por ejemplo, firmar documentos o realizar notas.

Disponible con el sistema operativo Windows 10 Pro, Fujitsu Stylistic R727 puede llegar a ofrecer una autonomía de hasta 10 horas de duración. El usuario tiene a su disposición diferentes configuraciones con el fin de que pueda elegir la que mejor se ajuste a sus necesidades. Por ejemplo, el procesador –que pertenece a la séptima generación de la serie Intel Core- puede ser un i3, un i5 o un i7. Para el disco duro, por otro lado, las opciones posibles son tres: una unidad SSD de 128 Gb, 256 Gb o 512 Gb.

Con un puerto mini DisplayPort y una entrada USB 3.1 (entre otras interfaces), la cámara frontal incorpora un sensor de 2 megapíxeles de calidad mientras que la trasera –que tiene autofoco- escala hasta los 5 megapíxeles. También es compatible con la tecnología de transmisión inalámbrica bluetooth 4.1, admite tarjetas de memoria microSD/microSDHC/microSDXC, y dispone de dos altavoces estéreo y dos micrófonos digitales.

Para concluir, indicar que las dimensiones del producto como tableta son de 319 x 201 x 9,5 mm. El peso es de 830 gr pero si le acoplamos el teclado para utilizarlo como portátil éste se sitúa en 1,170 kg.

Disponible con el sistema operativo Windows 10 Pro, Fujitsu Stylistic R727 puede llegar a ofrecer una autonomía de hasta 10 horas de duración

Fujitsu España
Camino del Cerro de los Gamos, número 1
28224 Pozuelo de Alarcón (Madrid)
Teléfono: 91 784 90 00
Web: www.fujitsu.com/es
Precio: Desde 1208,79 euros

HP EliteBook x360

Sofisticado y potente. Así es la propuesta de la multinacional norteamericana que facilita hasta cinco opciones de uso y ofrece un paquete de medidas de seguridad muy completas.

Hasta las páginas de este artículo llega el convertible EliteBook x360, un equipo de diseño compacto y elegante que ha sido sometido a un proceso de 'artesanía de precisión'. Así, por ejemplo, muestra cortes de diamante sobre un monobloque de aluminio. Hay que indicar –sin embargo- que esta máquina no sólo destaca o sobresale por esta sofisticada carta de presentación, pues toda su estructura se muestra duradera ya que según ha explicado el propio fabricante ha sido desarrollada para superar las pruebas MIL-STD, un estándar de carácter militar.

Brinda una flexibilidad de 360º para que el usuario pueda utilizarlo en cualquier situación, proporcionando hasta cinco modos de uso que corroboran su alta versatilidad. El modo Tienda es idóneo para compartir vídeos y presentaciones, mientras que el de Medios se utiliza para colocar la pantalla en primera línea y reproducir toda clase de contenidos. Luego se encuentra la modalidad Conferencia: en este caso, el EliteBook x360 puede adoptar una forma totalmente plana, siendo perfecto para la colaboración y las conferencias gracias a sus micrófonos dobles y sonido. Precisamente, y en lo que audio se refiere, el equipo lleva el sello de la marca Bang & Olufsen y altavoces premium. El cuarto modo es Tablet y permite transformar el portátil en una tableta fina y ligera para estar conectado durante los desplazamientos. Por último, se encuentra el modo Portátil con funciones completas y recomendado para la multitarea.

La firma promete una autonomía de hasta 16 horas y 30 minutos, y como parte de la familia HP Elite incluye opciones de especial interés desde el punto de vista de la seguridad. Este es el caso de Sure Start Gen3 o BIOS auto-reparable con protección de memoria en tiempo de ejecución (SMM); es decir, que supervisa, recupera y restaura la BIOS en memoria ante cualquier vulneración a nivel de seguridad manteniéndose intacta ante posibles ataques. Por otro lado, HP WorkWise es una aplicación para teléfonos inteligentes centrada también en la seguridad, con información de rendimiento en tiempo real y preparada para ofrecer protección contra manipulaciones.

En lo referente al inicio de sesión, el usuario cuenta con tres posibles opciones: cámara IR, sensor de huellas dactilares o lector de tarjetas inteligentes. HP, en otro orden de cosas, pone al servicio de sus clientes el kit Manageability Integration: se utiliza para acelerar la creación de imágenes y la gestión de hardware, BIOS y seguridad a través de la solución de software de administración Microsoft Center Configuration Manager. En el momento de la adquisición de este modelo, se tiene la opción de elegir la función Sure View. Con ella se activa un modo de privacidad gracias a la cual la pantalla se mostrará oscura para todos excepto para nosotros, protegiendo la información confidencial.

La configuración de este HP EliteBook x360 incluye los últimos procesadores de la séptima generación Intel Core, una memoria RAM DDR4 de hasta 16 Gb, unidades de estado sólido Gen3 PCIe y opciones de almacenamiento doble. La pantalla de 13,3 pulgadas posee resolución Full HD e incorpora protección Corning Gorilla Glass y, además, cuenta con dos puertos USB 3.1 (uno de ellos de carga), uno USB de clase C con Thunderbolt, microHDMI y micro SIM externa, entre otras características.

La configuración de este HP EliteBook x360 incluye los últimos procesadores de la séptima generación Intel Core

HP Enterprise
Calle Vicente Aleixandre, número 1
Parque Empresarial Madrid- Las Rozas
28232 Las Rozas (Madrid)
Teléfono: 902 990 011
Web: www.hp.es
Precio: Desde 1813,79 euros

Lenovo ThinkPad X1 Yoga

Su lápiz digital es compatible con las aplicaciones del paquete Office 2016 y, además, cuenta con una función de carga rápida para la batería. Hay disponibles varias configuraciones, una de las cuales incluye una pantalla OLED de 14 pulgadas.

Lenovo eligió la última edición de la feria CES de Las Vegas para presentar su nueva generación de productos ThinkPad X1. A ella pertenece este nuevo Yoga, disponible ahora en dos colores: al diseño tradicional en color negro hay que sumar una versión en plata metalizado que resulta sofisticada. Esta máquina ha sido sometida a más de 200 pruebas de calidad (para brindar una alta durabilidad y resistencia) y se muestra al consumidor como un dispositivo renovado y flexible, capaz de adaptarse a las necesidades de aquellos trabajadores que reclaman opciones multimodo. Otra de sus novedades, es que una de sus configuraciones admite la incorporación de una pantalla OLED que muestra negros más puros y colores más vivos. Con un breve tiempo de respuesta, el contraste entre las zonas iluminadas y las que están en sombra es mucho más nítido. Asimismo, se ha rediseñado el bolígrafo recargable que incluye (compatible con las aplicaciones de Office 2016) y mejorado el teclado para una experiencia más cómoda y agradable.

El nuevo Lenovo ThinkPad X1 Yoga posee una bisagra de 360º, gracias a la cual es posible elegir entre distintos modos de uso según cada momento. Está el modo clásico o portátil para cuando, por ejemplo, haya que redactar un informe o completar una hoja de cálculo. Pero también puede utilizarse como tableta o si hiciese falta girar su pantalla de 14 pulgadas para que el teclado (al que Lenovo ha bautizado como Wave) se repliegue y las teclas permanezcan bloqueadas.

En lo a conectividad se refiere, y aunque nos encontremos en una zona en la que no exista una red Wi-Fi próxima, como cuenta con una conexión LTE-A (4G) nos aseguraremos siempre la conexión y el acceso a todos los datos y aplicaciones disponibles en nuestra nube informática. Con una autonomía de algo más de 15 horas según datos del fabricante, dispone de una función de carga rápida capaz de proporcionar una recarga del 80% en sólo una hora.

La seguridad ha sido mejorada y gracias a Windows Hello ya no es necesario recordar la contraseña elegida para nuestro equipo. Basta con utilizar el lector de huellas dactilares, aunque de manera opcional es posible adquirir este híbrido con una cámara infrarroja con tecnología de reconocimiento del rostro.

También hay que destacar la inclusión de la tecnología Intel Thunderbolt 3. En este caso, y conectando un cable del puerto USB-C a uno de sus dos puertos Thunderbolt 3, el resultado es un ancho de banda superior tanto para datos como para vídeo, además de un suministro de alimentación. A este respecto, comentar que uno de los accesorios disponibles es una estación de acoplamiento llamada ThinkPad Thunderbolt 3 para la multitarea: esta estación es compatible con dos pantallas 4K o tres Full HD y con un único cable es posible obtener hasta 13 puertos adicionales para todos nuestros periféricos.

La seguridad ha sido mejorada y gracias a Windows Hello ya no es necesario recordar la contraseña elegida para nuestro equipo

Lenovo
Abedul, P.N. Empresarial
c/ de Serrano Galvache, 56. 28033 Madrid
Teléfono: 902 18 14 49
Web: www.lenovo.com
Precio: Desde 2148,79 euros (principios de abril)

Microsoft Surface Pro 4

Bañada por una cubierta de magnesio, esta tableta se transforma en un portátil con la funda Type Cover. Su diseño es más estilizado que el de su predecesora, lo que no le impide mostrarse más potente y rápida.

Tomó el relevo del dispositivo Surface Pro 3, y lo hizo para brindar a los usuarios una potencia y un rendimiento superior mostrando al mismo tiempo un diseño mucho más estilizado y ligero (se encuentra disponible a partir de los 766 gr). Asimismo, Microsoft da la posibilidad a sus clientes de ejecutar a través de ella la versión completa de su paquete Office además de Windows 10 Pro, incluyendo Windows Hello (para iniciar sesión), el navegador Microsoft Edge y el asistente Cortana.

El fabricante ha desarrollado diferentes versiones de su producto, pudiendo elegir el modelo de procesador (Intel Core m3 o la sexta generación de los modelos i5 e i7) y el tamaño de la unidad SSD que integra (desde los 128 Gb al terabyte de capacidad). Con un grosor de 8,4 mm, Surface Pro 4 incorpora una pantalla multitáctil de 12,3 pulgadas y tecnología PixelSense caracterizada por su alto contraste y poco reflejo. La resolución se sitúa en 2.736 x 1.824 píxeles. En otro orden de cosas, señalar que proporciona una autonomía de hasta nueve horas (modo reproducción de vídeo) y que su funcionamiento también resulta más silencioso con respecto a predecesora porque la refrigeración se ha mejorado y es más eficiente.

Microsoft Surface Pro 4, que dispone de un soporte trasero en varias posiciones, puede convertirse en un ordenador portátil gracias a la funda-teclado Type Cover. A la venta en tres colores (negro, azul y azul brillante), el teclado mecánico ha sido rediseñado para escribir de manera más fluida y rápida. Esta funda-teclado se conecta a la tableta a través de un puerto específico, se llama puerto de funda y completa al resto de conexiones disponibles: dos USB 3.0 de tamaño completo, lector de tarjetas de memoria microSD, toma de auriculares y mini DisplayPort. La funda-teclado de Microsoft tiene unas dimensiones de 295 x 217 x 4,9 mm, pesa 310 gr e incorpora teclas de función (F1 a F12) y acelerómetro. De igual forma, posee botones dedicados para métodos abreviados de Windows, ajuste de brillo de la pantalla y controles multimedia.

Un 30% más rápida, la memoria RAM puede ampliarse hasta los 16 Gb. Soporta bluetooth 4.0 y un chip TPM para seguridad empresarial. A la cámara para la autenticación de rostros de Windows Hello se ha añadido una frontal de 5 megapíxeles de resolución con vídeo 1080p y otra posterior con sensor CCD de 8 megapíxeles, autofoco y vídeo 1080p también. Los micrófonos son estéreo al igual que los altavoces, que arrojan sonido Dolby Audio Premium.

Microsoft Surface Pro 4, que dispone de un soporte trasero en varias posiciones, puede convertirse en un ordenador portátil gracias a la funda-teclado Type Cover

Microsoft Ibérica
Paseo Club Deportivo, número 1
Parque Empresarial La Finca, Edificio 1
28223 Pozuelo de Alarcón (Madrid)
Teléfono: 91 391 90 00
Web: www.microsoft.es
Precio: Desde 999 euros.
Precio Type Cover: 149,99 euros

ECIJA

Tormentas solares y continuidad de negocio

Javier López,
socio de ECIJA

Como culmen a su mandato como Presidente de Estados Unidos, Barack Obama provocó una alarma generalizada en el planeta el mes de octubre pasado, cuando informó que había firmado una orden ejecutiva en la que ordenaba coordinar esfuerzos a sus Agencias federales para predecir y detectar eventos meteorológicos del espacio, como destellos solares (breve e intensa erupción en la superficie del Sol que se asocia con manchas solares), partículas de energía solar (iones y electrones expulsados desde el Sol por esas erupciones) y ruidos geomagnéticos (afectación del campo magnético de la Tierra por la actividad solar), así como alertar a los ciudadanos, proteger la infraestructura crítica y recuperarse de los daños.

n efecto, el Sol emite continuamente partículas cargadas eléctricamente (protones, electrones y núcleos de helio), que constituyen el viento solar que, en ocasiones, se ve perturbado por la liberación explosiva en la atmósfera solar de millones de toneladas de estas partículas en pocas horas, dando lugar a una tormenta solar que se propaga por todo el sistema planetario. Así, una tormenta solar es una variación pronunciada del campo magnético terrestre debido a que porciones de la energía solar son transferidas a nuestra magnetosfera, habitualmente en conexión a grandes llamaradas solares que emiten materia en nuestra dirección.

Estos fenómenos ocurren con frecuencia y, aunque normalmente no llegan a producir efectos relevantes en nuestro planeta, pueden afectar a infraestructuras clave, como el Sistema de Posicionamiento Global (GPS), que alteraría satélites, circulación aérea, sistemas de comunicación y la distribución eléctrica; con lo que quedarían perturbadas simultáneamente la salud y la seguridad a nivel global.

Es ahora cuando está empezando a crecer la preocupación por este tema, debido a la extrema dependencia que tiene nuestra civilización actual de la tecnología basada en la electricidad (la llamada ciberelectroesfera), que gestiona nuestros servicios diarios, así como de la energía que la alimenta, debido a que la práctica totalidad de los suministros que requerimos diariamente dependen de ello: electricidad, agua, mantenimiento de centrales nucleares, alimentos, salud, transporte, comunicaciones, etc. Para comprobar hasta qué extremo esto es así, baste recordar que en marzo de 2016 un ataque cibernético cambió los niveles de las sustancias químicas del agua de una planta potabilizadora del Reino Unido poniendo en peligro una ciudad entera, aunque, afortunadamente, se detectó a tiempo y nadie enfermó.

Sin embargo, no sería la primera vez que un fenómeno meteorológico espacial provoca un impacto en la era moderna. En efecto, durante el llamado evento Carrington, una tormenta solar en 1859 inutilizó el telégrafo en Europa y Estados Unidos. Se calcula que, si ocurriera hoy en día, miles de transformadores quedarían destruidos, privando de suministro eléctrico a continentes enteros durante meses o, quizá, años. En 1967, en plena guerra fría, las consecuencias pudieron ser más graves, pues tres potentes erupciones solares dañaron los radares que Estados Unidos tenía para detectar misiles soviéticos, con lo que estuvo cerca de iniciar un ataque defensivo. Más recientemente, en 1989, un transformador eléctrico de New Jersey quedó inutilizado a causa de una eyección de plasma solar dejando sin energía eléctrica a seis millones de personas en Quebec (Canadá).

A nivel empresarial, esté fenómeno constituye un riesgo relevante a tener en cuenta, ya que todos los procesos productivos, adminis-

trativos, comerciales, de comunicación, etc. están altamente tecnificados, por lo que la falta de suministro eléctrico podría suponer una paralización imperiosa. Mayor efecto tendría aún si se trata de una empresa tecnológica, donde la práctica totalidad de su actividad estuviera inmersa en la tecnología.

Entonces, ¿qué acciones se pueden tomar para evitarlo? Si se trata de un colapso a nivel planetario, poco podríamos hacer, pero si la incidencia es más reducida, se pueden adoptar medidas técnicas y jurídicas para tratar de minimizar los efectos. Desde el punto de vista legal, la pionera en aprobar un plan de acción de protección civil para eventos de clima espacial y tormentas solares fue la Comunidad Autónoma de Extremadura en 2012, en la línea de las recomendaciones del Congreso de los Diputados sobre la necesidad de elaborar planes preventivos ante el riesgo de tormentas solares, al igual que otros países europeos como Reino Unido, Francia, Alemania, Holanda y Bélgica. Asimismo, la Comisión Europea tiene proyectadas medidas preventivas frente a las tormentas solares como la monitorización del clima espacial mediante el Global Disaster Alert and Coordination System.

Sin embargo, estas recomendaciones están orientadas a ayudar a la supervivencia personal de los afectados, y no a asegurar la continuidad de negocio de las empresas. Para ello, es necesario acudir a las normas internacionales de la ISO (International Organization for Standardization), que son certificables mediante un proceso de auditoría en la que se evalúa el cumplimiento de los controles; y que permiten disponer de un plan de prevención en el que cada profesional y responsable de la empresa sepa exactamente lo que tiene que hacer para minimizar el impacto ante cualquier riesgo que amenace a la organización, como sin duda sería una situación de emergencia creada por una tormenta solar, así como calcular cuánto tiempo se tardaría en volver a una situación aceptable o, si es posible, normalizada.

Entre ellas hay que destacar la ISO 27001, que establece un estándar para implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) según el Ciclo de Deming –Plan, Do, Check, Act (PDCA)–, centrándose en datos de negocio, pues la información y las partes interesadas en el tratamiento de esa información (trabajadores, clientes, etc.) son los activos fundamentales de la organización que hay que proteger. Para ello, establece diez puntos que hay que cumplir con obligaciones de tipo organizativo o de gestión, y a su vez 114 controles para chequear dicho cumplimiento. Estos puntos a cumplir (en realidad, son siete, ya que los tres primeros son definiciones y referencias), son los siguientes: contexto de la organización, liderazgo, planificación, soporte, operación, evaluación de desempeño y mejora. También hay que tener en cuenta la ISO 27002, que establece el proceso de gestión de la ISO 27001, constituyendo una suerte de tutorial para implementar dicho estándar, sus normas y controles, y que, aunque no obliga a hacer la implementación exactamente como indica, resulta de utilidad.

Asimismo, ha de observarse la ISO 22301, que establece un estándar para la Gestión de Continuidad de Negocio (SGCN), organizando la realización de un análisis de riesgos y controles, pero en este caso se centra exclusivamente en que la continuidad de negocio esté más gestionada en caso de desastres u otros escenarios. Aunque los puntos de control son más genéricos, el análisis de riesgos es más duro porque exige un análisis de impacto en el negocio teniendo en cuenta los procesos nuevos y los cambios en la esfera de la seguridad y del negocio, exigiendo que se calcule el tiempo objetivo de recuperación a la situación anterior, así como el tiempo máximo tolerable de incidencia.

Los DataLakes, una evolución en el análisis de los datos

Enrique Serrano, director general de Tinámica

En 2012 comienzan a lanzarse los primeros DataLakes en banca como primeras iniciativas en proyectos de big data. El concepto es simple: bajo un mismo repositorio de datos, almacenar todas las fuentes de datos posibles, sin transformaciones previas ni complicados procesos de carga, solo datos en su estado bruto tal cual son escupidos por un sistema operacional o por un sensor. La idea es poder "pescar" cualquier tipo de información para interrelacionarla después, sin las barreras impuestas por un Data Warehouse DWH (almacén de datos) o las restricciones de un datamart, como dato agregados dentro de un DWH.

Hasta el momento, los datos que se generan por la actividad diaria se trasforman y normalizan para ser almacenados en el DWH bajo ciertas reglas de negocio y sobre un modelo de datos que ya establece sus relaciones básicas. Por ejemplo, ticket de caja con tienda, referencia de artículo, cantidad, cliente, etc. Una vez dentro del DWH, la información se agrupa en datamarts para un mejor y más rápido cálculo. Todo esto ha funcionado relativamente bien hasta que se han incorporado fuentes de datos nuevas con diferentes estructuras en los datos como las fotos, videos, tweets, o información de blogs de navegación en webs, etc. Además de todo esto, el ingente volumen de datos ha llevado a evolucionar los sistemas informacionales a nuevos sistemas de big data que permitan la ingesta, almacenamiento y proceso de cualquier tipo de dato, tenga la estructura que tenga y en tiempo real. De ahí que la función de los DataLakes sea ingestar toda la data posible, sin límite, y con unas ventanas de carga rápidas en el tiempo dejando que sea un experto analista de datos o data scientist el que decida qué hacer con ellos, como interrelacionarlos y buscar patrones ocultos en los mismos. A partir de aquí se inician las fases de integración y transformación de los mismos para su posterior análisis. Por ello, la principal función de los DataLakes es realizar Data Discovery entre todos los datos, tarea que no permitían los antiguos Data Warehouse con la información compartimentada en departamentos a través de los data marts: datamart de producción, comercial, de riesgos, de productos, geográficos, etc. A través del data Discovery se trata de buscar patrones ocultos de comportamiento y relación entre los datos que no son visibles a golpe de vista o con un análisis tradicional de los mismos. Los DataLakes constituyen hoy en día uno de los pilares principales de los primeros proyectos de big data en las grandes compañías. Esta técnica que fue introducida inicialmente por bancos, telecos y más tarde compañías eléctricas, es actualmente un concepto muy extendido, que se aplica en cualquier tipo de compañía y supone un cambio de filosofía en cuanto al tratamiento de los datos para su posterior análisis.

Las empresas pueden de verdad tener una visión cliente 360 grados al disponer en un repositorio único de toda la información de sus clientes, de tal forma que al llamar al call center este puede visualizar en tiempo real la posición y el valor como cliente para sí poderle ofrecer la mejor atención y poder ofrecer los productos más atractivos en cada caso.

XXIV EDICIÓN
15-16 marzo
PALACIO MUNICIPAL DE CONGRESOS
MADRID

ASLAN 2017 CONGRESS & EXPO

Tecnologías en red para impulsar la Transformación Digital

El papel de la tecnología y de los expertos IT cambiará más en 2017 que en los últimos diez años. Estamos en el punto de inflexión impuesto por el fenómeno de la Digitalización. Responsables IT, partners tecnológicos, service providers y startups tienen la oportunidad de liderar la Transformación Digital aportando su talento, experiencia y conocimiento tecnológico.

Conocer las últimas innovaciones tecnológicas, y cómo alinearlas con el negocio, es el gran reto en la nueva era digital y el foco principal de ASLAN2017.

"Leading innovation...

...network is everything"

GLOBAL SPONSOR

DELL EMC · itconic · econocom · WALHALLA · Hewlett Packard Enterprise

CONGRESS SPONSOR

Extreme · SOPHOS · GLOBAL SWITCH · SCC

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

Síguenos y participa **#ASLAN2017**

CELEBRACION SIMULTÁNEA

Smart energy Congress & Expo "Energy Efficiency in the Digital Age"

NOVEDAD: Corporate DataCenter EXPO
Un ecosistema de proveedores especializados para mejorar la eficiencia en los Centros de Datos Corporativos
"El corazón de la Economía Digital"

ORGANIZA

@asLAN

Creamos espacios de encuentro y divulgación tecnológica gracias al apoyo de más de 100 empresas asociadas.

Los servicios gestionados MPS y la seguridad

Es frecuente ver cómo contenidos celosamente protegidos en sus repositorios digitales quedan después fuera del control corporativo una vez que son impresos

Jose Mª de la Fuente. Business Development Manager, Managed Print Services Canon España

Vivimos en un mundo en constante evolución en el que la tecnología avanza a un ritmo exponencial y afecta de manera progresiva a la práctica totalidad de nuestras actividades diarias, tanto en el terreno personal como en el laboral. Obvia decir que a mayor número de tareas y procesos soportados de forma electrónica mayor es la cantidad de información sensible o confidencial que estos manejan. Las empresas se esfuerzan para establecer las medidas necesarias para mantener bajo control la información en formato digital, y emplean mecanismos de cifrado, categorización de contenidos y/o sistemas de control de acceso.

Gradualmente se introducen nuevos sistemas que tienden a reducir el empleo del papel, pero lo cierto es que buena parte de los actuales procesos de negocio siguen relacionados de un modo u otro con este medio (especialmente en algunos sectores como el financiero, el sector legal o la administración pública). No parece que esto vaya a cambiar de forma drástica en el corto o medio plazo, por lo que debemos asegurarnos de que "el papel" recibe la atención que merece en materia de seguridad. Es frecuente ver cómo contenidos celosamente protegidos en sus repositorios digitales quedan después fuera del control corporativo una vez que son impresos. Es también habitual que las funciones de escaneado y envío sean de acceso libre, permitiendo que cualquiera pueda digitalizar contenidos (en ocasiones incluso de forma anónima), compartirlos con terceros, almacenarlos en unidades extraíbles o incorporarlos a procesos de negocio sin contar con la mínima información necesaria para validar su autenticidad u origen.

En Canon, la seguridad es siempre el factor clave a observar a la hora de diseñar nuestros servicios gestionados de impresión (MPS), que combinan la tecnología y los servicios necesarios para hacer que este tipo de problemas sean algo del pasado. Nuestros equipos multifunción forman ya una parte integral de las infraestructuras de nuestros clientes y se han convertido en el punto de acceso por defecto para todo tipo de flujos documentales corporativos. Hoy en día estos equipos ofrecen un conjunto impresionante de funciones (impresión, copia, digitalización, envío, fax, almacenamiento, servicios web, etc) y se integran con potentes herramientas de gestión que los hace insustituibles. No podemos por tanto ignorar el papel vital que desempañan y somos especialmente cuidadosos en garantizar la seguridad en todos los flujos de trabajo documentales que soportan.

La clave para garantizar que un sistema sea seguro es establecer un alto nivel de seguridad por defecto. Así, a la hora de confeccionar un sistema MPS para cualquiera de nuestros clientes siempre recomendamos que se observen ciertas normas básicas de seguridad. Estas indica-

Segunda generación

XGE

XTREME GAMING ENERGY SERIES

XGEII GAMING ATX12V v2.31 APFC 82+ LED ON/OFF

La serie gaming XGE II de TOOQ genera energía de alto rendimiento para jugadores entusiastas.
Activa o apaga la luz led azul del ventilador desde la unidad; no más molestias nocturnas o en el trabajo "formal".
Cables extra largos y mallados. Ventilador ultra silencioso con control automático de velocidad. Potencias de 525W, 600W, 700W y 800W.

Un corazón para configuraciones de gama alta_

Garantiza más del 82% de eficiencia

80 PLUS BRONZE

TooQ
CREATE ▼ INSPIRE

www.tooq.com

Por lo que respecta a las medidas de control y auditoría, se pueden adaptar en función de los requerimientos específicos de cada cliente, y pueden incluir desde opciones básicas de registro y control, como la creación de un registro documental en pdf de los documentos

ciones incluyen el control de acceso a los dispositivos y sus funciones, el cifrado de la información extremo a extremo y los sistemas de borrado automático de memoria en los dispositivos que garantizan que la impresión es realmente segura.

Por lo que respecta a las medidas de control y auditoría, se pueden adaptar en función de los requerimientos específicos de cada cliente, y pueden incluir desde opciones básicas de registro y control, como la creación de un registro documental en pdf de los documentos, hasta otras más avanzadas como la inclusión de marcas de agua en cualquier trabajo impreso o escaneado (bien sea en formato texto o mediante códigos de barras 2D) con un identificador único que permite hacer un seguimiento exhaustivo del mismo. También se pueden implementar medidas muy específicas, como el análisis a tiempo real de los contenidos con posibilidad de desencadenar determinadas acciones (por ejemplo, la notificación inmediata al responsable de seguridad) cuando se encuentran palabras o términos "clave" incluidos previamente en un listado de seguridad.

No obstante existen innumerables opciones que pueden ser configuradas en función de las necesidades de cada empresa y de las características propias de cada proyecto. Me gustaría con esto invitar a la reflexión sobre el papel esencial que juegan los dispositivos multifunción como parte de la cadena de seguridad y sobre los riesgos asumimos cuando no se toman las medidas de control oportunas.

FUTURE OF RADIO

Descubra el mundo de la interconexión de audio en red de Hama, nuestra contribución a una casa siempre conectada. Música siempre y donde quiera, con una calidad de sonido fascinante, así como un diseño moderno.

¿Recuerda las últimas vacaciones en el Mar del Sur, los sonidos caribeños y la sensación de vacaciones en la playa? Nuestras radios por Internet traen la música del Caribe y, por supuesto, de otros lugares del Mundo a su hogar. Con más de 30.000 estaciones de radio, la selección es casi interminable y le permitirá encontrar el tipo de música que desee en cada momento. Nuestras radios digitales están preparadas para el futuro: cuentan con módulos de recepción para DAB y DAB + (Radio Digital) y, por lo tanto, podrán ser operativas en muchos países europeos, pudiendo así disfrutar de su música sin interferencias, en calidad de CD sin ninguna conexión a Internet.

La mayoría de nuestras radios disponen de una conexión USB, lo cual resulta ideal para disfrutar de su colección de música digital, tanto si está almacenada en un sistema NAS local (Network Attached Storage) o en cualquier otro medio de almacenamiento. Y, si lo desea, también puede hacer streaming de la música almacenada en su Smartphone.

¿Aún no es suficiente? Bueno, la mayoría de nuestras radios poseen una interfaz para conectarse a Spotify, a través de la cual podrá reproducir y almacenar su música favorita, sin necesidad de usar el Smartphone, únicamente guardando la lista de reproducción... Y la fiesta podrá comenzar con solo presionar apenas unos botones en su radio.

Gracias a la aplicación UNDOK para Smartphone, los usuarios de iPhone y Android podrán controlar la radio a través de su móvil y realizar la configuración inicial completa. De manera cómoda y fácil.

Y para los que aún quieren más: Existe la posibilidad de combinar varios altavoces y radios para escuchar su música de una manera absolutamente sincronizada en toda la casa, lo que se conoce como Multiroom. Debe tener en cuenta que no todos los dispositivos deben tener todas las funciones, p.ej.: una radio con CD es suficiente para reproducir su música en los demás altavoces que formen parte de ese grupo o red. En Hama disponemos de una docena de dispositivos compatibles, para ofrecerle una solución inteligente para cada situación.

Muchos de nuestros dispositivos disponen de Bluetooth, permitiendo así encontrar cuál es la opción que mejor se adapta a su propósito.

Experimente el Mundo de la interconexión de audio en red de Hama y déjese llevar por éste!

"SIN CALIDAD, LA TRANSFORMACIÓN DIGITAL NO EXISTE"

Sogeti es uno de los principales líderes del mundo en calidad de software y testing. Un concepto que no es entendido por numerossas empresas que lo ven como un gasto innecesario. Para hablar de ello Byte TI entrevistó a José Luis Antón, Testing & Software Quality Director de la compañía.

Manuel Navarro Ruiz

¿Qué papel juega la calidad del software en la transformación digital?

Creeemos que es necesario que se manejen bien las dos TIs. Por un lado las TI tradicionales, que todavía existen y que es el core de la organización y luego la que denominamos Business IT que se tiene que adaptar a esta nueva realidad. Es desde el punto de vista de la calidad, lo importante es entender cuáles son los procesos de calidad que debemos seguir para que esa transformación sea exitosa. Como esto va tan rápido, tenemos que poner mucho énfasis en el tema de la calidad porque si no, la transformación digital está condenada al fracaso.

Han lanzado recientemente el sello IOTrust, ¿qué persigue este nuevo sello?

Se trata de un sello que está focalizado en garantizar la seguridad de las aplicaciones que hay en cualquier dispositivo: desde un ordenador, a un smartphone o incluso un coche. IOTrust aporta una garantía en lo que se refiere a la seguridad que está en el mercado. Gracias a él nos aseguramos ciertos aspectos que garantizan y certifican aspectos como la autenticación, la autorización de accesos, la seguridad perimetral, etc. En definitiva se trata de generar confianza en el usuario de ese determinado dispositivo.

Los dispositivos IoT, sobre todo los primeros, se desarrollaron sin medidas de seguridad. ¿Qué problema ve aquí?

El tema es que los dispositivos que ya están desarrollados no son tan críticos como los actuales. A esos dispositivos que nacieron sin seguridad, se les puede hacer un análisis y se puede trabajar sobre ellos en base a las reglas de IOTrust. El problema es que hay que ir a cada uno de esos dispositivos a hacerles las pruebas, pero medidas de seguridad se les puede poner. Hoy, IoT es más crítico que antes y no se pueden correr riesgos porque afecta a multitud de dispositivos.

Lo que nosotros decimos en este IOTrust es que hay que empezar desde el principio a implantar medidas de seguridad en cualquier dispositivo de IoT.

La calidad de software, ¿no está reñida con el presupuesto?

Al final, la calidad hay que verla como una actividad que ayuda a reducir los costes del área de TI y que ayuda sobre todo a cumplir con el time-to-market. Además, también es fundamental para mantener o mejorar la percepción que se tiene de una determinada compañía por parte de los clientes.

¿Cómo puede ayudar al time-to-market si se exige que una aplicación esté lista en un breve periodo de tiempo, sin importar la calidad de la misma?

El time-to-market y la reducción de costes se logran si hacemos y ejecutamos los procesos de testing y de calidad a conciencia. Para ello hay que integrar la calidad desde el principio en cualquier proceso de desarrollo. Lo que normalmente ha sucedido es que se saca la aplicación y sobre ella se van corrigiendo los errores y poniendo parches. Con eso, lo que sucede es que si algo costaba diez, al final va a costar treinta.

Si empezamos a introducir la calidad desde el principio, vamos a ir reduciendo tiempos y costes porque no vas a tener que trabajar dos veces sobre el mismo proyecto. Si a la calidad la enfocamos simplemente como algo que hay que hacer para pasar ciertos exámenes, no nos aportará valor y producirá un sobrecoste.

¿La empresa española apuesta por la calidad?

Cada vez más. Lo podemos ver en los últimos informes y estudios que desde Sogeti hemos realizado. Ahora mismo, algo más de un 30% del presupuesto de IT se destina a la calidad. Lo que vemos es que en España está cambiando y que las organizaciones ven a la calidad como una herramienta más para ayudar al negocio.

José Luis Antón

Testing & Software Quality Director de Sogeti

EL PRECIO DE LAS COSAS

Por Miquel Barceló

A primeros de febrero nos enteramos de que tres jóvenes de Barcelona, Andrés Bou, Marc Canaleta y Horacio Martos, habían vendido su empresa Social Point a la firma multinacional Take-Two por 250 millones de dólares.

Para situarnos, recordemos que, entre otras cosas, Take-Two fue la creadora hace ya años, de un videojuego de gran éxito: Grand Theft Auto (GTA), mientras que Social Point, creada en 2008, se había destacado recientemente como una brillante y prometedora empresa de juegos de Facebook.

Social Point tuvo tres rondas de inversiones en las que participaron primero Nauta y después Greylock, Idinvest y el BBVA. Al final, en 2014, Highland Capital aportó 22 millones para completar unos 36 millones de inversión. No se trata de una empresita de nada sino de algo serio con mucho y prometedor futuro por delante. Parece que, en el ejercicio de 2016, con sus 270 empleados y sus juegos Monster Legends y Dragon City entre otros logró unos ingresos de 90,8 millones de euros y un beneficio de explotación de 19,9 millones.

Andrés Bou y Horacio Martos se graduaron en Ingeniería Informática en mi Facultad, la Facultad de Informática de Barcelona (FIB) de la Universidad Politécnica de Cataluña y después siguieron un máster de emprendeduria en Paris. En el año 2011, el Cercle Fiber (creado por ex-alumnos de la FIB) les otorgó el premio FiberEmprenedors de 2011. De Marc Canaleta sólo sé que ha estudiado Diseño Gráfico en la Universidad de Barcelona.

A primera vista, la compra parece un claro retorno de la burbuja tecnológica cuando se llegaron a pagar por "cosas" como Terra millonadas sin cuento.

En cualquier caso, una empresa afortunada y de éxito como se dan, y se siguen dando en el mundillo de la informática. Aunque ahora el negocio parece estar no al servicio de otras empresas sino en la creación y distribución de juegos. Tumbos que da la vida...

Pero, ante cifras económicas tan alejadas de la experiencia cotidiana, no dejo de preguntarme si nuestra sociedad da el correcto valor a las cosas. El poeta ya nos advirtió que sólo los necios confunden valor y precio, pero a veces parece que el precio no se justifica con el valor. Estoy seguro que Andrés, Héctor y Marc se merecen el éxito: han trabajado duro, han encontrado el camino que sugiere nuestra sociedad y piensan seguir en la brecha esta vez como asalariados espero que de lujo de los nuevos propietarios Take-Two. Nada que objetar.

Con un salario mínimo como el que hay en España, en torno a los 10.000 euros anuales, tras digamos cincuenta años de actividad (una cifra más bien exagerada...), una persona obtendría tan solo medio millón en toda su vida laboral

Pero cifras como ésas suelen estar muy alejadas de la realidad de la vida cotidiana.

Permítanme algunas molestas comparaciones. Con un salario mínimo como el que hay en España, en torno a los 10.000 euros anuales, tras digamos cincuenta años de actividad (una cifra más bien exagerada...), una persona obtendría tan solo medio millón en toda su vida laboral. Incluso con un sueldo más que digno que alcanzara, pongamos, los 50.000 euros al año, en esos cincuenta años se llegaría "sólo" a dos millones y medio. 250 millones en nueve años, son muchos millones...

Vivimos en un mundo regido por el mercado, donde el consumo casi compulsivo se ha convertido en el verdadero motor de la economía. Por eso triunfan económicamente en nuestra sociedad quienes alcanzan el favor de los consumidores aunque sea con algo tan útil pero prescindible como los juegos, el deporte o la interpretación de cancioncillas intrascendentes y sumamente perecederas. Y lo hacen consiguiendo cifras que a todas luces parecen, y son, desorbitadas.

Ni que decir tiene que en otros casos, no tan directamente relacionados con el mercado, por ejemplo aquellos en los que es el propio individuo el que fija su sueldo, se llega al colmo de la exageración. Sirva el ejemplo de los desaprensivos e irresponsables (también en el sentido jurídico de la palabra...) directivos de banca de los que, sinceramente, estoy rotundamente convencido que cobran muchísimo, pero que muchísimo, más por su trabajo de lo que éste pueda valer...

Tal vez en lugar de salario mínimo debamos empezar a pensar en un salario máximo... No hay que confundir valor y precio, pero se hace.

Vodafone & Su negocio abierto 24h

"Con las Soluciones de Marketing Digital puedo mejorar el posicionamiento de mi negocio en Internet y conseguir nuevos clientes".

Con Vodafone, su proyecto preparado para el mundo digital. Infórmese en el 1500 y en vodafone.es/soluciones-digitales

Vodafone
Power to you

Con la Tarifa Digital Base desde 106€/mes (128,26€ IVA incluido) es un servicio titularidad de QDQmedia, S.A.U. (Solocal Group). Consulta condiciones y características en vodafone.es/soluciones-digitales