it Reseller
TECH&CONSULTING
Junio 2017 - nº 24

Gaming: el juego se convierte en negocio

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

it Digital MEDIA GROUP

Juan Ramón Melara
juanramon.melara@itdmgroup.es

Miguel Ángel Gómez
miguelangel.gomez@itdmgroup.es

Arancha Asenjo
arancha.asenjo@itdmgroup.es

Bárbara Madariaga
barbara.madariaga@itdmgroup.es

Colaboradores
Hilda Gómez, Arantxa Herranz, David Marchal

Diseño y maquetación revistas digitales
Contracorriente

Diseño y maquetación proyectos especiales
Eva Herrero

Producción audiovisual
Antonio Herrero, Ismael González

Fotografía
Ania Lewandowska

it Reseller TECH&CONSULTING

it User TECH & BUSINESS

it televisión

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

¿Te avisamos del próximo IT Reseller?

Gaming: más que una afición, un negocio con gran futuro

No son pocos los niños, jóvenes y adolescentes que han tenido que sufrir una regañina por parte de algún adulto por pasar mucho tiempo pegados a una videoconsola, un PC o un videojuego portátil. Pero el caso es que lo que hasta hace poco era solo una afición de algunos, se ha convertido en un negocio con un gran potencial de crecimiento.

El negocio que las consultoras auguran para el segmento del gaming es más que suculento, y nadie debería dejarlo escapar. Ordenadores de altísimas prestaciones, tarjetas gráficas de última hornada, grandes cantidades de memoria de última generación, accesorios, sistemas de refrigeración… y un largo etcétera de productos que suponen una ventana de negocio para el mundo de la distribución. Pero las previsiones no se acaban ahí, sino que la conjunción del gaming con otra de las grandes tendencias tecnológicas del momento, la Realidad Virtual, puede potenciar el desarrollo de un mercado que, lejos de ser un juego, es una de las grandes oportunidades a desarrollar en los próximos años.

Pero, para poder aprovecharla, será necesario, como siempre estar preparado, y no solo en el sentido de estar listo, sino en el sentido de estar siempre, formado. Saber lo que necesitan los clientes y asesorarles en su búsqueda sigue siendo, también en este terreno, la clave para convertir un negocio de bueno a inmejorable.

De hecho, ya llevamos varios meses hablando de eventos donde el gaming tiene más o menos protagonismo o, incluso, es el centro, pero en este En portada, os ofrecemos también la visión de las consultoras, que analizan el mercado en busca de tendencias y detalles que nos ayuden a entender hacia dónde vamos.

En definitiva, un negocio que, pese a que no es nuevo, y durante años ha estado generando significativos beneficios, se presenta ahora como una de las grandes oportunidades a desarrollar. Así que, como decimos de otras oportunidades, ¡no la dejéis escapar!

Juan Ramón Melara
IT Digital Media Group

Sumario

En portada

Reportaje

Responsabilidad Social Corporativa

Actualidad

Especiales IT Reseller

No solo it

Índice de anunciantes

KASPERSKY lab

KASPERSKY SECURITY AWARENESS

FORMACIONES DE CONCIENCIACIÓN EN CIBERSEGURIDAD

V-Valley/Vinzeo inaugura su Centro de Soluciones HPE y acerca su propuesta a 10 ciudades con V-Truck

Esprinet opta por un modelo colaborativo de gestión para su negocio de valor

En el último año, el negocio de valor de Esprinet en la Península Ibérica se ha visto impactado por dos operaciones que han venido a reforzar su posición, por una parte, y que han hecho necesaria una reorganización que culmina ahora con un modelo de gestión colaborativa, según definen sus principales responsables.

De izquierda a derecha, Carlos Preciado, José Ignacio Rodríguez, Javier Bilbao y Fernando Feliu.

Así, desde la compañía definen V-Valley como "la plataforma donde se unen Esprinet, Vinzeo y el negocio adquirido de IT Way para desarrollar el negocio de valor en España y Portugal", señala Javier Bilbao, presidente de V-Valley Iberian, que añade que en el negocio de volumen "nos mantenemos como dos entidades independientes, pero, en valor, las actividades son complementarias, de ahí que nos decidiéramos por un proyecto común. Actuaremos como tres empresas de forma independiente pero coordinada".

En todo caso, desde la firma estiman que se trata de "un modelo innovador", que se va a ver reforzado porque uno de los pilares de Esprinet para este 2018 es el desarrollo del negocio de valor, que, en el caso del mercado ibérico, tiene un gran potencial, unos 20 billones de euros, por la necesaria Transformación Digital de las empresas españolas. En este sentido, Bilbao apunta que, si ofrecen los servicios adecuados a los partners, "les ofrecemos la oportunidad de atrapar este negocio potencial".

Los pilares en los que se basa el negocio de valor de Esprinet, son dos. Por una parte, la división de Soluciones de Infraestructura, basada en las soluciones de Hewlett Packard Enterprise, que proviene del negocio tradicional de

> "En el modelo de negocio de valor no nos importa subir en el ranking. La clave en este negocio no está en el tamaño, sino en el conocimiento"
>
> Javier Bilbao

Vinzeo; y, por otra, todo el negocio de comunicaciones, seguridad, Comunicaciones Unificadas… proveniente de la suma de los negocios de IT Way y V-Valley.

Esta organización permite a la compañía, en palabras de Javier Bilbao, "asegurar un modelo de gestión por proyecto independiente, ofrecer productos y soluciones complementarios al fabricante principal en cada caso, y hacer crecer la oferta y modularla. Pretendemos ser un agregador de valor: tecnologías, soluciones y servicios".

Pero, además, esta forma de trabajar "nos permite multiplicar por tres la oferta de crédito a nuestros clientes. Podemos hacer una asignación más eficiente del crédito y atender a los clientes con mayor foco".

"Creemos", añade Javier Bilbao, "que la organización colaborativa tiene más sentido en valor que la búsqueda de sinergias. Queremos estar seguros de estar interpretando correctamente la estrategia de nuestros fabricantes".

Con todo, el negocio de valor del mayorista, que supone en este momento en torno a 85 o 90 millones de euros, debería duplicarse en dos años y medio, si se cumplen los objetivos marcados. Esta cifra no llevaría al mayorista a liderar el mercado nacional de valor, pero, como recalca Javier Bilbao, "en el modelo de negocio de valor no nos importa subir en el ranking. La clave en este negocio no está en el tamaño, sino en el conocimiento".

Eso sí, este responsable indica que, "si somos capaces de hacer nuestro trabajo, creceremos por encima del mercado y, si a futuro adquirimos alguna empresa que nos ayude a estar donde ahora no estamos, esto nos haría crecer, pero por mejorar la oferta y el servicio, no solo por crecer".

Un cambio en la aproximación al cliente

Si bien V-Valley nació con la vista puesta en el cliente, no en el centro de datos, la compra de IT Way provocó, tal y como explica Fernando Feliu, director de Ventas y Marketing V-Valley Iberian, "un giro en la aproximación al cliente, apostando por más comerciales técnicos, más certificaciones, y una visión del valor más orientada al centro de datos".

Lo que tiene claro Feliu es que con la nueva organización se complementa la oferta de Hewlett Packard Enterprise, y se apuesta por áreas de futuro como IoT o Analytics entre otras, apostando por una formación que busque "potenciar y

Empleo IT en 2017. Profesiones con futuro

Infoempleo y Deloitte se han unido para crear esta guía con el objetivo de arrojar un poco de luz sobre los nuevos desafíos a los que se enfrenta nuestro mercado laboral, que tiene en la tecnología a su principal motor de cambio. Además, se analizan 17 profesiones del sector IT que serán claves en el futuro.

desarrollar las capacidades de los resellers, no por sustituir sus capacidades por las nuestras".

Hablando de formación, los primeros pasos, en dos áreas donde el mayorista se encuentra bien posicionado: cloud y seguridad.

Pensando en el futuro, "estamos en la búsqueda activa de nuevos fabricantes", señala Feliu, "no solo fabricantes de renombre, sino que complementen nuestra oferta"; una búsqueda que va a apoyarse tanto en las tendencias del mercado como en las necesidades de los clientes.

Además, Feliu es consciente de que la nueva organización les va a permitir "emplear las herramientas financieras del grupo, lo que nos permite acometer proyectos que, hasta la fecha, no podíamos acometer"; siendo ésta una de las ventajas de la nueva estructura, junto con la especialización.

Preparados para la Transformación Digital

Como veíamos, la Transformación Digital de las empresas es una gran oportunidad, pero, como señala José Ignacio Rodríguez, Vinzeo IT Manager, "va a requerir una adecuación de todos los involucrados en el proceso de venta", de ahí que el mayorista quiera ayudar a sus partners ofreciéndoles tanto especialización como formación para adaptarse a los nuevos modelos de consumo, porque "todo cambio genera oportunidades. Pero si se quieren aportar soluciones, necesitamos transferir el conocimiento de las nuevas soluciones a los clientes", señala Rodríguez, que añade que "es necesario ofrecer servicios complementarios al canal para atienda las necesidades del cliente".

Con todo, este responsable estima que, la suya, es una proposición diferente para el partner por cuatro razones: el conocimiento profundo de las soluciones por la especialización, la estructura dedicada, las soluciones adicionales y el Centro de Soluciones, disponible tanto para los partners como para que estos muestren soluciones a sus clientes".

Primeras iniciativas para el canal

V-Valley inauguró el pasado 1 de junio un nuevo Centro de Soluciones HPE, donde con la tecnología del fabricante se mostrarán soluciones complementarias de otros fabricantes de la nómina del mayorista. Además, desde el 6 de junio, y por el plazo de un mes, llevará una

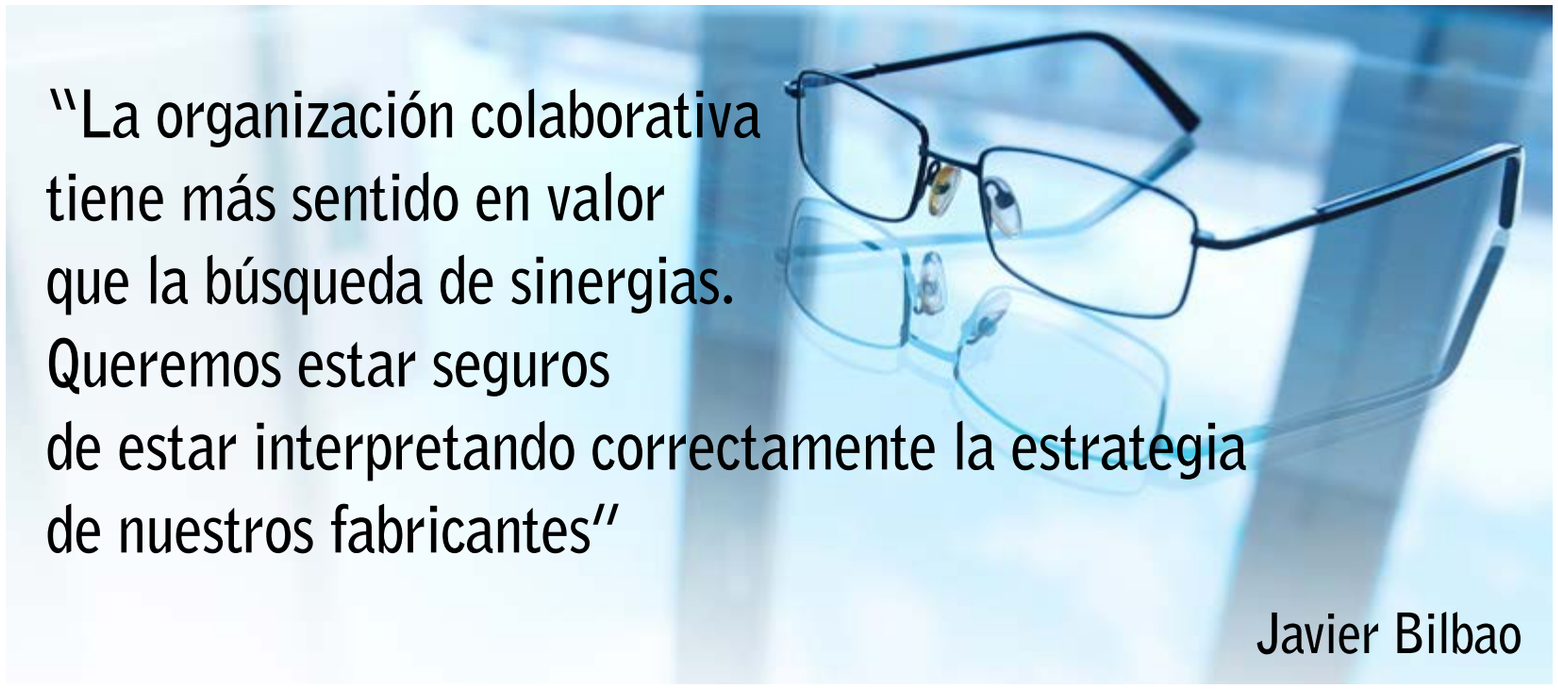
parte de este centro a 10 ciudades españolas dentro de un camión denominado V-Track, donde, además de acercar las soluciones a los partners, les permitirán a estos realizar demos a sus clientes.

Conectado con el Customer Technology Center recientemente inaugurado por HPE en su sede de Las Rozas, y con el Centro de Soluciones de V-Valley, el nuevo Centro de Soluciones HPE permitirá al mayorista mostrar a los partners no sólo el funcionamiento de la tecnología de Hewlett Packard Enterprise, dado que está reconocido como Centro de Excelencia de HPE en España, sino que, también, podrán ver cómo se integran estas tecnologías con las soluciones de otros fabricantes comercializados por el mayorista. Asimismo, en el centro se puede ofrecer formación y certificación, un entorno de desarrollo testeo y comercialización de apps, así como demos de soluciones híbridas, soluciones en VPC y demos cruzadas, para lo que también tiene especial interés el trabajo del mayorista con Microsoft y Azure.

Y, junto con esta iniciativa para acercar a los partners y sus clientes la tecnología y darles a conocer, de primera mano, cómo se integra con otras piezas del ecosistema de V-Valley, el mayorista recorrerá con un camión, V-Truck, diez ciudades españolas entre el 6 de junio y el 6 de julio. Dentro del V-Truck, el mayorista ha dispuesto un CPD móvil en el que los partners podrán ver cómo funcionan las nuevas tecnologías, así como mostrar a sus clientes las posibilidades de integración con otras tales como Microsoft Azure, Suse o CheckPoint.

El objetivo de esta iniciativa, así como del Centro de Soluciones, es “ayudar a los partners en la transición a un nuevo modelo de venta de partner de valor”, apuntaba Carlos Preciado, director de la división de Soluciones de Infraestructura de Vinzeo.

Como decíamos, el V-Truck tiene previsto realizar diez paradas en su periplo por España, empezando por Zaragoza, el próximo 6 de junio y terminando por Palma de Mallorca, un mes después, habiendo pasado en el camino por Tarragona, Málaga, Sevilla, Valladolid, Bilbao, Oviedo, Santiago de Compostela y Valencia.



Enlaces relacionados

- Esprinet compra Vinzeo
- Esprinet completa la adquisición de ITway
- V-Truck

Auranet CAP Series

Wi-Fi hasta 1750Mbps

Controlador por Hardware de AP Profesionales
Gestiona Fácilmente Cientos de CAPs

Indoor Wi-Fi Solutions

Mayor Capacidad de Conexiones

Mayor Capacidad de Gestión

Mayor Estabilidad

Más información en:

TP-Link Technologies Co., Ltd | www.tp-link.es | sales.es@tp-link.com

El mayorista reúne a más de 1.700 personas y 100 fabricantes en una nueva edición de su evento primaveral

TECH DATA MUESTRA EN HOLAMETIC17

su potencial tras la integración de Technology Solutions y refuerza su papel como especialista

Tech Data ha reunido en el CCIB de Barcelona a 1.700 personas en HolaMETIC17, un evento en el que ha contado con clientes y más de un centenar de fabricantes para mostrarles, entre otras novedades, los principales avances en la integración de Technology Solutions, adquirida hace unos meses al grupo Avnet, en la estructura de Tech Data, una compra que en el mayorista norteamericano definen con una sencilla operación matemática, "uno más uno, igual a tres", señalaba en su comparecencia ante los medios de comunicación Oriol Cornudella, managing director de Tech Data Iberia, porque, como explicaba Paulí Amat, country manager de Tech Data España, "la suma de uno, Tech Data, y otro, Technology Solutions, se convierten en tres: nuevos fabricantes, un nuevo catálogo para los clientes tradicionales de Tech Data, y nuevos clientes para los productos y soluciones de la oferta hasta la fecha de Tech Data".

HolaMETIC17 ha reunido a 1.700 asistentes y ha contado con la participación de más de un centenar de fabricantes que han podido aprovechar la ocasión para, además de transmitir las principales tendencias y dar a conocer sus nuevas soluciones y productos, ver, de primera mano, cómo evoluciona la integración en Tech Data de Technology Solutions.

De paso, el mayorista ha dado a conocer su estrategia, que, tal y como explicaba Paulí Amat,

se apoya en cuatro elementos principales. El primero de ellos pasa por seguir creciendo en el entorno SMB, “el canal donde más aporta un mayorista” y en el negocio especializado, “ayudando a los distribuidores a aprovechar un negocio rentable para todos”. El segundo de los elementos es la ya mencionada integración de Technology Solutions, que, como señalaba Amat, es “la operación más grande que se ha dado en el mundo de la distribución”. En tercer lugar, apostar e invertir en nuevas tecnologías, lo que denominan Next Generation Technologies, tales como cloud, analytics, IoT, Big Data y seguridad, además de una específica de formación y educación. De hecho, en algunas de ellas, como es el caso de cloud, el mayorista ya cuenta con una posición muy destacada, que se reforzará con la llegada de Amazon Web Services o Google a su oferta, lo que se produciría en la segunda mitad del año. Y, por último, la Transformación Digital dentro de la propia Tech Data, con iniciativas como Hola Tech Data, para comunicación con los clientes, o Ecom Booster, un programa para potenciar el uso de herramientas electrónicas entre los clientes que se puso en marcha el pasado mes de septiembre y que ha generado una evolución muy significativa en el uso de las mismas. En este sentido, y de cara a la segunda mitad del año, Tech Data trabaja también en nuevos modelos de Dispositivos como Servicio, aportando flexibilidad a los clientes a la hora de adquirir los smartphones, tabletas o portátiles para su empresa, permitiéndoles ajustar su consumo y su pago a las necesidades reales en cada momento.

HolaMETIC17

Como decíamos, han sido 1.700 los asistentes a HolaMETIC17, un evento que, por primera vez ha contado con un área de mesas redondas temáticas, formato que se ha consolidado en anteriores ediciones de Metic Madrid Especialista.

Así, a la zona de exposición, que superó los 2.000 metros cuadrados de superficie, se suma la conferencia en la sala plenaria, ofrecida por Chema Alonso, CDO de Telefónica, y las mesas redondas, que pusieron en foco en cuatro grandes oportunidades en el mundo de las TI: hiperconvergencia, cloud híbrida, colaboración e Internet de las Cosas.

Además, en las habituales salas paralelas, el mayorista mostró las ventajas de las soluciones de pago por uso; Microsoft habló del papel de Azure en el terreno de la seguridad y el cumplimiento normativo, así como de la aportación de Skype for Business para afrontar ventas y proyectos, las nuevas plataformas de negocio inteligentes y el cambio digital a Cloud. Por su parte, Hewlett Packard Enterprise mostró cómo generar negocio para la empresa con Aruba Central, y las infraestructuras componibles con Synergy. Asimismo, GFK habló de gaming y otros motores de crecimiento; Context de nuevas oportunidades y tendencias en el mercado; SonicWALL de las oportunidades en el entorno de la seguridad perimetral; y Axis de cómo se puede potenciar el negocio con soluciones de vídeo, audio, analíticas y control de acceso.

HolaMETIC17 ha reunido a 1.700 asistentes y ha contado con la participación de más de un centenar de fabricantes

Mueve tu negocio a la velocidad de la movilidad y la nube

Las pymes están adoptando nuevas tecnologías, como la movilidad y el cloud, para ayudarles a competir en el nuevo entorno de trabajo móvil, y necesitan una infraestructura de red simple y fiable que pueda ser soportada por recursos de TI limitados. Aruba, una empresa de Hewlett Packard Enterprise, les ofrece una cartera integrada de soluciones de acceso inalámbrico y por cable, de seguridad y gestión de red simplificadas.

En cualquier caso, ven una estrategia triple de volumen, valor y servicios de negocio que desde Tech Data quieren aplicar en todas las divisiones, para lo que, a lo largo de este año, se irán redefiniendo los modelos de negocio hacia esta visión.

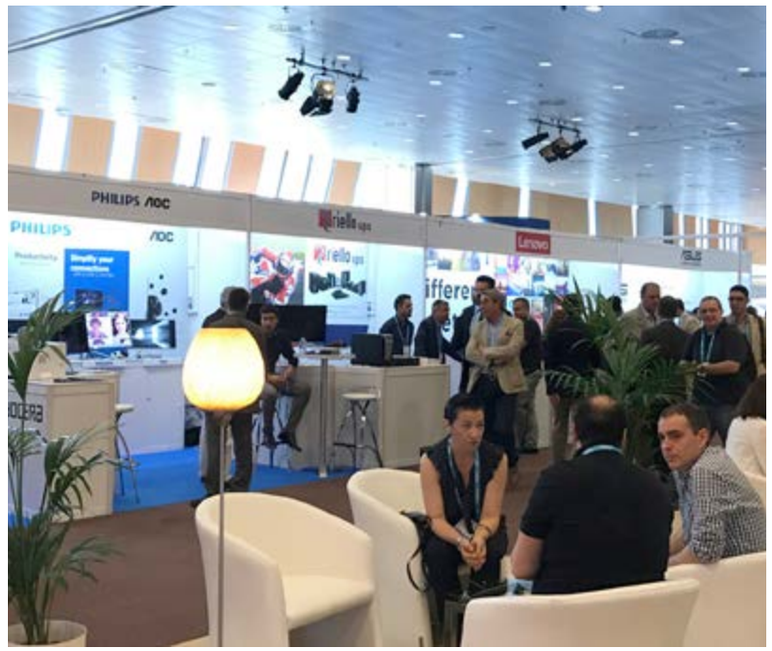
Todo esto después de un año en el que el mayorista se mantuvo en línea con los crecimientos del mercado, y que dejó un reparto de negocio por tipo de cliente que otorga al segmento SMB un 41%, al VAR un 30% y en retail un 29%, si bien señalaba el propio Paulí Amat que el negocio retail no es tanto el de la venta de productos a este tipo de clientes, sino el de los servicios que están proporcionando a algunos fabricantes en este terreno.

Si hablamos por área de negocio, podemos ver que el segmento PC representa el 23,3%, Movilidad un 26,5%, CAD un 2,9%, o Maverick un 2,6%, por poner algunos ejemplos, mientras que, si hablamos de transiciones electrónicas frente a no electrónicas, el ratio, que pone a Tech Data España a la cabeza de Europa, es de un 70% de transacciones electrónicas, casi 20 puntos porcentuales más que en septiembre, cuando se puso en marcha la ya mencionada iniciativa Ecom Booster.

Y, hablando de estas iniciativas electrónicas, el mayorista quiere seguir potenciando Hola Tech Data, su nueva plataforma de comunicación electrónica para la compañía y sus partners, con la que quieren complementar la herramienta de venta on line, InTouch, y que seguirá creciendo y ganando funcionalidades en los próximos meses.

Por último, Paulí Amat quiso detenerse en la valoración del momento que vive el mercado,

Tech Data trabaja también en nuevos modelos de Dispositivos como Servicio, aportando flexibilidad a los clientes a la hora de adquirir los smartphones, tabletas o portátiles para su empresa



una realidad positiva que, según las consultoras, se traduce en un incremento del 10%, menos de la mitad de lo que están creciendo las cifras de Tech Data, donde se aprecia, según indicaba Amat, crecimientos en el área SMB y en nuevas tecnologías donde el mayorista quiere seguir manteniendo su foco de especialización.

Integración de TS

Oriol Cornudella quiso repasar cómo se está produciendo la integración de Technology Solutions, lo que, según este responsable, "viene a reforzar la oferta de contenido y talento alrededor del negocio de valor", lo que permite decir a Tech Data que, tras esta integración, continúan siendo "una empresa de especialización". Eso sí, las cifras resultantes de la suma de ambas compañías, ponen a Tech Data "en el número uno en Europa en Distribución de tecnología", con 100.000 unidades de producto vendidas al día, más de 20.000 clientes, y más de 5.000 personas.

El foco especializado tras la integración va a estar en las tecnologías mencionadas anteriormente, seis áreas (cloud, seguridad, movilidad, convergencia, analytics y formación y educación), para las que "se van a crear equipos con recursos para desarrollar estos negocios", si bien desde Tech Data reconocen que no son divisiones que vayan desarrollándose y creciendo en paralelo, sino que llevan sus propios ritmos y desarrollos y hay que adaptarse a ellos.

En cuanto a la cobertura geográfica, Europa representará el 53 por ciento del negocio, área principal junto con Estados Unidos, si bien ya un 3% del total llegará del continente asiático.

En el caso de la Península Ibérica, hablamos de 120 empleados, más de un millar de clientes, más de 40 fabricantes y un negocio acumulado de más de 270 millones de euros, si bien, como recalcaba Santiago Méndez, Sales & Marketing director Value Added, Tech Data Iberia, y general manager, Azlan, "lo importante es el talento que hemos incorporado para las nuevas líneas de soluciones y fabricantes".

A partir de ahora, según este responsable, hay que seguir trabajando para que "se nos reconozca como un jugador de referencia en el mercado de la seguridad", y se va a potenciar la división de Educación y Formación con nuevos acuerdos de formación certificada, "porque tenemos los conocimientos, las herramientas y las capacidades para hacerlo". Además, se va a trabajar para traer a España algunos contratos que Avnet Technology Solutions tenía en Europa, pero no en nuestro país, situación similar a la que se daba en Portugal.

Enlaces relacionados

- Hola Tech Data
- Tech Data finaliza la adquisición de Avnet Technology Solutions
- Beneficios de la unión de Tech Data y Technology Solutions
- Tech Data Azlan quiere ser un referente para HPE
- El software en la economía de la Unión Europea

TRANSFORMA TU CASA EN UN
HOGAR CONECTADO

ALCATEL baby monitor · BeeWi · bq · D-Link Building Networks for People · elgato · leotec · MEDISANA · PHILIPS hue
momit · motorola · NETGEAR · POLAR · SAMSUNG · wattio · wemo

Esprinet Ibérica, S.L.U. Campus 3·84 - Nave 1 C/ Osca, 2 , Pol. Plaza 50197, Zaragoza, España • Telf. +34 976 766 110 - Fax: +34 876 296 018 • **www.esprinet.com**

El fabricante anuncia cambios en política de canal durante Fujitsu World Tour

Fujitsu traslada todo su negocio al canal de distribución

Fujitsu ha anunciado importantes novedades en materia de canal. La firma busca que todo el negocio que realiza en España sea a través de su red de partners, compuesta, en España, por 1.624 resellers. En la actualidad, el canal realiza el 71% de la facturación de Fujitsu en nuestro país.

Ha sido durante la celebración de Fujitsu World Tour cuando Francisco Rodríguez Cano, director de canal de Fujitsu España, ha anunciado las novedades que la compañía tiene para su red de venta indirecta y que buscan que todo el negocio que realice la compañía en nuestro país provenga de sus partners. Ésta es una decisión que se ha tomado a nivel europeo y que busca, sobre todo, "ganar cuota de mercado".

Estructura de venta indirecta

En la actualidad, la red de venta indirecta de Fujitsu en Europa está compuesta por 27.000 partners que realizan el 80% del negocio de la multinacional asiática en la región. En el caso de España, ésta está formada por 1.624 resellers, los cuales tienen una participación del 71% en el negocio de Fujitsu. "Queremos que el 100% del negocio se realice a través de canal". ¿El plazo? "Lo antes posible", ha des-

"Queremos que el 100% del negocio se realice a través de canal lo antes posible"

Francisco Rodríguez Cano, director de canal de Fujitsu España

tacado Francisco Rodríguez Cano. En este momento, Fujitsu se encuentra comunicando tanto a partners como a clientes los cambios que va a realizar en la política de canal. Como en todo "hay algunos clientes que se lo están tomando mejor y otros peor". No obstante, ha reconocido que esto no ha cogido por sorpresa a nadie "ya que es una tendencia en el mercado".

Para ello, Fujitsu ha realizado una reorganización territorial, dividiendo España en cuatro grandes áreas. "Cada zona tendrá un account terrotory específico y un director por geografía. Éste es un cambio importante porque ofrecemos al canal todo el apoyo necesario para realizar su labor", asegura Francisco Rodríguez Cano, quien ha explicado, también, que se ha habilitado una oficia de canal para dar soporte a los partners.

La firma también ha explicado las novedades que ha presentado en referencia a su programa de canal. Ahora, Select Partner Program "es más sencillo" ya que no hay barreras financieras para desarrollarse como un select Expert, y se ha simplificado las especializaciones. "También existen normas más claras de compromiso".

Nuevas oportunidades alrededor de PrimeFlex

Dentro de su iniciativa de canal, Fujitsu ha creado nuevas oportunidades para la línea PrimeFlex. "De una forma relativamente sencilla, el canal puede ofertar proyectos más complejos", ha destacado Francisco Rodríguez Cano. Además, ha presentado un programa de pago por uso para soluciones Eternus All-Flash. En este sentido, el director de canal ha destacado la buena marcha del negocio de almacenamiento flash, con lo que ésta representa una oportunidad de negocio para el canal. A grandes rasgos, este programa permite ofertar "una solución de almacenamiento Eternus DX 100 S4 o DX200 S4 con discos SSD". Una vez que se haya aprobado la operación por parte del área financiera, los pagos del cliente serán decrecientes (el primer año a 0,074 euros por GB, el segundo a 0,063 euros por GB y el ter-

Con esta estrategia, Fujitsu pretende continuar creciendo en el área de centro de datos "nuestro negocio más consolidado", y hacer foco en PrimeFlex

cero a 0,052 euros por GB). "El primer año es obligatorio, después puede renunciar en cualquier momento con un preaviso de seis meses sin ningún tipo de penalización ni para el cliente ni para el partner".

Nueva política de rebates

Mención especial para la nueva política de rebates. "Hemos decidido incrementarlos". De esta forma, Fujitsu ha decidido añadir un 3% de rebate en la venta de soluciones PrimeFlex. "Los resellers cobrarán este incentivo desde el primer euro" en vez de por objetivo de facturación, tal y como se cobran el resto.

Asimismo, aquellos partners que registren un proyecto en Salesforce (herramienta de gestión de clientes de Fujitsu) también tendrán un 1% de rebate adicional. Esta herramienta se engloba dentro de Fujitsu Select Connect cuyo objetivo es "automatizar la comunicación con nuestros partners para agilizar sus negocios".

Otra de las ofertas de Fujitsu para su canal, la App, se ha visto mejorada. "Hemos añadido un sistema online de mensajería" que busca mejorar la comunicación con su canal.

Áreas de crecimiento

Con esta estrategia, Fujitsu pretende continuar creciendo en el área de centro de datos "nuestro negocio más consolidado", y hacer foco en PrimeFlex, "resultado de grandes alianzas".

Francisco Rodríguez Cano también ha tenido palabras para el negocio de PC. "No espera-

EN QUÉ CONSISTE FUJITSU CLOUD SERVICE K5

CLICAR PARA VER EL VÍDEO

mos crecer, aunque hemos tenido buenos resultados en el área de empresa".

En cuanto a sus resultados, "hemos crecido un 7% en el área de servicios, en el mercado CCD hemos estado en línea con el mercado y también hemos crecido en la venta de Eternus y Primergy".

Fujitsu ha decidido añadir un 3% de rebate en la venta de soluciones PrimeFlex

Mayoristas

Francisco Rodríguez Cano también ha tenido palabras para su canal mayorista. En la actualidad, éste está compuesto por 5 fuguras: Arrow e Ingram Micro para la parte de valor, Aryan y Valorista para la de volumen y GTI, con el que la compañía comenzó a trabajar hace ocho meses aproximadamente y "con el que estamos muy contentos". ¿El motivo? "GTI tiene un nivel de partners, de conocimiento del área de software que nos ayudará en el mercado". Además, "nosotros le ayudamos a posicionarse en la venta de hardware". it

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- Información sobre Cloud K5
- Toda la información sobre la oferta de Fujitsu para el canal
- Hábitos sobre una TI híbrida
- Barómetro de emprendimiento de éxito en España
- Bankia Índicex. La digitalización de las empresas en España
- Plan Digital 2020. La digitalización de la sociedad española

La gama PowerLine convierte los enchufes de tu casa en emisores Wi-Fi, ampliando la cobertura a cuaqluier rincón de tu hogar.

- Donde haya un enchufe, hay Wi-Fi.
- Conéctate a la Wi-Fi desde cualquier dispositivo en toda tu casa.
- Utiliza PLC con enchufe incorporado para no desperdiciar ni una sola toma de corriente.
- Enchufar, Emparejar y ¡Disfrutar de la Wi-fi!.

Kit Powerline Wi-Fi AC Gigabit AV1200
con enchufe incorporado: TL-WPA8630P KIT

Saber más...

DMI Computer

TP-Link Technologies Co., Ltd. | www.tp-link.es | sales.es@tp-link.com

La Jornada sobre Ciberseguridad remarca la importancia de este sector

España quiere ser un referente en ciberseguridad

José Antonio Nieto Ballesteros, Secretario de Estado de Defensa en el Ministerio del Interior, ha analizado la evolución de la ciberdelincuencia durante la Jornada de Ciberseguridad organizada por el Club Diálogos para la Democracia, en la que también se han explicado cuál es la estrategia de nuestro país. La intención del Ministerio es lograr que España sea un referente en seguridad digital, al igual que lo es en seguridad física.

Durante la Jornada de Ciberseguridad, organizada por el Club Diálogos para la Democracia, José Antonio Nieto Ballesteros, Secretario de Estado de Defensa en el Ministerio del Interior, ha explicado que nos encontramos ante una nueva realidad digital que ya se encuentra al mismo nivel "que el resto". Asimismo, ha hecho un repaso a la situación de la ciberseguridad en nuestro país.

En este sentido, ha recordado que hay 7.395 millones de personas en el mundo, de los que el 46% se conecta a Internet, "lo que supone que hay más gente con acceso a la Red que con acceso a agua potable"; el 31% utiliza redes sociales; el 51% dispone de un teléfono móvil; y el 27% de la población mundial se conecta a Internet desde sus dispositivos móvil". Ante estos datos "nuestro mundo está virando. La sociedad se está adaptando a una nueva realidad".

En opinión de José Antonio Ballesteros, "hay que utilizar la revolución digital en beneficio de la humanidad. Necesitamos potenciar el uso de Internet para la educación y no convertirlo en una amenaza".

En este punto, el Secretario de Estado de Defensa del Ministerio del Interior ha asegurado que "es necesario que las administraciones se adapten" de tal manera que "no se dejen grietas para las ciberamenazas".

Las cifras de Daesh en Internet

Una de las grandes preocupaciones actuales es el ciberterrorismo. Así lo ha destacado José Antonio Nieto Ballesteros, Secretario de Estado de Defensa del Ministerio del Interior, quien ha asegurado que "Daesh ha descubierto la potencialidad de Internet para sus fines", siendo la labor de captación el principal objetivo. "El mal se desarrolla bien", ha destacado Nieto Ballesteros, quien ha destacado que Daesh ha sabido utilizar las redes sociales e Internet como herramienta de propaganda, de captación, de formación, y de financiación.

"La conversión del terrorismo se ha convertido en un fenómeno viral", ha señalado Nieto Ballesteros, quien ha recordado que los últimos atentados que ha sufrido Europa se realizaron por personas que "fueron captadas, adiestradas y encaminadas" en Internet.

Según cifras aportadas por Nieto Ballesteros, Daesh ha sido capaz de captar a 35.000 personas en Internet. La organización terrorista dispone de "46.000 cuentas en Twitter, de las que 6.000 cuentas utilizan bots".

"Al mismo ritmo que pierde en el espacio físcio, lo gana en la Red", ha destacado el Secretario de Estado de Defensa, quien ha explicado que ya se habla del "Cibercalifato Unido", una organización que une grupos de hackers al servicio de Daesh.

Rob Wainwright, director de Europol, "informó de que se había encontrado más de 2.000 elementos extremistas en 52 plataformas".

Durante su intervención, Antonio Nieto Ballesteros ha destacado la labor de las fuerzas y cuerpos de seguridad del estado en esta materia. "El trabajo frente al ciberterrorismo ha sido un éxito". Esto se ha debido a que "conocemos la potencialidad de las ciberamenazas en la Red", con lo que "no estamos esperando a que se produzca un atentado, sino que tratamos de anticiparnos y luchar desde el origen".

Esto se ha debido a que "tristemente conocemos el daño del terrorismo yihadista" con el 11-M como referente. Desde ese momento, "se han realizado 230 operaciones policiales que han tenido como resultado la detención de 761 personas". Sólo esta legislatura (el Congreso se constituyó en julio de 2016), se han realizado 50 operaciones con 81 detenidos".

Para luchar contra el ciberterrorismo José Antonio Nieto Ballesteros aboga por la cooperación pública de todos los Ministerios y comunidades autónomas; la cooperación público privada con sectores sociales y la cooperación internacional. En este último punto, destacó que es imperativo contar con una estrategia común a nivel de la UE. "España ha realizado una apuesta clara para que haya una defensa global en la UE".

"La cooperación está haciendo que España se proteja y se proteja bien",

Juan Antonio Nieto Ballesteros, Secretario de Estado de Defensa del Ministerio del Interior

Preocupación en Europa

La ciberdelincuencia "permite la deslocalización y dificulta la labor policial", ya que "en casi todas sus acciones existe un componente internacional que dificulta el conocimiento". A todo esto, hay que unir que "el acceso a herramientas básicas de hacking cada vez es más sencillo", lo que está provocando que "se esté incrementando el número de la ciberdelincuencia en el mundo". No en vano, el cryptoware

"Hay que concienciar a los usuarios del problema del uso de la tecnología y de sus riesgos",

Luis Jiménez Muñoz, Subdirector del Centro Criptológico Nacional

"es el principal tipo de malware en Europa". La ciberdelincuencia cada vez comete más acciones "como el robo de identidad, el fraude financiero, el robo de datos en redes sociales o la explotación infantil".

Es tal la preocupación que ha alcanzado que la UE ya ha incorporado el ciberterrorismo o el crimen organizado "en su variante cibernética" a su estrategia de seguridad.

En el caso de España, en 2016 se produjeron 66.586 ciberdelitos, un 10,7% más que en 2015, siendo el fraude y las estafas y las ciberamenazas los principales actos delictivos denunciados. "En el primer trimestre de este año, el número de ciberdelitos se ha incrementado en un 22,3% en comparación con el mismo periodo del año anterior" y "el 25%de los usuarios de Internet en España ha sufrido ataques de algún virus.

Cooperación, la solución

Para luchar contra este tipo de delitos José Antonio Nieto Ballesteros aboga por la cooperación pública de todos los Ministerios y comunidades autónomas; la cooperación público privada con sectores sociales y la cooperación internacional.

En el primer punto "la Secretaria de Estado de Defensa del Ministerio del Interior colabora estrechamente con la Secretaria de Estado para la Sociedad de la Información y la Agenda Digital, así como con organismos como INCIBE o el CERT". La colaboración se extiende a otros Ministerios, como el de Justicia, "que nos está permitiendo reformar el código penal".

Este clima de cooperación "está haciendo que España se proteja y se proteja bien" ya que "lo que es seguro es que nos van a atacar".

Además de cooperación, José Antonio Nieto Ballesteros aboga por "educar a la sociedad civil", si no "es imposible que venzamos".

Perspectivas España 2017

Este informe, realizado por KPMG, con la colaboración de la CEOE, recoge la opinión de empresarios y directivos españoles sobre la situación económica actual y sus expectativas a corto y medio plazo. El contenido de este estudio se basa en una encuesta llevada a cabo durante los meses de noviembre y diciembre de 2016, que incluye algunas cuestiones recurrentes de carácter general sobre expectativas económicas y de gestión empresarial, y otras especificas en función de la coyuntura, tales como la transformación digital y el impacto del Brexit.

"La revolución digital es un hecho, no lo vamos a frenar y no la queremos frenar, pero hay que saber aprovecharla de manera segura". José Antonio Nieto Ballesteros ha finalizado destacando que "igual que España es una referencia en materia de seguridad física, queremos que lo sea en materia digital".

Nueva visión de la ciberseguridad

Por su parte, Enrique Cubeiro Cabello, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa, ha querido transmitir la visión militar sobre Ciberseguridad. Cubeiro ha definido el ciberespacio como el "quinto dominio de la guerra". El peligro reside en que se trata de un espacio en el que "no existe ningún tipo de control armamentístico y la infinidad de grupos, organizaciones e individuos aislados con muy diversas motivaciones tienen la capacidad de provocar daños muy graves en la sociedad". Por lo tanto, "coloca el corazón de una nación en primera línea de combate". Sin embargo, aunque las ciberamenazas son reconocidas como uno de los principales riesgos para la seguridad de la nación, "aún no hemos conseguido culminar ese gran paso que va de las palabras a los hechos".

Marcos Gómez, Subdirector de Servicios de Ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE) ha destacado durante su intervención de que "hay un hecho constatable y es que en el ciberespacio hay grandes oportunidades de todo tipo: sociales, económicas, Pero también hay ciberamenazas y riesgos, y por lo tanto hay que seguir trabajando en la detección y mitigación de los mismos". Y ha concluido asegurando que "esto es un trabajo de todos los agentes públicos y privados".

"El ciberespacio es el quinto dominio de la guerra",

Enrique Cubeiro Cabello, Jefe de Operaciones del Mando Conjunto de Ciberdefensa del Estado Mayor de Defensa

Luis Jiménez Muñoz, Subdirector del Centro Criptológico Nacional, ha destacado que para prevenir la "ingeniería social" que desarrolla los virus del tipo del ya famoso WannaCry, lo primero que hay que hacer es "concienciar a los usuarios del problema del uso de la tecnología de la información y de sus riesgos". A continuación, "hay que formarles, dotarles de conocimientos, habilidades y práctica".

WannaCry, presente en la jornada

Y WannaCry Durante la jornada, Nieto Ballesteros, hizo una valoración del ciberataque de WannaCry, asegurando que éste tuvo "un impacto en extensión y en profundidad" al afectar a 180 países y más de 300.000 ordenadores.

El Secretario de Estado de Defensa defendió el nivel de preparación de nuestro país ante amenazas de este tipo asegurando que, en el caso concreto de WannaCry, "España reaccionó con rapidez y agilidad" lo que hizo que "los efectos fueran muy limitados".

Asimismo, también se refirió a la actuación de Telefónica, una de las primeras grandes compañías en comunicar que estaba siendo víctima de un ciberataque. "Telefónica demostró que la mejor manera de hacer frente a un ciberataque como el de WannaCry es no ocultarlo".

Antonio Gavilanes Dumont, presidente del Club Diálogos para la Democracia, también se refirió al ataque de WannaCry, remarcando la

importancia que está adquiriendo la ciberseguridad y recordando que una de las "víctimas" más preocupantes fue el sistema de salud británico, al ser un servicio básico para los ciudadanos. "Debemos adoptar estrategias de prevención ya que se van a producir más ataques de este tipo".

Valoración de Telefónica

José Luís Gilpérez, director ejecutivo de Administraciones Públicas, Defensa, Seguridad y Big Data en Telefónica también valoró el ciberataque y la actuación de la operadora española.

En este sentido, Gilpérez ha asegurado que la estrategia que llevó a cabo Telefónica basada "en la confianza y la transparencia" fue "ya no sólo la adecuada, sino valiente". En su opinión, "el comportamiento responsable de Telefónica" a la hora de comunicar "de manera muy temprana" que estaba siendo víctima de un ciberataque ayudó a paliar los efectos que WannaCry hubiera tenido en España.

"El impacto real que ha tenido el incidente para la compañía, y el impacto real que ha tenido para la Administración, las empresas privadas y los ciudadanos, ha sido cero", ha asegurado José Luis Gilpérez, quien ha reiterado que WannaCry no afectó "a ninguno de los servicios que prestamos" los cuales "son esenciales para los ciudadanos, para las empresas y para las administraciones públicas".

Asimismo, el directivo de Telefónica ha explicado que nada más conocer que la operadora estaba siendo víctima de un ciberataque "se puso en marcha el protocolo de actuación, liderado por nuestro comité de seguridad". Éste "es el que decide cómo se tiene que actuar ante este tipo de situaciones".

Gilpérez, asimismo, ha recordado que ésta "no es la primera vez que tenemos que hacer frente a un incidente de este tipo". WannaCry "utilizó un vector de propagación habitual en las redes LAN", con lo que "sabemos cómo actúa, cómo se propaga, cómo se detecta y qué medidas tenemos que adoptar de manera inmediata".

Para Gilpérez "el protocolo y las medidas adoptadas fueron las correctas". Además, "la transparencia con la que actuó Telefónica hace que esté muy orgulloso de cómo reaccionó la compañía".

El directivo también destacó que Telefónica no perdió información de ningún PC de los que fueron atacados "ya que ésta no se encuentra en los equipos, sino que están en la cloud". it

Enlaces relacionados

- Ataques con exploits: de las amenazas diarias a las campañas dirigidas
- Informe Symantec sobre la seguridad de Internet (ISTR 2017)
- Informe sobre la responsabilidad de las entidades financieras ante el fraude electrónico
- Informe global sobre Seguridad de la Información 2016-2017 de EY
- La paradoja tras la experiencia del usuario de cripto-ransomware

La firma celebra una nueva edición de Agility en Barcelona

F5 Networks se centra en el área de sistemas para reclutar canal en España

Ha sido durante la celebración de Agility 2017, evento que F5 Networks llevó a cabo el pasado mes de mayo en Barcelona, cuando la firma ha presentado su estrategia para ayudar a las empresas a acelerar su Transformación Digital. "Damos la libertad a nuestros clientes desarrollar apps en cualquier momento y lugar".

Bárbara Madariaga. Barcelona.

François Locoh-Donou, recientemente nombrado presidente y CEO deF5 Networks, hizo hincapié, durante la inauguración de Agility 2017, evento que celebró en el proceso de transformación que se está produciendo en todas las industrias. "Hay muchas oportunidades tras el cambio" y ha señalado a Internet de las Cosas, la Seguridad y la Cloud como las tres grandes tendencias "que marcarán el futuro de las empresas en los próximos cinco años" ya que "serán las áreas tecnológicas más dinámicas".

"Somos expertos en aplicaciones y en infraestructuras", destacó Locoh-Donou haciendo referencia a que su firma puede ayudar a sus clientes en su viaje hacia la nube.

Durante su charla en Agility 2017, Locoh-Donou explicó la importancia que tiene la región EMEA para su compañía. "Tenemos una gran presencia en Europa, con 22 oficinas y muchos partners y clientes".

Sangeeta Anand, vicepresidente senior de gestión de producto y marketing de producto de F5 Networks, aprovechó su intervención para asegurar que DevOps, la movilidad y la cloud marcan el futuro de un sector en crecimiento. "El 73% de las empresas disponen de una estrategia de cloud híbrida, un 66% utilizan la cloud privada, y un 63% prefiere la cloud pública. Sólo un 8% no tiene interés en la nube". Con estos datos en la mano, Anand mostró la apuesta de la firma por ser un jugador esencial a la hora de ayudar a las empresas en su viaje hacia la cloud. "Un 85% de las empresas está comprometida con la arquitectura multicloud".

En este sentido, Anand volvió a remarcar que su compañía ofrece "libertad a las empresas para desarrollar aplicaciones en cualquier lugar" a través de "servicios de apps consistentes y seguros".

Importancia de la seguridad

John Kuhn, director senior de gestión de producto de seguridad de F5 Networks, centró su

presentación en explicar en qué consiste Security Application-Centric. Para ello se refirió al creciente número de amenazas y ataques. “La transformación de las aplicaciones ha provocado que haya nuevas amenazas”. La oferta de la firma se basa en ofrecer un mayor control sobre el acceso a las apps, a través de servicios centralizados y analítica de riesgos. Con esto, la firma ofrece protección para las aplicaciones, además de que dispone de una estrategia de seguridad que cubre todos los niveles.

F5 Networks quiere acelerar el viaje de las empresas hacia la multi-cloud y para ello ha realizado cuatro grandes anuncios en Agility 2017

Cohe-Laloum también se refirió a la Identidad Digital que ésta “se ha convertido en uno de los valores más preciados”. La actividad de “los hackers y de los Gobiernos” han puesto de manifiesto “la importancia de mantener los datos seguros”.

CONSEGUIR EL ÉXITO EN UN MUNDO MULTI-CLOUD

CLICAR PARA VER EL VÍDEO

La tecnología permitirá “a los humanos tener un mayor control de sus datos” y F5 Networks facilita esta labor “al desarrollar aplicaciones más rápidas, más seguras y más inteligentes”.

Cuatro grandes anuncios

En Agility 2017 la firma realizó cuatro grandes anuncios que permiten a las empresas “ofrecer de forma consistente servicios de aplicación en entornos multi-cloud, proporcionándoles

Alex López, country manager de F5 Networks Iberia

"Nos encontramos en un momento en el que queremos reclutar canal"

Durante F5 Agility 2017, un evento en el que ha reunido a partners y clientes para explicarles cuál es su propuesta para acelerar el viaje a la cloud de las empresas. Más allá de las cuatro novedades presentadas por la firma en el marco de Agility 2017, F5 Networks ha aprovechado para destacar la importancia que tiene su red de venta indirecta a la hora de cosechar buenos resultados.

Al igual que el resto de las compañías, el canal de distribución TI está en plena transformación. "El mundo de las comunicaciones y de los sistemas está en un momento de convergencia", destaca Álex López, country manager de F5 Networks para Iberia. "Tradicionalmente, nosotros trabajábamos con partners que están especializados en el mundo de comunicaciones". Aunque la intención de la firma es continuar trabajando con este tipo de reseller, Álex Lopez confirma que la intención es ampliar su red de venta indirecta con nuevos socios especializados en sistemas. "Nos encontramos en un momento en el que queremos reclutar canal".

El perfil de partner con el que quiere trabajar F5 Networks "es aquel que aúne conocimientos de los dos mundos", algo que, según Álex López, "está resultando complicado".

En ese momento, F5 Networks se está poniendo en contacto con "figuras propias del mercado de sistemas", aunque "también estamos tratando de averiguar cuáles de nuestros partners tradicionales de comunicaciones están empezando a trabajar en el mundo de sistemas".

La problemática para encontrar nuevo canal "no sólo es de F5 Networks", sino "de todo el sector", debido a que el canal se encuentra también en un proceso de transformación.

La tendencia es la cloud "y si un determinado partner está acostumbrado a otro tipo de negocio tiene que adaptarse".

Es más, y tal y como destaca Álex López, "cuando se produce un proceso de transformación en el mercado, como el que estamos viviendo en la actualidad, los partners tienen que pensar más allá para adaptarse o arriesgarse a que otro tipo de empresas absorban su negocio".

Álex López recuerda que el core de F5 Networks "sigue siendo el mismo, aunque en otro entorno".

En la actualidad, F5 Networks trabaja con tres tipos de partners: el propio de comunicaciones, los operadores (un canal muy importante para la firma desde el punto de vista de los servicios gestionados) y sistemas. "En este último tipo de reseller estamos en una fase muy inicial" en la que "nos estamos dando cuenta que es un segmento que se encuentra muy atomizados, donde hay un gran número de empresas de tamaño medio con un carácter local".

La intención de la firma es que de aquí a un año "dispongamos de un canal de sistemas conformado".

una mayor flexibilidad en su implementación, una seguridad más eficaz y un time-to-market más rápido", destacaron los principales directivos de la compañía.

Uno de los grandes beneficios que ofrece la compañía a las empresas, tal y como explicó Sangeeta Anand, vicepresidente senior de Gestión de Producto y Marketing de Producto en F5, es que "damos la libertad a nuestros clientes de desarrollar apps en cualquier momento y lugar". Aplicaciones "más rápidas, más inteligentes y más seguras"

2º Estudio de Competencias Digitales en la Empresa Española

El objetivo principal del estudio es realizar un diagnóstico sobre la situación actual de las empresas españolas en su relación con las competencias digitales. La estrategia orientada a la Atención al Cliente es la competencia digital más relevante para los directivos entrevistados, seguida de una mejora en el pago online y el aprovechamiento de la industria 4.0.

La estrategia de F5 Networks es una respuesta a las demandas de las empresas, que eligen "cada vez con más frecuencia" por desplegar aplicaciones múltiples en "clouds públicas y privadas, fuera y dentro de sus propios centros de datos" y que tienen que hacer frente a una serie de retos como "la gestión de diferentes entornos de desarrollo, grupos de herramientas y tecnologías de orquestación". En opinión de Anand," estas nubes proporcionan servicios para las aplicaciones de una manera no suficientemente portable o con una protección inadecuada".

En cuanto a los cuatro grandes anuncios que ha realizado F5 Networks en el marco de Agility 2017 éstos se centran en "ofrecer entornos diferentes para el despliegue de servicios".

> "Somos expertos en aplicaciones y en infraestructuras",
>
> François Locoh-Donou, presidente y CEO de F5 Networks

El primero de ellos es la disponibilidad de F5 BIG-IP Virtual Edition (VE) en Google Cloud, "con lo que ofrecemos soporte para el entorno de Google"; el segundo es la disponibilidad de Application Connector, con el que "ofrecemos servicios de aplicaciones desde el borde de la nube pública descubriendo automáticamente las cargas de trabajo alojadas en la nube de AWS", ofreciendo, sobre todo, "consistencia y seguridad"; el tercero es la disponibilidad, en DockerStore, del Proxy de Servicios de Aplicación; y el cuarto es el paquete de nube privada de OpenStack, con el que "aceleramos el despliegue en entornos OpenStack".

El futuro de las apps

Tras hacer un repaso a los principales cambios que se están produciendo en el mercado, con tecnologías como la Inteligencia Artificial, la movilidad, o Internet de las Cosas, entre otras, Lizzie Cohe-Laloum aseguró que el éxito de las empresas pasa por ofrecer a sus clientes verdaderas experiencias digitales. No en vano,

> "Los partners tienen que pensar más allá para adaptarse o arriesgarse a que otro tipo de empresas absorban su negocio"
>
> Alex López, country manager de F5 Networks Iberia

según el informe el Futuro de las Aplicaciones de la compañía, el 71% de los consumidores de EMEA "necesitan satisfacer su deseo de nuevas experiencias". Facilitar a las empresas esa tarea es una de los grandes objetivos de la compañía.

Según el informe, las organizaciones necesitan adaptarse a la nueva realidad de una manera rápida, además de que tienen que desarrollar modelos de colaboración proactiva y transparentes. "Esto es crucial en un contexto en el que la nueva normativa de Protección de Datos de la Unión Europea marcará la evolución de la economía digital, al igual que Internet de las Cosas, la Inteligencia Artificial o el machine learning".

El informe también pone de manifiesto la importancia de la seguridad. De hecho, y según el mismo, las "prácticas de datos seguras y enfocadas al consumidor" podrían emerger y convertirse en un estándar "equivalente a la sostenibilidad o el impacto medio ambiental". Asimismo, se producirán cambios en materia de protección de datos personales y a quién pertenecen. "La tendencia es que los usuarios se decanten por controlar y gestionar los datos de manera proactiva".

El informe señala que el futuro de las apps estará definido por la Inteligencia Artificial y el machine learning. "Es probable que los desarrollos en este campo incluyan servicios más personalizados y predictivos en áreas como la salud cognitiva".

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- Informe Desmitificando el panorama de amenazas
- Guía sobre estrategias de Protección DDoS: eligiendo el modelo correcto
- Informe La seguridad en los dispositivos IoT
- Informe El futuro de las Aplicaciones
- Informe sobre la responsabilidad de las entidades financieras ante el fraude electrónico
- Tecnología para hacer frente al fraude financiero
- Bankia Índicex. La digitalización de las empresas en España
- Plan Digital 2020. La digitalización de la sociedad española

Claves para la **automatización de procesos** y **servicios IT** con **ServiceNow**

#ITWebinars

22 de junio de 2017
11:00 A.M. (CET)

Regístrate

it User TECH & BUSINESS

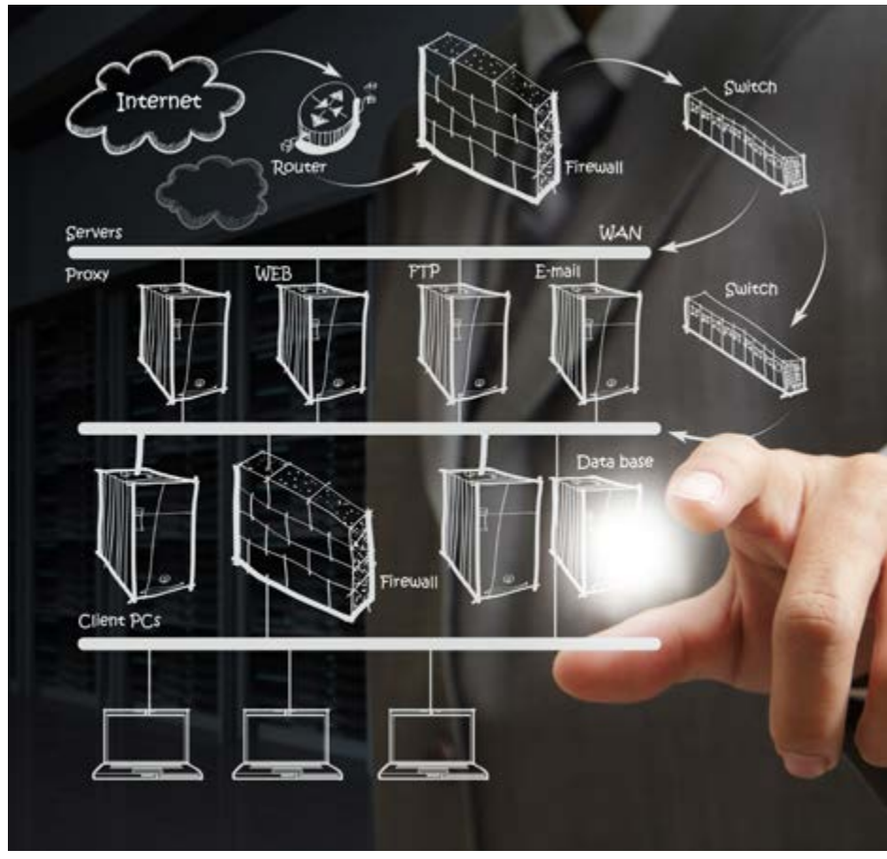
serem

servicenow®

Un estudio de GTDC revela el cambio en el rol de la distribución

El mercado europeo de TI crece a buen ritmo impulsando al canal

El mercado europeo de tecnología, a pesar de tener que estar haciendo frente a nuevos retos con el Brexit o las diversas elecciones, crece. En este crecimiento, el canal de distribución tiene mucho que ver a pesar de que se encuentra en un momento en el que la aparición de nuevas figuras, y nuevos mercados, está haciendo que su rol se transforme.

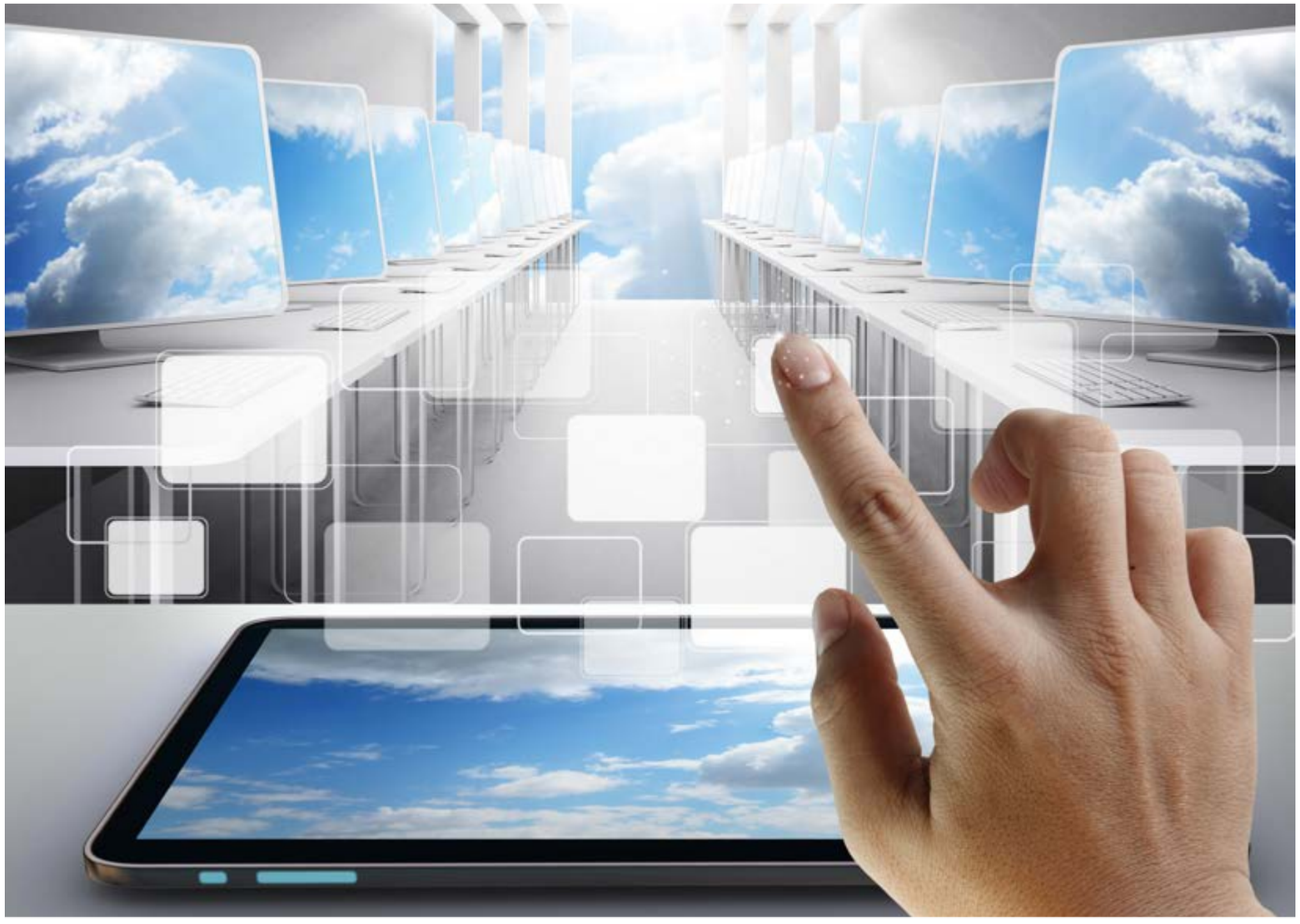


Según datos del GTDC, el primer trimestre fue sólido para la distribución de TI en Europa. A pesar de las dudas en el Reino Unido sobre las consecuencias del Brexit y el impacto de las elecciones que se han producido en Francia y que afectará a Alemania a finales de este año, la distribución de TI se mostró fuerte en los principales mercados.

En este sentido, el CEO del Global Technology Distribution Council (GTDC), Tim Curran, afirma que "nuestra investigación muestra al menos dos meses de crecimiento realmente bueno en Europa en su conjunto". Los sectores de telecomunicaciones y portátiles están funcionando con fuerza, así como otras áreas de nueva tecnología, como Internet de las Cosas. Varias categorías de productos de IoT crecieron fuertemente en febrero, los dispositivos optoelectrónicos y, especialmente, los sensores, experimentaron un crecimiento constante en Europa. Las ventas de chips para aplicaciones específicas también fueron positivas en Europa en comparación con el mes anterior.

Sectores que crecen… y decrecen

El sector de IoT está creciendo rápidamente, pero Gartner ha advertido que necesitará el soporte del canal de TI para ser eficaz: Nick Jones, vicepresidente y analista de Gartner, afirma que "IoT exige una amplia gama de nuevas tecnologías y destrezas que muchas organizaciones aún no han dominado. Un tema recurrente en el ámbito de IoT es la inmadurez de las tecnologías y servicios y de los vendedores que las proveen. Acabar con esta inmadurez y gestionar el riesgo que crea será un desafío



El sector de IoT está creciendo rápidamente, pero Gartner ha advertido que necesitará el soporte del canal de TI para ser eficaz

PC tradicionales en EMEA se estabilizaron en el cuarto trimestre de 2016, registrando una cifra cercana a cero y alcanzando los 20,7 millones de unidades vendidas, según IDC, los portátiles tuvieron un buen rendimiento en todas las regiones de EMEA, con una subida anual del 2,9%, y del 2,7% en Europa Occidental. La fuerte demanda se disparó en el segmento profesional, que creció un 10,1% en Europa occidental.

Cambio de rol en la distribución

A pesar de los buenos datos del sector, la distribución está cambiando rápidamente y, especialmente en Europa, está encontrando un nuevo rol como proveedor de servicios cloud, de comercio electrónico, de logística especializada y de soporte para el canal durante su transición a nuevos modelos de ingresos.

Además de proporcionar cobertura, incorporación y reclutamiento de nuevos canales en todos los mercados de Europa, el informe del GTDC identifica algunas de las formas en que

clave para las organizaciones que explotan el IoT. En muchas áreas de la tecnología, la falta de aptitudes plantea desafíos significativos". Los distribuidores ya están invirtiendo en esta área y se están preparando para respaldar a los partners con sus propios recursos.

Pero, no todo el crecimiento está en las nuevas tecnologías. Mientras que las ventas de

la distribución está trabajando para desarrollar nuevas líneas de negocio, en especial en los servicios, donde el paso a la adopción de la nube hace que sea mucho más fácil para los desarrolladores y proveedores de soluciones crear soluciones, pero donde todavía necesitan formas de llegar a sus clientes potenciales.

Los proveedores citados en el informe dicen que están utilizando la distribución para acceder a los mercados, en lugar de tener que abrir oficinas locales y proporcionar más recursos locales. Como explica Jeff Ready, CEO de Scale Computing, “en el pasado hemos utilizado un modelo de distribución de un solo nivel, pero ahora podemos usar la distribución para ejecutar y promover las relaciones de canal”. La distribución es clave para su negocio: “Tener un verdadero distribuidor valor añadido es importante y juega un papel importante en hacer que el canal sea parte de una comunidad efectiva”, apunta Ready.

Por otro lado, los canales se enfrentan con frecuencia a una oleada de nuevas líneas de productos potenciales, cada una de las cuales requiere una cuidadosa evaluación. Pocos jugadores del canal tienen los recursos para investigar el mercado continuamente, y trabajar en estrecha colaboración con los distribuidores puede guiarles en cuanto a qué productos van a ser los ganadores.

Según el director general de GTDC Europe, Peter van den Berg, La distribución ya no se trata sólo de recoger, empaquetar y enviar un producto. Los servicios que se ofrecen son muchos y variados, y se utilizan para complementar lo que el canal está haciendo. “El 65% del negocio de uno de los miembros más grandes de GTDC está ahora en los servicios”, asegura van den Berg, añadiendo que, “en los últimos dos años, los miembros de la GTDC han agregado más de 600 nuevos proveedores, por lo que son una buena fuente e indicador para los socios de canal que buscan ver qué productos y servicios tendrán éxito”.

La distribución europea está encontrando un nuevo rol como proveedor de servicios cloud

Enlaces relacionados

- El canal y la nube: oportunidades y retos
- La verdad sobre el ecosistema IoT
- La transformación de sector retail
- X Encuesta Mundial sobre el coeficiente digital de las empresas
- Barómetro del emprendimiento del éxito en España
- Bankia Index 2016: La digitalización de las empresas en España

Estrategias para la implementación de infraestructura hiperconvergente

Una opción de arquitectura de centro de datos hiperconvergente ofrece una nueva forma de reducir los costes y alinear mejor la TI de la empresa con las necesidades del negocio. En su forma más básica, la infraestructura hiperconvergente es el conglomerado de los servidores y dispositivos de almacenamiento que componen el centro de datos. Estos sistemas están integrados ofreciendo una gestión completa y fácil de usar. Aprende las mejores prácticas para evaluar, planificar y comprender el impacto potencial de la infraestructura hiperconvergente en tu centro de datos con esta guía.

Descubre cómo el CIO de Acer ha liderado la selección de software

ACER, uno de los principales fabricantes del mundo de PC, ha unificado los procesos de planificación, simulación y Business Analytics en una sola plataforma, simplificando los procesos de toma de decisiones y el entorno IT. Descubre cómo el CIO de ACER ha liderado la selección de software y el Proof of Concept, cuáles han sido los criterios de selección, las principales características consideradas y las soluciones software comparadas para una compra razonada, capaz de crear valor dentro de la empresa.

Impacto económico del desarrollo de aplicaciones de negocio con ServiceNow

Forrester ha analizado el potencial retorno de la inversión que las empresas pueden obtener tras implementar la plataforma de desarrollo de aplicaciones Now, proporcionada por ServiceNow, y cuyo objetivo es ayudar a los clientes a acelerar esos procesos y su digitalización. Entre los datos del estudio, destaca el hecho de que los trabajos de desarrollo se aceleraron en un 290%, permitiendo la entrega de beneficios seis meses antes de lo previsto.

6 consejos para aumentar la colaboración en DevOps y mejorar el rendimiento

Cuando fallan las aplicaciones, ¿de quién es la culpa? En el mundo DevOps actual, cada actor en la cadena de la entrega de aplicaciones cuenta para el rendimiento. En este libro encontrarás consejos para aumentar la colaboración y mejorar el rendimiento de cada uno de los roles que componen el equipo DevOps: el negocio, los ingenieros, la parte de pruebas y el equipo de operaciones.

La Documentación TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

WannaCry muestra cómo un ransomware puede desencadenar "la tercera guerra mundial"

A mediados del mes de mayo, un ransomware que aprovechaba una vulnerabilidad, ya parcheada, de Microsoft sembró el caos a nivel global. Se trataba de WannaCry, un "virus" que atacó a más de 300.000 de 180 países. Este ciberataque puso de manifiesto la importancia de estar alerta y preparado para hacer frente a una amenaza que puede causar más daños de los que se creen.

Fue el pasado 12 de mayo cuando se produjo uno de los ciberataques a nivel global más importantes que se recuerda. WannaCry, un tipo de ransomware que aprovecha una vulnerabilidad de Windows, comenzó a "secuestrar" ordenadores, siendo España uno de los primeros objetivos del mismo.

La voz de alarma saltó con Telefónica. La operadora española confirmó que estaba siendo víctima de un ciberataque asegurando que WannaCry había logrado penetrar en su red interna. Los hackers solicitaron el pago de un rescate en bitcoin, la popular moneda virtual, de unos 275 euros por ordenador y dieron un plazo de una semana para pagar. En caso de que ésta se negase amenazaron con borrar los archivos a los que habían tenido acceso. Aunque Telefónica no comunicó el número de ordenadores a los que los hackers habían tenido acceso, sí que aseguro que eran "cientos".

Pero Telefónica no fue la única gran empresa víctima de WannaCry en nuestro país. Gas Natural ordenó a los empleados que apagasen sus PC después de que apareciesen mensajes similares en la pantalla de los PC de algunos empleados exigiendo un rescate en bitcoin, la misma medida que puso en marcha Iberdrola.

En un primer momento, también se aseguró que otras empresas como BBVA, Vodafone o Capgemini habían sido víctimas del ataque, aunque las tres entidades negaron el hecho. Según INCIBE, el ataque afectó a 1.200 compañías y España ocupó el puesto 16 del ranking de naciones más atacadas.

Expansión internacional

España fue uno de los primeros países en ser atacado, pero no el único. Una de las víctimas más preocupantes fue el sistema de salud del Reino Unido. Este hecho puso de manifiesto la importancia que está adquiriendo la ciberseguridad, haciendo que llegase a la escena política. No en vano, el Partido Laborista acusó al Gobierno de Theresa May de dejar al Servicio de Salud vulnerable. “Para ser honesto, la respuesta del Gobierno ha sido caótica”, ha asegurado el portavoz de saludo del Partido Laborista, Jon Ashworth. “No han hecho caso de las advertencias de los expertos. Ahora entendemos lo que han hecho en las últimas semanas. Lo cierto es que si vas a recortar los presupuestos de infraestructura y no vas a permitir que el NHS invierta en mejorar su TI, vas a dejar a los hospitales abiertos a este tipo de ataques”.

Francia fue otro de los países que sufrió la virulencia de WannaCry, con Renault como máximo exponente. Giullaume Poupard, director de la agencia de seguridad cibernética de Francia, advirtió que los ataques continuarán “de manera regular” los próximos días o semanas.

En el caso de Rusia, éste fue el país más atacado por el gusano, afectando a miles de empresas entre las que se encontraban entida-

Se incrementa la sofisticación de los ciberataques respaldados por naciones

A partir de las observaciones de los expertos de Kaspersky Lab sobre la actividad de los actores de riesgo durante el primer trimestre, la compañía ha elaborado un informe en el que llega a algunas conclusiones destacadas. La primera de ellas es que se ha producido un notable aumento en la sofisticación de los ciberataques respaldados por Estados. Es más, se confirma que los actores de amenazas aprovechan los wipers, tanto para el cibersabotaje como para la eliminación de pistas después de las operaciones de espionaje.

En segundo lugar, la compañía asegura que los criminales que están detrás de los ataques dirigidos están diversificando sus objetivos. El seguimiento del grupo Lazarus ha permitido identificar un subgrupo al que Kaspersky Lab ha llamado BlueNoroff, y que ha estado atacando entidades financieras de diferentes regiones, incluyendo un ataque de alta repercusión mediática en Polonia. Se cree que BlueNoroff está detrás del atraco del Bangladesh Bank.

Y, en tercer lugar, debido al uso del fileless malware, que se utiliza en ataques llevados a cabo tanto por actores de amenazas como por todo tipo de cibercriminales en general, la detección y las investigaciones forenses se vuelven más complicadas. Los expertos de Kaspersky Lab han encontrado ejemplos en herramientas de desplazamiento lateral utilizadas en los ataques de Shamoon, en ataques llevados a cabo contra bancos en el Este de Europa, así como en acciones de otros muchos actores de APT.

En menos de una semana, WannaCry había atacado a más de 300.000 ordenadores de 180 países

Mariano J. Benito, Director de Seguridad/CISO de GMV

WannaCry: Un análisis post-mortem

El 12 de mayo, un ataque de tipo ramsomware impactó en varias empresas relevantes de todo el mundo. El ataque motivó también que, ya por precaución, ya para contención, se activasen los protocolos de incidencias de estas empresas y/o el apagado de sus redes informáticas.

Realmente, ¿Alguien se sorprendió de que ocurriese este incidente? El ransomware lleva siendo uno de los vectores de ataque más frecuentes y rentables que utilizan los malos para lograr sus objetivos. Es rápido, sencillo, efectivo, se transforma en dinero con facilidad. Debemos reconocer que tiene un éxito notable. En los últimos (digamos) tres años y fundamentalmente en usuarios particulares y pequeñas empresas, ha habido múltiples incidentes y muchas pequeñas grandes tragedias.

Lo realmente sorprendente fue el uso combinado de ransomware y gusano. La clave se llama CVE-2017-0145(2), MS17-010 (3) o "Eternalblue". Se trata de una vulnerabilidad en el servicio SMB de Windows que permite ejecución remota del código que desee el atacante. En 2015 fue (presuntamente) detectada por la NSA y utilizada para el desarrollo de la herramienta "EternalBlue". Su código fuente fue revelado el 14 de abril de 2017, abriendo el camino a su utilización. ¿Cómo? Por ejemplo, para distribuirse en una red con visibilidad SMB (como por ejemplo la de muchas grandes empresas) saltando de equipo en equipo. Para ello, WannaCry ejecuta dos tareas: replicarse en los demás equipos de la red; y ejecutar el malware wannacrypt0r. Esta segunda parte es mucho más llamativa y fácilmente detectable, y facilitó a las empresas detectar el ataque y lanzar sus procedimientos de respuesta.

¿Qué opciones de defensa teníamos ante WannaCry? realmente muchas y de las ya conocidas.

En primer lugar, la mejor protección es tener un buen plan de copias de seguridad. ¿Qué cifran el disco duro? Ningún problema, basta con reinstalar el equipo, restaurar la información afectada desde copia de seguridad y problema resuelto. Claro que en redes de miles de equipos es más práctico desconectar la red cuando hay pocos infectados y restaurar esos equipos antes de que infecten a otros.

La segunda medida es específica de este ataque particular y ya la había ofrecido Microsoft en el mes de marzo de 2017. La aplicación del parche MS17-010 permite eliminar la vulnerabilidad que usa WannaCry para propagarse y lo convierte en ramsomware normal. En este punto, la duda recurrente es por qué no estaba ya aplicado un parche de categoría crítica publicado dos meses antes. Cada organización tendrá su respuesta: Lo que es evidente es que el parche no estaba instalado en todos los equipos, ni en todas las organizaciones. También es evidente que no es sencillo aplicar parches en organizaciones de miles de equipos y/o extendidas geográficamente y/o con equipos en servicios en tiempo real y/o cuando depende del usuario particular. En todo caso, este punto debe ser un área de mejora clara en las organizaciones afectadas por WannaCry. Y posiblemente, en bastantes de las no afectadas.

La tercera medida explota una debilidad del propio código de WannaCry. Antes de propagarse o cifrar los equipos, hace una comprobación DNS para el dominio www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com y alguno otro similar. Si el dominio existe, el ataque para inmediatamente. Así, el registro del dominio que un investigador de malware había completado a las 48 horas del inicio del ataque detuvo este ataque a nivel mundial. También hubiera sido válido el registro (ficticio) del dominio en los DNS internos, parando el ataque a nivel de cada organización.

Además, se han propuesto muchas otras soluciones, tales como el filtrado de los puertos 137 y 138 udp, y 139 y 445 tcp; firmas de antivirus, ajuste de los sistemas NAC y/o DLP. Sobre todo en los primeros minutos del ataque, bienvenidas fueron.

Es recomendable no pagar el rescate pedido ya que, se rescate o no la información, en realidad se están financiando los siguientes ataques.

En definitiva, WannaCry llegó, causó mucho revuelo y pocos daños por la excelente respuesta de los profesionales de la seguridad. Pero es una oportuna llamada de atención a los máximos responsables de las organizaciones (y también a los responsables de seguridad, de negocio y CIOs) para que se aumente de forma expeditiva la dedicación de recursos a la seguridad. Y para mejorar en las prácticas actuales de las organizaciones en la materia.

des bancarias como Sberbank, el mayor banco ruso.

Y tras Europa o Estados Unidos (otro de los grandes objetivos de WannaCry), llegó el turno de Asia. El ransomware logró atacar a la policía china y a autoescuelas, y, aunque el gigante asiático fue como "particularmente vulnerable" tanto fuentes oficiales como compañías de seguridad aseguraron que la intensidad del ciberataque comenzó a disminuir a medida que pasaba el fin de semana. No obstante, la compañía Qihoo señaló que WannaCry había atacado a cerca de 30.000 organizaciones hasta el sábado por la noche, con PetroChina como uno de los grandes nombres afectados. Más de 4.000 eran instituciones de educación.

En el caso de Japón, el ransomware atacó a cerca de 600 empresas, entre las que se encontraban Hitachi o Nissan, mientras que en Indonesia la víctima fue un hospital de lucha contra el cáncer.

CÓMO FUNCIONA EL RANSOMWARE QUE PUSO AL MUNDO EN JAQUE

CLICAR PARA VER EL VÍDEO

En menos de una semana, WannaCry había atacado a más de 300.000 ordenadores de 180 países.

En una primera estimación, West Coast cree que el coste de este ciberataque podría alcanzar los 4.000 millones de dólares a nivel global. Por su parte, la Unidad de Consecuencias Cibernéticas de Estados Unidos (un instituto sin ánimo de lucro que avisa a gobiernos y negocios sobre los costes de los ciberataques) ha hecho una previsión más modesta al cifrar, el coste del ciberataque, en unos 1.000 millones de dólares.

¿Quién es el culpable?

¿De dónde provino? Tanto la Inteligencia de Estados Unidos como Kaspersky Lab o Symantec señalaron a Corea del Norte como el responsable del ciberataque de WannaCry, basándose en una versión anterior del ranso-

Telefónica, el sistema de salud británico, Renault, Nissan o Sberbank, algunas de las víctimas del ciberataque

mware, que apareció en programas utilizados por Lazarus, un grupo de hackers que varias compañías aseguran que forma parte de las operaciones de ciberataques dirigidas por Corea del Norte.

No obstante, si se ha señalado a alguien ha sido a la Agencia de Seguridad Nacional de Estados Unidos (NSA). En este sentido, y durante el mismo fin de semana en el que el gusano estaba atacando con toda su virulencia, Brad Smith, asesor legal de Microsoft, destacó que "hemos visto aparecer en WikiLeaks vulnerabilidades almacenadas por la CIA, y ahora esta vulnerabilidad robada a la NSA ha afectado a clientes en todo el mundo". Como resultado "los hospitales, las empresas, los gobiernos y los ordenadores domésticos se han visto afectados" por el ciberataque.

"Este ataque es otro ejemplo de cómo almacenar vulnerabilidades por parte de los gobiernos es un gran problema" y comparó el mismo con "el robo de armas convencionales Tomahawk al ejército de Estados Unidos". Smith consideró que es imperativo que se cambien los métodos y que los ciberataques se adhieran a las mismas normas que rigen el mundo físico.

"Los gobiernos de todo el mundo deben tratar este ataque como una llamada de atención. Necesitan adoptar un enfoque diferente, necesitamos que consideren los daños que provocan a los civiles la acumulación de estas vulnerabilidades y el uso de estos exploits". Ésta es una de las razones por las que Microsoft solicitó "una nueva Convención Digital de Ginebra" en la que "informar de las vulnerabilidades a los proveedores, en lugar de almacenarlas, venderlas o aprovecharlas" sea un requerimiento gubernamental.

Por su parte, los medios de comunicación estatales de China criticaron la actuación de Estados Unidos en le ciberataque, asegurando que éste había obstaculizado la puesta en marcha de una serie de políticas para paliar las cibera-

Ray Pompon. Principal Threat Research Evangelist, F5 Networks

WannaCry anda suelto, aprenda a defenderse

Hace más de una década que el pionero del malware Dr. Peter Tippett acuñó la expresión "desastre viral" para describir la situación en la que con más de 25 máquinas infectadas en una única red, se producía un punto de inflexión que conducía irremediablemente a la caída total de la misma.

Con el nuevo WannaCry, que bloquea todos los archivos de un ordenador hasta que el propietario pague un rescate, nos encontramos ante un desastre viral que parece haber puesto en peligro a secciones enteras de infraestructuras críticas.

El daño se está extendiendo por todo el mundo y afectando a organismos como hospitales, por lo que, si algún paciente llega a morir por esto, quizá por vez primera, tengamos que enfrentarnos a un caso de homicidio por malware, lo que sin duda, supondrá un antes y un después para la seguridad y el compliance.

Este malware está usando MS17-010, a.k.a. "EternalBlue" (un exploit liberado por la NSA) para introducirse en la red de cualquier persona que no haya parcheado esta "vieja" vulnerabilidad. El exploit afecta al protocolo de compartición de archivos SMB (Server Message Block), que a menudo aparece abierto dentro las redes, facilitando, por tanto, la rápida propagación del ataque.

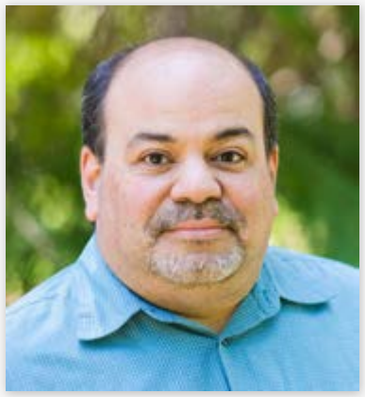
Tal como vivimos anteriormente con los ransomwares Cerberus y Apache Struts, los ciberdelincuentes no pierden tiempo actualizando las cabezas de los proyectiles de sus malwares. Cuando se abre un nuevo flanco, vuelven a aparecer las mismas amenazas de siempre, aunque con un envoltorio diferente, consiguiendo, una vez más, engañarnos e introducirse en nuestras redes.

WannaCry penetra en las redes de muchas formas diferentes. La más peligrosa es a través de Microsoft SMB (Server Message Block). Los expertos en seguridad informan que un dispositivo con SMBs en Internet sin protección puede ser atacado en menos de tres minutos. Sin embargo, WannaCry también utiliza métodos tradicionales de propagación de malware, a través de archivos adjuntos en correos y acciones de phishing.

La forma más frecuente del ransomware WannaCry llega, sin embargo, como un cargador con una DLL AES cifrada, que escribe un archivo llamado "t.wry". Este archivo es descifrado por una clave de malware de 128 bits embebida, que es lo que cifra los archivos del disco de la víctima. Mediante el uso de un método de carga cifrada, el malware nunca es escrito directamente en el disco en forma no cifrada y permanece invisible para los antivirus tradicionales.

Al cifrar los archivos de la víctima, también escanea todos los IPC$ y SMBs visibles. Utiliza la vulnerabilidad Microsoft MS17-010 SMB para obtener acceso y para infectar estos sistemas. Es este comportamiento el que ha permitido a WannaCry poner en jaque rápidamente redes enteras en cuestión de minutos.

La variante primaria de WannaCry usó un dominio no registrado para controlar la distribución, a.k.a. "the kill switch". Un experto en seguridad llamado MalwareTech, registró y hundió el dominio, logrando detener esta versión de WannaCry. Sin embargo, ya se han liberado otras variantes del malware, por lo que el peligro sigue siendo real.



Consejos para defenderse

- Bloquear el acceso de SMB a Internet, ejecutándolo a través de los puertos TCP 137, 139, 445 y puertos UDP 137, 138.
- Aplicar el parche de Microsoft para la vulnerabilidad MS17-010 SMB con fecha 14 de marzo de 2017.
- Filtrar y supervisar el correo electrónico para evitar ataques de phishing, observando los archivos adjuntos ejecutables y habilitados para macros.
- Dotar a los usuarios con los menores privilegios que sea posible, permitiéndoles solo el acceso a los recursos que necesitan para realizar sus trabajos, a fin de contener el daño que pueda causar una cuenta de usuario comprometida.
- Reducir y restringir los privilegios administrativos. Segregar las cuentas de los administradores del sistema de las cuentas de usuario que utilizan para leer correos y navegar por la web. Restringir el acceso a puertos TCP, como los 22, 23 y 3389.
- Configurar controles internos de acceso para contener el contagio dentro de las redes. Bloquear o restringir SMB (puertos TCP 137, 139, 445 y puertos UDP 137, 138).
- Enviar boletines internos a los usuarios con respecto a este brote, advirtiéndoles de las medidas de precaución con respecto a archivos adjuntos, además de evitar el uso de dispositivos externos en la red corporativa.
- Realizar copias de seguridad periódicamente.

menazas a raíz del ataque e hicieron un llamamiento a su país para que sustituya "de manera urgente" la tecnología extranjera por la desarrollada por compañías chinas.

Nuevas variantes

Días y semanas más tarde se empezaron a descubrir nuevas amenazas como Adylkuzz, un malware que en vez de bloquear los equipos y pedir un rescate, se queda latente en miles de ordenadores, crea una red de robots informáticos o bots infectados para usarse en remoto a las órdenes de los ciberdelincuentes. Una vez que se ha instalado en el sistema operativo de un ordenador, Adylkuzz descarga una serie de instrucciones para generar criptomonedas de forma legal sin que sus dueños lo sepan, y luego robarlas.

Además, el Departamento de Seguridad Nacional de Estados Unidos advirtió, un par de semanas más tarde de que WannaCry amenazase la seguridad mundial, que había detectado otra amenaza similar. Ésta afecta a Samba, sistema desarrollado para su uso en Linux y Unix y que amenaza a más de 100.000 ordenadores que utilizan versiones del software. El organismo hizo un llamamiento a usuarios y administradores para que actualicen sus sistemas y apliquen el parche antes de que la nueva vulnerabilidad vuelva a sembrar el caos global.

Qué hacer para protegerse

Y tras el ataque, llegaron las recomendaciones. En el caso de Gartner, la consultora aconseja a las empresas poner en marcha tres tipos de acciones. La primera es dejar de culpar a los responsables y centrarse en las causas fundamentales. En este sentido, Microsoft Windows XP, un sistema operativo que ha sido golpeado duramente por WannaCry, puede ser integrado en sistemas clave como parte de los paquetes de control. En los sistemas embebidos, como terminales de punto de venta, equipos de imágenes médicas, sistemas de telecomunicaciones e incluso de producción industrial, hay que asegurarse de que el proveedor pue-

de proporcionar una ruta de actualización. Y es imprescindible hacer esto, incluso si se usan otros sistemas operativos embebidos, como Linux u otras variantes de Unix, ya que es seguro asumir que todo el software complejo es vulnerable al malware.

En segundo lugar, hay que aislar los sistemas vulnerables. Habrá algunos que, aunque todavía no están afectados por el malware, siguen siéndolo. Es importante darse cuenta de que éstos son a menudo de los que más se depende. Una solución temporal útil es limitar la conectividad de red; es decir, identificar los servicios que puede desactivar, especialmente los vulnerables, como el intercambio de archivos de red.

Finamente, hay que mantenerse a la expectativa, asegurándose de que las herramientas de detección de malware están actualizadas, totalmente operativas y examinando el tráfico. Por otro lado, es aconsejable confirmar que los sistemas de análisis de comportamiento de los usuarios y de la entidad, análisis de tráfico de red e información de seguridad y administración de eventos no están teniendo un comportamiento inusual, y que los manejadores de incidentes responden. Asimismo, aconseja mantener al personal técnico enfocado en resolver asuntos claves y permitir que alguien responda preguntas externas.

Enlaces relacionados

- Big Data, gran aliado contra el fraude financiero
- Tecnología para hacer frente al fraude financiero
- Una nueva ciberseguridad frente a amenazas desconocidas
- Ataques con exploits: de las amenazas diarias a las campañas dirigidas
- Informe Symantec sobre la seguridad de Internet (ISTR 2017)
- Informe sobre la responsabilidad de las entidades financieras ante el fraude electrónico
- Informe global sobre Seguridad de la Información 2016-2017 de EY
- La paradoja tras la experiencia del usuario de cripto-ransomware

#ContentMarketingIT

¿Quieres conocer todas las posibilidades que ofrece la **Videovigilancia IP Unificada**?

Gracias a D-Link, puedes descubrir las ventajas de apostar por una solución de Videovigilancia IP Unificada

Accede a este documento digital y descubre las claves de la Videovigilancia IP Unificada.

it User TECH & BUSINESS

Las unidades SSD conquistan el mercado del almacenamiento y el canal

El deseo de cambiar a unidades de estado sólido (SSD) continúa creciendo, a medida que tanto los consumidores como los clientes corporativos ven los beneficios de rendimiento que supone actualizarse desde unidades de disco duro. De hecho, Context prevé que para 2020 el 90% de los componentes de almacenamiento serán SSD. Si no aparece una tecnología que le pueda hacer sombra, las unidades SSD se irán posicionando cada vez más como un estándar, y el canal de distribución deberá estar ahí para promover su implantación, tanto en el mercado de consumo como en el ámbito empresarial. De la evolución de este mercado y su atractivo para el canal hemos hablado con MCR y Tech Data.

Las unidades de estado sólido se han convertido en un estándar, y su conquista del mercado del almacenamiento parece imparable. No en vano, según la firma de investigación Forward Insights, el pasado año se comercializaron un

total de 63 millones de SSD en todo el mundo a través del canal, con Samsung representando el 21% del mercado, seguido de Kingston, con el 16%.

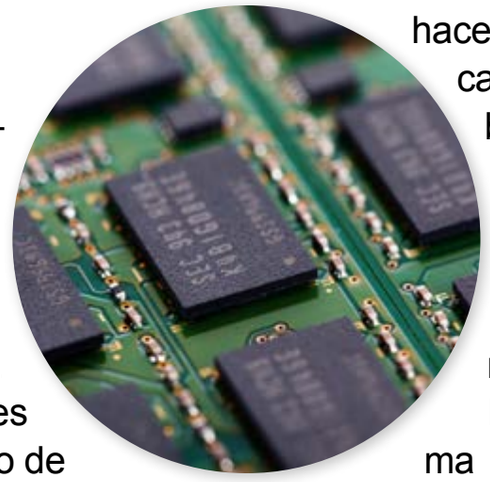
Por su parte, Context señala que, en 2016, por primera vez las ventas de SSD superaron a las de las unidades de disco duro. “A medida que el precio de los SSD cae y su capacidad aumenta, en 2017 esta tendencia continuará”, señala Gurvan Meyer, analista senior de investigación del Equipo Empresarial de Context. “En 2014, predijimos que el 90% de los componentes de almacenamiento serían SSD para 2020, y la industria está bien encaminada para lograrlo”.

Respecto a la evolución de las ventas de SSD este año, según datos de algunas consultoras, durante el primer trimestre se vendieron más de 30 millones de unidades. “A medida que los precios vayan ajustándose, veremos crecimientos que podrían llegar a los dos dígitos”, augura Eduardo Moreno, director general de MCR.

“El 90% de nuestros partners venden soluciones de este tipo”

Eduardo Moreno,
director general de MCR

Múltiples ventajas



Mientras que las ventas de discos duros físicos se han visto ralentizadas por la progresiva adopción de la nube, en paralelo, las memorias SSD se han ido imponiendo por sus ventajas. Más velocidad (hasta 4 o 5 veces en algunos casos), menor tiempo de arranque, un consumo inferior, menor peso, resistencia prácticamente total a los golpes, son las principales ventajas para Joan Teixidor, division manager de Periféricos y Componentes de Tech Data España. “Además, hasta hace poco, los SSD eran dispositivos caros, pero ahora mismo, sin embargo, son mucho más asequibles, y, si bien continúan siendo más caros que los HDD, ya empiezan a tener precios muy interesantes para el usuario medio”, añade Teixidor.

Los SSD ya se utilizan ya de forma masiva, especialmente en dispositivos de movilidad. Sus ventajas incluyen unas velocidades de transferencia que pueden incluso triplicar la que ofrecen los discos duros “tradicionales” y reducen el tiempo de arranque del sistema operativo y el acceso a las aplicaciones. Además, la ausencia de partes móviles les permite mejorar el ruido emitido, la emisión calorífica y el consumo.

Respecto al tipo de clientes están impulsando la demanda, para Eduardo Moreno, de MCR, “el mercado de consumo sigue siendo, sin duda, el protagonista en ventas de soluciones SSD, pero el segmento Enterprise también continúa creciendo, como es lógico, ya que los centros de datos exigen cada vez tecnologías más optimizadas, aumentando la capacidad y reduciendo el espacio de almacenamiento. Es cuestión de tiempo que acabe imponiéndose”.

Por su parte, Joan Teixidor, de Tech Data, ve una evolución positiva tanto en uno como en otro ámbito. “En el segmento de consumo, los usuarios consideran los SSD como aliado imprescindible para conseguir la mejor configuración de su ordenador. Por su parte, las empre-

¿Qué tecnología impera en el mercado SSD?

Hasta hace unos años, la mayoría de las unidades SSD a la venta estaban preparadas para conectarse por SATA, pero este tipo de conexión, pensada para discos duros, suponía un cuello de botella importante que reduce su rendimiento, de ahí que los discos SSD basados en el estándar PCI Express (PCIe) sean cada vez son más populares. Además, en los últimos años ha surgido un nuevo formato, M.2, con una apariencia más o menos similar a los módulos de memoria RAM, que es bastante habitual en ultrabooks y equipos ligeros, y que se está convirtiendo en el más habitual.

"El estándar actual es el M.1, pero ya hay formatos más avanzados como el M.2, mucho más compacto, que permiten crear equipos más delgados y ligeros. Los SSD en formato de disco de 2,5 pulgadas proporcionan la mejor relación calidad-precio. Y crece sobre todo con fuerza el formato PCIe, que es el que ofrece mayor rendimiento", explica Eduardo Moreno, de MCR. En cuanto a capacidad, el directivo comenta que "en unidades internas, el estándar actual está entre 250 y 500GB, en tanto que, en unidades externas, los más demandados son los de 4TB, pero ya hay modelos de hasta 60TB".

Joan Teixidor, de Tech Data, afirma por su parte que, "hace algún tiempo, el formato habitual es el de 2,5 pulgadas, el habitual para portátiles, aunque se pueden usar también en ordenadores a través de adaptadores. En cuanto a las capacidades, las más vendidas son las de capacidad baja/media, entre 120 y 250GB, cuyo coste está en torno a los 100 euros, si bien depende mucho de las necesidades del comprador".

sas comienzan a considerarlo como una seria alternativa", señala el directivo.

Aumento de precios

Está claro que los SSD se están imponiendo, pero desde el cuarto trimestre de 2016 tienen serios problemas de disponibilidad, lo que coarta su crecimiento. Y es que, precisamente su elevada demanda, sumada la escasez de memorias flash NAND, ha hecho que haya menos stock y, como consecuencia, en los úl-

timos meses los fabricantes han incrementado su precio. Concretamente, un informe de la compañía analista Trendfocus determina que el precio de los SSD se ha visto incrementado en un 36% en el último año, y que la tendencia es que siga subiendo hasta un 28% hasta final de año, si bien comenzaremos ver ligeras reducciones de precio a principios de 2018.

Este hecho podría poner algunas trabas a la actual tendencia de incorporar SSD en los sistemas OEM pre-montados, así como en los últimos portátiles que han salido al mercado, perjudicando con ello las ventas globales de PC. Y, probablemente, la tendencia de los usuarios de sustituir sus viejos discos duros por SSD también se verá afectada. este respecto, Joan Teixidor, de Tech Data, señala que “tras varios trimestres en los que hemos visto subir los precios, parece que en los próximos meses la situación se va a estabilizar, y es muy probable que el mercado se consolide. Según estimaciones de Gartner, en 2019 el mercado estará inundado de memorias DRAM y NAND, lo que provocará que vuelvan a caer los precios”.

Eduardo Moreno, de MCR, también ve con optimismo la evolución del mercado, comentando que “es cierto que había cierto temor a que el mercado se viera afectado por la falta de suministro de memorias NAND Flash, debida a su vez al enorme crecimiento en la demanda de memorias de este tipo por parte del sector del smartphone. Pero el mercado está respondiendo: los suministros de unidades SSD se han incrementado y su popularidad es cada vez más elevada”.

“Es un negocio con márgenes interesantes”

Joan Teixidor, division manager de Periféricos y Componentes de Tech Data España

Atractivo para el canal

Aunque habrá que ver cómo evoluciona, está claro que estamos ante un mercado en auge que atrae a cada vez más figuras, y también en el canal, un canal constituido tanto por mayo-

El mercado de consumo sigue siendo el protagonista en ventas de soluciones SSD

ristas y resellers, como por etailers, integradores de sistemas y proveedores de soluciones.

"Está claro que es un producto número uno en ventas en la actualidad, y por eso atrae a todos los jugadores del mercado, ya que es un negocio que no para de crecer, y que además abarca a todo tipo de clientes. Los márgenes, en cualquier caso, son muy similares a otros productos, incluso a los que en teoría sustituyen, y son bajos, esa es la verdad. Pero se vende mucho, y eso compensa", asegura Eduardo Moreno, de MCR.

Para este mayorista, el peso de las soluciones SSD es muy importante, cada vez más en los últimos años, y sigue creciendo, a lo cual se suma que ya distribuye algunas de las marcas más reconocidas. "Actualmente, se puede decir que el 90% de nuestros partners venden soluciones de este tipo, ya que es un producto muy demandado por el usuario final", señala Moreno.

Por lo que respecta a Tech Data, es un área de negocio en continuo crecimiento que representa alrededor de un 15% de sus ventas de almacenamiento. "Es que estamos hablando, más que de productos, de una nueva solución para almacenar datos. En ese sentido, por supuesto es un negocio rentable, y para algunos perfiles lo será más en unas categorías de producto, como, por ejemplo, las unidades externas para el mercado de consumo, y para otros la vía de entrada estará en otras categorías, como la de unidades internas en grandes proyectos corporate. Los márgenes variarán constantemente, pero se podría decir que es un negocio con márgenes interesantes", concluye Joan Teixidor.

Enlaces relacionados

- En 2016 se vendieron 63 millones de unidades SSD en el canal
- Las ventas de SSD a usuarios empresariales en Europa Occidental crecen un 43,2%
- El papel del canal es clave en la transición al almacenamiento flash
- El mercado de SSD crecerá un 40% anual hasta el año 2022

#ContentMarketingIT

¿Quieres descubrir **las claves** que definen el nuevo **puesto de trabajo**?

Gracias a Intel,
descubrimos
las tecnologías
que potencian el nuevo
puesto de trabajo.

Accede a este documento digital
y descubre cómo puedes
transformar tu negocio.

Hogares casi "a estrenar"

La solidaridad puede tener muchas formas. Una puede ser la aportación económica; otra, la aportación de bienes materiales que otros necesitan; pero, en el caso que nos ocupa en estas páginas, hablamos de la colaboración y la implicación en labores de reparación y adecuación de una de las casas de acogida de la Fundación Adelias. Samira Brigüech, su presidenta, nos relata uno de estos ejemplos, en esta ocasión, de la mano de Veritas.

Teresa Angelino se metió en el despacho de Marco Blanco, country manager de Veritas. Sabía que se estaba tomando un café en un momento de relax dentro de su alocada agenda, y quería que la escuchara con atención.

Le propuso que los empleados de la compañía donaran un día o una media jornada para hacer algo de lo que pudieran sentirse orgullosos: hacer un servicio a la comunidad, como lo llaman en Estados Unidos, país en el que casi es una obligación que los empleados de las empresas donen un par de días al año a alguna ONG. Además, esas horas, la compañía los convierte en euros para la ONG en función de las horas donadas.

Un granito de arena de cada uno

Sabía que la Fundación Adelias ofrece alojamiento en sus pisos de acogida de Madrid a niños que viven en situaciones de pobreza

La Fundación Adelias nace de la mano de empresarios, ejecutivos y jueces que piensan, profundamente, que un mundo mejor es posible. Dedicamos tiempo, fondos, talento e ilusión para trabajar por niños y adolescentes en dos ámbitos fundamentales: educación y salud.
Movidos por un compromiso con la sociedad, con la población más vulnerable, los niños, trabajamos construyendo hospitales, Casas Cuna, Escuelas, impulsando el progreso y el desarrollo. Movemos especialistas de un lado a otro del continente y formamos a los hombres del futuro para cambiar la realidad de las comunidades para las que trabajamos. El foco es España en materia educativa y Marruecos en el ámbito de la salud.

¿Quieres colaborar?

Puedes hacer tus aportaciones en la cuenta ES27 2100 6274 3202 0003 5801 o, si lo prefieres, tienes otras opciones en este enlace

y que necesitan tratamiento quirúrgico para salvarles la vida o hacérsela más llevadera. Quería proponerle a Marco pintar y decorar uno de esos pisos, que sabía por la Fundación que estaban en mal estado.

Marco Blanco ni siquiera la dejó terminar. Le entusiasmó tanto la idea que le pusieron fecha en ese mismo instante, él también quería participar activamente.

Un grupo de empleados de diferentes departamentos contestó a la convocatoria, sería un día especial. Un día en el que uno no piensa en sus problemas, pero sí en los demás, en el dolor ajeno. Un día para desconectarse de Whatsapp, de Facebook y de los mensajes de correo electrónico que nos saturan con fuegos continuos el día a día.

Manos a la obra

El 11 de mayo simbolizó trabajar para otros y dejar una huella en un lugar en el que muchos niños vivirían durante los próximos meses. Un hogar que oliera a nuevo.

Compraron los monos de trabajo, las brochas y los botes de pintura, pequeño material para reparar "heridas" en los armarios, baños, cocina, cogieron una super caja de herramientas y se dirigieron a Rivas-Vaciamadrid.

Pasaron el día en 45 metros cuadros. Pulieron, pintaron, lijaron, limpiaron… ingenieros, administrativos, comerciales… haciendo el trabajo de una cuadrilla de pintores. Eran los transformadores de pisos, pero sin estar en un reality show televisivo.

Hubo muchas risas, alegría y un brindis final, porque el resultado fue de 10.

Las familias llegaron al piso y se encontraron un espacio casi para estrenar, se podía sentir la magia, la que se deja en los lugares donde se hacen las cosas de forma altruista.

Una experiencia que no olvidarán nunca y que volverán a repetir pronto en otro de los pisos de acogida, porque la solidaridad, bien entendida, engancha

Una experiencia que no olvidarán nunca y que volverán a repetir pronto en otro de los pisos de acogida, porque la solidaridad, bien entendida, engancha.

Gracias amigos de Veritas, espero que seáis una inspiración y que cunda el ejemplo en otras muchas empresas del sector. Hay un largo camino que recorrer en el mundo del voluntariado corporativo.

Enlaces relacionados

Fundación Adelias

¿Cómo sobrevivir al ransomware de cifrado?

KASPERSKY lab

¿Cómo sobrevivir al ransomware de cifrado?

Recientemente, todos los medios de comunicación hemos llevado a nuestras portadas o a nuestros sumarios el ataque sufrido por una larguísima lista de empresas y entidades que han convertido en protagonista al ransomware WannaCry. A partir de ahí, surgen una serie de preguntas, ¿estamos seguros? ¿Qué ha provocado esta incidencia? ¿Cómo protegerse? ¿Qué hacer ahora? Y, sobre todo, ¿podría haberme afectado a mí? En las páginas siguientes trataremos de responder a todas ellas.

En primer lugar, vayamos a lo más genérico: ¿qué es el ransomware? El crimen organizado está detrás de gran parte del malware actual y su intención es ganar dinero. Como su propio nombre indica, el ransomware es un tipo específico de malware cuyo objetivo es lograr el pago de un rescate a cambio de desbloquear el acceso a un recurso que pertenece a la víctima.

En el caso del ransomware de cifrado, o cryptors, los activos "secuestrados" son los archivos y los datos que se almacenan en el dispositivo infectado. El cryptor cifra los datos de la víctima en un formato ilegible y los datos solo se pueden descifrar mediante la clave de descifrado necesaria, pero dicha clave solo la proporcionará el criminal cuando la víctima pague el rescate.

Mientras que los usuarios se enfrentan a exigencias de rescate de 300 a 500 dólares, los cibercriminales saben que los datos pueden ser muy valiosos para una empresa, por lo que la suma del rescate es mucho mayor. Si uno de los dispositivos está infectado, el atacante suele ofrecer un margen de 48 a 72 horas para pagar el rescate.

Si no paga dentro del plazo, es probable que el precio del descifrado aumente. Si vence el segundo plazo y el pago no se ha realizado todavía, es probable que la clave de descifrado se elimine. En ese punto cabe la posibilidad de que sea imposible recuperar sus archivos en un formato legible. Incluso, si paga el rescate, no hay garantía de que sus datos se descifren. Algunos cryptors incluyen errores de software que pueden hacer que no funcione, por lo que el proceso de descifrado fallará. En otros casos, es posible que el criminal

RANSOMWARE EN ATAQUES DIRIGIDOS

CLICAR PARA VER EL VÍDEO

no tenga la intención de descifrar nada y solo quiera obtener el dinero de la víctima.

Pero, como siempre, la realidad no es la misma para un usuario en su domicilio que para una empresa y, en este caso, los efectos perniciosos son todavía mayores. A pesar de que los criminales suelen exigir cantidades más elevadas a víctimas de empresas, el rescate solo representa una pequeña parte de los costes totales para la empresa. Este ataque puede dar lugar a pérdidas económicas mucho mayores.

En la "era de la información" actual, cualquier pérdida temporal de datos puede interrumpir totalmente los procesos fundamentales para la empresa, lo que se traduce en pérdida de ventas, reducción de la productividad, costes más que significativos para recuperar el sistema y revertir la situación al momento anterior al problema.

Según un informe de Interdisciplinary Research Center in Cyber Security de la Universidad de Kent en febrero de 2014, más del 40% de las víctimas de CryptoLocker cedió a pagar el rescate

Sin embargo, la permanente pérdida de datos puede tener consecuencias mucho más graves, como un efecto negativo en la posibilidad de la empresa de competir en el mercado, una reducción de las ventas a largo plazo, o imposibilidad de acceder a datos y recursos necesarios para el día a día de la empresa.

Incluso, se puede poner en peligro a toda la empresa, si, por ejemplo, se pierde la posibilidad de acceder a todos sus registros de ventas, archivos de clientes, datos contables, información de productos y datos de diseño.

El tristemente famoso WannaCry

El más famoso incidente de seguridad informática en las últimas semanas ha sido WannaCry, que ha infectado a más de 200.000 ordenadores. Durante el primer día del ataque, descubrimos que WannaCry estaba en 74 países, incluido el nuestro, si bien, aunque en Espa-

NO MORE RANSOM!

Las fuerzas y cuerpos de seguridad y las compañías tecnológicas han unido fuerzas para interrumpir las operaciones de los cibercriminales que hacen uso del ransomware. El portal No More Ransom, puesto en marcha en julio de 2016, es una iniciativa del National High Tech Crime Unit de la policía de Países Bajos, el European Cybercrime Centre de Europol y dos compañías de ciberseguridad, Kaspersky Lab e Intel Security, con el objetivo de ayudar a las víctimas de ransomware a recuperar sus datos cifrados sin tener que pagar a los criminales.

Desde su puesta en marcha, se han adherido a esta iniciativa más de 80 nuevos miembros, entre fuerzas de seguridad, como Guardia Civil, y empresas privadas del mundo de la ciberseguridad.

El proyecto también se dirige a educar a los usuarios sobre cómo funciona el ransomware e informar sobre qué contramedidas se pueden tomar para prevenir eficazmente una infección. Esta iniciativa está accesible en este enlace.

Pero, además de consejos preventivos, los usuarios pueden encontrar en esta página herramientas para el descifrado de archivos, así como los enlaces correspondientes en diferentes jurisdicciones para poder denunciar, en caso de haber sido atacado.

ña la repercusión ha sido muy grande en los medios, no ha sido uno de los países más afectados.

WannaCry tiene dos partes. La primera es un exploit que se encarga de la infección y de la propagación. La segunda es un cifrador que se descarga en un ordenador después de ser infectado.

La primera supone la gran diferencia entre WannaCry y la mayoría de cifradores. Para infectar un ordenador con un cifrador normal, el usuario debe cometer un error, como, por ejemplo, hacer clic en un enlace sospechoso, permitir que Word ejecute macros maliciosas o descargar un adjunto malicioso de un mensaje de correo electrónico. Un sistema puede ser infectado con WannaCry sin que el usuario haga nada.

Los creadores de WannaCry se han aprovechado de un exploit de Windows conocido como EternalBlue y que Windows parcheó con la actualización de software MS17-010 el 14 de marzo del presente año. Mediante el exploit, pudieron obtener acceso remoto a los ordenadores e instalar el cifrador.

Después de hackear con éxito un ordenador, WannaCry intenta distribuirse por toda la red local hacia otros ordenadores del mismo modo en que lo haría un gusano. El cifrador busca la vulnerabilidad EternalBlue

Solo el 40% de las empresas consideran el ransomware un peligro serio

en otros ordenadores y, cuando WannaCry encuentra un dispositivo vulnerable, lo ataca y cifra sus archivos.

Por tanto, al infectar un ordenador, WannaCry puede infectar a toda una red local y cifrar todos los ordenadores de la misma. Por ello, las grandes empresas son las que más han sufrido por el ataque de WannaCry (a más ordenadores en la red, mayor puede ser el daño).

Como cifrador, WannaCry se comporta como cualquier cifrador: cifra los archivos de un ordenador y pide un rescate para descifrarlos. Se parece mucho a una variación de CryptXXX.

WannaCry cifra diferentes tipos de archivos, incluyendo los documentos de Office, imágenes, vídeos y otros tipos de archivos que puedan contener información importante para el usuario. Las extensiones de los archivos cifrados se renombran a .WCRY y el archivo se vuelve del todo inaccesible.

Tras esto, el troyano cambia el fondo de pantalla con una imagen que contiene la información sobre la infección y las acciones que se supone que el usuario debe llevar a cabo para recuperar los archivos. WannaCry deja notificaciones en formato de archivos de texto con la misma información en todas las carpetas del ordenador para asegurarse de que el usuario recibe el mensaje.

Como de costumbre, una de las acciones era transferir cierta cantidad de dinero, en bitcoins, a los malhechores. Tras ello, dicen que descifrarán todos los archivos. En un principio, los ciberdelincuentes pedían 300 dólares, pero luego subieron el rescate a 600 dólares.

En este caso, también intentan intimidar a las víctimas afirmando que la cantidad del rescate se incrementa pasados tres días y, es más, diciendo que pasados siete días es imposible descifrar los archivos.

Y la salida al problema no es el pago, dado que no hay garantías de que los delincuentes vayan a descifrar los archivos tras recibir el mismo. De hecho, en otras ocasiones simplemente borraron los archivos, evitando cualquier opción de los usuarios de recuperarlos.

Formas y efectos del ataque

Más allá del caso de WannaCry, y al igual que la mayoría del resto de tipos de malware, existen muchas maneras en las que un cryptor puede encontrar una vía de entrada a ordenadores y otros dispositivos. Sin embargo, dos de las formas más comunes son las denominadas Phishing spam y Water holing. En el primero de los casos, la víctima recibe un mensaje de correo electrónico con un archivo adjunto infectado o el texto incluye un enlace a un sitio web de phishing, mientras que, en el segundo caso, al visitar un sitio web legítimo que es popular entre un tipo específico de usuarios o función laboral, como un foro de contabilidad o un sitio de asesoramiento empresarial, por ejemplo, el dispositivo del empleado se puede infectar. En estos casos de infección oculta, el sitio web ya se habrá infectado con el malware, que está listo para aprovechar vulnerabilidades en los dispositivos de los visitantes.

Un cryptor puede atacar una amplia gama de dispositivos, desde equipos de sobremesa a infraestructuras de escritorios virtuales, pasando por tabletas y smartphones.

Además, si el dispositivo que está sufriendo un ataque también está conectado a una unidad de red (que permite compartir archivos corporativos), es probable que el cryptor cifre dichos archivos compartidos, con independencia del sistema operativo en el que se está ejecutando el servidor de archivos.

Lamentablemente, sea cual sea el dispositivo que sufra el ataque, no se requieren derechos de administrador para la mayoría de las acciones maliciosas que realizan los cryptors.

Algunos consejos para estar protegidos

Dado que cruzar los dedos y esperar que no nos afecte no parece una solución adecuada para hacer frente a las amenazas, es necesario, además de contar con las herramientas adecuadas, de las que hablaremos a continuación, seguir unos sencillos pasos que nos ayudarán a mantenernos más seguros.

El primero de ellos es la formación a los usuarios que, normalmente, son el eslabón más débil de la cadena. Deben ser conscientes de los riesgos y, sobre todo, de las consecuencias e implicaciones que tiene abrir un mensaje sospechoso o acceder a determinadas páginas o foros.

El segundo, es contar con una copia de seguridad actualizada de forma constante y que estemos seguros de que se puede recuperar.

Y, tercero, mantener actualizado tanto los sistemas operativos y las aplicaciones de la red y de los dispositivos, así como las herramientas de seguridad que protegen toda la infraestructura de la empresa. Además, convendría contar con una herramienta de seguridad que permita administrar el uso de internet en cada puesto de trabajo, controlar quién y desde dónde se accede a los datos corporativos y que administre el lanzamiento de programa, pudiendo bloquear aquellos que sean perjudiciales o, simplemente, sospechosos.

Kaspersky EndPoint Security for Business

Kaspersky Endpoint Security for Business ofrece una seguridad a varios niveles para ayudar a proteger las empresas contra amenazas conocidas, desconocidas y sofisticadas, incluidos los cryptors. Junto con las actualizaciones constantes, incluye técnicas de comportamiento, heurísticas y proactivas, así como tecnologías con asistencia en la nube para una rápida respuesta a las nuevas amenazas.

Un elemento importante de esta solución es System Watcher, que supervisa el comportamiento de todos los programas que se ejecutan en los sistemas y compara cada comportamiento del programa con los modelos de comportamiento de malware típico. Si se detecta cualquier comportamiento sospechoso, System Watcher pone automáticamente la aplicación en cuarentena.

Como mantiene un registro dinámico del sistema operativo o el registro, permite deshacer las acciones maliciosas que se implementaron antes de que el malware se identificara. Además, System Watcher controla constantemente el acceso a determinados tipos de archivos, incluidos documentos de Microsoft Office, y almacena temporalmente copias si se accede a alguno de estos archivos. Si System Watcher detecta que se trata de un proceso sospechoso, como un cryptor, que accedió a los archivos, las copias de seguridad temporales se pueden utilizar para restablecer los archivos al formato sin cifrar. Aunque las copias de seguridad temporales generadas por System Watcher no están diseñadas como reemplazo a una estrategia de

copia de seguridad completa de los datos, pueden ser valiosas para ayudar a la empresa a protegerse contra los efectos de un ataque de cifrado.

Junto con System Watcher, el control de privilegios en las aplicaciones también permite a los administradores limitar los recursos esenciales del sistema a los que se permite acceder a las aplicaciones, incluido el acceso al disco de nivel bajo. Las vulnerabilidades, o errores de software, dentro de cualquiera de las aplicaciones y sistemas operativos que se ejecutan en sus dispositivos pueden proporcionar puntos de entrada para ataques de malware, incluidos los cryptors.

Estas herramientas de evaluación de vulnerabilidades y gestión de parches automatizadas pueden analizar los sistemas, identificar las vulnerabilidades conocidas y ayudarle a la empresa a distribuir los parches necesarios y las actualizaciones, de manera que las vulnerabilidades de seguridad conocidas se puedan eliminar. Esto también ayuda a evitar que el malware se aproveche de las vulnerabilidades en aplicaciones y sistemas operativos, y controla específicamente las aplicaciones atacadas con más frecuencia, entre las que se incluyen Adobe Reader, Internet Explorer, Microsoft Office y Java, a fin de proporcionar un potente nivel adicional de seguridad.

Las herramientas flexibles de control de aplicaciones, además del marcado en lista blanca dinámico, hacen que sea fácil permitir o impedir el inicio de programas. Además de bloquear los programas incluidos en la lista negra, puede optar por aplicar una política de denegación predeterminada para algunas de sus estaciones de trabajo y servidores, de modo que solo se ejecutarán las aplicaciones que se encuentran en su lista blanca; como resultado los cryptors se bloquearán automáticamente.

Las herramientas fáciles de usar le permiten configurar las políticas de acceso a Internet y supervisar el uso de Internet. Puede prohibir, permitir o inspeccionar las actividades de los usuarios en sitios web individuales o categorías de sitios, como redes sociales, juegos o sitios de apuestas, para reducir las probabilidades de que los usuarios visiten un sitio web infectado por un cryptor.

Por su parte, el motor antiphishing con asistencia en la nube ayuda a evitar que los empleados se conviertan en víctimas de campañas de phishing y spear phishing que pueden llevar a infecciones por cryptors.

Enlaces relacionados

- Herramienta gratuita anti-ransomware
- #nomoreransomware
- Kaspersky Lab Daily
- Kaspersky Endpoint Security for Business
- Soluciones de Kaspersky Lab para la empresa
- Por qué elegir Kaspersky Lab frente al ransomware
- Impacto financiero de la seguridad en el negocio

Un entorno seguro:
la base para la Transformación Digital

V-Valley
the Value of esprinet

La ciberseguridad afronta el reto de proteger y respaldar el negocio

Un entorno seguro: la base para la Transformación Digital

El mundo de la seguridad es tan complejo como apasionante. Además, lamentablemente, ha estado de total actualidad en las últimas semanas por el incidente WannaCry, si bien es una de esas áreas del negocio que nunca pasan de moda, porque es una prioridad indiscutible para cualquier empresa. Eso sí, en los últimos tiempos hemos ido viendo cómo cambia la aproximación a este terreno, porque nos enfrentamos a una realidad totalmente diferente que no puede ser defendida con la visión tradicional. Conozcamos los detalles.

Y para poder conocer en profundidad todo lo relacionado con las tendencias en seguridad, hemos querido recurrir a algunos expertos que nos han ofrecido su visión sobre este particular. En este sentido, una de las compañías a las que hemos recurrido ha sido Check Point Software, desde donde Fernando Herrero, director de Canal, nos pone sobre la pista de las tendencias que desde su compañía detectan en el mercado. En palabras de Herrero, "el mundo de la seguridad está en constante cambio. Los cibercriminales no descansan en su empeño por encontrar nuevas formas de ataques que penetren en los endpoints y los servidores de las empresas. Por esta razón, tenemos que actualizar constantemente nuestras tendencias, para poder adelantarnos a los malhechores. En la actualidad, la batalla contra el cibercrimen se celebra sobre todo en cinco frentes: dispositivos móviles, Internet de las Cosas, infraestructuras críticas, prevención de amenazas y cloud".

Por su parte, desde Kaspersky Lab nos advierten de que, "como hemos observado con WannaCry, el último ciberataque a empresas de todo el mundo, el cibercrimen no desaparece, sino que cada vez es más preocupante y aparecen nuevas amenazas que ponen en riesgo la seguridad corporativa de las empresas. Como pronosticamos a principios de año, el ransomware iba a ser el protagonista en cuanto a ciberamenzas, además de los implantes pasivos, que casi no muestran señales de infección en el sistema, y se pondrán de moda y crecerá la "mercantilización" de los ciberataques financieros con recursos especializados. El ciberespionaje se dirigirá a dispositivos móviles e Internet of Things; las infecciones cortas serán más populares y el

WANNACRY:EL RANSOMWARE QUE PUSO AL MUNDO EN JAQUE

ransomware, como el ataque de hace unas semanas, seguirá aumentando".

Desde Microsoft nos explican que la seguridad es una parte más de una tecnología que puede transformar el panorama empresarial. "La tecnología", nos apuntan, "tiene un carácter disruptivo que hace posible nuevos modelos de negocio, habilita nuevas fuentes de ingresos para las empresas y está dando forma a un nuevo panorama industrial. Garantizar la seguridad y la privacidad cumpliendo con la normativa vigente es fundamental en el proceso de transformación digital de las empresas. En un contexto en el que cada vez más empleados traen sus propios dispositivos a sus empresas, usan apps y acceden a información confidencial, la protección de las empresas requiere un nuevo enfoque. El crecimiento de los ciberataques en número e impacto directo en el negocio de las empresas ha hecho que la seguridad pase a ocupar la atención de la más alta dirección".

En una línea similar se expresa Alberto Tejero, director comercial de Panda Security, al señala que las empresas "sufren y sufrirán más ataques y cada vez más avanzados. Los ciberdelincuentes están continuamente buscando puntos débiles para entrar en las redes corporativas, y, una vez dentro, utilizan movimientos laterales para acceder a la información que buscan para robarla. Además, el ransomware, gran protagonista de 2016, seguirá siéndolo también a lo largo de este 2017, junto con los ataques DDoS. También hay que resaltar que vivimos un momento muy delicado en las relaciones internacionales. Diferentes amenazas de guerras comerciales, espionaje, arancelarias, que pueden tener grandes -y graves- efectos en el campo de la seguridad informática, pudiendo entorpecer las iniciativas existentes de compartición de información con estándares y protocolos de actuación internacionales".

"Por otro lado", añade, "a nivel de usuarios particulares, IoT es la próxima pesadilla de seguridad, ya que estos dispositivos no han sido diseñados con la seguridad como punto fuerte; y, cómo no, los móviles, donde los dispositivos Android se llevan la peor parte".

Desde el punto de vista de SonicWall, "y con referencia a nuestro informe anual de seguridad 2106", señalan, "hemos observado como tendencias que el volumen de muestras únicas de malware descendió hasta los 60 millones, un descenso del 6,25%; que la creación de malware para el Punto de Venta descendió un 93% desde 2014;

LA SEGURIDAD, SEGÚN... CHECK POINT

En palabras de Fernando Herrero, "nuestra propuesta pasa por proteger absolutamente todos los puntos débiles de la compañía. Para esto, lo primero que hacemos es una consultoría a cada empresa. Después, les decimos los agujeros que existen en su estrategia de seguridad, y les ofrecemos una oferta completamente personalizada, de acuerdo con sus necesidades. En el caso de los miembros del canal de distribución, nos aseguramos de ofrecerles tecnologías que no protejan solo su información, sus equipos y sus redes, sino también toda la relativa a los demás eslabones de la cadena".

¿Son efectivas las estrategias tradicionales?

Para Alberto Tejero, "hay que tener en cuenta que el paradigma de la seguridad digital ha cambiado. Las fórmulas tradicionales de catalogación de virus y amenazas han dejado de ser efectivas. La evolución de las amenazas y la multiplicación de endpoints (PC, móvil, tablet…) requieren un servicio basado en la análisis y monitorización continúa de la actividad de las aplicaciones".

De la misma opinión son los responsables de Spamina, que señalan que "las medidas tradicionales de seguridad en el correo electrónico, como son el antivirus y el antispam, ya no son suficientes para los usuarios. El email y la mensajería instantánea son los canales más accesibles para la difusión de malware y los hackers diseñan cada vez amenazas más sofisticadas, difíciles de detectar. Hace falta implementar soluciones con tecnologías avanzadas que permitan analizar los ficheros y las url que aparecen en tiempo real, justo cuando el usuario intenta acceder".

"Si hablamos por estrategias tradicionales, la utilización de un firewall clásico o un UTM, obviamente, no", apuntan desde SonicWall, y añaden que "es fundamental mantener una defensa multicapa y, sobre todo, realizar toda la inspección en cada capa sobre el tráfico cifrado y aportar tecnología de Sandboxing multimotor para la protección de ATP y amenazas día cero, todo esto con entender la organización como un todo, y dotar de todas las capas de seguridad necesarias en los accesos remotos, y en la recepción y envío de correo".

La única opinión discordante, pero con matices, la ofrece Fernando Herrero, que comenta que estas estrategias tradicionales "siguen siendo importantes en la estructura de seguridad de una empresa. De hecho, consiguen bloquear casi el 100% de todos los ataques conocidos que intentan penetrar en los servidores y los endpoints de las compañías. El problema viene con las amenazas desconocidas y las de día cero que, al no haberse detectado nunca antes, no pueden ser interceptadas. Por esto, las compañías deben implementar soluciones avanzadas, ya que no se basan en detectar las amenazas, sino que las previenen. Esto lo hacen con tecnologías como el sandbox avanzado, la extracción de amenazas y la detección a nivel de CPU".

que el tráfico encriptado Secure Sockets Layer/Transport Layer Security ha aumentado un 38% año tras año, situándose en un promedio del 60% del total del tráfico; que los cibercriminales desviaron su atención hacia nuevas amenazas, incluyendo los ataques ransomware, que han aumentado 167 veces año tras año; y que los dispositivos vinculados al Internet de las Cosas han creado un nuevo vector de ataque, abriendo la puerta a ataques de negación de servicio distribuidos a gran escala".

Por último, desde Spamina, nos recuerda que "en los últimos años, las empresas han evolucionado su forma de comunicación utilizando herramientas que agilicen la interlocución, como es el caso de la mensajería instantánea a través de dispositivos móviles. Esto abre nuevas puertas de acceso a ciberdelincuentes, además de provocar un incremento de errores internos, ya sean intencionados o no, que causan desvío o pérdida de la información".

Pero antes de terminar, hemos querido pulsar la opinión de un mayorista, eslabón imprescindible en la cadena de la seguridad. Y, precisamente, la llegada de una nueva normativa en cuestión de protección de datos es una de las cosas que destacan desde V-Valley. Así, tal y como nos explican desde la firma, "hay una gran tendencia hacia la protección de las amenazas desconocidas. Hoy en día, el antivirus y el firewall tradicional no son 100% efectivos y las soluciones que hay actualmente en el mercado basadas en el análisis de comportamientos y en los firewalls de nueva generación, demuestran que estamos en un sector

LA SEGURIDAD, SEGÚN... KASPERSKY LAB

Tal y como nos explican desde el fabricante, "el enfoque efectivo en las estrategias de seguridad pasa por tratar la amenaza con un conjunto de soluciones y tecnologías de protección multi-capa. Ya no se trata sólo de prevenir incidentes, sino de predecir, detectar y responder a ellos. Y hacerlo de forma flexible, fiable y efectiva, teniendo en cuenta que la seguridad no es un estado, sino un proceso en constante evolución".

que avanza rápidamente y que necesita estar al día de las soluciones actuales. Además, el nuevo reglamento europeo de la protección de los datos de sus ciudadanos (GDPR) obliga a hacer conscientes a los dueños de las empresas de la importancia de asegurar los datos de las mismas, para cumplir la legislación y evitar posibles sanciones económicas. Por último, el movimiento de las empresas hacia la nube, como Azure de Microsoft, abre nuevas necesidades de securizar entornos híbridos, donde la red no está tan definida como tradicionalmente".

PRINCIPALES AMENAZAS

Para Alberto Tejero, "la mayoría de amenazas que existen hoy en día son aquellas que buscan algún beneficio económico, directo o indirecto. Uno de los tipos de ataques más prevalentes hoy en día en el mundo de la empresa es el del ransomware, que secuestra la información y pide un rescate para poder recuperarla. A continuación, tenemos ataques protagonizados por troyanos cuyo principal objetivo es el robo de información confidencial o robo de credenciales. También hay amenazas que tratan de comprometer cuentas de correo corporativo. Es una forma más evolucionada de realizar phishing. En este tipo de ataques hay más conocimiento acerca de las víctimas y alguien se hace pasar por el CEO o por un alto ejecutivo e instruye a una persona para que realice determinadas acciones. Por ejemplo, realizar una transferencia a una determinada cuenta".

Una opinión similar tienen en Spamina, desde donde nos explican que "tanto las empresas como los usuarios están expuestos al robo de su información por ciberdelincuentes para enriquecerse. En el ámbito empresarial el impacto va más lejos aún, siendo la propiedad intelectual y la reputación dos factores a tener muy en cuenta. No es sólo el valor de lo que han robado, sino el impacto futuro en la actividad empresarial".

Y es que, como nos recuerdan desde SonicWall, "las empresas y los usuarios con acceso a internet están expuestos a todas las actividades de los cibercriminales, desde las suaves, como que sus equipos estén comprometidos y pertenezcan a una red de bootnet, para ser utilizados como servidores de envío de spam o unidades de ataques de denegación de servicio distribuido,

LA SEGURIDAD, SEGÚN... SONICWALL

Según la estrategia de SonicWall, "lo primero es definir la organización como un todo, y abordar todas sus áreas, con soluciones de seguridad colaborativas, para minimizar al máximo las posibles brechas de seguridad". Se trata de una estrategia que abarca varios elementos, tales como "securizar la red, una solución robusta de acceso remoto de usuarios, utilización de soluciones de seguridad eficaces en el punto de acceso, y protección de los servidores de correo".

El eslabón más débil

Los responsables de Kaspersky Lab tienen claro que "la seguridad de una empresa es tan fuerte como su eslabón más débil y normalmente suelen ser los empleados. En este caso, la formación y conciencien en materia de seguridad debería incluirse como parte integral de las estrategias de seguridad con el fin de prevenir y minimizar los riesgos".

Para Fernando Herrero, "un gran porcentaje de los ataques que sufren las empresas tienen su desencadenante en un archivo descargado por un empleado. Basándonos en esto, podríamos decir que el eslabón más débil es el factor humano. ¿Cómo evitar que se conviertan en aliados involuntarios de los ciberdelincuentes? El primer paso es la concienciación y la formación de las plantillas. Si los trabajadores tienen unos conocimientos básicos de seguridad, dejarán de caer en las trampas puestas por los hackers, como los mensajes de phishing. Además, esta educación debe ser cumplimentada con un entorno seguro de trabajo, que les impida descargar cualquier documento sospechoso o acceder a un link peligroso".

La misma opinión tienen los responsables de SonicWall, que comentan que "todos los ataques de Spear Phising, ingeniería Social… tienen como destinatarios a los usuarios. La forma de solventarlo o minimizarlo es realizar una formación bastante básica, sobre la recepción de mensajes, sus enlaces y sus adjuntos. Otro aspecto es la prevención de utilización de dispositivos de almacenamiento extraíble" por parte de estos usuarios. "El desconocimiento, la falta de concienciación y la rápida difusión de los ataques", apuntan desde Spamina, y añaden que "los errores internos, generalmente no intencionados, son los más extendidos. Por eso, es importante que las empresas implementen soluciones que permitan administrar políticas automáticas para la prevención de la fuga de datos".

Por último, Alberto Tejero indica que "la movilidad y la multiplicación de endpoints suponen un reto a la seguridad de las compañías. La tecnología es una herramienta posibilitadora de la flexibilidad laboral. Pero hay que dotarse de las herramientas necesarias para garantizar la seguridad".

hasta los más peligrosos, como ataques de día cero, ransomware, o malware en general".

Para los responsables de Kaspersky Lab, "el crecimiento de ciberamenazas, cada vez más preparadas y dañinas, hace que tanto empresas como usuarios tengan que estar en alerta constante. Desde ataques DDoS a APT, pasando por el ransomware, como el ataque global de este mes, son algunas de las amenazas a las que más están expuestas las organizaciones. Los usuarios tampoco se libran de los cibercriminales, y pueden ser víctimas de numerosas amenazas. Por ejemplo, existe un tipo de malware en Android que, además de robar datos financieros de mensajes de texto y de voz, es capaz de superponer ventanas que simulan páginas oficiales de inicio de sesión para hacerse con información personal y bancaria de los usuarios. También las infecciones por ransomware, cada vez más, afectan a usuarios finales a través de dispositivos móviles".

En este sentido, desde Check Point añaden que "las personas y las com-

pañías tienen que hacer frente en su día a día a ciberamenazas de todos los tipos. En los últimos meses, han tomado mucha fuerza los Exploit Kits, programas maliciosos que descubren y explotan vulnerabilidades. Cuando lo hacen, descargan en el equipo infectado ransomware como WannaCry o gusanos como Slammer. Otro vector de ataque importante es el phishing, y su variante móvil smishing. A través de correos fraudulentos y webs falsas, los ciberdelincuentes engañan a los usuarios para que den información personal o instalen malware. Tampoco conviene olvidarse de las botnets, conjuntos de robots que existen en casi todas las empresas, y que se alojan en los equipos infectados a la espera de que su creador les dé una instrucción, como lanzar un ataque DDoS contra una dirección IP o robar información personal o corporativa".

¿CÓMO RESPONDER A ESTAS AMENAZAS?

Según nos indica Fernando Herrero, desde Check Point, "al igual que las empresas están alcanzando en los últimos años la transformación digital y la omnicanalidad, también lo hacemos nosotros. Por esa razón, hemos creado la infraestructura de seguridad del futuro, Check Point Infinity. Infinity no se encarga solo de proteger los ordenadores que hay en la sede o la sucursal de una empresa, sino también todos los dispositivos móviles que utilizan sus empleados y los entornos cloud. A través de una única plataforma de seguridad, una prevención de amenazas anticipada y un sistema de protección consolidado, Check Point Infinity permite a las empresas tomar el control de su seguridad".

Para Kaspersky Lab, "vivimos en un mundo donde la pregunta ya no es si seremos atacados, sino cuándo y cómo de rápido serás capaz de recuperarte. No hay una única tecnología de protección perfecta y nunca la habrá. El enfoque efectivo en las estrategias de seguridad pasa por tratar la amenaza con un conjunto de soluciones y tecnologías de protección multi-capa. Ya no se trata sólo de prevenir incidentes, sino de predecir, detectar y responder a ellos. Y hacerlo de forma flexible, fiable y efectiva, teniendo en cuenta que la seguridad no es un estado, sino un proceso en constante evolución".

Desde el punto de vista de soluciones de seguridad, apuntan desde SonicWall, "lo primero es definir la organi-

LA SEGURIDAD, SEGÚN... MICROSOFT

Según comentan desde Microsoft, la compañía cuenta con tres elementos fundamentales. Primero, "incorpora la seguridad en los productos y servicios desde el principio, ofreciendo una plataforma ágil y robusta, capaz de actuar más rápido para detectar las amenazas y responder a las infracciones de seguridad incluso en las organizaciones de mayor tamaño. En segundo lugar, la inteligencia de las inmensas fuentes de datos de Microsoft, le confiere una visión única que le permite identificar modelos sospechosos a través de machine learning e inteligencia humana para detectar pronto las amenazas y responder con rapidez. Y, tercero, Microsoft trabaja con la industria e identidades compartiendo información sobre vulnerabilidades con más de 50 partners, de forma que los clientes puedan protegerse lo más rápido posible".

La visión del mayorista

Para conocer esta visión del mayorista, hemos conversado con V-Valley, cuyos responsables nos indicaban que "Nuestro papel principal es trabajar con los fabricantes para llegar a todos los distribuidores de informática que quieran especializarse en el mercado de la seguridad TI. La capacitación de partner y el soporte antes, durante y después del proceso de venta, es nuestra prioridad. De este modo, independientemente del tamaño del reseller, siempre estará acompañado y con soportado para garantizar el éxito de cada proyecto".

En el caso específico de V-Valley, "nuestra especialización y capacitación, junto con la estrecha relación que tenemos con los fabricantes de seguridad con los que trabajamos, permite que trabajemos con nuestros resellers para detectar en sus clientes la oportunidad de negocio y la necesidad de estar protegidos. Les ofrecemos mensajes personalizados por cada tamaño de empresa al que se dirigen de modo que puedan enfocar la venta directamente a las necesidades y preocupaciones que tiene cada tipo de empresa. No es el mismo el mensaje el que deben utilizar los resellers que trabajan los sectores de educación, que por ejemplo los que se dedican al sector industria o a verticales específicos como el de los ERP".

Junto con esto, "proporcionamos todas las herramientas y recursos necesarios para generar demanda, desde material para detectar oportunidades, generar campañas de telemarketing y contenido para realizar webinars o eventos presenciales con sus clientes finales. Tenemos disponibles consultores pre-preventa certificados y especializados que dimensionarán adecuadamente la solución y, en el caso de ser necesario, preparan un proceso de prueba o piloto para que la tecnología sea probada in-situ. Demostrar lo que la tecnología es capaz de hacer hoy en día y hacer conscientes de las amenazas y problemas que hay en las redes informáticas, es un factor clave que acelera el proceso de decisión de compra. Por último, está la parte de puesta en marcha e implementación, donde nuestro equipo de servicios tecnológicos está a disposición de todos los partners que aún no se sientan capacitados para hacer este proceso de forma autónoma. Independientemente de si el reseller decide formarse técnicamente, nosotros apoyamos también la fase de implementación y de transferencia del conocimiento".

Con ello, "cualquier reseller que vea que hay interés o necesidad de implementar soluciones de seguridad en sus clientes y quiera explorar esta oportunidad, puede trabajar conjuntamente con nuestro equipo que dará visibilidad el más adecuada por tamaño de cliente final y de sector vertical de los mismos. A partir de ahí es el reseller el que decide cuánto quiere capacitarse y a qué ritmo".

zación como un todo, y abordar todas sus áreas, con soluciones de seguridad colaborativas, para minimizar al máximo las posibles brechas de seguridad. Primero, securizar la red con un firewall de nueva generación con todas las capas de protección necesarias, antimalware, filtro de acceso a web, IPS-IDS, antiBootnet, GeoIP, sandboxing de nueva generación multimotor y, sobre todo, teniendo la capacidad de realizar la inspección profunda de paquetes sobre tráfico cifrado SSL /TLS y SSH, sin limitación de tamaño, ni de puertos ni de protocolos. A esto hay que añadir, una solución de acceso remoto de usuarios robusta con doble factor de autentificación, con mecanismos de control de EndPoint, basado en las propias reglas de la compañía, con capacidad de seleccionar las aplicaciones a utilizar corporativas y que estas mismas gestiones el acceso a través de túneles SSL securizados. Además, utilización de soluciones de seguridad de EndPoint eficaces y, a ser posible, de diferente tecnología que las que se tienen en el perímetro y en la red. Y, junto con ello, protección de los servidores de correo, con soluciones altamente eficaces, con diferentes motores de antivirus y con sandboxing multimotor de nueva generación y con capacidad de encriptación de los correos".

LA SEGURIDAD, SEGÚN... PANDA SECURITY

En opinión de Alberto Tejero, "en Panda Security apostamos por un enfoque disruptivo, proactivo y estructuralmente diferente al de los productos de seguridad tradicionales. Con Adaptive Defense ofrecemos seguridad para el endpoint a través de una plataforma cloud basada en la investigación, análisis, categorización y correlación permanente en tiempo real del comportamiento y el contexto de apertura de todas las aplicaciones que se intentan ejecutar en cada equipo. Adaptive Defense es capaz de obtener automáticamente una clasificación determinista para el 99,99% de los casos de forma directa. Los casos restantes se procesan mediante un equipo de técnicos especialistas en seguridad cuya misión es establecer el riesgo de esas aplicaciones y, sobre todo, mejorar el sistema de clasificación para que sea capaz de resolver automáticamente estos nuevos casos en el futuro".

Por su parte, Microsoft promueve "una actitud renovada en materia de seguridad. La mayoría de las organizaciones tienen una estrategia contra las amenazas basada en 3 pasos: proteger, detectar y responder. Este modelo no ha cambiado en los últimos 20 años y todavía es relevante hoy. Sin embargo, hemos cambiado la forma en que se ejecuta cada uno de ellos en todos los productos: proteger, con funcionalidades que protegen la identidad, datos, aplicaciones, dispositivos e infraestructura, tanto si es en la nube como si no, y esto implica considerar todos los end-points críticos desde sensores al datacenter; detectar, a partir de señales específicas, monitorización de comportamientos y machine learning que permitan una respuesta inmediata; y responder, cerrando el gap entre el descubrimiento y la acción".

Así, Microsoft está construyendo una plataforma "con una aproximación holística que tiene en cuenta todos los puntos críticos en un mundo regido por la movilidad y la nube. La inversión en esta plataforma se hace en cuatro categorías: identidad, aplicaciones y da-

LA SEGURIDAD, SEGÚN... SPAMINA

En Spamina, "nuestra visión es ir un paso por delante de los hackers. Nuestra estrategia se basa en considerar la comunicación empresarial como un todo, entender la cadena y los procesos de colaboración, y ofrecer una solución flexible, fácil de implementar, que sea accesible en todos los eslabones de esta cadena. La oferta de Spamina va desde soluciones para la protección del correo electrónico a soluciones de archivado y cumplimiento de normativas, y está disponible para todos los servidores de correo en modo nube pública, privada o híbrida. Además, esta experiencia nos ha llevado a desarrollar nuestra propia solución de correo, Parla con la seguridad integrada".

tos, dispositivos e infraestructura, con un enfoque inclusivo de la tecnología que nuestros clientes ya estén utilizando. Microsoft cuenta con una amplia inteligencia en materia de seguridad cibernética creada a partir de los miles de millones de puntos de datos de las diversas fuentes que analiza y cuenta con un ecosistema de partners que mejoran los estándares del sector permitiendo a sus clientes a llevar a cabo sus procesos de transformación digital de una forma segura".

En opinión de Spamina, "el reto pasa por movilizar las infraestructuras al Cloud. Un proceso que, si bien está adoptado por la mayor parte de las compañías, aún mantiene un nicho reacio al cambio. El Cloud permite a las compañías aligerar costes de gestión e infraestructuras, pero, sobre todo, la flexibilidad de adaptar las soluciones de seguridad a los requerimientos del negocio de manera inmediata".

Finaliza Alberto Tejero, Panda Security, indicando que disponen de "una fórmula que visibiliza y controla todo lo que sucede en el endpoint: software ejecutado, aplicaciones vulnerables y comportamiento de usuarios para ofrecer una solución 360. Con este tipo de protección podemos utilizar la tecnología para que nos ofrezca flexibilidad, ya que podemos ofrecer un altísimo nivel de seguridad en todos los dispositivos desde los que trabajemos".

ENLACES DE INTERÉS

- ⇉ Check Point Software
- ⇉ Kaspersky Lab
- ⇉ Microsoft
- ⇉ Panda Security
- ⇉ Spamina
- ⇉ SonicWall
- ⇉ V-Valley

Estos mercados son dos de los segmentos de tecnología de consumo que mejor están funcionando

El canal se mueve hacia el gaming y la Realidad Virtual

El gaming ha pasado a ser un mercado casi exclusivo de los entusiastas a convertirse en una de las grandes oportunidades de negocio. Así lo constatan numerosas consultoras que destacan el potencial de éste para el canal de distribución TI. Además, está impulsando otros sectores, como la Realidad Virtual, que ya ha entrado en una fase de democratización. Estos dos segmentos marcarán el futuro del consumo y los resellers no pueden, ni deben, dejar de lado.

El gaming es uno de los segmentos de tecnología de consumo que mejor están funcionado en los últimos años. No en vano, datos de la Asociación Española de Empresas Productoras y Desarrolladoras de Videojuegos (DEV), elevan a más 500 millones de euros el volumen de ingresos de esta industria, una cantidad nada despreciable, pero casi nada comparado con las previsiones se manejan para este año. Algunas consultoras, vaticinan que el crecimiento interanual podría acercarse al 90%. España, además, es, según datos de EAE Business School, el décimo territorio mundial con un mayor número de gamers, en torno a los 20 millones.

GfK es otra de las consultoras que constata el buen momento que está viviendo el mercado de gaming. Según datos de la misma, el año pasado esta área generó un volumen de nego-

GAMING, APPS Y SOCIAL MEDIA, OPORTUNIDADES DE UN MERCADO EN CRECIMIENTO

CLICAR PARA VER EL VÍDEO

Jonathan Wagstaff, country manager de Context en Reino Unido e Irlanda

La oportunidad del gaming para el canal

A no ser que en los dos últimos años se haya vivido debajo de una roca, es difícil escapar al crecimiento que está experimentando el mercado de Gaming PC. A día de hoy ya es algo muy común saber que el SKU de los juegos tiene un ASP mucho más alto que el de los sistemas estándar y que los accesorios para los juegos ofrecen un excelente margen y permiten fijar unas tarifas mejores a los retailers.

En el pasado, el mercado de PC Gaming estaba acotado a los entusiastas que tenían las capacidades de para construir o actualizar sus propios sistemas de sobremesa con mejores GPU, o para aquellos que conocían desarrolladores de sistemas y estaban dispuestos a pagar por sus servicios Premium. En la actualidad estamos viendo un gran impulso de algunos OEM, como HP, Lenovo y otros desarrolladores de sistemas pre-construidos, con el objetivo de llegar a aquellos recientes conversos de consolas de gaming.

Sin embargo, quizás es más importante conocer por qué el mercado de PC Gaming está creciendo. Uno de los grandes impulsores es el segmento de los eSports, cuyos aficionados juegan, mayoritariamente, con un ratón y una configuración de teclado. Esto descarta la mayoría de los

títulos propios de la consola, ya que los gamepads no ofrecen la precisión necesaria para competir en primera persona en juegos de "pistoleros" o de estrategia. Las cifras de eSports hablan por sí solas. Twitch tiene más de dos millones de usuarios al día.

Los aficionados de eSports no siempre utilizan juegos de PC, de la misma manera que los aficionados al fútbol raramente juegan a este deporte. No obstante, hay muchos usuarios que sí que quieren imitar a sus héroes, aunque tradicionalmente sólo hayan jugado con consolas. El secreto acerca de los ratios de velocidad del PC y la calidad GFX también está al descubierto y es notable que Microsoft está realizando grandes esfuerzos en marketing ante la llegada de Xbox Scorpio con información sobre su FPS incluida. Sólo se tiene que mirar el número de títulos que se están desarrollando para el PC, que en la actualidad superan a los de la consola, para saber por dónde sopla el viento.

La oportunidad para el canal está ahí, pero requiere prestar especial atención a esta categoría en particular. Si se venden sistemas OEM, hay que asegurarse de informar, claramente, a los consumidores cuáles son los títulos que se pueden utilizar en un PC y cuáles están preparados para la Realidad Virtual. Si se va a tener en stock el ratón o los auriculares más populares para el mercado de juegos, hay que asegurarse de que se conoce profundamente qué es lo que se está vendiendo.

Por último, los bajos tipos de interés que hay en la actualidad en la UE han convertido al crédito en una buena opción para la venta de este tipo de sistemas. Hay que tener en cuenta que el hecho de que un PC cueste unos 1.000 dólares no significa que los más jóvenes abandonen este mercado.

cio de 165 millones de euros entre la venta de PC y de periféricos. En total, en 2016 se comercializaron un millón de unidades y por cada PC comercializado se vendieron 6 periféricos. “El precio medio de PC gaming es de 1.009 euros”, se destaca desde la consultora que puntualiza que esto supone duplicar el precio medio del mercado de PC. Las estimaciones de GfK sitúan el crecimiento del valor del mercado en un 61%, lo que supone que España crece por encima de otros países europeos como Francia, Alemania, Reino Unido o Italia.

En el terreno de los PC de sobremesa, GfK desvela que los ordenadores para gaming registraron un aumento de ingresos de un 75%, con un crecimiento de ventas del 58%. La demanda de portátiles para gaming también se incrementó en un 95% en unidades vendidas y un 46% en volumen de ingresos. Casi la mitad de los ordenadores portátiles de gaming vendidos en lo que va de año superaron los 800 euros. Los productos de gaming demuestran ser una categoría atractiva para los fabricantes y retailers.

El mercado de periféricos para gaming también muestra un excelente potencial de ingresos. Los teclados, ratones y auriculares experimentaron un fuerte crecimiento en el primer semestre de 2016. Los teclados fueron particularmente populares entre los consumidores, registrando un crecimiento en ingresos del 23%, superando los 86 millones de euros en el primer semestre. Los auriculares se venden igual de bien, con el aumento de ingresos de un 19%.

Áreas geográficas

Geográficamente, y según datos de Transparency Market Research (TMR), el mercado de gaming está liderado por Norteamérica y Europa, debido a la fácil disponibilidad en estas regiones de los últimos lanzamientos del mercado, así como los últimos avances en computación y diseño gráfico. Pero la demanda tanto de hardware como software está aumentando en Asia Pacífico, donde la adopción de la cultura occidental ha generado una gran base de usuarios. Asia Pacífico será un mercado clave en los próximos años debido a la creciente prosperidad de los consumidores en países como Japón, India, China, Corea del Sur y Taiwán.

Uno de los principales impulsores del mercado mundial de gaming es la creciente disponibilidad de Internet de banda ancha en regiones en desarrollo, como Asia Pacífico, ya que los jugadores pueden expe-

España es, según datos de EAE Business School, el décimo territorio mundial con un mayor número de gamers, en torno a los 20 millones

En el terreno de los PC de sobremesa, GfK desvela que los ordenadores para gaming registraron un aumento de ingresos de un 75%, con un crecimiento de ventas del 58%

rimentar con los juegos en línea. El aumento de los ingresos de los consumidores en las regiones emergentes también ha impulsado la demanda de hardware de gaming, como las consolas.

¿Por qué crece?

Para Fernando Suárez, Product Manager de MCR, estos datos corroboran el gran potencial de este mercado, que va a suponer una nueva revolución en el segmento del consumo. “El progreso en las tecnologías ha sido el factor principal de crecimiento del mercado, pero también han influido otros, como la convergencia entre los juegos y otros soportes como el cine y la TV, o la tendencia hacia una experiencia plena, que ha hecho que, incluso dentro del propio nicho del gaming hayan surgido numerosos “sub-nichos” que agrandan aún más el mercado y su progresión”, señala.

Con los juegos para móviles en pleno auge y lo que parece ser de nuevo un mercado receptivo a las videoconsolas, sumado al lanzamiento de nuevos productos, 2017 va a ser un año crucial para la industria del gaming. A medio plazo se perciben también otros factores, como es el caso la realidad virtual, donde ya hemos visto productos prometedores, como el casco Oculus Rift o las gafas Sony Playstation VR, y donde se esperan novedades. Otro apartado de gran importancia, especialmente para el distribuidor, es el fenómeno de las ventas online, que para los retailers está planteando un reto importante.

“El gaming es, sin lugar a dudas, la nueva revolución en el mercado de consumo”, explica Fernando Suárez. “El canal ha de prepararse

Ensambladores de PC de sobremesa han visto en los eSports y el gaming la oportunidad perfecta de reavivar las ventas

para lo que se avecina. Especialización, agilidad y, sobre todo, adaptación a los nuevos modelos de distribución, serán claves para aprovechar todas las oportunidades que se vislumbran en el horizonte".

La innovadora y dinámica estructura de precios del mercado de gaming es otro factor clave para el crecimiento del mercado. Debido a la creciente demanda de smartphones avanzados, muchos desarrolladores de juegos han adoptado un modelo de ingresos basado en anuncios.

EL MARKETING Y LA REALIDAD VIRTUAL

CLICAR PARA VER EL VÍDEO

Si bien esto no tendrá un impacto notable en la demanda de juegos para PC, ha ampliado el alcance del mercado mundial de gaming de manera significativa.

Sectores que se benefician del gaming

El auge del mercado de gaming está beneficiando a otros sectores que, en los últimos años no han atravesado sus mejores momentos. Éste es el caso del mercado de PC de consumo o de las pantallas.

En el caso del primero, un estudio de Context explica que el segmento de PC de consumo se mantendrá estancado en Europa occidental. Existe la posibilidad de que la escasez de componentes, que afectó la disponibilidad de productos en la segunda mitad del año pasado, lleve a aumentos de precios en la primera mitad de 2017 que podrían afectar la demanda. Sin embargo, es probable que el mercado se beneficie de la continua demanda de PC para gaming. Si bien este segmento sigue

Modelo de consumo de TI como servicio para la innovación empresarial

El modelo "TI como servicio", no solo desde la nube pública, sino también in situ para crear un entorno de TI híbrida y flexible, puede hacer que TI consuma los recursos necesarios de la forma adecuada para mantener y promover la innovación en la empresa. Este modelo permite que una organización pague según consuma, y admite pagos mensuales, lo cual significa que la empresa ve el valor en un ciclo recurrente. IDC analiza este enfoque y la propuesta de HPE para ayudar a la TI a acelerar la transformación digital.

siendo pequeño en términos de volumen, las nuevas tecnologías, incluida la realidad virtual, también impulsarán un crecimiento que tendrá un efecto positivo en los ingresos y los márgenes.

A pesar de que la caída del mercado de PC ha lastrado las ventas de monitores de consumo, se espera que el resultado total se mantenga con respecto al año pasado, gracias al crecimiento de las líneas de monitores para empresa y gaming. En este sentido, según datos de Asus, las ventas de monitores alcanzaron los 120 millones de unidades durante 2015 y se mantuvieron a un nivel similar en 2016. Aunque durante 2015 solo se vendieron cerca de 600.000 unidades de monitores gaming, en 2016 el volumen total superó los 1,2 millones de unidades vendidas. Atendiendo a los pedidos actuales, para este año se espera que las ventas de monitores gaming crezcan hasta los 2,5 millones y hasta los 3,5 millones en 2018. Ello dependerá de la disponibilidad de paneles y de las fluctuaciones de los tipos de cambio.

A pesar de que los modelos gaming solo suponen entre un 1 y un 2% de las ventas, su elevado precio impulsa su valor productivo hasta el 3%.

En el segmento de monitores tradicionales, el tamaño más buscado es 21,5 pulgadas, con 23 y 24 pulgadas en segundo lugar. Actualmente, los monitores de 24 pulgadas con un precio entre 299 y 400 dólares representan el 70% de las ventas del segmento gaming, seguidos de los de 27 pulgadas y los modelos de 34 y 35 pulgadas. Se espera que crezca la demanda de monitores con un tamaño superior a 35 pulgadas.

La demanda de portátiles para gaming también se incrementó en un 95% en unidades vendidas y un 46% en volumen de ingresos

El mercado de eSports, nuevo negocio para el canal

Otra de las grandes oportunidades para el canal de distribución es el mercado de los

Fernando Suárez, Product Manager de MCR Infoelectronics

Gaming: una nueva revolución en el mercado de consumo

El segmento del juego es uno de los apartados de la tecnología que mejor han funcionado en los últimos años. Desde la Asociación Española de Empresas Productoras y Desarrolladoras de Videojuegos (DEV), se estima que esta industria supone ya en torno a los 1.000 millones de euros. Una cantidad nada despreciable, pero casi nada comparado con las previsiones se manejan para este año, que pasan de nuevo por un fuerte crecimiento, y una tendencia similar para los próximos ejercicios. Algunas consultoras, incluso, calculan que el crecimiento interanual podría acercarse al 90%. España, además, es, según datos de EAE Business School, el décimo territorio mundial con un mayor número de gamers, en torno a los 20 millones.

Estos datos son una buena muestra del enorme potencial de este mercado, que va a suponer una nueva "revolución" en el segmento del consumo. Un mercado que en los últimos años ha evolucionado de forma vertiginosa, y donde el progreso en las tecnologías ha sido el factor principal de crecimiento, pero también han influido otros como la convergencia entre los juegos y soportes como el cine y la TV. La tendencia hacia una "experiencia plena" (ergonomía, calidad audiovisual, accesorios…) ha hecho que, incluso dentro del propio nicho del gaming, hayan surgido numerosos "sub-nichos" que agrandan aún más el mercado y su progresión: desde PCs y portátiles, hasta soluciones más específicas como fuentes de alimentación y sistemas de ventilación, sillas y mesas de gaming, gafas, cascos, ratones y teclados, alfombrillas, monitores, sistemas de almacenamiento, soluciones audiovisuales…

Con los juegos móviles en pleno auge, la realidad virtual a la vuelta de la esquina, y el continuo lanzamiento de nuevos productos, 2017 va a ser un año crucial para la industria del gaming. Los eSports están reavivando el mercado con márgenes saludables en un segmento en el que parecía que sólo se podía competir por precio. Un mercado que está ya a disposición no sólo de los dealers especializados, sino de todos aquellos distribuidores de tecnología que deseen aprovechar la oportunidad de negocio que supone.

Para MCR el gaming es un área clave. De hecho, somos el primer mayorista que ha introducido una oferta completa con productos de todo tipo, hasta los más específicos. El objetivo está claro: construir la oferta más completa, y aportar al distribuidor herramientas e información clara y detallada sobre los productos, para que le resulte fácil vender. Asimismo, contamos con un grupo dedicado específicamente a este segmento, así como una página web sobre gaming donde se muestra una gran variedad de contenidos, productos por categorías o comunicación directa con los expertos.

El gaming es, sin lugar a dudas, la nueva "revolución" en el mercado de consumo. El canal ha de prepararse para lo que se avecina. Especialización, agilidad y, sobre todo, adaptación a los nuevos modelos de distribución, serán claves para aprovechar todas las oportunidades que se vislumbran en el horizonte.

El 42% de los mayoristas de EMEA considera el gaming como una de las tres principales categorías con un gran potencial de crecimiento en 2017

eSports. Según SuperData Research, éstos generan 748 millones de dólares, con Norteamérica y Europa representando la mitad de ese mercado, y el total de espectadores creció este año hasta los 188 millones. Pues bien, los analistas auguran unos ingresos de 2.000 millones en el futuro cercano.

Por todo ello, se ha generado un mercado enorme, que acaba de comenzar, y que, en el caso del PC ha supuesto una resurrección. Ensambladores de PC de sobremesa han visto en los eSports y el gaming la oportunidad perfecta de reavivar las ventas, con el lanzamiento de equipos con diseños agresivos y hardware de última generación que buscan seducir al público joven que busca dedicarse a jugar de forma competitiva. No sólo el mercado de ordenadores, también el de periféricos y componentes, viven gracias a los eSports. Pero es que, además, dentro del propio mercado han surgido numerosos nichos de producto que aportan soluciones para gaming específicas, y que vienen a multiplicar su potencial.

Los mayoristas de EMEA ven en el gaming una oportunidad

Y con estos datos en la mano, no es de extrañar que los mayoristas vean en este mercado una gran oportunidad. Un estudio presentado en DISTREE EMEA señala que el 42% de los mayoristas considera el gaming como una de las tres principales categorías con un gran potencial de crecimiento en 2017. Dos terceras partes desearían ampliar el número de marcas en este segmento.

"El mercado de productos y accesorios para gaming en EMEA continúa creciendo y el impulso que se está generando alrededor de la realidad virtual (VR) garantiza que el gaming sigue siendo una prioridad en el canal como categoría de crecimiento para 2017", señala Christophe Painvin, director de DISTREE EMEA 2017.

Por su parte, Liam McSherry, director de marketing de DISTREE EMEA, afirma que “los resultados de la encuesta también muestran que dos tercios de los mayoristas quieren aumentar activamente el número de marcas que llevan”.

Painvin añade que “construir los canales de comercialización adecuados de forma rápida y eficiente puede dar a las marcas de gaming una gran ventaja en la región EMEA”.

Qué tienen que hacer los mayoristas

El desarrollo de los negocios de gaming y de realidad virtual requerirá los mayoristas establezcan relaciones más estrechas con los retailers y e-tailers en el lado del consumidor, y con partners centrados en mercados verticales en el entorno B2B, señalan desde Context.

Cada vez más mayoristas se están enfocando en el segmento del gaming y la realidad virtual. Y es que, como explica Jonathan Wagstaff, country manager de Context en Reino Unido e Irlanda, “el gaming para PC está creciendo rápidamente y ofrece márgenes más altos, particularmente en torno a los periféricos. El juego multijugador está despegando y las ganancias de los e-sports muestran que los jugadores profesionales de títulos como DOTA 2 pueden ganar más dinero que el ganador de Wimbledon. La realidad virtual impulsará aún más este mercado”.

Según Context, el año pasado entramos en una nueva era: la democratización de la Realidad Virtual

Además, la realidad virtual no sólo estará en el dominio del consumidor. Wagstaff predice que su uso en el sector profesional será enorme, y ya está despegando en la educación. “Instituciones médicas ya están usando dispositivos como Oculus Rift para enseñar procedimien-

El desarrollo de los negocios de gaming y de realidad virtual requerirá que los mayoristas establezcan relaciones más estrechas con los retailers, e-tailers y partners centrados en mercados verticales

tos médicos y ya se han hecho algunos descubrimientos asombrosos, como el uso que la Universidad de Duke ha hecho de la realidad virtual para ayudar a los parapléjicos a recuperar el movimiento y sensibilidad de algunos músculos. Cada hospital y cada organización en el mundo desarrollado va a querer esta tecnología".

Qué pasa con la Realidad Virtual

La realidad virtual ya está en la lista de prioridades de muchos mayoristas. La oportunidad de este mercado no está tanto en la venta de dispositivos en sí, como en el contenido, porque representa ingresos recurrentes. Evidentemente, los mayoristas seguirán vendiendo los dispositivos, pero se pueden lograr mayores márgenes asociándose para administrar el contenido.

Context refuerza la importancia de las asociaciones. En su encuesta sobre Realidad Virtual en Europa, la consultora encontró que el 26% de la gente preferiría comprar de retailers de tecnología especializados. El desarrollo de los negocios de gaming y de realidad virtual requerirá los mayoristas establezcan relaciones más estrechas con los retailers y e-tailers en el lado del consumidor, y con partners centrados en mercados verticales en el entorno B2B, concluye Wagstaff.

"El año pasado entramos en una nueva era: la democratización de la Realidad Virtual", señala Elena Montañés, country manager de Context en España, quien destaca la importancia de este segmento para el canal. "En 2016, el precio medio de venta de los PC

con capacidad para soportar la realidad virtual vendidos a través del canal de distribución fue de 1.494 euros, mientras que el precio medio de venta de los accesorios de gaming fue de 48 euros, mucho mayor que el precio medio de los accesorios estándar, que se situó en los 23 euros".

Montañés explica que todavía "no se ha producido una adopción masiva de la Realidad Virtual en el mercado de consumo", con las oportunidades que esto implica para la red de venta indirecta. "A pesar de no haber una adopción masiva, las ventas se han acelerado en tercer y cuarto trimestre de 2016 e inicios de 2017", gracias a productos como la PlayStation VR de Sony. Además, "las ventas de los accesorios VR han empezado a aparecer en el canal en el tercer y cuarto trimestre 2016 con el lanzamiento de Oculus Touch".

Realidad Virtual, más allá del mercado de consumo

La realidad virtual ya está siendo aplicada en algunas industrias, como la educación y el turismo, pero los pensadores avanzados están encontrando maneras de usarla para hacer las estancias hospitalarias más agradables y tratar ciertos problemas de salud mental, como la ansiedad y la depresión. Las grandes corporaciones están viendo el potencial de ésta, tratando de encontrar aplicaciones para sus propias empresas.

"Podrías pensar que es absurdo sugerir que podría haber aplicaciones de VR para tu pequeña empresa, pero es inevitable", afirma Vishal Sanghvi, directora de estrategias y campañas de marketing de Intel Corporation. A medida que la tecnología se vuelva más asequible y un mayor número de consumidores adquiera los dispositivos de VR, surgirán nuevos usos de la tecnología. "Y las posibilidades para las pequeñas empresas son, quizás, las más interesantes. Imagina a los clientes que caminan a través de tu tienda, viendo tus productos, pudiendo incluso cogerlos o probarlos, todo en un mundo virtual", añade Sanghvi.

"La nueva tecnología está dando a los emprendedores la oportunidad de competir con las grandes empresas como nunca antes. No se puede decir cómo la nueva tecnología, como la realidad virtual, va a cambiar la forma en que vivimos, pero es fácil ver que está obligada a cambiar la forma en que hacemos negocios", concluye Sanghvi.

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- Gaming, un gran negocio para el canal
- Cómo vender productos de gaming
- El mercado de la Realidad Virtual en Europa y España. Context
- Oportunidades que ofrece el mercado de gaming según GfK

Sumario No Solo IT

Legal IT

El ransomware y nuestra privacidad

Por Lorena P. Campillo,

abogada especialista en Derecho de las Nuevas Tecnologías

Management y Canal

La creciente magnitud del negocio IoT para el canal

Por José Luis Montes Usategui,

director de Smart Channel Technologies y director de Channel Academy

En la nube

36 sombras de la computación

Por Kevin L. Jackson,

experto en Cloud y fundador de Cloud Musings

Psicobusiness

Psicología, negocio y resultados inmediatos a través de la evaluación

Por Asier de Artaza,

director de www.yesmanagement.es

Desde mi análisis

El tsunami de la automatización del trabajo

Por Fernando Maldonado,

analista asociado a Delfos Research

Tecnología y Negocio

Contribución de la digitalización al crecimiento económico, al empleo y a la competitividad de la empresa española

Por Jorge Díaz-Cardiel,

Socio director general de Advice Strategic Consultants

Internet de las Cosas

IoT en las empresas

Por Dario Ferraté,

consultor TIC

La creciente magnitud del negocio IoT para el canal

José Luis Montes Usategui
Director de Smart Channel Technologies
Director de Channel Academy

Recuerdo cuando hace un par de años asistí al primer Congreso Mundial de IoT, y la impresión que entonces me causo: pequeño para ser el principal encuentro mundial, pero excelentemente organizado, lleno de contenidos de altísima calidad y de cosas interesantes que ver y gente experta con la que hablar … y con escasa afluencia de visitantes del Canal TI español.

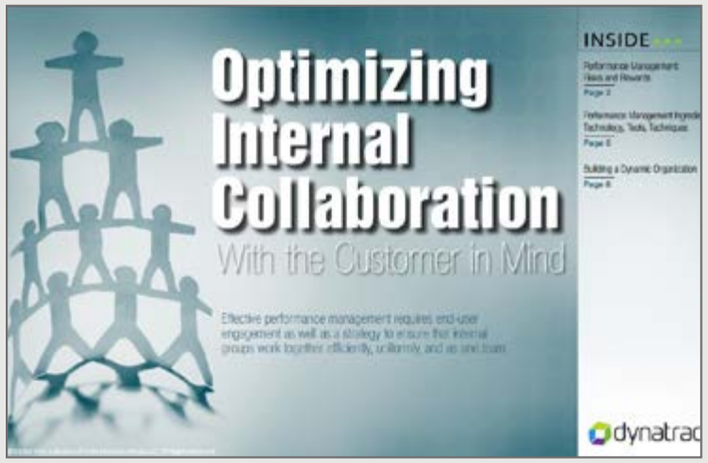
Estamos a pocos meses de la tercera edición, y el Congreso ha crecido al ritmo que la temática en la que se basa: es ahora el doble de grande en espacio, un 30% mayor que el del año pasado, con más de 220 expositores, se espera que lo visiten cerca de 11.000 personas (el doble que un ASLAN o el triple que un Cisco Connect, por poner dos muy exitosos ejemplos cercanos, y respetados por su masiva afluencia), y más de 200 conferenciantes del máximo nivel mundial, entre otras ya impresionantes crecientes cifras que muestran que será una cita planea de potencial.

Pero, ¿seguirá estando poco presente el Canal TI español en esta cita? Es de esperar que no sea así, y de hecho la organización señala

“Experto de referencia en el Sector, con 25 años de experiencia real como directivo y consultor en más de 100 de las empresas más relevantes del mercado en sus diversos segmentos, habiéndose convertido en uno de los mejores conocedores de la distribución TIC actual y de las tendencias del futuro en el desarrollo de sus modelos de negocio”.

Cómo optimizar la colaboración interna

La gestión efectiva del rendimiento requiere afinidad con el usuario final -en este caso, el empleado-, así como una estrategia para garantizar que los grupos internos trabajan juntos de forma eficiente, uniforme y como un único equipo. En este libro se describen algunas pautas para optimizar la colaboración interna gracias a las soluciones de gestión de rendimiento de aplicaciones (APM)



¿Te avisamos del próximo IT Reseller?

que los Integradores de Sistemas, VAR o Service Providers son uno de los targets que buscan activamente, y que ya son un porcentaje de cierto peso entre los perfiles de asistentes. Viendo el perfil de las personas inscritas, lo cierto es que la mayoría son personas de alta dirección de sectores realmente relevantes, un mix de perfiles verdaderamente elevado y de peso, y una parte de ellos provienen del Canal TI internacional, y españoles entre ellos.

Pero por si eres de los que desconocías este evento, o de los que todavía te estás planteando tu asistencia al mismo, voy a aprovechar que el Pisuerga pasa por Valladolid para hablar sobre el estado del negocio IoT en el Canal y, de paso, darte algunas razones (espero que buenas) para que nos veamos en los pasillos de la cita de octubre.

En los inicios, el IoT era visto en nuestro sector TI como algo muy industrial que rozaba colateralmente a nuestro sector, y que por ello presentaba barreras para entrar a hacer negocios y todavía escaso interés. Por supuesto, no se nos ocultaba que eso era una situación transitoria que iría evolucionando hasta tocar de lleno a nuestros modelos de negocio “core”, así que la opinión general que yo recogía era que era pronto para entrar de lleno y que tocaba observar e ir haciendo pequeños experimentos.

Apenas 3 o 4 años después la situación ha evolucionado mucho cualitativa y cuantitativamente, de forma acelerada, y en estos momentos toca de lleno de forma múltiple lo que el sector TI es tal y como lo conocemos. Es hora, pues, de hacer una aproximación más decidida y extensa para aquellos actores del valor añadido que todavía no lo hayan hecho.

Nuestros clientes y nuestras tecnologías están mutando debido al creciente impacto de la IoT

Para empezar, la IoT está transformando casi la totalidad de los segmentos y sectores B2B y B2C: todas las Industrias, las Ciencias de la Salud, el Transporte y la Logística, las Utilities, Agricultura, Retail, por supuesto las Smart Cities, nuestro propio sector Tecnológico, los Servicios Ciudadanos y hasta la Educación. Y la

Al menos la mitad de los actores relevantes no son de nuestro sector ni cercanos, y eso significa que hay un enorme terreno vacío entre ellos y nosotros que debemos de recorrer rápidamente

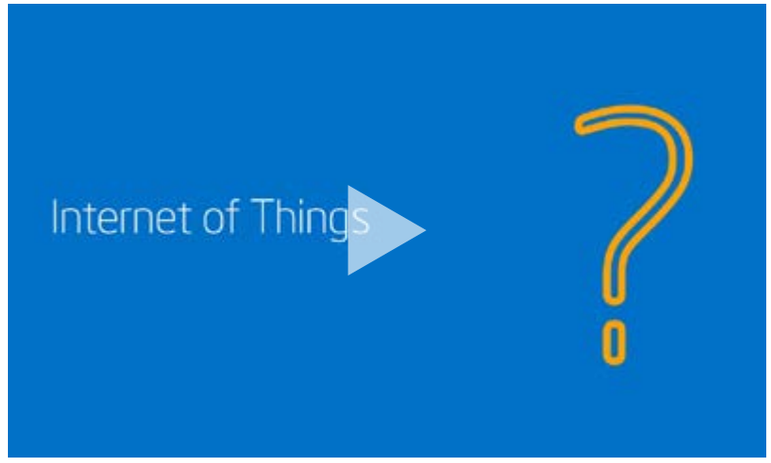
mayor parte de nuestro Canal TI de valor añadido tiene fuertemente sectorializada su forma de abordar el mercado, sea porque poseen soluciones o desarrollos específicos para sectores concretos, o sea porque abordan de forma sectorializada la manera de construir soluciones tecnológicas estándar, y poseen conocimientos y experiencias sectoriales en todo ello, desarrollando discursos verticales de negocio y teniendo a menudo divisiones de profesionales específicas para algunos de estos sectores.

Por tanto, si tan sectorial es la aproximación al negocio del Canal TI de alto valor, está claro que no puede estar ajeno a cualquier penetración tecnológica relevante que ocurra en ese marco, y la IoT transforman de forma radical en muchos casos la forma en que los procesos de digitalización generan competitividad en ellos.

Pero no es solamente una razón de imbricación de nuestro modelo de negocio en los cambios fundamentales que sufren los modelos de negocio de nuestros clientes lo que nos empuja a abrirnos decididamente a la IoT: es que nuestras tecnologías más centrales están también entroncando de forma absoluta con lo que IoT trae y comporta, y eso significa que nuestras propias áreas tecnológicas se transforman y, obviamente, no podemos dejar de navegar remando con fuerza en ese mismo sentido so pena de quedarnos fuera de nuestros propios marcos tecnológicos.

Así, la enorme cantidad de millones de dispositivos IoT que ya están funcionando, y cuya extensión está cogiendo velocidad exponencial, implican transformaciones e impactos fundamentales en áreas tecnológicas clave nuestras como son las comunicaciones (imposible condensar en una línea todo lo que en este campo está cambiando debido a la conexión IoT), la nube (la transforman, entre otras razones, al exigir computación en sus bordes), el Big Data (ya hoy se generan más datos por cosas que por personas, y eso es un cambio total de paradigma), la Ciberseguridad (ya hoy una parte relevante de los ataques se generan, transmiten y/o tienen por objetivo dispositivos y redes IoT), la BI (la transformación competitiva sectorial que la IoT comporta no proviene de su capacidad de generar datos sino de la potencialidad brutal de analizarlos), las redes (las actuales, al menos las tradicionales, directamente no sirven) y hasta los desarrollos de software (que, por ejemplo,

¿QUÉ SIGNIFICA INTERNET DE LAS COSAS?



CLICAR PARA VER EL VÍDEO

> Mi consejo es que traces ya un plan trianual para transformar tu empresa en este campo porque ni va a ser rápido ni va a ser fácil, pero va a ser imprescindible

se hibridan al gestionar nuevas realidades confluentes de naturalezas informáticas e industriales). Podría seguir poniendo ejemplos de áreas tecnológicas centrales de nuestros modelos de negocio que están viendo como algunos de los vectores de crecimiento, innovación y adopción más importantes son hoy ya empujados por la IoT y no por nuestras TI tradicionales.

Así, nuestros clientes y nuestras tecnologías están mutando debido al creciente impacto de la IoT, y eso hace que resulte perentorio meternos de cabeza en nuestra propia transformación en compañías basadas en IoT, te lo digo así de radicalmente para que te desprendas de cualquier tipo de prevención y te muevas rápida y decididamente: no es que la IoT sea un nicho de creciente interés, es que al igual que con la nube no puedes dejar de meter IoT en el corazón de tu modelo de negocio.

Y todo ello con varios retos a abordar, y uno de ellos especialmente relevante y sobre el que quiero poner un poco de foco de atención: el universo IoT está ganando madurez y fuerza, pero es en una gran parte totalmente ajena a nuestro sector TI. Así, al menos la mitad de los actores relevantes no son de nuestro sector ni cercanos, y eso significa que hay un enorme terreno vacío entre ellos y nosotros que debemos de recorrer rápidamente. Ambos. Ellos deben de aproximarse a nosotros (me consta que les interesa mucho), y nosotros a ellos. Si miras la lista de expositores, incluso la de esponsors, del Congreso, verás que hay una gran cantidad de nombres ajenos o directamente desconocidos en el sector TI, junto con los más notables "nuestros" pero también con algunas ausencias sorprendentes.

Nos urge meternos de lleno en ese ecosistema, entenderlo, entablar relaciones, generar conocimiento en nuestras organizaciones, adoptar tecnologías y soluciones y empezar a llevarlas a nuestros clientes, descubrir en ellos quiénes son los contactos relevantes en estas áreas y trazar accesos a los mismos, efectuar cambios en nuestro "offering" y en nuestra forma de abordar el mercado y el negocio. El IoT Congress es una excelente etapa en ello, pero ni de lejos debería de ser la única, y mi consejo es que traces ya un plan trianual para transformar tu empresa en este campo porque ni va a ser rápido ni va a ser fácil, pero va a ser imprescindible. Nos leemos el mes que viene.

Enlaces relacionados

- I [IoT World Congress Barcelona 2015]
- W [Ataques con Exploits, de las amenaza diarias a las campañas dirigidas]
- W [GDPR: soluciones para la gestión de datos personales]
- I [IoT World Congress 2017]
- I [IoT WC Áreas Temáticas]

Psicología, negocio y resultados inmediatos a través de la evaluación

Asier de Artaza
Director de yes

Nacido en Bilbao hace 44 años, es Top Ten Management Spain en Psicobusiness; gestión de conflictos, interacciones y relaciones positivas. Liderazgo y negociación. Presta servicio para alta dirección en Psicobusiness para el desarrollo de directivos y creación de equipos directivos de Alto rendimiento. Además, es especialista sobre marketing estratégico industrial, de centros de innovación y tecnológico, donde negocio y personas son aspectos clave.
Ha formado parte de varios Consejos de Administración y trabajado en 8 compañías, sectores y localizaciones. Es Licenciado en Empresariales y Marketing, en la actualidad Cursa las últimas asignaturas de su segunda carrera, Psicología. Es Máster en Consultoría de Empresas, Máster en Digital Business, Posgrado en Dirección Financiera y Control Económico; Mediador Mercantil y Certificado en Coaching Skills for Managers

Dijo “yo soy un gran jefe”, y le sometimos inmediatamente a un 360º. Esta frase u otras más moderadas, como “todos tenemos nuestras cosas, pero yo sé que mi equipo está totalmente conmigo”; u otras más funcionales, como “en mi departamento todos tienen perfectamente claro lo que tienen que hacer”, son habituales por responsables de muchas empresas. Bueno, e incluso, nos podemos encontrar con algunas más explosivas como, “sé que mis empleados matarían por mí, me quieren mucho”.

En fin, y esto en los profesionales preparados y actualizados que tienen claro que las personas son la clave de los negocios, en los que no, mejor ni hablar. Lo cierto es que muchas veces caemos en el error de que todo lo hacemos bastante bien con nuestro equipo. Y si la actitud, preparación y consideración de las

personas ya es un punto importante a favor, diríamos que es condición necesaria pero no suficiente. Nadie, como responsable de otras personas, puede saber si su actuación es correcta al 100%, porque, de hecho, esta consideración no le pertenece a él, sino a su equipo. La perfección es imposible, así que, sin duda, el contraste de nuestra creencia con la realidad siempre aportará puntos de mejora.

Hablemos entonces para los que no lo conozcan o simplemente tengan una ligera idea, de qué es una evaluación 360º. La evaluación 360º, que surge ante las limitaciones de la práctica adicional de arriba abajo típica de la evaluación, consiste en una serie de cuestionarios contestados por jefes, compañeros, subordinados, e, incluso, clientes, los cuales cubren todos los estamentos o grupos significativos con los que el evaluado tiene relación.

Empresas como la sueca Ensize, ponen en valor todas sus ventajas como el ser una retroalimentación de múltiples fuentes con diferentes perspectivas del evaluado; cómo ayuda a través de la evaluación de abajo arriba, de los miembros del departamento hacia el responsable; o cómo provoca la mejora global del equipo, del individuo y de la organización. Claro que su aportación es tremenda si intervienen clientes, ya que la mejora puede tener efectos inmediatos sobre los resultados.

En fin, muchas ventajas para una mecánica en el fondo sencilla, y que lo tiene claro desde la reflexión de "¿qué mejor que escuchar de los que trabajan conmigo lo que piensan de mi actuación, para que lo contraste con lo que yo creo, y a partir de aquí obtenga puntos de mejora inmediatos, directos y reales?".

Lo que no hay que olvidar es que para que este sistema funcione y dé buenos resultados, debemos contar con mucho rigor y profesionalidad, y trabajarlo con un experto y contar, el experto o la empresa receptora del servicio, con las herramientas de máximo rigor técnico desde el ámbito de la evaluación de personas.

Algunas empresas disponen de simples y potentes soluciones tecnológicas de ésta y otras herramientas como DISC en las que, de forma absolutamente ejecutiva desde su plataforma Cloud, te permiten realizar fácilmente un análisis 360º. Desde una interfaz intuitiva se envían

Analítica de Big Data o cómo tomar decisiones con fundamento

El análisis de los grandes volúmenes de datos que atesoran las empresas les permite ver más allá de la realidad diaria: entender qué ha pasado con sus clientes y por qué y, en base a ello, diseñar nuevas estrategias que les lleven a estar un paso más allá de su competencia. Lee en este Centro de Recursos IT User más sobre el cambio que aporta el análisis de Big Data a tu organización.

análisis de múltiples preguntas a todos los participantes, produciendo, en base a la información generada, completos informes personalizables, de gran rigor, alcance y fácil interpretación visual y lectura. Todo en cuestión de unos minutos, sin contar obviamente el tiempo de contestación de las preguntas.

Esta evaluación completada por múltiples personas se compara con la evaluación realizada por el propio evaluado, y así se obtienen puntos de mejora entre lo que el evaluado considera y la imagen real que los demás tienen de él, de su gestión.

El resultado es una información muy rica, cuantitativa y cualitativa que facilita la reflexión y posterior introducción de cambios, según las divergencias obtenidas.

Los bloques temáticos a analizar, a veces relacionados con cómo actúa el evaluado (responsable del equipo generalmente) y otras con cómo gestiona a su equipo, suelen girar en torno a la profesionalidad en la gestión de los objetivos del departamento; la eficacia de la comunicación, la implicación y motivación con su equipo, la capacidad para actuar desde aproximaciones nuevas o delegar en el equipo, la práctica en la entrega y recepción de feedback, la resolución de problemas consideraciones sobre integridad y confianza...

La evaluación 360º es una herramienta que produce resultados inmediatos tanto en las personas como en la gestión del negocio

Un aspecto importante es el criterio de elección de los evaluadores, sobre los que hay que decidir desde qué categorías se conformarán (jefes, compañeros, pares, clientes…), qué número de ellos participará, y quiénes concretamente serán los que participen. Las dos primeras cuestiones las decide la dirección junto con el experto que le esté asesorando, dadas unas características concretas del programa. La tercera la elige el propio evaluado. También hay que pensar que es bueno si evalúan personas de confianza de éste, ya que estarán implicados queriendo ayudar, y, aparte, suelen ser más duras evitando el efecto indulgencia, a lo cual también ayuda la especificidad de las preguntas

Un aspecto siempre crítico es la reacción de los evaluados a esta experiencia, ya que afectará a su aceptación o rechazo de los resultados y a su posterior desempeño. Hay que tener especial precaución con que personas con alta autoestima tienden a rechazar los resultados y rebatirlos, encontrando justificaciones de todo tipo. Y viceversa con personas de baja autoestima.

Elementos favorecedores contextuales para el buen resultado de la prueba son la presencia en el evaluado de un sentimiento de autoeficacia individual (la creencia de una persona en su capacidad de tener éxito en una situación particular) y la existencia en la organización de un clima organizacional positivo. También debemos tener en cuenta, especialmente en resultados negativos, tratar de dar los resultados en una situación donde esté presente un espíritu de confianza y seguridad para los empleados. Por ejemplo, en evaluaciones de varias personas, es muy procedente la entrega de los resultados en privado. Y complementar aquella con la puesta en común en grupo de elementos, ideas y las conclusiones generales, de esta manera los evaluados aprecian la normalidad de sus divergencias con los evaluadores, lo que facilita la aprobación de los resultados y su consideración constructiva.

En cualquier caso, antes de poner en marcha un sistema de evaluación 360º debemos

reparar en algunas variables que marcarán su éxito o fracaso, como son: la confianza de los empleados en la empresa, la implicación de la Dirección en toda la experiencia, si el momento en el que se encuentra la compañía es estable, la existencia o generación de una cultura de errores (el error es apreciado como una oportunidad de mejora, no como un hecho negativo) y de un clima de apoyo que traduzca la evaluación en una oportunidad de mejora y no en una amenaza, y la fijación de mejoras a largo plazo que produzcan un cambio integral y sólido.

Y, para terminar, vamos a mencionar cinco recomendaciones prácticas desarrolladas por Lévy-Leboyer. En primer lugar, menciona que se debe clarificar con anterioridad los objetivos, el procedimiento y qué va a suponer para los empleados. Continúa con que, en el caso que haya varios evaluadores del mismo grupo, se promedien las puntuaciones, además de que debe de haber más de cuatro evaluadores para conseguir el anonimato de estos. Como tercera recomendación, menciona que el informe debe contemplar los puntos fuertes y débiles del evaluado, así como un plan de desarrollo sobre sus áreas de mejora. Otra aportación de Lévy-Leboyer es que los resultados obtenidos solo se entreguen al evaluado, que, además de ser el afectado, es el único que puede interpretarlos adecuadamente, desde su conocimiento y participación. Como quinto, y retante, punto señala

> Antes de poner en marcha un sistema de evaluación 360º debemos reparar en algunas variables que marcarán su éxito o fracaso

lo interesante de establecer perfiles colectivos de las competencias de un servicio, función o departamento cara al desarrollo de sistemas de compensaciones, programas de formación...

Sin duda, la evaluación 360º es una herramienta de práctica obligada en todas las organizaciones que la contemplen desde las consideraciones mencionadas. Como hemos comentado su práctica produce obviamente resultados inmediatos tanto en las personas que producen los resultados, como en la gestión del negocio; o, dicho de otra manera, desde el Psicobusiness.

Enlaces relacionados

- I Herramientas de evaluación y licencias
- I Servicios de desarrollo directivo y equipos de alto rendimiento
- I Harvard Business Review, how to get 360º reviews right
- I Lévy-Leboyer y la evaluación 360º
- W Tres elementos esenciales de TI para la pequeña y mediana empresa
- W Cómo aprovechar los datos para adquirir y retener clientes
- W Internet de las Cosas hoy y mañana

Contribución de la digitalización al crecimiento económico, el empleo y la competitividad de la empresa española

Jorge Díaz-Cardiel
Socio director general de Advice Strategic Consultants

Economista, sociólogo, abogado, historiador, filósofo y periodista. Ha sido director general de Ipsos Public Affairs, socio director general de Brodeur Worldwide y de Porter Novelli Int.; director de ventas y marketing de Intel y director de relaciones con Inversores de Shandwick Consultants. Autor de más de 5.000 artículos de economía y relaciones internacionales, ha publicado más de media docena de libros, como Innovación y éxito empresarial Hillary Clinton versus Trump: el duelo del siglo; La victoria de América; o Éxito con o sin crisis, entre otros. Es Premio Economía 1991 por las Cámaras de Comercio de España.

Mucho se habla de Digitalización y el uso intensivo de las TIC. Estados Unidos incorporó ambos a su PIB -único país del mundo en hacerlo- en agosto de 2013, revisando la serie histórica de su crecimiento económico desde 1933, en plena Gran Depresión, momento en que se produce la generación del mayor número de patentes tecnológicas de la historia: es un período en la intrahistoria de Norteamérica que se sitúa entre el final de la Segunda Revolución Industrial y los inicios de la Tercera. No olvidemos, a modo de ejemplo, que Hewlett-Packard fue creada en un garaje de Palo Alto en 1939, cuando aún duraba la Gran Depresión (no acabó hasta 1946).

Nosotros no tenemos las TIC como un componente del PIB. Pero la Digitalización, para España, busca mejorar la competitividad de nuestro tejido productivo y fomentar su crecimiento, la expansión internacional y la creación de empleo de calidad, mediante un mejor aprovechamiento de las TIC y el desarrollo de la

economía digital. Cualquiera otra cosa es verborrea barata.

La utilización eficiente e intensiva de las TIC en las empresas es un factor imprescindible para mejorar la productividad de nuestra economía. El comercio electrónico es otro de los indicadores que señalan el nivel de desarrollo tecnológico de una sociedad: aumentó el 20,1% en 2016. Para su impulso, la Digitalización necesita el desarrollo de un Plan de TIC para la PYME y los autónomos y comercio electrónico con medidas integrales en colaboración con los agentes económicos y sociales y otros niveles de la Administración.

La industria de los contenidos digitales presenta un enorme potencial de crecimiento que la sitúa como uno de los sectores más relevantes para la economía digital y de aplicación transversal al resto de sectores de la economía. Para fomentar el desarrollo de esta industria es menester que el proceso de Digitalización de nuestra economía establezca el desarrollo de un Plan integral para la industria de contenidos digitales.

La internacionalización de las empresas TIC se sitúa como uno de los elementos principales para el crecimiento económico y la generación de empleo. Como escribió el presidente Bill Clinton en “Back to work”: “un empleo de manufactura TIC genera 16 puestos de trabajo en otros ámbitos empresariales. Las TIC son, por tanto, un job multiplier”. Es por ello que la Digitalización ofrece las herramientas adecuadas para establecer un Plan de internacionalización

La Digitalización española exige un Plan de Servicios Públicos Digitales en los ámbitos de salud y el bienestar social, Administración de justicia y educación, que se sitúe como una palanca fundamental para el fortalecimiento de la Industria TIC que da soporte a la economía digital

de empresas tecnológicas capaces de generar empleos en otros sectores de actividad.

La industria electrónica en España se enfrenta a un proceso complejo de adaptación. Para mejorar su competitividad, la Digitalización supone aumentar la colaboración público-privada e identificar y potenciar las oportunidades que se presentan en este nuevo escenario.

El desarrollo de las industrias de futuro es imprescindible para continuar con la modernización y el crecimiento sostenible de la economía española. Para ello, la Digitalización tiene líneas de actuación para potenciar el desarrollo y uso del cloud computing, las Smart cities, la Con-

vergencia, la Inteligencia Artificial, el Big Data, la Robótica, entre otros ámbitos y tecnologías de futuro.

Además, la Digitalización española exige un Plan de Servicios Públicos Digitales en los ámbitos de salud y el bienestar social, Administración de justicia y educación, que se sitúe como una palanca fundamental para el fortalecimiento de la Industria TIC que da soporte a la economía digital. El presidente Barack Obama dedicó -en febrero de 2009- el 10% de su "Paquete de Estímulo para Reactivar la Economía" (Economic Recovery Act; 787 billones de dólares, a los que más tarde añadió otros 400 billones en septiembre de 2011 en TIC, para estimular la economía americana) a la digitalización de las Administraciones Públicas Federales, consciente del "efecto tractor" que tienen del sector privado.

Incentivar el uso transformador de las TIC en nuestras empresas

La utilización eficiente e intensiva de las TIC en las empresas, especialmente en las pyme y microempresas, es un factor imprescindible para mejorar la productividad de nuestra economía. En ese contexto, ¿qué supone la Digitalización? Impulsar el acceso de banda ancha ultrarrápida en la pyme; abordar el fomento del uso intensivo de las TIC en las empresas desde un enfoque integral; apoyar el desarrollo de soluciones TIC adaptadas a sectores insuficientemente atendidos; y promover el uso de la factura electrónica, por su "efecto arrastre".

El Estudio Advice de Éxito Empresarial mide la aportación a la economía de las TIC, sus aplicaciones y la implantación en las empresas. Según dicho estudio, realizado semestralmente desde 2006 hasta la primavera de 2017, "la Digitalización de nuestras empresas -3,2 millones según el Dirce-INE; 99,88% de ellas son PYMES y autónomos- añadiría un punto porcentual (1pp o 1%) anual al Producto Interior Bruto de España. Esto, desde el punto de vista macroeconómico, llevaría consigo un cambio esencial del modelo productivo español, menos dependiente del Sector Servicios, Turismo y Construcción, para aumentar el peso de la Industria hasta el 20% del PIB, al tiempo que se desarrolla la llamada Economía del Conocimiento de la mano de la Cuarta Revolución Industrial. En este supuesto, las repercusiones en el empleo español -tipo, calidad, cualificación, temporalidad…- serían muy fuertes: primero, se doblaría la creación de empleo anual, pasando del medio millón de nuevos trabajadores en 2015 y 2016, respectivamente, a la generación de un millón de em-

El World Economic Forum desearía que, en países avanzados como España, se procediera al grado máximo del desarrollo de la economía digital mediante la creación de clusters o ecosistemas sostenidos por sí mismos

Encuesta Mundial sobre el Coeficiente Digital de las Empresas

El nivel de digitalización de las empresas españolas se sitúa en línea con el de los principales países desarrollados, según recoge la Décima Encuesta Mundial sobre el Coeficiente Digital de las Empresas, elaborada por PwC, la cual señala que las compañías están apostando por desarrollo de nuevas tecnologías disruptivas como el Internet de la Cosas, la Inteligencia Artificial y la robotización para mejorar la eficiencia y la productividad.

pleos anuales, a los que estaría asociado una mayor cualificación y formación profesional, mejores salarios, trabajos de calidad y mayor longitud de los contratos". Las tesis empíricas del Estudio Advice de Éxito Empresarial están avaladas por los informes anuales del World Economic Forum que, en enero de 2017, coincidieron en el análisis y en el diagnóstico.

El World Economic Forum, además, desearía que, en países avanzados como España, se procediera al grado máximo del desarrollo de la economía digital mediante la creación de clusters o ecosistemas sostenidos por sí mismos, siguiendo el ejemplo de Silicon Valley en California, el sector de seguros en Boston, el financiero en Wall Street de Nueva York, la energía en Texas y el ocio y el entretenimiento en Los Ángeles (todos, ejemplos americanos, como puede verse). Nosotros hemos defendido sistemáticamente esta tesis desde 2012, dejándolo "for the record" en innumerables intervenciones en prensa, radio, televisión e Internet y en cuatro extensas obras publicadas: Éxito con o sin crisis (LID, 2012), Recuperación económica y grandes empresas (Eunsa, 2015), Innovación y Éxito Empresarial (Eunsa, 2016) y Empresas y empresarios más exitosos (Estudios Políticos y Económicos Internacionales, 2017).

Tanto el Estudio Advice de éxito empresarial como el World Economic Forum, en sus estudios conjuntos, desearían que dichos clusters o ecosistemas empresariales independientes se extendieran entre todas las empresas y sectores de España, informando, por tanto, la actividad de la PYME y los autónomos. Ya existen algunos ejemplos en País Vasco, Madrid, Cataluña y Valencia.

Sin embargo, hoy, estos microcosmos empresariales, en España, se han creado en torno a grandes empresas que son vanguardistas y pioneras en sus sectores de actividad: es el caso de Telefónica, hoy ya Telco Digital que ofrece todo el catálogo de servicios digitales para empresa y sector público (Internet de las Cosas, Convergencia y Contenidos, Cloud Computing, Robótica, Inteligencia Artificial y, muy especialmente, Análisis de los Datos basado en Big Data, entre otras soluciones) y que aporta, ella sola un 1% al PIB cada década, máxime con el tendido y desarrollo de la fibra óptica hasta el hogar, llegando ya a 20 millones de unidades inmobiliarias con una cuota de mercado del 42%. Vodafone, anglosajona, está siguiendo el mismo camino y dando pasos en la correcta dirección.

CaixaBank es el primer banco digital del mundo y primer banco de España por cuota de mer-

cado (28%). Es motivo de orgullo para muchos que un banco catalán, español, sea líder mundial, por ejemplo, en banca móvil digital. Y no hay que olvidar que, junto a la modernidad se une la historia: CaixaBank proviene de La Caixa de quien, ya en los tiempos de la Segunda República Española, se decía que "España no se entiende sin La Caixa", aunque, entonces, se llamara de otra manera.

De la misma forma en que César Alierta, José María Álvarez-Pallete, Chema Alonso en Telefónica, han impulsado la Telco Digital, en La Caixa-CaixaBank, han sido Isidre Fainé (también presidente de Gas Natural Fenosa y de la Fundación Bancaria La Caixa), Jaume Giró, Gonzalo Gortázar… quienes han modernizado La Caixa-CaixaBank, recibiendo desde 2009

premios todos los años, como banco más innovador del mundo en TIC y Digitalización, de Forrester, Gartner, IDC, The Banker, Euromoney y Advice Strategic Consultants.

El Corte Inglés acaba de anunciar que vende gafas a medida mediante la impresión 3D. Para muestra, baste un botón, dice el refrán. La realidad es que El Corte Inglés se ha convertido en el líder del comercio electrónico en España, batiendo por igual a Amazon.es y a Mercadona, por poner dos ejemplos. Su joven presidente, Dimas Gimeno, ha tenido como objetivo la Transformación Digital de El Corte Inglés desde el mismo día en que tomó posesión, en septiembre de 2014. Y lo está consiguiendo con éxito según CommScore, IDC, Gartner y Advice.

Mucho se habla de Smart Cities y de la televisión y los contenidos asociados a las empresas operadoras de telecomunicaciones. Nada de esto sería posible sin empresas como Cellnex Telecom, empresa catalana y líder europeo en gestión de infraestructuras de telecomunicaciones. Y lo mismo se aplica al líder mundial de gestión de infraestructuras, Abertis, quien gestiona con tecnologías inteligentes el mayor número de autopistas del mundo. Gas Natural Fenosa -como Hewlett-Packard en el mundo de la computación moderna- tiene de todo: CRM, ERP, BI, SCM, IA y toda la sopa de letras de la Digitalización para poder, no solo ser eficiente en sus procesos, sino poder proveer energías limpias y ser líder mundial en el Índice de Sostenibilidad del Dow Jones.

Y, para terminar: solo el 0,12% de nuestras empresas son grandes. No llegan a 4.000. Pero de La Caixa-CaixaBank, Telefónica, El Corte Inglés, Abertis, Gas Natural Fenosa, Cellnex Telecom…, dependen cientos de miles de pymes y autónomos. Empresas tecnológicas como HP Inc y HPE y, especialmente, Sage, cuidan de las PYMES y los autónomos para que se suban al tren de la Digitalización.

Enlaces relacionados

- [Internet de las Cosas: hoy y mañana]
- [15 ideas para la Transformación Digital de tu negocio]
- [X encuesta mundial sobre el coeficiente digital de las empresas]
- [Estudio ADVICE de Éxito Empresarial]
- [World Economic Forum]

El ransomware y nuestra privacidad

"Cuando veas las barbas del vecino cortar pon las tuyas a remojar"

Refrán popular

En la era tecnológica en la que vivimos, en la mayoría de casos, toda nuestra vida está en los dispositivos inteligentes (tablets, pc, portátiles, smartphones…), que pueden ser víctimas de "secuestros digitales". Y con ello, nuestra protección de datos se vería seriamente afectada. Por tanto, no queda más opción que conocer las amenazas y contar con las salvaguardas adecuadas.

Lorena P. Campillo
Abogada especialista las Nuevas Tecnologías en Derecho de las Nuevas Tecnologías

En este post veremos qué es un "ransomware" y cómo actuar, según la Agencia Española de Protección de Datos.

¿Qué es un ransomware?

Un ataque ransomware es un secuestro de información por una organización criminal que consigue ejecutar un programa dañino en un equipo. La manera más fácil de infectar es a través de una página web, un correo electrónico o descargando ficheros.

A continuación, el programa atacante cifra los ficheros de los datos del ordenador atacado, de manera que no sean accesibles hasta que se descifren. El rescate permitiría descifrarlos y recuperarlos, de lo contrario quedarían inservibles o eliminados definitivamente. La organización criminal, para no ser identificada, solicita

Lorena P. Campillo es licenciada en Derecho por la Universidad Carlos III y abogada ejerciente especialista en Derecho de las Nuevas Tecnologías. Máster en Abogacía Digital y de las NNTT por la Universidad de Salamanca. Miembro de Enatic (Asociación abogados expertos en NNTT). Miembro de Club de emprendedores UC3M y jurado de los premios sello de excelencia. Socióloga especialista en cambios sociales de la era Digital. Colaboradora en despachos internacionales.

una transferencia en Bitcoins (monedas virtuales). No suelen ser cantidades excesivamente altas puesto que los ataques son masivos.

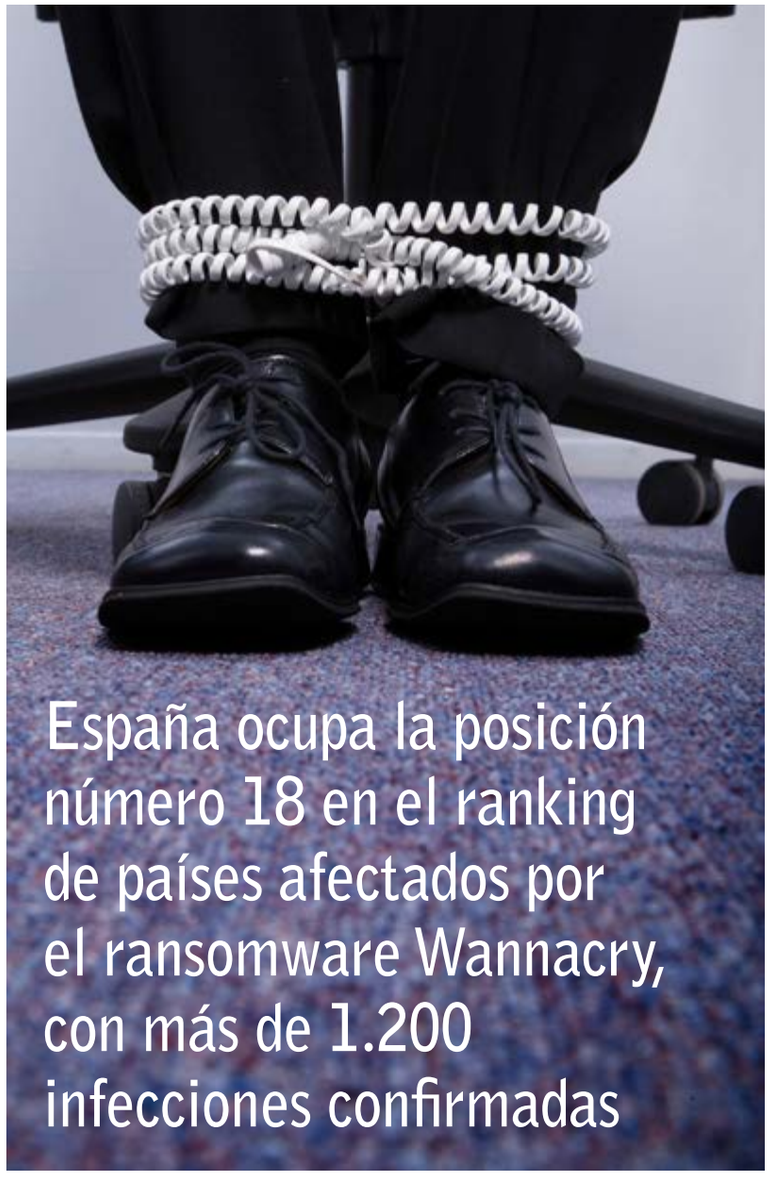
En el ataque del pasado 12 de mayo, el programa se distribuyó dentro de un fichero adjunto y además aprovechaba la vulnerabilidad del resto de los dispositivos conectados en red local. Este ataque afectó a más 360.000 equipos, ha tenido impacto en 180 países diferentes. España ocupa la posición número 18 en el ranking de países afectados por el ransomware Wannacry, con más de 1.200 infecciones confirmadas.

¿Por qué ocurre?

Aunque los sistemas operativos, navegadores y antivirus son cada vez más sofisticados, en la propia sofisticación hay "agujeros" de seguridad aprovechados por los atacantes. La producción y aplicación de "vacunas" no suele ser instantánea y no siempre éstas son compatibles con los programas dañinos.

¿Cómo se puede solucionar?

No existe una protección absoluta, ya que siempre va a existir un grado de exposición. El riesgo habrá que gestionarlo, y la AEPD aconseja lo siguiente:

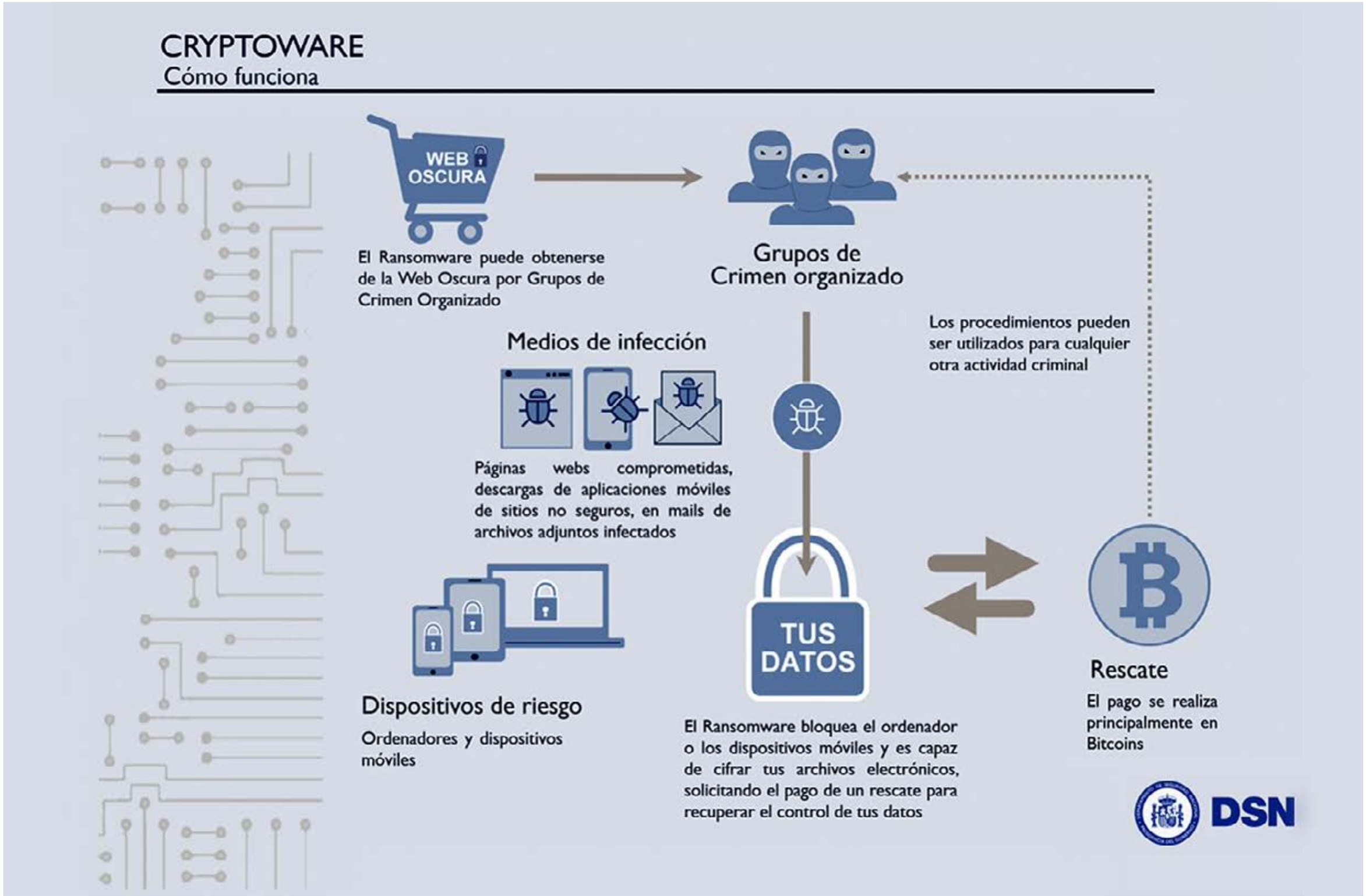


- 1º. Tener un buen diseño de seguridad de las redes y concienciación ("SECURITY BY DESIGN" o seguridad desde el diseño) de los usuarios. Por ejemplo, tener al día los contratos de mantenimiento del software con proveedores.
- 2º. Contar un plan de actuación ante un ataque. Es lo más complejo para las organizaciones.
- 3º. A posteriori, realizar un análisis de daños y efectuar las reparaciones posibles. En España, por ejemplo, podemos contar con la ayuda del INCIBE, que ofrece diversos servicios gratuitos. También, otra solución a tener en cuenta siempre es la recuperación de una copia de seguridad de los datos una vez que el agujero de seguridad se ha cerrado.

En definitiva, es necesario concienciar y el cumplimiento normativo por parte de los responsables de seguridad. La AEPD pone a disposición del usuario varias guías acerca de la seguridad y privacidad en Internet.

REUNIÓN DEL CONSEJO NACIONAL DE CIBERSEGURIDAD 17/5/2017

CLICAR PARA VER EL VÍDEO


CRYPTOWARE
Cómo funciona
WEB OSCURA
El Ransomware puede obtenerse de la Web Oscura por Grupos de Crimen Organizado
Grupos de Crimen organizado
Los procedimientos pueden ser utilizados para cualquier otra actividad criminal
Medios de infección
Páginas webs comprometidas, descargas de aplicaciones móviles de sitios no seguros, en mails de archivos adjuntos infectados
Dispositivos de riesgo
Ordenadores y dispositivos móviles
TUS DATOS
El Ransomware bloquea el ordenador o los dispositivos móviles y es capaz de cifrar tus archivos electrónicos, solicitando el pago de un rescate para recuperar el control de tus datos
Rescate
El pago se realiza principalmente en Bitcoins
DSN

¿Podría tu empresa sobrevivir a un cryptor?

Aprende a protegerte del ransomware de cifrado

Los últimos ataques de ransomware han afectado a numerosos equipos de todo el mundo. Conoce en este documento qué es un cryptor, el software malicioso que cifra tu información y pide un rescate por ella, y cómo puedes proteger tu empresa.

Un ataque ransomware es un secuestro de información por una organización criminal que consigue ejecutar un programa dañino en un equipo. La manera más fácil de infectar es a través de una página web, un correo electrónico o descargando ficheros

La colaboración público-privada es esencial en estos casos (CERT del Centro Criptológico Nacional, CERT de Seguridad e Industria operado por INCIBE, el Centro Nacional para la Protección de Infraestructuras Críticas, CNPIC, el Departamento de Seguridad Nacional…)

¿Qué tiene que ver la ciberseguridad de las organizaciones con la privacidad?

Hemos hablado de secuestros digitales, pero ahora extendamos el problema a un ámbito más general: la fuga de información. Las consecuencias de la fuga de información derivan casi siempre en daños reputacionales y san-

ciones penales, civiles, administrativas o deontológicas…

Lo determinante en estos casos es definir el tipo de datos que se han podido ver afectados.

El nuevo reglamento europeo de protección de datos contempla una serie de obligaciones para el responsable del tratamiento (Art. 33 y 34) acerca de notificar dicha violación a la autoridad de control (AEPD).

Esta comunicación es importante al objeto de que las personas afectadas por la fuga de sus datos estén informadas del incidente y de los datos que han sido sustraídos, a fin de que puedan tomar las acciones oportunas para su seguridad, tales como el cambio de contraseñas, la revocación de números de tarjetas, ser especialmente cautelosos con eventuales accesos a sus cuentas de correo... Además, se debe proporcionar algún canal para que los afectados puedan mantenerse informados sobre la evolución del incidente y las distintas recomendaciones que pueda realizar la organización a los afectados, con el objetivo de minimizar las consecuencias. La fuga de la información al fin y al cabo es la pérdida de la confidencialidad de los datos de los ficheros de las organizaciones.

Enlaces relacionados

- W Guía de privacidad y seguridad en Internet
- W Informe del ransomware WannaCry con vacuna y medidas para su detección y desinfección
- I Los ataques 'ransomware' y cómo protegerse
- I Protección ante la oleada de ransomware
- I Herramientas anti-ransomware
- I Herramientas ante-botnet
- I Evolución del impacto de WannaCrypt en España
- W Código de Derecho de la Ciberseguridad
- W Directiva "NIS" (Seguridad de las redes y sistemas de información de la Unión)
- W Ataques con Exploits, de las amenaza diarias a las campañas dirigidas
- W GDPR: soluciones para la gestión de datos personales

TU CANAL DE VÍDEOS IT

INFORMATIVO IT

DIÁLOGOS IT

IT WEBINARS

CASO DE ÉXITO IT

MESA REDONDA IT

TU PRODUCTORA DE CONTENIDOS AUDIOVISUALES

WEBINARS

ENTREVISTAS

EVENTOS

VÍDEOS

INFORMATIVOS

www.ittelevision.es

El tsunami de la automatización del trabajo

Fernando Maldonado
Analista asociado a Delfos Research

Todo parece indicar que una nueva ola de automatización del trabajo va a tener como consecuencia una destrucción neta de empleo. Al menos es lo que se desprende de los últimos estudios publicados al respecto. Pero, de momento, sus efectos todavía no se están notando: ya debería estar dejando un rastro en unos incrementos de productividad que no terminan de llegar.

Los escenarios futuros son variados, aunque hay una corriente de futurólogos que vislumbran un futuro sin trabajo. De hecho, reputadas voces como la de Bill Gates o el Nobel de economía Robert J. Schiller ya se han posicionado a favor de la tesis del comité para asuntos legales del Parlamento Europeo que recomienda que "los robots" paguen impuestos para compensar el coste económico y social de la pérdida de empleo.

Algo difícil de aplicar dada la extensa tipología de robots. Basta asomarse a la ISO stan-

Ayuda a conectar la oferta y la demanda de tecnología asesorando a la oferta en su llegada al mercado y a la demanda a extraer valor de la tecnología. Anteriormente, Fernando trabajó durante más de 10 años como analista en IDC Research donde fue Director de análisis y consultoría en España.

Internet de las Cosas: hoy y mañana

Este informe de HPE revela que el 85% de las empresas planean implementar IoT para 2019, impulsadas por la necesidad de innovación y eficiencia empresarial. La investigación encuestó a 3.100 responsables de TI y de negocios de 20 países para evaluar el estado actual de IoT y su impacto en diferentes industrias. Los cinco grandes sectores que ya están obteniendo los máximos beneficios de IoT son el empresarial, industria, sanidad, retail y la Administración Pública.

El impulso más inmediato al cambio proviene de la robotización automática de procesos que centra su propuesta de valor en la ejecución de tareas rutinarias a partir de reglas predefinidas

dard 8373 para hacerse una idea. En cualquier caso, se trata de una llamada de atención sobre los cambios que se avecinan en el mercado laboral.

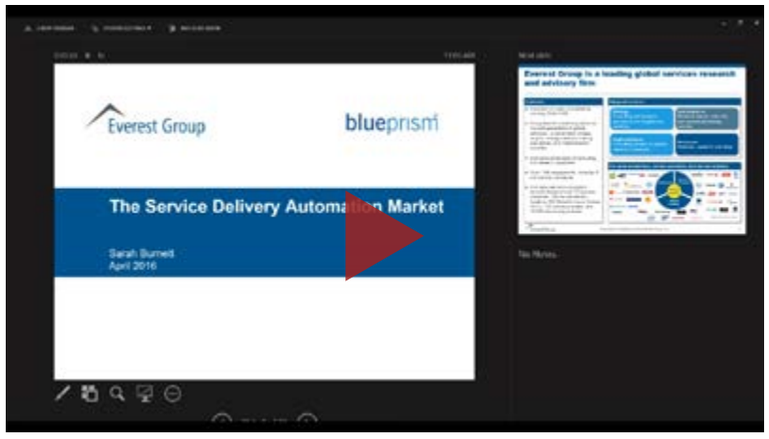
El impulso más inmediato al cambio proviene de la robotización automática de procesos – RPA, en sus siglas en inglés- que centra su propuesta de valor en la ejecución de tareas rutinarias a partir de reglas predefinidas. Y que promete liberarnos de tareas de oficina tediosas. En consecuencia, aquel puesto de trabajo que consista en este tipo de tareas está amenazado.

ROBOTIC PROCESS AUTOMATION

CLICAR PARA VER EL VÍDEO

Por otro lado, la inteligencia artificial y los sistemas cognitivos entran con una proposición de valor más elevada. Por ejemplo, los asistentes personales, dotados de inteligencia artificial, están siendo diseñados para hacer a sus usuarios más productivos. Además, algunas tareas podrán ser “disparadas” y supervisadas por algoritmos que se convertirán en nuestros nuevos “jefes”. Es decir, ni empleado ni “jefe” está a salvo de una mayor automatización de parte de su trabajo. Así, McKinsey calcula que un 45% de las tareas que actualmente realizan los

GANAR PRODUCTIVIDAD CON RPA



CLICAR PARA VER EL VÍDEO

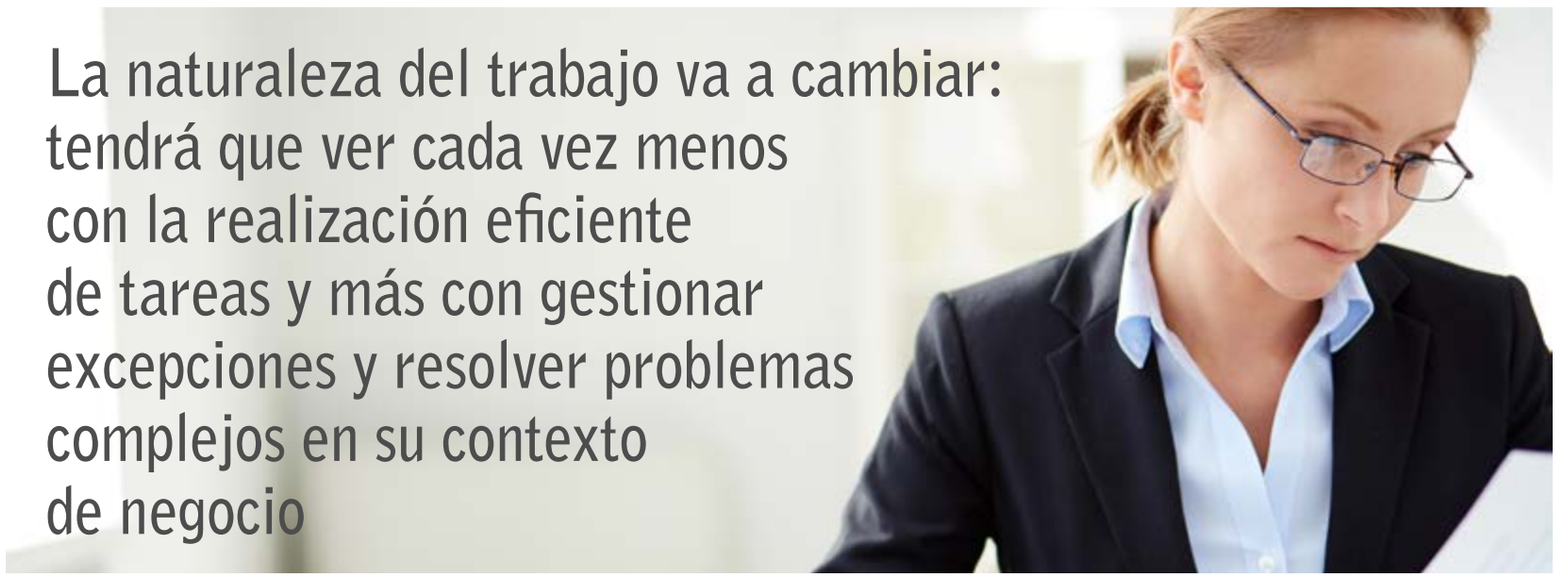
CEO son susceptibles de una mayor automatización.

La automatización de momento se centra en tareas concretas, estamos lejos de desarrollar una inteligencia artificial general que nos sustituya por completo. Por tanto, el escenario que plantea es híbrido: humano y máquina se complementan. Desde esta perspectiva se pueden plantear opciones interesantes, como, por ejemplo, que se haga realidad la reducción de la jornada laboral de 40 horas semanales.

La decisión de cómo y cuándo lanzarse a la automatización por parte de cada empresa requiere un análisis de dónde tiene sentido aplicarla. Por ejemplo, habrá que tener en cuenta que toda esta inteligencia todavía no es infalible y también se equivoca, por lo que habrá que contraponer su probabilidad de acierto con los costes de fallo. Por eso mientras que para recomendarnos nuestra próxima compra cobran plena autonomía, en los diagnósticos médicos todavía requieren del juicio de las personas.

Lo que está claro es que la naturaleza del trabajo va a cambiar: tendrá que ver cada vez menos con la realización eficiente de tareas y más con gestionar excepciones y resolver problemas complejos en su contexto de negocio.

Mientras existan estos problemas tendremos trabajo. Eso sí, asistidos cada vez más por la inteligencia artificial y los sistemas cognitivos.



¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- Recomendación del comité de asuntos legales
- Opinión de Schiller sobre impuestos y robots
- Estándar ISO sobre robótica
- Ataques con Exploits, de las amenaza diarias a las campañas dirigidas
- GDPR: soluciones para la gestión de datos personales

36 sombras de la computación

Todo el mundo ha oído hablar de 50 Sombras de Grey. ¿Conocemos también las “36 Sombras de la Computación”? No son más que una nueva forma de describir las 36 soluciones específicas propias de entornos TI híbridos. Cualquier empresa que se plantee transformar la manera de aprovechar al máximo las tecnologías de la información, debería evaluar sus opciones mediante un análisis del proceso de transición que conecta tres dominios concretos de alto nivel y sus sub-dominios más relevantes:

- **Modelo de implantación IT**
  - Tradicional
  - Proveedor de Servicios Gestionados
  - Proveedor de Servicios Cloud
- **Modelo de Servicios de Tecnología**
  - Infrastructure-as-a-Service
  - Platform-as-a-Service
  - Software-as-a-Service

Kevin L. Jackson
Experto en Cloud y fundador de Cloud Musings

Kevin L. Jackson es experto en cloud, Líder de Opinión “PowerMore” en Dell, y fundador y columnista de Cloud Musings. Ha sido reconocido por Onalytica (una de las 100 personas y marcas más influyentes en ciberseguridad), por el Huffington Post (uno de los 100 mayores expertos en Cloud Computing en Twitter), por CRN (uno de los mejores autores de blogs para integradores de sistemas), y por BMC Software (autor de uno de los cinco blogs sobre cloud de obligada lectura). Forma parte del equipo responsable de nuevas aplicaciones de misión para el entorno de cloud de la Comunidad de Servicios de Inteligencia de los EEUU (IC ITE), y del Instituto Nacional de Ciberseguridad.

El nivel de control global sobre seguridad de datos y opciones de tecnología viene directamente determinado por nuestras preferencias en el modelo de despliegue

Modelo de Despliegue

- Privado
- Híbrido
- Community
- Público

Todas las combinaciones posibles de lo anterior -3 Modelos de TI x 3 Modelos de Servicio x 4 Modelos de Despliegue- dan como resultado las “36 Sombras de la Computación”. Estos dominios y sub-dominios delinean un proceso estructurado de toma de decisiones cuyo objetivo es asignar la carga de trabajo más adecuada para cada entorno IT, y donde es importante comprender que las decisiones no son estáticas. A medida que los objetivos de negocio, las opciones en tecnología y los modelos económicos van cambiando, también puede cambiar el valor relativo de cada una de las combinaciones anteriores para nuestros intereses como organización. Otra cuestión esencial en este sentido es la muy escasa probabilidad de que alguna de las soluciones específicas mencionadas pueda por sí sola cubrir todas las necesidades de nuestra empresa; es de esperar que sea necesaria una combinación de dos, tres, o hasta 10 de ellas. Ésta es la razón por la que la TI Híbrida y la intermediación en servicios cloud son habilidades tan importantes en el repertorio de cualquier equipo moderno de sistemas.

La implantación de sistemas da respuesta -a alto nivel- a las tres opciones de estrategia de implantación más frecuentes entre aquellas empresas que se marcan como objetivo la transformación digital:

- Mantener la estrategia actual, en la que se utiliza un centro de datos corporativo convencional para satisfacer las necesidades de la actividad de negocio
- Seleccionar y contratar a un proveedor de servicios gestionados (MSP) en un proceso de compra tradicional mediante RFP/concurso, o
- Cubrir necesidades mediante ofertas comerciales estándar de uno o más proveedores de servicios cloud (CSP).

Las claves principales para la selección de un modelo de implantación son el establecimien-

Plan Digital 2020: La digitalización de la Sociedad Española

La CEOE propone en este informe una serie de líneas para el diseño de estrategias y medidas enfocadas a adaptar la digitalización a sectores específicos, desde la educación, la innovación, el emprendimiento y las administraciones, hasta la industria, los servicios, las infraestructuras o las pymes. Las 215 propuestas que contempla el Plan tienen como objetivo sumar a España al conjunto de países europeos que lidera la digitalización.

to de procesos corporativos de gobernanza de sistemas (opciones primera y segunda de las anteriores), o la aceptación de procesos de gobernanza de sistemas mediante CSP (tercera de las anteriores). Todas estas opciones se ven influidas claramente por los planes de inversión de capital y los cambios a largo plazo en cada modelo de negocio. Las decisiones en el dominio del Modelo de Servicios de Tecnología deberían corresponderse con los objetivos marcados para las habilidades de nuestro personal y su nivel de formación, ámbito en el que la Infraestructura como Servicio -IaaS- es el enfoque que se adapta a las mayores exigencias, con la máxima flexibilidad y diversidad de opciones. El extremo contrario viene representado por el Software como Servicio -SaaS-, en el que las necesidades de personal técnico se reducen al mínimo, pero donde el entorno actúa como barrera de protección para nuestros procesos y modelos de negocio. Por otro lado, el nivel de control global sobre seguridad de datos y opciones de tecnología viene directamente determinado por nuestras preferencias en el modelo de despliegue. En el modelo Privado, la organización retiene el control absoluto

sobre todas las características de la plataforma de sistemas de información, aunque elegir esta opción implique las mayores inversiones en capital financiero y humano. El modelo Público se sitúa justo al otro lado, al requerir una alineación estratégica con el proveedor de servicios cloud, a cambio de menores exigencias en inversiones de capital y personal. Las opciones Híbrida y Community se sitúan, por último, a mitad de camino, para ofrecer, a menudo, unas capacidades operativas y económicas bastante singulares.

Nuestro Equipo de Transformación Digital deberá someter a debate y discusión lo que estas “36 Sombras de la Computación” implican para el futuro, evitando que estas importantes decisiones puedan estar sujetas a

Las decisiones en el dominio del Modelo de Servicios de Tecnología deberían corresponderse con los objetivos marcados para las habilidades de nuestro personal y su nivel de formación

conjeturas o opiniones subjetivas, y asegurándose de que cualquier comparativa y cualquier opción se valoren siempre sobre datos reales. Es aquí donde las herramientas de Mediación de Servicios Cloud pueden jugar un papel importante en nuestros esfuerzos hacia la transformación digital. Cada organización deberá

plantearse cuidadosamente qué aplicaciones de negocio deberán migrarse a qué “sombra”, ya que ciertas aplicaciones podrán ejecutarse de manera óptima en servidores físicos convencionales, pero otras podrán requerir la seguridad añadida de una nube privada o de una nube pública de nivel corporativo. Existirán incluso otras aplicaciones para las que nubes de menor precio, de tipo “commodity”, podrán ser una opción viable, con ahorro de costes. Las mejores estrategias de TI híbrida deberán tener también en cuenta -además de los planes de migración y las opciones cloud- las habilidades necesarias para la migración y la gestión de tecnologías; una vez decidido el entorno objetivo para cada uno de nuestros procesos de negocio, quizás sea necesario un cierto nivel de redefinición de la arquitectura de aplicaciones.

(El presente contenido se está sindicando a través de distintos canales. Las opiniones aquí manifestadas son las del autor, y no representan las opiniones de GovCloud Network, ni las de los partners de GovCloud Network, ni las de ninguna otra empresa ni organización)

Una plataforma de mediación en servicios cloud puede ayudar a cualquier equipo que se enfrente al reto de la Transformación Digital con el uso de datos reales para perfilar cargas de trabajo, y con una toma de decisiones basada en datos, y ajustada a las arquitecturas, opciones tecnológicas y modelos de despliegue más adecuados. La mediación en servicios cloud hace posible que cualquier empresa pueda diseñar soluciones para su paso a producción y realizar estimaciones de coste incluso antes de arrancar la transformación digital.

Enlaces relacionados

- I 50 Sombras de Grey
- I Modelo de Servicios de Tecnología
- I Proveedor de servicios gestionados
- I Proveedores de servicios cloud
- I Mediación de Servicios Cloud
- I Transformación Digital
- W Ataques con Exploits, de las amenaza diarias a las campañas dirigidas
- W GDPR: soluciones para la gestión de datos personales

IoT en las empresas

Darío Ferraté
Consultor TIC

Ingeniero Superior de Telecomunicaciones por la UPN con más de 19 años de experiencia en Consultoría Estratégica de Negocio y Desarrollo de Negocio/Sales dentro del Grupo Atos; ha sido responsable, para Iberia, de ofertas estratégicas globales como Atos MyCity (Smart Cities). En 2015 colaboró con IDC como analista sénior en IoT y Smart Cities, entre otras actividades. Colabora activamente como consultor TIC en el Ministerio de Defensa y como consultor estratégico funcional en Renfe Fabricación y Mantenimiento. Su último reto es el de desarrollo y puesta en marcha de www.comparandovinos.com, un comparador de precios de vinos, destilados, espumosos con más de 5.500 productos.

Seguramente muchos de vosotros habéis podido leer o ver algún vídeo donde se indica que Internet de las cosas (IoT) potenciará enormemente el mercado y uno de los principales beneficiarios se encuentra en el sector de retail o ventas al por menor. Esto ya está siendo una realidad a día de hoy y será mucho mayor aún, casi con total seguridad, en los próximos años.

Como os decía, mirando vídeos de IoT y soluciones novedosas pude apreciar que las más completas son las orientadas al hogar o a las ciudades, mostrando distintas soluciones (luces automáticas, control de presencia, electrodomésticos inteligentes, robot para el hogar, sistemas de parking inteligentes, señalizaciones...). Sin embargo, nuestras vidas transcurren (en muchos casos) en nuestro entorno de trabajo, donde pasamos una gran parte del día y también en los medios de transporte, sean propios o públicos.

Hablando de esto último, los medios de transporte, os contaré la solución que ha planteado Tesco, una cadena de supermercados establecida principalmente en Reino Unido y Asia que, según tengo entendido, ocupa el 2do lugar en ventas. En Corea del Sur, ha decidido cambiar el nombre a la cadena por Homeplus y, aprovechando el cambio de nombre, ha dado un giro al negocio desarrollando un supermercado virtual en diferentes estaciones de metro de Seúl.

Pude ver una solución que me pareció muy curiosa de cara a facilitar la vida a los ciudada-

La transformación digital en el sector retail

La transformación digital del sector retail viene impuesta principalmente por los cambios en el comportamiento de los consumidores y en la forma y momento de realizar el proceso de compra (consumidores conectados). Entre las tendencias que destaca el estudio figura la evolución hacia modelos "as a Service".

HOMEPLUS, TIENDA VIRTUAL DE METRO EN COREA DEL SUR

CLICAR PARA VER EL VÍDEO

nos. ¿Cuántas veces hemos estado pensando en el tiempo que perdemos durante la semana, traslados para cumplir con nuestras obligaciones, y, cuando llega el fin de semana, a hacer la compra y coincidir con todos aquellos que, al igual que nosotros, no tenemos tiempo durante la semana?

En el vídeo se indicaba más o menos lo siguiente: "… casi todos los ciudadanos debemos realizar las compras en el supermercado y dada la vida ajetreada que llevamos y el escaso tiempo que tenemos de lunes a jueves (en el caso más favorable), solo nos queda el viernes por la tarde, el sábado y en algunos casos el domingo para "reabastecernos". ¿Os suena? Seguro que sí y más aún si vivimos en las principales capitales. Los fines de semana son "terribles" con colas para comprar carnes, pescados, pesar nuestras frutas y verduras y no hablar a la hora de pagar y, ya que estamos, a la hora de desplazarnos al "súper" y tener que aparcar. Todo esto hace que estemos "tensos" y que la compra semanal se convierta en una "tortura".

¿Habéis probado hacer la compra cualquier día de la semana en cualquier horario comprendido entre las 10 y 17? ¡¡¡Desaparece cualquier síntoma de tortura, os lo aseguro!!!!

Volviendo al tema, Homeplus decidió aprovechar las marquesinas instaladas en las estaciones de metro para poner fotografías en tamaño real que reflejan a la perfección las distintas góndolas con productos envasados (carnicería, charcutería, pescadería, frutas y verduras, conservas, limpieza…). De esta forma, mientras

Homeplus decidió aprovechar las marquesinas instaladas en las estaciones de metro para poner fotografías en tamaño real que reflejan a la perfección las distintas góndolas con productos envasados

Estoy seguro de que, usando un poco la imaginación, tenemos a nuestro alcance un buen número de oportunidades para todos los gustos

se espera la llegada del metro, a través de sus smartphones y con una aplicación del propio supermercado, pueden ir seleccionando los productos deseados y cargarlos en su carrito de la compra. Una vez finalizado, el importe es cargado en la cuenta que tengamos asociada y el producto es enviado a nuestros hogares en la franja horaria seleccionada. Con esto, la empresa en cuestión ha incrementado sus ventas enormemente y los ciudadanos pueden disponer de más tiempo libre, menos estrés e igual servicio. Una idea que me ha parecido brillante para todos los usuarios que utilizan este transporte público… Si te ha sorprendido la idea, ¡más te va a sorprender cuando sepas que está funcionando desde noviembre de 2010! ¡Sí, lleva 7 años en el mercado con un éxito increíble!

Hoy, en un evento al que asistí, se comentó que existen muchas iniciativas para que la gente consuma más aprovechando los tiempos muertos y que éstas tienen un éxito importante. Parece que cuando nos aburrimos tendemos a gastar dinero y si es útil, mejor aún, pero… ¿y si lo llevamos más allá? Estoy seguro que cuando los coches autónomos sean el medio de transporte que utilicemos (cada vez estamos más cerca y, según información de ese mismo evento, BMW está tomando la delantera en el coche autónomo, los que requerimos usar el automóvil para desplazarnos al lugar de trabajo, durante el tiempo de trayecto podremos aprovechar para realizar un sinfín de cosas que, a día de hoy, es prácticamente imposible. ¡Ahí sí que se disparará el infoentretenimiento y el comercio electrónico!

Esto, bajo mi punto de vista, está genial de cara a generar negocio y valor para las empresas y los consumidores. Estoy seguro de que, usando un poco la imaginación, tenemos a

nuestro alcance un buen número de oportunidades para todos los gustos.

Retomando el tema de los vídeos de IoT con aplicaciones para ciudades, me he puesto a buscar IoT para empresas y salen una buena cantidad de artículos que indican, entre otras cosas, que es un potenciador, que las tres cuartas partes de las empresas consideran que IoT es crucial para tener éxito en un futuro… pero echemos un vistazo con ojos críticos y preguntémonos: ¿cuánto de "inteligencia" tiene mi empresa? ¿Qué soluciones ampliamente conocidas y recomendadas para el hogar tengo implementadas en nuestras oficinas? ¿Controlamos las luces? ¿Y la temperatura de cada dependencia? ¿Qué pasa si dejamos encendido el ordenador cuando nos vamos del trabajo? En definitiva, ¿hacemos un uso eficiente de las utilities (agua, gas, luz)? Y si a todas estas preguntas hemos contestado que "sí", ¿analizamos la información para saber cómo optimizar, por ejemplo, los espacios? Ahí es donde los dispositivos conectados ayudan en gran medida a contestar todas estas preguntas y a realizar acciones para hacer que las empresas sean más sostenibles, los recursos sean mejor aprovechados y nuestra calidad de vida en nuestro "segundo hogar" sea más placentero.

Ya, por terminar, en el evento de hoy, se hablaba de oficinas inteligentes, con soluciones realmente novedosas, en las que las salas de reuniones no tienen los proyectores típicos (que en el mejor de los casos están colgados desde el techo), y las luces (LED) son totalmente inteligentes, solo se encienden si detectan presencia. En la sala se sustituye una pizarra de papel (y la búsqueda de rotuladores que "pinten" correctamente) y hasta las pizarras electrónicas por una pantalla "todo en uno" que hace las funciones de monitor, videoconferencia, pizarra digital interactiva donde todos los participantes, independientemente de donde estén, pueden pintar, remarcar, aumentar, resaltar cualquier nota, imagen y/o presentación que se esté compartiendo. Claramente vi que esta solución es aplicable a múltiples sectores y, por supuesto, la telemedicina es una de ellas. Ya os iré comentando como avanza el tema.

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

En un evento al que asistí, se comentó que existen muchas iniciativas para que la gente consuma más aprovechando los tiempos muertos y que éstas tienen un éxito importante

¿Te avisamos del próximo IT Reseller?

Enlaces relacionados

- Soluciones para salas de reuniones basadas en Cloud
- Tesco Homeplus
- Obtén lo mejor de dos mundos con la TI Híbrida
- Simplifica tu manera de consumir TI
- Infraestructura en Cloud

it User
TECH & BUSINESS

Cada mes en la revista, cada día en la Web.