it Reseller
TECH&CONSULTING
Noviembre 2017 - nº 28

Plantronics muestra el futuro de las comunicaciones

Context analiza la situación del mercado de TI en España

Ingram Micro celebra una nueva edición de su Simposium

Appliances de seguridad, más opciones para proteger el negocio

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

Servicios de impresión

Tendencia al alza en un mercado maduro

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

IT Digital Security
Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores
Hilda Gómez, Arantxa Herranz, Reyes Alonso

Diseño revistas digitales
Contracorriente

Diseño proyectos especiales
Eva Herrero

Producción audiovisual
Antonio Herrero, Ismael González

Fotografía
Ania Lewandowska

it User TECH & BUSINESS
it Reseller TECH&CONSULTING
it Digital Security
it televisión

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

Servicios de impresión, una oportunidad en un mercado maduro

El de la impresión es un mercado muy maduro. Prácticamente todas las empresas, incluidas las más digitales, cuentan con un número adecuado de impresoras, ya sean láser, de inyección o, incluso alguna queda todavía en el parque instalado, matriciales. Y, si miramos a los usuarios domésticos, la cosa no es muy diferente, aunque es cierto que, de un tiempo a esta parte, hay algunos usuarios que han decidido no tener una impresora propia y utilizar los servicios de impresión que les ofrecen algunas empresas.

Esto tiene una parte positiva y otra negativa, como todo en esta vida. La parte positiva es que siendo un mercado muy desarrollado y con un gran parque instalado de máquinas, el negocio adicional a la venta de propio producto, es decir, la venta de consumibles, sigue proporcionando beneficios a las empresas, tanto fabricantes como del mundo de la distribución. Por el contrario, al ser un mercado maduro, los niveles de crecimiento trimestrales no suelen ser elevados y, a veces, ni siquiera son positivos.

Para las empresas, además, la impresión se ha convertido en muchos casos en un problema, porque no hay forma de controlar los costes, predecir la disponibilidad de las máquinas o asegurar de que las impresoras no se convierten en focos de problemas alrededor de la confidencialidad de la información. Y, para solventar estas novedades, se han desarrollado los servicios de impresión.

En realidad, servicios de impresión es un concepto muy amplio, porque incluye todo aquello que se le puede ofrecer a un cliente alrededor de la impresión: control de costes, seguridad, optimización, sistema de alertas previas… es decir, una serie de acciones por las que los clientes están dispuestos a pagar con la idea de ahorrar costes, aumentar la eficiencia o incrementar la seguridad.

De los tradicionales servicios de pago de coste por página a los modernos servicios de optimización del flujo de la información en la empresa, todo aquello relacionado con la impresión sigue siendo una oportunidad de negocio, porque, si bien algunas empresas ya han dado el paso, otras muchas todavía no, y hay que aprovecharlo.

Juan Ramón Melara
IT Digital Media Group

Sumario

En portada

Especiales IT Reseller

Herramientas para potenciar el negocio

TechData

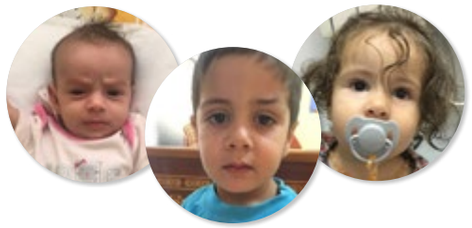
Índice de anunciantes

¿Te avisamos del próximo IT Reseller?

IT Digital Security

Descubra la nueva apuesta por la información sobre seguridad de IT Digital Media Group

Responsabilidad Social Corporativa



Antes, un orfanato; ahora, un hogar

Reportaje

Dispositivos de seguridad, un negocio en el que el canal es clave

Actualidad

Ingram Micro supera los objetivos al crecer un 20% en España

Plantronics muestra el futuro de las comunicaciones en su XIV Evento de Canal

Entrevista con Fadi Moubarak, vicepresidente de canales de Avaya Internacional

Huawei apuesta por la Inteligencia Artificial en su Huawei Mate 10

El ecosistema de partners se transformará totalmente en 2021

El canal de distribución TI español crece un 8,7%

Puertas abiertas. Acuerdos cerrados.

Nos centramos totalmente en los partners, todo el tiempo.

Kaspersky Lab facilita todo lo posible el crecimiento del negocio de nuestros partners. Es por eso que nuestro programa de partners se alinea con su modelo empresarial, gracias a la flexibilidad de su diseño para asegurar márgenes excepcionales y oportunidades de crecimiento.

Obtenga más información en www.kaspersky.com/partners.

El mayorista mostró al canal dónde se encuentran las oportunidades de negocio en su Simposium

Ingram Micro supera los objetivos al crecer un 20% en España

Durante la celebración de su Simposium, Jaime Soler, director general de Ingram Micro para España y Portugal, ha explicado cómo está siendo el comportamiento del mayorista. Soler ha afirmado que la firma ha superado los objetivos de crecimiento, gracias al comportamiento tanto de su negocio de volumen como de valor.

Bárbara Madariaga. Barcelona.

La Cúpula de las Arenas de Barcelona volvió a acoger una nueva edición del Simposium de Ingram Micro, un evento que, a falta de cifras oficiales, asistieron "el mismo número de personas que el año pasado", tal y como aseguró Sara Zamora, directora de marketing de Ingram Micro, y contó con el apoyo de 102 marcas.

Durante el evento, Jaime Soler, director general de Ingram Micro para España y Portugal, explicó cómo estaba siendo el comportamiento del mayorista este año, destacando que, si el mercado de distribución en España ha crecido un 8,7% en entre enero y septiembre de este año, Ingram Micro ha cosechado "un crecimiento bastante superior a la media", de alrededor del 20%. Esto ha hecho que el mayorista haya

Encuesta sobre la experiencia de los usuarios de almacenamiento flash

Esta encuesta a 1.000 profesionales de TI sobre el cambio al almacenamiento flash revela que antes de adoptar esta tecnología, el 71% de los encuestados tenía dificultades para alcanzar sus objetivos de protección de datos críticos. Después de flash, ese número se redujo al 29%. El 90% de los que ejecutan cargas de trabajo de virtualización de servidor en sus entornos de almacenamiento All-flash responden que esta carga de trabajo funciona bien.

ganado “casi tres puntos de cuota de mercado” y haya superado las expectativas tanto en el área de valor como en la de volumen como en la combinada.

No obstante, no todas las áreas han crecido. “El área de Mobility ha obtenido unos resultados un poco por debajo de los del año pasado”. Esto se ha debido a que “hemos apostado por una serie de fabricantes que han crecido menos en el mercado”. Ingram Micro no contempla dejar de apostar por estas firmas, sino que su intención es “añadir nuevos fabricantes a nuestra oferta” para lograr que esta área crezca.

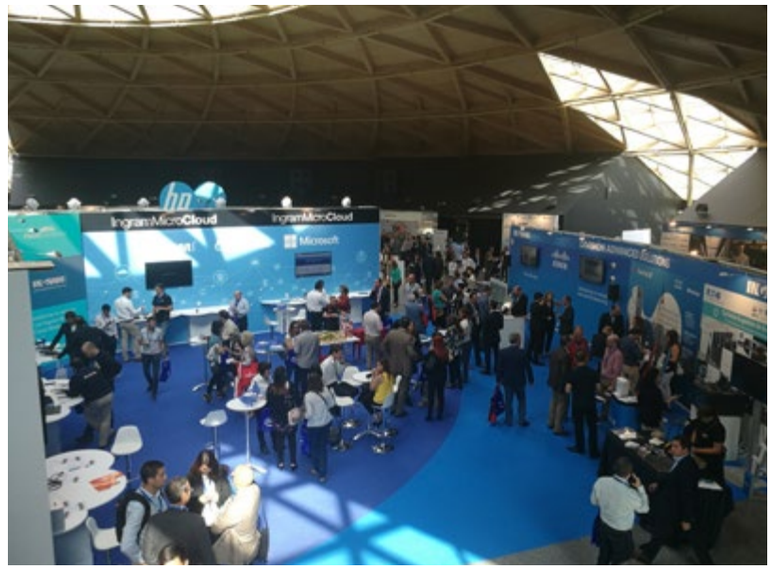
A pesar del área de movilidad, Ingram Micro “ha superado no sólo los objetivos de facturación, sino también de rentabilidad”, destacó Jaime Soler, quien confió en que, de cara al último trimestre del año, “sigamos el mismo ritmo de crecimiento”.

Mercado de volumen

David Belenguer, director del área de volumen de Ingram Micro, destacó el buen comportamiento de su división gracias a, entre otras cosas, el área de sistemas. “Es el que hemos registrado un mayor crecimiento tanto en valor absoluto como porcentual”. Dentro de ésta han sido los portátiles y tablets “donde se han producido los mayores incrementos”. La venta de periféricos, por su parte, “crece a doble dígito”.

En el caso del negocio y los monitores éste es un negocio “con gran crecimiento, especialmente en gran formato”. En este sentido, David Belenguer aseguró que “duplicamos el crecimiento del mercado”, en gran medida gracias al comportamiento de un segmento en clara expansión, como es el gaming. “Los componentes y el networking se encuentran en una fase de transición”, mientras que el de impresión es un

> “Ingram Micro ha superado no sólo los objetivos de facturación, sino también de rentabilidad”
>
> Jaime Soler, director general de Ingram Micro para España y Portugal



El área de Mobility ha obtenido unos resultados un poco por debajo de los del año pasado

área dispar. “Los consumibles decrecen, pero la subida experimentada por los equipos láser e inyección de tinta compensan la caída de otros segmentos”.

Mercado de valor

Alberto Pascual, director del área de valor de Ingram Micro, destacó el crecimiento que ha experimentado su área, el cual está “concentrado en el segmento de la pequeña y mediana empresa”. Concretamente “hemos registrado una subida de doble dígito tanto en Advanced Solutions como en Specialities.

Esta división ha llevado a cabo una serie de iniciativas como, en el caso de Advanced Solutions, “la construcción de centros de datos que está disponible al 100% para el canal”, el desarrollo de soluciones propias o la apuesta por la ciberseguridad, un ámbito en el que “es básico ofrecer una oferta global”. Si hablamos de Specialities, “hemos desarrollado un porfo-

“En la situación actual, Madrid nos ofrece más estabilidad que Barcelona”

Ingram Micro ha sido el primer mayorista con sede en Barcelona que anuncia su traslado, en este caso a Madrid, un sector que tiene una gran presencia en Cataluña. El mayorista aseguró en un comunicado que esta decisión “no afecta a las sólidas relaciones que la compañía mantiene con sus clientes y fabricantes” y no tendrá impacto en su capacidad “para continuar proporcionando el alto nivel de servicio y soporte por el que es reconocida”.

La decisión de trasladar la sede fiscal y social a Madrid tiene como objetivo garantizar el pleno desarrollo de su actividad, “a todos los niveles”, en un marco legal estable. Ingram Micro cuenta con una plantilla de 750 personas y trabaja con más de 10.000 distribuidores tanto en España como Portugal.

Durante la celebración de la XVI edición del Simposium de Ingram Micro, Jaime Soler, director general de Ingram Micro, se refirió a la decisión adoptada por el mayorista de trasladar tanto su sede social, como fiscal, de Barcelona a Madrid.

En este sentido, Soler reiteró que el objetivo de este movimiento es “buscar un marco legal más estable”, destacando que “con la situación actual” de incertidumbre, “Madrid nos ofrece más estabilidad que Barcelona”.

No obstante, Jaime Soler aseguró que la decisión “es meramente empresarial” y se ha adoptado pensando tanto en su plantilla, como en el canal de distribución y los fabricantes. “Queremos que tanto nuestros trabajadores, como los resellers y los fabricantes se sientan en un marco de seguridad”.

La decisión, que se comunicó el pasado martes 11 de octubre, ha sido bien acogida “por clientes, fabricante y empleados”. Estos últimos, además, “tienen confianza”.

Jaime Soler puntualizó que el cambio de sede “no es una decisión táctica”.

Preguntado por si en un futuro, Ingram Micro podría trasladar tanto sus almacenes como empleados fuera de Cataluña, Jaime Soler afirmó que “nuestra intención es seguir creciendo. No buscamos la territorialidad sino aquello que nos aporte más valor” independientemente de la zona.

Durante el Simposium de Ingram Micro, el mayorista también tuvo palabras para valorar cómo ha sido el primer año de la compra de One2One

lio verticalizado que cubre la parte de IoT y de Industria 4.0, con el que queremos ofrecer al canal nuevas oportunidades de negocio".

En el área AV/Pro, "nos encontramos en un momento de renovación tecnológica. Estamos apostando por la señalización digital y por ofrecer una solución más completa", destacó Alberto Pascual.

Asimismo, y con el objetivo de que "el canal tenga un protagonismo especial", Ingram Micro también ha puesto en marcha una serie de iniciativas de Transformación Digital como es el caso del programa Ingram Micro-ESADE.

Esta división cuenta con 64 fabricantes, lo que "nos ha permitido consolidar la oferta que necesita el canal".

Compra de One2One

Durante el Simposium de Ingram Micro, Jaime Soler también tuvo palabras para valorar cómo ha sido el primer año de la compra de One2One. Así, destacó que esta empresa de logística "cubre un espectro al que nosotros no llegábamos", destacando que la capacidad logística "es mucho mayor".

Soler también destacó la calidad de la firma destacando que "son los mejores en su sector", gracias a que cuenta con "el apoyo de un buen equipo" donde la profesionalidad es la principal característica. "Disponen de una cultura de servicio muy importante".

En este primer año "ha habido una labor de aprendizaje importante. Hemos integrado funciones y hemos aprovechado el negocio". El reto ahora es "explicar este aprendizaje de puertas hacia fuera". En definitiva, "estamos muy contentos en cuanto al negocio de integración que tenemos".

Alfonso Cualladó, director general de One2One, destacó que, antes de la adquisición, la compañía facturaba "unos 28 millones de euros". De cara a este año, One2One prevé incrementar la facturación en un millón de euros, gracias a la labor que se realiza desde sus instalaciones en Madrid y las Islas Canarias, "desde la que damos servicio a toda España en menos de 24 horas".

"Después de 15 años de trayectoria, One2One era una compañía rentable, pero con problemas de crecimiento debido a nuestro tamaño". Estos problemas de crecimiento "se solventan con nuestra integración en Ingram Micro".

Cualladó reconoció que "hemos estado en una fase de ajustes entorno a la organización y ahora nos encontramos en disposición de ofrecer servicios de valor añadido asociados a la venta de tecnología".

Enlaces relacionados

- [Se acelera el ritmo de consolidación del canal TI]
- [Ingram Micro ingresa 10.830 millones de dólares en el segundo trimestre]
- [¿Están tus empleados preparados para el puesto de trabajo digital en tienda?]
- [Consumo de TI para PYMES]
- [Indice de madurez digital en las empresas]

Diseño elegante

Portégé X20W: Diseñando la perfección

Ultrafino con tan solo 15,4 mm de grosor y 1,1 kg de peso, por lo que te lo puedes llevar a cualquier lugar. Su chasis está fabricado con magnesio de gran resistencia y tiene un elegante acabado en azul y dorado. Además, incluye nuestro sistema de refrigeración de aire híbrido para mantener una temperatura óptima.
También incorpora potentes procesadores Intel® Core™ de 7.ª generación.

Toshiba Portégé X20W. Diseño elegante.

Obtén más información en: **www.toshiba.es/X20W**

Intel Inside®.
Para una productividad extraordinaria.

El fabricante reúne en Sevilla a sus principales resellers

Plantronics muestra el futuro de las comunicaciones en su XIV Evento de Canal

Plantronics ha reunido en Sevilla a más de 50 partners de España para explicarles cuál es el futuro de la compañía y del mercado de comunicaciones unificadas. No en vano, el fabricante quiere ser uno de los jugadores relevantes y apuesta por el canal de distribución y por soluciones de valor. IT Reseller acudió a Sevilla como único medio de canal y entrevistó a Christopher Thompson, vicepresidente a nivel mundial para el área de marketing B2B de Plantronics.

Bárbara Madariaga. Sevilla.

Plantronics reunió a sus principales resellers en la región Iberia para explicarles las novedades de la compañía, tanto de estrategia, como de producto y de canal. Durante la reunión de partners, Christopher Thompson, vicepresidente a nivel mundial para el área de marketing B2B de Plantronics, explicó cuáles son las principales tendencias del mercado, las cuales pasan por la colaboración. “La voz, el vídeo, las aplicaciones de comunicación están marcando las tendencias del mercado”, siendo la voz, “uno de los servicios más importantes”.

Estrategias para la implementación de infraestructura hiperconvergente

Una opción de arquitectura de centro de datos emergente, denominada infraestructura 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.

"Desde Plantronics invertimos en el canal para que podamos crecer de manera conjunta, a través de soluciones globales",

Christopher Thompson, vicepresidente a nivel mundial para el área de marketing B2B de Plantronics

Otra de las grandes tendencias del mercado hace referencia al área de customer service. "La irrupción de la telefonía móvil ha cambiado el área de contact center. En cierta forma, los smartphones han dotado de mayor complejidad a esta área, pero también de mayor valor. Nuestra estrategia se centra en simplificar este mercado, sin quitar el valor añadido que ofrece. Ofrecemos soluciones de colaboración que permiten a las empresas ser más productivas y potenciar el customer service".

Christopher Thomson, además, destacó la importancia que está adquiriendo el mercado de auriculares, el cual "está creciendo enormemente". En el caso de Plantronics, "estamos totalmente preparados para aprovechar este mercado, ofreciendo las mejores soluciones de colaboración a las empresas. Somos la mejor opción".

Mercado empresarial versus consumo

Asimismo, Christopher Thomson destacó que la línea que separa la parte empresarial de la de consumo es cada vez más difusa. "Los usuarios utilizan los mismos productos para su parte profesional como para la personal". En el caso de Plantronics, "desarrollamos productos B2B para diferentes áreas".

Durante el XIV Evento de Canal de Plantronic, Christopher Thomson resaltó la importancia que tiene España para el global de la compañía. La relación con Latinoamérica, "España tiene una cultura similar, con un idioma común, y los países latinoamericanos se fijan en la Península Ibérica", el contexto europeo en el que se encuentra Iberia, o la fortaleza de algunos sectores como son la Administración Pública, la banca o las telecomunicaciones, son los principales factores que hacen que España sea un país importante para Plantronics.

Durante la reunión, Plantronics aprovechó para lanzar Manager Pro, "una solución que es estratégica para nosotros y que puede hacer crecer el negocio de nuestro canal"

Importancia del canal

El canal de distribución es una parte esencial para Plantronics, no en vano, su estrategia es cien por cien canal. Christopher Thomson reconoció que los resellers se encuentran en medio de una transformación, la misma que está afectando al resto de la industria, y que necesitan disponer de buenas soluciones y de programas completos por parte de los fabricantes para aportar valor a sus clientes. "El precio ya no es lo más importante para el canal de distribución. La tendencia, en el mercado de las comunicaciones unificadas es aportar valor". En este sentido, Thomson destacó que, para que el canal pueda competir con el mercado retail, "tiene que diferenciarse y ofrecer a las empresas productos y servicios que se adapten a sus necesidades y no entrar en una guerra de precios". Desde Plantronics invertimos en el canal para que podamos crecer de manera conjunta, a través de soluciones globales".

Mensajes a su canal

Durante la celebración de la XIV Evento de Canal, Plantronics trasladó a sus resellers una serie de mensajes "claros y concisos". Durante la reunión, Plantronics aprovechó para lanzar Manager Pro, "una solución que es estratégica para nosotros y que puede hacer crecer el negocio de nuestro canal".

Asimismo, en el evento, Plantronics hizo hincapié en las mejoras que ha realizado en su programa de canal. En este sentido, Agustín Santos, es director de distribución de Plantronics Iberia, aseguró que uno de los puntos fuertes es la generación de leads. "Invertimos para que nuestro canal pueda hacer negocio a través del registro de nuevas oportunidades"

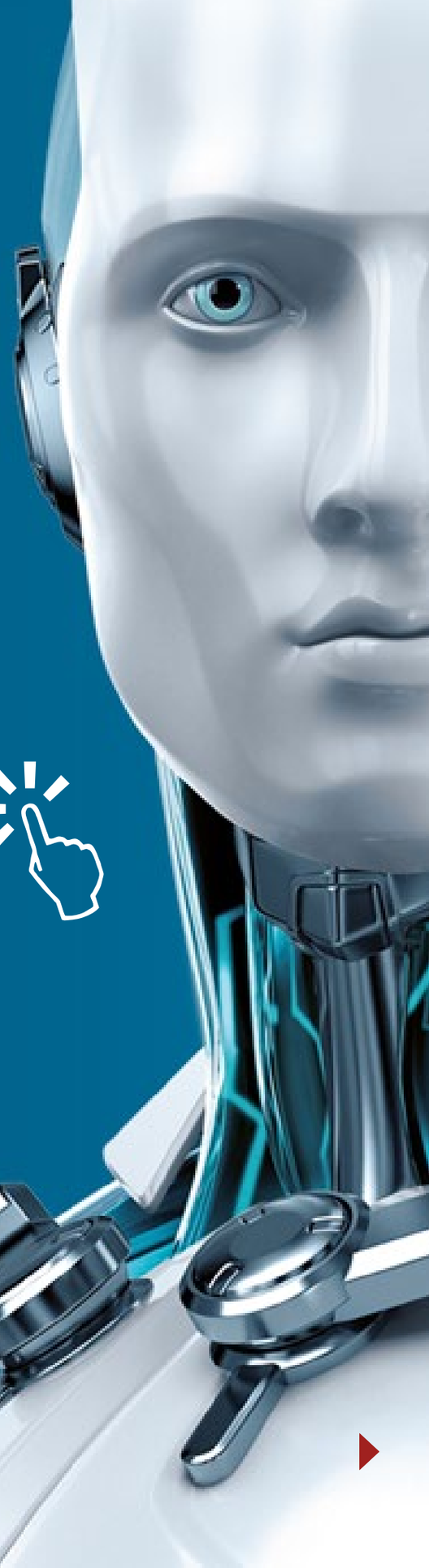
Dentro del programa de canal, y teniendo en cuenta que la firma apuesta por el valor, "potenciamos toda nuestra oferta formativa y animamos a los resellers a que aprovechen los cursos". Las demos, "queremos que nuestro canal pruebe los productos con sus clientes", o los diferentes programas de incentivos han sido otros de los temas importantes que se han tratado durante el encuentro.

Enlaces relacionados

- La oferta de Plantronics
- Cómo la transformación digital impacta en los OEM
- La transformación digital en el mercado retail
- Consumo de TI para PYMES
- Indice de madurez digital en las empresas

ENJOY SAFER TECHNOLOGY

La mejor protección para ti, tus clientes y tu negocio con tecnología **NOD32**



GRANDES MÁRGENES

SOPORTE PREMIUM

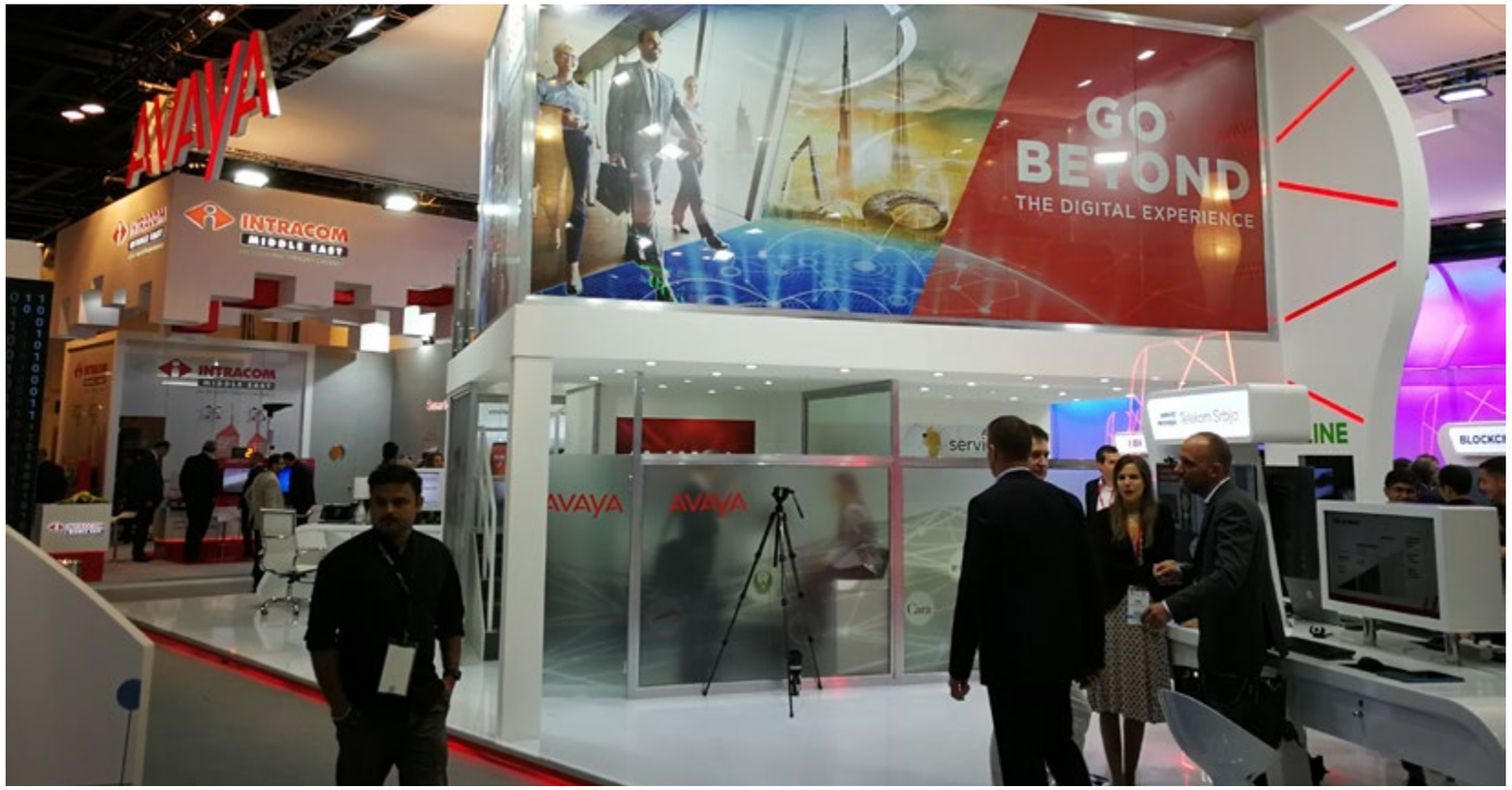
SIN VENTAS MÍNIMAS

PROTECCIÓN DE CARTERA

FORMACIÓN CONTINUA

¡HAZTE DISTRIBUIDOR, CON NOSOTROS ES MUY FÁCIL!

Tel. 96 291 33 48 - www.eset.es/canal-de-distribucion



Fadi Moubarak, vicepresidente de canales de Avaya International:

"Los partners son los que enriquecen nuestras soluciones"

Aprovechando la presencia en GITEX Technology Week, IT Reseller ha tenido la oportunidad de conversar con Fadi Moubarak, vicepresidente de canales de Avaya International, quien nos ha ofrecido una visión de lo que el fabricante espera de sus partners en este momento.

Miguel Ángel Gómez (Dubai)

Tal y como nos explica el propio Fadi Moubarak, "éste es un evento muy relevante, porque nos permite, en un único punto, llegar a una gran variedad de clientes y partners. GITEX nos acerca a una gran variedad de empresas que pueden venir a ver no solo que lo podemos ofrecer a día de hoy, sino también lo que está por venir. Es una oportunidad para socializar con partners y clientes y mostrarles las tendencias hacia donde se dirige el futuro".

Específicamente en esta ocasión, "es una oportunidad para nuestros clientes para ver lo que les proponemos de cara a los próximos doce meses, donde pensamos que hay que poner el

Mejores prácticas para optimizar la experiencia digital del cliente

Para determinar la madurez de la gestión que hace una marca de la experiencia digital de sus usuarios, se necesita una combinación de métricas de negocio y TI y un campo de trabajo para mejorar el negocio digital. Estas herramientas proporcionan a los ejecutivos de CX y profesionales de operaciones TI la capacidad de evaluar dónde se encuentra su marca dentro de un rango de capacidades para la gestión del rendimiento de la experiencia digital.

Este informe analiza la evolución de la gestión del rendimiento de la experiencia de cliente y cómo las organizaciones pueden desarrollar y establecer prácticas y procesos para atraer, retener e incrementar su base de clientes optimizando la experiencia de usuario.

Avaya muestra en GITEX la tecnología llevada a la práctica

Avaya ha mostrado en GITEX Technology Week, de la mano de una quincena de partners, diferentes casos de uso reales que avanzan en la experiencia del cliente más allá de la tecnología.

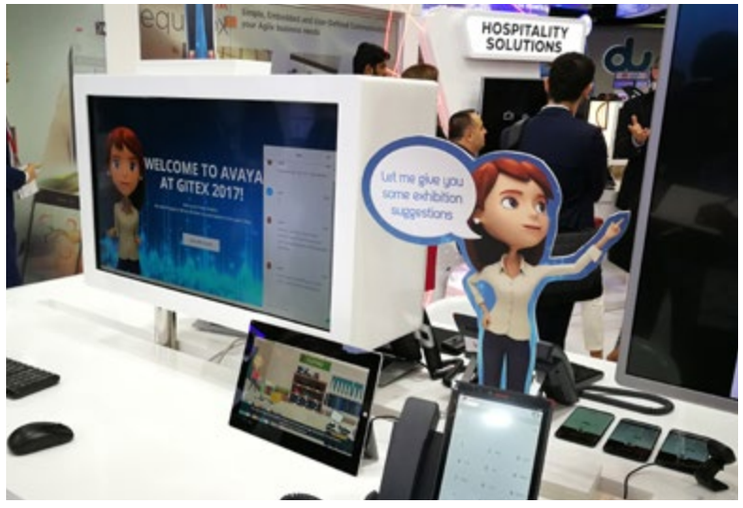
No se trata solo de tecnología, sino de cómo ésta resuelve las problemáticas de los clientes y mejora la experiencia de uso. Éste es el planteamiento con el que Avaya ha acudido a GITEX Technology Week, el evento tecnológico de referencia en Oriente Medio que se está celebrando esta semana en Dubai. En esta cita, Avaya mostró cómo su plataforma tecnológica puede convertirse en la base para el desarrollo de tecnologías y servicios que ayuden en las empresas en su camino hacia la Transformación Digital.

En un stand donde muestran diferentes casos de uso en segmentos como Sanidad, hospitality, seguridad pública, finanzas o bancos, entre otros, Avaya quiere mostrar el valor de su propuesta tecnológica basada en estándares y cómo sobre ella pueden seguir desarrollándose proyectos en base a tecnologías emergentes como blockchain, inteligencia artificial o Internet de las Cosas.

Pero Avaya no ha puesto el foco en la tecnología, sino en cómo mejorar con ella la experiencia de uso de los clientes en diferentes verticales, en cómo integrar diferentes soluciones para ayudar a las empresas a mejorar su atención al cliente y la experiencia de uso de éste, algo que, según la consultora Gartner, es una necesidad principal para casi el 90 por ciento de las organizaciones.

Nidal Abou-Ltaif, presidente de Avaya Internacional, recalcaba que "proporcionar una experiencia de uso superior precisa cumplir con sus expectativas en todas sus interacciones, ya sean digitales o físicas. Los clientes quieren una misma experiencia de uso independientemente del canal o el dispositivo usado en cada momento".

De ahí que la firma haya acudido a GITEX Technology Week para mostrar cómo están trabajando con diferentes partners para crear soluciones flexibles y orientadas a satisfacer las demandas de los usuarios y ayudar a las empresas en su evolución en el mundo digital, afirmaba este responsable.



JIM CHIRICO, CEO DE AVAYA, EN GITEX TECHNOLOGY WEEOK 2017

CLICAR PARA VER EL VÍDEO

foco y, precisamente, hemos querido mostrarles en el stand un conjunto de soluciones enfocadas a funcionalidades relevantes para los clientes. No es tanto mostrar las tecnologías que hay por debajo y que dan soporte a las soluciones, sino llevar la conversación a lo que realmente es relevante para el cliente y cómo pueden ayudarle estas soluciones en su problemática concreta".

Un cambio de enfoque

Este enfoque representa un cambio en la forma de acercarse con los partners a los clientes en un evento como éste. "La conversación tecnológica", apunta Moubarak, "llega en un tercer o cuarto escalón en una relación iniciada alrededor de las necesidades del negocio. Es fundamental entender al cliente y tratar de comprender lo que necesita, las funcionalidades que precisa para resolver sus problemas. Y una vez establecido esto, las piezas de la tecnología se van incorporando a la discusión".

Pero, además, en Avaya son conscientes de otra problemática en la que los partners pueden ayudarles con los clientes. En palabras de Fadi Moubarak, "vivimos en un mundo eminentemente tecnológico o más bien sobreexpuesto a la tecnología, tanto a nivel personal como profesional. En todo lo que hacemos hay tal nivel de tecnología que no somos capaces de sacar tiempo

"Es fundamental entender al cliente y tratar de comprender lo que necesita, las funcionalidades que precisa para resolver sus problemas. Y una vez establecido esto, las piezas de la tecnología se van incorporando a la discusión"

La presencia del nuevo CEO

Avaya ha contado en GITEX con la presencia de su nuevo CEO, Jim Chirico, máximo responsable de la compañía desde la retirada anunciada el pasado mes de agosto de Kevin Kennedy.

Jim Chirico ha hablado en GITEX Technology Week con socios y clientes para transmitirles el compromiso de la compañía de "seguir invirtiendo tanto en tecnologías tradicionales como emergentes", con el objetivo de proporcionar "la mejor experiencia para los usuarios". "Hemos simplificado y consolidado nuestras operaciones y estructuras para mejorar nuestra situación y seguir aportando soluciones innovadoras al mercado", afirmaba Chirico, y añadía que los cambios en la compañía les permiten "ser más flexibles y más rápidos a la hora de llevar nuestras soluciones al mercado".

Además, este responsable recordaba la importancia de los partners al afirmar que "tenemos la tecnología, pero esto es solo una parte. Queremos ir más allá de la tecnología, estando cerca de clientes y partners".

Y un mensaje como conclusión, "Avaya es fuerte y continuará creciendo de manera consistente en el futuro".

para conocer en profundidad todas las características y posibilidades, y acabamos usando solo un 15 o un 20 por ciento de esta capacidad que tenemos. Y este reto no va a desaparecer. Lo que hacemos para solucionarlo, es abrir nuestra plataforma a los desarrolladores para que aprovechen todas las funcionalidades de la tecnología de forma automática, con lo que son las aplicaciones las que usan nuestra tecnología, no los clientes; las aplicaciones de negocio de nuestros clientes usan todas las funcionalidades de la tecnología de forma transparente para ellos. Así recortamos el tiempo de aprendizaje. En cuanto lo hace la aplicación el cliente se beneficia de forma transparente, no hay que enseñarles de nuevo a usar las funcionalidades. Enseñamos a las aplicaciones a usar la tecnología y los clientes se benefician de ello de forma automática".

Y en este escenario, "los partners son los que enriquecen nuestras soluciones con piezas desarrolladas con tecnologías emergentes como chatbots, IoT, blockchain… Y para ellos es una excelente oportunidad para vender sus servicios y soluciones en escenarios de negocio que ellos conocen perfectamente, porque están cerca de los clientes. Ellos saben qué es prioritario para los clientes y lo que necesitan en cada momento".

La evolución del ecosistema de partners

Pero, cómo afecta este posicionamiento a los miembros del canal más tradicional de Avaya.

Blockchain para mejorar la experiencia digital del usuario

Avaya ha mostrado en GITEX Technology Week cómo la integración de nuevas tecnologías, como blockchain, Internet de las Cosas o la Inteligencia Artificial, pueden facilitar su labor de proporcionar a los clientes una experiencia de uso transformada y adecuada a sus necesidades.

Y en esta experiencia digital basada en las soluciones tradicionales de Avaya tienen cabida también innovadoras tecnologías que servirán para adecuar más esta experiencia a las necesidades de los clientes y los negocios. De ahí que Avaya esté mostrando casos de uso integrando tecnologías como blockchain, IoT o IA.

Y es que en los últimos meses Avaya ha redefinido sus tecnologías tradicionales para permitir a sus partners desarrollar sobre ellas soluciones y servicios que mejoren la experiencia digital de sus clientes, lo que lleva a pensar a sus responsables que, con la integración de estas tecnologías, cuentan con una propuesta de soluciones adecuada para gestionar la experiencia digital del cliente en cualquier sector vertical. De hecho, algunos, como Banca, Seguridad Civil, Transporte, Retail u hospitality se están viendo en el stand de la firma en la cita de Dubai.

Uno de estos ejemplos, en colaboración con Avanza Solutions, es el índice de felicidad en blockchain, que permite a las empresas gestionar de forma dinámica las diferentes interacciones digitales del cliente, independientemente de cuál sea el medio o el lugar. La solución facilita que las empresas aprovechen las posibilidades de blockchain para recoger e integrar datos, de forma segura, de diferentes fuentes, tales como chats, web, correo electrónico, contact center o social media. A partir de estos datos, las compañías podrán conocer el grado de satisfacción de sus clientes en sus interacciones digitales en tiempo real.

De hecho, aunque las consultoras como Gartner estiman que casi el 90 por ciento de las empresas buscan competir en experiencia al cliente, solo el 6 por ciento, según datos de Aberdeen Group, están satisfechos de cómo aprovechan los datos que tienen de estos clientes para mejorar su experiencia digital.

En palabras de nuestro interlocutor, “es una evolución. Algunos de ellos ya han iniciado el camino hacia el nuevo escenario y han potenciado sus capacidades para este nuevo nivel, pero algunos todavía necesitan hacerlo, y nosotros les estamos ayudando, trabajando con otros partners más específicos de desarrollo. Existen posibles escenarios, pero si un partner conoce las necesidades de negocio de su cliente, puede entrar en contacto con uno de estos partners del ecosistema para trabajar en una solución, o pueden adquirir ellos mismos estas capacidades para solventar la necesidad de su cliente. Tenemos ejemplos de partners que han creado una solución completa sobre tecnología de Avaya y un desarrollo de otro partner del ecosistema, añadiendo tecnología de terceros sobre todo ello”.

En todo caso, “contamos con los programas y las herramientas para ayudarles en esta evolución, dependiendo de cada uno de los posibles escenarios que se puedan plantear. Sea cual sea su situación, podemos ayudarles, pero son ellos los que deben iniciar este proceso evolutivo para no quedarse atrás. Queremos ser muy transparentes: podemos ayudarles, pero son ellos los que deben querer cambiar y convivir con los nuevos tipos de partners que ya han entrado en el ecosistema. Porque no podemos olvidar que nuevos partners provenientes del

> "Ya no se trata de cuánto puedes obtener por implementar soluciones de Avaya, sino qué negocio puedes obtener integrando soluciones y servicios alrededor de la tecnología de Avaya"

mundo del software pueden trabajar, y de hecho lo hacen, con partners del mundo de las comunicaciones para llevar las soluciones a los clientes. Lo que vemos es que la relación entre partners ya no es jerárquica, basada en diversos tipos de contratos, sino que la mezcla es mucho mayor".

Esta nueva realidad ofrece una clara oportunidad de desarrollar negocio no son con Avaya, sino alrededor de Avaya. En este sentido, Moubarak añade que "ya no se trata de cuánto puedes obtener por implementar soluciones de Avaya, sino qué negocio puedes obtener integrando soluciones y servicios alrededor de la tecnología de Avaya, porque en un escenario complejo de una solución avanzada, el componente de Avaya podría estar en torno al 30 o el 40 por ciento del total, lo que supone una gran oportunidad para los partners. La oportunidad no está en integrar y soportar nuestra solución, sino en ofrecer una solución completa al cliente".

Oportunidades en diferentes verticales

En este escenario, quisimos saber en qué segmentos verticales cree Avaya que hay oportunidades para los partners. En opinión de Moubarak, "en todos los segmentos verticales. Como puede verse en los diferentes ejemplos que hemos traído a GITEX, nuestros partners pueden personalizar las soluciones sobre nuestra

tecnología en todo tipo de segmentos verticales, porque la automatización y la experiencia de usuario son requisitos que afectan a todos los mercados hoy en día. Todas las industrias están cambiando y todas lo hacen alrededor de la experiencia de usuario, y mientras esto siga siendo así, seguiremos teniendo oportunidades".

Sin embargo, estas oportunidades solo estarán disponibles si los partners entienden que deben evolucionar su modelo de negocio. Si perseveran en un modelo tradicional, "estarán en problemas, es una cuestión de tiempo. ¿Cuándo? Dependerá de cada mercado, de cada país. Ellos son los que deben liderar el cambio. Deben poner el foco en los clientes, pero no solo en los tradicionales, sino también en los nuevos, porque hay muchas empresas que surgen nuevas, con un nuevo modelo en mente, no sujetas por el legacy, y estas empresas pequeñas de hoy son las grandes empresas del futuro, así que hay que empezar a pensar en ellas para preparar el futuro". it

Enlaces relacionados

- Avaya
- Avaya en GITEX Technology Week 2017

nilox

E-BIKE

MADE IN ITALY

Descubre las nuevas e-bike de Nilox, ¡Perfectas para desplazarse por la ciudad! Próximamente en Esprinet!

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**

Los nuevos terminales coinciden con la llegada de una nueva versión de EMUI

Huawei apuesta por la Inteligencia Artificial en su Huawei Mate 10

Huawei ha presentado en Munich los que pasan por situarse como los nuevos buques insignia de la compañía, el Mate 10 y el Mate 10 Pro, donde prima la apuesta por la Inteligencia Artificial, de la mano del procesador Kirin 970. La compañía ha confirmado la disponibilidad del Mate 10 el 2 de noviembre en los primeros países, incluidos España, con un precio de 699 €, muy lejos de los precios de otros modelos de gama alta anunciados recientemente.

Miguel Ángel Gómez (Shenzhen -China- y Munich)

La nueva propuesta de Huawei para la gama alta, los Huawei Mate 10 y Mate 10 Pro, si bien solo el primero de ellos llegará a España el mes que viene, se centra en convertir un dispositivo “smart” en “inteligente”, aprovechando la potencia que ofrece la conjunción del procesador Kirin 970 y el nuevo EMUI 8.0, sin olvidar otros aspectos ya presentes en la familia Mate, como la cámara Leica Dual o la batería de larga duración.

Tal y como ha recalcado Richard Yu, CEO de Huawei Consumer Business Group, se trata del primer móvil “con unidad de procesamiento neural”, lo que da comienzo a una nueva era de smartphones “inteligentes”. Una inteligencia que busca, por una parte, mejorar la experiencia de uso y, por otra, potenciar el rendimiento del dispositivo.

La base de estos dispositivos es el procesador Kirin 970, dado a conocer durante la pasada edición de IFA. Se trata, como ya hemos publicado anteriormente, del primer chip con una unidad dedicada de procesamiento neural (NPU). Kirin 970 cuenta con tecnología de fabricación en proceso de 10 nm de TSMC, y se compone de una CPU ARM Cortex de ocho núcleos, una GPU Mali G72 de 12 núcleos que se equipa en un chipset por primera vez, y la primera NPU diseñada específicamente para un dispositivo móvil. Además, cuentan con un procesador de imágenes dual para mejorar la fotografía en base a Inteligencia Artificial. La

NPU y la arquitectura de procesamiento móvil HiAI de Huawei incrementan el rendimiento en un 25% y mejoran eficiencia energética hasta en un 50% en determinadas tareas.

A partir de la nueva tecnología Huawei FullView Display, Huawei Mate 10 ofrece una pantalla de 5,9 pulgadas, con un formato de 16:9, marcos muy reducidos y compatibilidad con el estándar HDR10. Se trata de una pantalla 2K (2.560x1.440) RGBW HRD, con un brillo de 730nits. Por su parte, el Huawei Mate 10 Pro de 6 pulgadas, cuenta con una pantalla OLED en formato 18:9, con una resolución de 2.160x1.080, y un contraste de 70.000:1.

Ambos dispositivos presentan chasis acabados en cristal 3D, curvados simétricamente en

Inteligencia Artificial Móvil, propuesta de Huawei con smartphones 'que aprenden'

Dispositivos que aprendan del uso y del entorno. Así quiere Huawei que sean sus teléfonos inteligentes, y con Kirin 970 y su NPU (siglas en inglés de Unidad de Procesamiento Neural) se da el paso hacia la Inteligencia Artificial Móvil, que aúna las posibilidades de la IA en el dispositivo y la IA en la nube.

La introducción de la Inteligencia Artificial en los dispositivos les permite entender el entorno y aprender del comportamiento del usuario, y abre la puerta a opciones más avanzadas en aspectos como el procesamiento en tiempo real, la realidad aumentada, la comprensión del lenguaje o la fotografía, que se potencia por el reconocimiento de la escena y el objeto, así como una gestión más eficiente de batería y consumo o un mayor nivel de privacidad.

Kirin 970 se apoya en una CPU de 8 núcleos y una GPU de nueva generación de 12 núcleos. Fabricado con un proceso de 10 nm, Kirin 970 cuenta con 5.500 millones de transistores en una superficie de un centímetro cuadrado. Se trata de la primera plataforma de procesamiento móvil para IA en contar con una unidad de procesamiento neuronal. En comparación con un chipset con una CPU de cuatro núcleos Cortex-A73, la nueva arquitectura de procesamiento de Kirin 970 lo permite ofrecer 25 veces más rendimiento, con una eficiencia 50 veces superior.

Para que la comunidad de desarrolladores pueda aprovechar las posibilidades de Kirin 970, Huawei lo propone como una plataforma abierta para IA móvil, abriendo el chipset a terceros.

El potencial de negocio de 5G – Digitalización de la industria y otras oportunidades

La digitalización industrial a través de 5G podría generar un negocio de 23.300 millones de euros en España en 2026. Los sectores más activos en la adopción del 5G serán energía (utilities), fabricación, seguridad pública y salud. Según este estudio de Ericsson y la consultora Arthur D. Little, a escala global se espera que 5G genere más de 1,2 billones de dólares en ingresos.

"Mate 10 y Mate 10 Pro son los primeros móviles con unidad de procesamiento neural, lo que da comienzo a una nueva era de smartphones inteligentes"

Richard Yu, CEO de Huawei Consumer Business Group

sus cuatro bordes para ofrecer un agarre más ergonómico, y una banda reflectante que contribuye a resaltar la nueva cámara dual Leica. Esta cámara combina dos sensores: uno RGB de 12 megapíxeles y uno monocromo de 20 megapíxeles, que trabajan al unísono con un sistema de estabilización óptica de la imagen y ofrecen el diafragma más luminoso del mundo con f/1.6 dual, un efecto bokeh mejorado por IA y zoom digital asistido por IA. Los nuevos sistemas de reconocimiento de objetos y escenas en tiempo real asistidos por IA, que seleccionan automáticamente los ajustes apropiados en función del objeto y el entorno en el que se realiza la fotografía, son compatibles además con una función de zoom digital mejorado por IA y un sistema de detección de movimiento asistido por IA que permiten realizar retratos más definidos e imágenes de mayor nitidez.

En lo que también se diferencian en es que el Mate 10 Pro cumple con el estándar IP67, de resistencia al polvo y al agua, y el Mate 10 el IP53, de resistencia a las salpicaduras y que, en caso de entrarle polvo, no limita su funcionamiento.

En cuanto al sonido, cuenta con Huawei Easy Talk, que mejora el nivel de la voz, permite hablar en susurros y reduce el ruido de ambiente, además de aprender de la voz del usuario con su uso. En cuanto a la salida de audio, es de 384k/32bit.

Otro elemento que define estos dos smartphones es la batería, de 4.000 mAh, que, junto con un sistema inteligente de gestión de batería y el menor consumo del chip, logra incrementar la autonomía del dispositivo. Es compatible con la carga rápida de 4,5 V / 5A de bajo voltaje, capaz de alimentar el dispositivo desde 1% a 20% en 10 minutos, y 1% a 58% en 30 minutos, un

LANZAMIENTO DE HUAWEI MATE 10 Y MATE 10 PRO EN MUNICH

CLICAR PARA VER EL VÍDEO

Huawei premia la fotografía con smartphones en Next-Image

Huawei quiere seguir potenciando la fotografía en los teléfonos inteligentes y ha decidido crear, en colaboración con el International Center of Photography, unos premios a fotografías hechas con smartphones, junto con otra serie de iniciativas dentro de la campaña Next-Image.

En los últimos modelos de smartphones, Huawei ha mantenido una apuesta clara por la fotografía como una de las puntas de lanza de sus terminales, conscientes de que el incremento de la tecnología fotográfica en los smartphones ha abierto las puertas a transformar la imagen en toda una experiencia visual. Estamos en un momento transformador de la fotografía, definía Changzhu Li, Vice president Handset Business para Huawei Consumer Business Group, quien apuntaba también que cada día se suben a las redes sociales más fotos de las que todos los profesionales hacen en un año.

Por todo ello, y manteniendo la apuesta por la fotografía, Huawei ha llegado a un acuerdo con el ICP (International Center of Photography) de Nueva York para poner en marcha, dentro de la campaña Next-Image, la primera edición de sus galardones anuales Next-Image. Puedes encontrar toda la información en este enlace.

sistema de carga rápida que ha recibido la Certificación de seguridad de carga rápida TÜV, garantizando una carga segura de extremo a extremo.

Los Huawei Mate 10 y Huawei Mate 10 Pro se lanzarán al mercado con la versión totalmente nueva de EMUI, la 8.0, de Huawei, basada en Android 8.0. Las nuevas características incluyen un motor de inteligencia artificial para aprovechar al máximo las capacidades del Kirin 970; un traductor acelerado de IA para ofrecer una traducción interactiva más rápida y precisa para una experiencia de comunicación más fluida; una función de proyección fácil para conectar la nueva serie Huawei Mate a una pantalla más grande; soporte para una experiencia de escritorio completa: ya sea duplicando o ampliando la pantalla del smartphone como un PC.

Además, junto con los dispositivos, Huawei va a comercializar una serie de accesorios, entre los que destacan la cámara EnVizion 360, que permite tomar fotografías de 5K y videos de 2K de 360 grados; batería externa de supercarga de 10.000 mAh y un sistema de supercarga para el coche; un kit magnético para el vehículo; una funda de cuero inteligente; unos auriculares Hi-Res; y Smart Scale, que puede supervisar y analizar información de salud, como el porcentaje de grasa corporal y el índice de masa corporal a través de una aplicación móvil.

Una nueva versión de EMUI

Coincidiendo con el anuncio del Huawe Mate 10, se libera la versión 8.0 de EMUI, la capa de software de personalización de los dispositivos de Huawei que corre sobre Android, y que según explica Christophe Coutelle, VP software marketing de Huawei Devices, “representa un gran salto, además de una clara apuesta para alinearnos con la nueva versión de Android”.

La nueva versión de EMUI, con la vista puesta en la Inteligencia Artificial y el Machine Learning, quiere seguir apostando por el concento Born Fast, Stay Fast de su predecesor, algo que permite a los dispositivos de la compañía,

"La NPU es un paso adelante para diferenciarnos en hardware, pero la principal diferencia está en el software"

Christophe Coutelle, VP software marketing de Huawei Devices

según las cifras que comparte Christophe Coutelle, ofrecer, tras 18 meses de uso, un rendimiento del 85 por ciento de su capacidad global, ofreciendo una experiencia de usuario "como el primer día", señala.

Entre los cambios de esta versión destaca un nuevo sistema de ficheros, algunas funciones concretas como el scrolling de imágenes, o una mejora en la gestión de los contactos, si bien los cambios principales están en las nuevas posibilidades que el chip Kirin 970 ofrece alrededor de la IA. Así, gracias al denominado AI Vision Engine, se mejora el reconocimiento en tiempo real del escenario y la adaptación de los parámetros para una mejor imagen, además de mejorar las imágenes recibidas por WhatsApp.

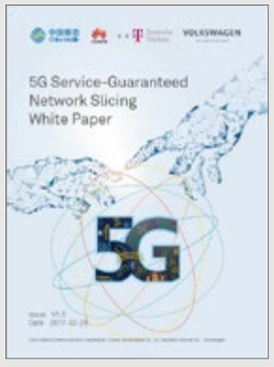
En una línea similar, el AI Experiencie Engine ofrece consejos inteligentes (Smart tips) para mejorar la protección ocular cuando se hace uso del dispositivo en condiciones de poca luz.

Con el AI Apps Engine se abre la API para, por una parte, mejorar el rendimiento de las aplicaciones sobre el nuevo EMUI y, por otro, para permitir a los desarrolladores aprovechar la potencia de la nueva NPU. Un ejemplo de esto es la renovada aplicación de traducción en tiempo real diseñada por Microsoft a partir el uso de la NPU, que viene precargada en los smartphones.

A nivel de productividad, con Easy Projection permite compartir los contenidos del dispositivo con un cable, sin necesidad de una dock, además de eliminar las notificaciones mientras se

¿Qué es la tecnología 5G Network Slicing?

Las generaciones anteriores de redes móviles permitían voz, datos y vídeo, principalmente. Pero 5G cambiará la sociedad y abrirá el ecosistema de las telecomunicaciones a las industrias verticales. Les ayudará a alcanzar una visión de "Internet de todas las cosas" con servicios de conexión ubicua, altamente fiables, y una latencia ultra baja, para un número masivo de dispositivos. La tecnología de network slicing introducida en este documento es una de las capacidades esenciales que permitirá a 5G cumplir con esta visión.



comparte el contenido en una pantalla grande; asimismo, se puede usar el dispositivo como un PC con el modo Mobile PC Experience.

Preguntado por el resultado de las apps en este modo concreto, Coutelle señala que "depende de cada aplicación. Por ejemplo, Office sí está optimizada para este uso, pero, en los casos que no, funcionarían como un simple espejo de lo que ve el usuario en su móvil".

Conviene señalar que el nuevo EMUI 8.0 llegará a dispositivos anteriores, si bien las funcionalidades relacionadas con la IA no podrán ser aprovechadas por los usuarios, al no disponer del procesador Kirin 970.

Aprendizaje del dispositivo

Como hemos venido señalando, el dispositivo aprende con el uso que el usuario hace de él. Sin embargo, esta información "es local, no sale del terminal y, si se cambia de dispositivo no es posible exportar el perfil". Es más, el terminal aprende sobre el uso que se hace del propio terminal, no de las aplicaciones.

Aprovechando la posibilidad de hablar con Christophe Coutelle, quisimos preguntarle por qué los dispositivos de Huawei no cuentan con medidas de seguridad biométricas más allá de la huella dactilar. En este sentido, nos explica que "creemos que la huella es, por experiencia y usabilidad, suficiente. Integrar un sensor para el iris, por ejemplo, encarecería el coste y, además, necesita espacio para su ubicación. No creemos que este reconocimiento del iris ofrezca ventajas sobre la huella dactilar, algo aplicable también al reconocimiento facial".

Pese a que, como señala Coutelle, "Huawei es uno de los fabricantes de dispositivos Android que más rápido entregan las actualizaciones a los usuarios", también añade que "estamos acelerando esta entrega de actualizaciones, sobre todo en el caso de la seguridad".

Quisimos saber también qué papel tiene el software a la hora de que un usuario decida adquirir un terminal u otro. Para este responsable, "tenemos que mejorar el conocimiento en el retail de la importancia de la experiencia de uso. Estamos haciendo muchos esfuerzos, y hemos conseguido hablar del rendimiento, la cámara, la batería… y todo está relacionado con el software. El MPU es un paso adelante para diferenciarnos en hardware, pero la principal diferencia está en el software". it

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- Galardones NextImage
- Huawei Mate 10
- EMUI
- ¿Están tus empleados preparados para el puesto de trabajo digital en tienda?
- Consumo de TI para PYMES
- Índice de madurez digital en las empresas

INVITACIÓN

mcr
feeling technology
www.mcr.com.es

- 20 categorías
- 79 productos nominados
- 44 marcas
- Sistema de votación abierta para clientes

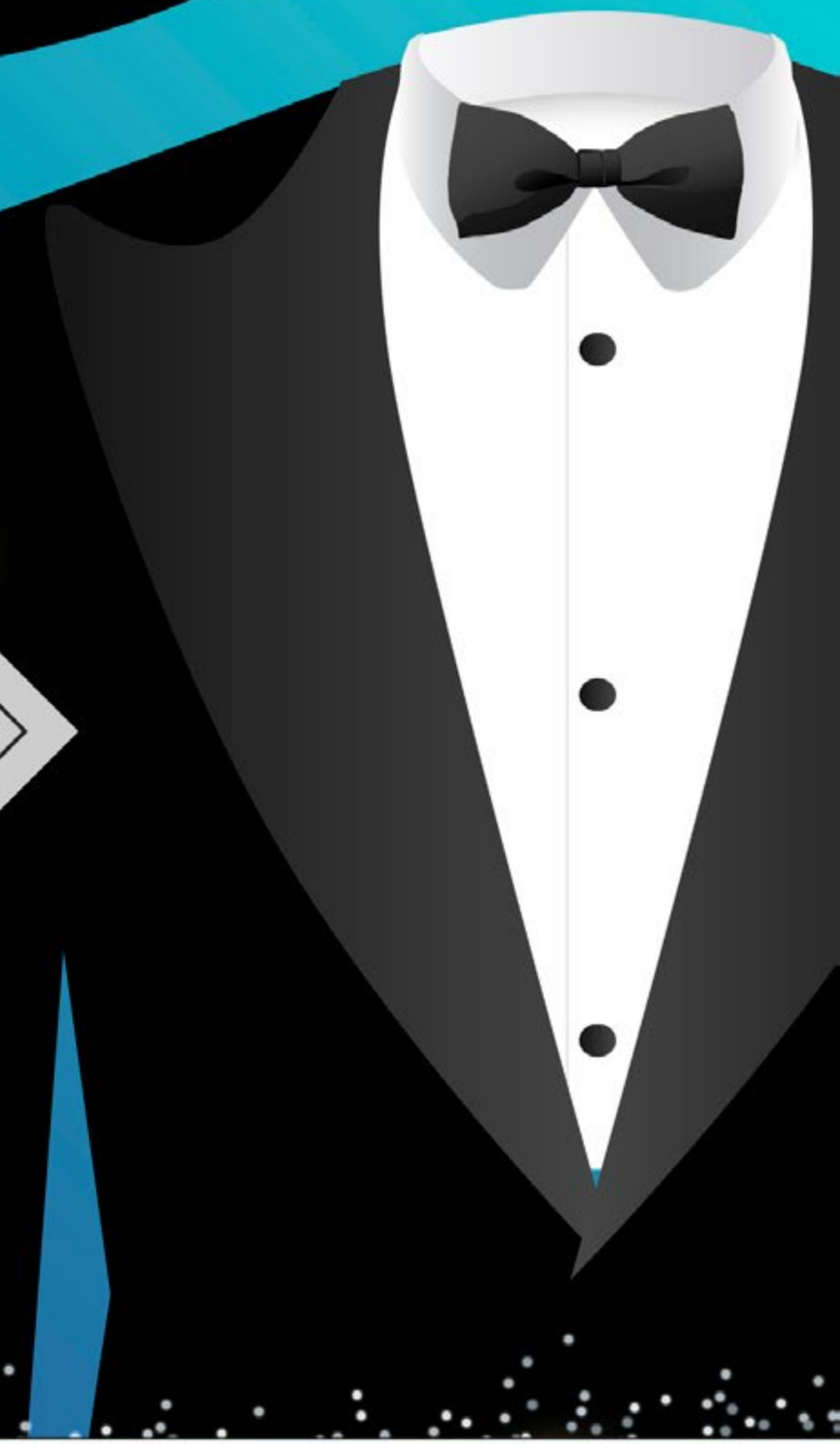
PREMIOS MCR2017

30 de noviembre

20:30h

★★★

OPIUM
MADRID



SAVE THE DATE

SOLO CLIENTES MCR
DATE DE ALTA

Celebramos **10 AÑOS** de premios

Patrocinadores oficiales: SAMSUNG WD SanDisk

Según datos de Context, correspondientes a los nueve primeros meses del año

El canal de distribución TI español crece un 8,7%

A falta del último trimestre del año, el canal de distribución TI español goza de buena salud. Ésta es una de las principales conclusiones que se puede sacar de los datos ofrecidos por Context, que revelan que, de enero a septiembre de este año, la facturación de éste creció un 8,7% obteniendo unos ingresos de 3.149 millones de euros. No obstante, el comportamiento no ha sido igual para cada tipo de partner.

Según datos de Context, el canal de distribución TI goza de muy buena salud. No en vano, entre enero y septiembre de este año, la red de venta indirecta de nuestro país creció un 8,7% en comparación con el mismo periodo del año anterior, generando unos ingresos de 3.149 millones de euros, frente a los 2.897 millones de euros que se obtuvo en los nueve primeros meses del año pasado.

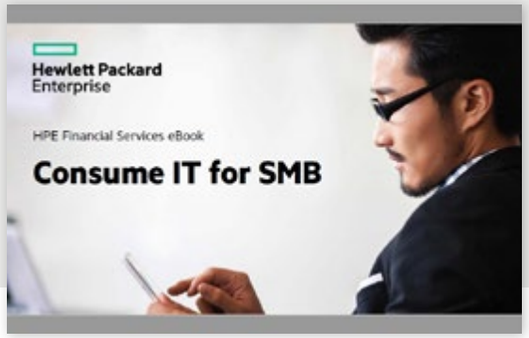
Algunas cifras

Atrás quedaron los años de crisis. Por lo menos eso es lo que se puede pensar si atendemos a los datos proporcionados por la consultora, en los que se destaca que la facturación obtenida por el canal de distribución TI crece. Concretamente, en el primer trimestre de 2016, la red de venta indirecta ingresó poco más de 930 millones de euros, cifra que se incrementó en el segundo trimestre hasta alcanzar los 1.006 millones de euros. En el tercer trimestre se experimentó una caída de ingresos, situándose estos en los 960 millones de euros, para pasar a los 1.404 millones de euros en el último trimestre del año pasado, el mejor hasta el momento.

Si atendemos a las cifras de este año, los tres periodos superaron los 1.000 millones de fac-

Consumo de TI para pymes

La transformación digital es clave para ser competitivos, pero, por lo general, los costes de mantener y renovar la tecnología son demasiado altos para las pymes. Descubre en este whitepaper cómo los modelos de financiación flexibles y de consumo de tecnología de HPE Financial Services pueden ayudar a tu negocio.



El sector TIC y de contenidos creció un 6,8% en 2016

El sector evoluciona favorablemente desde su vuelta al crecimiento en 2014, dejando atrás los años críticos de la crisis.

Así lo revela un avance de las cifras de 2016 que se darán a conocer a finales de año cuando Red.es presente su informe anual sobre el sector TIC y de los contenidos, del que ahora conocemos los grandes datos. Según Red.es, el sector TIC y de los contenidos español facturó más de 105.000 millones de euros, lo que refleja una subida del 6,8% con respecto al anterior ejercicio y confirma la tendencia positiva iniciada en 2015.

De ellos, 88.015 correspondieron al sector de Tecnología y Comunicaciones, que ingresó 88.015 millones de euros, lo que situó el crecimiento en un 7%. Mientras, la cifra de negocio del sector de los contenidos se elevó a 17.000 millones de euros, lo que supone un aumento de casi el 6% si se compara con los resultados de 2015.

Las cifras preliminares apuntan también que este aumento va acompañado de un mayor número de empresas y del aumento del empleo. En este sentido, ya hay más de 33.170 empresas, un 3,3% más que en 2015, y el empleo alcanzó los 471.860 trabajadores, un incremento del 4%.

La cantidad de empresas que operan en el sector TIC son 23.427, un 4% más que en el año anterior, y en el de contenidos 9.749. El primero ocupa a 367.000 personas, mientras que el sector de los contenidos, da empleo a 103.954.

turación (1.051 millones en el primer trimestre, 1.049 millones en el segundo y 1.048 millones de euros en el tercero).

Y si se hace la comparación trimestre a trimestre, los ingresos en el primer trimestre de 2017 crecieron un 13% en comparación con el mismo periodo del año anterior, un 4,3% si lo que se compara son los dos segundos trimestres del año, y un 9,2% en relación al tercer trimestre de 2017 versus el mismo periodo de 2016.

Resultados por tipo de distribuidor

Los datos ofrecidos por Context también desgranan el comportamiento del canal de distribución por tipo de canal. La consultora destaca el buen comportamiento experimentado por los pequeños y medianos resellers, los cuales vieron incrementar un 18,2% su facturación en el primer trimestre de este año, un 2,6% en el segundo y un 11,9% en el tercero.

El canal obtuvo unos ingresos de 3.149 millones de euros, frente a los 2.897 millones de euros que se obtuvo en los nueve primeros meses del año pasado

Los denominados como Retail Chain, es decir, las grandes cadenas de retail, vieron crecer su facturación en el primer trimestre de este año un 5,9%. En el segundo trimestre, la subida experimentada fue del 1,6%, mientras que, en el tercero, ésta alcanzó el 8,4%.

Los nueve primeros meses para los distribuidores empresariales (corporate resellers) han sido dispares. Mientras que estos comenzaron 2017 creciendo a doble dígito (concretamente un 14,3%), los siguientes dos trimestres han seguido creciendo, pero más moderadamente. En el segundo, la facturación de este tipo de partners experimentó una subida del 4,6%, mientras que, en el tercero, el crecimiento fue del 2,4%.

Y si los reselleres empresariales han tenido un año dispar, las ventas de los etailers empresariales se llevan la peor parte a pesar de que en el segundo trimestre de este año vieron incrementar sus ventas un 13,5%. Esta subida no ha paliado las caídas registradas en el primer y tercer trimestre, del 12,2% y el 14,8% respectivamente.

En cambio, los etailers que orientan su negocio al mercado de consumo están registrando un buen año, con subidas del 18,9%, 26,6% y 14,6% en el primer, segundo y tercer trimestre respectivamente.

Por último, las tiendas de telefonía han logrado, en el tercer trimestre, recuperarse. Si éstas comenzaron el año cayendo un 38,4% en el primer trimestre, y un 13,6% en el segundo, han experimentado un crecimiento del 147,9% en los meses de julio, agosto y septiembre de este año.

Áreas de interés

Los datos ofrecidos por Context también desvelan en qué áreas están más interesados los resellers para ser ayudados por los mayoristas. En este sentido, el 40,6% de estos cree que los mayoristas pueden ayudarles a generar negocio y posicionarse en el mercado en el área de Hardware as a Services (HaaS). Por detrás, con un 39,5% se sitúa el segmento de Software as a Service (SaaS), un 28,3% en Internet de las Cosas, un 25,3% en Platform as a Service (PaaS), un 23% en Infraestrucuture as a Services (IaaS), un 22,4% en servicios de impresión gestionados (MPS), y un 16,5% en las casas inteligentes o Smart Home.

Enlaces relacionados

- [¿Están tus empleados preparados para el puesto de trabajo digital en tienda?]
- [Datos del sector TIC y de contenidos en 2016 de Red.es]
- [Índice de madurez digital de las empresas]
- [Estado de la digitalización de las empresas y administraciones públicas españolas]
- [Datos de Context]

DMI
Computer

- 17.000 m² de superficie con capacidad para 12.000 palets
- Amplia cartera de fabricantes y productos
- Solución comercial, logística y técnica global
- 27 años de trayectoria y experiencia en el sector
- Ubicación estratégica en el corredor de Henares
- 4 Delegaciones comerciales: Málaga, Alicante, La Coruña y Portugal
- Servicio de entrega en 24 horas
- Cuidada política de calidad y medio ambiente

3GO · acer · alcatel · AMD · Antec · AOC · ARCHOS · ASRock · ASUS · BLUESTORK · brother · CoolBox · CREATIVE · DELL · DENVER · EPSON · e-star · GAMDIAS · geeks!me · HUAWEI · intel · Microsoft · MK Micro

cellularline · differo · doro · DURACELL · GEMBIRD · Genius · GIGABYTE · Gigaset · gioteck · GOLLA · Hannspree · Hewlett Packard Enterprise · Hisense · HITACHI · (Intenso) · KASPERSKY · Kingston · Lenovo · LG · i-Link · logitech · MEDION · msi · PHILIPS · PNY · PORT · RICOH · Salicru · SAMSUNG · SEAGATE · TEN GO! · THE G LAB · TOSHIBA · tp-link · TRITON · vernee · ViewSonic · WD · weimei · waxter · ZTE

MADRID • Avda.Sistema Solar, 34 (esq. c/Marte) - Pol. Ind, San Fernando • Teléfono: 91 670 28 48 • 28830 • San Fernando de Henares

Tu mayorista de confianza

Los distribuidores de tecnología siguen transformándose y creciendo

El ecosistema de partners se transformará totalmente en 2021

Según IDC, al menos el 30% de las figuras actuales en el canal de partners no existirán en el formato que conocemos hoy. Los fabricantes necesitarán actualizar sus programas de canal, proporcionando los incentivos y habilidades adecuadas para impulsar nuevas oportunidades en la era digital.

Según IDC, las alianzas serán un elemento crítico para el éxito de las organizaciones en 2020. Y es que, las alianzas estratégicas son una forma sencilla y viable de ofrecer alternativas en la creación, ejecución y soporte de la experiencia de cliente deseada, creando valor en un mercado específico.

La dinámica de transformación de los negocios y la economía de la Transformación Digital ofrecen oportunidades excelentes para las alianzas. No obstante, los partners deben emprender una transformación y ampliar las habilidades y capacidades para permanecer competitivos a la hora de resolver problemas complejos de negocio. Por ello, IDC anticipa que, para 2018, el 65% de los principales partners del mercado cambiarán su modelo de negocio para poder adecuar la oferta de servicios de a sus clientes.

La nueva era de la digitalización y la transformación de los negocios hace que todos los tipos de empresas deban de reexaminar y modificar su ecosistema como máxima prioridad. Para 2018, el 49% de los CIO avanzarán en

sus iniciativas de Transformación Digital construyendo lazos entre los equipos de tecnología y las líneas de negocio, impulsando iniciativas de innovación, cambio cultural y nuevas prácticas. Además, en 2017 el 20% de las principales empresas del mercado desarrollarán la habilidad de permitir a los clientes crear su propio servicio, dando el control al cliente de la propia experiencia.

Para soportar todos estos cambios se debe hacer una revisión completa de las operaciones relacionadas con la experiencia de usuario, incluyendo marketing, ventas, proceso de pedidos, desarrollo, entrega y soporte. Los fabricantes necesitarán actualizar sus programas de canal, proporcionando incentivos y formaciones adecuadas para impulsar nuevas oportunidades en la era digital. Asimismo, como la 3ª Plataforma continuará cambiando el ecosistema de partners, los fabricantes deben ser más ágiles para soportar y aumentar las oportunidades en los nuevos mercados especializados.

Según IDC, el ecosistema de partners se transformará totalmente en 2021, y al menos el 30% de las figuras actuales en el canal de partners no existirán en el formato que conocemos hoy. Las nuevas figuras deberán gestionar los siguientes requisitos del negocio:

- Un nuevo modelo de relación, con una experiencia centrada en el usuario, con una estrategia que proporcione una simplicidad y relevancia a las actividades complejas, incorporando mejoras en la seguridad mediante un acceso basado en la nube.
- Mejora de la retención de los clientes y gestión del consumo de los mismos.
- Gestión de la información clave para el negocio, ofreciendo los datos necesarios a los clientes, partners y usuarios internos y gestionando el acceso a la inteligencia de negocio y herramientas analíticas de forma sencilla.
- Compromiso de la dirección para la mejora de la organización, la infraestructura y el soporte.

Según IDC, las alianzas serán un elemento crítico para el éxito de las organizaciones en 2020

Cómo la transformación digital impacta en los OEM

Este documento de IDC examina cómo la transformación digital está cambiando los modelos de negocio de los OEM (fabricantes de equipos originales), y su rol en el suministro de soluciones verticales por parte de proveedores especializados en campos, por ejemplo, como el de los sistemas médicos o la videovigilancia, quienes integran el hardware, el software y los servicios de dichos OEM para construir una solución final.

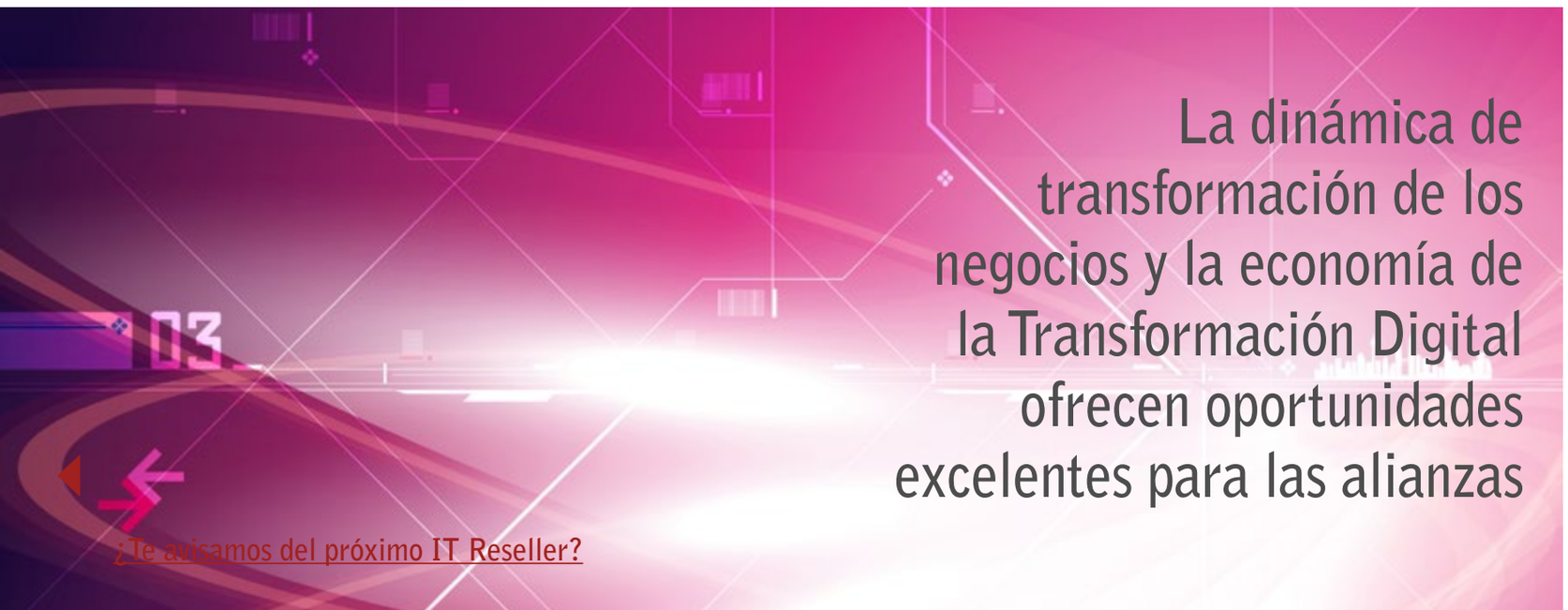
Continuar con el crecimiento

Pero no sólo IDC cree que los partners de tecnología continuarán transformándose. El Global Technology Distribution Council (GTDC) concluyó su 15ª cumbre anual en San Francisco, que este año reunió a un número récord de participantes, entre ellos más de 80 fabricantes y aproximadamente 70 altos ejecutivos de los mayores distribuidores de tecnología del mundo. Los miembros distribuidores del GTDC generan más de 130.000 millones de dólares en negocios anuales de productos y servicios en todo el mundo

La conferencia de este año contó con una amplia gama de oradores, paneles y sesiones temáticas centradas en las principales tendencias del mercado, las mejores prácticas de asociación con distribuidores y una extensa red de contactos con numerosas reuniones individuales programadas como parte de la oportunidad única de conectarse con múltiples CEO y otros distribuidores líderes durante los dos días de la Cumbre.

Destacó la intervención de Tim Curran, CEO de GTDC, que explicó en su presentación que la imagen tradicional de la distribución como especialistas de recoger, empaquetar y enviar ha sido borrada por la continua evolución de la industria hacia servicios y ofertas de productos innovadores, incluyendo la entrada de más de 600 nuevos proveedores entrando en el ecosistema de distribución cada dos años. Curran también señaló que cientos de fabricantes existentes y nuevos en el canal están experimentando un crecimiento. Entre los segmentos de mercado de mayor éxito está el de infraestructura hiperconvergente, que muestra un aumento de las ventas interanuales del 500% durante los primeros siete meses de 2017.

"A pesar de toda la disrupción que atraviesa la industria de la tecnología actual, los distribuidores están demostrando nuevamente su capacidad para adaptarse y crecer", afirmó Curran. "La mezcla masiva de soluciones integrales disponibles por parte de los distribuidores ahora va mucho más allá en el ámbito de los servicios para complementar sus carteras de productos en continuo desarrollo". it



Enlaces relacionados

- El canal y la nube, oportunidades y retos
- Ranking Global de Cloud Computing de la BSA
- Hábitos sobre una TI híbrida
- Barómetro de emprendimiento de éxito en España

it Digital Security

Todo lo que necesitas saber de Ciberseguridad está a un click

Una propuesta informativa compuesta por una publicación digital, una página web para profesionales de la seguridad, así como Dialogos ITDS, Webinars o desayunos de trabajo con los principales referentes del sector.... ¡¡¡Y no te pierdas nuestras entrevistas!!!

Dispositivos de seguridad:
un negocio en el que el canal es clave

La demanda de dispositivos de seguridad va en aumento, a medida que las empresas, grandes y pequeñas, buscan proteger su información con productos avanzados, como cortafuegos de próxima generación y dispositivos de gestión unificada de amenazas. Al lanzamiento de productos que cubren todos los escenarios de amenazas posibles, especialmente el ransomware, se suma la labor de los mayoristas, que están contribuyendo al crecimiento de este segmento a medida que forman y capacitan a los proveedores de soluciones en las tecnologías y exploran oportunidades en mercados verticales clave. De ello hemos hablado con Fortinet, WatchGuard, Ingram Micro y Arrow ECS.

La ciberseguridad es compleja y también lo son las tácticas usadas por hackers para evadir las técnicas de seguridad actuales. Como señala Carlos Vieira, country manager de WatchGuard Iberia, “los hackers están trabajando duro para diseñar malware más sofisticado que nunca. Mediante el empaquetado, el cifrado y el polimorfismo, los cibercriminales pueden ocultar sus ataques para evitar la detección”.

Retos de seguridad

Efectivamente, en la actualidad, las organizaciones de todos los tamaños están cercadas por una ola incesante de malware. Según una reciente encuesta de Fortinet, el 85% de las compañías han sido víctimas de un incidente de seguridad en los dos últimos años. El malware y el ransomware son los más extendidos y los que, tras Wannacry y Petya, han tenido mayor repercusión mediática. Aproximadamente, el 47% de las compañías reconocen haber sufrido este tipo de ataque y aún hoy los perciben como uno de los mayores riesgos a los que se enfrentan.

“Principalmente, el ransomware ha ‘democratizado’ la seguridad informática: cualquier compañía ahora puede ser objeto de un ataque que perjudique gravemente su cuenta de resulta-

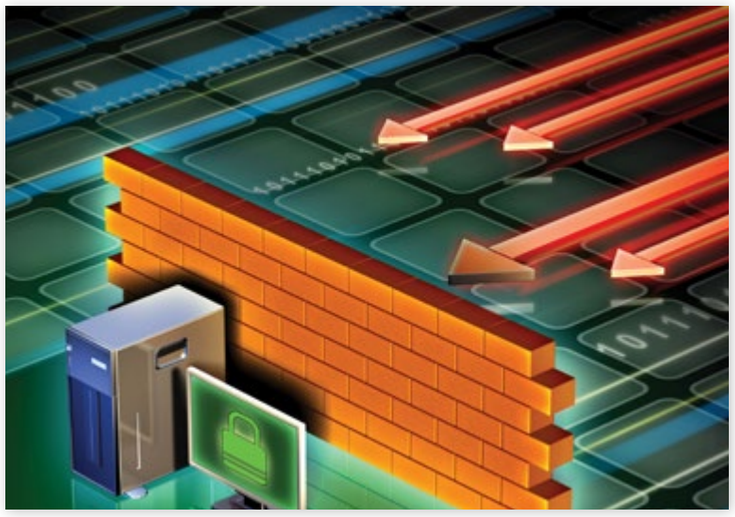
Oportunidad para el canal

El de la seguridad es un mercado interesante. Prueba de ello es el cada vez mayor crecimiento en el número de resellers que incluyen los dispositivos de seguridad en su oferta y la entrada de grandes compañías globales en este entorno. "Aunque aún hay mucho camino por recorrer, estamos encontrando una mayor demanda e interés por parte de los partners, que miran más a la seguridad como alternativa para ofrecer valor a los clientes, así como para complementar el círculo de negocio", afirma Carlos Vieira, de WatchGuard.

Se trata de un mercado muy atractivo para el canal por los siguientes motivos:

- Es una alternativa o una oportunidad para completar el círculo de la infraestructura de TI del cliente, abarcando los 360º de un proyecto. Cada vez son más los partners de canal que incorporan la seguridad a su oferta, y esto es porque ven oportunidades de negocio.
- Permite aportar servicios de valor añadido: formación, soporte, consultoría, instalación, etc.
- Se trata de un sector que genera beneficios y permite fidelizar a los clientes.

Para Antonio Anchustegui, de Ingram Micro, "los márgenes son saneados y más importantes que la media del sector. La proporción asociada de servicios puede superar el 50% del negocio, que además es recurrente, lo que sitúa al partner en una posición estratégica en el cliente final al conocer su seguridad con todo detalle. Al tener actualizaciones frecuentes hay oportunidades frecuentes de interactuar con el cliente asegurando el control de la cuenta, y existe la posibilidad de expandir el negocio sin incrementar proporcionalmente recursos gracias a las consolas multidispositivo".



dos y su actividad", declara Antonio Anchustegui, business manager Virtualization, Security & Networking en Ingram Micro.

Para Sara Crespo, channel account manager de Fortinet Iberia, "la difusión y repercusión de este tipo de ataques hace que la importancia de la ciberseguridad dentro del nuevo ecosistema generado por la transformación digital sea cada vez mayor e implique más eslabones de responsabilidad e inversión dentro de las compañías, especialmente teniendo en cuenta que el 80% de los usuarios afirma que no volvería a colaborar con una empresa si ha sufrido una violación de sus datos personales".

Por su parte, José Luis Paletti, security presales engineer en Arrow ECS, afirma que "el tipo de amenazas ha ido evolucionando y, si bien hace unos años, bastaba con motor de antivirus basado solamente en firmas, hoy en día es necesario elementos de análisis dinámico, como, por ejemplo, tecnologías de sandboxing que sean capaces de encontrar ataques basados en vulnerabilidades y que vengan por diferentes medios".

Junto con el creciente panorama de amenazas, un importante dinamizador de este mercado está siendo el Reglamento General de Protección de Datos (GDPR), ya que provoca que el consejo de dirección de cualquier compañía se vea claramente implicado en la estrategia e inversión en seguridad.

Confianza digital en las empresas

Este estudio, del ONTSI en colaboración con INCIBE, examina los activos tecnológicos y de información de las empresas, así como el modelo de gestión de seguridad de dichos activos, la preparación de las empresas en materia de seguridad TIC, las herramientas y medidas de seguridad que implementan en el desarrollo de su actividad, los incidentes y sus consecuencias desde el punto de vista del negocio y el comportamiento de las empresas en materia de privacidad (protección de datos personales) y transacciones electrónicas.

"La llegada del nuevo Reglamento General de Protección de Datos no es una amenaza en sí, pero su obligado cumplimiento supone que la revisión y actualización de las políticas y medidas de seguridad. Todo esto hace mover al mercado y, por supuesto, hace que las empresas sean cada vez más conscientes de la necesidad de implementar no sólo medidas de seguridad acordes a los nuevos tiempos, sino renovar sus infraestructuras", apunta Carlos Vieira, de WatchGuard.

El cumplimiento normativo se une a los retos a los que debe hacer frente cualquier organización, entre los que destacan la falta de visibilidad, que hace que muchas veces no se detectan las brechas de seguridad; la falta de personal cualificado, y la creciente complejidad de la arquitectura. Todo ello hace que la seguridad TI reciba cada vez más atención por parte de los directivos de cualquier tipo de organización, y aumente la demanda de profesionales y soluciones preparadas para dar solución a un nuevo entorno en el que tanto el marco regulatorio como las consecuencias derivadas de un ciberataque convierten a la seguridad en algo inherente al desarrollo diario del negocio.

UTM como motor de crecimiento

Conscientes de todos estos retos, las empresas han comprendido la necesidad de protegerse apostando por dispositivos de seguridad dedicados, de ahí que este mercado no haya parado de crecer ni en los peores años de la crisis. Los últimos datos de IDC, correspondientes al segundo trimestre de este año, revelan que, a nivel mundial, el mercado de dispositivos de seguridad experimentó un crecimiento positivo en ingresos del 9,2%, hasta los 3.000 millones de dólares, mientras que las ventas también crecieron un 7%, alcanzando las 706.186 unidades.

"Ganan peso con rapidez los partners de servicios de seguridad gestionados"

Carlos Vieira, country manager de WatchGuard Iberia

En lo que respecta a España, se trata de un mercado maduro, pero en crecimiento constante, con una demanda de soluciones al más alto nivel, que ofrezcan no solo protección reactiva sino visibilidad y remediación de la manera más automatizada posible. “En nuestro país hay un nivel de conciencia alto en cuanto a la importancia de la seguridad y la necesidad de evolucionar a medida que las amenazas van surgiendo. El hándicap suele ser el presupuesto, que condiciona en muchas ocasiones la adaptación”, comenta José Luis Paletti, de Arrow ECS.

Dentro de este mercado, el segmento de dispositivos de gestión unificada de amenazas (UTM) es uno de los motores de la tendencia de crecimiento, según IDC alcanzando un volumen de ingresos récord de 1.600 millones de dólares y un crecimiento interanual del 16,8%, el mayor crecimiento entre todos los segmentos del mercado. El mercado UTM representa a nivel global más del 50% de los ingresos del mercado de dispositivos de seguridad.

Las pymes impulsan la demanda

Si bien las grandes empresas han sido históricamente el principal objetivo de los ciberataques, las pequeñas y medianas empresas son ahora las más atacadas, razón por la cual se han convertido en un importante motor de crecimiento en el mercado. Los dispositivos de seguridad, como los UTM, pero también los cortafuegos de próxima generación que tienen una mayor funcionalidad, están siendo implementados cada vez más por las pymes para prevenir ese tipo de incidentes, sino quieren arriesgarse a perder su negocio como resultado de un ataque.

“Para las pymes el malware presenta desafíos de enormes proporciones, ya que enfrentan las mismas amenazas que las empresas más grandes, pero con menos recursos a su disposición”, afirma Carlos Vieira, de WatchGuard Iberia. “Todavía encontramos un alto porcentaje de compañías que tienen dispositivos y sistemas obsoletos o muy básicos que deben actualizar, especialmente entre las pymes”.

Por su parte, Sara Crespo, de Fortinet Iberia, destaca la mediana y pequeña empresa y los entornos distribuidos como aquellos en los que este tipo de solución encaja de forma natural en sus necesidades, señalando que, “entre los aspectos más valorados por los usuarios cabe destacar la flexibilidad, la reducción de costes por consolidación, la simplificación en la gestión y la integración completa de las piezas críticas en seguridad”.

Respecto a la tecnología UTM, Carlos Vieira, de WatchGuard, explica que ésta “empezó siendo muy valorada en el ámbito de la pyme y las empresas con oficinas distribuidas, y hoy hasta las grandes corporaciones cuentan con ellos. Todos los sectores verticales ya disponen de UTM y han comprobado cómo esta tecnología les encaja y que les permite seguir con sus procesos de evolución y adaptación a los nuevos tiempos”. José Luis Paletti, de Arrow ECS, añade que, si bien, “históricamente los UTM han sido productos más enfocados a pequeña y mediana empresa, el mercado ha cambiado, y hoy por hoy este tipo de dispositivos, se han ido adaptando a nivel corporativo, existiendo modelos también para gran empresa, incluso carrier class”.

Por su parte, Antonio Anchustegui, de Ingram Micro, explica que, “hasta 200 o 300 puestos, el UTM es la norma, por su eficacia, coste y sencillez en la gestión. La disponibilidad de pago por uso, el tener una gama completa que cubra

> “Lo más habitual es encontrar partners que dan valor añadido al producto”
>
> José Luis Paletti, security presales engineer en Arrow ECS

segmentos de detección y prevención de intrusiones y de redes privadas virtuales (VPN) experimentaron un descenso.

Canal como asesor experto

El mercado de la seguridad es complejo y la prescripción y correcta aplicación tanto de soluciones como de políticas es esencial a la hora de contar con una correcta protección. No en vano, una reciente encuesta de WatchGuard Technologies realizada a sus partners, desvela que un 45% de los revendedores creen que menos de la mitad de sus clientes cuentan con

> "Los socios de canal se convierten en uno de los puntos de confianza de los responsables de las compañías"
>
> Sara Crespo, channel account manager de Fortinet Iberia

cualquier necesidad, el adaptarse tecnológicamente a nuevas necesidades, un throughput suficiente para aprovechar las nuevas líneas, y un modelo de negocio rentable, son lo más demandado por los partners, que al final son los que eligen la tecnología de los clientes finales en estos entornos".

Otros segmentos que también tiran del mercado son los cortafuegos de próxima generación (NGFW) y los dispositivos de gestión de contenidos, que también tuvieron subidas del 9,5% y del 6,4%, respectivamente, mientras que los recursos adecuados para administrar adecuadamente las alertas de seguridad entrantes, y el 63% no cree que la mayoría de sus clientes entienda la diferencia entre los UTM y los NGFW.

Casi el 80% de los resellers encuestados no cree que sus clientes se preocupen por las diferencias existentes entre las dos categorías de dispositivos, y sólo quieren saber que su negocio está protegido por las últimas soluciones de prevención de amenazas. Esto sugiere que los clientes de seguridad confían en los

Ciberamenazas y Tendencias. Informe del CCN-CERT, edición 2017

Este informe del CCN-CERT hace balance de los principales ciberincidentes registrados en 2016, los agentes de la amenaza, sus métodos de ataque, las vulnerabilidades explotadas y las principales medidas de mitigación a tener en cuenta a la hora de mejorar la protección. De él se desprende que el ciberespionaje (tanto económico como político) se mantiene como la principal amenaza para la seguridad nacional.

revendedores y en proveedores de servicios de seguridad gestionados y en sus recomendaciones sobre dispositivos y estrategias de seguridad.

Efectivamente, la complejidad de este entorno hace que los usuarios requieran de servicios de terceros a la hora de afrontar con éxito una estrategia de ciberseguridad que cubra sus necesidades de forma adecuada sin impactar en el negocio. De ahí que el papel del canal como prescriptor y asesor experto sea clave en este mercado.

“El papel que juega el canal es clave y crítico, diría yo, pues la labor que realiza de consultoría, asesoría, formación, evangelización, etc. es enorme. Para compañías como WatchGuard, que somos una organización 100% canal, nuestros partners de canal son el núcleo de nuestro negocio y dependemos de ellos para lograr el éxito”, asevera Carlos Vieira, de WatchGuard. “Por tanto, el canal es fundamental y más si hablamos de los partners de valor añadido, especialmente en la parte de preventa de soluciones, el trabajo de concienciación y dimensionamiento para estar al lado de los clientes y ser su apoyo ante cualquier incidente, consulta, etc.”

El canal de distribución es cada vez más especializado y profesionalizado, tanto en el diseño de estrategias adaptadas de seguridad,

como en ofrecer servicios gestionados de seguridad. Y es que, los integradores y proveedores de servicio deben afrontar los cada vez más exigentes y específicos requisitos de los usuarios. Entre los requisitos que el canal de seguridad debe cumplir se encuentra la formación constante, así como la capacidad de comprender los requisitos específicos de cada tipo de usuario ya sea por su tamaño o sector de actividad.

“Los socios de canal se convierten en uno de los puntos de confianza de los máximos responsables de las compañías a la hora de decidir inversiones y estrategias de protección de sus máximos activos, por lo que su conocimiento en profundidad de las últimas amenazas y cómo afrontarlas y adaptarlas de manera eficiente es un requisito crítico”, puntualiza Sara Crespo, de Fortinet.

Partners muy variados

Como mercado en crecimiento, con importantes barreras de entrada debido a los requisitos específicos y especialización requerida, la seguridad atrae la atención e inversión de resellers con perfiles muy variados.

La potencial oferta de servicios, incluida la instalación, mantenimiento, gestión, formación, etc., así como la fidelidad que genera en el usuario la confianza depositada en el socio que se ocupa de la asesoría en materia tan delicada como la seguridad, facilita un dinamismo y desarrollo constante en ofertas diferenciadoras por parte del canal de distribución.

“Lo más habitual es encontrar partners que dan valor añadido al producto, aportando su experiencia y conocimiento de los distintos productos. La experiencia es clave, así como la inquietud por adquirir conocimientos sobre nuevas tecnologías aplicadas a la seguridad”, concreta José Luis Paletti, de Arrow ECS.

De la misma opinión es Carlos Vieira, que señala que “todos los partners que añadan valor y

"Los márgenes son saneados y más importantes que la media del sector"

Antonio Anchustegui, business manager Virtualization, Security & Networking en Ingram Micro

tengan conocimiento en sistemas, networking, seguridad, cloud y virtualización, son los que mejor posicionados están a la hora de ofertar soluciones y hacer cross-selling, es decir, que podrán ofrecer una solución complementaria al producto o servicio adquirido, aportando valor. En cuanto a los requisitos de venta, la formación técnica continua se sitúa en la base de todo. También deben tener competencias en el terreno de la venta para detectar oportunidades, ofrecer soporte, etc.".

Por otra parte, aunque la venta online de este tipo de dispositivos es compleja, ya que dificulta la necesaria labor de asesoría al usuario, si bien para soluciones sencillas se trata de una opción que cuenta con cierta demanda de mercado. Un ámbito donde tiene cabida el canal online son los servicios gestionados de seguridad, donde algunos especialistas han sido capaces de desarrollar portales online de auto-aprovisionamiento, gestión y configuración de mecanismos de seguridad.

"Analizando el mercado de dispositivos de seguridad y su distribución, vemos que ganan peso con rapidez los partners de servicios de seguridad gestionados y en el futuro gran parte de estas soluciones se distribuirán a través de ellos", concluye Vieira.

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- El mercado de dispositivos de seguridad crece un 9%
- Cada vez más compañías de seguridad confían en la distribución
- La ciberseguridad afronta el reto de proteger y respaldar el negocio
- El mercado de seguridad TI europeo crecerá un 16% en 2018
- El 83% de los partners citan el ransomware como la gran preocupación de sus clientes
- ¿Están tus empleados preparados para el puesto de trabajo digital en tienda?
- Consumo de TI para PYMES
- Índice de madurez digital en las empresas

Discover the New

Una nueva dimensión para la tecnología

La agilidad y la toma de decisiones basada en datos son dos requisitos de los negocios actuales. ¡Descubre en este nuevo Centro de Recursos cuál es el nuevo estilo de tecnología!

Patrocinado por MICRO FOCUS

Herramientas para potenciar el negocio

Tech Data
Advanced Solutions

¿Te avisamos del próximo IT Reseller?

Noviembre 2017

Herramientas para potenciar el negocio

La división de HPE de Tech Data pone en marcha una serie de iniciativas y acciones continuas, orientadas a potenciar el negocio de los distribuidores. Son acciones que apuntan en diferentes líneas de actuación, desde la parte más comercial con promociones específicas, así como otra serie de iniciativas: webinars, formaciones, soporte técnico para hacer más rentable y fácil el trabajo de los distribuidores.

En concreto, son tres las grandes líneas de trabajo de Tech Data y HPE. Por una parte, la puesta en marcha de la iniciativa de negocio del Ecosistema OEM de HPE, una plataforma orientada a ayudar al canal de distribución a abordar la Transformación Digital de sus clientes.

En segundo lugar, la web de promociones de Tech Data, que ofrece una serie de herramientas y acciones encaminadas a incentivar el negocio del canal alrededor de las soluciones de Hewlett Packard Empresarial, con elementos tales como descuentos especiales, formación o exclusivos programas de incentivos.

En tercer lugar, la promoción de la venta de Aruba Central y otras soluciones de red de la firma, explicando bien qué son, cómo funciona, la sencillez de uso y como ofrecer la mejor alternativa al partner con precios especiales y bundles determinados.

Acelerador de oportunidades: Ecosistema OEM de HPE y Tech Data

Tech Data a través de su división exclusiva de HPE, ha lanzado una iniciativa para potenciar el Ecosistema OEM de HPE, una plataforma orientada a ayudar al canal de distribución a abordar la Transformación Digital de sus clientes ofreciendo un portfolio completo e integrado representado por los principales fabricantes del mercado. Esta iniciativa está arropada, no solo por un sólido catálogo tecnológico, sino por el adecuado soporte comercial y técnico, así como todos los recursos necesarios que Tech Data aporta.

Tal y como puede verse en la página web creada alrededor de este Ecosistema OEM, son varias las ventajas que pueden obtener los distribuidores. La idea inicial de este proyecto es crear y poner en manos del canal soluciones conjuntas destinadas a transformar, proteger, habilitar y potenciar los proyectos de los distribuidores, en base al conocimiento, la innovación y el soporte de Hewlett Packard Enterprise y de la División HPE de Tech Data. Con ello, se pretende acelerar y mejorar la agilidad y la experiencia del usuario en los procesos de Transformación Digital de las empresas.

En cuanto a las ventajas, como decíamos, son principalmente, un único punto de contacto para el distribuidor, tanto para la parte de hardware como de software de la solución; mejorar el servicio a par-

Herramientas para potenciar el negocio

¿QUIERES CONOCER TODAS LAS VENTAJAS Y POSIBILIDADES QUE OFRECE EL ECOSISTEMA **OEM DE HPE Y TECH DATA**?

VISITA ESTA PÁGINA WEB

HPE y Tech Data quieren ayudar a sus clientes en la misión de acompañar y guiar a las empresas en su camino hacia la Transformación Digital

tir de Support Services; acceder a servicios que cubran todo el ciclo de vida de la solución; acelerar la entrega de soluciones; y, además, soporte en castellano, para facilitar el trabajo de los distribuidores.

Las diferentes soluciones del Ecosistema OEM se organizan en cuatro grandes áreas: Transformación, apoyada en una TI híbrida; Seguridad, encaminada a proteger la empresa digital; Productividad, con la idea de habilitar la transformación del puesto de trabajo; y Poder de los Datos, con la vista puesta en potenciar a las empresas basadas en datos.

Pero, ¿qué soluciones se incluyen en este Ecosistema OEM? Las soluciones incluidas en este ecosistema son la que aparecen reflejadas en la imagen incluida en esta misma página.

Enlaces relacionados

- Ecosistema OEM Hewlett Packar Enterprise Tech Data
- Soluciones del Ecosistema OEM

Tech Data impulsa la venta de soluciones de HPE

La web de promociones de Tech Data ofrece una serie de herramientas y acciones encaminadas a incentivar el negocio del canal alrededor de las soluciones de HPE. Descuentos especiales, formación y programas de incentivos, son algunas de las posibilidades que Tech Data ofrece en esta página.

Como parte de las herramientas que la división de HPE de Tech Data dispone para ayudar a los distribuidores en el desarrollo de negocio, la web de promociones y webinars de Tech Data para el canal cuenta con diferentes acciones exclusivas del mayorista que incluyen algunas tales como descuentos en la compra de determinadas soluciones, regalos por la venta de productos de distintas familias, formaciones, financiación, programas de incentivos…

En la página de promociones de Tech Data Azlan con HewlettPackard Enterprise pueden encontrar:

- Un punto único de información a todas las promociones vigentes de HPE y Tech Data
- Calendario de webinars (Negocio y soluciones de Tech Data y HPE)
- Herramientas con la información de los Programas de Desarrollo de Negocio de HPE.

PARA ESTAR AL DÍA DE LAS **PROMOCIONES Y WEBINARS DE HPE Y TECH DATA,**

VISITE ESTA PÁGINA

La web de promociones y webinars de Tech Data para el canal cuenta con diferentes acciones de la mano del mayorista y HPE

Enlaces relacionados

Web de promociones HPE

Tech Data explica las ventajas y sencillez de la gestión de red en la nube con Aruba

Las organizaciones que buscan nuevas formas más eficientes de optimizar sus inversiones de red, así como de mejorar sus operaciones, necesitan soluciones que se adapten a la evolución continua de sus necesidades

La solución de gestión en la nube de Aruba ofrece la combinación de herramientas de interfaz orientadas a las tareas, funcionalidades de configuración granulares y visibilidad de gestión de red con categoría empresarial, todo ello junto con las ventajas operativas y económicas que conlleva un servicio en la nube.

¿TIENES ALGUNA DUDA?

CONSULTA CON JORGE FERREIRO, EXPERTO EN ARUBA DE TECH DATA

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

La solución de red en la nuble incluye Aruba Central, es una solución, que basándose en las ventajas de Aruba Instant, es capaz de ofrecer una gestión cloud centralizada y una serie de servicios adicionales.

Aruba Central permite gestionar desde un punto único todos sus cluster de iAP, además de realizar despliegues de forma sencilla y sin errores gracias a Zero Touch Provisioning, y ofrecer un servicio de analíticas de presencia y uno de invitados con múltiples opciones de auto-registro.

Es una herramienta interesante tanto desde el punto de vista de partners como de clientes. Para los primeros, representa la posibilidad de ofrecer al cliente un servicio gestionado (configuración y monitorización) que, además, nos ofrece informes de manera automática, mientras que, para los segundos, representa desde una gestión sencilla, accesible desde cualquier lugar, hasta ofrecer un acceso de invitados adecuado.

Tech Data y HPE, subrayan el interés de estas soluciones no solo desde el punto tecnológico, sino también comercial, ya que ofrecen promociones especiales y budles específicos a precios muy competitivos.

La apuesta por estas soluciones de Aruba tiene ahora una razón añadida, las nuevas promociones puestas en marcha por Tech Data

Enlaces relacionados

Promociones de Tech Data con Aruba

Antes, un orfanato, ahora, un hogar

En muchas ocasiones, la intención de ayudar, de hacer algo por los demás, está presente, al igual que el compromiso y las ganas de colaborar. Pero hay veces en las que la realidad supera ampliamente lo que nosotros pensábamos y nos damos cuenta de que no basta, de que tenemos que hacer más. Uno de estos casos es de lo que nos habla este mes Samira Brigüech, presidenta de la Fundación Adelias, que nos relata cómo era la situación en Nador hace una década y qué le llevó a poner en marcha la Fundación.

Cuando llegué hace 10 años a Nador para hacer un donativo como una ciudadana anónima, no esperaba encontrarme una tragedia de tal magnitud. Me encontré una docena de bebés abandonados que malvivían en una habitación de 12 metros cuadros. Eran 12 bebés con solo una persona para atendernos y un hombre que se dedicaba con ahínco y con todo su cariño a conseguir alimento para "comprar "un día más de supervivencia para los pequeñitos. Doce bebés hambrientos y desesperados por unos brazos que les dieran el calor de un padre o de una madre. Sin agua caliente ni calefacción, sin poder salir a la calle para recibir unos rayitos de sol por falta de medios y un entorno de tristeza y desamparo que me arrugó el alma durante meses.

Decidí crear la Fundación con otros empresarios, jueces y ejecutivos que pensaron que podíamos hacer algo grande: luchar contra la pobreza infantil. Trabajar con ahínco para que muchos niños abandonados por sus padres, por diferentes razones, pudieran encontrar un hogar en el que crecer sanos física y emocionalmente mientras Asuntos Sociales les buscaba unos padres.

El primer grupo de niños costó mucho sacarlo adelante, trabajamos duro para evitar las secuelas, que la precariedad en la que habían vivido les dejara una huella que no fuera muy difícil de superar.

Dos años después volví con la financiación que me proporcionaron Sanitas, Banco Sabadell, Medtronic y el Boston Consulting Gruop, que se sintieron emocionados y comprometidos en la creación de este nuevo hogar, porque no me gusta mucho la palabra orfanato. Es una palabra descarnada que te hace pensar en la soledad y la tristeza de estar en un lugar oscuro.

Construimos una casa de 200 metros cuadrados con jardín y trabajamos duramente para formar al personal en el cuidado del recién nacido.

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.

adelias FUNDACION



También con el niño abandonado con 3 o 4 años que ya era consciente de que la cosa "se había puesto fea", porque sus padres hacía días o meses que no volvían a buscarle.

Estos niños, antes de estar bajo el amparo de la Fundación, tenían graves problemas de salud, desnutrición y trastornos de la conducta por ausencia afectiva. Sanitas, Banco Sabadell y Medtronic gestionaron el mayor programa de voluntariado corporativo para impulsar la Casa y la gestión responsable de los niños. Más de 150

Colabora con la Fundación, hazte socio y participa en nuestros proyectos contra la pobreza infantil.

La cuenta bancaria de la Fundación:

ES2 2100 6274 32 02000 35801

Decidí crear la Fundación con otros empresarios, jueces y ejecutivos que pensaron que podíamos hacer algo grande: luchar contra la pobreza infantil

personas en el transcurso de 2 años convirtieron la Casa Cuna en un modelo de gestión humana y sanitaria por encima de cualquier expectativa imaginable.

Poco a poco, el boca a boca hizo su trabajo y decenas de familias querían adoptar a esos niños tan bien cuidados y que nada tenían que ver con aquéllos que había vivido en la primera etapa de la creación y que tanto rechazo producían.

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Esta casa está íntegramente financiada y mantenida por la Fundación Adelias desde sus inicios. Nuestra misión es asegurarnos de que este hogar siga permitiendo a niños sanos y niños con discapacidad, tener una vida segura, una alimentación acorde a sus necesidades, los recursos sanitarios adecuados y un ambiente familiar que les ayude en el tránsito a vivir con unos padres adoptivos.

Nuestros niños son abandonados al nacer en un 70% de los casos y el resto nos son entregados por la policía al encontrarles en situación de abandono, normalmente en la calle.

Desde su creación, más de 250 niños han sido recogidos en la Casa y han sido adoptados en unas condiciones excepcionales de salud, física y mental. Los niños discapacitados que no son adoptados o con graves problemas de salud, quedan bajo la tutela de la Casa y son cuidados hasta sus últimos días.

Enlaces relacionados

Fundación Adelias

Los servicios de impresión gestionados han sido una de las claves de la recuperación de este sector

El mercado de impresión crece y ofrece múltiples oportunidades al canal

Si ha habido un mercado que ha sufrido en los últimos años, ése ha sido el de la impresión. La crisis ha golpeado, y mucho, este segmento que ha tenido que transformarse para poder sobrevivir y adaptarse a los nuevos tiempos. Tras una época de caídas, y al igual que ha ocurrido con otros segmentos, el mercado de impresión se ha recuperado gracias, entre otras cosas, a áreas como la impresión 3D o los servicios gestionados.

Noviembre 2017

Las ventas de impresoras se estabilizan. Ésta es una de las principales conclusiones de diversos estudios que corroboran que, a pesar de haber sido uno de los segmentos que más ha sufrido durante los años de la crisis económica, está en recuperación.

Si hablamos de EMEA, los últimos datos de Context afirman que las ventas de equipos de impresión continuaron mejorando en el segundo trimestre de 2017 y registraron un aumento interanual del 4%, en comparación con un descenso del 3% registrado en el mismo período de 2016. Esta mejora se debe, según José Ramón Sanz, responsable de marketing de producto de Brother Iberia, a que "la impresión está muy ligada al ciclo económico. La economía en positivo suele traer adherido el crecimiento tanto de la venta de equipos como el número de páginas que las empresas imprimen: a mayor actividad, mayor necesidad de imprimir".

Un crecimiento que ha tenido lugar principalmente "en los segmentos de impresoras monocromo de menos de 500 euros y de equipos multifunción color, también de menos de 500 euros", destaca Juan Leal, director general de Lexmark Ibérica. "Este incremento en las ventas de productos para grupos de trabajo pequeños está impulsado principalmente por las pequeñas y medianas empresas".

Europa Occidental

Si nos centramos en Europa Occidental, esta región representó casi el 70% de todas las ventas de hardware de impresión en EMEA, y reflejó el desempeño en la región en su conjunto, registrando una mejora significativa con respecto a la caída del 6% del mismo trimes-

"El mercado de pago por uso cada vez genera más curiosidad. El canal es el primer beneficiario de un mayor número de oportunidades"

José Ramón Sanz, responsable de marketing de producto de Brother Iberia

Servicios de impresión gestionados en 2017

Este informe examina las principales tendencias en uso de servicios de impresión gestionados (MSP), un planteamiento que permite a las empresas adquirir las capacidades que requieren, eliminando los costes, complejidad y riesgos de una infraestructura de impresión sin gestionar.

Muchos proveedores de MSP están reposicionando los MSP bajo el abanico de los flujos de trabajo, la automatización de procesos o la gestión del contenido.

tre del año anterior. Las ventas de impresoras multifunción láser registraron un crecimiento interanual del 10%, y fueron en gran parte responsables del incremento general.

"Esto se debió principalmente a las ventas a Alemania, Francia y el Reino Unido", señala Zivile Brazdziunaite, analista de mercado de Imaging en Context.

La venta de multifuncionales representó un crecimiento del 3% en Francia, mientras que en Alemania y Reino Unido se produjo un aumento de dos dígitos en la venta de todas las categorías, en contraste con las caídas de dos dígitos observadas en el mismo trimestre el año pasado. En el Reino Unido, esto se debió principalmente al aumento de la demanda de multifuncionales de inyección de tinta, mientras que la venta de hardware láser representó un crecimiento interanual del 12% en Alemania.

Mientras tanto, las ventas de unidades a Italia y los Países Bajos se contrajeron.

Crecen las ventas, cae el valor

En cambio, si atendemos al último estudio de IDC, este destaca que este mercado, creció, en términos de unidades, durante el segundo trimestre de este año. En total se vendieron 4,7 millones de unidades en Europa Occidental durante el segundo trimestre del año, 173.000 más que en el mismo periodo del año anterior.

A pesar del crecimiento en la venta de impresoras, el valor de mercado cayó un 5,6%. No obstante, los resultados no han sido iguales para todos los segmentos. En el caso de las impresoras de inyección de tinta, la facturación creció un 1,5% (la caída de los ingresos del segmento láser descendió un 6,9%). La caída de la facturación del sector de las impresoras

La impresión 3D, en crecimiento

Según un estudio de Context, a pesar de que el mercado de impresión 3D, sobre todo en sectores como el industrial y el profesional, no ha cumplido las expectativas en los últimos dos años, este año crecerá. Las innovaciones en áreas como la salud dental o el deporte serán claves en el despegue de la impresión 3D.

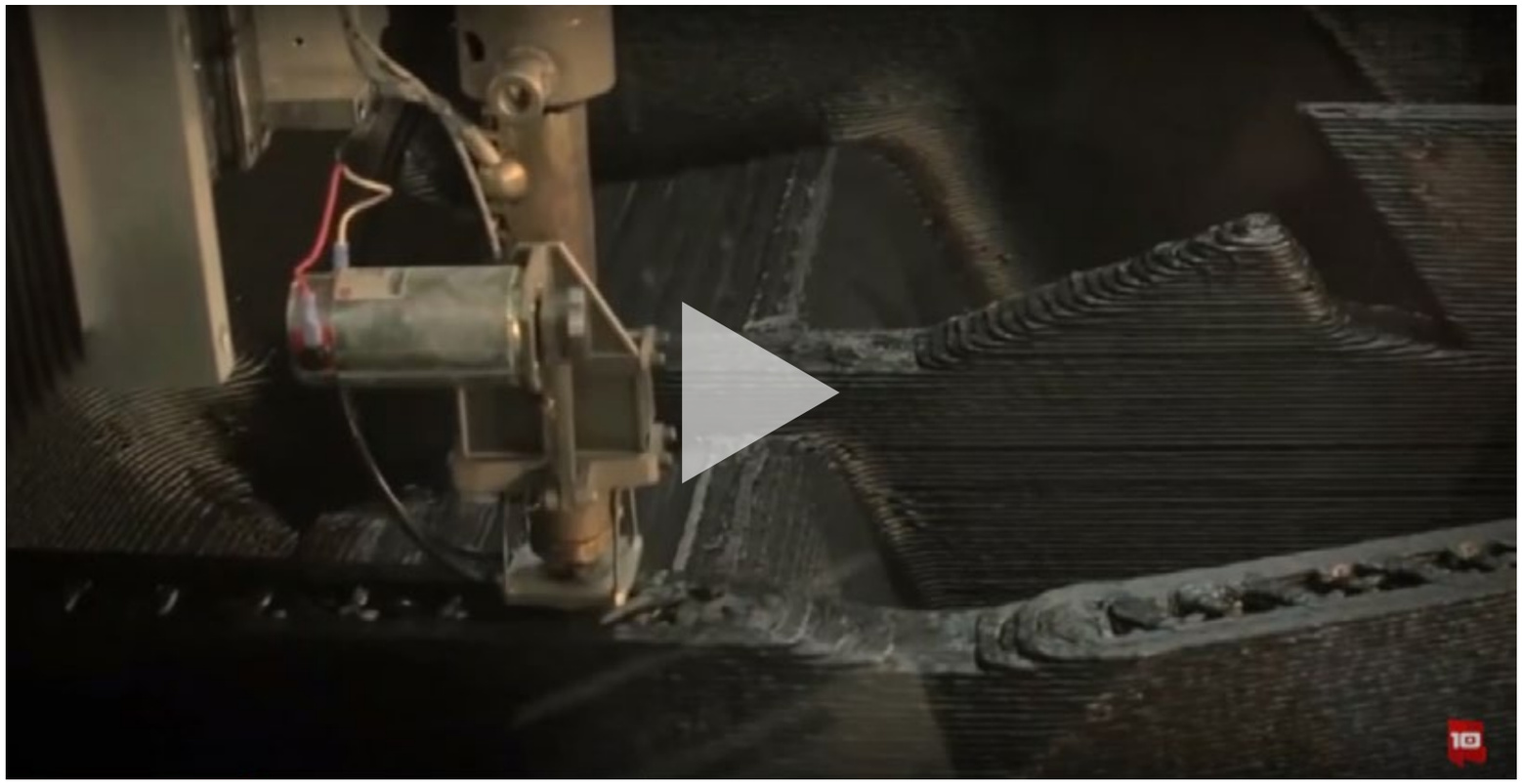
El mercado de impresión 3D continúa representando una oportunidad de negocio para el canal de distribución TIC. Así se desprende del último estudio de Context en el que se destaca que las ventas de impresoras 3D crecerán un 39% este año y un 42% CAGR en los próximos cinco años.

"La demanda de impresoras personales y de sobremesa continúa creciendo en el segmento profesional, en educación y en lo que se conoce como aficionados. También se está empezando a comprobar que existe cada vez una mayor demanda en el área de prototipos profesionales de gama baja", destaca la consultora. Los ingresos de todas las ventas de impresoras experimentarán un crecimiento del 33% CAGR en los próximos cinco años, con el mercado industrial/profesional generando la mayor parte de las ventas. En total, éste representará el 80% del total de los ingresos. En relación al mercado personal y de sobremesa, éste liderará las ventas de unidades.

A pesar de que el mercado de impresión 3D para las áreas industrial y profesional no cumplió con las previsiones, Context pronostica que éste se recuperará este año. Concretamente, y según la consultora crecerá un 16%.

Los motivos del crecimiento será el incremento de las ventas de fabricantes como EnvisionTEC (sobre todo en el sector dental) o el anuncio del uso de Carbon por parte de Adidas, que será utilizada en el desarrollo de sus próximas zapatillas deportivas. Otros jugadores, como 3D Systems, también contribuirán a este crecimiento. Por mercados, el aeroespacial, el médico o la automoción apostarán por el uso de la impresión 3D.

10 COSAS SORPRENDENTES HECHAS CON IMPRESIÓN 3D



CLICAR PARA VER EL VÍDEO

láser (la subida de la venta de unidades fue de un 4,7%) se debe a que los precios de los equipos son cada vez más bajos.

Resultados por áreas

Por áreas, la venta de impresoras de inyección de tinta para empresas experimentó otra caída, continuando con la tendencia de los últimos cuatro trimestres. Las ventas cayeron un 5,9% en el segundo trimestre. Los equipos multifunción cayeron un 5,1% en términos de volumen, aunque su valor se incrementó un 9,7%. Esto se debe al incremento del precio medio de venta (de un 73%) de los equipos A3. El formato A4, por su parte, representa el 75,1% del segmento MFP de inyección de tinta, que, a su vez, representa el 89,8% del total de las ventas del negocio de inyección de tinta.

En total, los equipos multifunción aglutinaron el 80,7% del total de las ventas en Europa Occidental durante el segundo trimestre de este año, lo que representa un leve descenso en comparación con el segundo trimestre de 2016, cuando representó el 81,4%. Los MFP láser y de inyección de tinta aumentaron un 2,9%, mientras que las impresoras láser e inyección de tinta mostraron un comportamiento aún más fuerte con un aumento del 7,9%.

Caen los equipos laser

No obstante, no todas las categorías crecen. En el segundo trimestre, las ventas de periféricos de impresión láser en Europa Occidental registraron una disminución anual del 5% año, impulsadas por la caída de la demanda de impresoras con una sola función, según datos de Context.

Las ventas cayeron en todas las categorías, excepto para los multifuncionales láser. Las ventas de estos dispositivos en el canal mayorista aumentaron un punto porcentual, mientras

#ITWEBINARS

it Digital Security

Jueves, 26 de octubre - 11:00 (CET)

Regístrate en este IT Webinar y conoce las principales claves de la Regulación Global de Protección de Datos, la nueva normativa europea que exige una nueva forma de gestionar y proteger la información que manejan las empresas, y que será de obligado cumplimiento a partir del 25 de mayo de 2018. ¿Están preparados tus sistemas?

Registro

Martes, 28 de noviembre – 11:00 (CET)

Las organizaciones exigen e implementan nuevas soluciones que les permitan agilizar las operaciones, aprovechar nuevas oportunidades de negocio y ofrecer un mejor servicio a sus clientes.
Pero estas nuevas soluciones y tecnologías también requieren que los responsables de TI mantengan la protección de los activos de su organización y de sus clientes, incluso cuando decidan mover el control de la red, las plataformas, las aplicaciones y los datos más allá de las tecnologías y límites tradicionales de su organización.

Registro

que las de impresoras láser continuaron contrayéndose, nada menos que un 11%, como resultado de la tendencia a apostar por los dispositivos multifunción. El descenso fue más fuerte de lo habitual para la temporada, debido a las vacaciones de Semana Santa.

Sin embargo, las ventas de hardware de impresión láser de alta velocidad en el canal mayorista continúan aumentando, a medida que los precios de los dispositivos láser mono y color siguen cayendo. El precio medio de venta de las impresoras láser mono registró un descenso del 3% y se sitúa en la actualidad en los 163 euros, mientras que el precio de los dispositivos láser color es de 418 euros, un 8% menos. En los últimos dos años, las ventas de hardware de impresión láser mono con velocidades de más de 21 páginas por minuto aumentaron en 10 puntos porcentuales, hasta el 66% mientras que las ventas de hardware de impresión láser color con velocidades de más de 21 páginas por minuto se incrementaron en 11 puntos porcentuales, hasta el 47%.

Por países, la mayor caída de ventas se registró en Bélgica, donde disminuyeron un 36%, mientras que en España las ventas de impresoras láser cayeron un 2%. “Los mayoristas de la mayoría de países de Europa Occidental experimentaron descensos en ventas de hardware de impresión”, explica Zivile Brazdziunaite.”La excepción fue el Reino Unido donde las ventas crecieron un 8%, si bien los ingresos descendieron ligeramente. El proceso del Brexit abre una gran incertidumbre en el país, donde el aumento de la inflación ha afectado el gasto”.

“La transformación digital de los procesos de las empresas es uno de los motivos de este crecimiento”

Juan Leal, director general de Lexmark Ibérica

HP lidera el mercado con una participación del 41%, seguido de Brother y Samsung, con sendas cuotas del 18% y 16%, respectivamente. Las ventas de hardware de impresión láser de Brother en el trimestre se incrementaron un 12%, debido a la buena evolución de los dispositivos de gama baja que se venden en los canales de venta de consumo retail y etailer.

Qué pasa en España

España no es ajena a la mejora del mercado de impresión. “En la primera mitad de 2017 las ventas de equipos láser, que son los equipos que están orientados a las empresas, crecieron un 7%, y las ventas en los últimos 12 meses han superado las 500.000 unidades, lo cual supone la cifra más alta de ventas desde 2008-2009, en tiempos pre-crisis”, explica José Ramón Sanz.

Según los datos de Context, España experimentó un incremento de un punto porcentual en el trimestre, impulsado por el sólido desempeño

de los multifuncionales láser. En este sentido, Sanz puntualiza que “los datos de Infosource, que son los que recogen las ventas de los fabricantes, muestran un comportamiento mejor en España que en Europa, donde el mercado se comporta de manera estable”.

Juan Leal se refiere a los datos de IDC para explicar cuál es la situación que está viviendo el mercado de impresión en España. Según los datos de esta consultora, “España creció en unidades un 5% comparado con el año anterior en el mismo período, lo que es un poco superior a los datos de EMEA, que creció un 3%.

El crecimiento en España se debe principalmente a las ventas de impresoras y equipos multifunción color de menos de 500 euros, y también a los equipos multifunción monocromo de más de 500 euros”.

Áreas de crecimiento

España tampoco es ajena a la tendencia europea y son “los equipos multifunción y color los equipos que más están creciendo”, asegura José Ramón Sanz. “En los equipos multifunción se debe a dos motivos fundamentales: por un lado, la necesidad de escanear es cada vez es más frecuente en las empresas y, por otro lado, la capacidad de escanear es un valor añadido del producto con respecto a un equipo que solamente imprime. Esto se ve favorecido por el hecho de que, cada vez más,

Aumentan las ventas de consumibles originales en el canal europeo

Según datos publicados por Context, los ingresos de los distribuidores de consumibles de impresión de fabricantes de equipos originales se han mantenido estables en el primer semestre de 2017, aumentando un 2% interanual en los cinco principales países de Europa Occidental, incluida España. Este crecimiento fue el resultado del incremento en los ingresos de los cartuchos de tinta, y el aumento de los precios de venta tanto de los cartuchos de tinta como de tóner.

Mientras que, en el primer semestre, las ventas unitarias de cartuchos de tinta y tóner se redujeron un 4% y un 2%, respectivamente, los precios medios de venta del tóner crecieron un 4% hasta los 87 euros, y los de los cartuchos de tinta un 8% hasta los 19 euros. La debilidad de la libra frente al euro explica en parte el aumento de los precios, pero los fabricantes también venden cartuchos de tinta y tóner de alto rendimiento, promoviendo la reducción del coste por página tanto para los compradores de impresoras de inyección de tinta de alta capacidad como para los que optan por los acuerdos de servicios gestionados de impresión.

Los precios medios en el canal mayorista aumentaron en los cinco principales países de Europa Occidental, excepto en Alemania, donde los precios de la tinta y el tóner cayeron un punto porcentual. La mayor subida se registró en el Reino Unido, donde los precios del tóner subieron un 13% y los de los cartuchos de tinta un 15%.

Reflejando el esfuerzo continuo de los fabricantes para impulsar las ventas de impresoras de inyección de tinta en el entorno profesional, las ventas de cartuchos de tinta en el canal de resellers para empresas siguen siendo fuertes, mientras que las ventas de los mayoristas a los etailers corporativos continúan aumentando.

La transformación digital en el sector retail

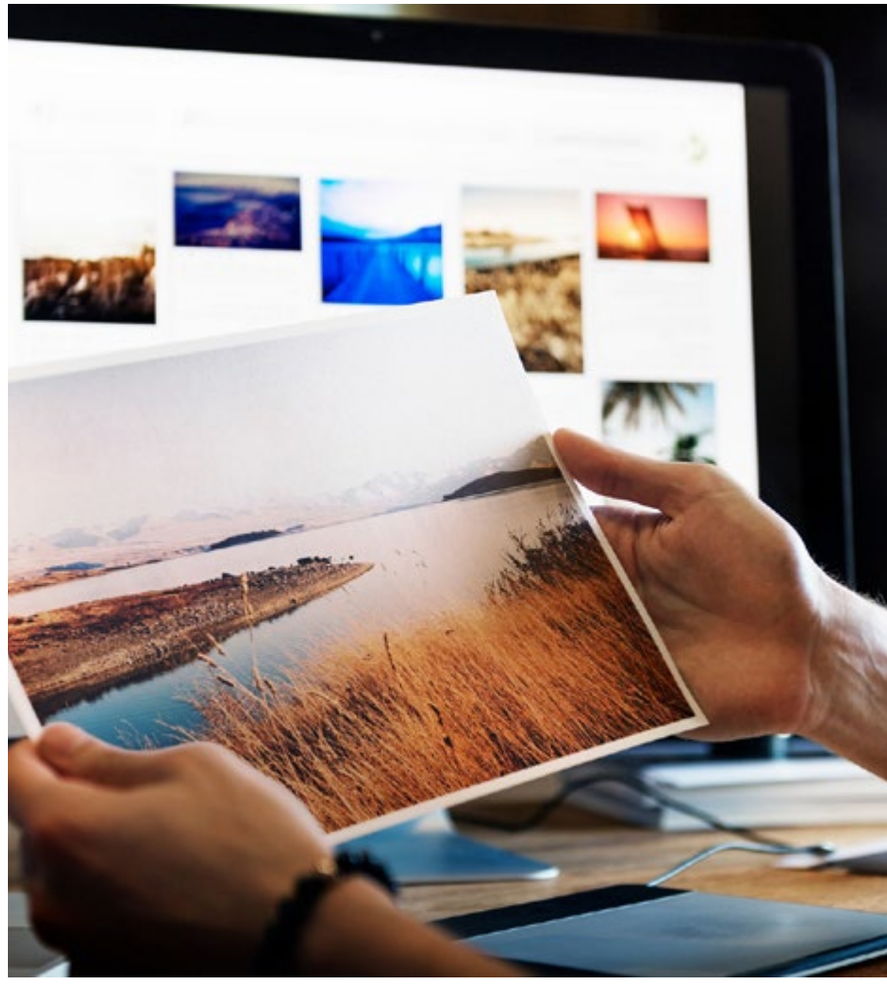
La transformación digital del sector retail viene impuesta principalmente por los cambios en el comportamiento de los consumidores y en la forma y momento de realizar el proceso de compra (consumidores conectados). Entre las tendencias que destaca el estudio figura la evolución hacia modelos "as a Service". En este sentido, las soluciones Retail-as-a-Service (RaaS) muestran un nuevo mundo de posibilidades para que pequeñas empresas puedan potenciar su desarrollo digital. Desarrollar modelos RaaS permite gestionar de forma flexible los picos de tráfico en campañas comerciales así como ofrecer soluciones personalizadas.

el diferencial de precios entre una impresora y una multifunción es cada vez menor".

Los procesos de digitalización que están abordando la gran mayoría de las empresas españolas también están detrás de esta subida. Así lo considera Juan Leal al afirmar que "la transformación digital de los procesos de las empresas es uno de los motivos de este crecimiento, que requiere dispositivos inteligentes capaces de manejar los flujos de datos con soluciones adaptadas a las diferentes necesidades de las empresas".

Y es que, y tal y como reconoce José Ramón Sanz, "aunque en España la tasa de impresoras es superior en ventas a la de las multifuncionales, la cifra está ya muy próxima al equilibrio. Se prevé que en un par de años se venderán más equipos multifunción que impresoras". En los equipos que imprimen a color "esto ya ocurre de hace un tiempo: efectivamente se venden más equipos multifunción que impresoras a color".

Los últimos datos de Context afirman que las ventas de equipos de impresión continuaron mejorando en el segundo trimestre de 2017 y registraron un aumento interanual del 4%



Previsiones para el segundo semestre

Llegados a este punto, ¿se va a mantener el crecimiento en el segundo semestre del año? "En España creemos que durante el segundo semestre va a continuar la tendencia positiva en los productos color, con crecimientos que pueden llegar a dos cifras, mientras que en 2018 se mantendrá estable con respecto a 2017 en el mercado láser color", afirma Juan Leal.

Cómo debe ser el Centro de Datos de Nueva Generación

Lee en este documento cuáles son los 5 principios de la arquitectura que debe guiar la construcción del Centro de Datos de Nueva Generación: la escalabilidad, el rendimiento garantizado, la gestión automatizada, la garantía de los datos y las eficiencias globales. Todos ellos representan un cambio de paradigma que lleva al negocio a la misma velocidad que se mueve la tecnología.

Cómo elegir un sistema de gestión de base de datos (DBMS)

Las organizaciones que utilizan tecnologías ETL de extracción, transferencia y carga de datos y Changed Data Capture (CDC), están luchando para mantenerse al día con la demanda actual de análisis de datos en tiempo real, lo que afecta negativamente a sus oportunidades de negocio y a su eficiencia.
Este estudio de IDC destaca la necesidad creciente de análisis de datos en tiempo real en las organizaciones empresariales actuales.

La empresa digital: transformando las TI con nuevas infraestructuras

Cerca de la mitad de las empresas consideran que es muy importante o crítico transformarse en una empresa digital a corto plazo (antes de dos años). En este sentido, aquellas que más progresan en su digitalización -los líderes digitales-, valoran una infraestructura TI flexible y eficiente y lo clasifican como uno de los tres principales habilitadores, a bastante distancia de otros factores (rapidez en el despliegue, dirección estratégica, integración digital, resultados sobre la experiencia del cliente o procesos internos y aspectos culturales). En España el 63% de los encuestados eligen esta opción. Lee este informe de Interxion e IDC y conoce cuáles son las tendencias en alojamiento de infraestructura TI, los potenciadores e inhibidores de la transformación digital y dela migración a cloud, y cómo superar los desafíos de TI de la transformación digital.

Mejores prácticas para crear software

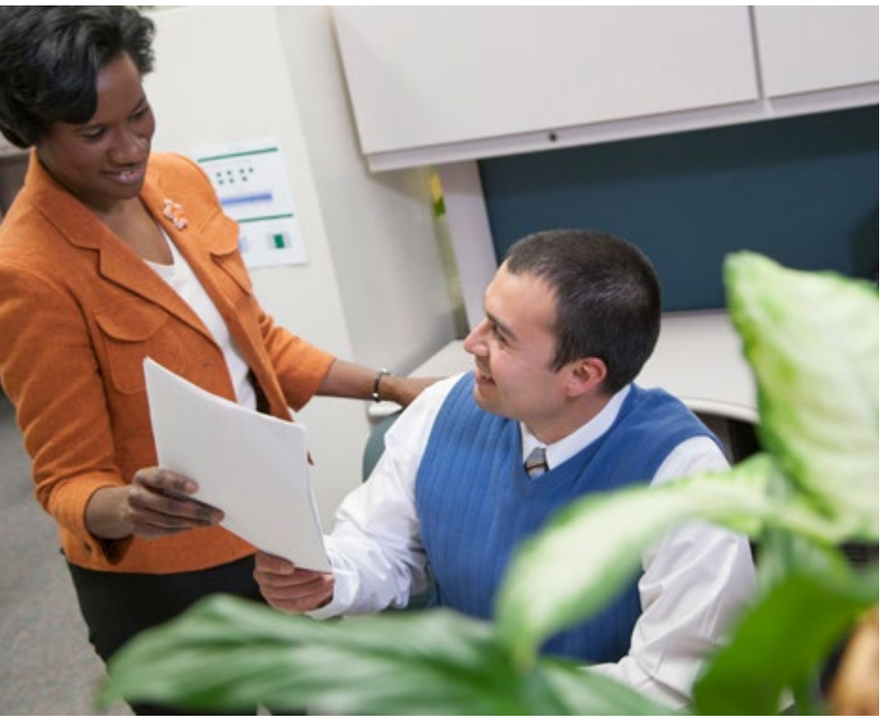
Dominar el desarrollo de software moderno utilizando una fábrica de software moderna es la clave del éxito para las organizaciones europeas. Esta es una de las conclusiones que se presenta en este estudio de Freeform Dynamics, según el cual, un 21% de los encuestados europeos son considerados “Expertos en la Fábrica de Software Moderna”, pues aplican los principios clave de agilidad, automatización, analítica de la información y seguridad. El estudio revela una distancia importante entre estos “Expertos en la Fábrica de Software Moderna” y el resto de encuestados en diversos ámbitos, que van desde los ingresos y beneficios, la dirección ejecutiva o la asunción de riesgos, a la adopción de herramientas y enfoques de software modernos.

La Documentación TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

Según GfK, los servicios gestionados de impresión crecerán un 77% el próximo año



José Ramón Sanz se muestra más comedido al afirmar que “en la medida en que se mantengan las condiciones actuales del ciclo económico, no se prevén cambios en las tendencias remarcadas”.

Servicios de impresión gestionados

Los servicios de impresión gestionados han sido una de las claves de la recuperación de este sector. Así lo demuestra un estudio de Quocirca que indica que cada vez más industrias invierten en servicios de impresión gestionados (MPS), especialmente la industria financiera y la de servicios profesionales, que son las que piensan aumentar más su partida de gasto en este ámbito, un 50% en el caso del sector financiero y un 60% en el de los servicios profesionales.

La producción de documentos suele ser uno de los mayores gastos de una empresa. Muchas no son conscientes de cuánto les cuesta la impresión o de que los costes visibles solo representan un 20% del total. Una investigación de All Associates Group apunta a que una organización media puede gastar hasta 10.800 euros por empleado al año en impresión, incluso antes de sumar el coste de utilizar los servicios de empresas de impresión externas. Gartner añade que las compañías gastan entre un 1% y 3% de su facturación en estos procesos, y no son conscientes de que los servicios de impresión gestionados podrían ayudarlas a conseguir ahorros de hasta el 30%.

Los servicios de impresión gestionados abarcan una amplia oferta de soluciones y servicios de valor dirigidos a gestionar y optimizar el entorno de impresión. Su crecimiento está impulsado por la necesidad de controlar los costes tanto financieros como ambientales, a través de la reducción de consumibles y el uso del papel, así como obtener más control sobre la seguridad de los documentos e impulsar la impresión desde dispositivos móviles.

La importancia de este mercado también queda patente en las previsiones realizadas por GfK. La consultora, a partir de las estimaciones del canal relacionado con la impresión, estima que los servicios gestionados de impresión crecerán un 77% el próximo año. Para el conjunto de 2017, GfK señala que el mercado mayorista de dispositivos y consumibles de impresión cerrará 2017 con una facturación de aproximadamente 500 millones de euros.

Desde GFK señalan que la falta de surtido, la falta de apoyo en marketing y los tiempos de entrega insuficientes son las principales razones para el cambio de mayorista.

“El futuro de la industria del printing pasa por aprovechar tecnologías como cloud, Big Data y gestión documental para aportar nuevos servicios de valor a unas empresas con oficinas ubicuas y empleados en movilidad”, apuntó Jorge Álvarez, managing director de TPS. “Al romper con el concepto de oficina tradicional el sector de la impresión debe enfrentarse a nuevos retos como el cumplimiento con GDPR y la seguridad, el acceso más sencillo a los dispositivos de impresión desde cualquier sitio y dispositivo y la consecución de ahorros y rentabilidad”.

En este nuevo escenario, Antonio Guirau, manager Iberia OPS category lead de HP Inc., re-

Según All Associates Group, una organización media puede gastar hasta 10.800 euros por empleado al año en impresión

cuerda que en un entorno de mayor volumen de datos (40Zb para 2020), más cosas conectadas (25.000 millones de objetos conectados en 2020) y mayores riesgos de seguridad (incremento anual del 48% de las amenazas) hay que evolucionar hacia servicios y tecnologías que ayuden a mejorar la experiencia de los clientes, como por ejemplo con servicios de diagnóstico y resolución remotos, servicios predictivos frente a servicios reactivos, optimización de los viajes de servicio o la oferta de herramientas que se integren con las plataformas de otros fabricantes y proveedores.

Pago por uso

Aunque el concepto de pago por uso no es nuevo, la adopción de la tecnología por parte de las empresas ha hecho que este tipo de modelos cada vez tengan más adeptos entre las PYMES. ¿Los motivos? Al conocido ahorro de costes, se suma la flexibilidad y la disponibilidad de una tecnología imposible de alcanzar de otro modo.

El problema para que estos modelos sean una realidad sigue siendo el mismo que hace unos años. “Es necesario que muchas empresas cambien su mentalidad para que entiendan que es posible beneficiarse de las ventajas que ofrece la tecnología sin necesidad de poseerla”, destaca diversos expertos.

Y es que, y tal y como revela atisa, el pago por uso se ha convertido es una herramienta estra-

Rendimiento digital: la importancia para el retailer

Este estudio recoge datos globales sobre cómo el tiempo de respuesta, la complejidad de la página web y las cambiantes de mandas de los consumidores impactan en los ingresos de las tiendas y distribuidores. El informe recoge datos de España, así como mejores prácticas para este sector de actividad.

vicios cloud representan una gran oportunidad para aquellas pequeñas y medianas empresas que no dispongan de áreas de tecnología internas o que cuenten con infraestructuras sencillas e, incluso, obsoletas, por lo que, más allá de ahorrar costes, de ganar velocidad y flexibilidad, las empresas estarán mejorando su seguridad y ofreciendo una imagen mucho más moderna y actual, acorde a los tiempos que vivimos.

"El mercado de pago por uso cada vez genera más curiosidad. El canal es el primer beneficiario de un mayor número de oportunidades, sin la necesidad de dotarse de recursos especializados o expertos", destaca José Ramón Sanz.

El pago por uso se ha convertido es una herramienta estratégica para todas aquellas empresas que quieran acelerar su Transformación Digital

tégica para todas aquellas que quieran acelerar su transformación digital. Dicho proceso, del que más tarde o más temprano participarán todos los actores del mercado, exige a las organizaciones, mejorar el uso de la tecnología para adaptarse a los nuevos requerimientos de los clientes, pero también de los empleados.

Hay muchos modelos en función de cómo se quiera invertir en tecnología. La nube y los diferentes modelos de explotación de los ser-

"La tendencia de cambio del modelo transaccional al modelo contractual está ganando impulso, motivado por factores como la necesidad de controlar los costes de impresión, la transformación digital y seguridad entre otros. En Europa, un 14% de los dispositivos A4 y más del 90% de los dispositivos A3 se venden bajo algún tipo de contrato", recuerda Juan Leal. "Los servicios de impresión gestionada están creciendo y el canal es una pieza clave en este modelo de pago por uso. En Europa el canal representa casi la mitad de la venta de servicios de impresión y su peso está aumentando". it

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- [El canal avanza hacia los servicios de impresión gestionados]
- [Tendencias de IDC sobre el mercado de impresión 3D]
- [Tendencias de Quocirca sobre los servicios de impresión gestionados. 2017]
- [Calidad y ahorro, las claves para la impresión profesional]
- [Observatorio de competitividad empresarial. La Sociedad de la Información]
- [Consumo de TI para PYMES]

it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Noviembre 2017 - nº 2

Next Generation llega al endpoint

De ciberdelincuentes a empresarios

Ciberseguridad y Cloud, ¿son compatibles?

Y si no cumplo la GDPR, ¿qué?

Ciberseguridad industrial, el nuevo campo de batalla

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

Next Generation llega al endpoint

La seguridad en el endpoint, o sea en cualquier dispositivo que se conecte a Internet, ha avanzado mucho en los últimos años. Los antivirus, que tanta protección ofrecieron durante años, y que siguen siendo una capa importante de la seguridad actual, corrían el riesgo de quedarse cortos a la hora de proteger amenazas, ya que éstas eran cada vez más avanzadas y complejas. Amenazados de muerte hace unos años, los antivirus no sólo sobreviven, sino que tienen gran importancia en la detección de estos riesgos. Para ello, añadir nuevas funcionalidades era cuestión de tiempo y aquí tenemos lo que denominamos Next Generation Endpoint Security. Las nuevas soluciones de seguridad han tenido que avanzar no sólo desde el punto de vista de la seguridad, sino teniendo en cuenta la cantidad y variedad de los endpoint. Ya no sólo hablamos de un ordenador, hay que tener en cuenta los teléfonos móviles, las tabletas, las impresoras o proyectores, el reloj inteligente y, en general, cualquier dispositivo conectado a la red. Todo ello supone un enorme desafío para los responsables de TI y de seguridad de las empresas. Los últimos avances, antes llamados análisis de comportamientos y ahora machine learning, siguen reforzando el posicionamiento de las soluciones de seguridad endpoint.

Este nuevo número de IT Digital Security resume además, los primeros eventos que hemos realizado en nuestra puesta de largo. El primero de ellos se centró en la GDPR. Un webinar que contó con la participación de Kaspersky, Micro Focus, ESET y Netskope, cada uno de los cuales planteó cómo hacer frente a la legislación de protección de datos que será de obligado cumplimiento el próximo 25 de mayo de 2018. Entre las advertencias de los expertos que se trata de una regulación y que por tanto no prohíbe nada, pero lo regula todo y que el tiempo apremia; pero no todo es negativo porque para muchos la regulación supondrá una ventaja competitiva para quienes la cumplan y está forzando a muchas empresas a reevaluar dónde se encuentran sus datos.

La seguridad cloud fue la temática de un desayuno de trabajo que bajo el titulo Ciberseguridad y cloud: ¿son compatibles? Reunió a Kaspersky, Trend Micro, Check Point, Micro Focus y DXC para dejar claro que bien entendida y diseñada la nube no sólo no es una barrera para la seguridad, sino un habilitador.

IT Digital Security
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

IT Digital Security
Rosalía Arroyo
rosalia.arroyo@itdmgroup.es

Colaboradores
Hilda Gómez, Arantxa Herranz, Reyes Alonso
Diseño revistas digitales
Contracorriente
Diseño proyectos especiales
Eva Herrero
Producción audiovisual
Antonio Herrero, Ismael González
Fotografía
Ania Lewandowska

IT User TECH & BUSINESS
IT Reseller TECH&CONSULTING
IT Digital Security
IT televisión

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

En Portada

Next Generation llega al endpoint

Actualidad

Desayunos ITDS

KASPERSKY lab

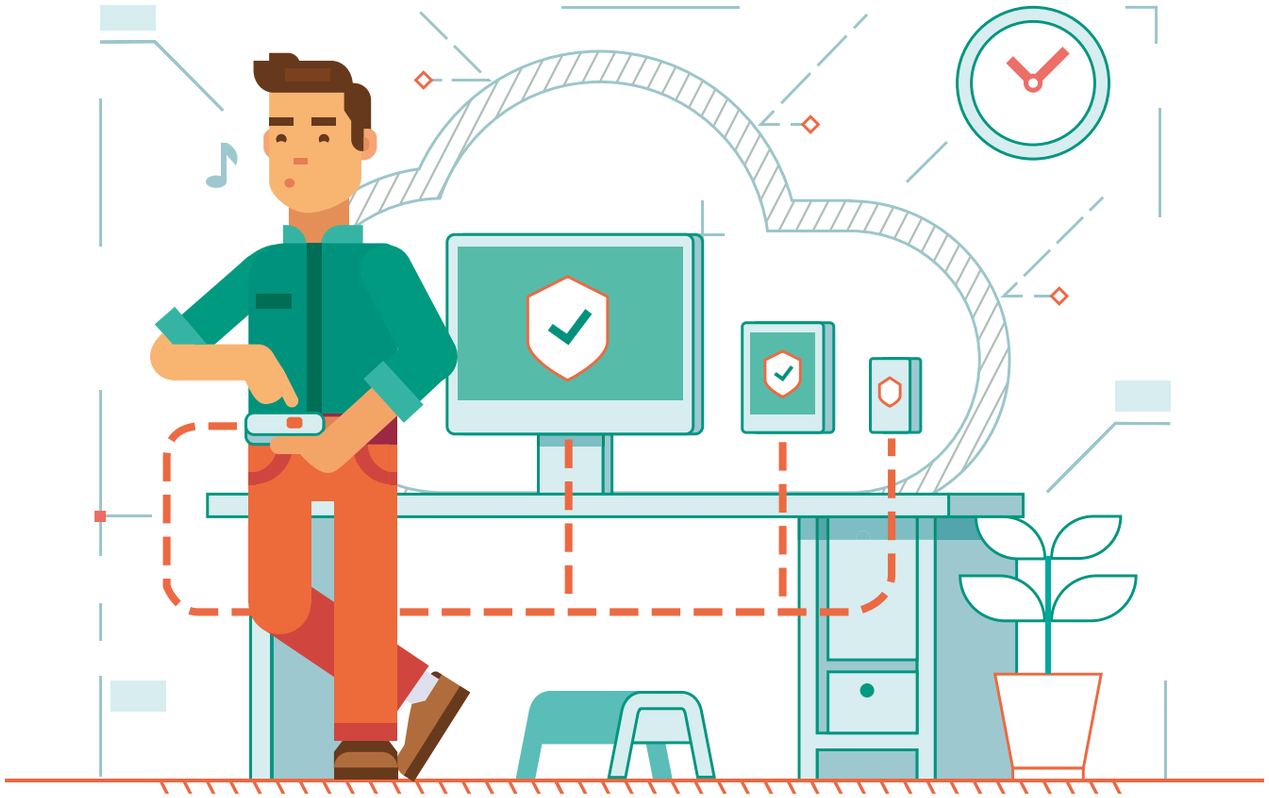
No solo IT

La GDPR incrementará el gasto en seguridad

¿Estamos seguros ante las pruebas digitales?

El DPO a vista de águila

Índice de anunciantes



Deje que fluya su creatividad. Y aleje las ciberamenazas

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

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

cloud.kaspersky.com

Bad Rabbit, el caos vuelve a la red

Bad Rabbit es el nombre con el que han bautizado al nuevo ransomware que ha generado el caos en internet gracias un exploit de la NSA, la Agencia de Seguridad Nacional de Estados Unidos. La nueva oleada de malware de cifrado inició su actividad en Rusia para después extenderse por Europa del este, dejando sin actividad a agencias de noticias, estaciones de tren e incluso aeropuertos.

Bad Rabbit parece apuntar específicamente a las redes corporativas mediante el uso de métodos similares a los utilizados por NotPetya el pasado mes de junio, un ciberataque que echó abajo ordenadores en todo el mundo.

El método de infección inicial de Bad Rabbit se produce a través de descargas en sitios web infectados. El malware está disfrazado como una actualización falsa de Adobe Flash Player que una vez instalada en el ordenador de la víctima intenta propagarse por la red a través de SMB (Server Message Block). Para obtener las credenciales necesarias, BadRabbit viene con una versión de Mimikatz (Hacktool.Mimikatz), una

herramienta de hacking que es capaz de cambiar privilegios y recuperar contraseñas de Windows en texto sin formato. El malware también usa una lista codificada de credenciales predeterminadas usadas comúnmente para intentar adivinar las contraseñas. Además de esto, intentará explotar la vulnerabilidad EternalRomance para propagarse a computadoras vulnerables.

Bad Rabbit vs Petya

Bad Rabbit tiene muchas similitudes con el brote de Petya (Ransom.Petya) de junio de 2017. Ambas familias de malware usan un estilo similar de nota de rescate y emplean un mecanismo de auto-propagación.

Investigadores de Crowdstrike, una firma de seguridad endopoint, detectaron que la DLL (biblioteca de enlaces dinámicos) de Bad Rabbit y NotPetya comparten el 67% del mismo código, lo que indica que las dos variantes de ransomware

Bad Rabbit a escena

Que el ransomware se ha puesto de moda no es nada nuevo. Se ha puesto de moda entre los ciberdelincuentes porque tiene éxito, y tiene éxito porque usuarios y empresas pagan. Y como los rescates se pagan, y además se hacen en bitcoins, una moneda virtual difícil de rastrear, menos trabajo para los malos, que ya no tienen que ir al mercado a vender los datos robados.

El ransomware no es nuevo, lleva décadas entre nosotros, pero las nuevas variedades tienen más capacidad, como su capacidad de propagación, de evasión de las detecciones, de cifrado de los archivos e incluso de facilitar a los usuarios el proceso de pago.

El ransomware tiene tanto atractivo que ya se han desarrollado toolkits para que los menos entendidos puedan lanzar ataques. E incluso modelos de negocio como Ransomware-as-a-Service que han generado muestras tan potentes y conocidas como CryotoLocker, CryptoWall, Locky o TeslaCrypt. Se calcula que CryptoWall ha sido capaz de generar 320 millones de dólares en ingresos.

El de Bad Rabbit, es el tercer gran ataque de ransomware en este 2017 después de los de Wannacry y Petya, y el tiempo dirá si su nombre permanecerá en los libros de historia. Entre los que por el momento ya tiene su podio destaca CryptoLocker, un malware que apareció en 2013 y con el que se inició la era de los ataques de ransomware a gran escala. Cryptolocker se extiende a través de mensajes de spam y se calcula que entre 2013 y 2014 fue capaz de infectar más de medio millón de máquinas.

Considerado como una de las variantes de CryptoLocker, este ransomware se centró en el mercado de videojuegos y en 2016 fue el responsable del 48% de los ataques de ransomware.

A finales de 2015 apareció SimpleLocker, que pasa a la historia no sólo por ser el que considera como primer ransomware para Android, sino el primer ransomware conocido que para el pago utilizó un descargador de troyanos, lo que hizo que fuera más complicado detectarlo. Aunque su origen es de Europa del Este, tres cuartas partes de las víctimas fueron de Estados Unidos.

Cuando se detectó a mediados de 2017, WannaCry fue bautizado como “el peor ataque de ransomware de toda la historia”. Bloqueó la actividad de hospitales, estaciones de radio y se extendió por todo el mundo. Se habla de más de 250.000 infecciones en más de 116 países. Además, formó parte de la primera oleada de ataques que utilizaron herramientas de hacking de la NSA, en este caso EthernalBlue.

Uno de los aspectos más notables de Bad Rabbit es el uso de al menos tres herramientas de código abierto de terceros

Las víctimas de Bad Rabbit son redirigidas a una página de Tor que demanda el pago de 0,05 bitcoins, unos 250 euros

no sólo están estrechamente relacionadas, sino que incluso podrían ser el trabajo de la misma persona u organización.

Ambas amenazas también contienen un componente que se dirige al registro de inicio maestro (MBR) de un ordenador infectado, sobrescribiendo el MBR existente.

Sin embargo, mientras Petya utiliza EternalBlue y los exploits relacionados de EternalRomance para propagarse, además de las técnicas clásicas de propagación de redes SMB, BadRabbit no usa EternalBlue y solo usa EternalRomance junto con la propagación clásica de SMB. En segundo lugar, Petya era técnicamente un limpiador en lugar de ransomware, ya que no había forma de recuperar una clave de descifrado.

Uno de los aspectos más notables de BadRabbit es el uso de al menos tres herramientas de código abierto de terceros. Además de Mimikatz, BadRabbit también usa la herramienta de cifrado de código abierto DiskCryptor para realizar el cifrado, junto con controladores de ReactOS, una alternativa de código abierto para Windows, lo que reduce la cantidad de actividad sospechosa detectable en una computadora infectada.

EternalRomance

Cuando se detectaron los primeros ataques de Bad Rabbit, se creyó inicialmente que el malware estaba utilizando EternalBlue, el exploit que ayudó a extender a Wannacry, pero poco tardaron los expertos en darse cuenta de que no era el caso y que lo que se estaba utilizando en realidad era una vulnerabilidad conocida como EternalRomance, que fue la utilizada para la distribución de NotPetya.

Y de lo malo, lo peor, porque tanto EternalBlue como EternalRomance son vulnerabilidades que fueron parcheadas por Microsoft el pasado mes de marzo, lo que vuelve a poner de manifiesto, una vez más, que la gestión de vulnerabilidades es una asignatura pendiente entre las empresas, y eso a pesar del impacto que están teniendo ataques como los de Petya o Wannacry.

En lo que se refiere a Bad Rabbit, la implementación de EternalBlue se usa para sobrescribir el contexto de seguridad de la sesión del kernel. Eso le permite lanzar servicios remotos e intentar encontrar otros sistemas cercanos a través de las conexiones SMB, para después propagar el ransomware. Recordemos que NotPetya utilizó EternalRomance para instalar la puerta trasera DoublePulsar.

En ambos casos, las acciones son posibles debido a la forma en que EternalRomance permite

El ransomware no es nuevo, lleva décadas entre nosotros, pero las nuevas variedades tienen más capacidades

al atacante leer y escribir datos arbitrarios en el espacio de la memoria del kernel para propagar ransomware.

Pagar o no pagar

Iniciada la Ruta en Rusia, ya ha habido organizaciones de Rusia, Corea del Sur o Polonia que han reconocido haber sido víctimas del malware. Sin embargo, y a pesar de que a Bad Rabboit se le compara con Wannacry y NotPety, el número total de infecciones es bastante inferior. Frente a los cientos de miles de sistemas que cayeron víctimas de esas amenazas, se calcula que Bad Rabbit ha impactado en menos de 300 organizaciones.

Es difícil saber cuántas empresas han pagado. Las víctimas son redirigidas a una página de pago de Tor que demanda el pago de 0,05 bitcoins, unos 250 euros, para descifrar los archivos cifrados. A las víctimas se las amenaza con incrementar el rescate en caso de no pagar antes de 48 horas.

Para el cifrado se ha utilizado DiskCryptor, que es un software de código abierto para cifrado de disco. Las claves son generadas utilizando CryptGenRandom y después protegidas por una clave pública RSA 2048 codificada.

Enlaces de interés...

- La Economía del Ransomware
- Tratando con el Ransomware
- La nueva generación de ransomware ha llegado, ¿quieres conocerla?
- Locky ha vuelto, ¿qué sabes de él?

MICRO FOCUS®

Discover

the New

De ciberdelincuentes a empresarios

Chantaje y secuestro de la información son sólo algunas de las actividades con las que el negocio del cibercrimen se ha convertido en uno de los más rentables. Capaz d generar daños por valor de cientos de miles de dólares en la economía mundial, el cibercrimen se ha profesionalizado y hoy en día funciona como cualquier empresa, con sus horarios, sus inversiones en I+D y la búsqueda de talento.

Lo que empezó siendo poco más que un juego, el robo de calderilla a la compañía de telefónica, se ha convertido en un negocio que supera, en ingresos, al de la droga, que no deja de crecer, y que se ha profesionalizado. Hablamos del cibercrimen, que ha convertido los datos y la información en moneda de cambio. En un negocio rentable.

La evolución del cibercrimen está muy ligada a la propia evolución de internet. A más capacidad de las redes y de los dispositivos, mayores los ataques; cuanta más gente y dispositivos conectados haya, más objetivos. Pura matemática exponencial.

La primera gran oleada del cibercrimen se produjo en los 80, con la proliferación del correo electrónico. La siguiente, en los años 90, coincidió con la evolución de los navegadores; no sólo había muchas opciones, sino muchas vulnerabilidades y los virus se expandían rápidamente. Al principio del 2000 se añadieron a la ecuación las redes sociales, o miles de millones de usuarios exponiendo información personal que los ciberdelincuentes supieron utilizar para realizar robos de identidad. Ahora el cibercrimen es una industria que funciona y genera cientos de miles de millones de dólares cada año.

Historia del cibercrimen

Cuando se habla de cibercrimen y ciberdelincuentes, es casi imposible saber cuándo se produjo el primer ciberataque, el primera atentado contra internet y sus sistemas. Pero sí que hay una serie de hitos que han marcado la historia negra de Internet, hechos que marcaron un antes y un después.

Los hackers más famosos

Evgeniy Mikhailovich Bogachev. Autor de Game Over Zeus y de Cryptolocker, Bogachev es uno de los hackers más buscado del mundo. Mientras que con el primero fue capaz de infectar más de un millón e ordenadores en todo el mundo, con el segundo, un ramsonware, exorsionó a varios miles de usuarios.

El FBI cree que Bogaches es el líder de una banda de criminales y ha ofrecido una recompensa de tres millones de dólares a quien ofrezca información que lleve a su detección

Nicolae Popescu. A este rumano se le considera el cabecilla de una trama que inserta anuncios falsos en webs de subastas que, tras ser adjudicados, nunca llegaban a los ganadores. Estuvo a punto de ser atrapado en una macro operación en la que se requisaron cientos de miles de dólares, armas y coches de lujo, pero de la que Popescu logró escapar.

Kevin Mitnick. Conocido como El Cóndor, es uno de los hackers más conocidos. Fue a partir de los años 80 cuando sus actividades llamaron la atención de las autoridades, y cuando ganó fama. Mitnick hackeó sistemas empresariales, como los de Nokia y Motorola, para robar secretos corporativos. Incluso llegó a hackear a otros hackers. El Departamento de justicia le consideró el criminal informático más buscado de la historia y cumplió más de siete años de prisión. Actualmente se dedica a la consultoría y asesoramiento en materia de seguridad.

"Ya han venido". Eso es lo que le dijo su padre a Michael Calce, un estudiante canadiense de 15 años, cuando abrió la puerta a dos agentes del FBI. Como en la mayoría de las ocasiones, fue la curiosidad la que metió a Calce en problemas, después de encontrarse en Internet con una aplicación de denegación de servicio que le sirvió para lanzar un ataque, el día de san Valentín de 2000, que afectó a eBay, Amazon y Yahoo! Presumir de sus actividades fue lo que colocó a las autoridades tras su pista.

Alberto González es el autor de uno de los mayores ataques de phishing de la historia. Se robaron 170 millones de cuentas bancarias de todo el mundo y su autor fue condenado a 20 años de prisión.

Vladimir Levin centró su actividad en el robo de dinero. Fue capaz, a mediados de los 90, de robar diez millones de dólares del banco Citibank desde su piso de San Petesburgo. No sólo tuvo que devolver el dinero, sino que fue condenado a tres años de prisión y una multa de 250.000 dólares.

Detenido en febrero de 2016, Cracka fue acusado de hackear el correo personal del director de la CIA, John Brennan, del director de la NSA, James Clapper, y del consejero de

ciencia y tecnología de la Casa Blanca, John Holdren. Cracka, quien resultó ser un adolescente británico de 16 años, también fue acusado de publicar en Internet información privada de más de 30.000 empleados del gobierno de Estados Unidos.

Alexsey Belas es el hacker que está detrás de la brecha de seguridad que afectó a Yahoo! en 2014 y en la que quedaron expuesta la información de más de 500 millones de usuarios.

Más que un hacker, Ourmie es un grupo que últimamente se ha vuelto muy popular. Se le acusa del robo de miles de perfiles de redes sociales, actividad que le ha valido más de medio millón de dólares en pocos meses. Son quienes están detrás del hacker de la cuenta de Twitter y Pinterest de Marck Zuckerberg.

Para muchos John Draperg es el primer hacker. A primeros de los años 70 descubrió la manera de estafar a la compañía eléctrica. Sus investigaciones le llevaron a construir una caja que reproducía un silbato que permitía hacer llamadas de larga distancia gratuitas. Publicó la información sobre cómo hacerlo en Internet.

No había acabado la década de los 70 cuando apareció el primer tablón de anuncios electrónico online, convirtiéndose en un método preferido de comunicación entre usuarios de internet. Este sistema permitió el libre, y rápido, intercambio de conocimientos, incluyendo consejos y trucos para hackear ordenadores.

La primera persona convicta por delitos de cibercrimen fue, a primeros de los 80, Ian Murphy, más conocido como Captain Zap. Junto con tres amigos, Murphy hackeó los sistemas de la compañía telefónica AT&T para modificar la hora del reloj que mide los tramos de facturación. De forma que los clientes que llamaron al mediodía se beneficiaron

La primera gran oleada del cibercrimen se produjo en los 80, con la proliferación del correo electrónico. La siguiente, en los años 90, con la evolución de los navegadores

de tarifas reducidas, mientras que a los que esperaron a la medianoche para telefonear a sus parientes lejanos, se les tarificó por hora punta.

El primer virus informático que salió de los laboratorios y tuvo una expansión real fue Elk Cloner. Fue escrito por Rich Skrenta, un estudiante de 15 años, para los Apple II en 1982 y se extendía a través de los floppy disk.

En 1983 se estrena la película Juegos de Guerra, popularizando la figura del hacker. En la película un adolescente hackea el sistema informático del gobierno a través de una puerta trasera hasta casi provocar la tercera guerra mundial.

En 1988 Robert T. Morris, hijo de un científico de Nacional Security Agency, creó un gusano capaz de replicarse y auto enviarse para comprobar la extensión de internet. Infravaloró a la criatura, que fue capaz de infectar a más de 600.000 equipos. Fue juzgado y condenado en enero de 1990 a pagar una multa de 10.000 dólares, cumplir 400 horas de servicio comunitario y tres años de libertad vigilada. Sólo se libró de la cárcel porque el juez consideró que no había "intención de fraude ni engaño" en su 'modus operandi'.

Aunque el ransomware esté ahora más de moda que nunca, fue en 1989 cuando se produjo el primer caso a gran escalad de ransomware. El virus llegó a través de un cuestionario sobre el virus del SIDA y, una vez descargado, mantenía datos informáticos secuestrados, pidiendo un rescate de 500 dólares. En la misma fecha se arresta a un grupo por robar datos del gobierno de los Estados Unidos y del sector privado y vendérselos a la KGB.

Las actividades de Masters of Deception y Legion of Doom, fundados respectivamente Acid Phreak (MoD) y Lex Luthor (LoD), a finales de los 80 llevaron a hablar de las Guerras de Hackers. Ambos grupos andaban a la gresca, bloqueando activamente las conexiones del otro, hackeando los ordenadores y robando datos. Parece que la lucha se inició en uno de esos tablones de anuncios electrónico online que hemos mencionado, un Bulletin Board System (BBS), donde se reunían miembros de ambos grupos.

Sus constantes gamberradas y ciberataques acabaron con la Operación Sundevil, una gran redada efectuada los días 7 y 8 de mayo de 1990 en diferentes ciudades de Estados Unidos por más de 150 agentes del Servicio Secreto y policía local contra el hacking al sistema telefónico y tráfico de tarjetas de crédito robadas (dos de las principales actividades de estos grupos de hackers). El resultado de la operación fue de tres detenidos, 27 órdenes de búsqueda, además de 42 ordenadores y más de 23.000 floppy disk; pero sobre todo fue el gran mensaje que se envió a la comunidad de hackers: No sois impunes.

A Kevin Lee Poulson fue al primer hacker condenado al que se le prohibió el uso de Internet en su sentencia. Se hizo famoso por hackear las líneas telefónicas de Los Angeles y de la radio KIIS-FM, para asegurarse que él sería la persona que tras una llamada ganara el premio de un Porsche. Tras ser detenido fue declarado culpable de los delitos de escuchas ilegales, espionaje electrónico, fraude, blanqueo de dinero y obstrucción a la justicia, y condenado a cinco años de cárcel.

El lanzamiento de la World Wide Web en 1994 permitió a los hackers crear sus propias páginas web donde compartir conocimiento. Precisamente fue el acceso a ese tipo de información lo que le sirvió a un estudiante inglés para hackear el programa nuclear de Corea, la NASA y otras agencias de Estados Unidos utilizando un Commodore Amiga.

El paraíso de los hackers

Râmnicu Vâlcea, también conocido como hackerville, es un pequeño pueblo de Rumanía. Está situado a apenas tres horas de la capital, cuenta con poco más de 100.000 habitantes y su principal fuente de riqueza es el cibercrimen.

Audis y BMW llenan sus calles y aunque nadie sabe a ciencia cierta cuándo se popularizó este tipo de actividad para muchos la revolución de los 90, cuando la gente tuvo la oportunidad de acceder a ordenadores y herramientas más sofisticadas, fue el detonante.

BIENVENIDOS A "HACKERVILLE", LA CAPITAL MUNDIAL DEL CIBERCRIMEN | SINFILTROS.COM

CLICAR PARA VER EL VÍDEO

Ahora dedicadas al fraude online, las organizaciones de cibercriminales de Hackerville son herederos de las antiguas redes del narcotráfico y los asesinatos a sueldo.

Ahora el cibercrimen es más rentable, y también menos peligroso.

Las nuevas generaciones ya no realizan sus actividades a punta de pistola, sino tras la pantalla de un ordenador, con tecnologías que enmascaras sus movimientos y conversaciones hasta hacerles casi indetectables. Se añade que las fronteras, las mismas que en internet crean un mundo más global que nunca, les protegen.

Son la mente brillante del fraude online mientras que los muleros, ciudadanos repartidos por todo el mundo consiguen lavar el dinero enviándolo desde sus cuentas a Rumanía a través de servicios de dinero que, como Western Union, permite hacerlo de forma anónima.

La primera persona convicta por delitos de cibercrimen fue, a primeros de los 80, Ian Murphy, más conocido como Captain Zap

Un año después, en 1995, aparece el primer virus macro, un tipo de virus escrito en lenguaje informático y embebido en las aplicaciones. Al ejecutarse cada vez que se abre una aplicación, es fácil para los hackers extender su creación. Los virus macro se siguen utilizando.

En 1997 un informe de FBI dejaba claro el alcance del cibercrimen al asegurar que el 85% de las empresas de Estados Unidos habían sido hackedas, y que la mayoría ni siquiera lo sabían. De hecho, ese mismo año el Chaos Computer Club hackeó el software Quicken, siendo capaz de realizar transferencias financieras sin que los bancos o sus clientes se dieran cuenta.

Durante el último año de la década de los 90 se produjo la que ha sido una de las mayores infecciones informáticas de la historia. Su protagonista fue Melissa, un virus macro desarrollado con la intención de utilizar cuentas de email para enviar campañas masivas de email. Los daños ascendieron a más de 80 millones de dólares.

A partir del siglo XXI el número y tipo de ataques online crecieron exponencialmente, los ataques de denegación de servicio distribuido alcanzan ya 1TBps y a empresas de todos los tamaños, con los mayores recursos han sido víctimas de ataques que han dejado expuesta la información de miles de millones de usuarios; hablamos de AOL, de Yahoo!, de Sony...

Los hackers han pasado de ser adolescentes que probaban sus habilidades a ciberdelincuentes con horarios y vacaciones, a empresarios que contratan talento e invierten en herramientas y objetivos.

HISTORIA DE LOS HACKERS INFORMÁTICOS [LOS INICIOS] DOCUMENTAL - DISCOVERY CHANEL

CLICAR PARA VER EL VÍDEO

Un negocio bien montado

Se calcula que detrás del 80% de los ciberataques hay una organización cibercriminal, una empresa que funciona como cualquier otra, con sus jerarquías, departamentos y horarios. Parecería, por tanto, que fuera sencilla su detección y detención. Sin embargo, el negocio está muy bien montado.

Igual de importante es que si se quiera hacer algo ilegal, no se tiene que ser un experto, tan sólo hay que saber lo que se quiere y dónde encontrarlo.

Ahí es donde entra la llamada Deep Web, o Dark Web, para algunos el Deep Dark Web, donde las actividades ilegales se ofrecen al mejor postor. Son sitios difíciles de encontrar, a menudo sólo para

> La industria del cibercrimen se ha profesionalizado y especializado. Cada uno cumple su papel para ser más rentables

En primer lugar, los ciberdelincuentes se esconden detrás de un ordenador y han aprendido a hacer uso de las técnicas de hardware y software necesarias capaces de enmascarar sus actividades.

socios y donde se puede comprar un malware, o contratar un ataque de denegación de servicio. En esa Deep Web el malware-as-a-service está a la orden del día, igual que el anonimato.

Enlaces de interés...

- W Cómo defender mi empresa híbrida de brechas y amenazas
- W Todo lo que siempre quisiste saber sobre Callisto Group
- Criptodivisas, el próximo gran objetivo de los hackers
- Locky ha vuelto, ¿qué sabes de él?

Se calcula que en 2016 el cibercrimen costó a la economía mundial 450.000 millones de dólares y que se robaron unos 2.000 millones de registros con información personal. Es una epidemia que se extiende y no es probable que vaya a decaer. De hecho, hay quien ya ha realizado sus cálculos y prevé que para 2019 el negocio del cibercrimen tenga unos costes de hasta 2.100 billones de dólares, y de 6.000 billones para 2021.

Quién es quién

En este mundo del cibercrimen organizado cada uno juega su papel. Se trata de una economía integrada por especialistas, cada uno de los cuales se ha focalizado en una tarea. Están los que escriben los virus y quienes infectan los ordenadores, los que crean redes de botnets con esos ordenadores infectados y los que son capaces de monetizar los datos robados.

Por un lado están los llamados Kinping, que son las personas que buscan especialistas para llevar a cabo sus planes. Estos Kinpings tienen en su equipo administradores encargados de movilizar la fuerza laboral, pagar los contratistas y hacer el trabajo sucio relacionado con la tare de convertir los datos robados en dinero.

Existen también los escritores de exploits kits, que son herramientas que permiten explotar vulnerabilidades de forma automática en el lado del cliente y que cualquier usuario podría utilizar. Quizá el mercado de los exploits kits ya no es el que era, pero estos kits siguen siendo capaces de generar un gran impacto.

Los llamados Pastores de Bots son los especialistas capaces de crear botnets, o redes de bots. Puede utilizar un kit de exploit o escribir su propio código para infectar máquinas que añadir a esa red de máquinas zombies que después se pueden utilizar dentro de un ataque de denegación de servicio o para lanzar campañas de spam.

También está el Cazador de Vulnerabilidades. Bucea en Internet y busca en sites de banca o comercio electrónico fundamentalmente en busca de fallos que pueda explotar para adentrarse en los sistemas y robar información, productos o dinero.

Los clonadores de tarjetas son los expertos en convertir la información robada sobre una tarjeta de crédito en una tarjeta bancaria falsa que se pude utilizar en un cajero o un terminal para robar dinero o hacer compras. Dentro de este grupo están los llamados Cashers, que son los que se dedican a coger las tarjetas robadas para sacar dinero de los cajeros.

Las llamadas mulas suelen ser usuarios poco precavidos a los que se les contacta para que abran cuentas bancarias y muevan el dinero robado para blanquearlo.

INTRODUCING

CHECK POINT
INFINITY

THE CYBER SECURITY ARCHITECTURE OF THE FUTURE

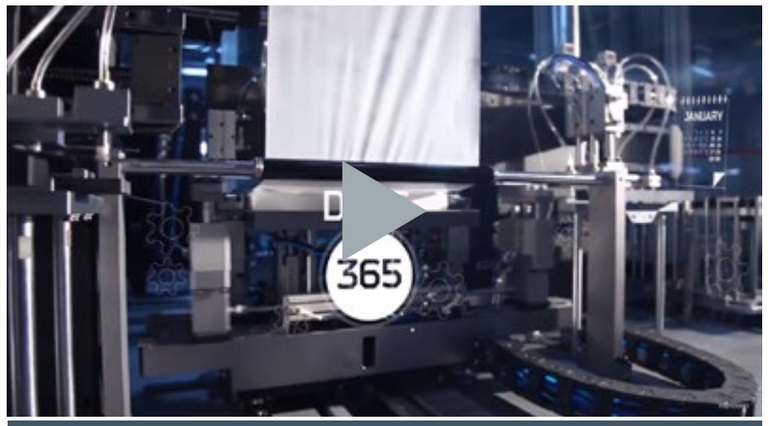
CLOUD MOBILE THREAT PREVENTION

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen

Los ataques a sistemas industriales van en aumento. Y no se trata de una intuición, sino de una realidad respaldada por los datos. Además de los riesgos asociados a los ataques a cualquier organización, los ataques a sistemas industriales pueden tener unas consecuencias más desoladoras. Descubre cómo estar protegido y cómo enfrentarse a esta nueva corriente.

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen



CIBERSEGURIDAD INDUSTRIAL DE KASPERSKY LAB — CLICAR PARA VER EL VÍDEO

El 67 % de los administradores de seguridad de IT/ OT percibe el nivel actual de ciberamenazas sobre los sistemas de control industrial (ICS) como crítico o alto

Los ciberataques a sistemas de control industriales están aumentando de forma importante, como puede verse en las diferentes figuras incluidas en este texto, obtenidas todas ellas del Informe de Amenazas de Kaspersky Lab ICS CERT. De hecho, el 67 % de los administradores de seguridad de IT/ OT percibe el nivel actual de ciberamenazas sobre los sistemas de control industrial (ICS) como crítico o alto, lo que representa un aumento de más del 43 % con respecto a las conclusiones del último año. La interrupción de la cadena de suministro y del negocio se sitúa como la principal preocupación mundial en los últimos cinco años; los ciber-riesgos son la principal inquietud emergente. En lo que respecta a las empresas con sistemas de infraestructuras industriales o críticas, los riesgos nunca han sido mayores, porque la seguridad industrial tiene consecuencias que van mucho más allá de la protección de las empresas y la reputación. Cuando se trata de proteger los sistemas industriales contra ciberamenazas, surgen consideraciones sociales, ecológicas y macroeconómicas.

Modelos obsoletos para enfrentarse al problema

Pese a que la concienciación es mayor, muchos modelos de seguridad están basados todavía en el aislamiento físico de los sistemas, pensando que esto es suficiente. Pero la realidad demuestra que no lo es. En la era de la Industria 4.0, la mayoría de las redes industriales están disponibles a través de Internet, sea o no por propia elección. Una investigación de Kaspersky Lab ICS CERT, que utiliza datos de Kaspersky Security Network, indica que los PC industriales reciben ataques con regularidad del mismo malware genérico que afectan a los sistemas empresariales (TI), incluso conocidos troyanos, virus y gusanos. Durante la segunda mitad de 2016, se bloquearon en el mundo intentos de ataques en el 39,2 % de los ordenadores protegidos por Kaspersky Lab clasificados como componentes de infraestructura industrial.

Un ejemplo de esta idea es Conficker, que, aunque no es específicamente industrial, obligó a cortar el suministro de una central eléctrica nuclear alemana durante varios días en abril de 2016. El problema no se produjo por penetración directa al sistema de control de la central, sino mediante la infección de la red de la oficina adyacente.

Otra creciente amenaza para los ICS es el ransomware. La gama y diversidad del ransomware ha crecido masivamente estos años. La aparición del ransomware es muy significativa para el sector industrial; estas infecciones pueden causar daños de gran impacto y alcance en los sistemas críticos, lo que hace que los ICS sean un objetivo potencial particularmente atractivo, tal y como demuestran varios incidentes de ataques del ransomware contra los sistemas SCADA durante 2016. El ransomware diseñado para atacar sistemas industriales puede tener su propio plan: en lugar de cifrar datos, el malware puede empezar a interrumpir las operaciones o a bloquear el acceso a un activo clave.

Amenazas específicas

Al igual que las amenazas genéricas, la seguridad industrial debe luchar contra el malware específico de ICS y ataques dirigidos: Stuxnet, Havex, BlackE-

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen

La seguridad en estos entornos, donde la disponibilidad es fundamental, debe apuntar en tres líneas diferentes: procesos, empleados y tecnologías

Amenazas y factores de riesgo	Tecnologías de Kaspersky Lab
Aparición de dispositivos de red no autorizados en la red industrial	El control de integridad de la red detecta dispositivos nuevos/desconocidos.
Aparición de comunicaciones no autorizadas en la red industrial	El control de integridad de la red supervisa las comunicaciones entre dispositivos conocidos/ desconocidos.
Comandos de PLC maliciosos de: • Operador o un tercero (por ejemplo, contratista) por error • Persona interna (acciones fraudulentas) • Atacante/malware	DPI industrial analiza las comunicaciones desde y hacia los PLC y control de los comandos y los valores de parámetros del proceso tecnológico.
Ataques de red	Un avanzado sistema de detección de intrusiones identifica todos los patrones de ataque de redes conocidos, incluida la explotación de vulnerabilidades en software y hardware industrial
Falta de datos para la investigación y el análisis forense	Herramientas forenses: supervisión y registro seguro de eventos en la red industrial sospechosos y ataques detectados

nergy, PLC Blaster, Ladder Logic Bomb, Pin Control Attack… la lista crece rápidamente. Como los ataques Stuxnet y BlackEnergy han demostrado, una unidad USB infectada o un único correo electrónico de spear-phishing es todo lo que se necesita para que atacantes bien preparados crucen el aislamiento físico air-gap y penetren en una red aislada.

Muchos ataques dirigidos a complejos industriales utilizan la red corporativa y los ICS para lanzarse y propagarse. Por ejemplo, durante el ataque BlackEnergy contra la red eléctrica de Ucrania en diciembre de 2015, que provocó un grave corte de suministro, los hackers utilizaron varios vectores de ataque. Primero robaron las credenciales de acceso al sistema SCADA del entorno corporativo mediante un ataque de spear-phishing. Después, los hackers comenzaron a apagar la red eléctrica manualmente y, a continuación, sembraron un programa KillDisk malicioso en la red industrial que borró o sobrescribió datos de los archivos esenciales del sistema, provocando el bloqueo de la máquina del operador. En paralelo, el centro de llamadas de la empresa fue objeto de un ataque DDoS para impedir que los clientes informaran del apagón.

Un enfoque diferente de la ciberseguridad

La estrategia diseñada por Kaspersky Lab se apoya en una serie de amenazas que no pueden ser obviadas. Nadie está a salvo porque la seguridad al cien por cien no es posible. Por tanto, la pregunta ya no es si seremos atacados, sino cuándo y cómo de rápido serás capaz de recuperarte, porque no hay una única tecnología de protección que nos garantice la seguridad cien por cien.

La apuesta de Kaspersky Labs se basa en un enfoque efectivo que trata la amenaza de forma holística (integral) con un conjunto de soluciones com-

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes fue diseñada específicamente para abordar las amenazas a nivel de operador en entornos de ICS. Protege los servidores ICS/SCADA, las HMI y las estaciones de trabajo de ingeniería contra varios tipos de ciberamenazas que pueden deberse a factores humanos, malware genérico, ataques dirigidos o sabotaje.
KICS for Nodes es compatible tanto con los componentes de hardware y software de los sistemas de automatización industrial como con SCADA, PLC y DCS.
Las tecnologías de control de integridad de KICS for Nodes incluyen control de la instalación y el inicio de las aplicaciones de acuerdo con políticas de marcado en lista blanca (prácticas recomendadas para redes de control industrial) o lista negra; control del acceso de las aplicaciones a los recursos del sistema operativo: archivos, carpetas, o registro del sistema, por ejemplo; control de todo tipo de archivos que se ejecutan en entornos Windows, lo que incluye .exe, .dll, .ocx, controladores, ActiveX, scripts, intérpretes de línea de comandos y controladores de modo kernel; actualización de datos de reputación de la aplicación; categorías de aplicaciones predefinidas y definidas por el cliente para gestionar las listas de aplicaciones controladas; ajuste de controles de aplicaciones para diferentes usuarios; y modos de prevención o de solo detección: bloquear cualquier aplicación que no esté en la lista blanca, o bien, en modo de "vigilancia", permitir la ejecución de aplicaciones que no estén en la lista blanca pero registrando su actividad en Kaspersky Security Center, donde se pueden evaluar.

Así, la seguridad no debe ser solo un producto, sino un proceso continuo; la concienciación y el conocimiento de las personas es fundamental, porque cualquiera puede acabar siendo una amenaza por desconocimiento o mala fe; y las tecnologías deben ser específicas para este tipo de problemática.

pleto y tecnologías de protección multicapa, porque no podemos olvidar que no se trata solo de prevenir incidentes, sino también de predecir, detectar y responder a los incidentes. Y todo ello de forma eficaz, fiable y flexible, porque la seguridad no es un estado, es un proceso que evoluciona y del que hay que estar siempre pendiente.

¿Qué aporta la visión de Kaspersky Lab que sea diferenciador? La respuesta es True Cybersecurity. Se trata de un elemento que previene incidentes; los predice y detecta, y responde a ellos de forma eficaz, flexible y fiable. Todo esto, apoyado en el catálogo de soluciones de Kaspersky Lab, en la combinación de la inteligencia humana y el aprendizaje automático, y en un concepto adaptativo, protegen la empresa de la nueva generación de amenazas, minimizando los riesgos.

Además del malware y los ataques dirigidos, las organizaciones industriales hacen frente a otras amenazas y riesgos para las personas, los procesos y la tecnología. Y subestimarlos puede tener graves consecuencias. Entre estos factores de riesgo se incluyen los errores de terceros (operadores o contratistas), acciones fraudulentas, cibersabotaje, problemas de cumplimiento o falta de concienciación y de datos relevantes para la investigación forense.

Por este motivo, es necesaria una ciberseguridad industrial especializada. Solo los proveedores de ciberseguridad que comprendan las diferencias entre las empresas industriales y las empresas estándar orientadas a los datos pueden ofrecer soluciones para satisfacer las singulares necesidades de seguridad de los sistemas de control industrial y su infraestructura. Forrester Research aconseja a las organizaciones industriales que están seleccionando proveedores de seguridad que "busquen experiencia especializada en el sector". Forrester identifica a Kaspersky Lab como uno de los pocos proveedores con experiencia especializada en este sector.

De hecho, Kaspersky Lab colabora con los principales proveedores y organizaciones de automatización industrial, como Emerson, SAP, Siemens, Schneider Electric, Industrial Internet Consortium y muchos otros, para establecer compatibilidad,

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen

Los servicios son una parte muy importante de Kaspersky Industrial CyberSecurity, dado que Kaspersky Lab proporciona el ciclo completo de servicios de seguridad, desde la evaluación de la ciberseguridad industrial hasta la respuesta a incidentes

procedimientos especializados y marcos de cooperación que protejan los entornos industriales no solo frente a las amenazas existentes y emergentes, sino también contra los ataques dirigidos. Asimismo, ha desarrollado una oferta de soluciones especializadas para responder a determinadas necesidades del mercado de ciberseguridad industrial: Kaspersky Industrial CyberSecurity (Kaspersky Industrial CyberSecurity).

Kaspersky Industrial Cybersecurity

Estas instalaciones, que ya no pueden protegerse permaneciendo aisladas, pueden verse amenazadas por malware y ataques dirigidos, así como por riesgos tales como los cibersabotajes, la falta de informes de incidentes, la normativa y regulaciones, las acciones fraudulentas, los errores de terceros, la falta de conocimiento, o la falta de datos contrastados para el análisis forense.

Kaspersky Industrial CyberSecurity for Networks

La solución de seguridad a nivel de red de Kaspersky Lab funciona en el nivel de protocolo de comunicación industrial (Modbus, conjunto IEC, ISO...), analizando el tráfico industrial para encontrar anomalías a través de la tecnología avanzada DPI (inspección exhaustiva de paquetes). También se proporciona control de la integridad de la red y capacidades IDS.

KICS for Networks proporciona una supervisión de anomalías del tráfico de red pasiva y de seguridad de red al mismo tiempo que se mantiene invisible para los posibles atacantes.

La capacidad de aprendizaje automático ofrece una detección de anomalías industriales a un nuevo nivel, lo que posibilita el descubrimiento de incidentes en las redes industriales más complejas y que se reconfiguran con frecuencia. Mientras, KICS for Networks permite la identificación de todos los activos de red conectados vía Ethernet, lo que incluye servidores SCADA, HMI, estaciones de trabajo de ingeniería, PLC y RTU. Todos los dispositivos nuevos o desconocidos y sus comunicaciones se detectan automáticamente. Esto permite a los equipos de seguridad crear un inventario propio, fiable y seguro de activos de red, en lugar de utilizar herramientas de gestión de activos de OT/IT potencialmente vulnerables que suelen ser objetivo de los atacantes.

Por último, la solución de Kaspersky Lab ofrece a los usuarios industriales un sistema de registro seguro que proporciona herramientas digitales para el análisis de datos y análisis forense. El sistema también impide la realización de cambios en los registros de ICS

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen

La seguridad en estos entornos, donde la disponibilidad es fundamental, debe apuntar en tres líneas diferentes: procesos, empleados y tecnologías. Así, la seguridad no debe ser solo un producto, sino un proceso continuo; la concienciación y el conocimiento de las personas es fundamental, porque cualquiera puede acabar siendo una amenaza por desconocimiento o mala fe; y las tecnologías deben ser específicas para este tipo de problemática.

En el caso de Kaspersky Lab, la respuesta es Kaspersky Industrial Cybersecurity, un conjunto de tecnologías y servicios pensados para hacer frente a este tipo de amenazas.

Kaspersky Industrial CyberSecurity es un conjunto de tecnologías y soluciones que proporcionan una seguridad operativa eficaz contra las ciberamenazas en todas las capas de ICS, incluidos servidores SCADA, HMI, estaciones de trabajo de ingeniería, PLC y conexiones de red industriales, todo ello sin afectar a la continuidad operativa ni a la coherencia de los procesos tecnológicos.

Como decíamos, Kaspersky Industrial CyberSecurity se compone de soluciones y servicios, un elemento muy importante porque la compañía ofrece el ciclo completo de servicios de seguridad, desde la evaluación de la ciberseguridad industrial hasta la respuesta a incidentes.

Antes de adentrarnos en la formación, recordemos que Kaspersky Industrial CyberSecurity dispone de una única consola de administración, Kaspersky Security Center, que permite la gestión centralizada de políticas de seguridad; posibilidad de establecer diferentes configuraciones de protección para los distintos nodos y grupos; prueba simplificada de actualizaciones antes de su despliegue en la red, lo que garantiza la plena integridad del proceso; y acceso basado en funciones en línea con las políticas de seguridad y acciones urgentes.

Asimismo, destacan dos elementos de la solución: KICS for Nodes y KICS for Networks.

Formación: un elemento básico

Otro elemento importante es la formación, y es que Kaspersky Lab ofrece cursos diseñados tanto para expertos en seguridad de IT/OT como para operadores e ingenieros de ICS. Durante la formación, los participantes adquieren un mayor conocimiento de las ciberamenazas pertinentes, sus tendencias de desarrollo y los métodos más eficaces para protegerse contra ellas. Los cursos también permiten a los profesionales de seguridad seguir desarrollando sus habilidades en áreas específicas, incluidos los Pen Testing de ICS y la ciencia forense digital.

Pero, para aumentar la concienciación sobre las cuestiones de ciberseguridad industrial, además de promover las competencias necesarias para abordarlas y resolverlas, Kaspersky Lab ofrece formación basada en gamificación, para gestores de seguridad e ingenieros.

Además, el equipo de expertos de respuesta a ciberemergencias de ICS prepara informes de inteligencia de seguridad actualizados.

Los programas de formación permiten aprovechar los conocimientos, la experiencia y la inteligencia frente a amenazas en ciberseguridad industrial de Kaspersky Lab.

Sistemas industriales, el nuevo escenario de la lucha contra el cibercrimen

Concienciación sobre la ciberseguridad	Formación y desarrollo de habilidades de ciberseguridad	
Para sus ingenieros/ trabajadores de la planta industrial:	Para profesionales de IT/OT:	Para profesionales de seguridad de IT/OT:
Ciberseguridad básica	Ciberseguridad industrial avanzada	Pen Testing de ICS para profesionales
Para la gestión:		Ciencia forense digital de ICS para profesionales
Industrial Cybersafety Games		

En torno al 80 % de los incidentes de ciberseguridad son provocados por errores humanos. Estos errores humanos pueden salir muy caros e incluso ser letales cuando los incidentes pueden dañar sistemas importantes o paralizar completamente procesos industriales. En un entorno donde el panorama de amenazas está en constante evolución y los ataques dirigidos que dependen de errores humanos están en alza, la mejor defensa son trabajadores formados, para los que las prácticas de trabajo ciberseguras sean automáticas e instintivas.

Por eso, todos los empleados pueden ser formados y concienciados acerca de la seguridad, si bien, para los responsables del IT/OT, existe un segundo nivel de formación en ciberseguridad.

Empezando por los primeros, los cursos de concienciación y formación de Kaspersky Industrial CyberSecurity se han desarrollado para permitir a los principales operadores de infraestructura, proveedores de utilities y fabricantes proteger mejor sus entornos industriales frente a interrupciones y daños causados por incidentes y ataques cibernéticos.

La concienciación sobre la ciberseguridad industrial consta de módulos de formación interactivos, presenciales y online, y para todos los empleados que interactúen con sistemas informatizados industriales y para sus superiores.

El segundo nivel de cursos, la formación y desarrollo de habilidades de ciberseguridad, combina teoría y práctica y permite a los formados trabajar con expertos para desarrollar sus capacidades en predicción, prevención, detección y respuesta al cibercrimen.

Se desarrolan en tres áreas, principalmente: conocimiento básico de ciberseguridad de sistemas de control industrial, Pen Testing de ICS y Ciencia forense digital de ICS. El primero ofrece formación sobre el panorama de amenazas y los vectores de ataque que ponen en riesgo el entorno industrial. El segundo permite a los profesionales de seguridad de IT/OT llevar a cabo Pen Testing

integrales y exhaustivos en entornos industriales y recomendar las acciones de corrección apropiadas desde un punto de vista experto, mientras que el tercero capacita a estos profesionales para llevar a cabo investigaciones forenses correctas en entornos industriales.

Enlaces de interés...

- I Ciberseguridad Industrial
- W 7 razones para elegir Kaspersky Industrial
- W Ciberseguridad para infraestructuras eléctricas
- W Kaspersky Lab ICS CERT Reporte Amenazas
- W Programas de concienciación y formación de Kaspersky Industrial CyberSecurity
- W Kaspersky Industrial CyberSecurity

BE SURE TO BE FREE

BLINDA TUS “SUPERCONFIDENCIAL”

#BlindaTuLibertad

Garantiza que lo que pasa en tu empresa se queda en la empresa.
Descubre lo último en ciberseguridad empresarial.

ESET ENJOY SAFER TECHNOLOGY™

Y si no cumplo la GDPR, ¿qué?

Apenas quedan unos meses para que GDPR, una de las normativas más exigentes en materia de protección de datos entre en vigor. Se trata de la mayor reforma legislativa en materia de privacidad y protección de datos de los últimos 30 años. Busca dar a los ciudadanos europeos mayor control sobre su información privada, además de mejorar la seguridad de las empresas que operan tanto en la UE como en otras partes del mundo pero que trabajan con información de ciudadanos europeos.

La fecha de acerca, pero parece que aún queda mucho camino por recorrer. Para analizar el impacto de esta normativa, cómo abordarla y cuáles son los mejores modos de cumplir con la misma IT Digital Security organizó un webinar en el que participaron Pedro García-Villacañas, Director Técnico de Kaspersky Lab Iberia; Juan Julián Moreno Piedra, IM&G Pres-Sales Manager, EMEA South en Micro Focus; Carlos Tortosa, responsable de grandes cuentas de ESET España y Alain Karioty, Regional Sales Director Latin America en Netskope.

Kaspersky

La GDPR es una regulación, no una directiva, explica Pedro García-Villacañas. “Lo que significa que no prohíbe nada, pero lo regula todo”, añade el directivo. Y dice también el directivo de Kaspersky que ha sido diseñada para unificar las normas en la Unión Europea y que afecta no sólo a las empresas que realicen su actividad en la Unión Europe, sino a todas las que operen o trabajen con datos de usuarios del Viejo Continente.

Una de las novedades de la GDPR es que redefine lo que es el dato personal, que no sólo son nuestros nombres y apellidos, sino nuestras direcciones IP, alias o cualquier aspecto que pueda ser incluido en un formulario digital. No se le olvida al directivo recordar que las multas de la GDPR son hasta el 4% de la facturación mundial o hasta 20 millones de euros, o que en caso de una fuga de la información hay que comunicar esa brecha de seguridad a los organismos competentes, que son dos de los aspectos que más llaman la atención de la nueva regulación.

En todo caso para Pedro García-Villacañas, “el verdadero impacto de la GDPR en las empresas es cómo gestionamos, almacenamos y tratamos los datos”, explica Pedro García-Villacañas

El directivo de Kaspersky dice también que la GDPR es positiva para la seguridad, y que todo lo que sea concienciación y añadir medidas y defensas para mejorar nuestros datos es positivo.

Los cinco requisitos a los que Kaspersky considera que deben prestarse más atención

"El verdadero impacto de la GDPR en las empresas es cómo gestionamos, almacenamos y tratamos los datos"

Pedro García-Villacañas, Director Técnico de Kaspersky Lab Iberia

a la hora de cumplir con la GDPR son: la figura del DPO, o responsable de protección de datos; las organizaciones deberán asumir cierta responsabilidad sobre los datos que tratan, gestionan o almacena; el consentimiento explícito del usuario para utilizar los datos que proporcionan a la organización; la notificación obligatoria de una posible brecha de seguridad y se añade el concepto de privacidad desde el diseño, que significa que cualquier acción que se realice dentro de la organización debe tener en cuenta la privacidad desde el minuto cero.

"Hemos adecuado parte del portfolio de seguridad que tenemos para ayudar a las empresas a cumplir con la GDPR", dice en el webinar el Director Técnico de Kaspersky Lab Iberia. Uno de los elementos es proporcionar formación sobre concienciación, además de detectar los ataques lo antes posibles. No hay que olvidar, dice pedro García Villacañas, el "implementar mecanismos dentro de nuestros procesos que ayuden a ser capaces de notificar a tiempo esas infracciones y gestionar de forma adecuada esas notificaciones, y por último debemos estar constantemente probando, accediendo y evaluando nuestros sistemas para comprobar que la regulación está siendo eficiente".

Micro Focus

Preguntado sobre el principal reto al que se enfrentan las empresas para cumplir con la GDPR, Juan Julián Moreno Piedra, IM&G Pres-Sales Manager, EMEA South en Micro Focus, habla de plazos. Lay se promulgó en abril y será de obligado cumplimiento el próximo 25 de mayo de 2018; "todas las empresas debían estar avanzando en ese cumplimiento", dice el directivo, añadiendo que queda realmente muy poco tiempo para demostrar el regulador que la estamos cumpliendo".

La transparencia, el DPO, el derecho al olvido, la portabilidad, son alguno de los nuevos conceptos que añade la ley y que las empresas deben tener en cuenta, según el directivo de Micro Focus.

La mayoría de las empresas están dando los primeros pasos hacia cumplir con la GDPR, dice Juan Julián Moreno; en relación a la pequeña y mediana empresa "están empezando a despertar", dice el

CINCO PASOS PARA HACER DEL DATA MASKING UNA REALIDAD

Cada vez más empresas confían en el enmascaramiento de datos, o Data Masking, para proteger proactivamente sus datos, mejorar los mandatos de cumplimiento de seguridad de datos y evitar los costos asociados con las infracciones de datos. La mejor práctica para el enmascaramiento de datos incluye cinco pasos: Descubrir, Clasificar, Configurar, Desplegar y Mantener.

"Se hace necesario vigilar dónde están los datos que se encuentran en el cloud y qué datos están en qué nubes y en qué aplicaciones"

Alain Karioty, Regional Sales Director Latin America en Netskope

directivo, recordando las grandes multas que tiene la ley, “multas que son para los propietarios de los datos, y no para los que los procesen”.

Desde Micro Focus la propuesta hacia la GDPR no sólo se plantea desde el punto de vista del cumplimiento “sino desde la eficiencia operativa, mejorar los procesos, mejorar en la productividad”.

Para responder a las inquietudes de las empresas que han de hace frente a la GDPR, Micro Focus ha planteado una serie de preguntas, asociando los artículos de la regulación a los que deben darse respuestas y “aprovechando toda la infraestructura, todos los productos que tenía Micro Focus desde antes de GDPR y que ya estaban integrados entre sí, pues conseguir una manera de gestionar toda la información desde un punto de vista normativo”, dice Juan Julián Moreno.

Añade el directivo también que además de la experiencia en la gestión de la información, Micro Focus la tiene en seguridad, encriptación, anonimización… integrado en el gobierno de la información”.

ESET

Para Carlos Tortosa, responsable de grandes cuentas de ESET España, el mayor impacto que va a tener a GDPR es el poder aplicar una serie de servicios o de solucione tecnológicas que nos van a permitir una mayor protección de los datos. Y recoge los datos de un estudio que dice que el “80% de las empresas consideran que no tienen suficiente formación para cumplir con GDPR”, que un 97% cree que no llegará a tiempo y que sólo un 9% de los responsables de TI cree que para el 25 de mayo su empresa estará adecuada a la regulación.

En los consejos de la firma de seguridad para cumplir con la GDPR el que se monitorice la información, saber dónde van los datos, dónde están almacenados, que se diseñe un plan de acción de cara al reglamento y que se adecúe ese plan de acción a nivel tecnológico para que la adaptación sea completa. Entra las medidas una solución de cifrado de datos y protección del acceso a los mismo, como pueden ser DesLock o Secure Authentication

Propone el directivono sólo clasificar y controlar la información, sino aplicar políticas, controlar los

"Desde Micro Focus la propuesta hacia la GDPR no sólo se plantea desde el punto de vista del cumplimiento, sino de eficiencia operativa"

Juan Julián Moreno Piedra, IM+G Pres-Sales Manager, EMEA South en Micro Focus

"Se hace necesario un plan de acción de cara al reglamento y que se adecúe a nivel tecnológico"

Carlos Tortosa, responsable de grandes cuentas de ESET España

dispositivos desde lo que se acceder a los datos, etc., para mantener un control. Aún así "desde 2013 hasta hoy se producen, 60 brechas de seguridad cada segundo, y un 30% son brechas internas", dice Carlos Tortosa, que asegura que es un porcentaje demasiado elevado. El nivel de protección puede ser muy alto, pero de poco vale cuando se tiene el enemigo en casa, dice el directivo, por eso es tan conveniente hacer un seguimiento de la información.

Netskope

Por el cambio de comportamiento de los usuarios tanto en el uso de aplicaciones, incluido el desde dónde se hace necesario una nueva solución de seguridad que permita proteger las aplicaciones que están el cloud y vigilar dónde están los datos que se encuentran en el cloud y qué datos están en qué nubes y en qué aplicaciones. Con esta explicación arranca Alain Karioty, Regional Sales Director Latin America en Netskope, su participación en el webinar. Se refiere el directivo a CASB, o Cloud Access Security Manager.

"La propuesta de Netskope para la GDPR se basa en un calendario que hemos definido hasta mayo de 2018, donde se plantean cuatro etapas: Auditar, Racionalizar, Controlar y Reportar", dice Karioty.

Auditar supone conocer los datos por su perfil y que pueden estar alojado en distintas nubes y aplicaciones sin tener ningún control. "Es bueno saber dónde están los datos y qué aplicaciones los están utilizando", asegura el responsable de Netskope para España y Latinoamérica. Una vez que tenemos este conocimiento el siguiente paso es Racionalizar, que significa identificar los riesgos, seleccionar aplicaciones, definir la política de datos y educar a los usuarios para utilizar la aplicación correcta.

Para poder controlar las aplicaciones lo que hace Netskope es definir una serie de criterios, como pueden ser la localización de los centros de datos, la propiedad de los archivos y se aplica un índice de confianza, si es recomendable para las empresa o no. "Estamos aplicando criterios relacionados con el cumplimiento de GDPR, de forma que un cliente puede ver qué aplicaciones cumplen con la regulación y cuáles no", explica Karioty.

La cuarta etapa, Reportar, supone tener un cierto control de cómo se están utilizando las aplicaciones de forma que pueda reducirse el llamado Shadow IT y mejorarse la adopción de las tecnologías propuestas por la empresa. Y todo ello mejora el cumplimiento con la GDPR.

CASB es una tecnología que viene a ser cada vez más necesaria porque cada vez nos conectamos más a aplicaciones cloud desde más dispositivos yu desde fuera de la empresa", asegura Alain Karioty, Regional Sales Director Latin America en Netskope.

Enlaces de interés...

- Automatizar sus necesidades en torno a GDPR con Micro Focus
- Netskope para La GDPR
- GDPR: ¿Cómo puede ayudar Kaspersky Lab a cumplir la normativa?
- Control de la información: de la Responsabilidad a la Tranquilidad

NUEVO.
PERO NO NACIDO AYER.

CSC Y HPE ENTERPRISE SERVICES AHORA SON DXC TECHNOLOGY.

DXC.technology/GetItDone

DXC.technology | THRIVE ON CHANGE.

Ciberseguridad y cloud: ¿son compatibles?

Almacenar tus datos y aplicaciones remotamente y como servicio ha ayudado a reducir los costes de operaciones de las empresas. Indudables son las ventajas que el cloud ha traído a la industria, pero también genera grandes retos. Si sumamos la movilidad a la deslocalización de los datos y las aplicaciones como consecuencia de utilizar servicios en la nube, ¿podemos garantizar que cada usuario sólo accede a lo que debe? ¿Qué lo hace desde donde debe? ¿Con el dispositivo adecuado?

Estas y otras preguntas se han planteado en el que ha sido el primer desayuno de IT Digital Seguridad sobre Ciberseguridad y cloud, en el que han participado Bosco Espinosa de los Monteros, director de preventa de Kaspersky Lab; José de la Cruz, Director Técnico de Trend Micro; Eusebio Nieva, Director Técnico de Check Point para España y Portugal; Carlos Barbero, Identity, Access and Security de Micro Focus; y Rubén Muñoz, Iberia Country Lead Security Advisory Services de DXC.

El desayuno se iniciaba con algunas cifras aportadas por Juan Ramón Melara, moderador del evento junto con Rosalía Arroyo por parte de IT Digital Security: El 41% de las cargas de trabajo empresariales ya se están ejecutando en la nube, y se espera que el porcentaje se incremente hasta el 60% para el próximo año; según un estudio de IDC, el 87% usuarios cloud ya han adoptado una estrategia de nube híbrida, y que el gasto va a pasar del 37% en 2016 al 47% en 2018. Los datos indican, según Juan Ramón Melara, que el cloud es una realidad más tangible, y que la seguridad ha pasado de ser una barrera a un habilitador de la nube.

Para Bosco Espinosa de los Monteros la seguridad "no era tanto un stopper como una incertidumbre", y añadía el directivo que se dependía totalmente de los proveedores de los servicios, que no había un gran conocimiento las medidas a adoptar y que la legislación no estaba clara. A día de hoy, sin embargo, no sólo se ve una oferta más madura, sino también más conocimiento.

José de la Cruz ha asegurado que la nube "nos ha aportado mucha flexibilidad", pero siempre existía el riesgo de la seguridad. Y cree el ejecutivo que actualmente la tecnología está lo suficientemente madura para que una compañía se plantee el paso a la nube, "donde además tenemos medidas de seguridad más inmediatas de las que podemos tener en nuestras instalaciones".

"Podemos poner todas las medidas que queramos, pero tenemos un problema principal que es el usuario"

Rubén Muñoz, Iberia Country Lead Security Advisory Services de DXC

El director Técnico de Check Point para España y Portugal, Eusebio Nieva, decía en su intervención inicial que la seguridad tradicional también tiene que seguir a las operaciones que se están haciendo en la nube. "La seguridad tiene que tener una continuidad, y eso es lo que estamos ofreciendo los fabricantes, no dejar que la nube vaya sola".

Para Carlos Barbero un punto importante es mantener el control de los usuarios, la gestión de contraseñas... Ahora se pueden implementar los sistemas de seguridad locales en la nube y existen normativas que están regulando todo este mercado. Decía Bardero que las empresas son muy conscientes de que el uso de Dropbox es extenso, pero que las normativas están forzando ciertas limitaciones.

"Históricamente se ha visto seguridad pomo un stopper, no sólo para cloud sino para otras muchas tecnologías", decía Rubén Muñoz. Añadía el directivo que en realidad la seguridad es una necesidad para cualquier ámbito de la visa empresarial, pero que el cloud ha sido una ampliación del horizonte de posibles problemas, "y esos posibles problemas dentro del cloud implican otra vez al eslabón más débil de la cadena, que es el usuario".

Seguridad híbrida

Una de las preguntas planteadas en el desayuno es si una vez que hablamos de cloud y seguridad, esta cambia dependiendo del tipo de cloud: pública, privada o híbrida. Para el director de preventa de Kaspersky Lab, una vez que el recurso es accesible desde el exterior da igual. La única diferencia, explicaba Bosco Espinosa de los Monteros, es quién

SEGURIDAD Y CLOUD, ¿SON COMPATIBLES?

CLICAR PARA VER EL VÍDEO

pone las medidas de seguridad; si es privada las tienes que poner la empresa, y si es pública las tiene que poner el proveedor.

"Lo que un cliente tiene que hacer claramente es escoger el proveedor de servicios adecuado y leerse muy bien el contrato para ver qué medias de seguridad están aplicando", decía el ejecutivo de Kaspersky. Y no es un consejo que deba echarse en saco roto, ya que como recordaba el directivo, "la obligación de proteger el dato es del propietario del dato, no es del proveedor que está dando el servicio", añadía Espinosa de los Monteros antes de plantear que la adopción de la nube debe ser muy medida.

Rubén Muñoz, que diferenciaba entre tendencia y moda cuando habla de la nube, se mostró de acuerdo, y aseguraba que "no tenemos que caer en la moda de pasar al cloud", añadiendo, que no cree que la elección de la nube dependa de la seguridad, sino del modelo de negocio que tenga el cliente. "La problemática que hay es que parece que hay una moda que dicta que dentro de la transformación digital se tiene que pasar al cloud con una cierta obliga-

"Bien hecha y bien entendida, la nube puede solucionar algunos problemas de seguridad tradicionales"

Eusebio Nieva, Director Técnico de Check Point para España y Portugal

ción. Yo creo que la elección principal es qué necesita tu modelo de negocio y luego veremos cómo securizar eso".

Es prácticamente imposible hablar de seguridad y que la GDPR no entre en escena. La nueva regulación de protección de datos será de obligado cumplimiento el próximo 25 de mayo y su impacto en la seguridad del cloud se deja sentir, entre otras cosas, en el proveedor que un cliente ha de escoger. Para el Iberia Country Lead Security Advisory Services de DXC, la oferta de los proveedores de servicios cloud está madurando; "antes nadie preguntaba dónde estaban los datos, y ahora se pregunta dónde están y dónde se procesan… Se avanza en las preguntas porque hay un marco regulatorio que te está obligando como cliente a hacer frente a un problema que antes no preocupaba".

Los marcos regulatorios están impactando en la manera de acceder a la nube, planteaba Eusebio Nieva. Para el directivo la seguridad es un control y éste es mucho mayor en una nube híbrida o propia, pero al mismo tiempo, a día de hoy existe una oferta mucho mayor de servicios de seguridad que equipara la que ofrece cualquier propuesta, "por lo que esas fronteras se están difuminando y las empresas se están planteando el acceso al cloud de otra manera".

Para el ejecutivo de Micro Focus la seguridad en la nube es una constante que "dependerá de donde esté ubicado el objeto y del nivel de acceso". Y recuerda que ese objeto puede estar en la nube o en una plataforma privada; "si tengo el riesgo de que un usuario utiliza sus credenciales para acceder a Office 365 sin ningún tipo de control y alguien hace una campaña de phishing y se ve afectado, no se está poniendo en peligro el correo en la nube, sino toda la organización. Por eso digo que la seguridad tiene que ser una constante".

El nuevo paradigma de la seguridad

Planteado por Juan Ramón Melara a qué se enfrenta la seguridad más allá de la GDPR, José de la Cruz aseguró que desde el punto de vista de seguridad es muy importante contar con la flexibilidad. Explicaba el directivo que el cliente puede estar en la nube, en la nube híbrida –que es lo que está cobrando más fuerza precisamente por eses tema de la flexibilidad, pero podría darse el caso de que una solución estuviese completamente onpremise, "y lo que tenemos que proporcionar a nuestros clientes es la flexibildad para que su solución de seguridad pueda adaptarse a cualquier entorno para que esté siempre protegido".

Para Eusebio Nieva, la adopción de la nube, de las nuevas tecnologías, de la movilidad… lo que está haciendo es cambiar los paradigmas de seguridad. Aseguraba el ejecutivo de Check Point que el paradigma del perímetro se está modificando, pero que no se trata de que no exista, sino de que lo estamos ampliando. "Bien hecha y bien entendida, la nube puede solucionar algunos problemas de seguridad tradicionales, pero claro, hay que aplicar tecnología", aseguraba Nieva.

Carlos Barbero planteaba que las compañías sólo ven la nube como un ahorro de costes, pero añade

"El 41% de las cargas de trabajo empresariales ya se están ejecutando en la nube, y se espera que el porcentaje se incremente hasta el 60% para el próximo año"

que al final es importante entender que hay ahorro de costes pero que se tienen que extender las medidas de seguridad que se van un poco del perímetro. Y que "si las credenciales de tu CEO están en internet no creas que al final van a ir dueño del servicio cloud. Normalmente van a ir al responsable de seguridad de tu compañía".

Para Rubén Muñoz el hándicap es el de "meter a terceros en el camino de tu securización". Y es que, si al final se opta por un proveedor de servicios cloud, tiene que haber un nivel de confianza. "No es tan sencillo poner tecnología de protección en el cloud. Porque hay proveedores que intentan monopolizar hasta cierto punto la capacidad de securizar su servicio cloud".

Seguridad intrínseca

Durante el desayuno el directivo de Kaspersky Labs propuso hacer una comparativa de lo que es la implantación del cloud con lo que ocurrió hace un tiempo con los dispositivos móviles para no cometer los mismos errores. "Coloquemos primero la seguridad intrínseca, no intentemos luego colocar un parche, porque vemos que eso no funciona", dice Bosco Espinosa de los Monteros, añadiendo que si se va a ir al cloud hay que hacer un plan y un estudio serio de lo que se quiere y cómo se quiere. "Está claro que los proveedores tienen cada vez más madurez y que las ofertas son más estándares, pero no se trata de ir al cloud porque es más barato, sino de ver todo lo que implica y lo que me cuesta", aseguraba el directivo.

"A día de hoy todos sabemos los peligros de ir a la nube", recordaba Nieva, asegurando que en algunos de los experimentos realizados por Check Point en la nube "desde el mismo momentos que das de alta un servicio, aunque no haga nada, empiezan a atacarte. Es ponerle en marcha, poner una dirección IP y empezar a recibir ataques".

Que el mercado de la seguridad vaya por detrás de los ciberdelincuentes es, en opinión de Rubén Muños, una percepción errónea, "y se tendría que dar más valor al trabajo que se está realizando".

Nieva añadía que la inmensa mayoría de los ataques, por no decir todos, "podrían haberse evitado con tecnologías existentes", pero que el problema es que muchos casos la usabilidad y seguridad no vana de la mano y, a día de hoy, el usuario tiene demasiado poder frente a la seguridad. Decía el directivo de Check Point que no hay que dejar que los usuarios hagan todo lo que quieren hacer, o bajo todas las condiciones que quieran hacerlo.

"Coloquemos primero la seguridad intrínseca. No intentemos luego colocar un parche, porque eso no funciona"

Bosco Espinosa de los Monteros, director de preventa de Kaspersky Lab

Bosco Espinosa remarca que se da prioridad a que el usuario se sienta cómodo, a que la interfaz sea amigable… y no le decimos que es su responsabilidad pinchar en un enlace malicioso. La concienciación y formación del empleado en materia de seguridad se pone sobre la mesa, sobre todo cuando Eusebio Nieva recuerda que durante el ataque de Wannacry las empresas de seguridad no se vieron afectadas porque sus empleados tienen más conciencia.

La responsabilidad del empleado, del usuario, es tan reducida que si se dejara que fueran ellos los encargados de implementar los parches de seguridad, "algunos no lo harían en meses", decía Bosco Espinosa.

"Wannacy puso de manifiesto la ineficiencia de los sistemas de parcheado actuales. En muchos casos, por motivos de continuidad de negocios, o que la aplicación no sea compatible… a veces no se puede instalar porque no es compatible", decía José de la Cruz, añadiendo que se tienen que buscar métodos alternativos, como puede ser parcheado virtual, que ayude a protegerse de ese tipo de amenazas.

El ejecutivo de Trend Micro también habla de concienciación, algo que considera fundamental porque "al fin y al cabo el usuario es el último firewall y si no tiene un mínimo de concienciación más tarde o más temprano nos la va a liar". Y eso llevó a José de la Cruz al siguiente punto, que es la visibilidad; "si yo he aprendido algo es que lo más importante para mí es la visibilidad, saber qué está pasando en mi red; me importa menos que tener un ataque y una serie de equipos infectado siempre que sepa cuáles son y qué red tengo que cortar. Creo que lo peor que puede pasar desde el punto de vista de seguridad es no tener visibilidad de lo que ha pasado, por dónde han entrado"

Shadow IT

Aunque la palabra está de moda, para Rubén Muñoz, el shadow It es simplemente "el uso incorrecto de la infraestructura IT de las empresas. Esto se llama ahora Shadow IT, pero ocurre desde que hay un PC en una mesa". Decía el ejecutivo de Micro Focus que el problema es que alguien ha decidido que el usuario sea administrador de la máquina y tenga esos permisos.

Para Eusebio Nieva, el shadow IT tiene dos vertientes. Por un lado, el uso totalmente incorrecto, y por otro la adaptabilidad de los sistemas de TI tradicional a las necesidades de los usuarios. Y es que muchos usuarios han utilizado servicio cloud considerados como Shadow It, porque la empresa no se los proporcional de manera instantánea o de manera legal. El problema termina siendo del responsable de TI, primero por no haber cortado todos esos caminos, y segundo por no proporcionar una solución. En todo caso el ejecuto de Check Point aseguraba que "el shadow it es una evolución natural de las necesidades de los usuarios. La empresa debe ser sensible a todas esas modalidades de trabajo y dar a los usuarios lo que necesitan".

Ruben Muñoz prefiere dar una vuelta a ese enfoque y plantea que la empresa sí que ha puesto a disposición del empleado unas herramientas, plataformas o servicios controlados y securizados

"Es importante entender que la nube genera ahorro de costes, pero implica extender las medidas de seguridad que se van un poco del perímetro"

Carlos Barbero, Identity, Access and Security de Micro Focus

"Creo que lo peor que puede pasar desde el punto de vista de seguridad es no tener visibilidad de lo que ha pasado, por dónde han entrado"

José de la Cruz, Director Técnico de Trend Micro

que no convencen al usuario porque no le permiten hacer ciertas cosas.

En todo caso, ahora se han dado cuenta, están empezando a tomar medidas. Para José de la Cruz, la buena noticia es que ya hay soluciones que ya contemplan estos retos de shadow", dice el ejecutivo refiriéndose al CASB (Cloud Access Security Manager)

Seguridad Cloud

Al término del desayuno se pide a cada fabricante una reflexión sobre al reto de la seguridad Cloud. Para Boscpo Espinosa de los Monteros, "el mundo cloud da muchos dolores de cabeza pro también muchas facilidades", y recordaba que no sólo se trata de securizar la nube, sino de apoyarnos en ella para mejorar la protección y hacer que el mundo cloud pueda ser mejor.

Haciendo hincapié en lo que se ha hablado, José de la Cruz dijo que el cloud manifiesta muchas ventajas, y que las soluciones de seguridad que la protejan tienen que ser lo mismo: escalables, flexibles. "Y hago siempre mucho hincapié en estos tres puntos cuando hablo de seguridad: una solución de seguridad que se precie tiene que proporcionarnos visibilidad, control, y flexibilidad".

Eusebio Nieva explicó que en Check Point se está incidiendo mucho en que todas las tecnologías y servicios que se consumen como parte de la nube tienen que tener las mismas características de seguridad que las que se utilizan comúnmente en un entorno más privado, y además no hacer perder ninguna de las características beneficiosas que da la nube. Además "para nosotros las tecnologías de seguridad tienen que ser preventivas, siempre, porque nos han demostrado que son fundamentales para las amenazas que están viniendo, y que en la nube van a ser las mismas".

"En Micro Focus entendemos que la nube es una evolución natural, pero sí es importante todo lo que tiene que ver con la gestión de identidad, la gestión del acceso, la trazabilidad, y sobre todo la seguridad en sí misma: qué hacen los usuarios, dónde va y qué es lo que está pasando", dijo Carlos Barbero

Rubén Muñoz explicó que desde DXC Technology "lo que estamos haciendo es asesorar todo ese paso previo de selección de proveedores de cloud y las mejores medidas de seguridad para acompañar a ese proveedor. Ahí es donde aportamos valor. En ese paso de acompañamiento de cloud y posterior gestión". it

Enlaces de interés...

- Top Threats to Cloud Computing Plus: Industry Insights
- Gestión del riesgo y la seguridad a la velocidad del negocio digital
- Hablando de 2018, los presupuestos en Seguridad van a aumentar
- Las brechas de datos en el cloud continuarán aumentando

THE RANSOMWARE X.

Mediante la integración de tecnologías de Machine Learning a sus mecanismos de detección, la solución **Trend Micro™ XGen ™ endpoint security** protege contra el ransomware y garantiza la integridad de sus datos.

El ransomware es sólo una parte del problema. Su vulnerabilidad, representada por la "X", también podría ser un ataque de tipo Zero Day, una amenaza debida al comportamiento de sus usuarios o cualquier actividad que comprometa la integridad de sus datos y de su reputación.

What's your X? Tren Micro™ XGen™ endpoint security es la solución.

#WhatsYourX

TREND MICRO™

trendmicro.es/xgen

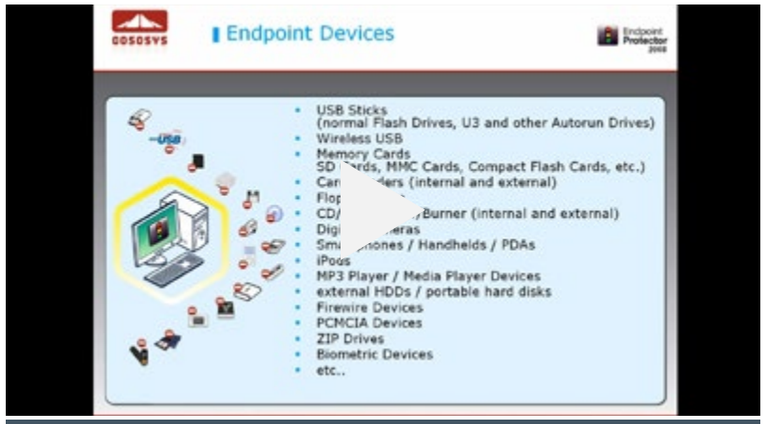
Next Generation llega al endpoint

Durante muchos años el antivirus tradicional fue el elemento básico para asegurar los endpoint. Aún hoy se considera una parte importante de la seguridad de un sistema, pero la propia evolución de los ataques, cada vez más sofisticados, han hecho que pierda peso y que se hable de de una seguridad endpoint mucho más completa. ¿Qué es un endpoint? Cualquier dispositivo con capacidad para conectarse a la red, y eso incluye no sólo los ordenadores, teléfonos móviles e incluso tabletas, sino las impresoras, los terminales punto de venta (TPV) o los smartwatches y pulseras de fitnets.

La seguridad endpoint ha evolucionado radicalmente en los últimos 25 años, nos cuenta José de la Cruz, director técnico de Trend Micro. Explica el directivo que, en sus primeros días, el malware o el spam eran la única preocupación, pero que el auge de la economía sumergida de la piratería, un panorama de TI en constante cambio y el comportamiento de riesgo de los usuarios ha provocado un crecimiento exponencial de las amenazas sofisticadas como el phishing, los ataques dirigidos, el malware móvil y, ahora, el ransomware. Por eso, "una solución de seguridad para endpoint tiene que ser capaz de proteger todos y cada uno de los posibles vectores de ataque a los que se encuentra expuesto", asegura el directivo.

María Campos, directora regional de McAfee para España y Portugal, coincide con José Campos en que el número de amenazas e incidentes de seguridad continúa creciendo. "Hemos sido testigos, una vez más de que no existen "balas de plata" contra el malware avanzado y los procesos de malware hunting", asegura la directiva, añadiendo que desde McAfee se considera que una solución completa de protección del Endpoint debe abordar tres áreas: Antivirus Tradicional (EPP – End Point Protection), Malware Avanzado (Reputación, machine learning, deep learning) y Malware Hunting (EDR- Endpoint Threat Detection and Response) con una aproximación integrada de agente único que evite los retos que suponen los sistemas aislados.

Parece claro que las soluciones de seguridad han evolucionado desde la simple detección del malware a contar con nuevos mecanismos de detección,



¿QUÉ ES LA SEGURIDAD ENDPOINT? **CLICAR PARA VER EL VÍDEO**

"pasando de basarse únicamente en firmas de virus a sistemas heurísticos primero y, posteriormente, análisis de comportamiento y sistemas de detección inteligentes basados en una conectividad permanente a los sistemas de inteligencia sobre amenazas de cada empresa. Otras funcionalidades como la gestión remota y centralizada, el cifrado de datos y comunicaciones o la monitorización de la red en busca de posibles comunicaciones maliciosas con centros de mando y control se han ido añadiendo como capas adicionales para ofrecer una seguridad más efectiva", explica Josep Albors, responsable de investigación y concienciación ESET España.

Ángel Victoria, country manager de G Data España, añade que una solución de seguridad endpoint no sólo debe ofrecer una protección antimalware integral en tiempo real, proteger cualquiera de las plataformas que convivan en la red y funcionar en segundo plano sin afectar al rendimiento de los equipos. "Si realmente funciona, lo ideal es que el usuario no sepa ni que la tiene instalada", dice el directivo.

Alfonso Ramírez, director de Kaspersky para España Y Portugal, dice que tanto el endpont como el perímetro deben protegerse, pero que es necesario ir un paso más allá de la detección y posterior resolución; "la predicción y el análisis son fundamentales y hay que incorporarlos a cualquier estrategia de seguridad", asegura el directivo.

Next Generation Endpoint Security

Queda clara la necesidad de una solución de seguridad endpoint más allá del simple antivirus, que la seguridad evoluciona a la par que el malware y las amenazas, y que siempre hay un paso más que dar. Y de igual manera que los firewalls pasaron a ser Next Generation Firewalls, la seguridad endpoint pasó a ser una seguridad Next Generation Endpoint Protection, un término que se ha ido gestando en los últimos dos o tres años en un momento en el que las empresas intentaban decidir que si reemplazaban su solución antivirus por algo nuevo.

Next Generation Endpoint Protection, o NGEP, es un término acuñado al margen de cualquier estándar, perpetuado, eso sí, por fabricantes que buscan distinguir sus productos del grueso de soluciones de seguridad endpoint

¿Cuándo se considera que la seguridad endpoint es Next Generation? "Cuando responde con éxito a las ciberamenazas en cualquiera de sus formas y en cualquiera de las fases de un ataque", dice Ángel Victoria.

Para Josep Albors "la definición de 'Next-Gen' es principalmente una estrategia de marketing utilizada por algunas empresas para referirse a técnicas de

"El enfoque tradicional de seguridad ya no es adecuado para hacer frente a las ciberamenazas"

Alfonso Ramírez, director general de Kaspersky Lab Iberia

detección que hace más de una década que han sido implementadas por compañías de seguridad veteranas en el sector como ESET". Dicho esto, el responsable de investigación y concienciación de la compañía eslovaca de seguridad añade que una Next Generation Endpoint secuerity es "aquella capaz de realizar análisis de comportamiento de una muestra para detectar posibles actuaciones maliciosas que no hayan sido detectados por un análisis por firmas o heurístico. Asimismo, la conexión permanente a sistemas de inteligencia sobre amenazas ayuda a reducir el tiempo de detección de un nuevo malware, permitiendo una reacción más rápida y efectiva".

Trend Micro habla de "next-generation" cuando la solución de seguridad del endpoint implementa todos los mecanismos existentes en el mercado, tanto tradicionales como de vanguardia, y lo hace de manera coordinada y efectiva. "El concepto 'next-generation' implica innovar en los métodos para combatir las amenazas. Esta innovación radica en la combinación de diversas técnicas de defensa intergeneracionales que aplican de forma inteligente la tecnología adecuada en el momento oportuno, dando como resultado una protección más eficaz y eficiente contra una amplia variedad de amenazas".

De acuerdo se muestra María Campos, que tras asegurar que la compartición de inteligencia en tiempo real tras la detección de una amenaza y la capacidad de inocular al resto de terminales de la red se ha transformado en una necesidad si aspiramos a construir entornos resilientes, dice que "la seguridad endpoint de nueva generación no sólo abarca la protección, sino la detección y la remediación como pilares claves en el desarrollo de una seguridad integral".

Teniendo en cuenta las indicaciones de estos expertos y las que ofrece la industria, podríamos decir que entre las tecnologías que una solución de protección endpoint de próxima generación debe incluir no pueden faltar: Análisis previo a la ejecución basado en el aprendizaje automático; análisis de eventos centralizados; explotar la prevención o la mitigación; detección basada en análisis de comportamiento;

El antivirus ha muerto

Hace unos años, concretamente en mayo de 2014, el mercado convulsionó cuando Brian Dye, Senior VP de Symantec declaró ante el Wall Street Journal que el antivirus estaba muerto. El impacto era mayor teniendo en cuenta que por aquellos tiempos, cuando Symantec y Veritas aún no se habían separado, el 40% de los ingresos de la compañía procedían de la venta de Norton 360.

Brian Dye reconoció que el software antivirus sólo era capaz de detectar el 45% de los ataques de malware. Era la época de Stuxnet, cuando los virus comenzaron a hacerse cada vez más complejos, cuando pasaron de generar ataques relativamente simples que sólo buscaban información sobre tarjetas de crédito a formar parte de programas de espionaje o incluso desatar una guerra.

En realidad, el antivirus no murió y tres años después sigue muy presente, pero acompañado de otras soluciones. Semanas después Eugene Kaspersky lo explicaba muy bien al asegurar sobre los antivirus que los "rumores de su muerte son exagerados. Las firmas antivirus existen y siguen siendo importantes, aunque no sean lo más importante. Es como el cinturón de seguridad de tu coche; tienes que tenerlo, pero no es la parte más importante".

Pasado el caos de un titular muy llamativo, los expertos en seguridad dijeron que en realidad las declaraciones de Brian Dye estaban en línea con lo que la compañía había estado haciendo, que no era otra cosa que añadir, desarrollar y explotar otros elementos de seguridad para el endpoint más allá del antivirus, como análisis de comportamiento o la sandbox, añadiendo capa tras capa de seguridad.

Symantec estaba diversificando sus productos y moviéndose hacia una propuesta de detección y respuesta, que implica el seguimiento de fugas de datos y otras intrusiones, así como la prevención de nuevas repercusiones de los datos robados. Los nuevos productos, dijo en aquellos tiempos el VP de Symantec, "asumirán que los ciberdelincuentes entrarán en el sistema, pero ayudarán a las compañías a responder y controlar el daño.

De forma que el antivirus sigue muy vivo, formado una parte importante de una solución de seguridad y siendo una más de las herramientas que se necesitan para mantener el endpoint a salvo.

"La seguridad endpoint de nueva generación no sólo abarca la protección, sino la detección y la remediación como pilares clave"

María Campos, Directora Regional de McAfee para España y Portugal

detección y bloqueo de comportamiento Ransomware; análisis de Sandbox; reversión de cambios después de la detección de un evento; aislamiento de punto final en caso de detección o evento sospechoso; detección retrospectiva, es decir, identificar máquinas previamente infectadas después de que un archivo se identifica como malicioso.

Personal vs Profesional

Identificado lo que debería de ser una solución de seguridad endpoint avanzada, cabría preguntarnos, por dejarlo claro, qué diferencia una enfocada a un mercado de usuario final de una profesional. Y eso porque siendo España un país de pymes se tiende a optar por productos más económicos sin tener en cuenta otros valores.

La diferencia más importante, en opinión de Ángel Vitoria, es que "la ciberseguridad profesional no se deja en manos del usuario final, está sujeta a unas reglas concretas y se administra de forma centralizada por parte de un responsable de sistemas". Y a esto se añade que en el endpoint profesional existen una serie de capas de seguridad que no se ofrecen ni siquiera en las versiones más completas de la seguridad doméstica, "como son la automatización de parches y actualizaciones de los programas instalados, la monotorización de los equipos para detectar procesos lentos o fallidos, o la posibilidad de impedir la instalación de programas ajenos a la compañía, por ejemplo".

Para José de la Cruz, director técnico de Trend Micro, las soluciones profesionales están orientadas a proteger el flujo de información existente en entornos empresariales, lo que implica "implementar una protección mucho más robusta combinando tecnologías de última generación y minimizando el impacto sobre el usuario final y, por tanto, su productividad". Hay que tener en cuenta también que la solución empresarial "debe ser capaz de generar información al administrador de la misma: informes, alertas, etc. y de integrarse con otras soluciones ya sean del propio fabricante o de terceros".

Conectarse a una herramienta de gestión que permita al administrador de la red conocer el estado de todos los endpoints o actuar como sensor para detectar posibles intrusiones en la red corporativa y

alertar de este hecho, es una de las características que, en opinión de Josep Albors, debe tener una solución de seguridad corporativa.

El fin del antivirus

Antivirus es una palabra mágica, y lo es porque se mantiene con el tiempo, convertida en un concepto de lo que prácticamente ya no existe. No es que los virus no existan, sino que ahora se habla malware porque más allá de los virus hay troyanos, ransomwares… Por eso parecería que debería haberse impuesto el término antimalware, y no sólo añadido en un conjunto de siglas conocidas como AV/AM. Y se sigue hablando de soluciones antivirus aunque lo que se compra y se vende va mucho más allá, aunque las empresas de seguridad sigan teniendo en su oferta un Antivirus, convertido en la oferta más básica, por debajo de un Internet Security o un Total Security.

Como apunte curioso, Symantec intentó hace años retirar Norton Antivirus de su oferta. No era la propuesta que más se vendía y la prueba se hizo en el mercado portugués, pero no funcionó y hoy en día la mayoría de fabricantes tiene un "antivirus" en su portfolio.

¿Ha muerto en antivirus? "Si entendemos antivirus como un repositorio de firmas capaz de desactivar o bloquear a una buena colección de malware, su recorrido desde luego es limitado. Este era el antivirus de los 80. Pero ni siquiera los gratuitos encajan ya en esa definición. Desde entonces ha evolucionado tanto como lo ha hecho la industria del cibercrimen o la industria de los smartphones. Y sin embargo nos seguimos refiriendo a él, por una cuestión de economía de palabras, como antivirus. Por eso hablamos ahora de «Next Generation», para subrayar su evolución, porque realmente, se parecen muy poco", explica Ángel Victoria.

"Hablamos de next-generation cuando la solución de seguridad del endpoint implementa todos los mecanismos existentes de manera coordinada y efectiva"

José de la Cruz, director técnico de Trend Micro

El responsable de investigación y concienciación ESET España es mucho más conciso al asegura que "el antivirus no ha muerto, sino que está en evolución constante".

Para José de la Cruz algunos fabricantes afirman que el antivirus (refiriéndose a los motores basados en firmas) está muerto; "esto se basa en la premisa de que, hoy en día, existe un gran volumen de amenazas de tipo 'día cero', es decir, amenazas que han sido generadas y distribuidas en pocos minutos donde aún los motores antivirus no disponen de firmas para bloquearlas siendo esta técnica poco efectiva para este tipo de ataques". Aun así, y teniendo en cuenta que muchos ataques se producen de manera recurrente reutilizando viejos componentes detectados por motores tradicionales, podemos asegurar que en antivirus no ha muerto.

"La protección tradicional del endpoint a través del antivirus se hace necesaria pero no suficiente", dice la responsable de McAfee en España. Añade la directiva que es sin duda un pilar fundamental no sólo para la detección y bloqueo de los ataques conocidos sino también como herramienta de limpieza tras una posible infección. En todo caso, "complementar el antivirus con capacidades de detección de malware avanzado y herramientas de malware hunting que nos ayuden a mejorar la

El impacto del BYOD

Si por endoint consideramos los smartphones, tabletas o relojes inteligentes, además de los ordenadores e impresoras, ¿qué impacto ha supuesto el Bring Your Own Device? Ya no sólo hay que proteger uno o dos terminales por empleado, sino bastantes más, ya no sólo hay que tener en cuenta un plataforma, sino varios sistemas operativos compitiendo entre sí.

Para Josep Albors, el BYOD supone un importante quebradero de cabeza, ya que la utilización de un mismo dispositivo tanto para fines corporativos como personales impide establecer medidas de gestión y protección adecuadas; “el usuario quiere seguir teniendo el control total de su dispositivo, pero esto choca frontalmente con las políticas de gestión de aplicaciones y bloqueo de contenido que se suelen aplicar a los dispositivos corporativos”.

La línea que separa lo profesional de lo personal es cada día más fina. Vivimos en un entorno conectado donde existe una creciente preocupación entre las empresas porque los empleados utilicen sus redes para conectar sus dispositivos BYOD (Bring Your Own Device), dispositivos que, en opinión de María Campos, “son los más vulnerables a infecciones debido a que el malware puede esquivar fácilmente los sistemas de autenticación cuando se conecta a la red corporativa de una organización. Por ello, estos dispositivos BYOD pueden convertirse en una puerta abierta al malware y al robo de información”. Para hacer frente a estas amenazas, la propuesta de McAfee es la de implementar una estrategia de seguridad que contemple la detección, contención y reacción ante cualquier ataque, desde el endpoint hasta la nube y protegiendo el dato allá donde esté.

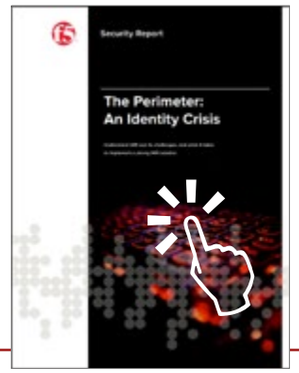
La tendencia cada vez más frecuente del BYOD lleva a Trend Micro a hablar de “políticas restrictivas de acceso a la información desde dispositivos no corporativos”. En opinión de José de la Cruz, alguna de las soluciones más populares aplicadas para mitigar este riesgo “es el acceso a la información mediante escritorios virtuales. En estos entornos, el usuario puede visualizar y trabajar con la información corporativa desde su dispositivo personal pero, una vez cerrada la correspondiente aplicación, no dejaría ningún rastro de información confidencial sobre el propio dispositivo”.

Para G Data el BYOD “ha obligado a nuestras redes informáticas a recorrer el mundo viajando en los bolsillos de los empleados que, además, se conectan sin precauciones ni reparos a la primera red que se cruza en su camino”. La solución que propone la compañía alemana de seguridad es sencilla: transformar los dispositivos móviles de los empleados en clientes “normales”, administrados por las mismas leyes que afectan al resto de clientes e incluidos en las políticas de seguridad TI de las empresas, es decir, que funcionen a imagen y semejanza de las estaciones de trabajo, portátiles o servidores que ya funcionan en la red.

En opinión de Kaspersky “es necesario contar con una plataforma de seguridad capaz de proteger todos los dispositivos desde los que se acede a información de la empresa y los empleados deben ser conscientes de los riesgos”. Entre las recomendaciones de la compañía destaca el establecer un plan de movilidad y no improvisar según vayan surgiendo los problemas; es necesario proteger los dispositivos móviles a través de una solución integral que garantice la seguridad de toda la red corporativa de la compañía. “Las empresas necesitan desarrollar una estrategia para eliminar los dispositivos personales o empresariales de la red corporativa, así como los datos almacenados en caso de extravío o robo, o si un empleado deja la compañía”.

EL PERÍMETRO: UNA CRISIS DE IDENTIDAD

Este documento le ayudará a reconsiderar, reinventar y volver a diseñar sus estrategias de IAM, o de gestión de identidades y accesos. Garantizar la autenticación segura para todas las aplicaciones y abordar los riesgos inherentes asociados con los controles de acceso descentralizados y la dispersión de identidad se ha convertido en asunto primordial.



postura de seguridad y resiliencia de la organización se convierte en una necesidad absoluta en la nueva era digital".

Machine Learning

Como "antivirus", "machine learning" es una palabra mágica. Se ha puesto de moda al calor de la Inteligencia Artificial y parece que sin aprendizaje de máquina nada tiene sentido. Pero como confirma Josep Albors, el machine lñearning, o al menos su aplicación en el mercado de la seguridad, no es tan nuevo como nos quieren hacer creer. "El machine learning viene aplicándose en las soluciones de seguridad desde hace más de una década, y juega un papel crucial para detectar amenazas que evolucionan a partir de otras anteriores e incluso para detectar malware completamente nuevo basándose en su comportamiento", asegura el responsable de investigación y concienciación de la compañía eslovaca. Añade que el machine learning ayuda a las soluciones de seguridad a diferenciar entre código malicioso y software inocuo, evitando los molestos falsos positivos que muchas veces pueden causar más daño que una infección por malware.

Además de machine learning, María Campos añade de Inteligencia artificial y deep learning como "tecnologías imprescindibles para aumentar la eficacia de las operaciones de seguridad. En la actualidad, los ciberataques continúan aumentando, desbordando a los equipos de seguridad y dificultando su capacidad de detección, contención y reacción ante el creciente número de amenazas", explcia la directiva.

Para el director técnico de Trend Micro, machine learning "es una capa más de protección que hay que añadir a la solución para garantizar la seguridad del endpoint. Ésta en concreto es especialmente efectiva a la hora de detectar amenazas desconocidas o de día cero.

En opinión de Ángel Victoria, machine learning es una de esas tecnologías que permiten situar al antivirus en el peldaño de la Next Generation. "Sin embargo, nuestra experiencia nos dice que lo que las empresas buscan es seguridad y eficacia y les importa poco cómo bautizamos la industria nuestros hallazgos", añade el directivo.

"El Machine Learning es una de esas tecnología que permiten situar al antivirus en el peldaño de la Next Generation"

Ángel Victoria, Country Manager G Data España y Portugal

Tiempo de respuesta

La última pregunta que le hacemos a nuestros expertos tiene que ver con el tiempo de detección del malware de las actuales soluciones de seguridad endpoint. Para María Campos, es evidente que las empresas necesitan acelerar los tiempos de respuesta de detección y remediación de estos ataques. A pesar de ello, asegura que la realidad es que muchas de las actuales soluciones de seguridad endpoint "ya permiten realizar análisis con mayor rapidez y compartir información sobre amenazas en tiempo real. De esta forma, las organizaciones pueden llevar a cabo acciones inmediatas contra aplicaciones, webs o archivos potencialmente maliciosos".

José de la Cruz dice que existen unos mecanismos más rápidos y eficientes que otros, lo que "refuerza la necesidad descrita anteriormente de disponer de una solución que combine de manera coordinada todos ellos minimizando así dichos tiempos de detección y, por tanto, el riesgo".

Para Ángel Victoria el tiempo de detección del malware de las actuales soluciones de seguridad endpoint es suficiente. Añade el directivo que sólo pueden hablar de la seguridad endpoint de la compañía para señalar que "servimos actualizaciones regulares en periodos que en ocasiones se cuentan por minutos. Pero es que una solución endpoint no vive solo de estas actualizaciones, especialmente si queremos instalarnos en la next generation".

Josep Albors reconoce que siempre hay un margen para la mejora "pero si comparamos los tiempos de reacción actuales frente a nuevas amenazas con los que teníamos hace unos años se ha mejorado considerablemente en este aspecto. Todo esto es debido a la implementación de sistemas de inteligencia sobre amenazas, que hacen que aplicándolos a las soluciones de seguridad endpoint estas sean más efectivas".

"El antivirus no ha muerto, a pesar de lo que digan algunos, sino que ha ido evolucionando durante toda su historia y seguirá haciéndolo"

Josep Albors, responsable de investigación y concienciación ESET España

Compartir en RRSS

Enlaces de interés...

- W ¿Son suficientes las soluciones de seguridad endpoint de próxima generación?
- W Ciberamenazas: exploits en el endpoint
- W Movilidad y servicios financieros
- I El mercado del BYOD sigue creciendo
- I La ciberseguridad es la principal preocupación en un despliegue IoT
- V ¿Qué es la seguridad endpoint?

#ITWEBINARS

it Digital Security

Jueves, 26 de octubre - 11:00 (CET)

Regístrate en este IT Webinar y conoce las principales claves de la Regulación Global de Protección de Datos, la nueva normativa europea que exige una nueva forma de gestionar y proteger la información que manejan las empresas, y que será de obligado cumplimiento a partir del 25 de mayo de 2018. ¿Están preparados tus sistemas?

Registro

Martes, 28 de noviembre – 11:00 (CET)

Las organizaciones exigen e implementan nuevas soluciones que les permitan agilizar las operaciones, aprovechar nuevas oportunidades de negocio y ofrecer un mejor servicio a sus clientes.
Pero estas nuevas soluciones y tecnologías también requieren que los responsables de TI mantengan la protección de los activos de su organización y de sus clientes, incluso cuando decidan mover el control de la red, las plataformas, las aplicaciones y los datos más allá de las tecnologías y límites tradicionales de su organización.

Registro

JUAN GARCÍA MORGADO

Juan García Morgado
Research Manager IDC España
Juan García Morgado, Research Manager de IDC, realiza servicios de consultoría y análisis a las principales empresas del sector TI. Juan se incorporó a IDC en 2016 como Analista Senior. Anteriormente, lideró la división de plataformas de servidores para canal de Intel para EMEA. Con una extensa carrera profesional en el sector de las Tecnologías de la Información, ha ocupado distintos puestos de responsabilidad en empresas como Intel (gerente de ventas y marketing), Bull, Microsoft e Indra, como consultor de tecnología. Juan ha cursado estudios de Informática por la Universidad de Sevilla y cuenta con un posgrado en Marketing y Comunicación por la UOC.

La GDPR incrementará el gasto en seguridad

El Reglamento General de Protección de Datos europea (GDPR, General Data Protection Regulation, en inglés) 2016/19 representa un cambio fundamental en el que la Unión Europea gobierna los datos personales y la privacidad. Dicho reglamento introduce cambios sustanciales en la manera en el que los datos deben ser gobernados y protegidos. IDC cree que el cumplimiento de GDPR transformará por completo cómo las empresas gestionarán los datos, el almacenamiento y la seguridad. La nueva regulación continuará promoviendo el gasto en la gestión de seguridad empresarial durante los próximos cinco años y tendrá un impacto significativo tanto en la inversión en software de seguridad como en el mercado de servicios.

IDC prevé que, entre 2017 y 2021, el gasto en seguridad asociado a GDPR tenga un crecimiento

acumulado compuesto (CAGR) de un 19.5%, con un pico en el gasto en 2019, donde alcanzará 162.7 millones de euros en España. Es importante destacar que estas cifras muestran una porción del mercado de la seguridad español que será impactado

IDC prevé que, entre 2017 y 2021, el gasto en seguridad asociado a GDPR tenga un crecimiento acumulado compuesto (CAGR) de un 19,5%

por GDPR. Esta previsión representa sólo una parte del mercado existente en seguridad.

GDPR influenciará una parte significativa de la inversión hasta 2021 en las siguientes áreas:

- Servicios de Seguridad (20.3% CAGR): gestión de servicios de seguridad (28.5%) y consultoría, formación e implementación (18.7%)
- Software de Seguridad (18.8% CAGR): control de contenidos (16.3%), endpoint (13.5%), gestión de identidades y acceso a la información, IAM (18.7%), gestión de la seguridad y vulnerabilidad, SVM (20.7%) y análisis forense (35.2%).

Es importante destacar que el gasto no se distribuirá de igual manera. Según la última encuesta sobre GDPR de IDC las empresas españolas creen que el gasto de seguridad para el cumplimiento de GDPR se incrementará en las siguientes tecnologías:

- Prevención de pérdida de datos, con un 55% de respuestas afirmativas.
- Seguridad específica para entornos en la nube, con un 46% de respuestas afirmativas.
- Gestión de identidades y acceso a la información, con un 44% de respuestas afirmativas.
- Tecnologías de encriptación de la información, con un 43% de respuestas afirmativas.

Por otro lado, el 28% de las empresas encuestadas ven GDPR como una oportunidad para la mejora de la eficiencia del gobierno de la información de la empresa, mientras que sólo el 8% de las empresas encuestadas ve el cumplimiento de GDPR como una ventaja competitiva en el mercado.

Hay que recordar que GDPR es una prioridad de negocio, no sólo un problema de TI. Las implicaciones del no cumplimiento y, por tanto, las sanciones relacionadas, incrementan el riesgo de negocio de forma sustancial. Este es un tema prioritario para los miembros de los comités de dirección de todas las empresas. Las empresas deben estar preparadas para justificar internamente las inversiones de tecnología y procesos para el cumplimiento de GDPR como una prioridad, no como un gasto adicional.

IDC predice que el cumplimiento de GDPR consistirá en una curva de adopción con dos velocidades: la primera consistirá en aquellas empresas que quieran utilizar GDPR como ventaja competitiva y la segunda, compuesta por aquellas empresas que sólo quieran hacer lo mínimo para cumplir la regulación y evitar las sanciones. Ambas aproximaciones son válidas, aunque el uso de tecnología y la implementación de los procesos asociados a cada una de las curvas variarán significativamente.

Existe relativamente poco tiempo para que las empresas desplieguen las necesarias modificaciones y adecuaciones a sus sistemas para poder cumplir GDPR, pero, además, GDPR no debería considerarse como un problema aislado. La Direc-

El 28% de las empresas encuestadas ven GDPR como una oportunidad para la mejora de la eficiencia del gobierno de la información de la empresa

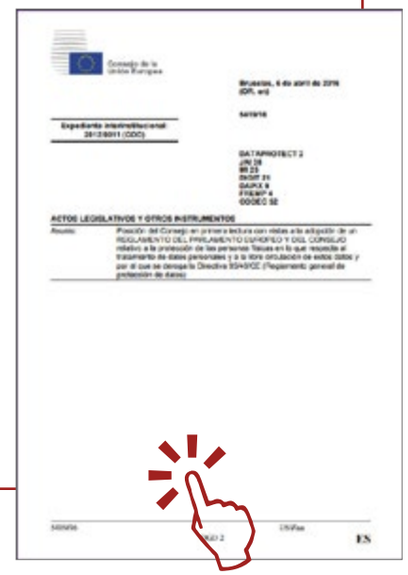
tiva de Red y Sistemas de la Información (popularmente conocida como NIS) y la Regulación de Comunicaciones Electrónicas (ePrivacy) deben ser tratadas de forma paralalela y complementaria.

La entrada en vigor de GDPR será un antes y un después dentro del mundo de la seguridad empresarial, especialmente en la gestión del dato. IDC predice que la implementación de proyectos asociados con dicha regulación influya de forma muy positiva en el gasto TI de las empresas españolas. No obstante, existen dudas acerca del éxito de cumplimiento de la mayoría de las empresas españolas debido a una combinación de incertidumbre, ausencia de tiempo y recursos y aversión al cambio que hará que el gasto asociado a GDPR se ralentice. Además, las organizaciones con sedes centrales fuera de la Unión Europea pueden infravalorar el impacto del no cumplimiento de GDPR en sus negocios. Algunas empresas, especialmente aquellas pequeñas y medianas fuera de la UE, con negocios hacia la propia Unión están adoptando una postura de "espera" que impactará a corto plazo en la posibilidad de realizar negocios con empresas de países miembro.

LA GDPR EN ESPAÑOL, QUE NO TE LA CUENTEN

Hay mil y un documentos sobre la GDPR, la General Data Protection Regulation, la mayoría de los cuales destacan los cambios más importantes de la normativa, los artículos que más impacto pueden tener en las cuentas de la compañía, o qué pasos se deben seguir en caso de detectarse una brecha de seguridad.

Pero si no quieres que te la cuenten, aquí la tienes, en español.



Enlaces de interés...

- 7 preguntas que los CIOs deben responder para cumplir con la GDPR
- Enmascaramiento de Datos y GDPR
- GDPR como ventaja competitiva
- Menos de la mitad de las empresas tienen un plan estructurado para cumplir con la GDPR

Orquestación de seguridad con Inteligencia de Amenazas

Debido a que el panorama de ciberseguridad cambia rápidamente, ¿cómo sabes si la tarea que has automatizado ayer seguirá siendo relevante mañana? ¿Hay alguna nueva información o inteligencia relacionada con esta tarea que pudiera afectar cómo debería funcionar? No siempre se puede estar seguro de que lo que estamos haciendo ahora será lo más eficiente para mañana, y mucho menos en una hora, o la próxima vez que se ejecute la tarea.

Generaciones de Machine Learning en Ciberseguridad

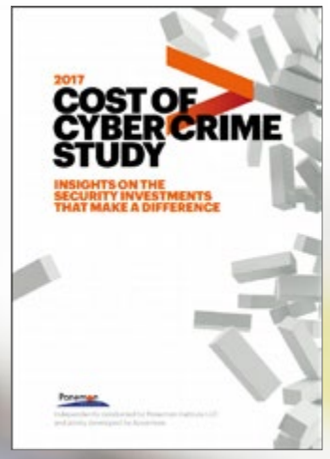
¿Listo para comprobar todas las afirmaciones sobre inteligencia artificial (AI) y aprendizaje automático (ML) en ciberseguridad? Este documento técnico define las Generaciones de Machine Learning y explica los niveles de madurez de la inteligencia artificial (AI) y el aprendizaje automático (ML) que se aplican a la ciberseguridad en la actualidad.

15 Casos de uso crítico de CASB

A medida que las empresas adoptan servicios cloud prácticamente en todas las líneas de negocio, el mercado de la seguridad en la nube está madurando. El descubrimiento basado en registros, una propuesta conocida como Cloud Access Security Broker (CASB) es ahora una apuesta en la mesa. En este documento se proponen 15 casos de uso repartidos entre la seguridad de los datos, la protección contra amenazas y el uso de ciertos servicios y actividades.

El Coste del Cibercrimen

Los ciberataques están provocando un serio impacto financiero en las empresas de todo el mundo. Según un informe elaborado por Accenture y Ponemon Institute, en 2017 el coste medio de la ciberdelincuencia se incrementó hasta los 11,7 millones de dólares por organización, un aumento de 23% respecto a los 9,5 millones de 2016 y un 62% más que hace cinco años. El informe también recoge que cada compañía sufre, de media, 130 brechas de seguridad por año, un 27,4% más que en 2016, y caso el doble que hace cinco años.



La Seguridad TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

¿Estamos seguros ante las pruebas digitales?

Cada vez nos encontramos más la necesidad de presentar pruebas digitales ante cualquier litigio. Afortunadamente la Ley ampara y las personas cada vez toman más conciencia de la necesidad de presentar pruebas conforme a Ley.

CARLOS ALDAMA SAÍNZ

@carlosaldama

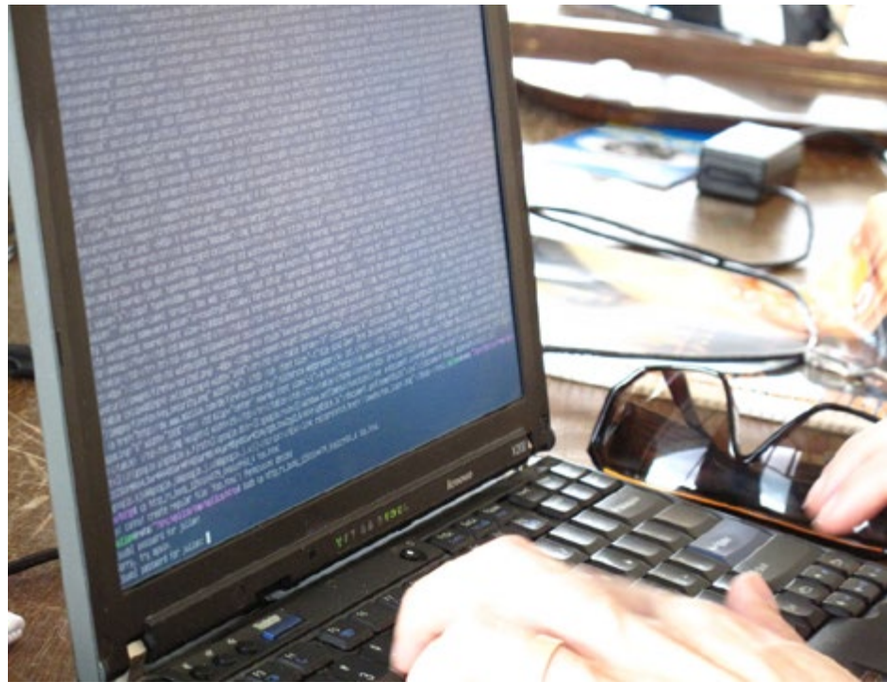
Carlos Aldama Saínz
Perito Ingeniero Informático
Carlos Aldama Sáinz es Perito Informático en exclusiva desde hace más de siete años y con más de 20 años de experiencia en el sector de las nuevas tecnologías, trabajando como consultor y auditor en diferentes empresas.

Ya son pocas las personas que presentan correos electrónicos en papel (y sin dato técnico alguno) o saca “capturas de pantalla” de WhatsApp o incluso presentan unos textos “sacados” de una grabación de audio.

La cadena de custodia dentro de la informática ya parece que comienza a calar en la mayoría de los abogados. Sin embargo… ¿Estamos ante un todo vale?

Como Perito Informático he tenido la oportunidad de encontrarme en los juzgados todo tipo de escenarios, pero últimamente se están incluso impugnando (o intentándolo) cualquier prueba digital con la excusa de “poder ser manipulada” y en parte no falta razón, sin embargo debemos preguntarnos ¿Existe algo hoy en día que no pueda ser manipulado? Si no pudiera manipularse ¿Cuál sería el sentido de la existencia de los peritos informáticos?

Evidentemente las pruebas digitales se pueden manipular, pero ahí es donde entra el Perito Informático, esa figura (de parte o judicial) que garantiza tras análisis técnico (importante esto último) que las pruebas aportadas son veraces y no han sufrido cambio alguno.



Cada vez que alguien aporta conversaciones de WhatsApp en un procedimiento se hace refe-

Dado que una parte de las pruebas digitales puede ser objeto de manipulación, se debe considerar el establecimiento de una correcta cadena de custodia de la información

rencia a la posibilidad de cambio, pero si se realiza un examen forense es posible determinar la existencia de indicios que puedan demostrar una manipulación de las pruebas.

Ocurre lo mismo con los correos electrónicos, sin embargo, debemos tener en cuenta que por un lado la presentación en papel no es la manera de presentarlo, así si nos atenemos a la Ley 59/2003 de Firma Electrónica (LFE) se estable en su artículo 3.5 que:

"Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado."

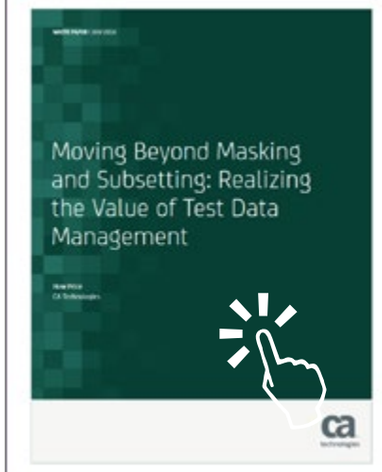
Pero no sólo eso, sino que además la propia Ley en su artículo 267 obliga a que los documentos se aporten en su medio original o mediante copia autenticada por el fedatario público competente.

Es decir, en situaciones de archivos de audio, WhatsApp, correos electrónicos y cualquier otro medio digital, la prueba debe presentarse en su formato original, pero además debe presentarse con una garantía de no manipulación, es decir, con un experto perito informático que pueda garantizar dichos extremos.

Respecto a los fedatarios públicos que autentican los datos debemos tener garantía de que den fe de lo que ven (algo incuestionable), pero que además todo lo que ven no haya sido previamente manipulado (algo para lo que no todos están técnicamente preparados, como es lógico y donde nuevamente se apoyan en la figura de los peritos informáticos).

MÁS ALLÁ DEL DATA MASKING, HACIA LA GESTIÓN DE DATOS DE PRUEBA

Las empresas modernas generalmente tienen bases de datos grandes y complejas, con decenas de millones de registros almacenados en numerosos formatos y utilizando conjuntos de herramientas dispares. Las organizaciones que desean aprovechar los beneficios de un mejor TDM deberían reevaluar la generación de datos sintéticos en toda la empresa, así como la forma en que almacenan, administran y proporcionan datos.



Cada vez nos encontramos más la necesidad de presentar pruebas digitales ante cualquier litigio

Enlaces de interés...

- El Blog del Perito Informático
- El rastro Digital del Delito

Estamos viviendo la era de la información (o incluso de la sobreinformación), todos nos apoyamos en medios digitales y es habitual por tanto que los usemos (si es necesario) en temas de litigiosidad, pero no olvidemos que debemos presentar estas pruebas conforme a Ley y con las máximas garantías para evitar que tras un largo recorrido por la justicia, se pueda desbaratar todo en el último minuto y se dude de la autenticidad de una prueba presentada y que esta incluso pudiera servir para decantar hacia un lado o hacia el otro el resultado del juicio.

Desde mi experiencia he visto presentaciones (impugnadas, lógicamente) de correos electrónicos en papel que la parte contraria no ha admitido, pero también he visto “informes técnicos” que sin rigor alguno dicen haber analizado determinado material informático y ser cierto, pero no permitiendo a las partes acceder al mismo (anulando el derecho a contraste para defensa) ni exponiendo en el informe los análisis que se han seguido para dar lugar a las conclusiones expresadas en el mismo. Esto es realmente grave, dado que igualmente se puede llevar a no tener en consideración la prueba presentada.

Dado que una parte de las pruebas digitales puede ser objeto de manipulación, se debe considerar el establecimiento de una correcta cadena de custodia de la información. Una clara cadena de custodia del medio digital y una correcta documentación de la misma es esencial para que en el momento del análisis (por cualquiera de las partes) se pueda comprobar si durante todo el proceso se ha podido quebrar esta y por lo tanto acceder a la misma para su manipulación.

Con todo lo anterior quiero concluir este artículo indicando que efectivamente, todo es manipulable (y más cuando hablamos de 0 y 1), pero para ello se debe argumentar y presentar de manera técnica (y con conocimiento de las leyes para mostrarlo de manera acorde a estar), pero entendible y que llegue a todos los públicos toda la información técnica objeto de análisis. Sin duda una buena presentación escrita y correcta defensa en juzgado de una prueba informática dará lugar a unos resultados claros y contundentes en los que se afirme si realmente la prueba es veraz o no.

ÁLVARO PURAS DE LUIS

Director de la Oficina de Protección de Datos. Colegio de Registradores de España

Licenciado en derecho y con más de tres años de experiencia en la protección de datos e IT, Álvaro Puras de Luis se estrenó como Data Protection Officer en American Express España. Desde hace unos meses es el Director de Protección de datos del CORPME (Colegio de Registradores de la Propiedad, Mercantiles y Bienes Muebles de España)

El DPO a vista de águila

Los riesgos sobre los datos personales se multiplican de manera proporcional a la transformación que está sufriendo el mundo digital. A medida que se desarrollan nuevas tecnologías y se acelera la globalización de la economía, la sociedad y circulación de datos personales se elimina cualquier tipo de frontera física; incrementándose las vulnerabilidades de la información personal de los usuarios de "La Red". De la mano con estos nuevos riesgos, se ha aprobado y publicado normativa comunitaria que otorga nuevos derechos de protección de datos a los usuarios, al igual que principios de calidad de los datos, y ahí radica el binomio amenaza-oportunidad de negocio.

Por esto, las organizaciones que consigan reciclarse y adaptarse a los nuevos requisitos del Reglamento General de Protección de Datos (RGPD), diseñando su modelo de negocio basado en el dato desde la privacidad; se encontrarán en una posición de ventaja respecto a sus competidores, además de generar la confianza suficiente para atraer a potenciales clientes y usuarios. Uno de los principales nuevos requisitos normativos es el de designar a un Data Protection Officer (DPO), el cual deberá actuar como un "guardián de la privacidad", y con mayor recelo que nunca, teniendo en cuenta la relevancia de las sanciones.

A grandes rasgos, el día a día de un DPO debe

Bajo la GDPR, el Data Protection Officer (DPO) deberá actuar como un "guardián de la privacidad"

consistir en ser el último responsable en la toma de decisiones y enfoque de todas aquellas nuevas iniciativas o desarrollos que afecten a la protección de los datos personales. Del mismo modo, la de educador dentro de la entidad, proporcionando formación a todos los empleados, concienciando de la importancia de la privacidad, generando protocolos preventivos y reactivos ante cualquier brecha de seguridad de la información.

Igualmente se debe encargar de la implantación de mecanismos que permitan auditar y comprobar que los anteriores protocolos y controles funcionan correctamente; otorgando con ello, las suficientes garantías de respeto de los derechos de protección de datos personales. Se debe registrar lo anterior en los oportunos documentos, que deberán estar en todo momento a disposición de las Autoridades de Control (en el caso de España, la Agencia Española de Protección de Datos).

Algunos de los retos ante los que se enfrenta todo DPO son, en líneas generales: (i) demostrar que se han establecido procedimientos internos previos a la creación y puesta en marcha de nuevas actividades de tratamiento de datos personales; debiendo ser consultado en todo momento el DPO; (ii) revisión interna continua y evaluación de calidad de los mecanismos y/o controles; (iii) identificación e inventario de todos los flujos de información de datos personales (data mapping); (iv) establecer procedimientos internos de gestión y notificación eficaces de brechas

Quedará al arbitrio de los responsables y encargados del tratamiento de datos personales la determinación de qué reglas y medidas de seguridad se aplican

de seguridad, y por último, el reto más exigente pero el que garantizará el cumplimiento del requisito del "privacy by design"; (v) la realización de las Evaluaciones de Impacto sobre la Protección de Datos (EIPD) o "Privacy Impact Assessments".

No entraré en el presente a artículo a analizar las EIPD ya que, a día de hoy, hay una gran inseguridad jurídica y práctica respecto a la metodología a seguir para su elaboración. Esto es debido a que las Guías y Directrices que se han publicado hasta el momento, no establecen pautas concretas respecto a qué procedimientos de análisis de riesgos son los más adecuados, ni se establece un listado marco de medidas de seguridad a aplicar para mitigar los riesgos, especialmente los altos. No obstante, a medida que avanzan los meses, parece claro que quedará al arbitrio de los responsables y encargados del tratamiento de datos personales la determinación de qué reglas y medidas de seguridad se aplican para la elaboración de las EIPD y en el gobierno de la información personal (resultará muy interesante tener en cuenta las ISO, Esquema Nacional de Seguridad, etc.).

Otro escollo en el camino será tener establecidos procedimientos de respuesta y notificación de brechas de seguridad de la información, puesto que el plazo de notificación a la Autoridad de Control establecido en el RGPD es de 72 horas; siendo un plazo extremadamente breve para recabar información detallada y elaborar un análisis del alcance de la brecha, así como, dado el caso, una posible notificación a los sujetos afectados.

El DPO, al igual que un águila, debe volar de manera independiente, reportar directamente al más alto nivel de dirección y controlar el campo visual desde arriba; gozando de una perspectiva amplia y de 360 grados de todos los asuntos relativos a la protección de datos. Tendrá que participar en los grupos de trabajo a cargo de la seguridad y tecnología de la información personal y cumplimiento normativo, entre otros. Sólo cuando su perspectiva sea así de amplia, logrará tener una visión, tanto externa como interna, de la organización. El DPO, por tanto, tendrá que actuar como bisagra y punto de cooperación entre la entidad a la que presta sus servicios y las Autoridades de Control.

Enlaces de interés...

- Data Protection Officer, el nuevo superhéroe
- Directrices para el Data Protection Officer (DPO)
- La GDPR en español, que no te la cuenten
- Cuatro consejos para empezar a prepararte para la GDPR

- Cuatro consejos para empezar a prepararte para la GDPR

Sumario No Solo IT

Management y Canal

No les interesa la tecnología

Por José Luis Montes Usategui,

director de Smart Channel Technologies,
director de Channel Academy
y vicepresidente de Walhalla cloud.

Psicobusiness

La Transformación sin el Efecto Colchón

Por Asier de Artaza,

director de www.yesmanagement.es

En la nube

La gestión financiera de la TI híbrida

Por Kevin L. Jackson,

experto en Cloud y fundador de Cloud Musings

Desde mi análisis

El valle inquietante

Por Alberto Bellé,

Principal analyst de Delfos Research

Legal IT

La protección de datos, una utopía clandestina

Por Ignacio González Gugel,

abogado, Socio Fundador de dPG Legal
y Responsable del Departamento
de Asesoría Jurídica

No les interesa la tecnología

Estuve hace un par de semanas en Londres, en el congreso EMEA (Europe, Middle East and Africa) de la CompTIA, invitado por la organización y exponiendo tecnología de Walhalla, la compañía de nube híbrida en la que participo. Resulta tremendamente estimulante, a menudo también retador, asomarse a las ventanas internacionales más exigentes.

José Luis Montes Usategui
Director de Smart Channel Technologies
Director de Channel Academy y vicepresidente de Walhalla Cloud

Hace unos cuantos años que tengo relación con la CompTIA, la que hoy puede considerarse la asociación mundial de canal TI de valor añadido, que acoge también ya a los principales fabricantes y mayoristas del sector, habiéndose convertido en el mayor y más profesional foro global sobre venta de soluciones y servicios de tecnologías de la información. La verdad es que confieso que me encantan, sé de lo que hablo y es MUY difícil conseguir lo que ellos han construido, y lo que siguen construyendo.

Fue un auténtico disfrute participar del encuentro esos dos días, y me gustaría compartir contigo algunos de los aprendizajes que me he llevado de ello. Creo que son relevantes, pienso que el que crea que ya lo sabe todo comienza desde ese día a empeorar, estoy convencido

> "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".

Creo que nos enfrentamos a algo tan grande que en solitario ni el mayor de nosotros será capaz de salir con éxito suficiente

de que en este sector no solo no lo sabemos todo, sino que lo poco que creemos saber está cambiando delante de nuestras narices, y sostengo con convicción de que es ahí fuera, en la calle, donde nos esperan los millones de lecciones que todavía hemos de aprender. Y, ¿sabes qué? … ME PARECE APASIONANTE.

Lo primero que quiero contarte es que mi compañero Quique y yo éramos los únicos españoles allí. Mira, no sé por qué es, pero en los foros internacionales somos muy pocos los de nuestro país que estamos presentes, aunque sea como meros asistentes. No sé si es porque es limitado nuestro nivel de inglés, aún y en nuestro sector tan internacionalizado, y la gente se corta antes de ir a estos foros. O porque no nos enteramos de que existen… si es así, ¿por qué no nos enteramos? ¿Los buscamos, nos interesa enterarnos, estamos conectados con los canales de información adecuados para enterarnos?

El otro día me confesaban en una multinacional española que en Europa están yendo solamente a vender a Polonia, porque los otros mercados les dan respeto … ¿mande? Hace poco escribí una tribuna sobre este tema, así que no me voy a extender más aquí, pero tenemos una barrera falsa, un espejismo que vencer porque no hay nada que nos falte para triunfar en todas partes, si quitamos acaso un ecosistema inversor de la talla de los que tienen empresas israelís, americanas o inglesas. Pero ni un paso atrás, hay que apartar la cortina y ver que nada nos impide estar ahí, en el estrado.

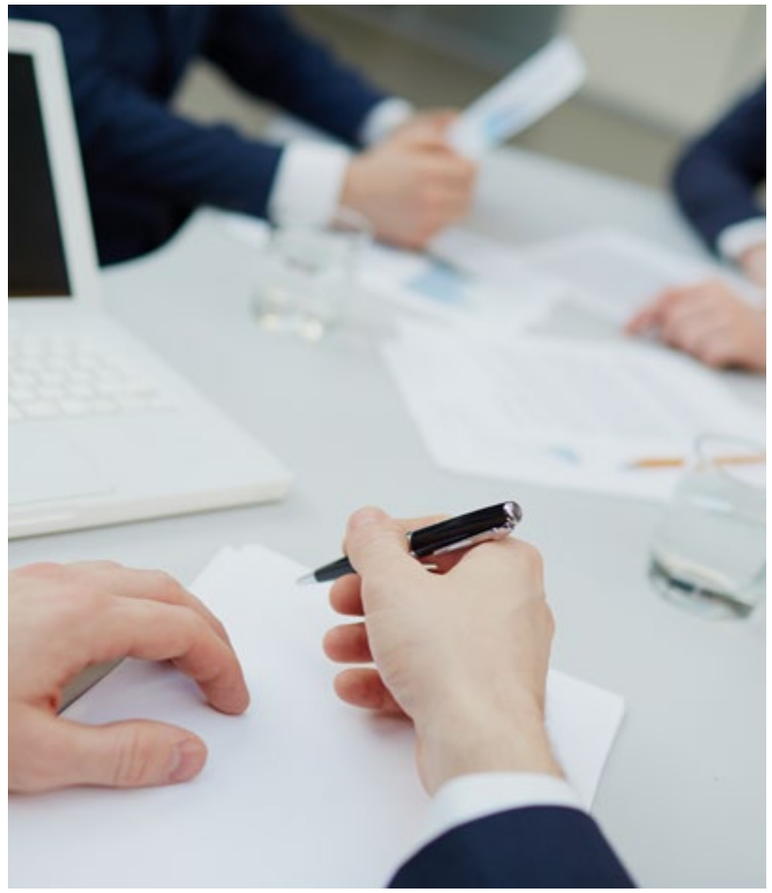
También pude ver la magnífica organización, la exquisita gestión profesional de cada detalle, que disfrutas en los congresos internacionales, incluso en los más modestos. Pero, y es algo que a mí me encanta, en el EMEA CompTIA

Cambios en las tecnologías disruptivas: innovación a nivel global

Este informe de KPMG proporciona perspectivas de las tendencias de innovación tecnológica que se encuentran en el mundo, las principales barreras para comercializar esa innovación y una visión de las mejores prácticas innovadoras en el campo de la tecnología. Esta edición recoge los principales hubs de innovación a nivel mundial.

tuvieron ese nivel organizativo SIN perder el puntito humano, personal, que disfrutas en los encuentros mucho más pequeños. Sentías que las personas hablaban a personas, que había interés en recoger individualmente a cada asistente, que se generaba un ambiente cercano y cálido, aún y siendo más de 500 personas allí congregadas.

Otra cosa que me llevo es haber escuchado montones de conversaciones entre los partners asistentes, con unas sinceras y grandes ganas de colaborar entre ellos, a pesar de ser potencialmente (o no tan potencial) competidores. Se contaban sus problemas, sus dudas, sus retos, y se daban consejos supervaliosos entre ellos: juntos se hacían mejores y, así, juntos hacían mejor el Sector TI. Es una dinámica virtuosa que me encantó comprobar de nuevo, no es la primera vez que la veo en el marco de la Comp-



El canal más avanzado ha evolucionado desde la Integración de Sistemas o el perfil VAR de modelo de negocio hacia el de MSP, Managed Services Providers

TIA y me parece una aportación de valor colectiva de mucho peso, que tengo que decir que raramente veo aquí. La verdad es que, simplemente, creo que nos enfrentamos a algo tan grande que en solitario ni el mayor de nosotros será capaz de salir con éxito suficiente. A lo mejor estoy siendo un poco apocalíptico, disculpa, pero al menos sí que me podrás reconocer que no hay mejor ocasión para coopetir, para competir, pero también para cooperar.

Y dejo para el final la lección más importante que me traje de Londres … y es que a los part-

Salvo alguna charla sobre cosas como blockchain, en la agenda no había casi nada de tecnología, todas las ponencias eran del tipo "cómo sacar negocio de…

ners allí presentes no les interesa la tecnología. ¿A que suena raro de narices? Pues tal cual. Salvo alguna charla sobre cosas como blockchain, en la agenda no había casi nada de tecnología, todas las ponencias eran del tipo "cómo sacar negocio de …" donde los puntos suspensivos eran la GDPR, la digitalización empresarial, un mundo cambiante, o la venta colaborativa. Ni nube híbrida, ni big data, ni SDN, ni nada de lo que aquí domina las agendas de nuestros eventos. ¿Por qué? Porque el canal más avanzado ha evolucionado desde la Integración de Sistemas o el perfil VAR de modelo de negocio hacia el de MSP, Managed Services Providers. Así que lo primero que preguntan es "y yo, ¿cómo haré negocio ofreciendo servicios con tu propuesta?". Si la respuesta que les das les interesa, ya si eso te preguntan por la capa de tecnología que subyace, para obviamente ver si les convence. Así que en la zona de exposición había unos 50 fabricantes, y ninguno hablaba de tecnología, ni uno de los posters o documentaciones de los stands mostraban tecnología: el mensaje central siempre era "haz un estupendo negocio ofreciendo servicios a tus clientes acerca de XXXXX". Debo decir que una gran parte de dichos servicios estaban orientados al Disaster Recovery as a Service, una de las principales propuestas de valor que nosotros llevábamos, así que eso, el compliance con la GDPR, o la ciberseguridad gestionada han sido los asuntos que más interés han concitado en este encuentro EMEA. ¿Son los que te interesan a ti?

Enlaces relacionados

- Congreso CompTIA en EMEA
- CompTIA
- Agenda canal en el Congreso de EMEA de CompTIA

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

La transformación sin el efecto colchón

El éxito de una transformación digital, cultural, estratégica… no está en la solución técnica

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

"Tenemos el cambio ahí mismo, no es tan complejo, las ideas las tenemos claras, yo lo tengo claro, soy el precursor de todo, soy el último eslabón en la cadena".

Pues sí, pero lo que también debemos saber es que la organización es conformista por naturaleza, y no entiende de cambios y menos si deben de ser rápidos.

Y la verdad, podemos tener la mejor de las estrategias, la mejor foto con la que se pueda visionar una transformación empresarial, pero tenemos delante personas, y, nunca lo olvidemos, tenemos delante nuestro, el conformismo, el exceso de confianza, la satisfacción con lo conocido y el rechazo al cambio. Llamémosle a todo ello para entendernos, el statu quo que todo lo amortigua, hablemos de "El efecto colchón".

Quizá tu perspectiva desde un Puente de Mando del buque es eufórica con ganas de cambiar el futuro de la compañía. Tu insuperable motivación y tu destreza técnica en la gestión te puede hacer pensar que las personas de la organización están también ya en otro "modo", pero posiblemente seas tú el único que lo estás, y desde esas gafas percibes con dioptrías la realidad.

Al fin y al cambo juzgamos y percibimos el estado de ánimo de los demás influenciado por el que uno tiene en ese momento, así que, porque nosotros estemos de "subidón", por ahí abajo estarán como siempre.

Aquél es otro mundo, ellos no llevan como tú meses recibiendo inputs de diferentes reflexiones, estudios, maduraciones y revisiones estratégicas que les hayan ido cambiando su configuración mental sobre la situación de la empresa y la necesidad y dirección del cambio. Bueno ellos tampoco son directores, a los que se les atribuye una capacidad diferencial de flexibilidad y adaptación al cambio.

Posiblemente, si bajas un par de peldaños en la organización, en vez de tener un ejército dispuesto a pasar a la acción práctica y querer aportar cosas, nos encontraremos con gente que se queja de su situación ante el nuevo postulado de cambio. Realmente comprende que hay que hacer cosas nuevas, pero no lo encaja de manera eficaz. Ya que lo más probable es que una parte más pancha del regimiento vaya a su ritmo mientras otra no menos muy importante esté estresada.

El verdadero sentido de urgencia es la cuestión clave, generalmente desatendida, por desconocimiento o porque gestionar personas no es fácil, da pereza, y más si no disponemos de procedimientos y técnicas adecuadas

Sí, estresada porque al final su propia personalidad les condiciona a estar muy atareados tratando de afrontar frenéticamente múltiples tareas. Actividades varias de las que probablemente pocas estén subidas al eje central que lleva al éxito de la organización, pero bueno esto sería ya entrar en material de alineamiento de la actividad con la estrategia o productividad en general. Lo dejamos para otro artículo.

Conclusión, esta sobrecarga ineficaz les hace vivir en una constante de agobio que sustituye a la tensión inteligente, por prisas y estados irritables al cambio. Una tensión inteligente que genera urgencia positiva y que, bien gestionada, alineada y en la dirección correcta, es el motor imparable hacia el cambio efectivo.

Pero volvamos al quid de la cuestión, “El Colchón”, éste es el foco de la transformación y no la foto estratégica (ideas brillantes de estructura, procesos y números en dinámicos powerpoints).

Conseguir la inactividad del colchón es lo que no asegura el buen resultado de trasformación, así que a por él sin sobrestimar su potencia destructiva contra el cambio y su prevalencia ante los impactos e intentos de conseguirlo.

Así que sabemos que la norma del pasado prevalecerá ante las nuevas oportunidades, nuevos procesos o retos en general que se le presenten, acolchará todos estos, y, es que es normal, lleva muchos años consolidándose, así que en unos meses no podremos con él... salvo

LA IMPORTANCIA DE LA URGENCIA

CLICAR PARA VER EL VÍDEO

que diseñemos y ejecutemos un exquisito programa de cambio y transformación.

Y no quiere decir esto que las personas no se den cuenta de que hay retos inminentes, sino que piensan que no va con ellos, que ellos concretamente hacen lo que corresponde y esas cuestiones conciernen a aquella persona de aquel departamento.

Total, que llega el gran momento, ¡la puesta en práctica del powerpoint! Con un primer despliegue de las directrices del cambio, y su frenética implementación. Aparentemente, la actividad se vuelve intensa llena de reuniones, presentaciones, dinámicas, puestas en común, ajetreo, ruido, llamadas, mensajes, informes, emails, más emails… marejada a fuerte marejada.

La presión del cambio ha hecho efecto, pero un efecto de temporal caótico fruto de la presión, y no del movimiento ganador, implicado, sensibilizado y con orientación a ganar. En definitiva, muy spanish, presencialismo, horas ocupadas a punta pala, mucho reporte al superior… una vez más, poca eficacia y mucho desgaste, un desastre.

Y, ¿cuál es el antídoto para resolver el efecto colchón? La creación de un verdadero sentido de urgencia y su recreación dinámica a lo largo del proceso.

Y, ¿cómo lo conseguimos? Primero, centrándonos únicamente en las cuestiones críticas, traccionadas por una contundente determinación ganadora que trabajará por acometer algo importante cada día de forma constante.

Constante, concepto nuclear, la gente debe mantener en su pensamiento que la acción determinada sobre las cuestiones críticas de éxito es necesaria ya, no de vez en cuando o cuando le pueda hacer un hueco en la agenda.

Como podemos intuir, la diferencia con la marejada que nos generaba la presión de la dirección ante una organización dominada por el efecto colchón, es que mientras que antes todo el mundo se ocupaba el tiempo con la Mirada más hacia dentro, ahora la Mirada es hacia afuera. Y es hacia afuera con una fuerza motivadora interna que lidera inteligentemente un comportamiento proactivo y alerta a la información, ágil, auténtica y con iniciativa hacia la acción relevante para el éxito, esté delante o haya que salir a buscarla.

Optimizando la experiencia digital: estudio de la transformación IT y digital

El mundo de los servicios TI y el de los servicios empresariales están uniéndose como nunca antes. Esto está impactando en la cultura de IT y en la organización y provocando, a la vez, que los servicios de TI, los servicios digitales y los servicios empresariales estén convirtiéndose en una única línea interconectada. Los dos principales impulsores de esta transformación están actualmente entrelazados: el hecho de que los servicios digitales estén impactando, y en muchos casos re-creando, modelos de negocio, no está en absoluto desvinculado de la llegada de una nueva generación de consumidores más inclinados a ver los servicios digitales como parte de sus vidas diarias.

Este informe proporciona algunos puntos destacados de la transformación de TI y digital tras la investigación de la consultora EMA, e introduce un ejemplo real de iniciativa de transformación digital en una compañía de viajes de nivel mundial.

Todo ello ejerce un círculo vicioso, del que todos se retroalimentan y en el que nadie piensa ya en el presencialismo, en el realizar muchísima cantidad de tareas triviales… sino que es gobernado por un instinto de ganar y para ello busca las opciones más astutas priorizando en aquello que más resultado le dará. En definitiva, desde el liderazgo horizontal y vertical de cada persona en su contribución desde su posición a su organización.

Sin duda, este sentido de urgencia es crítico y debe ser materia fundamental al comienzo y lo largo de todo el proceso de transformación, porque no se produce de forma natural, no es fácil conseguirlo y además hay que trabajar sin descanso para mantenerlo.

Como hemos venido viendo, y era el objetivo de este artículo, el verdadero sentido de urgencia es la cuestión clave, generalmente desatendida, por desconocimiento o porque gestionar personas no es fácil, da pereza, y más si no disponemos de procedimientos y técnicas adecuadas; de ahí el foco que ponemos en el psicobusiness tratando siempre de acercar la eficacia en la gestión del negocio con la maximización de la gestión de las personas. Porque el fondo de todo esto es mover en una dirección corporativa las emociones de las personas, como alguno dice por ahí, los corazones.

Hagamos realidad esta primera etapa de un proceso de transformación, generemos ese sentido de urgencia en los siguientes cuatro ámbitos. Primero identificando las amenazas potenciales que tenemos ante nosotros y mostrando los diferentes escenarios con los que nos encontraremos en el futuro. Segundo, examinando las oportunidades que pueden surgir y explotarse. Seguido debemos comenzar dinámicas de discusión, que acerquen el exterior de la empresa, que sean honestas dando razones convincentes y dinámicas para conseguir que la gente se sensibilice, hable, piense… y haga el cambio como algo suyo. Cuarto, y último elemento, cuenta con la opinión y soporte de clientes, stakeholders externos y gente del sector en general que fortalezcan tus argumentos.

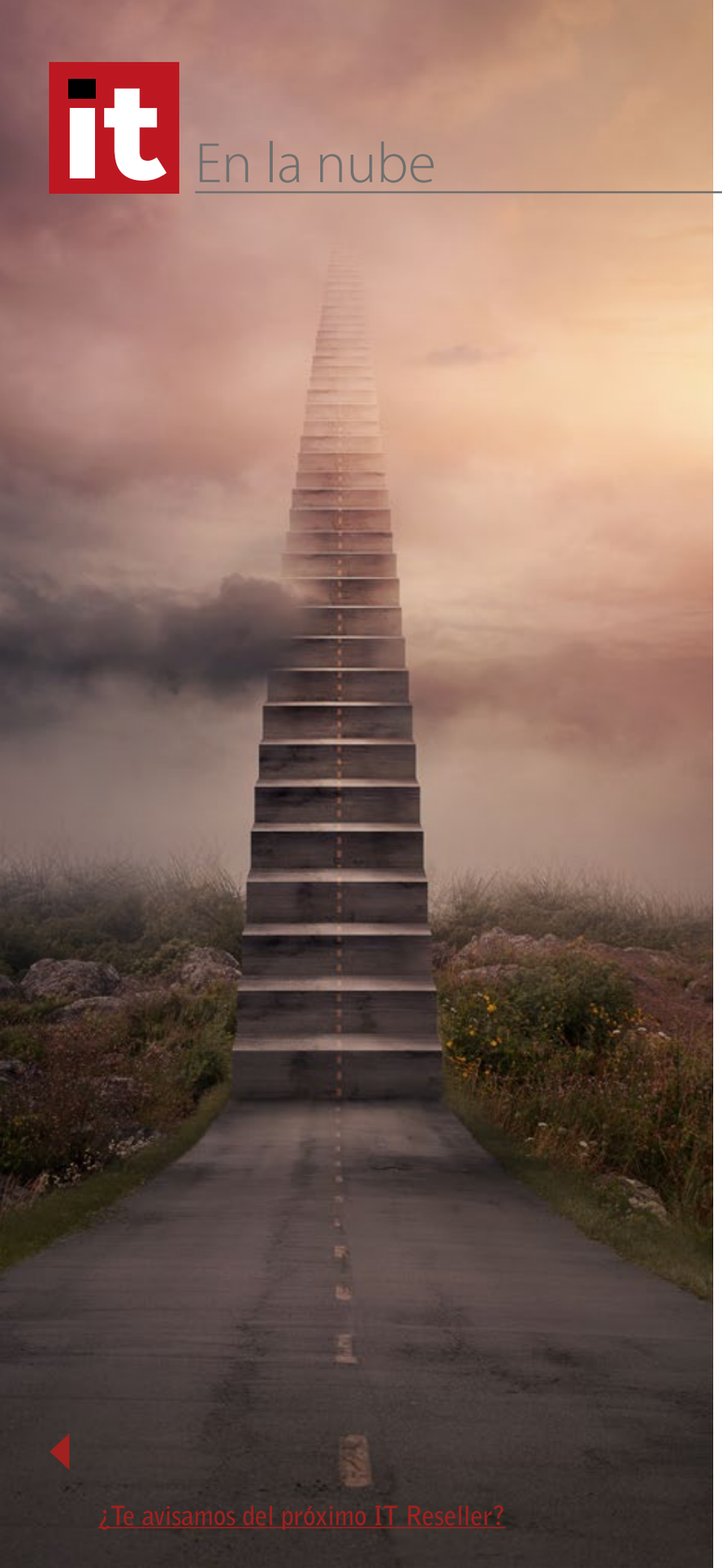
¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Una realidad a remarcar es la tendencia cíclica al desvanecimiento de este sentido de urgencia y, por tanto, la necesidad de implantar planes y un estilo de dirección y de asentamiento cultural que integren la realimentación constante de este activo llamado “sentido verdadero de urgencia”. Especialmente en estos tiempos en que ya no hablamos de gestionar un cambio excepcional en la organización cada 5 o 10 años, ahora la constante es el cambio continuo y lo excepcional la estabilidad, el sentido auténtico de urgencia es la normalidad.

Enlaces relacionados

- Sentido de urgencia
- ¿Están tus empleados preparados para el puesto de trabajo digital en tienda?
- Consumo de TI para PYMES
- Índice de madurez digital en las empresas



La gestión financiera de la TI híbrida

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.

Los costes fuera de control en el cloud computing pueden estar causando una crisis en el sector de las tecnologías de la información. El número -cada vez mayor- de necesidades a resolver, los plazos de transición, cada vez más largos, y las confusas expectativas del mercado han convertido la palabra “transformación” en algo sucio, por lo que las cuestiones sobre la forma de gestionar variaciones y desviaciones de costes entre distintos proveedores proliferan en todos los ámbitos. Un reciente artículo en Cloud Tech nos explica que, si bien la nube pública ofrece ahorros de costes considerables en comparación con otras opciones de nube

privada o instalaciones in situ, también puede incurrir en significativos costes ocultos. Ciertas funcionalidades operativas, como el auto-escalado, pueden disparar los costes con el aumento de la demanda de recursos, haciendo difícil planificar el gasto, y complicando más aún los cálculos de presupuesto. Hay una necesidad acuciante de establecer un sistema holístico y heterogéneo que permita monitorizar los costes de los servicios cloud desde el punto de vista del consumo -por ejemplo, el de una aplicación, o el de una unidad de negocio-, y con suficiente detalle sobre los recursos en uso (por ejemplo, almacenamiento o servicios de computación).

Centrar nuestros esfuerzos en el gobierno de la nube y en la gestión de costes y activos es un paso esencial para aprovechar al máximo las ventajas operativas de la nube híbrida

Justo en la cúspide de todas estas cuestiones nos encontramos al Director Financiero, figura clave en la elaboración del presupuesto de la mayoría de las organizaciones, y responsable de las decisiones financieras clave para cada compañía. Éste es el espacio en el que el espectro de responsabilidades sobre costes en TI se amplía, desde aquellos asuntos puramente financieros, como:

- La optimización
- Las previsiones y proyecciones, y
- Los informes financieros,
- hasta asuntos más mundanos, pero cruciales para la fiscalización contable, como:
- "Showbacks" (visibilidad completa de gastos) y "chargebacks" (asignación de gastos)
- Reconciliación de cargos, y
- Gestión de políticas presupuestarias

La causa más frecuente de estos problemas financieros es la incapacidad para mantener los activos virtuales bajo control en la nube. Muchas empresas pierden por completo la visibilidad y el control de sus costes de cloud compu-

ting simplemente por no identificar ni realizar un seguimiento de dichos activos, algo que desgraciadamente sólo puede detectarse después de haber instanciado cientos o incluso miles de activos en cada entorno cloud.

Los expertos han definido, además, un proceso en cinco pasos que puede permitir a cualquier empresa establecer un sistema de control y gobierno para los costes de sistemas en una nube híbrida.

- **Paso 1:** Establecimiento de umbrales y políticas de gobierno para los servicios
- **Paso 2:** Acceso a las cuentas de provisión de servicios cloud
- **Paso 3:** Monitorización de los costes de servicio, incluyendo costes recurrentes y costes por uso
- **Paso 4:** Comprobación del cumplimiento de límites de coste y uso de activos mediante los motores de analítica de costes correspondientes; identificación y seguimiento de cambios
- **Paso 5:** Simulación y optimización de acciones de control y cumplimiento para un mejor control de costes

La gestión del gasto y de los activos entre distintas nubes híbridas hace necesario disponer de datos útiles y aplicables, que permitirán al director financiero centrar su atención en aquellos activos que rinden al nivel esperado y aquellos que no lo hacen. Por otro lado, el análisis predictivo y las recomendaciones basadas en la experiencia pueden también contribuir a identificar el nivel de prioridad adecuado para aquellos cambios que puedan producir un impacto más eficaz.

La gestión del gasto y de los activos entre distintas nubes híbridas hace necesario disponer de datos útiles y aplicables, que permitirán al director financiero centrar su atención en aquellos activos que rinden al nivel esperado y aquellos que no lo hacen

Estas dificultades pueden ser muy evidentes, pero, en cualquier caso, la solución elegida para mantenerlas bajo control deberá incluir una gestión integral de la nube híbrida. De hecho, las entidades financieras están empezando a ser conscientes del papel crítico que pueden desempeñar en la gestión del modelo de gastos de explotación inherente al cloud computing. Ya están empezando a llegar al mercado servicios diseñados específicamente para

la gestión financiera de medición de servicios cloud, facturación, cargas de trabajo y políticas de prestación de servicios.

Estos servicios de naturaleza financiera permiten a las empresas dar respuesta al aumento de los costes y de la complejidad del cloud computing, proporcionándoles además directrices para los pasos a seguir en su transformación hacia la nube híbrida. El uso de la analítica predictiva hace posible monitorizar y facilitar recomendaciones a través de un único cuadro de mando, por lo que el departamento financiero y el de sistemas pueden contar con un sistema de referencia para el gobierno de dicha nube, pudiendo establecer y aplicar, además, puntos de control mediante políticas de corte financiero y técnico. Estos servicios permiten combinar la identificación de activos con políticas que ayuden al director financiero a delimitar y responder a la variabilidad de los indicadores de su ámbito, antes de que éstos se conviertan en un problema, y, finalmente, la utilización de tecnologías cognitivas permite aprovechar la experiencia del proveedor elegido en cada momento para ofrecer recomendaciones basadas en analítica y servicios cognitivos avanzados. Cualquier acción relacionada con dichas recomendaciones permitirá un uso más racional de la nube, la predicción de futuras tendencias y la identificación de cualquier elemento improductivo.

Si su empresa se enfrenta ahora a estos retos para su transformación, y desea saber más, puede echar un vistazo al concepto de "Cloud Brokerage". Centrar nuestros esfuerzos en el gobierno de la nube y en la gestión de costes y activos es un paso esencial para aprovechar al máximo las ventajas operativas de la nube híbrida.

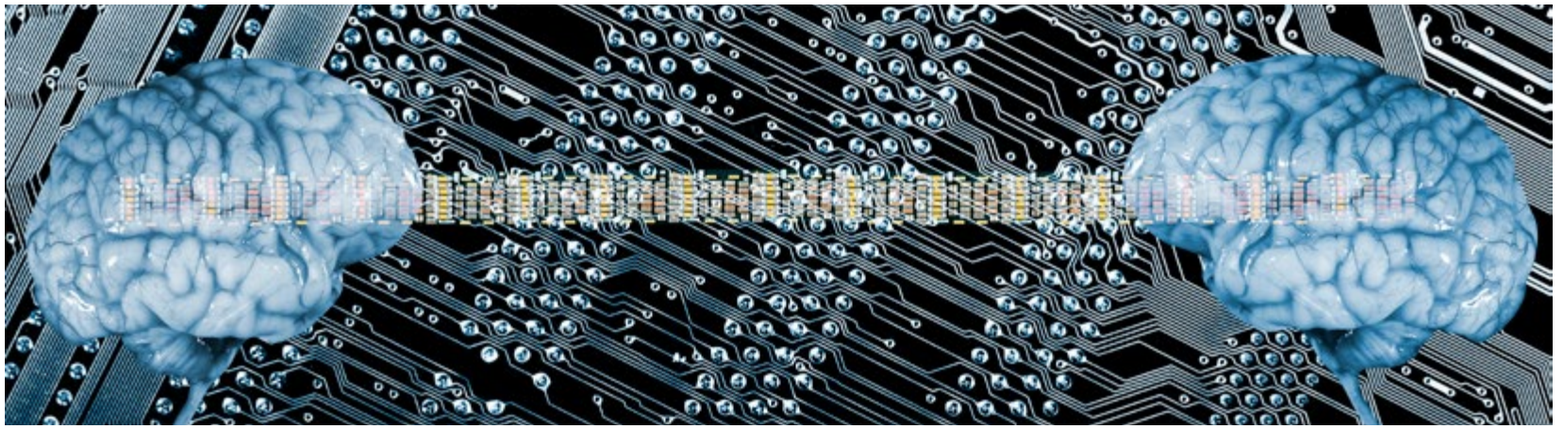
(El presente contenido se está sindicando a través de distintos canales. Las opiniones aquí manifestadas son las del autor, y no representan las opiniones de GovCloud Network, ni las de los partners de GovCloud Network, ni las de ninguna otra empresa ni organización)

¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Enlaces relacionados

- Los costes fuera de control en el cloud computing
- Riesgos de una estrategia single-cloud
- Optimización
- Incapacidad para mantener los activos virtuales bajo control en la nube
- Sistema de control y gobierno para los costes de sistemas en una nube híbrida
- Cloud Brokerage
- Observatorio de competitividad empresarial. La Sociedad de la Información
- Consumo de TI para PYMES



Alberto Bellé
Principal analyst de Delfos Research

La inteligencia artificial tiene que recorrer una montaña rusa: el valle inquietante

Los avances en inteligencia artificial son fascinantes, y la promesa que ésta encierra entra en lo que hace años habríamos calificado como ciencia-ficción. Sin embargo, su éxito comercial vendrá determinado por la disposición de los humanos de aceptarla. En la práctica, el proceso de aceptación requiere superar en algún momento una etapa de fuerte aversión, lo que se denomina el valle inquietante (proviene de la expresión en inglés "uncanny valley"). Esta dinámica debe entenderse en los casos comerciales antes de apresurarse a tomar una decisión.

Vivimos una ola de predicciones que presenta un futuro con robots que se hacen cargo de la mayoría de nuestras tareas, creando un nivel de vida mucho más alto, donde los humanos nos concentraremos en tareas de valor añadido. La pregunta que a menudo se pasa por alto es cómo las personas vamos a asumir el viaje hacia ese futuro prometedor.

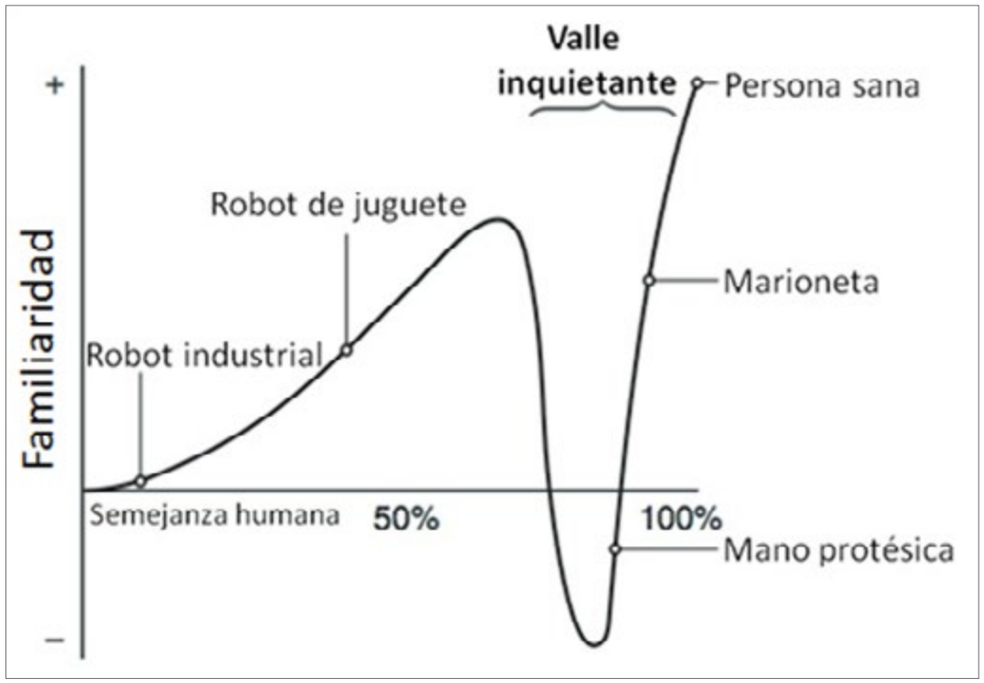
El ciclo de vida tecnológico es bien conocido, sigue un camino ascendente, que puede tomar la forma de un salto en la curva S, con saltos disruptivos en el camino. Sin embargo, en el

Alberto Bellé es principal analyst en Delfos Research, una consultora especialista que ayuda a proveedores tecnológicos y a empresas de diferentes sectores a entender y rentabilizar la oportunidad de negocio del dato. Alberto ha modelado y cuantificado mercados tecnológicos, entre ellos el de Big Data, en las consultoras IDC (Madrid) y BRG (Londres). Asimismo, ha colaborado con la Comisión Europea supervisando la estrategia comercial de decenas de proyectos de innovación, siendo algunos de ellos premiados a nivel europeo.

La promesa de la Inteligencia Artificial: redefiniendo la gestión del trabajo futuro

A finales de esta década, la inteligencia artificial entrará en masa en los negocios. Pero al contrario que anteriores olas tecnológicas, que han trastocado las funciones de los puestos directivos, los recientes avances en IA afectarán a todos los niveles. Imagínese una organización donde la IA automatice la agenda, la asignación de recursos y la generación de informes, eliminando pesadas tareas administrativas. Imagine también lo que la analítica, la simulación y las pruebas asistidas por Inteligencia Artificial pueden ejercer en la toma de decisiones, en la estrategia y en la innovación de toda la empresa.

caso de las interacciones entre humanos y máquinas, la forma de la curva y la dinámica del proceso son bastante diferentes. Comprender esta diferencia podría marcar la diferencia entre el éxito y el fracaso de un proyecto de inteligencia artificial. Esto se sabía hace unos 40 años, y la curva de aceptación se denomina el valle inquietante. El concepto fue acuñado por el investigador de robótica japonés Masahiro Mori. Describe nuestro ciclo de respuesta al interactuar con un robot. Se muestra en el gráfico a continuación:



Inicialmente, nuestra respuesta a la apariencia de un robot es positiva ya que esta se va volviendo cada vez más humana. Sin embargo, en algún momento, cuando el robot tiene aspecto humano, pero no del todo, provoca una fuerte repulsión. Ese es el valle inquietante. Solo cuando la apariencia del robot se vuelve prácticamente indistinguible de la del ser humano, la respuesta emocional vuelve a ser positiva.

Lo interesante es que el valle inquietante no se aplica solo a la robótica, sino a las tecnologías que representan una interacción entre humanos y máquinas inteligentes. En este caso, la clave es poder identificar los factores que definen la experiencia entre persona y máquina, más allá de la apariencia física.

Cada tecnología se encuentra en diferentes puntos en el valle. Por ejemplo, las imágenes y representaciones digitales de humanos lo cruzaron hace años. Otras tecnologías todavía están tratando de subir desde el fondo. Vamos a explorar dos casos:

El primero es la inteligencia artificial orientada al cliente. Los beneficios que la IA puede traer son excelentes: una oferta de autoservicio permanente, que puede crear experiencias de alta calidad cuando se combinan con Big Data y análisis. Esto se ha propuesto como la solución a los desafíos crónicos de outsourcing, ya que las organizaciones luchan por encontrar personal de atención al cliente que combine

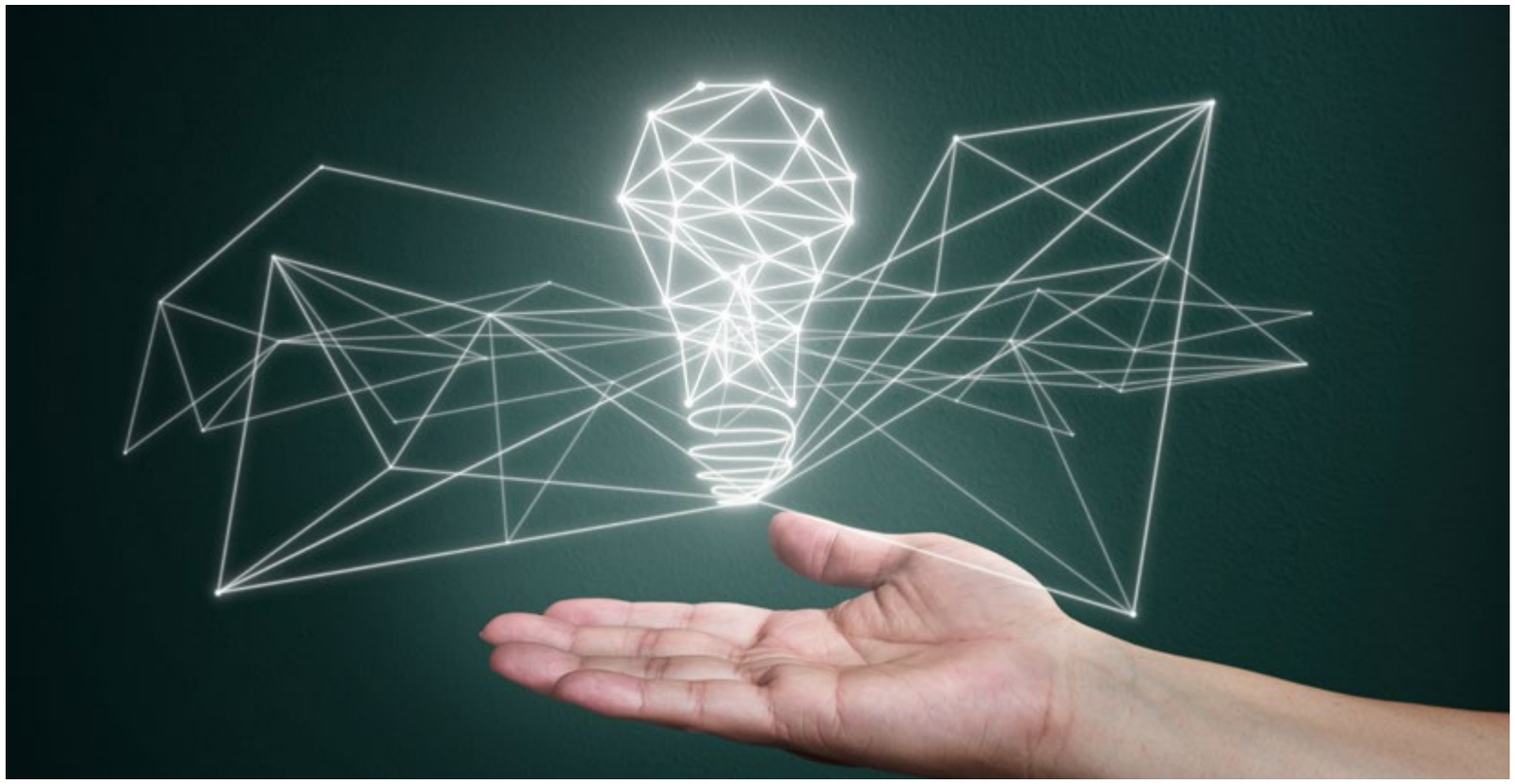
excelencia en sus habilidades, lealtad laboral y salarios competitivos.

Los sistemas básicos de IVR proporcionaban una solución rentable para problemas simples. Con la evolución de la inteligencia artificial, y la llegada de los chatbots y asistentes personales, la gama de problemas que se pueden resolver es potencialmente mucho más amplia. Sin embargo, la experiencia del cliente se puede resumir como incómoda. Existe una impresión general de que la máquina no es capaz de entender realmente a una persona, más allá de resolver un conjunto de escenarios predefinidos. Un estudio publicado en la revista Science en marzo de este año ilustra este punto (el enlace aparece al final del artículo).

Estos sistemas aún no tienen la capacidad de reconocer o evaluar sus propias limitaciones. Además, no pueden tratar la incertidumbre y la ambigüedad, que están presentes en alto grado en la comunicación humana. En definitiva, no conseguido todavía atravesar el valle.

El segundo caso es el de los robots antropomórficos. Después de crear un valor indiscutible en varios sectores (por ejemplo, fabricación), la industria de los robots se está volcando en satisfacer las necesidades humanas y sociales, en áreas como la atención a personas mayores, servicios domésticos o incluso niños con necesidades especiales. En principio, los robots pueden mejorar sustancialmente la calidad de vida de muchas personas, y ayudar a resolver la encrucijada de la dependencia.

Con la evolución de la inteligencia artificial, y la llegada de los chatbots y asistentes personales, la gama de problemas que se pueden resolver es potencialmente mucho más amplia. Sin embargo, la experiencia del cliente se puede resumir como incómoda



En este caso se combinan apariencia física e inteligencia artificial. Existen abundantes desarrollos de robots, que parten de la premisa que al mostrarse la expresividad de la cara y la tecnología del lenguaje, pueden construirse fuertes conexiones emocionales. Invito al lector a que consulte el siguiente enlace y evalúe en qué parte del valle se encuentran los robots que aparecen, y el grado de la conexión emocional.

Además del impacto que nos produzcan estas máquinas, falta un elemento cuando se trata de interactuar con personas: inteligencia emocional. Estas máquinas carecen de una conciencia básica. Como humanos, detectamos que solo estamos tratando con un algoritmo o un motor, por sofisticado que sea, y de esas interacciones no surge la empatía. Es decir, siguen en el valle.

Pero, ¿qué pasaría si un robot atravesara el valle inquietante? Supongamos que lo hace y supera la prueba de Turing (creada para determinar si el comportamiento de una máquina es realmente indistinguible de la de un ser humano). En este caso, puede aparecer una nueva clase de problemas. Un claro ejemplo es el ídolo pop japonés generado por ordenador Aimi Eguchi, que era una combinación digital de las características de seis miembros del grupo pop llamado AKB48, y fue capaz de engañar y luego causar una fuerte conmoción a millones de fans en 2011. Esta anécdota es solo una versión inocua de otros problemas que pueden ocurrir, que dejo a la imaginación del lector.

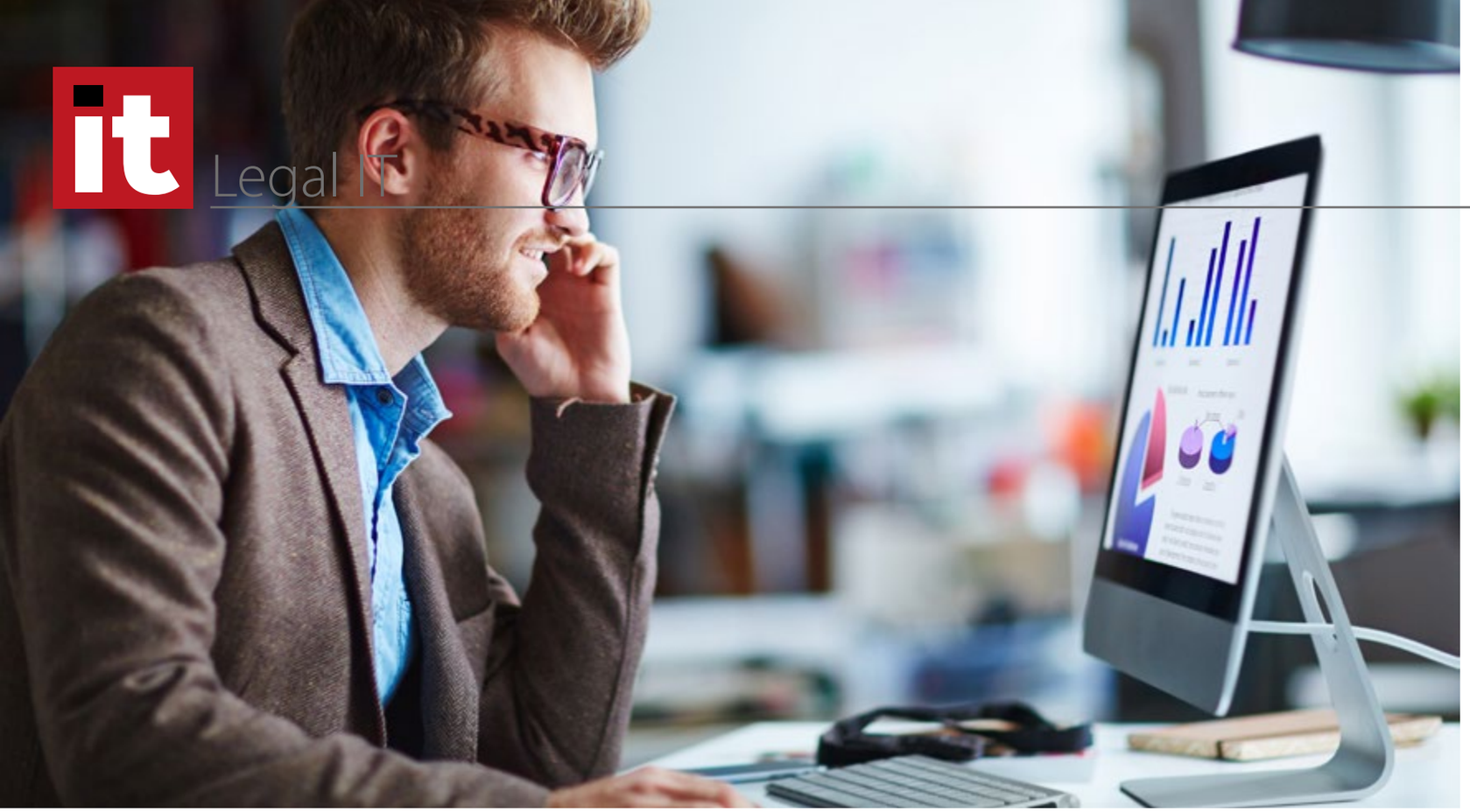
Podemos terminar determinando límites, estableciendo qué actividades pueden realizar los robots y cuáles deben permanecer en el dominio humano

Está claro que no nos gustan los robots que no han atravesado el valle, pero tampoco está claro hasta dónde la sociedad permitirá que los robots entren en áreas consideradas genuinamente humanas. Podemos terminar determinando límites, estableciendo qué actividades pueden realizar los robots y cuáles deben permanecer en el dominio humano. Esto es particularmente claro en el caso de los dilemas éticos. Será necesario crear un diálogo multidisciplinar que aborde estas cuestiones.

Por el momento, el paso más inmediato para cualquier organización que desarrolle estas soluciones sería evaluar dónde se encuentran en el valle inquietante, y qué pasos son necesarios para cruzarlo. No son los entusiastas desarrolladores quienes deben hacer la evaluación, sino los clientes, o las personas que tienen que ponerse en manos de la inteligencia artificial.

Enlaces relacionados

- Cuidado con los robots emocionales
- Robots tan espeluznantes que perseguirán tus sueños
- El misterioso valle de las interacciones humano-robot



Ignacio González Gugel
Abogado, Socio Fundador de dPG Legal y Responsable del Departamento de Asesoría Jurídica

La protección de datos, **una utopía clandestina**

Cumplir la normativa referente a protección de datos parece un sueño inalcanzable. Es una utopía, si se tiene en cuenta el exceso de información y datos que llegan a empresas cada minuto y que debiendo ser analizados, pueden ser objeto de filtraciones o ciberataques. En realidad, el mundo de internet es un mundo abierto y desconocido en el que depositamos nuestra confianza ofreciendo datos de alta sensibilidad.

Esta utopía es clandestina ya que parece que la protección de datos, que indiscutiblemente camina de mano de la tecnología, estuviese oculta tras una sólida e indestructible fachada, pero en realidad está recluida en un habitáculo insípido y vulnerable del que se aprovechan las grandes compañías.

Un reciente estudio de Dell revela que el 82% de los profesionales de las áreas comerciales y de TI encargados de la seguridad de los datos se muestran preocupados por la entrada y el cumplimiento del nuevo reglamento. A pesar de ello, más del 80% aseguran saber muy poco acerca de lo que esta ley supondrá.

Licenciado en Derecho por la Universidad Complutense de Madrid (1998) y Máster en Derecho de las nuevas Tecnologías y Telecomunicaciones por la Universidad Pontificia de Comillas (2001). Es el responsable de los Departamentos de procesal de dPG y de la empresa Indemnización por Accidente S.L. y del área de Compliance. Profesor del Máster de Acceso a la Abogacía en la Universidad Cardenal Cisneros.

Tras varios intentos por comprender qué es exactamente lo que este Reglamento ofrece como mejoras, aparentemente innovadoras respecto a lo que la hasta ahora Ley Orgánica de Protección de Datos suponía, puedo concluir que en realidad no existe tanta diferencia.

La Ley Orgánica de Protección de Datos reconocía el consentimiento tácito del usuario, modalidad que daba lugar a infinidad de confusiones y malentendidos y en muchos casos permitía a la empresa asumir el derecho a cobrar por servicios o suscripciones que el usuario jamás tuvo intención de contratar. Para solventar esto, el nuevo reglamento determina que el consentimiento dependerá de una clara acción afirmativa.

Pero seamos claros, no importa si ese consentimiento es expreso o tácito, ya que nos vemos obligados a prestar ese consentimiento. Empresas como Cabify piden nuestros números de DNI tras realizar el primer trayecto. ¿Para qué? Ya tienen el número de tarjeta y además realizan el cobro de antemano y les damos acceso a nuestra ubicación. ¿No es suficiente? Parece que no.

Este nuevo reglamento plantea además una serie de retos que deberán hacerse efectivos desde su momento de aplicación y su obligado cumplimiento, el próximo 25 de mayo. Habrá empresas que lo tengan más fácil porque tecnológicamente estén más desarrolladas. Pero supone una difícil tarea para las pequeñas y medianas empresas, especialmente por no tener la capacidad de supervisión y monitorización que poseen las grandes.

Y SI NO CUMPLO CON GDPR, ¿QUÉ?

CLICAR PARA VER EL VÍDEO

Cómo dar cumplimiento al nuevo Reglamento General de Protección de Datos de la UE

El próximo mes de mayo de 2018 entrará en vigor la aplicación del nuevo Reglamento General de Protección de Datos de la UE (General Data Protection Regulation, GDPR) y aún existe una gran confusión acerca de cómo dar cumplimiento al GDPR. Muchas organizaciones aún no tienen una estrategia o no saben por dónde comenzar.

Este documento revisa algunos de los principales aspectos que introduce el nuevo Reglamento General de Protección de Datos de la UE (General Data Protection Regulation, GDPR) así como qué estrategia pueden seguir las empresas e instituciones públicas para cumplir con este nuevo reglamento.

GDPR: DÓNDE ESTÁN LOS DATOS A PROTEGER

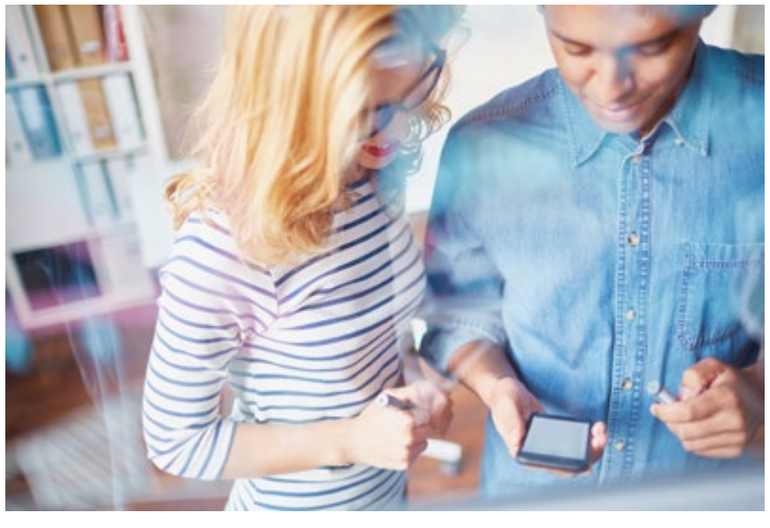
CLICAR PARA VER EL VÍDEO

La nueva normativa presenta también la figura del Data Protection Officer, que adquiere carácter obligatorio en las empresas y su tarea principal es la de supervisar y proteger los datos de los usuarios y la empresa. El problema es: ¿cómo se va a abordar esto en la práctica? Sin duda, esto supondrá un gasto para todas las empresas que pretendan tener todo en regla y así evitar las sanciones de hasta 20 millones de euros que este nuevo reglamento impone por el incumplimiento de sus preceptos.

No es la única incógnita que plantea la nueva ley. ¿Cómo se va a controlar que el derecho de los ciudadanos al olvido, como otorga éste, se lleve a cabo en un mundo digital en el que parece que no hay control? ¿Cómo se van a recopilar datos biométricos y de genética? Pero, sobre todo, ¿para qué? ¿Cuál es la razón que hace indispensable recopilar esta serie de datos? ¿Es control o se trata simplemente de una merma en la privacidad?

¿Cómo va a compaginarse este reglamento con el creciente interés en el Big Data que transmite y recopila toneladas de información quedando registrada y pudiendo ser visible y llegar a manos de quien no queremos que llegue?

Empresas como Google ejercen un tremendo poder sobre todos. Pareciera que debemos estarle agradecidos a esta empresa por hacernos la vida más fácil, por ser “voluntariamente” quienes damos nuestro consentimiento para facilitar nuestra información. Resulta paradójico que para sentirnos más libres y protegidos estemos dando una información y un consentimiento, que en la mayoría de los casos es obligado, para poder continuar desempeñando funciones del día a día.



¿TE HA GUSTADO ESTE REPORTAJE?

Compártelo en tus redes sociales

Hemos dejado que las empresas conozcan tan bien quiénes somos, qué nos gusta y qué hacemos, que ahora resulta difícil, si no imposible, volver atrás. Sin duda, solo cabe quedar expectante con lo que la tecnología pueda y quiera hacer de nosotros.

Enlaces relacionados

- V [Y si no cumplo con GDPR, ¿qué?]
- W [GDPR: cómo lograr una gestión adecuada de la información]
- I [Más de un tercio de las empresas no sabe si debe cumplir con GDPR]
- V [GDPR: dónde están los datos a proteger]
- I [Los altos directivos europeos suspenden en implantación de GDPR]
- W [Siete preguntas que los CIO deben responder para cumplir con GDPR]

it User
TECH & BUSINESS

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