it Reseller
TECH&CONSULTING
Diciembre 2017 - nº 29



# La tecnología protagonista de las compras navideñas

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


it Digital MEDIA GROUP

**Juan Ramón Melara**
juanramon.melara@itdmgroup.es

**Miguel Ángel Gómez**
miguelangel.gomez@itdmgroup.es

**Arancha Asenjo**
arancha.asenjo@itdmgroup.es

**Bárbara Madariaga**
barbara.madariaga@itdmgroup.es

**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

¿Te avisamos del próximo IT Reseller?

# Nueva campaña de Navidad, nuevas expectativas de negocio

*Anualmente hay una serie de hitos que se repiten en nuestras vidas y nos afectan de forma más o menos directa. Algunos de ámbito festivo, como los Sanfermines o Las Fallas; otros de índole económica, como la fecha límite de la Declaración sobre el Impuesto de la Renta; otros reiterados pero sin fecha fija, como el inicio de las vacaciones de verano; y otros, como el que nos ocupa aquí, que sirven para poner el broche, ya veremos si de oro o no, del mercado de consumo en nuestro país y como termómetro para conocer cómo está realmente la venta de tecnología en el segmento Retail y otros canales de gran consumo.*

*Nos referimos, como ya habrán adivinado, si no por el texto, sí por la fecha, a la tan mencionada campaña de Navidad, a la que, de un tiempo a esta parte le han salido dos grandes competidores, o aliados, según se mire, como son el Black Friday y el Cyber Monday.*

*Como esto no se trata de a quién quieres más, si a papá o a mamá, o de a quién le pides los juguetes, si a Papá Noel o a los Reyes Magos, tanto los pasados Black Friday y Cyber Monday como la próxima campaña de Navidad, han puesto su granito en el granero del mercado de consumo español, y todo parece indicar que este año tenemos razones para ser optimistas.*

*Los datos que llegan desde estas dos importadas tradiciones del consumo norteamericano son positivos, y el valor medio de la cesta de la compra de los españoles se ha incrementado de forma considerable. Ahora llega la campaña de Navidad, donde la tecnología tiene más competencia en los lineales, tanto por otros regalos como por alimentación y decoración, pero todo parece indicar que nuevamente la tecnología, cada vez más indispensable para la población en general, se coronará como la reina de las navidades. Solo falta que las previsiones se confirmen y tengamos, este año sí, una feliz campaña de Navidad. Al menos, esto es lo que opinan tanto las consultoras como los jugadores del mundo de la distribución TI que hemos preguntado en la elaboración de nuestro En Portada de este mes. Esperemos que todos estén en lo cierto.*

***Juan Ramón Melara***
***IT Digital Media Group***

# Sumario

## En portada


## IT Digital Security


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

## Responsabilidad Social Corporativa

Voluntariado, una forma de realización personal ayudando a los demás

## Actualidad

MMe 2017 trae a Madrid “la nueva Tech Data”

El canal de distribución de TI en Europa crece a buen ritmo

Los partners pueden jugar un papel crítico en la adaptación a GDPR

¿Qué mejoras necesitan las tiendas on-line?

## Especiales IT Reseller

MCR premia a los mejores de 2017 en la décima edición de sus galardones

## Reportaje

DaaS: un negocio disruptivo para el canal de PC corporativos

## Índice de anunciantes



¿Te avisamos del próximo IT Reseller?

No solo it

# 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 espera cerrar el año facturando más de 1.000 millones y creciendo el doble del mercado**

# MMe 2017 trae a Madrid 'la nueva Tech Data'

*Poco más de un año después del anuncio de la compra por parte de Tech Data de Avnet Technology Solutions, la nueva Tech Data se ha presentado en Madrid en la tercera edición de Metic Madrid Especialista, un evento en el que el mayorista ha reunido a cerca de un millar de personas para contarles las líneas básicas de su estrategia, y mostrarles las nuevas oportunidades de negocio que se abren en el mercado alrededor de lo que denominan Advanced Solutions.*

El estadio Santiago Bernabéu ha acogido la tercera edición de MMe, Metic Madrid Especialista, un evento en el que Tech Data, además de hablar de las posibilidades de negocio alrededor de las nuevas tecnologías que irrumpen en el mercado como en años anteriores, ha querido presentar la nueva realidad de la compañía, un presente y, sobre todo, un futuro marcado por la compra de Avnet Technology Solutions anunciada hace ahora poco más de un año.

La nueva Tech Data se define de dos maneras. En palabras, por la intención de consolidarse como "el enlace vital entre proveedores y distribuidores en el nuevo ecosistema TI con una propuesta de soluciones extremo a extremo", señalaba Santiago Méndez, Advanced Solutions director Tech Data Iberia, o por números, una compañía con unos ingresos pro-forma en 2017 de 36.000 millones de dólares y más de 115.000 clientes a nivel global, si bien sus res-

ENTREVISTA A PAULÍ AMAT, COUNTRY MANAGER DE TECH DATA ESPAÑA


CLICAR PARA VER EL VÍDEO

# "Tech Data cuenta con una gran ventaja competitiva, una propuesta de valor extremo a extremo"

## Oriol Cornudella, managing director de Tech Data Iberia

ponsables quieren que se relacione la nueva compañía con conceptos tales como eficiencia, conocimiento, calidad de servicio, experiencia de usuario y cuidada ejecución en todos los aspectos.

Y es que todos los cambios llevados a cabo por el mayorista en los últimos meses son imprescindibles para seguir posicionados en un mercado cambiante. En palabras de Oriol Cornudella, managing director de Tech Data Iberia, "los mayoristas necesitamos evolucionar para seguir siendo competitivos", si bien añade que Tech Data cuenta con una gran ventaja competitiva, "una propuesta de valor extremo a extremo".

La nueva estrategia pasa por sacar provecho del catálogo de soluciones y servicios y de la amplitud del número de clientes, incrementar las inversiones para potenciar los negocios alrededor de tecnologías de nueva generación; buscar nuevos modelos de venta y delivery; aprovechar su presencia en los diferentes mercados y clientes; y consolidarse como una referencia en todos los ámbitos.

### Dos divisiones para una propuesta extremo a extremo

La nueva Tech Data se divide en dos divisiones de negocio. Por una parte, incluyendo todo lo relacionado con el PC), la división End-Point Solutions, y, por otra, relacionado con las llamadas tecnologías de nueva generación, Advanced Solutions, que, a nivel global, se reparten en un peso similar, 45% cada una, dejando en manos de los negocios especializados el restante 10%. Sin embargo, en el caso español el reparto es un tanto diferente, y se estima que la división End-Point Solutions podría suponer algo más del 65%, mientras que Advanced Solutions supone un tercio de la facturación. Eso sí, los porcentajes cambian cuando hablamos de beneficios, dado que, en ese caso, Advanced Solutions supone en torno a la mitad de la cifra acumulada, porque, como explicaban desde el mayorista, la rentabilidad de las operaciones de Advanced Solutions es un 50% superior que las de End-Point Solutions.

En cualquier caso, estos pesos en los ingresos podrían evolucionar de cara a los próximos años, dado que las oportunidades de crecimiento son mayores en las soluciones de nueva generación, como Cloud, donde se estima un incremento de la oportunidad del 30%, Software del 9%, Analytics del 7% o Security del 7%, frente a incrementos del 3% esperados en la oportunidad alrededor del negocio de movilidad o el 1% en el caso de las tecnologías específicas del centro de datos.

Por este motivo, los grandes focos de a compañía para los próximos meses estarán puestos en áreas como Cloud, donde Tech Data de la mano de proveedores como Microsoft, IBM o Amazon; Analytics e IoT; Seguridad, un negocio creciente, sobre todo, con la incorporación de nuevos contratos provenientes de Avnet TS; y servicios.

## El papel del cloud en la nueva Tech Data

Tanto Santiago Méndez como Martín Trullas, Next Generation Manager, reconocían que cloud va a ser uno de los focos fundamentales para el año próximo, porque no podemos olvidar que las previsiones de Canalys apuntan a que en 2019 el 50% de las ventas de soluciones cloud se harán en un modelo 2 Tier, y que las estimaciones para los próximos dos años es un incremento de la cifra de negocio, tomando como referencia los asientos, del 160% anual.


> "En cloud ser el número 1 nos da una ventaja competitiva importante con la base instalada"
>
> Oriol Cornudella

Además, reconocían los responsables de Tech Data que se trata de un negocio "con unos márgenes muy importantes", y quieren hacer valer su posición, porque "somos número 1 de venta de soluciones cloud de Microsoft", en un negocio que este año ha duplicado las cifras del año anterior, y que el año próximo volverá a duplicarlas, si se cumplen las previsiones.

Para Oriol Cornudella, "ser el número 1 nos da una ventaja competitiva importante con la base instalada", y justificaba su posición en el negocio porque "somos capaces de dar al cliente una propuesta cloud extremo a extremo".

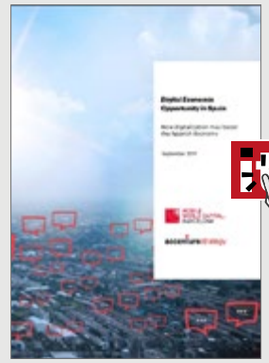
## Duplicar el crecimiento del mercado

A punto de adentrarnos en las últimas semanas del año, los responsables de Tech Data han hecho también balance del año, un ejercicio en el que estiman que van a crecer el doble del mercado, cifra, la del mercado, que podría situarse entre el 8 y medio y el 9 por ciento.

El incremento de negocio de Tech Data en nuestro país, que superará al cierre del ejercicio los 1.000 millones de euros, se apoya en negocios como la movilidad, el software, la mencionada cloud y el negocio especializado.

Este crecimiento ha provocado que Tech Data haya ganado, según sus responsables, cuota

## *Oportunidades de la economía digital en España*



Accenture Strategy y Mobile World Capital Barcelona han alineado sus conocimientos y esfuerzos para desarrollar este estudio con dos objetivos: determinar el impacto de la aceleración de la Transformación Digital en España y crear conciencia de la urgente necesidad de esta aceleración entre todos los actores involucrados.


# 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.

## Tech Data prepara nuevas Software Stores dedicadas para sus fabricantes

Disponible a partir del próximo febrero, las nuevas tiendas, a las que se puede acceder a través de la pestaña Software en el área principal del sitio web InTouch de Tech Data, cubren Acronis, Adobe, McAfee, Microsoft y Veritas. El objetivo es facilitar a los revendedores la búsqueda de las licencias o suscripciones.

Tech Data cambiará a los usuarios de Licensing Online (LOL) a sus nuevas Software Stores y su herramienta InTouch a partir del próximo mes de febrero, según recoge un artículo de IT Europa. Las nuevas Software Stores dedicadas para sus proveedores tienen como objetivo facilitar a los revendedores la búsqueda de las licencias o suscripciones adecuadas para los clientes, e incluirlas en presupuestos y pedidos estándar.

Las nuevas tiendas, a las que se puede acceder a través de la pestaña Software en el área principal del sitio web InTouch de Tech Data, cubren Acronis, Adobe, McAfee, Microsoft y Veritas. Todas las licencias y suscripciones disponibles también se pueden encontrar a través de una búsqueda y ser incluidas en las ofertas y los pedidos como líneas de pedido normales.

Los cambios se han realizado para reunir todas las opciones de software en un solo sistema. Según Lauren Cooke, directora de ventas de software en Tech Data, "el panorama del mercado del software está cambiando y todos los proveedores se están moviendo a un modelo de suscripción. Sentimos que era hora de reunir todas las opciones de software, ya que esto facilitará la tarea de los socios, ya hayan utilizado principalmente licencias o hayan vendido productos de paquete completo en el pasado. Con las nuevas Software Stores, es más fácil encontrar lo que desea e incluirlo en un pedido normal ".

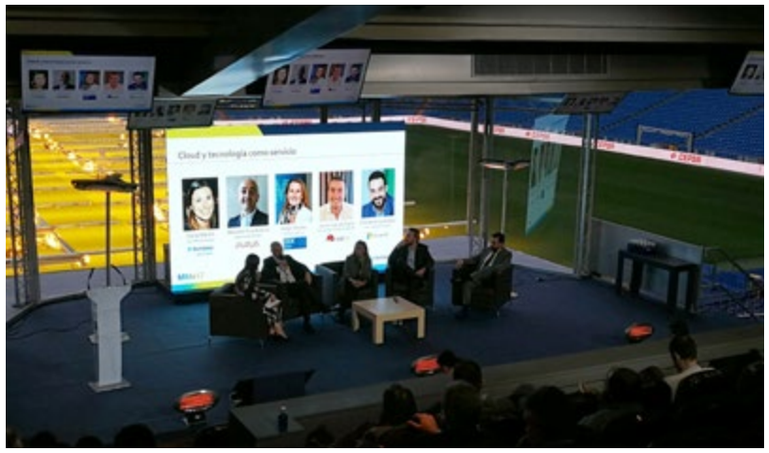
El espacio de Microsoft ha sido el primero en promocionarse en la nueva prestación Software Store incluida en el portal InTouch. En las páginas de Microsoft Store, el distribuidor puede encontrar una jerarquía de productos de Microsoft, con un motor de búsqueda de productos de licencia e información sobre los programas de licencias del fabricante, las últimas novedades o las promociones vigentes o los productos más solicitados. Gracias a la integración con los sistemas de Microsoft, el procesamiento de los pedidos es sencillo, rápido y totalmente automatizado.

de mercado en España, que podría estimarse en el 23 o el 24 por ciento del total, "a Esprinet, Vinzeo, algo a Ingram Micro, y algo a otros mayoristas de nicho", si bien también añadían que este año se han incrementado los nuevos negocios, el negocio nuevo en partners tradicionales, y el negocio tradicional en partners nuevos. Y también ha apoyado estos números la homologación en Patrimonio para soluciones de Educación, "lo que ha ayudado a nuestros distribuidores a realizar nuevos negocios", o el lanzamiento de los nuevos servicios, que ya


presentaron en la pasada edición de MeTIC, a lo largo de estos meses.

De hecho, según cifras globales, aplicables a España, un 40% de los clientes del mayorista lo son de las dos divisiones, lo que también aporta razones para la evolución de la cifra total de negocio.

Mención aparte merece la seguridad, "responsable de gran parte del crecimiento de este año", apuntaba Méndez, que es ha vito reforzada por la entrada de nuevos jugadores y contratos procedentes de Avnet TS. De hecho, se han



incrementado tanto el negocio concreto de seguridad, explicaban los responsables de Tech Data, como el área de seguridad en proveedores más establecidos en el fabricante, con lo que el área de seguridad gana protagonismo en la propuesta de soluciones extremo a extremo de la firma.

También a lo largo de estos meses ha tenido lugar el cambio de sede del mayorista a Madrid, “donde se encuentran dos tercios de nuestros recursos”. El cambio se ha producido, tal y como explicaba Oriol Cornudella, “por coherencia y por reducción de riesgos”.

Por último, cabe destacar que uno de los focos de Tech Data para el año próximo será Tech Data Academy, con la que pretenden incrementar la cifra de negocio alrededor de la formación a lo largo de los próximos meses.

## MMe2017 otorga protagonismo a las nuevas tendencias y oportunidades

Hablando específicamente de la tercera edición de MMe, las grandes tendencias tecnológicas y la oportunidad que traen consigo para el canal, fueron las grandes protagonistas de la cita, que reunió a alrededor de un millar de personas. Y es que Tech Data organizó el programa alrededor de una zona de exposición y cinco mesas redondas que trataron temas tale como las plataformas híbridas y os nuevos retos de la infraestructura; cloud y la tecnología como servicio; ciberseguridad y las nuevas soluciones para las nuevas amenazas; movilidad corporativa, el trabajo ya no es un lugar; y la modernización del puesto de trabajo, la transformación digital al servicio de los empleados.

Asimismo, la compañía aprovechó la oportunidad, como hemos comentado, para presentar la nueva Tech Data y su estrategia, así como el cambio de imagen corporativa experimentado en los últimos meses. Por último, quisieron dar a conocer la fecha del siguiente gran evento que prepara el mayorista, que ya será MeTIC 2018, que tendrá lugar el próximo 13 de marzo en la Ciudad Condal.

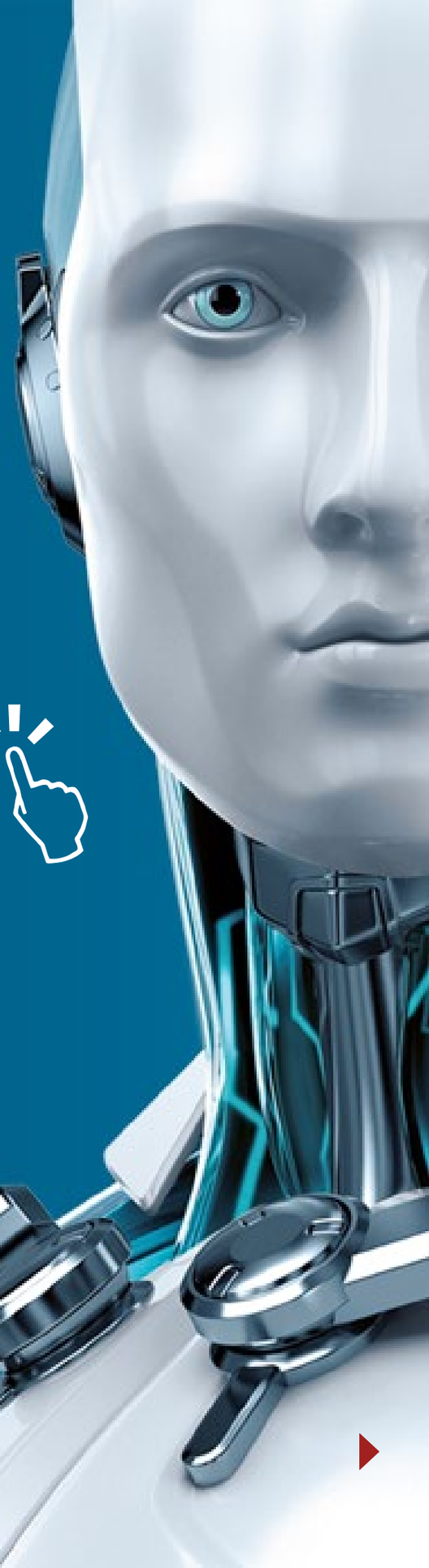


### Enlaces relacionados

- I HolaMeTIC2017
- W Herramientas para potenciar el negocio
- I Tech Data y Aruba promocionan la gestión de red en la nube
- I Tech Data promociona la venta de soluciones de HPE
- I Acelerador de oportunidades: ecosistema OEM de HPE y Tech Data
- W La verdad sobre el ecosistema de IoT
- W La reinvención digital: una oportunidad para España

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**

**Los ingresos de los mayoristas por ventas de PC continúan al alza**

# El canal de distribución de TI en Europa crece a buen ritmo

*Tres nuevos estudios del Global Technology Distribution Council (GTDC) confirman la expansión de la distribución de tecnología en Europa a través de tecnologías disruptivas, capacidades de servicios y modelos de dos niveles. Actualmente, los miembros de GTDC generan más de 130.000 millones de dólares, una gran parte de ellos en Europa.*

El mercado europeo está preparado para una aceleración en el negocio de distribución de tecnología, según tres informes recientes emitidos por el Global Technology Distribution Council (GTDC). Entre los factores clave que contribuyen a esta aceleración están las oportunidades de crecimiento creadas por desarrollos disruptivos como la Internet de las Cosas (IoT), la mayor utilización de servicios de TI y la adopción de modelos de distribución de dos niveles. Actualmente, los miembros del GTDC generan más de 130.000 millones de dólares en todo el mundo, con una amplia y creciente representación en Europa.

"El mercado europeo está preparado para aprovechar las fuerzas disruptivas que afectan a los canales de TI en todas partes", señala Tim Curran, CEO de GTDC. "La localización, la especialización y los modelos de distribución de dos niveles pueden haber sido vistos de manera diferente en el pasado, pero estos enfoques ahora se consideran ventajas comerciales importantes"

Los mayoristas y fabricantes están colaborando en los frentes operativo, estratégico y de desarrollo en Europa y en otros lugares, según el último informe de GTDC, 'The Distribution Landscape and Disruption'. El informe incluye

## *Informe Bankintercard. Transformación hacia un consumo más digital*

Los usuarios españoles de tarjeta han aumentado un 71% su gasto en compras online en tan solo cinco años. Para 2017, está previsto que este gasto sea de una media de 877 euros en consumo online, un 12% más que en 2016.

Asimismo, los consumidores online han pasado de realizar 8,1 movimientos de media en Internet en 2013 a los 13,5 estimados para 2017, lo que supone un aumento del 67% del número de compras en Internet en tan solo cinco años.


Estos son algunos de los datos del II Informe bankintercard, elaborado por Bankinter Consumer Finance sobre la base estadística de los movimientos de casi 800.000 usuarios de tarjetas de crédito.

una inmersión profunda en las tendencias que afectarán a los acuerdos de canal hasta el año 2022. Según éste, muchos proveedores, más del 60%, esperan disfrutar de servicios de mayor valor y un crecimiento empresarial sólido a través de la distribución de dos niveles en los próximos tres a cinco años.

## El mercado europeo está preparado para una aceleración en el negocio de distribución de tecnología, según tres informes recientes emitidos por el Global Technology Distribution Council

Por otra parte, de acuerdo con el informe 'Services Capabilities Transform IT Distribution in Europe', los mayoristas están alimentando el cambio en la forma en que se entregan e implementan los servicios de TI. Los mayoristas europeos entrevistados para el estudio confirman una utilización mucho mayor de los servicios por parte de fabricantes y proveedores de soluciones, pero ninguno maximiza el potencial de negocio de todos los servicios disponibles a través de los mayoristas. El informe incluye los resultados de la encuesta realizada a los principales mayoristas regionales y nacionales, que calificaron la generación de demanda, el desarrollo de soluciones y la formación y capacitación como las tres ofertas de servicios principales en la actualidad.

Finalmente, el estudio 'European Distribution Making the Difference' muestra una creciente confianza en los canales europeos, a medida que los proveedores aceptan más fácilmente

los acuerdos de distribución en la era digital. La localización y la especialización también están creando oportunidades para un nuevo crecimiento. Los distribuidores confirman un sólido primer semestre para la distribución de TI en Europa, a pesar de las continuas preocupaciones relacionadas con el Brexit y el impacto económico de las elecciones llevadas a cabo en algunos países. En general, las tendencias de distribución de TI apuntan a un sólido crecimiento en la región en 2017, incluso en las principales categorías de soluciones, que van desde la nube y la movilidad a la seguridad, la virtualización y la infraestructura hiperconvergente.

En el canal de distribución de Europa Occidental, el precio medio de los PC a principios del cuarto trimestre se situó en 590 euros, lo que representa una subida del 19% con respecto al mismo período del año pasado

## Los ingresos por ventas de PC continúan creciendo

Los principales mayoristas de Europa Occidental vieron cómo sus ingresos por ventas de PC seguían aumentando a principios del cuarto trimestre de 2017, después de un aumento significativo registrado en el tercer trimestre, según datos publicados por Context.

Concretamente, durante las primeras cuatro semanas del cuarto trimestre, los ingresos por ventas de PC registraron una subida anual del 6%, alcanzando los 938 millones de euros, tras el crecimiento del 9% producido en el tercer trimestre. El crecimiento continuo de los precios sigue estando impulsado por los aumentos en los precios medios de venta de los PC por parte de los distribuidores, que han aumentado lo suficiente como para compensar una disminución en los volúmenes de ventas.

En el canal de distribución de Europa Occidental, el precio medio de los PC a principios del cuarto trimestre se situó en 590 euros, lo que representa una subida del 19% con respecto al mismo período del año pasado. Este aumento comenzó hace aproximadamente un año es el resultado de los efectos de las fluctuaciones monetarias, la necesidad de los proveedores de compensar los crecientes costes de los componentes y un cambio en la demanda de productos hacia dispositivos de mayor valor, como PC de gaming y portátiles de alto rendimiento.

En lo que llevamos de año se ha notado una seria escasez de componentes, especialmente de memoria DRAM, que empeoró especialmente durante el tercer trimestre. Ello impulsó el alza en los precios de los componentes, que la mayoría de los fabricantes han repercutido en el precio de cara a los consumidores, en lugar de absorber el coste ellos mismos. Se espera que la escasez de DRAM continúe hasta 2018.



### Enlaces relacionados

- Global Technology Distribution Council
- The Distribution Landscape and Disruption
- Services Capabilities Transform IT Distribution in Europe
- European Distribution Making the Difference
- ¿Están tus empleados preparados para el puesto de trabajo digital en tienda?
- Índice de madurez digital de las empresas
- Estado de la digitalización de las empresas y administraciones públicas españolas

# V-Valley presenta sus 5 campañas de Valor

### SEGURIDAD S.O.S.

Sistemas Objetivo Securizados, adelántate a la GDPR

### COMUNÍCATE

Abre tus fronteras a un Mundo Global

### EL VALOR DEL CLOUD

Con los servicios Cloud rentabiliza de la forma más óptima todas las oportunidades

### CONÉCTATE

Estar conectado no es una opción, es una obligación

### BUILD IT

Construye tu futuro, adapta tu infraestructura a la transformación digital

**V-Valley**, la división de valor del **grupo Esprinet**, lanza al canal un plan de soluciones verticalizadas 360° para aquellos resellers que quieran introducirse en nuevos mercados y complementar su negocio tradicional en su evolución hacia la transformación digital.

V-Valley
the Value of esprinet

esprinet®

**V-Valley Iberian, S.L.U.** Campus 3·84 Nave 1 C/ Osca, 2,
Pol. Plaza 50197, Zaragoza, España
Telf. Barcelona +34 935 942 580 · Telf. Madrid +34 913 822 670
Telf. Zaragoza +34 976 971 119
**www.v-valley.com**

**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**

GDPR puede ser una oportunidad de crecimiento

# Los partners pueden jugar un papel crítico en la adaptación al GDPR

IDC estima que esta regulación representa una oportunidad de productos y servicios de seguridad de 3.500 millones de dólares para los partners y clientes que trabajan para cumplir con las reglas del GDPR. Los clientes están buscando ayuda de los socios para evaluar su preparación a la normativa.

Un estudio reciente muestra que el 75% por ciento de las empresas estadounidenses que consideran el GDPR como una prioridad han presupuestado 1 millón de dólares o más para cumplir la normativa, una cifra que en Europa oscila entre 100.000 euros y unos pocos millones. Vemos que la oportunidad para el canal está ahí, y muchos partners ya se han ido pre-

# Más de un tercio de las empresas no sabe si debe cumplir con GDPR

**WatchGuard Technologies ha publicado los resultados de un estudio global en el que se analiza el grado de conocimiento y comprensión que tienen las organizaciones sobre el próximo Reglamento General de Protección de Datos (GDPR) de la Unión Europea, así como su grado de preparación ante la inminente obligatoriedad de cumplir con él. Los resultados muestran una confusión generalizada sobre los criterios de cumplimiento de GDPR y una falta de preparación. Por ejemplo, un 37% de los encuestados simplemente no sabe si su organización necesita cumplir con GDPR, mientras que más de un cuarto (28%) cree que su empresa no necesita hacerlo en absoluto.**

De acuerdo con los criterios de GDPR, cualquier empresa que almacene o procese información personal sobre ciudadanos de la UE está obligada a su cumplimiento. De los encuestados que no creen que la ley se aplica a su organización, uno de cada siete (14%) recopila datos personales de ciudadanos de la UE, mientras que el 28% de los participantes que no estaban seguros sobre el cumplimiento de GDPR también recopila este tipo de información. Por lo tanto, según este documento, no sólo hay una falta general de concienciación sobre el nuevo reglamento GDPR, sino que los resultados de la investigación también ponen de relieve que las empresas están malinterpretando qué tipo de datos constituyen un mandato para el cumplimiento.

Por otro lado, y aunque muchas organizaciones han sido conscientes de GDPR durante algún tiempo, el informe asegura que sólo el 10% de los encuestados cree que su empresa está actualmente 100% lista para su entrada en vigor. En cuanto a la falta de claridad y comunicación en torno a GDPR, el 44% de los participantes declara que, en realidad, no saben lo cerca que está su organización del cumplimiento.

Asimismo, del 35% del total de los encuestado que informaron de que su organización necesita cumplir con GDPR, el 86% cree que actualmente cuenta con una sólida estrategia de cumplimiento en su empresa; con firewalls, VPN y soluciones de cifrado identificadas como las medidas de seguridad que con más probabilidad participen en estas estrategias. Sin embargo, el 51% de los entrevistados considera que su organización necesitará realizar cambios significativos en su infraestructura de TI para lograr cumplir el reglamento.

Finalmente, según este estudio, para aquellas empresas que aún no cumplan con el GDPR, los encuestados estiman que necesitarán una media de siete meses para completar los requerimientos. Para cerrar la brecha, casi la mitad (48%) de las organizaciones entrevistadas están, o podrían estar buscando ayuda para el cumplimiento en un tercero externo.

## *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.

# IDC estima una oportunidad de productos y servicios de seguridad de 3.500 millones de dólares para los partners y clientes que trabajan para cumplir con las reglas del GDPR

parando. De acuerdo con un post de Microsoft, los socios que se preparan para ayudar a los clientes en el cumplimiento del GDPR están reforzando sus servicios de cuatro aspectos clave: descubrir, administrar, proteger e informar.

En lo referido a descubrir, los socios deben identificar y hacer un inventario de cualquier dato personal que su organización o sus clientes hayan recopilado. Los partners pueden realizar evaluaciones de seguridad y riesgos, localizar datos personales relevantes y desarrollar un plan para lograr y mantener el cumplimiento.

A la hora de administrar, los partners pueden trabajar con sus clientes para desarrollar, implementar y administrar planes de cumplimiento, diseñando, configurando y monitorizando las políticas y controles apropiados para los datos y las aplicaciones de los clientes.

En el terreno de la protección, para prepararse para el cumplimiento, es importante establecer controles de seguridad para prevenir, detectar y responder a vulnerabilidades y brechas de datos. Los partners pueden ayudar a los clientes a monitorizar, analizar y actuar sobre la inteligencia de las amenazas y la información del comportamiento del usuario para abordar de manera efectiva las vulnerabilidades y las infracciones.

Por último, informar, porque los partners pueden ofrecer servicios gestionados para ayudar a los clientes a cumplir con sus requisitos de documentación y notificaciones, y responder de manera eficiente a las solicitudes de datos.

"Los partners pueden desempeñar un papel fundamental para ayudar a los clientes empresariales a adaptarse a la nueva regulación. Los clientes están buscando ayuda de los partners para evaluar su preparación al GDPR, lo que incluye evaluar sus entornos tecnológicos existentes. El valor de esa evaluación para el cliente es muy importante y puede generar ingresos añadidos a través de servicios gestionados, la

gestión de cambios, la reventa de tecnología y soporte, la capacitación del usuario final y los servicios de implementación", señalaba Diana Pallis, directora de marketing de partners de Office 365.

## GDPR como oportunidad de crecimiento

La cuenta atrás para la implementación del Reglamento General de Protección de Datos (GDPR) tiene a muchas empresas de TI cada vez más nerviosas. En la EMEA Member and Partner Conference de CompTIA, el fundador de Assure Data, Jim Sneddon, reveló cómo las empresas pueden transformar sus productos y procesos para lograr el cumplimiento, así como las posibles trampas y el camino hacia el cumplimiento, y quedó claro que aquellos que triunfen serán aquellos que vayan más allá del mero cumplimiento y usen el GDPR como una oportunidad de crecimiento empresarial.

Y SI NO CUMPLO CON GDPR, ¿QUÉ?


CLICAR PARA VER EL VÍDEO

> Aquellos que triunfen serán aquellos que vayan más allá del mero cumplimiento y usen el GDPR como una oportunidad de crecimiento empresarial

En virtud la normativa, una brecha de datos ya no se refiere solo a la pérdida de datos personales, sino que abarca cualquier acceso no autorizado, alteración o destrucción de esa información. Y cumplir con esto abarca a personas, procesos y procedimientos, así como a los productos.

Por ejemplo, la capacitación del personal debe transformarse para abarcar todo, desde la necesidad de que los departamentos de recursos humanos eliminen cualquier registro innecesario de ex empleados, hasta el nuevo imperativo de que los departamentos de marketing no compartan las bases de datos de contactos externamente sin consentimiento. Las empresas también necesitan averiguar si el personal está incumpliendo la regulación inadvertidamente al compartir información personal en la versión gratuita de aplicaciones como Evernote o Dropbox.

Los departamentos de marketing directo pueden incluso tener que obtener un consen-

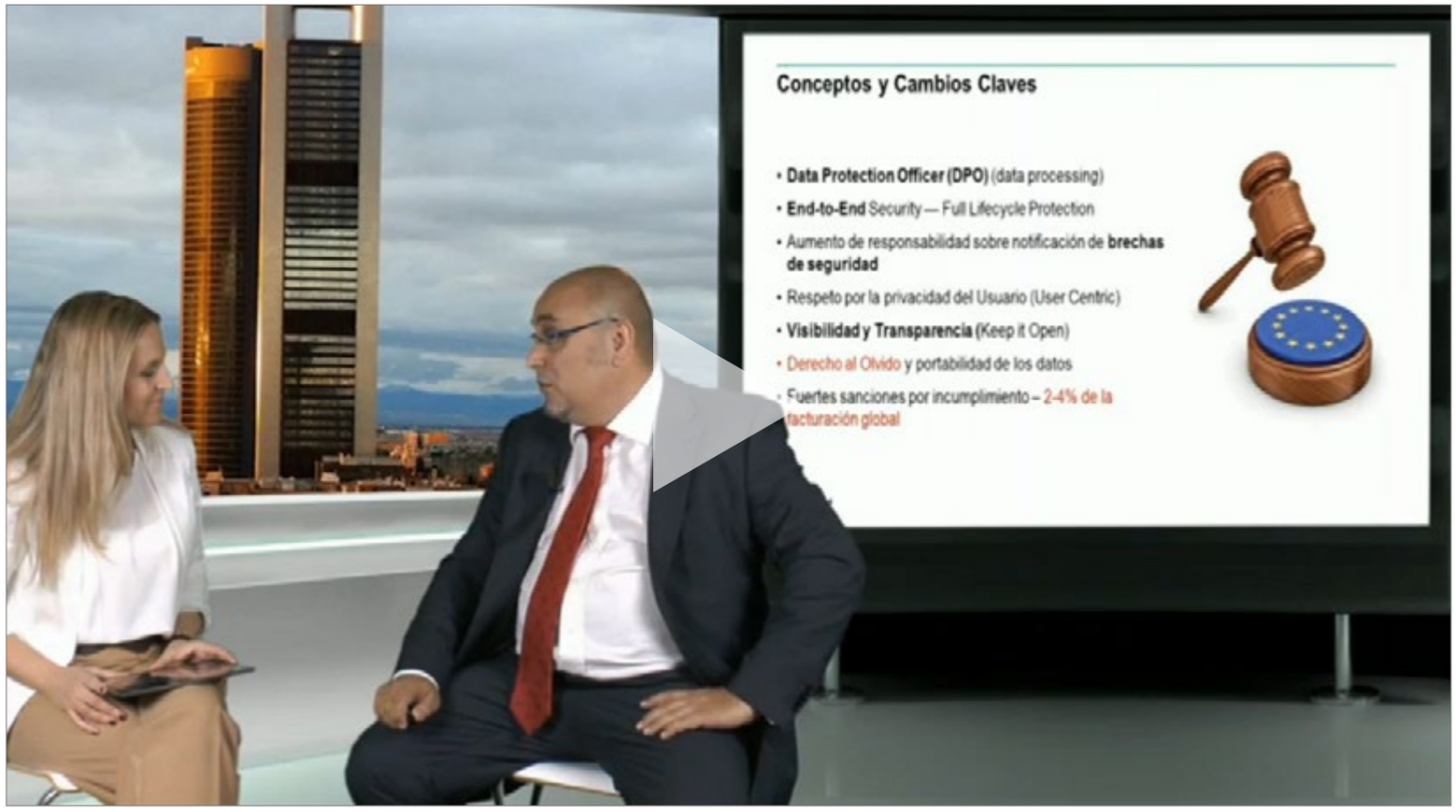
timiento explícito para la recolección y el uso de los contactos de correo electrónico para las comunicaciones B2C y B2B. Los contratos con terceros, como socios y proveedores, deben reescribirse para aclarar sus obligaciones de privacidad de datos y las empresas deben auditar regularmente a sus proveedores.

Todo esto también representa una gran oportunidad para aquellas empresas que lo hagan bien. Por ejemplo, las empresas que logren el cumplimiento pueden incluirlo en sus materiales de marketing y usarlo como una marca de garantía de calidad para atraer posibles socios y clientes.

Y el mismo proceso de aprender todos los consejos y herramientas para lograr el cumplimiento exitoso es una oportunidad para que las compañías de canal vendan esos consejos y herramientas a clientes y socios. Cada brecha en el cumplimiento de un cliente es una oportunidad para vender un nuevo módulo o producto. De esta forma, el "análisis de brechas" o el chequeo de salud de cada cliente es una herramienta potencial de ventas.



## GDPR: DÓNDE ESTÁN LOS DATOS A PROTEGER




CLICAR PARA VER EL VÍDEO

## Enlaces relacionados

- Y si no cumplo con GDPR, ¿qué?
- GDPR: cómo lograr una gestión adecuada de la información
- Más de un tercio de las empresas no sabe si debe cumplir con GDPR
- GDPR: dónde están los datos a proteger
- Los altos directivos europeos suspenden en implantación de GDPR
- Siete preguntas que los CIO deben responder para cumplir con GDPR

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

**Diversos estudios muestran las carencias del e-commerce y cómo podrían mejorar sus cifras**

# ¿Qué mejoras necesitan las tiendas on-line?

*La mitad de los españoles ya compran por Internet al menos una vez al mes, siendo el portátil el dispositivo más utilizado para ello. El domicilio sigue siendo el más habitual para recibir la compra, y Paypal la opción de pago preferida. El 20,5% de los eshoppers españoles reconocen haber comprado en webs fuera de nuestras fronteras. Pero el comercio electrónico representa solo el 11% del total de las compras en nuestro país. ¿Cómo podría mejorar este porcentaje?*

Pocos días antes del famoso Black Friday se presentaron los resultados de la segunda edición del eShopper Barometer, realizado por SEUR y DPDgroup, que revela que el comercio electrónico representa un 11% del total de las compras en nuestro país.

De acuerdo con el informe, la moda sigue siendo la categoría reina y representa el 48% de las compras, seguido por los productos de belleza y tecnología, con un 38% y un 36% del total de las compras online, respectivamente. Destaca la fuerte entrada de los productos frescos y bebidas, cuya compra online se sitúa en el 18%. Respecto a los dispositivos usados para hacer la compra, el ordenador portátil sigue liderando la lista en España, con un 60%, pero reduce la ventaja que tenía frente al smartphone, que ya es usado por el 48% de los compradores online españoles.

El informe índice especialmente en el grupo de los millennials, que es el responsable de subir la media de uso del portátil para comprar on-

## ¿Cómo ser el mejor en Internet?

Los consumidores digitales están motivando la mayor transformación de todos los sectores industriales. Comen, duermen y respiran con sus dispositivos móviles y esperan la misma experiencia de alta calidad si acceden a Internet desde sus equipos de sobremesa, en una tienda, o desde sus móviles. Conoce las mejores prácticas llevadas a cabo por los grandes referentes mundiales en sectores como la banca, distribución o medios de comunicación.


line, que llega a ser el 66%, acentuando más la diferencia con el resto de compradores. Llama la atención su confianza en las redes sociales, ya que el 42% reconoce que elige comprar en una tienda online basándose en las recomendaciones de estas plataformas, y la importancia que dan a que una web tenga su versión online bien adaptada, siendo un aspecto clave para el 55% de los millenials.

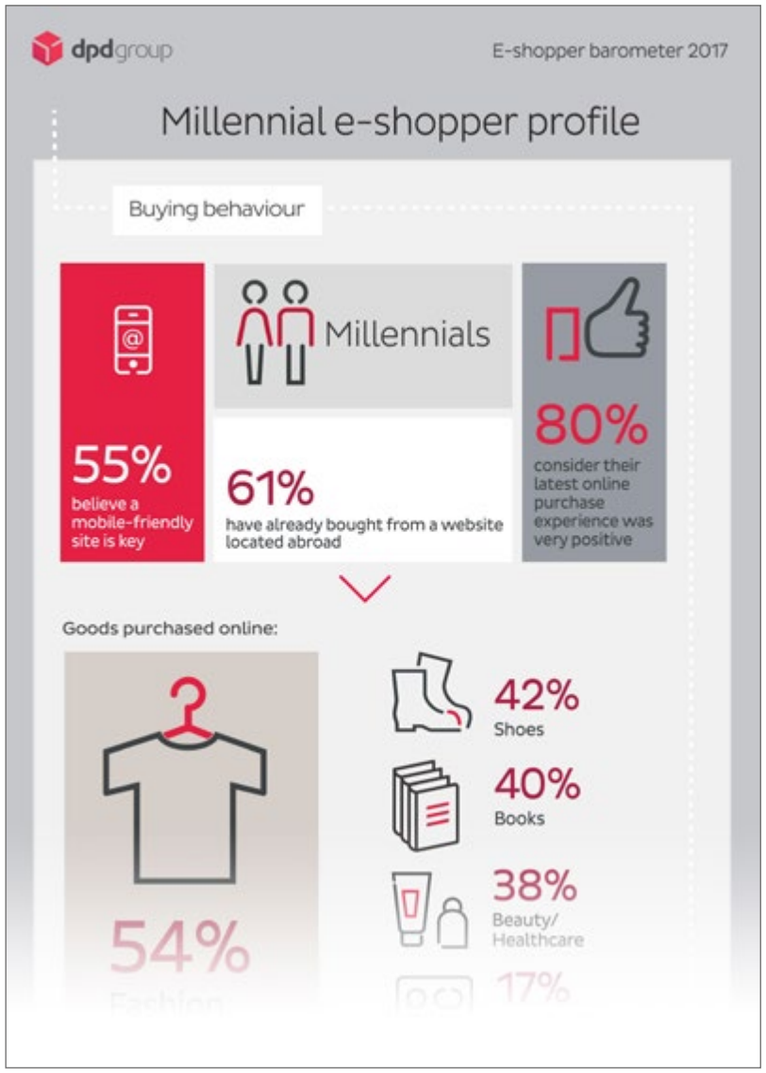
Respecto a la experiencia de compra online en España, ésta es cada vez mejor. Según el estudio, el 85% de los compradores online consideran que su última compra fue fácil y el 75% quedaron satisfechos con la experiencia. Sobre los principales motivos que impulsan la compra online, los procesos de entrega y devolución gratuitos se sitúan a la cabeza, con un 94% y un 93% de respuestas, respectivamente. La transparencia sobre el coste y las descripciones detalladas de los productos también son determinantes para el 91% y el 90% de los consumidores. En cuanto a las barreras para realizar compras online, los consumidores señalan los complicados procesos de devolución, los sitios web con problemas técnicos y la falta de artículos en stock.

Una vez realizada la compra, el 81% de los españoles prefiere recibir el pedido en su domicilio. Le siguen las tiendas físicas del vendedor y los puntos de conveniencia, una opción que cuenta con las mayores previsiones de crecimiento, concretamente, un 50% de los consumidores afirman que les gustaría usar estos


CLICAR PARA AMPLIAR

puntos para recoger sus pedidos. Además, el 65% de los compradores online suelen utilizar solo un lugar de entrega. Sobre el plazo de entrega, la entrega en el mismo día es la que tiene un mayor potencial de crecimiento: un 85% de los encuestados reconocen que la elegirían.

Sobre el lugar elegido para hacer las compras, el 20,5% de los eshoppers españoles reconocen haber acudido a webs fuera de nuestras fronteras, un porcentaje por encima de la media europea (19,2%). Entre los mercados extranjeros, China es el destino más elegido para




CLICAR PARA AMPLIAR

## El futuro de los retailers se encuentra en el Social Commerce

En España, el 81% de los internautas con edades comprendidas entre los 16 y los 55 años utilizan redes sociales, lo que equivale a 15 millones de usuarios. Así lo pone de manifiesto el Estudio Anual de Redes Sociales publicado por IAB Spain, que destaca que tan solo el 14% de los consumidores realizaron una compra a través de una red social durante el primer trimestre de 2016. Sin embargo, el 65% sí se vio influenciado en el proceso de compra.

A la vista de estos datos, desde Webloyalty señalan que, aunque no hayan logrado asentarse como principal canal de compra, las redes sociales pueden aportar un gran número de beneficios a los ecommerce. En primer lugar, permiten contar con un canal de comunicación bidireccional con clientes potenciales que ayuden a establecer con ellos relaciones y vínculos cercanos. Asimismo, herramientas como Facebook, Instagram o Twitter pueden servir de escaparate para los comercios que quieren dar a conocer sus productos, tanto a sus propios contactos como a terceros que puedan estar interesados. De esta forma, se aseguran el desarrollo de una amplia base de datos a través de la cual pueden impactar a miles de usuarios y posicionar su ecommerce. Según Eduardo Esparza, country manager de Webloyalty, "el uso de redes sociales por parte de las marcas sirve de apoyo a las actividades de compra-venta de productos online y offline gracias a la interacción con los usuarios".

El Social Commerce se considera así una nueva categoría de comercio electrónico. No obstante, las ventas obtenidas a través de estas plataformas sociales son residuales. Sin embargo, de acuerdo la investigación realizada por Sumo Heavy Industries, la única red social que ha conseguido asentar este modelo de negocio ha sido Pinterest, que sumó durante 2016 un total de 10.000 distribuidores a su plataforma, mientras que Twitter tuvo que cerrar su equipo de ecommerce.

este tipo de compras, seguido de Reino Unido y los Estados Unidos. Los principales motivos para comprar en el extranjero son contar con mejores ofertas y disponibilidad de productos específicos, mientras que las principales barreras son las tarifas adicionales y los procesos de entrega y devolución poco eficientes.

En cuanto a los métodos de pago, los monederos digitales como Paypal son la opción preferida de los compradores online españoles (un 57%), seguida de las tarjetas de débito/crédito (un 37%).

### Las tiendas online españolas precisan mejoras de usabilidad

De acuerdo con un estudio de Idealo, la totalidad de las tiendas presenta un carrito de compra satisfactorio en sus aspectos básicos, y

# Los millennials son los responsables de subir la media de uso del portátil para comprar on-line, que llega a ser el 66%, acentuando más la diferencia con el resto de compradores

muchas podrían mejorarlo añadiendo información extra como el tiempo de envío o los costes adicionales. En cuanto al proceso de registro, la mayoría de las tiendas sigue optando por su obligatoriedad.

Y es que la usabilidad es un aspecto fundamental en el ecommerce, pues influye en factores determinantes para la supervivencia de una tienda online, como la tasa de conversión. Para los posibles compradores, la usabilidad se ha de traducir en una mayor facilidad a la hora de navegar por una tienda online para poder realizar sus compras con la mayor efectividad posible. Pues bien, Idealo.es ha analizado las 50 tiendas online más importantes de su comparador teniendo en cuenta diversos factores a lo largo de todo el proceso de compra. Los resultados se dividen en cuatro fases: selección de producto, carrito de compra, registro y checkout.

El 28% de las tiendas analizadas envía directamente al usuario a la cesta de la compra tras elegir un producto, mientras que el 44% se decantan por la variante opuesta, permitiendo que el usuario permanezca en la página comprando sin interrupciones. Esta última opción ha ganado enteros entre las tiendas, el 86,4% de las cuales muestran algún tipo de animación visual que indica que se ha añadido un producto a la cesta de la compra. Otra posibilidad que se ha ido abriendo paso en España es la aparición de un pop-up dando al usuario la opción dirigirse directamente al carrito tras añadir un producto o seguir comprando, lo que supone una forma bastante inteligente de mantenerlo en el proceso de compra de forma activa. Un 28% de las tiendas deja al usuario elegir si quiere seguir comprando o ir directamente al carrito.

Las tiendas online aprueban con nota en los criterios básicos de usabilidad en el carrito, y una parte importante cumple criterios más avanzados. El 100% de las tiendas incluye en


CLICAR PARA AMPLIAR

# La recuperación de carritos abandonados dispararía los ingresos del Black Friday

Con la llegada del Black Friday y del Ciber Monday, y la posterior campaña de Navidad, se produce un claro incremento de la actividad en tiendas on-line. "Con tanta actividad competitiva, los minoristas y los fabricantes deben destacar en un ambiente muy abarrotado. Es vital que su actividad de promoción y precios sean juzgados a la perfección, ya que el Black Friday y el Ciber Monday son momentos críticos. Estas fechas son un período en el que los consumidores tienen sensación de urgencia, porque las ofertas tienen un plazo de validez muy corto y hay percepción de escasez de stock. Además, a través del gran número de impactos en comunicación, más usuarios son conscientes de las ofertas. Todos estos ingredientes, hacen que se multiplique exponencialmente el número de visitantes de los negocios online y, además, con


mayor predisposición a comprar", señala Lino Bort, director general de Blueknow.

Esta sensación de urgencia genera una compra online rápida que, en la mayoría de las ocasiones, se traduce en fallida a la hora del pago, lo que produce que el porcentaje de carritos abandonados llegue hasta el 80% frente al 70% habitual, según cifras del Instituto Baymard de Estados Unidos. En este sentido, para una empresa es más que importante plantear una estrategia de recuperación de cestas abandonadas en estas fechas.

Con la estrategia adecuada para recuperar carritos abandonados, en períodos como el Black Friday aumentarían los ingresos por encima del 10%.


el carrito una imagen de los productos seleccionados, su precio y el número de productos, y un 88% hace constar en el carrito los costes adicionales, como el coste de envío o el cargo por usar PayPal. Asimismo, el 66% incluye en el carrito de compra la posibilidad de introducir un código de descuento, el 46% muestra el tiempo de envío y el 44% las opciones de pago, unas informaciones pueden acabar de convencer a un comprador indeciso de no abandonar el carrito. Por último, el 24% de las tiendas opta por incluir dos botones para iniciar el checkout, uno encima y otro debajo de la lista de productos, lo que puede también incrementar el número de usuarios que continúa el proceso de compra.

Es cierto que existen compradores online que pueden echarse atrás en medio de una compra debido a un engorroso proceso de registro o porque no les apetece darse de alta. Conscientes de ello, el 34% de las tiendas dan la opción de comprar con una cuenta de invitado. Por otro lado, el 66% optan por el registro obligato-

> Según datos de Furgo, el 98% de los millennials reclama la compra rápida, y el 25% de los consumidores estaría dispuesto a pagar más por envíos inmediatos

**De acuerdo con un estudio de Idealo, la totalidad de las tiendas presenta un carrito de compra satisfactorio en sus aspectos básicos, y muchas podrían mejorarlo añadiendo información extra como el tiempo de envío o los costes adicionales**

rio, un 16% ofrecen un registro más cómodo a través del login en ciertas redes sociales. Sobre la cantidad de los datos, los usuarios ven excesiva la cantidad de datos que han de aportar a la hora de realizar una compra online. Las tiendas online en España han tomado nota en este sentido, y el 100% ofrece la opción de copiar la dirección ya introducida para el envío como dirección de facturación o viceversa, mientras que el 38% obliga a los usuarios a introducir su DNI al comprar online. Por otra parte, el 64% de las tiendas online analizadas incluye la casilla de aceptación de comunicaciones comerciales en algún punto del proceso de registro.

La tendencia a simplificar los pasos que se dan en el checkout es notable. Así, el número de pasos en el checkout ha bajado de 4,7 pasos de media en 2015 a solo 2,7 pasos en 2017. El 40% de las tiendas muestran todo el proceso en una sola página, una opción que no es siempre la más óptima, especialmente al hablar de dispositivos móviles en los que el usuario puede fácilmente perderse en una página demasiado "larga". El 96,7% de las tiendas que ofrece un checkout en varios pasos muestra en todo momento la lista de pasos y el paso en qué se encuentra el usuario.

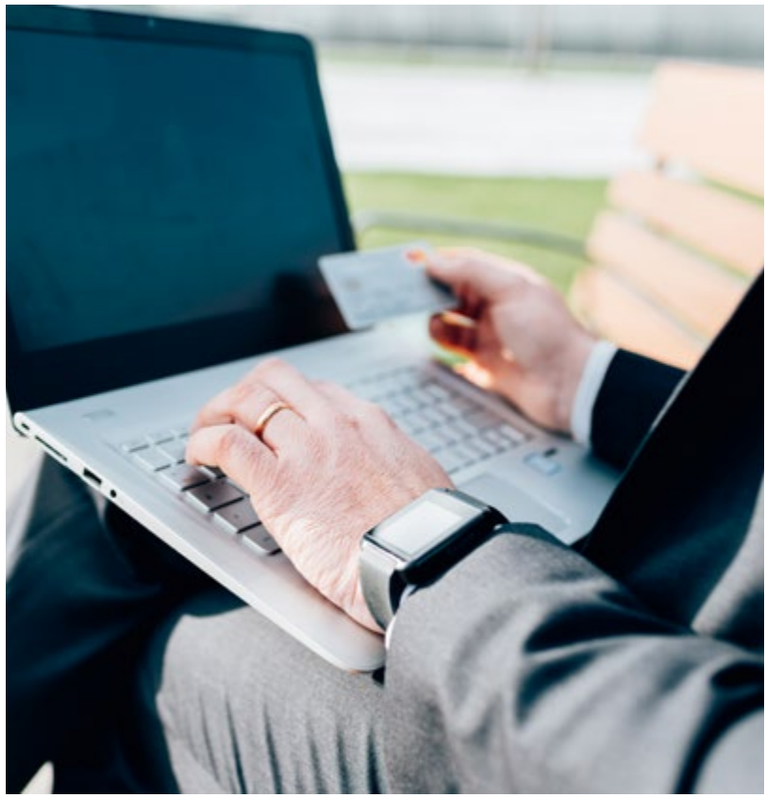
## Los envíos inmediatos son la clave para adaptarse al consumidor

Según datos de Furgo, el 98% de los millennials reclama la compra rápida, y el 25% de los consumidores estaría dispuesto a pagar más por envíos inmediatos. España es el quinto país en el ranking de consumo de e-commerce en Europa, con una tasa de crecimiento superior al 10% anual, pero con baja eficiencia logística

## *¿Están tus empleados preparados para el puesto de trabajo digital en tienda?*


En un futuro cercano, las tiendas van a desempeñar un rol muy diferente al actual, ya que los profesionales del sector esperan el desarrollo de nuevos formatos de los establecimientos comerciales. Como resultado, aquellos que quieran seguir siendo relevantes deberán adaptarse y desarrollar las capacidades y soluciones tecnológicas que se requieren en el nuevo puesto de trabajo digital en tienda. A pesar de ello, muchos profesionales del sector parecen estar quedándose atrás a la hora de adaptar sus equipos de trabajo a esta próxima era de cambios, tal como demuestra una gran parte de los participantes en este estudio de Avanade, al indicar que en los próximos años estiman difícil implementar cambios en las actividades de sus establecimientos.

Las empresas de comercio electrónico han transformado los procesos de compra, las formas de pago, pero también las entregas, que se adaptan a las necesidades del cliente ofreciendo mayores beneficios y comodidades, lo que a su vez les permite incrementar sus ventas. El marketplace de transportes Furgo ha re-



cogido datos que indican cómo los consumidores creen que deberían ser las entregas de sus pedidos online, de los que se desprende que los envíos inmediatos son la clave para adaptarse al consumidor, que compra el producto en función del tiempo de entrega que ofrece el e-commerce. Así, el 98% de los millennials reclama la compra rápida, mientras el 25% de los consumidores estaría dispuesto a pagar más por envíos inmediatos. Como consecuencia de ello, en países como Estados Unidos el 52% de los retailers que operan en el mercado ya ofrecen entregas 'same-day', es decir, en el mismo día de la compra.

Más allá de incrementar el volumen de ventas y diferenciarse de la competencia, es necesario implementar los envíos exprés para poder alcanzar una mayor fidelización de clientes, menor abandono de carritos, simplificación de procesos y menos reclamaciones. Esto representa una gran dificultad para España, que es el quinto país en el ranking de consumo de e-commerce en Europa, con una tasa de crecimiento del sector superior al 10% anual, pero con una baja eficiencia logística.

La mayor demanda de productos que requieren entregas inmediatas está en el sector tecnológico y de moda, pero esta demanda se está trasladando a los envíos de productos con grandes volúmenes. Como señalan desde Furgo, hasta ahora las compras de muebles y electrodomésticos no suponían una compra por impulso, sino que respondían a una necesidad y a una de decisión estudiada y meditada, por lo que podía no ser necesario un transporte rápido. Pero ahora, los consumidores hacen presión para conseguir estos envíos inmediatos igualando las condiciones de envío de otros productos, presión que se ve incentivada con el éxito de plataformas de segunda mano y ofertas de corta temporalidad.

¿TE HA GUSTADO ESTE REPORTAJE?

***Compártelo en tus redes sociales***

## Enlaces relacionados

- US Social Commerce 2017: Influencing and Driving Sales
- eShopper Barometer
- ¿Qué compran los europeos a través del e-commerce?
- Perfil comprador on-line del millennial europeo
- Perfil de los compradores on-line europeos
- La verdad sobre el ecosistema de IoT
- La reinvención digital: una oportunidad para 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!!!

# DaaS: un negocio disruptivo para el canal de PC corporativos

El dispositivo como servicio (DaaS) se ha convertido en un tema candente de la industria, con el potencial de revolucionar el mercado de PC profesionales. Para las empresas, DaaS les permite aumentar o reducir las implementaciones de dispositivos a medida que cambian las necesidades de sus empleados, pudiendo renovar sus dispositivos más rápidamente, actualizarse a nuevas tecnologías más fácilmente y, sin la responsabilidad de administrar y mantener los dispositivos, todo ello bajo un modelo OpEx. Las grandes firmas de TI, como Dell y Microsoft han abrazado la tendencia, al igual que los grandes mayoristas, como Ingram Micro. Con todos ellos hemos hablado sobre el potencial de este mercado.

En los últimos años, las ventas de PC han disminuido trimestre a trimestre, y en 2016, por primera vez desde 2007, el volumen de ventas cayó por debajo de los 65 millones de unidades. Para este año, Gartner predice que las ventas de PC en todo el mundo descenderán un 3%, que, si bien es la tasa de disminución más lenta de los últimos años, aliviada por la renovación de PC con Windows 10, indica que la demanda sigue sin recuperarse, ni siquiera en el entorno empresarial.

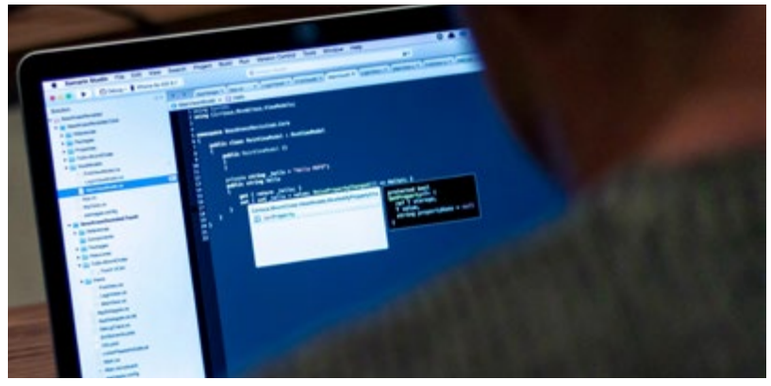
El mercado de PC profesionales lleva años enfrentándose la extensión de los ciclos de vida, a medida que las empresas retrasan la actualización de PC para centrarse en iniciativas más críticas, productos con mejores retornos y proyectos más amigables con la economía. Para frenar esta tendencia, y en consonancia con la tendencia 'as-a-Service', están empezando a proliferar en el mercado las ofertas de PCaaS o DaaS, que vienen a reducir las barreras financieras de las actualizaciones de PC y brindan la flexibilidad y escalabilidad que las adquisiciones tradicionales de PC no ofrecen.

"El mercado de PC para empresas, mientras lucha por mantenerse, podría beneficiarse de una fuerza disruptiva", afirma Linn Huang, director de investigación de Dispositivos y Pantallas de IDC. "A medida que los principales OEM se vuelven cada vez más enfocados en la empresa, esperamos que DaaS reciba cada vez más atención".

## Atractivo para las empresas

La idea de DaaS es relativamente nueva, pero las empresas son receptivas a la idea de comprar PC como servicio. En este sentido, una encuesta de IDC realizada a principios de este año descubrió que, aproximadamente una cuarta parte de los encuestados ya estaba buscando activamente estos servicios, y casi el 20% de los encuestados dijo que tenía planes de hacerlo en los próximos 12 meses.

Preguntadas sobre los motivos para adoptar DaaS, las empresas afirmaron que este modelo les permite escalar o reducir las implementaciones de dispositivos a medida que cambian las necesidades de sus empleados. El uso del modelo DaaS también significa que las organizaciones pueden renovar los dispositivos más rápidamente, actualizarse a nuevas tecnologías más fácilmente y, sin la responsabilidad de administrar y mantener los dispositivos.



Efectivamente, uno de los principales beneficios de DaaS es la capacidad de desplegar solo los dispositivos que se necesitan. Para Tom Mainelli, vicepresidente del grupo de Dispositivos de IDC, "la capacidad de implementar solo activos según sea necesario, en función de la carga de trabajo, es un gran logro. Esto significa que una empresa tiene la capacidad de flexibilizarse y agregar dispositivos a medida que crezca su fuerza de trabajo. Más importante aún, sin embargo, es la capacidad de flexión hacia abajo". Tradicionalmente, cuando las compañías compraban ordenadores y luego reducían personal debido a cambios estacionales o despidos, el resultado era una abundancia de equipos innecesarios. "En un modelo DaaS, el proveedor recupera esos dispositivos, y puede volver a implementarlos en otro cliente", añade Mainelli.

Por otra parte, al cambiar las compras de dispositivos de un gasto de capital (CapEx) a un

"Todas las figuras del canal deberán incluir en su catálogo en un futuro esta modalidad de venta"

Miquel Santamarta, sales director B2B de Ingram Micro


gasto operativo (OpEx), las empresas obtienen una mayor estabilidad y visibilidad en sus costes de TI. "En lugar de tratar de pronosticar la necesidad de futuras actualizaciones de hardware, esas actualizaciones están integradas en el plan de servicio", apunta Mainelli. Esto resulta especialmente importante para las pequeñas empresas, que no deben gastar el valioso tiempo, dinero y recursos de los directores de TI en el manejo cotidiano de PC, tablets y otros dispositivos.

Si bien el paso de ser propietario del dispositivo a pagar por usarlo, al principio crea algunas incertidumbres, el camino está abierto, y cada día más hay una buena acogida para este tipo de servicios, donde los clientes entienden el valor añadido que no se traduce sólo en el PC, ya que a esto se le añade toda una capa de servicios, como la personalización, la instalación y el soporte, que dan mucho más valor a la oferta. Si el proveedor de servicios hace bien su trabajo, se trata de una situación en la que todos salen ganando, con márgenes más atractivos para el fabricante y el distribuidor, y una experiencia simple y única para el cliente.

En cuanto al tipo de clientes que se muestran más interesados, existe un interés genérico en todos los segmentos, tanto en entornos pyme como en grandes multinacionales, aunque, como señala Miquel Santamarta, sales director B2B de Ingram Micro, "seguramente, la pequeña y mediana empresa es la que más provecho puede sacar de este modelo. Las razones son varias: capacidad de endeudamiento contenida, acceso a la última tecnología, ventajas fiscales, fácil acceso a recursos técnicos y de consultoría de que seguramente no disponen o que pueden utilizar para otros objetivos más rentables, renovación del parque instalado con el mínimo impacto".

## Los fabricantes soportan el modelo

Vemos que los beneficios son muchas, y cada vez más empresas de tecnología ven DaaS como una propuesta atractiva. Es el caso de Microsoft, que en julio del pasado año presentó un programa DaaS llamado "Surface as a Service", por el que las compañías podrán alquilar dispositivos Surface junto a suscripciones a Office 365 y Windows 10. Bajo el programa, los distribuidores autorizados pueden

## Del SaaS al DaaS

**Para aquellos partners que ofrecen software como servicio (SaaS), debería ser una opción natural añadir el hardware a la ecuación, un hardware que se actualiza y renueva sin necesidad de costes iniciales o costes de transición. Así lo cree David Prats, de Dell EMC, que se muestra convencido de que "a una fuerza comercial familiarizada con el concepto 'as-a-service' debería resultarle más fácil vender DaaS".**

Del mismo modo, un cliente que ya emplea el modelo as-a-service en su día a día está más abierto a utilizar DaaS. "Hacer entender el valor de este modelo a clientes que están acostumbrados a utilizar otros servicios de pago por uso es relativamente fácil", comenta Miquel Santamarta, de Ingram Micro.

María del Carmen Lamolda, de Microsoft, va más allá, afirmando que "el lanzamiento de una oferta de dispositivo + SaaS es la evolución natural del mercado. Cada vez más los clientes demandan esta solución conjunta, y Microsoft, junto a su ecosistema de partners y soluciones propias, es capaz de cubrir esta demanda creciente en el mercado. Es imposible separar el dispositivo de la suite ofimática y viceversa, por lo que Microsoft ha sabido conjugar a la perfección ambos entornos y fusionarlos en un espacio de soluciones globales para el mundo empresarial".

ofrecer esos dispositivos a través de una oferta de servicio gestionado a todos los revendedores y clientes de Microsoft, junto con servicios cloud gestionados, Office 365, Windows 10 y software independiente relevante.

"Surface como Servicio fue una propuesta que lanzó Microsoft en el evento de partners del pasado año en Toronto y durante este año se han desarrollado propuestas con distintos resellers, tanto con la suite de Office 365 y EMS como con soluciones propias de ISV que se han ofrecido en un modelo de renting tecnológico", afirma María del Carmen Lamolda, responsable de Canal de dispositivos Surface de Microsoft Ibérica.

Sobre la respuesta del mercado, Lamolda, señala que "la acogida ha sido positiva en el mercado español, donde podemos encontrarnos con soluciones de firma biométrica que unido a la potencia y funcionalidades del dispositivo ha supuesto una oferta rompedora, como ejemplo en el sector bancario y seguros". Lamolda añade que "también se ha visto una clara evolución y un creciente interés en el entorno de la pyme, donde la oferta de Surface con Office 365 se ha percibido como una solución completa para una mejora en la productividad y movilidad".

"Es una oportunidad muy interesante para partners con vocación de vender microinformática"

David Prats, responsable comercial DFS Iberia de Dell EMC

Otro de los fabricantes que se ha volcado con este mercado es Dell EMC, que el pasado mes de mayo presentó PC as a Service (PCaaS), una oferta que combina hardware, software, servicios del ciclo de vida y financiación en una solución que lo abarca todo, bajo un precio único y predecible por puesto de trabajo por mes a través de Dell Financial Services.

"La acogida del mercado español está siendo esperanzadora, como no podía ser de otra manera. Tengamos en cuenta los diferentes procesos de transformación que vienen sucediendo dentro del sector tecnológico, en donde, como no podía ser de otra manera también le llega

LOS TRES GRANDES BENEFICIOS DE PCAAS O DAAS


CLICAR PARA VER EL VÍDEO

el turno al PC. No debemos olvidar que el PC sigue siendo el activo principal dentro del entorno de trabajo, un entorno que se ha vuelto más complejo y exigente, toda vez que atiende diferentes tipos de usuarios con diferentes necesidades para cada caso", explica David Prats, responsable comercial DFS Iberia de Dell EMC, para quien "tener la capacidad de poder ofrecer a nuestros clientes un coste fijo por mes por usuario, donde cubramos sus necesidades, indudablemente añade valor para los clientes en este proceso de transformación".

"El lanzamiento de una oferta de dispositivo + SaaS es la evolución natural del mercado"

María del Carmen Lamolda, responsable de Canal de dispositivos Surface de Microsoft Ibérica

## Oportunidades para los partners

Aunque tímidamente, el canal TI ha empezado a sumarse al modelo DaaS, y cada vez hay más sensibilidad y conocimiento de vender y distribuir soluciones. "La respuesta es buena y estamos convencidos que en los próximos meses notaremos un gran crecimiento en estos tipos de iniciativas", comenta Miquel Santamarta, de Ingram Micro, que augura que "todas las figuras del canal deberán incluir en su catálogo en un futuro esta modalidad de venta".

Las oportunidades que presenta DaaS para los partners son muchas: fidelización del cliente mediante el control de sus activos tecnológicos, venta de servicios y consecuente incremento del margen, garantías de nuevas ventas a la finalización del contrato. "Afortunadamente capturar estas oportunidades es muy sencillo, ya que hacer entender el valor de este modelo a clientes que están acostumbrados a utilizar otros servicios de pago por uso es relativamente fácil", puntualiza Santamarta.

Son muchas las tipologías de partner que pueden hacer su entrada en el mercado, aunque David Prats, de Dell EMC, opina que "es una oportunidad muy interesante para partners con

## *PC como servicio, la forma inteligente de provisionar TI*

Los PC son elementos críticos d ela infraestructura de hardware. Sin embargo, como los administradores de TI tienen que centrarse en otras tareas como la movilidad, la transformación digital o la seguridad, la actualización de los PC se ha convertido en una prioridad secundaria.

Este informe de IDC explica qué es un PC como servicio y qué ventajas aporta a las organizaciones este modelo.

vocación de vender microinformática, combinado con prestación de servicios alrededor del hardware, servicios que ayuden a sus clientes finales a modernizar el parque existente y automatizar procesos ligados a la implementación, mantenimiento y seguridad del parque, todo ello con costes previsibles en el tiempo". "Para nuestros partners –prosigue Prats – la oportunidad tiene varias capas. Primero, la capilaridad que nuestros partners nos aportan a la hora de llevar el mensaje al mercado en todos los segmentos. Segundo, la combinación de servicios prestados por nuestros partners combinados con servicios 'in-house' de Dell, todo ello integrado en una cuota al mes por equipo, servicios incluidos".

Por otra parte, en el caso de Microsoft, los ISV también pueden participar. Según María del Carmen Lamolda, "los partners ISV tienen una gran oportunidad para potenciar la venta de sus soluciones, que, unidas a un dispositivo como Surface Pro o Surface Laptop, les posibilita la entrada en clientes que tienen en mente un reemplazo de dispositivos a corto y medio plazo dando una solución completa al cliente. Cualquier partner que esté interesado en posicionar su solución junto con nuestro dispositivo tendrá nuestro apoyo para ayudarle en el lanzamiento de la oferta conjunta".

En lo que todos coinciden es que el mercado y las ofertas seguirán creciendo, tanto en cuanto se sigan incrementando las ofertas de los partners, que seguirán contribuyendo a tener un ecosistema de soluciones cada vez más diverso.



## Enlaces relacionados

- Cómo puede tu empresa beneficiarse del PCaaS
- El PC de sobremesa sigue siendo el dispositivo principal de los empleados
- Dell Technologies ofrece modelos de consumo flexibles del PC al centro de datos
- El programa Surface as a Service de Microsoft cala en el canal
- Microsoft anuncia innovaciones tecnológicas e inversiones de canal
- HP Inc. simplifica la gestión del ciclo de vida de los PC con el programa DaaS
- Lenovo lanza una oferta de PC como servicio para empresas
- Cómo debe ser el centro de datos de nueva generación
- La empresa digital
- El impacto de la automatización en las operaciones de IT
- El reto de la Cultural Digital
- Innovación a nivel global

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

# MCR entrega sus Premios 2017

**El mayorista volvió a congregar al canal de distribución en una gala que cumplía 10 años**

# MCR entrega sus Premios 2017

*El pasado 30 de noviembre, MCR volvió a celebrar una nueva edición de sus Premios MCR. Este año, además, fue muy especial ya que cumplían diez años. El canal de distribución TI acudió a una cita que ya se ha convertido en todo un referente en el sector. En total se otorgaron 20 premios en una gala que contó con el patrocinio de Samsung, Sandisk y Western Digital, que quisieron mostrar su apoyo al canal.*


El pasado 30 de noviembre la sala Opium de Madrid acogió la gala de entrega de los Premios MCR 2017, todo un referente en el sector y más teniendo en cuenta que este año se celebró la décima edición.

MCR CELEBRA EL DÉCIMO ANIVERSARIO DE SUS PREMIOS


CLICAR PARA VER EL VÍDEO

## Cumplir 10 años es una muestra de que los Premios MCR ya están consolidados

Desde su creación, el objetivo de estos premios ha sido reconocer aquellas marcas que han gozado de una mayor aceptación y que más han contribuido al crecimiento del negocio. “Año a año hemos consolidado los premios”, destaca Pedro Quiroga, CEO de MCR. Tras 10 años “continuamos con la misma ilusión a la hora de convocar y celebrar este evento”.

MCR volvió a congregar a más de 400 personas en Madrid. “Conseguir la afluencia de gente que tenemos año tras año nos parece un gran éxito”, afirma Pedro Quiroga. Ésta es “una fiesta de la tecnología en la que distinguimos a los mejores proyectos y a las empresas más representativas para el canal”.

### Unos premios consolidados

El hecho de cumplir 10 años es una muestra de que los Premios MCR ya están consolidados. “Esta gala es un evento ya muy esperado por el canal y por los fabricantes, y no queremos defraudarles cuando se cumple su X aniversario”, explica Quiroga. “Así que hemos organizado un evento que ha servido para desconectar de la rutina laboral, pero que es un punto de encuentro entre todos los que formamos este sector”.

### 20 galardones

En la gala de los Premios MCR 2017 se otorgaron veinte galardones, para otras tantas ca-

tegorías. “La mayoría de las categorías no han cambiado”, asegura Pedro Quiroga, “pero sí es verdad que hay un área cada vez más protagonista, como es el gaming”. La edición de los premios de este año ha contado con hasta 5 categorías exclusivas dedicadas a este mercado, incluyendo Mejor Periférico, Mejor Portátil y Mejor Monitor, entre otros.

A la hora de entregar los Premios se valora, sobre todo, “la calidad”. En este sentido, y tal y como explica Pedro Quiroga, “los fabricantes suelen presentar a concurso sus gamas más altas y los productos más innovadores y de más prestigio”. No obstante, “en algunas ocasiones, los distribuidores, que son los que votan, premian que sean productos de mucho éxito”.

## Valoración de 2017 y previsión para 2018

Durante la gala de los Premios MCR 2017, Pedro Quiroga aprovechó para hacer un repaso de 2017 recordando que el año anterior “la inestabilidad política, al no tener Gobierno, afectó a los resultados globales del año”.

En cambio, en 2017 “se ha producido una consolidación del negocio. Los crecimientos están siendo interesantes y las cifras que están dando las consultoras como Context cifran la subida del mercado mayorista alrededor de un 6% o un 7%, con lo que está siendo un buen año para la red de venta indirecta”

Si de lo que hablamos es de los resultados de MCR, “estamos un poco por encima de las

## Listado de premiados

- Mejor periférico gaming: Razer Teclado Ornata Chroma
- Mejor dispositivo de juego: Thrustmaster Volante T-GT PS4/PC
- Mejor monitor de gaming: Asus ROG Swift PG348Q
- Mejor portátil de gaming: MSI GE63VR 7RE Raider
- Mejor chasis gaming: Corsair Crystal 570X
- Mejor tarjeta gráfica: Gigabyte GV-N1060WF20C
- Mejor placa base: Asus PRIME B250M-A
- Mejor disco duro externo: WD My Cloud Home DUO
- Mejor memoria PC: Kingston HyperX Fury Black 8GB
- Mejor memoria flash: Sandisk Ultra microSDXC 400 GB
- Mejor SSD interno: Samsung 960 EVO NVMe M.2 500 GB
- Mejor SSD externo: WD My Passport SSD 1TB
- Mejor proyector: BenQ MX528
- Mejor PC sobremesa: Acer Aspire U27 (AIO)
- Mejor monitor de consumo: LG 38UC99-W Curvo
- Mejor portátil: Acer Swift 3
- Mejor dispositivo de sonido: Creative Altavoces Sound Blaster X Katana
- Mejor dispositivo para el hogar: Gigaset Teléfono SL450
- Mejor empresa de innovación tecnológica: Intel
- Mejor solución empresarial: Samsung

El objetivo de estos premios es reconocer aquellas marcas que han gozado de una mayor aceptación y que más han contribuido al crecimiento del negocio

# Tres marcas quisieron participar en esta fiesta en calidad de patrocinadores oficiales: Samsung, Sandisk y WD, fieles al mayorista

cifras de Context", con lo que "estamos muy satisfechos de cómo va a acabar 2017".

De cara a 2018, el objetivo que se ha marcado MCR es "continuar creciendo", destaca Pedro Quiroga. "Año a año seguimos mejorando, seguimos creciendo como mayorista, seguimos introduciendo nuevos productos y seguimos apostando por la tecnología".

Con esta filosofía, "somos optimistas e intentaremos lograr los objetivos de crecimiento".

No obstante, Pedro Quiroga cree que el año que viene "el sector crecerá, pero no tanto como ha crecido en 2017 para el canal mayorista".

LOS FABRICANTES MUESTRAN SU APOYO A LOS PREMIOS MCR 2017


CLICAR PARA VER EL VÍDEO

## La opinión de los patrocinadores

Los Premios MCR 2017 contaron con tres patrocinadores: Western Digital y Sandisk (este último está integrado dentro de WD) y Samsung. Con este patrocinio, las tres marcas volvieron a mostrar su apoyo al canal de distribución en general, y a MCR en particular.

En palabras de Juan Sanz, director para el Sur de Europa de Western Digital, estar en la gala de entrega de los Premios MCR es "un orgullo". En este sentido, Sanz aprovechó para reiterar el compromiso de su compañía por la red de venta indirecta a la que definió de un "canal muy importante" para Western Digital.

"Los partner nos han apoyado a la hora de conseguir una serie de retos muy importantes

Juan Sanz, además, explicó que su compañía tiene “muchas oportunidades de negocio” y “muchos retos”. En la gala de los Premios MCR 2017, “un referente para el sector”, Western Digital “tiene la oportunidad de relacionarse con el canal de otra manera. Marca el inicio del trabajo” de cara al año que viene.



## En la gala de los Premios MCR 2017 se otorgaron veinte galardones

en este 2017”, asegura Juan Sanz, quien aprovechó la ocasión para reiterar su apuesta por el canal de cara al año que viene. “Queremos seguir creciendo de la mano de nuestro canal, para consolidar nuestra posición como líderes en el área de almacenamiento”.

Eugenio Jiménez, director del área de almacenamiento de Samsung España, también mostró su apoyo a la gala organizada por MCR. “Para una empresa como Samsung en general, y para la unidad de almacenamiento en particular, es un honor participar en los Premios”.

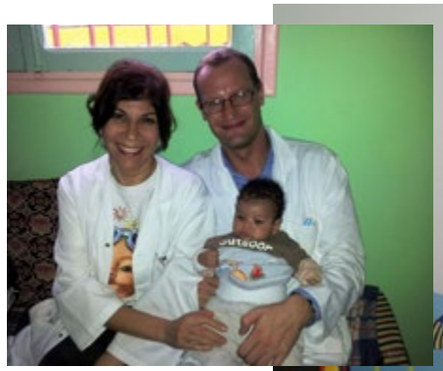
Jiménez destaca que el evento es “la culminación de un año de éxitos, sobre todo en la parte de SSD, y también de un gran crecimiento en la parte de tarjetas”.

Samsung “está encantado de trabajar con un partner como MCR y también con el gran canal de distribución al que atienden”, finaliza Eugenio Jiménez.

**Enlaces relacionados**

- Información sobre MCR
- Listado de nominados a los Premios MCR 2017

# Voluntariado, un paso en la realización personal ayudando a los demás



*Define la Real Academia Española de la Lengua el voluntariado, en su tercera acepción, porque las dos primeras tienen connotaciones militares, como conjunto de personas que se ofrecen voluntarias para realizar algo. Esto es cierto, pero todos sabemos que el voluntariado es algo más, y de ello nos habla Samira Brigüech, presidenta de la Fundación Adelias, en estas páginas.*

Está demostrado que las personas que realizan actividades de voluntariado son más felices y tienen una menor tendencia a la depresión. Las personas que donan tiempo a causas sociales tienen una mejor condición física y mental y muestran una conducta social más extravertida. Las personas que muestran un compromiso a largo plazo en las labores de voluntariado viven con menos estrés. Esto lo demostraron dos psicólogos de la universidad de Constanza allá por el año 2000.

Las psicólogas solicitaron a 105 trabajadores en activo que anotaran, durante dos semanas, las actividades que llevaban a cabo en su tiempo libre, entre ellas, trabajos voluntarios. También preguntaron a los participantes cuán recuperados se sentían al finalizar el día y observaron su comportamiento laboral en la jornada siguiente.

Probaron, que las personas que después del trabajo llevaban a cabo alguna actividad de voluntariado podían desconectar mejor de la rutina laboral. Este efecto recuperador también influía de manera positiva al día siguiente: discutían menos sobre problemas, prestaban más atención a sus compañeros de trabajo y les escuchaban más.

La fundación Adelias provee de un voluntariado flexible pensado especialmente para ejecutivos o directivos de empresa que disponen de poco tiempo.

Este sistema de voluntariado puede desarrollarse tanto en Marruecos como en España.

En España contamos con un plan de voluntariado enfocado al ámbito educativo y el de salud.

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

# Está demostrado que las personas que realizan actividades de voluntariado son más felices y tienen una menor tendencia a la depresión

¿TE HA GUSTADO ESTE REPORTAJE?

***Compártelo en tus redes sociales***

Trabajamos con niños enfermos que vienen a nuestro país para recibir tratamiento médico gratuito que no pueden recibir en sus países, por los altos costes hospitalarios y quirúrgicos, o por la complejidad de sus enfermedades. Los voluntarios donan tiempo durante la semana o en fin de semana para disfrutar de un tiempo con estos niños en los que, básicamente, se trata de hacerles felices durante unas horas. Jugando, leyendo, viendo una película, saliendo a tomar un refresco o, sencillamente, enseñándoles español.

También contamos con un programa de refuerzo educativo pensando para niños españoles, con baja renta familiar, para ayudarles a superar sus problemas de aprendizaje. Esta actividad se desarrolla en los hogares de los niños en función del tiempo que desea donar cada voluntario. Se trataba en las áreas en las que los

voluntarios tienen más conocimiento o talento: matemáticas, informática, física, manualidades, música, geografía...

Este programa también incluye la donación de equipos informáticos o dispositivos móviles, como tablets, para fomentar el aprendizaje.

En el apartado de voluntariado internacional, este programa se basa en donar una semana en nuestro orfanato, para trabajar con niños en espera de adopción. Esta labor consiste sencillamente en ser “padres” provisionales durante la semana de voluntariado, haciendo las tareas habituales de cualquier padre. Igualmente, en nuestra unidad de pediatría, se realizan trabajos con recién nacidos que necesitan una atención personalizada. No es necesario tener experiencia ni haber tenido la experiencia de la maternidad/paternidad. Las labores de cuidado a los bebés son explicadas por el personal del hospital y son aprendidos durante el primer día de voluntariado.

La experiencia vivida por los más de 400 voluntarios que han donado su tiempo a la Fundación Adelias, nos demuestra que estas acciones nos hacen sentir útiles a la sociedad y nos engrandecen como personas.

La ciudad de Nador, a 12 kilometros de Melilla, acoge tanto el orfanato como el hospital y la Fundación facilita la comunicación de los voluntarios internacionales con voluntarios locales para su rápida adaptación a la actividad y al entorno.

Si deseas formar parte de la cadena del bien y ser voluntario durante 2018 puedes solicitar más información aquí.

**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**

## Enlaces relacionados

Fundación Adelias

**Pistoletazo de salida a la época de mayor consumo del año**

# El optimismo invade la campaña de Navidad

*Estamos en Navidad. Durante el próximo mes, las luces, los villancicos, las comidas y cenas y los regalos serán los protagonistas indiscutibles. Comienza el período del año de mayor consumismo y el más importante para la facturación de las empresas. Este año, tanto las consultoras como los principales jugadores del sector mayorista TI se muestran optimistas. Y es que pronostican una muy buena campaña de Navidad, para el canal de distribución TI también.*

España continúa siendo uno de los países más optimistas, tanto en lo referente a la situación económica actual como a las perspectivas de futuro. Ésta es una de las principales conclusiones del Estudio de Consumo Navideño 2017 de Deloitte que destaca, además, que la percepción sobre la situación en los hogares españoles ha mejorado en comparación con años anteriores. Este optimismo económico será la razón principal para el aumento del gasto durante la campaña navideña de 2017.

## Cuánto representa la campaña de Navidad

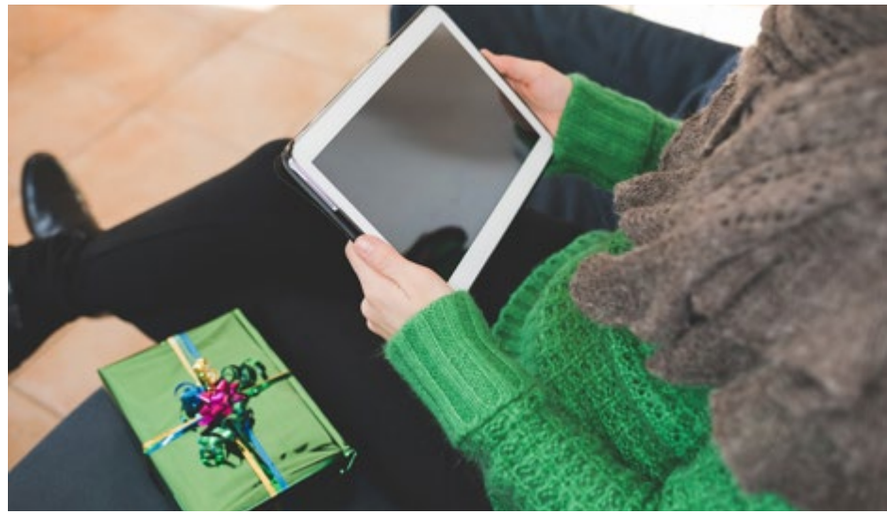
Y es que la campaña de Navidad es el periodo de ventas más importante para muchas compañías. Según datos de Adecco, "muchas empresas tienen cerca del 40% de su facturación ligada a este periodo", con lo que esto supone.

Esta situación no es ajena al canal mayorista TI. "En concreto para Tech Data, es una parte muy importante del global del año, aunque no podría cuantificar cuánto", destaca Paulí Amat, country manager de Tech Data España. "Lo que sí puedo decir es que para nosotros es un período clave, y de hecho trabajamos para sacar el máximo partido a estas fechas".

En este sentido, José Antonio Rodríguez López, director comercial de DMI, asegura que "el periodo comprendido entre el 1 de noviembre y el 31 de enero representa el 35% de las ventas anuales", mientras que, para Pedro Quiroga, CEO de MCR, "el último cuarto del año supone más del 25% de la facturación global de nuestro ejercicio, y la mayor parte de las ventas se concentra en la última parte del trimestre. Es decir, en dos meses manejamos prácticamente una cuarta parte de nuestro objetivo de negocio".

## Intención de gasto

El optimismo es tal que el informe de Deloitte destaca que, por primera vez, España superará a Reino Unido en intención de gasto para esta Navidad, pasando a liderar el ranking de países europeos encuestados. Los procesos de negociación del Brexit y las inestabilidades políticas han generado un optimismo más moderado en países como Reino Unido, Bélgica, Grecia o Rusia.



En el caso de España, este año gastaremos de media 633 euros en las compras navideñas, lo que supone un incremento del 3,3% frente al gasto real incurrido de los consumidores nacionales en 2016.

La mayor partida presupuestaria se la lleva la compra de regalos (252 euros), seguido de comida (195 euros), viajes (106 euros) y ocio


"Cada reseller sabe bien en qué promociones puede salir y en cuales no por una cuestión de la naturaleza de su negocio"

José Antonio Rodríguez López, director comercial de DMI Computer

La visión del analista

## La campaña de Navidad

**Llegan las navidades y con ello se incrementa la venta de dispositivos electrónicos. Las tablets, los ordenadores portátiles o los relojes inteligentes se posicionan siempre como buenas opciones de cara a sorprender a nuestros seres queridos. Sin embargo, año tras año, todos hemos ido acumulando una gran cantidad de dispositivos, ya sean empresariales o de consumo, lo que ha ocasionado que hoy nos encontremos ante un mercado bastante saturado.**

**Laura Castillo,**
*analista de IDC*

La actualización de dispositivos responde hoy en día a los ciclos de renovación, más que a la adquisición de nuevos elementos, debido a la mencionada saturación, pero también a la falta de novedades disruptivas. Esto provocó que en 2016 la caída de ventas fuera muy significativa. Sin embargo, en 2017 el mercado se está empezando a estabilizar.

Por ejemplo, las ventas de smarthphones prácticamente se duplicaron en España entre 2011 y 2015, tendencia que empezó a cambiar en 2016, con una bajada de las ventas cercana al -5%. Este año, la caída se ha suavizado, situándose en un -1,6%. Algo similar ocurre con las tablets y los ordenadores portátiles. Cabe destacar que aquellos dispositivos cuyas ventas más han crecido son los convertibles, los ultraligeros y los 2 en 1. Uno de los motivos de este crecimiento es la tendencia creciente hacia el trabajo en movilidad.

Por otro lado, las ventas de wearables en España aumentarán un 20,9% en 2017, frente al 2,2% de 2016. Esto se debe a que cada vez hay más proveedores que apuestan por este mercado, aumentando la tipología de productos y los campos de uso. A los wearables ligados al ocio o al deporte se unen aquellos enfocados en la salud, los servicios de campo o la atención al cliente. A pesar de este panorama esperanzador hay que tener en cuenta que nos encontramos ante un mercado menor en volumen, en el que aún quedan retos por superar, como la dependencia de los smarthphones.

Los próximos años son cruciales de cara a introducir novedades que impulsen el mercado. En opinión de IDC, las ventas tanto de smartphones como de PCs, tablets o wearables aumentaran a medida que los dispositivos ganen en conectividad y funcionalidades. La realidad aumentada o virtual y la inteligencia artificial, por ejemplo, serán dos capacidades cada vez más demandadas, tanto en el ámbito de consumo como en el empresarial. Cada vez más compañías incorporarán este tipo de capacidades para mejorar su flujo de procesos, ganando en agilidad y productividad, así como facilitando la toma de decisiones.

(80 euros). En España, el total de presupuesto para esta Navidad aumenta en todas las partidas, tendencia que también experimentan el resto de países europeos encuestados por Deloitte, siendo ocio y viajes las que experimentarán un mayor porcentaje de crecimiento.

Los videojuegos seguirán siendo, un año más, el regalo preferido para adolescentes, seguido de dinero. Cabe mencionar la fuerte entrada de los juegos de mesa en el top 10 de regalos para adolescentes, escalando 9 puestos y ocupando el octavo lugar.

### Previsiones de los mayoristas

El optimismo también reina en el canal mayorista. Pedro Quiroga destaca que MCR tiene depo-

sitadas “muchas expectativas en esta campaña”. Quiroga recuerda que “en 2016 todo se ralentizó un poco por diversos factores coyunturales, pero creemos que 2017 será un año mucho mejor y que en estos días que quedan de año se va a recuperar el crecimiento. Esperamos que ese incremento en la confianza de los consumidores tenga su reflejo en el nivel de gasto”.

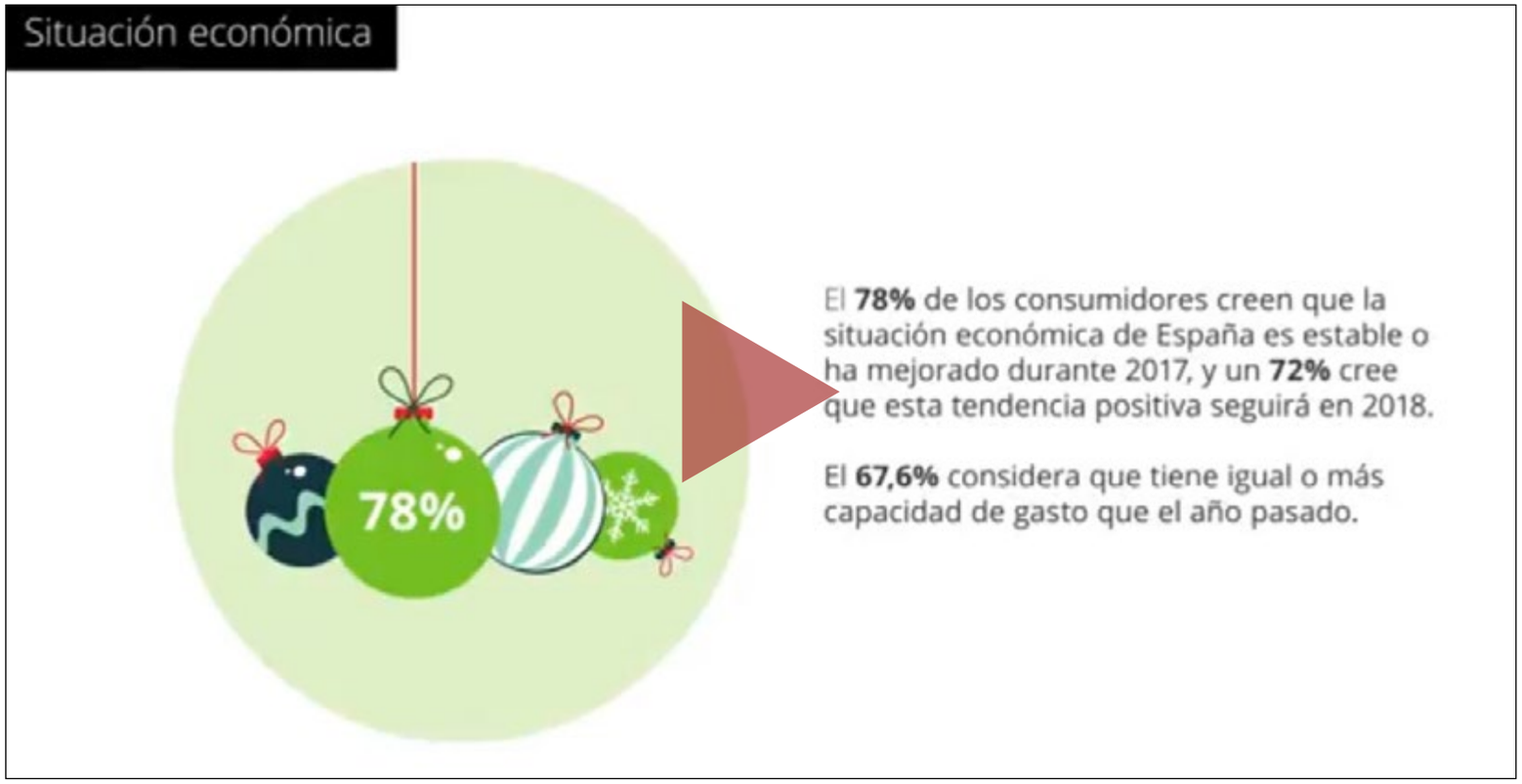
El objetivo de DMI es “crecer por encima del 20%” durante esta campaña de Navidad, tal y como reconoce José Antonio Rodríguez López.

2017 “será mejor que el año pasado”, asevera Paulí Amat. A la hora de realizar esta afirmación, Amat explica que en 2016 “la incertidumbre política y la difícil situación económica hicieron que el mercado no creciera como se esperaba. Este año, según nuestras previsiones, será mucho mejor, y somos moderadamente optimistas en cuanto al crecimiento en la facturación”.

## Aumento de la contratación

El optimismo reinante también quedará reflejado en el empleo. Según un estudio de Adecco, durante los meses de noviembre, diciembre y enero se firmarán más de un millón de contratos (1.083.400) de puesta a disposición, lo que supone un crecimiento del 14,7% que en el mismo periodo del año anterior. “Estamos en un momento de crecimiento económico que tiene su reflejo en la creación de empleo de estos meses”, asegura Luis Miguel Jiménez, director comercial de Adecco Outsourcing. “Las previsiones para la presente campaña navideña, tras cuatro años de incrementos interanuales de dos dígitos, nos hablan de una contratación récord que, si bien está muy ligada a la estacionalidad de la campaña, supone una puerta de entrada al mercado laboral que puede ser el acceso a un empleo estable”. Tras la campaña, un cuarto de las contrataciones podría prolongarse en los siguientes meses de 2018.

### CONSUMO NAVIDEÑO: PERCEPCIÓN DE LA SITUACIÓN ECONÓMICA DE LOS ESPAÑOLES




CLICAR PARA VER EL VÍDEO

El informe de Adecco destaca que los sectores protagonistas de la campaña serán el de gran consumo, atención al cliente y fuerza de venta, donde se esperan un incremento del un 30% en la contratación. En esta línea, el perfil comercial será el más buscado.

Otros sectores que también aumentarán su plantilla de cara a la Navidad serán alimentación, distribución y retail, logística y transporte,

# Próximos #ITWebinars

www.ittelevision.es


## El puesto de trabajo productivo:
### dispositivos y tecnologías para potenciar el rendimiento

**Martes, 30 de enero de 2018**


## Definiendo la seguridad de un SDDC

**Martes, 27 de febrero de 2018**


## Gestión de vulnerabilidades

**Martes, 27 de marzo de 2018**


## Estrategias para lograr una experiencia de cliente satisfactoria

**Jueves, 29 de marzo de 2018**

mitad de todos los contratos que se efectuarán entre noviembre y diciembre.

Las regiones que realizarán menos contratos en estas fechas serán Extremadura, con 2.543 contratos previstos (+8,8%) y Baleares, donde se firmarán 5.235 contratos, un 15% más que en la campaña anterior.

## La influencia del Black Friday

Aunque la primera quincena del mes de diciembre se mantiene como el período de mayor actividad para realizar las compras navideñas, el mes de noviembre sigue consolidándose como uno de los preferidos por los españoles para comprar. Según el estudio de Deloitte, el 31% de las compras para estas navidades se llevarán a cabo en noviembre, aprovechando los grandes descuentos que realizan las marcas con motivo del Black Friday, frente al 33% de la primera quincena de diciembre.

Y es que el Black Friday implica el inicio de la campaña de Navidad, ya que muchos consumidores adelantan sus compras a esta jornada comercio electrónico, electrónica, imagen y sonido, banca o contact center.

Por comunidades, Cataluña será la región que más contratos realice en estos meses, por encima de los 187.000, un 18,6% más que en la anterior campaña. Le seguirán Comunidad Valenciana, con 169.000 contratos (+13,9%), y Madrid, con 147.600 contratos (+16%). Estas tres regiones concentrarán así prácticamente la

> "Muchos clientes prefieren buscar especialistas que les informen de primera mano y que les asesoren sobre los productos que mejor se adaptan a sus necesidades"
>
> Pedro Quiroga, CEO de MCR

## *El comprador móvil ante las compras navideñas*


Durante la temporada de compras navideña -de noviembre a enero-, las compras a través de smartphones o tablets se disparan, especialmente en el segmento de población que va de los 18 a los 34 años. Este estudio revela los hechos y tendencias que los retailers online deben tener en cuenta para maximizar el periodo de compras que se aproxima. ¡Léelo!

da (cada año supone un porcentaje mayor del presupuesto navideño, habiendo incrementado en un 6% respecto al año pasado).

El crecimiento de las ventas durante el último fin de semana de noviembre (en el que se celebra el Black Friday y el Cyber Monday) es uno de los factores principales que ha hecho que el comercio de proximidad se anime a participar en esta jornada. En opinión de la Confederación Española de Comercio (CEC), "calculamos que en torno al 30% de las pymes de comercio aprovecharán esta fecha para ofrecer descuentos que les permitan ampliar sus ventas".

La CEC destaca el beneficio económico y social que supone la adhesión al Black Friday por parte de este tipo de comercio. "Esta campaña es positiva en cuanto que supone recuperar un período de descuentos con fechas acotadas, y en consecuencia esto genera una fiebre compradora".

La liberalización de los períodos de rebajas en 2012 tuvo como consecuencia más directa la confusión en el consumidor, que ya no tiene claro en qué momento va a encontrar los mejores precios y descuentos. En este sentido, "esta jornada de descuentos supone un fuerte efecto reclamo", afirman desde la CEC, si bien hace hincapié en que "la apuesta más importante para el pequeño y mediano comercio sigue siendo la campaña de Navidad y Reyes".

## Qué compramos durante el Black Friday

De acuerdo con Idealo, los productos más buscados en España durante este Black Friday fueron los smartphones, que estuvieron en la lista de la compra del 28,5% de los españoles, los cuales contaron con un descuento medio de un 3% durante la jornada.

## Estrategias de los mayoristas para incentivar las ventas del canal en Navidad

Año tras año, los principales mayoristas tecnológicos ponen en marcha iniciativas que buscan incentivar las ventas del canal en esta época del año.

- **DMI.** En el caso de DMI, José Antonio Rodríguez López explica que "una buena selección de las marcas más vendidas, con promociones bien planificadas, es clave para fomentar las ventas. La gestión que realiza nuestro equipo comercial es sumamente importante, queremos explicar a nuestros clientes los motivos que nos llevan a seleccionar estos productos y no otros".
- **MCR.** Pedro Quiroga, por su parte, afirma "como primer mayorista español en el mercado de consumo, para nosotros son, como decía antes, momentos clave que tienen un impacto decisivo. En este sentido, desde MCR contamos con programas de incentivos y fidelización que buscan potenciar las ventas en este período".
- **Tech Data.** Paulí Amat asegura que "en la parte comercial, como ya es habitual desde hace varios años, ponemos en marcha nuestra campaña de Navidad con regalos directos en función del importe de la compra del dealer. Y en la parte de operaciones, tenemos un plan específico que asegura por una parte la disponibilidad de los productos en los que la campaña de Navidad representa un incremento destacado de negocio, y por otra parte un seguimiento de procesos que garantice el nivel de servicio comercial, financiero y logístico ante un incremento importante de la demanda".

El segundo producto más buscado fueron los ordenadores portátiles, con un 19,5% de compradores, que pudieron encontrar un descuento medio de un 7% en este tipo de dispositivos.

Por su parte, los tablets ocuparon el tercer lugar, con el 16,8% de la demanda. La lista de productos más buscados se completó con las películas y series (12,3%), la música (12,1%), los libros electrónicos (10,6%), las cámaras de fotos (9,3%), los fitness trackers (8,5%) y los videojuegos (8,3%).

En cuanto al dinero que se gastaron los españoles en realizar sus compras durante este Black Friday, el estudio revela que la cuarta parte de los españoles gastará más de 100 euros. En concreto, un 16,5% contó con un presupuesto de entre 100 y 200 euros, el 4,9% gastó más de 200 y el 3,5% llegó hasta los 300 euros. Por su parte, algo más del 31% de los encuestados tenía la intención de gastar entre 50 y 100 euros y el 19,8% de los españoles gastaron menos de 50 euros.

## Influencia de las campañas de promoción

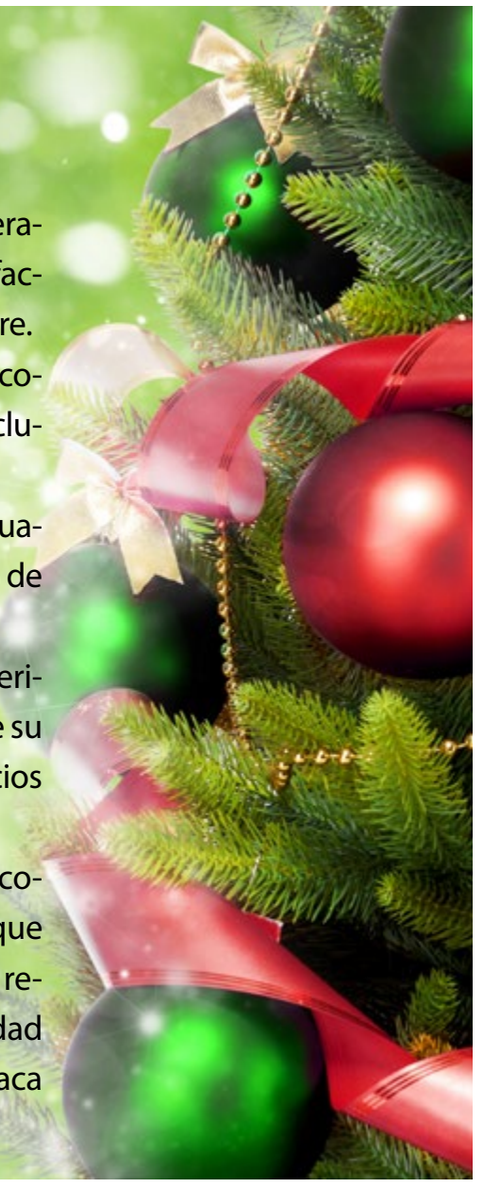
Las campañas de promoción para incentivar las ventas de cara a la Navidad, tipo Black

"La única vía de diferenciación está en el servicio, en el apoyo y sobre todo en el asesoramiento al cliente"

Paulí Amat, country manager de Tech Data España

# A pesar del auge de jornadas como el Black Friday, la Confederación Española de Comercio asegura que la apuesta más importante para el pequeño y mediano comercio sigue siendo la campaña de Navidad y Reyes

## El comercio catalán confía en la recuperación en Navidad



Según el Observatorio PIMEComerç, el comercio catalán confía en la recuperación económica a medio plazo, a pesar de la incidencia en las ventas y en la facturación que ha tenido el desafío independentista durante el mes de octubre.

En este sentido, la consulta destaca el optimismo en las previsiones de los comerciantes, ya que un 72,81% cree que las ventas serán las mismas, o que incluso aumentarán, durante los próximos meses.

De este modo, los comercios catalanes consideran que se trata de una situación coyuntural que, a pesar de haber afectado negativamente a un 62,89% de los consultados, puede solucionarse más adelante.

El estudio también refleja que el sector del comercio catalán no ha experimentado ningún tipo de boicot. Casi un 93% de las respuestas aseguran que su empresa no ha sufrido de forma notoria el rechazo a sus productos o servicios debido al panorama político actual.

"A pesar de que el conflicto político ha tenido una incidencia directa en el comercio en Cataluña, el sector lo entiende como un momento de transición que se puede resolver en los próximos meses, por lo que PIMEComerç pide a los representantes políticos que contribuyan a que el entendimiento y la estabilidad se abran paso y se normalice la situación económica y social del país", destaca el organismo en un comunicado.

Friday o Cyber Monday tienen "un impacto decisivo", explica Pedro Quiroga. "Estas iniciativas, en realidad, no sólo promocionan los productos, sino que tienen un papel informativo e incluso pedagógico. Obviamente, existe una vertiente comercial, enfocada a la venta, pero también es un vehículo de dinamización y de puesta en claro dónde están las principales novedades y tendencias", continúa el CEO de MCR.

En cambio, para José Antonio Rodríguez López, hay que diferenciar "entre la vía de compra que utilice el cliente final". En este sentido, continúa asegurando que "existen grandes diferencias entre las compras online y las offline. Las ventas online en los días claves como Black Friday y Cyber Monday son mayores en cuanto a número de pedidos, siendo las del mercado offline las que registran mayor importe medio y se utilizan más para los días de Papa Noel y especialmente Reyes".

Independientemente del canal, estas campañas "tienen una influencia importante, y no sólo porque sirven para fomentar las compras del canal, sino también porque es uno de los

momentos en que más cercanos nos sentimos a nuestros clientes", asegura Paulí Amat.

Lo que está claro es que, en menor o mayor medida, días como el Black Friday y el Cyber Monday están ganando peso, aunque "en España, y a diferencia de otros países en los que tienen una importancia clave para el negocio del mayorista y de los distribuidores, aún no importa en la misma medida", asegura Pedro Quiroga, quien reconoce que "ya se han convertido en días de actividad frenética, y complementan a la campaña de Navidad de una forma importante".

## ¿Saben los resellers aprovechar estos días?

Desde DMI se apunta a que "hoy en día no es posible mantener un negocio offline vendiendo con los precios online. Cada reseller sabe bien en qué promociones puede salir y en cuales no por una cuestión de la naturaleza de su negocio".

José Antonio Rodríguez López añade que "los resellers saben hacerse valer, han tenido que luchar en muchas batallas durante los últimos años por la rentabilidad, realizan una buena preventa, logran que el cliente final les confíe sus compras… Entre otros motivos gracias a la asistencia técnica que realizan buena parte de ellos, ése es el punto clave para ganar confianza y lograr la venta".

Los "días descuento" son "modas que se están consolidando poco a poco, en especial entre los consumidores más jóvenes, pero para nosotros ya suponen un hito importante en el año y, por qué no decirlo, un punto de incremento en las ventas. Y esa misma experiencia que nosotros percibimos es, precisamente, la que van teniendo los resellers cada vez más", añade Paulí Amat.

## ¿Dónde compraremos los regalos navideños los españoles?

El comercio electrónico continúa su senda alcista en nuestro país. Así lo indica una nueva edición del Estudio sobre Comercio Electrónico B2C del Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), de Red.es, que eleva a 25.354 millones de euros el volumen de negocio de este sector en 2016, un 22,2% más que en el año anterior. Este incremento se debe, sobre

CONSUMO NAVIDEÑO: PRESUPUESTO DE LOS ESPAÑOLES


CLICAR PARA VER EL VÍDEO


## *Estudio de consumo navideño*

El 'Estudio de Consumo Navideño 2017', elaborado por Deloitte, analiza las principales tendencias de consumo de los españoles para estas Navidades. Este año gastaremos de media 633 euros en las compras navideñas, lo que supone un incremento del 3.3% frente al gasto real incurrido de los consumidores nacionales en 2016.

todo, al aumento del gasto medio por comprador que alcanza los 1.198 euros, un 18% más que en 2015.

Este auge del comercio electrónico también se deja notar en las compras navideñas. No en vano, el estudio de Deloitte destaca que el 25% del presupuesto que destinarán los españoles a comprar en Navidad se gastará en canales online, lo que supone un incremento de un 10% respecto al año pasado.

Además, y aunque aún estamos lejos del resto de países europeos en lo referente a la compra online (incremento del 30%), las aplicaciones tecnológicas, desarrolladas por los comerciantes, están siendo muy bien recibidas por los consumidores.

Sin embargo, las compras offline o en tiendas físicas siguen siendo la opción preferida para realizar las compras. A pesar de que los grandes almacenes siguen siendo la principal opción, "los consumidores españoles no se casan con nadie", destaca el informe, y prefieren repartir sus compras entre las distintas alternativas: grandes almacenes (54%), cadenas especializadas (45%), hipermercados y supermercados (42%), comercio minorista (36%) y otros (16%).

### Como diferenciarse

Como muestran diferentes estudios, los españoles, cada vez más, apuestan por comprar sus regalos navideños a través de e-tailers. En el mercado de consumo, este tipo de compañías se han ido consolidando debido a que "es un mundo en el que los servicios, el soporte, la cercanía… no son tan relevantes como el precio, aspecto en el que el reseller tradicional tiene muy complicado competir", destaca Paulí Amat. "La única vía de diferenciación está en el servicio, en el apoyo y sobre todo en el asesoramiento al cliente, por lo que la clave está en conocer bien el mercado, los productos y al propio cliente".

## Smartphones y ordenadores portátiles reinaron durante el Black Friday y el Cyber Monday

Para José Antonio Rodríguez López, los resellers tienen que diferenciarse "como lo hacen en la actualidad, buscando la diversificación en sus negocios, manteniendo sus mostradores para la venta offline y sobre todo como reclamo de reparaciones, empleando todo el tiempo posible en la captación de empresas a las que realizar mantenimientos de equipos, redes, servidores, etc. En estos servicios el reseller se diferencia notablemente del e-tailer".

"El canal de distribución online se está consolidando como un actor clave en nuestro país, pero, en un mercado tan dinámico y complejo como es el de la tecnología, muchos clientes prefieren buscar especialistas que les informen de primera mano y que les asesoren sobre los productos que mejor se adaptan a sus necesidades", explica Pedro Quiroga. "Por tanto, y dando por supuesto que para el dealer "tradicional" es difícil competir en precio con el e-tailer, lo que ha de hacer es especializarse, aportando a los clientes un valor que no se puede encontrar en una página web".

**¿Cuáles serán los dispositivos más codiciados en la temporada navideña?**

Durante la campaña de Navidad, las marcas y los retailers ofrecen una gran variedad de ofertas en dispositivos electrónicos. Entre los productos que esperan atraer más a los consumidores figuran auriculares, tablets, pulseras de fitness, smartphones y televisores. Así lo indican las estimaciones de Gartner, que también prevé un aumento de ventas de smartwatches, altavoces inteligentes y auriculares inteligentes.

"Desde hace varios años, Black Friday se ha convertido en un motor de ventas en Europa, tanto en el comercio in-line como off-line. Vemos esta tendencia en muchos países europeos, incluido el Reino Unido, Alemania, Francia y España, donde Black Friday y Cyber Week se han convertido en términos bien conocidos para los compradores. Sin embargo, vemos algunas diferencias regionales entre Estados Unidos y Europa. En la mayoría de los casos, se relacionan con la disponibilidad del producto en lugar de las preferencias del producto", señala Annette Zimmermann, vicepresidenta de investigación en Gartner.

Respecto a cuáles serán los dispositivos más vendidos en Europa, Gartner señala que la demanda será similar a los Estados Unidos. Se espera que la conectividad celular incluida en el Apple Watch Series 3 estimule el interés de los consumidores por este producto en Europa. Apple ha alcanzado acuerdos con algunos de los CSP más grandes de Europa, incluidos Deutsche Telekom y Orange, inicialmente. Sin embargo, se necesitarán más acuerdos para impulsar una mayor adopción entre los consumidores en Europa.

El dispositivo estrella de Fitbit, Ionic, anunciado en IFA en septiembre, también podría estar en las listas. Sin embargo, el Reino Unido es el único país europeo donde actualmente funciona una de sus características más novedosas, Fitbit Pay. "Los servicios de pago de otros proveedores también son irregulares en Europa. Los servicios de pago eficientes y fiables en dispositivos móviles deben ser una prioridad para todos los proveedores en general, ya que

# Durante la campaña de Navidad, las marcas y los retailers ofrecen una gran variedad de ofertas en dispositivos electrónicos

impulsarán cada vez más la experiencia del usuario y fomentarán la lealtad a la marca", señala Zimmermann.

Como no podía ser de otra manera, los smartphones seguirán siendo un regalo de Navidad muy codiciado. Gartner espera que las ventas de terminales alcancen 1.570 millones de unidades en 2017, un 4,9% más que en 2016. Huawei continúa creciendo en Europa con una cuota de mercado del 11,9% en el tercer trimestre de 2017, registrando una subida anual del 10,2%, afianzándose en la tercera posición después de Samsung y Apple.

## Modos de pago

Y, ¿cómo pagamos? Los consumidores españoles siguen evitando las opciones de crédito en sus compras, tanto online como offline. El estudio de Deloitte señala que la opción de pago preferida para las compras en Internet son los monederos digitales (35%), aunque representan un porcentaje muy reducido de las adquisiciones presenciales (7%). El desconocimiento sobre estas aplicaciones de pago y la preocupación por la seguridad de los datos son las principales razones para su, todavía, escasa implementación.

Por su parte, el II Informe bankintercard, de Bankinter Financial Service, desvela que, el actual proceso de transformación digital está provocando que se produzca una transformación en los sistemas de pago. En la actualidad, el sistema que más éxito tiene es el contactless (el 31% de las compras con tarjeta se ha realizado utilizando este sistema en lo que va de año). El sistema wallet también está viviendo un rápido crecimiento, sobre todo entre los más jóvenes.

No obstante, y por segundo año consecutivo, el medio de pago principal de los españoles son las tarjetas. En este sentido, el informe señala que los usuarios españoles de tarjetas han aumentado un 71% su gasto en compras online en tan solo cinco años.

¿TE HA GUSTADO ESTE REPORTAJE?

***Compártelo en tus redes sociales***

## Enlaces relacionados

- Entrevistas completas a DMI, MCR y Tech Data
- Estudio Consumo Navideño 2017 de Deloitte
- Estudio Adecco, previsiones de creación de empleo noviembre, diciembre de 2017 y enero de 2018
- II Informe Bankintercard de Bankinter Consumer Finance
- Oportunidades de la economía digital en España
- ¿Están tus empleados preparados para el puesto de trabajo digital en tienda?
- Cómo hacer grandes cosas en los negocios
- Transformación digital en las empresas


## 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

it Digital Security

La publicación electrónica sobre Seguridad Digital que necesitas

Diciembre 2017 - nº 3

# Ataques DDoS, del pánico al reto


Check Point Experience 2017

Priorizando la gestión de vulnerabilidades

SIEM o la óptima gestión de eventos de seguridad


Por una Transformación Digital Segura

Recuperación ante desastres, ¿estás preparado?

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


# DDoS, del pánico al reto

**Afrontar su crecimiento. Este es el primer reto al que se enfrentan las empresas en lo que a ataques de Denegación de Servicios Distribuido, o DDoS, se refiere. Empezaron como casi todo, haciendo pruebas a ver qué pasaba, y con los años y la evolución de las tecnologías ya se lanzan ataques en los que participan miles de dispositivos. ¿El objetivo? Echar abajo una web, y estando como estamos en la era del cloud y el as-a-service, un ataque DDoS puede ser fatal.**

**En el segundo trimestre de este año los ataques DDoS se incrementaron un 28% y junto a los ataques UPD o DNS, que son tipos de ataques de Denegación de Servicio, este año se habla de Pulse Wave, que consiste en lanzar los ataques mediante oleadas de pulsos que hace que algunas soluciones tengan dificultades para contenerlo. Pero hay más, porque el IoT, millones de dispositivos conectados y con poca seguridad han entrado en el juego. Ejemplo la botnet Mirai, que el año pasado generó el pánico en Internet. Entre las empresas afectadas Dyn, un proveedor de servicios DNS que meses después sería comprada por Oracle por 600 millones de dólares. Se supo después que unos 14.500 dominios que utilizaban los servicios de Dyn abandonaron la compañía inmediatamente después del ataque.**

**Pero en este número de IT Digital Security también hemos prestado atención al mercado SIEM (Security Information and Event Management). Evolución de las herramientas de gestión y correlación de logs, los SIEM se han convertido en soluciones imprescindibles para saber lo que está ocurriendo gracias a su capacidad para consolidar toda la información respecto a posibles incidentes de seguridad.**

**IT Digital Security sigue adelante con su programa de eventos con un nuevo webinar titulado Por una Transformación Segura en el que portavoces de Check Point, Commvault, Trend Micro, Quest, Kaspersky y DXC plantearon sus propuestas para hacer de la digitalización un proceso seguro que debe tenerse en cuenta antes de iniciar ningún proyecto.**

**Nuestro segundo desayuno agrupó a representantes de Quest, Kaspersky, Check Point y DXC. Bajo el título Recuperación ante desastres, ¿estás preparado? se generó un interesante debate que puso de manifiesto que no es tan obvio, como debería, que las empresas cuenten con planes de backup, disaster recovery y continuidad de negocio. Y cuando los tienen, sobre todo en empresas grandes, pocos se han preocupado de comprobar si funcionan.**

IT Digital Security

**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

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

En Portada

# Ataques DDoS, del pánico al reto

## No solo IT

**La amenaza del cibermal sobre el ciberbien**

**Ciberseguridad & Talento: un problema global**

**Tú eres la clave para la protección de datos**

## Actualidad


**Check Point Experiencie 2017**

**Priorizando la gestión de vulnerabilidades**

**SIEM, o la óptima gestión de eventos de seguridad**

## Desayunos ITDS

**Recuperación ante desastres, ¿estás preparado?**

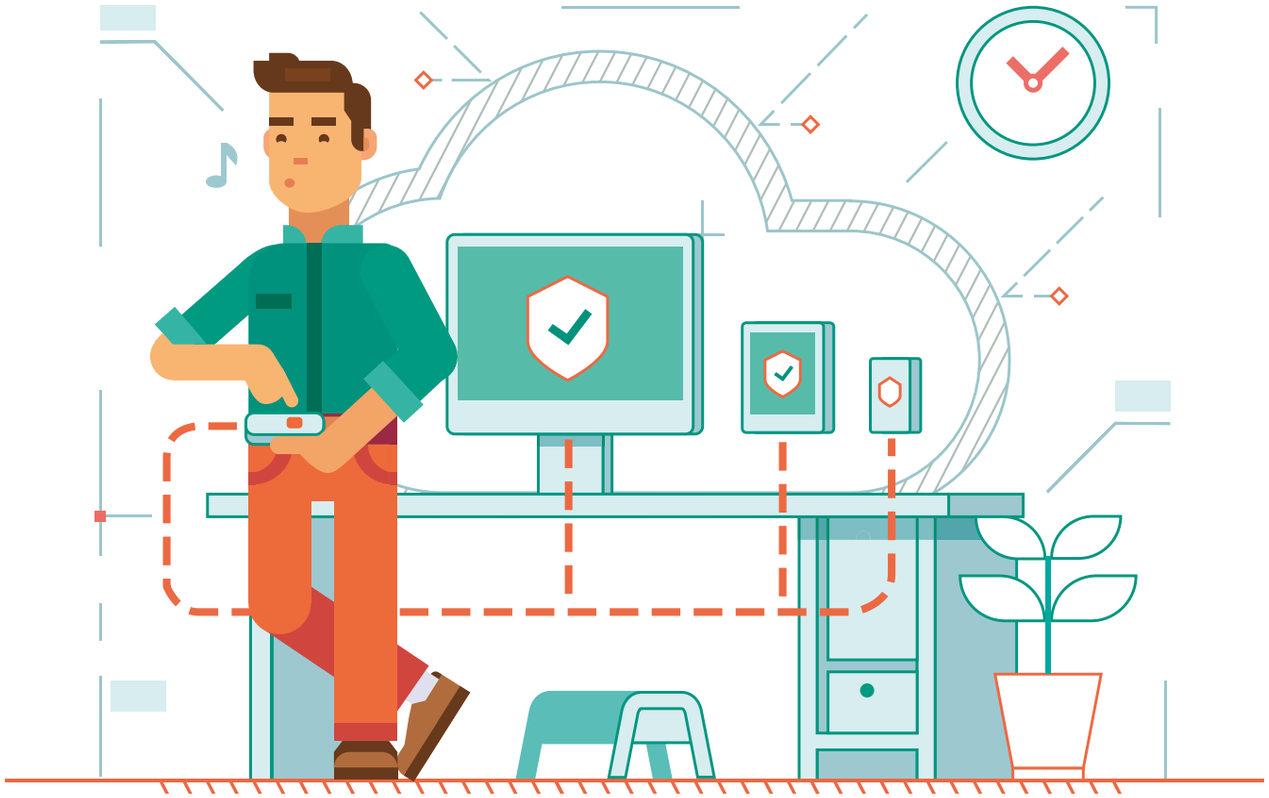
## Webinars ITDS

**Por una Transformación Digital Segura**

## Índice de anunciantes



¿Te avisamos del próximo IT Digital Security?



# 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**

## Check Point Experience 2017


# Check Point insiste en la necesidad de prevenir para evitar incidentes de ciberseguridad

**Ante el panorama de ciberamenazas que se plantea a las empresas, Check Point tiene claro que la prevención es la primera medida que debe tomar una empresa si no quiere verse comprometida. Y con esa intención diseña sus soluciones.**

Uno de los ataques de ciberseguridad descubierto por Check Point se ejecuta de una forma tan simple como descargando scripts para disponer de subtítulos en las películas. El ataque fue descrito por uno de los expertos del equipo de investigación que la firma tiene en Israel y que viajó a España con motivo del Check Point Experience 2017, que tuvo lugar los pasados 21 y 22 de noviembre en Toledo y al que acudieron 300 clientes y partners de la compañía para conocer sus últimas propuestas.

El panorama de ciberamenazas no es nada halagüeño, sobre todo si tenemos en cuenta que muchos de estos ataques se aprovechan del desconocimiento del usuario y de su confianza. También de los fallos en los procesos, como la falta de actualización del software o los sistemas empresariales a las últimas versiones disponibles, y porque el perímetro se ha ampliado tanto que los frentes a proteger ahora nos llegan hasta la nube. Por eso, la mejor medida para evitar un ciberataque es prevenir.


CHECK POINT EXPERIENCE 2017

CLICAR PARA VER EL VÍDEO

"Si la tecnología no está implementada como prevención no se va a poder parar ningún ataque. Todos los puntos de ataque deben tener una protección", aseveró Eusebio Nieva, director técnico de Check Point España y Portugal, durante su intervención, en la que describió los tres pilares de Check Point: una seguridad sin atajos, una arquitectura ubicua y una eficiencia operacional.

"Estamos muy concentrados en proporcionar soluciones, pero también miramos cómo está evolucionando la seguridad diaria", añadió Nieva apuntando que el objetivo de la compañía es "asegurarnos de que nuestros clientes no son vulnerables". En ese sentido, Check Point considera los sistemas de prevención de intrusiones como una pieza fundamental, "porque permiten actuar lo antes posible". También destacó el valor del equipo de investigación de la firma, que ha sabido responder ante exploits en un tiempo menor que el de otros proveedores, "si bien no estamos orgullosos cuando tardamos dos días en descubrirlo, aunque la competencia lo haga en una media de seis días".

Check Point Experience sirvió a la compañía para dar a la audiencia detalles de las novedades introducidas, como la nueva consola R80.10, o la incorporación de detección de campañas masivas de ransomware en la plataforma Infinity: "aplicamos machine learning, detección de campañas de scripting y firmas dinámicas", explicó el director técnico de Check Point. También destacó una nueva solución de protección para móviles – "que muchos quieren tener para su protección personal", y la oferta en la nube y la automatización.

> "Falta gente cualificada capaz de dar servicios de ciberseguridad, de implantar estas soluciones"
>
> Mario García, director general de Check Point

Respecto a la eficiencia operacional, Nieva aseguró "que somos la tecnología de referencia en gestión de una arquitectura completa. Porque tenemos una política de acceso unificada, nuevas tecnologías y formas de gestión". "Check Point va hacia la seguridad total -continuó-. Si tomas atajos, vas a tener problemas de seguridad. Si estas atento solo a una cosa, vas a tener un problema de seguridad. Intentamos cubrir todos los posibles problemas desde el pre-compromiso o los problemas de un pre-ataque, durante y después del ataque".

"Si la tecnología no está implementada como prevención no se va a poder parar ningún ataque"

Eusebio Nieva, CTO de Check Point


**Compromiso con el talento en materia de ciberseguridad**

Check Point Experience, antes conocido como Check Point University, también sirvió al proveedor de seguridad para exponer sus logros a nivel local. Así, Mario García, director general de la firma, hizo subir al escenario a todo el equipo de la filial, mostrándose orgulloso de los objetivos alcanzados. El directivo aseguró que "ha sido un buen año. A principios de 2017, contratamos a cuatro personas: en compañías como la mía, la facturación se estructura en función de las personas contratadas, y la facturación crece linealmente. Lo hemos conseguido. A mitad de año, vimos que falta gente cualificada capaz de dar estos servicios, de implantar estas soluciones. Así que hemos contratado a cuatro juniors que están pasando en Israel diez semanas para formarse y el año que viene tendremos cuatro ingenieros más para trabajar con nosotros. Hacemos una apuesta por la creación de talento. Cogemos a gente de la universidad, con 1 o 2 años de experiencia, ante la falta de profesionales formados. Las cosas van relativamente bien, y nos permiten hacer este tipo de inversiones".

Y si las cosas van bien para Check Point es porque las empresas cada vez están más concienciadas de la necesidad de seguridad, aunque todavía haya camino por recorrer. "Las empresas han entendido que se tienen que defender frente a los nuevos ataques que están llegando. El ransomware es muy serio, y hay que tener tecnologías que lo paren y que eviten el impacto en la empresa", señaló el responsable de la compañía en el mercado español. Aún falta, tal y como añadió García, "concienciación en materia de seguridad en el móvil. Estamos haciendo una labor en ese sentido y poco a poco algo se va avanzando".

**Enlaces de interés...**

- Check Point refuerza su negocio en España
- Check Point detecta una vulnerabilidad en los dispositivos LG SmartThinQ
- La totalidad de las empresas ha sufrido un ataque de malware móvil

MICRO FOCUS®

Discover

# the New

# Priorizando la gestión de vulnerabilidades

**Las soluciones de gestión de vulnerabilidades y seguridad son esenciales para las organizaciones, cada vez más necesitadas de gestionar los riesgos de seguridad, de contar con políticas y auditorías, y de consolidar toda la información sobre los posibles riesgos a los que se enfrentan.**

La gestión de las vulnerabilidades de software no es una opción. Los datos del último informe global de seguridad de Forrester indican que el 49% de las empresas ha sufrido una brecha de seguridad; de esta cifra un 56% había sufrido la brecha como un ataque externo como consecuencia de haberse explotado una vulnerabilidad de software.

La gestión de las vulnerabilidades es un reto importante para empresas de todos los tamaños. Y lo es porque nos encontramos en el entorno de TI más abierto, dinámico y fluido de todos los tiempos. Las aplicaciones y los equipos están distribuidos, los empleados son cada vez más móviles, el software se actualiza de manera constante. El perímetro de las empresas se ha difuminado y el volumen de vulnerabilidades crece año tras año.

De otro lado los hackers, cada vez más profesionalizados, cada vez más sigilosos y con herramientas capaces de explotar una vulnerabilidad de manera sencilla. Herramientas que, una vez validadas, venden para que otros con menos conocimientos técnicos puedan sacar provecho de fallos que, pudiendo haber sido reparados, aún siguen vigentes, esperando a quien quiera sacar provecho de ellos. En este sentido recientes informes ponen de manifiesto que muchas vulnerabilidades tienen disponibles herramientas de explotación en el mismo día que se publican.

Que algunas vulnerabilidades permitan a los atacantes la ejecución de código de su elección no hace sido convertir la gestión de las mismas en un elemento cada vez más importante dentro de las organizaciones.

Para Ascensio Chazarra, Security Services Leader de IBM España, el escaneo constante de toda la infraestructura de TI para detectar debilidades es una tarea compleja que puede ser costosa y un reto para cualquier empresa. Por tanto, “se hacen necesarias herramientas de gestión de vulnerabilidades que suponen un control básico en la gestión del riesgo de las organizaciones”.

En el ámbito estricto de la gestión tecnológica de vulnerabilidades, los sistemas de actualización de software resultan imprescindibles. Muchas empresas, entre ellas Microsoft recomiendan tecnologías basadas en System Center Configuration Manager (SCCM). Héctor Sánchez Montenegro, director de Tecnología de Microsoft Ibérica, explica que estas tecnologías ofrecen una consola de administración unificada con un conjunto automatizado de herramientas administrativas “para implementar software, proteger datos, supervisar el estado y aplicar el cumplimiento de normativas en todos los dispositivos de una organización. Tecnologías como WSUS (Windows Software Update Services) o Windows Update pueden igualmente ayudar en esta labor”.

> Los últimos incidentes masivos de seguridad, como Wannacry, han puesto de manifiesto la necesidad de disponer de mecanismos efectivos de gestión de vulnerabilidades
>
> Ascensio Chazarra, Security Service Leader de IBM España

A la hora de gestionar las vulnerabilidades es requisito imprescindible la identificación de las mismas. Detectarlas a la mayor brevedad es imprescindible para atajar cualquier intento de valerse de ellas para atacarnos. Para David Sánchez, responsable de Soporte Técnico de ESET España, el siguiente paso sería “subsanarlas antes de que

## Wannacry y Petya

**Un mes y medio después de que WannaCry mostrase el poder del ransomware para paralizar el mundo, el malware que afectó a empresas de la talla de Telefónica, Renault, PetroChina, Nissan o Hitachi, el mercado se veía golpeado por un nuevo ciberataque a escala global.**

**Se trataba de Petya, otro ransomware que no sólo utilizaba técnicas similares a WannaCry en cuando a secuestrar los ordenadores y exigir el pago de un rescate, sino que explotaba la misma vulnerabilidad: un fallo en debilidad en el protocolo del sistema operativo Windows para compartir en red que fue bautizado como EternalBlue.**

El parche de seguridad que solucionaba esta vulnerabilidad fue lanzado por Microsoft un 14 de marzo, antes de que el grupo ShadowBokers filtrara la existencia de la vulnerabilidad; vulnerabilidad que por cierto la Agencia Nacional de Seguridad de Estados Unidos había estado utilizando en secreto para obtener información.


La actualización se lanzó a través de Windows Update, inicialmente para las versiones de Windows posteriores a Windows Vista. Aunque posteriormente, y tras la gravedad del ataque, publicaría un parche para Windows 8, Server 2003 y XP.

En toda caso, casi dos meses después de estar disponible una solución para la vulnerabilidad EternalBlue, concretamente el 12 de mayo, se detecta un ataque a escala mundial que terminó afectando a miles de empresas. Que meses después se detectara un nuevo malware que explotaba la misma vulnerabilidad y tuviera éxito, demuestra que contar con una solución de gestión de vulnerabilidades no es una opción.

Wannacry y Petya también revelaron que muchas organizaciones no estaban preparadas para gestionar un incidente masivo de ciberseguridad y recuperar en el corto plazo sus procesos de negocio, lo que se denomina ciberresiliencia. Es necesario disponer de planes de respuesta efectivos que proporcionen funciones completas de retención, gestión y remediación de incidentes.

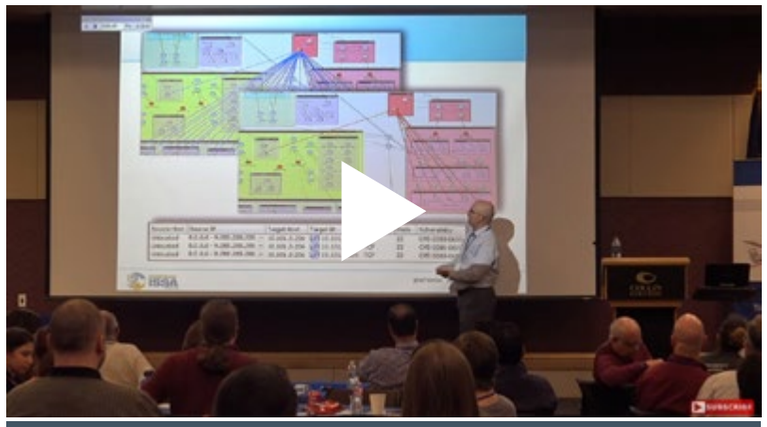
> La ausencia de mecanismos de gestión de vulnerabilidades es un error común y peligroso
>
> Héctor Sánchez, Director de Tecnología de Microsoft Ibérica

puedan ser utilizadas". Puntualiza el directivo que dentro del proceso de gestión de vulnerabilidades, existen puntos muy importantes como puede ser la evaluación del riesgo, que nos va a permitir priorizar las vulnerabilidades encontradas y a continuación aplicar las acciones necesarias para resolver la vulnerabilidad.

Javier Múgica, SE Leader Spain de F5 Networks, tiene claro que el paso más importante en el proceso de gestión de las vulnerabilidades es "lograr convertirlo en un verdadero proceso, con continuidad en el tiempo y con responsables con poder de decisión, con capacidad para poder tomar medidas de acuerdo a los resultados conseguidos". Añade Múgica que además, es muy importante que el análisis de las vulnerabilidades en aquellos elementos que por su naturaleza presentan una mayor exposición a ataques, como pueden ser los servicios web, se lleve a cabo de forma minuciosa. "También resulta esencial disponer de tecnologías de mitigación, como pueden ser los sistemas WAF (Web Application Firewall) o IPS, que permitan paliar las vulnerabilidades sin necesidad de esperar al parcheo de servidores y/o aplicaciones", añade el directivo.

De forma que el proceso de gestión de vulnerabilidades tiene como objetivo explorar las infraestructuras internas y externas de una organización para identificar y clasificar las vulnerabilidades y ofrecer medidas para remediar las amenazas. En opinión de Ascensio Chazarra, de IBM, los pasos más importantes en el proceso de gestión de vulnerabilidades son:

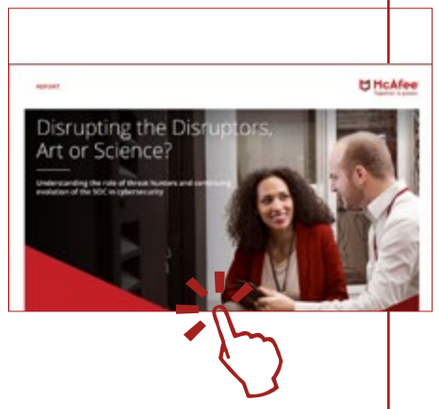
. Mantenimiento de base de datos actualizada en tiempo real con las vulnerabilidades
. Exploración/escaneo de vulnerabilidades ofreciendo avanzadas capacidades de escaneo que detectan las debilidades en la seguridad de los dispositivos de red, servidores, aplicaciones Web y bases de datos
. Establecimiento del nivel de seguridad identificando y clasificando vulnerabilidades



LA GESTIÓN DE VULNERABILIDADES NO ES SIMPLE — CLICAR PARA VER EL VÍDEO

## ¿QUÉ ES UN CAZADOR DE AMENAZAS? ¿NECESITAS UNO EN TU EQUIPO?

La caza de amenazas está desempeñando un papel decisivo en la lucha contra los ciberdelincuentes. Un cazador de amenazas es un profesional del equipo de seguridad encargado de analizar las amenazas a través del uso de pista e hipótesis y de su experiencia de años de investigación de ciberdelincuentes. La caza de amenazas está desempeñando un papel decisivo en la lucha contra los ciberdelincuentes. Descubre el valor que estos cazadores de amenazas aportan a los SOC, o centros de operaciones de seguridad. Y cómo impacta la adopción de tecnologías de automatización.



. Gestión del riesgo, utilizando datos anteriores para evaluar y gestionar mejor los riesgos de seguridad y reducir la exposición a amenazas, mediante la remediación, aplicación de controles secundarios o la asunción del riesgo.

Apunta también Ascensio Chazarra que hay que tener en cuenta que las herramientas de gestión de vulnerabilidades no protegen, por ejemplo, contra ataques denominados de “día zero” que explotan vulnerabilidades aún no divulgadas. “Para adelantarnos a estas amenazas avanzadas, los equipos de seguridad tienen que ser capaces de analizar flujos de la red, detectar comportamientos anormales, identificar patrones de actividades maliciosas y tener en cuenta el contexto completo de los eventos de seguridad que provienen de fuentes dispares”, asegura el directivo.

En cualquier caso, apunta Héctor Sánchez que conviene destacar que el uso de tecnologías de Cloud Computing, en modos SaaS, PaaS o IaaS, “nos ayudan en diferente medida a la tarea de mantener nuestros sistemas actualizados, tanto aquellos que se encuentren on premise (Microsoft Intune, Operations Management, etc..) como aquellos construidos sobre la nube y de cuya actualización se encarga directamente el proveedor de servicios en la nube”.

**¿Cuándo y quién debería adoptar una solución de gestión de vulnerabilidades?**

Cuanto antes. Esta debería ser la premisa respecto a cuánto adoptar una solución de gestión de vulnerabilidades. Si aún no cuentas con una solución de este tipo, ya vas tarde. Para convencerte sólo tienes que seguir el consejo de David Sánchez, de ESET: “Buscar en Google “lista de exploits” y acceder a alguna de las cientos de páginas que ofrecen exploits para explotar diferentes vulnerabilidades. El atacante lo tiene todo hecho, simplemente tiene que saber qué aplicación o sistema puede tener la empresa que sea vulnerable y lanzar el ataque”.

Y no se puede decir que no. Como afirma Javier Múgica, todos los entornos son susceptibles de adoptar una solución de este tipo; “a mayor número de activos, mayores serán los riesgos, pero el hecho de disponer de una infraestructura poco expuesta o un número menor de activos no implica que no se sea vulnerable o que se puedan omitir estos procesos”.

# El error más grave es no aplicar una política definida en lo que respecta a la gestión de vulnerabilidades, aunque sea como mínimo para los servidores de la organización

David Sánchez, Responsable de Soporte Técnico de ESET España

En cuanto a quién debería adoptar una solución de gestión de vulnerabilidades, lo cierto es que en los últimos años los ciberdelincuentes han cambiado su objetivo y éste ha pasado de ser el individuo a ser las empresas, siendo las motivaciones diversas, no sólo la económica. Ascensio Chazarra asegura que, aunque existen sectores especialmente "castigados", todas las empresas sin excepción pueden llegar a ser objetivo de la ciberdelincuencia, "por lo que todas las organizaciones deberían adoptar soluciones de gestión de vulnerabilidades como control básico, complementadas con un enfoque más proactivo de la gestión de seguridad basado en la integración automática con la correlación y la analítica".

El director de tecnología de Microsoft coincide al afirmar, de una manera más amplia, que la necesidad de seguridad no es exclusiva de una industria concreta o de un tamaño de empresa desde el momento que todas dependen de la información que manejan; "por ello, todas independientemente de sector o tamaño, deberían incorporar mecanismos de gestión de seguridad".

De igual parecer es el responsable de soporte técnico de ESET España, quien tras explicar que una solución de gestión de vulnerabilidades está al tanto de todos los sistemas y procesos que se ejecutan en los equipos de la empresa a tiempo real, avisa en cuanto se hace pública una vulnerabilidad y esto, a medio plazo, ahorra dinero y recursos a la empresa, cree que la adopción de este tipo de herramientas "no es una opción", sino que "debería de ser de las primeras preocupaciones a nivel de seguridad de la empresa a parte del antivirus y del cortafuegos".

Para el SE Leader Spain de F5 Networks, a medida que las empresas van siendo más pequeñas y disponen de menos recursos y/o conocimientos "se observa una tendencia hacia la relajación de los procesos de gestión de la seguridad, pero incluso en estos entornos son necesarios, por lo que la solución más adecuada para estos casos puede ser la externalización de los servicios a proveedores que puedan aportar el conocimiento y capacidad para su operación". En términos más generales asegura el directivo que cualquier compañía debe ser responsable de gestionar los riesgos y amenazas que sus sistemas de información puedan sufrir, incluyendo vulnerabilidades, disponibilidad, o integridad de la información.

**Errores más comunes**

No contar con una solución capaz de gestionar cantidad de vulnerabilidades que se descubren cada día, fallos de seguridad que exponen los sistemas y el negocio, es el error más grave en el que pueden caer las empresas. Los expertos consultores están de acuerdo en ello.

Además, Javier Múgica, de F5 apunta a una falta de capacidad de reacción ante el descubrimiento de una determinada vulnerabilidad y el tiempo requerido para la mitigación de la misma. Explica el directivo que en los procesos de parcheo y remediación intervienen muchas áreas, afectando, en muchas ocasiones, a las aplicaciones y sistemas operativos que, o bien por el volumen -muchos sistemas operativos afectados, por ejemplo-, o bien por la complejidad -parchear un aplicativo requiere desarrollo, pruebas, despliegue, etc.-, consumen demasiado tiempo. Es por ello que cada vez es más necesario el parcheo “virtual” de las vulnerabilidades -con sistemas WAF y/o IPSs-, para ayudar a reducir riesgos y ventanas de exposición.

Por su parte, Ascensio Chazarra apunta a que en el pasado muchas organizaciones implementaron herramientas de gestión de vulnerabilidades únicamente para cumplir con regulaciones de cumplimiento y políticas de seguridad, pero esas herramientas suelen ser soluciones aisladas en silos con escaneos para redes, aplicaciones y bases de datos por separado, lo que crea grandes ineficiencias tanto de tiempo como de esfuerzo. “Estas herramientas dispares suelen identificar un “mar” de vulnerabilidades que no están correlacionadas, categorizadas ni priorizadas, y que no generan información que se pueda utilizar”, explica el directivo, añadiendo que este enfoque reactivo se traduce en un proceso abrumador de gestión de parches y remediación en lugar de centrar los esfuerzos en las vulnerabilidades más críticas, y detectar debilidades ocultas que pasan inadvertidas en el escaneo periódico.

Para hacer frente a las amenazas avanzadas se necesita una analítica proactiva, predictiva y automatizada que permita comprender patrones normales de uso a fin de identificar rápidamente anomalías, actividades sospechosas y otras tendencias que supongan una amenaza y que ayuden a evitar la pérdida de datos y las interrupciones de servicio.

Además de la ausencia de mecanismos de gestión de vulnerabilidades como uno de los errores más comunes y peligrosos, Héctor Sánchez apunta

## Cada vez es más necesario el parcheo virtual de las vulnerabilidades, con sistemas WAF y/o IPS, para ayudar a reducir los riesgo y ventanas de exposición

Javier Múgica, SE Leader Spain, F5 Networks

a que la falta de una experiencia única de actualización “lleva además a una fragmentación de los sistemas que dificultan sobremanera su gestión y mantenimiento”.

Para David Sánchez, responsable de Soporte Técnico de ESET España, el error más grave “es no aplicar una política definida en lo que respecta a la gestión de vulnerabilidades, aunque sea como mínimo para los servidores de la organización”. A partir de ahí, añade el directivo que todavía existe una falta de concienciación grave sobre este problema de seguridad y que aún se percibe una falta de preocupación importante al respecto.

Apunta también David Sánchez que la forma de mitigar estas limitaciones es, sobre todo, con información y educación. “Las empresas están mucho más preocupadas por las APTs pero desconocen, en su gran mayoría, que este tipo de amenazas aprovechan vulnerabilidades para conseguir su objetivo y que teniendo las vulnerabilidades controladas y solucionadas pueden evitar, en un alto porcentaje, el riesgo de ser afectados por una APT”, asegura.

### Un futuro poco halagüeño

Y si ya vemos que las vulnerabilidades crecen, que cada vez hay más kits de exploits que permiten explotarlas de una manera relativamente sencilla, que la cantidad y variedad de las aplicaciones se ha multiplicado y que las empresas se ven desbordadas por mantener sus entornos adecuadamente parcheados, el futuro no puede sino ir a más.

Lo confirma el directivo de IBM, al asegurar que la tendencia de los últimos años pone de manifiesto un incremento de vulnerabilidades. La adopción de nuevas tecnologías en los procesos de transformación digital de las organizaciones sin las adecuadas medidas de seguridad por diseño, las vulnerabilidades en dispositivos móviles, que están en continuo aumento, o los plazos en el desarrollo de aplicaciones, cada vez más cortos y que obvian la seguridad en el ciclo de vida del software, pueden ser causas que lo justifiquen. A este hecho hay que sumar, continúa Chazarra, el incremento considerable de las vulnerabilidades en sistemas de control industrial y redes OT, de especial consideración al ser el soporte de infraestructuras críticas, y a los nuevos desafíos de seguridad que introduce el Internet of Things.

La ventana de tiempo que se abre desde que una actualización que corrige una vulnerabilidad se publica, hasta que esta es explotada por algún tipo de atacante o de malware, es cada vez más pequeña, recuerda Héctor Sánchez, para después asegurar que “es por ello por lo que es más necesario que nunca acelerar esos mecanismos de actualización, realizar las oportunas pruebas previas al despliegue de una actualización, asumiendo que el riesgo de no hacerlo es de por sí una inseguridad cada vez más difícil de asumir”.

Para David Sánchez, de ESET, si bien es verdad que a día de hoy la mayoría de los fabricantes que desarrollan sistemas o aplicaciones ya disponen de unos procesos claros de seguridad en ese desarrollo y que cada vez cuesta más detectar una vulnerabilidad, éstas siguen apareciendo y es necesario

que las empresas cuenten con una política efectiva y herramientas para gestionarlas. Añade que “el hecho de que se publique una vulnerabilidad en un sistema o aplicación no es algo que, en líneas generales, guste a los fabricantes o desarrolladores, ya que normalmente afecta a su imagen; sin embargo, es algo positivo para los usuarios ya que permite estar informado sobre la vulnerabilidad en cuestión y ayuda a que los fabricantes o desarrolladores trabajen o proporcionen una rápida solución.

Un punto importante en el panorama actual de las vulnerabilidades es el trabajo que realizan los white hat o hackers éticos, ya que gracias a su trabajo los usuarios estamos más seguros”.

Javier Múgica, de F5, recuerda que el número de exploits descubiertos en el tiempo es cada vez mayor, y añade que existe una multitud de informes que están disponibles en Internet y que muestran claramente el incesante incremento de vulnerabilidades y cómo, además, los tiempos requeridos para que una determinada vulnerabilidad sea explotada de forma masiva son cada vez más cortos. “El crecimiento exponencial de dispositivos conectados (IoT), que en muchos casos carecen de una gestión remota eficaz, va a causar múltiples incidencias de seguridad, por lo que el futuro no resulta especialmente halagüeño”, asegura.

### Adopción entre la empresa española

El as-a-service, los servicios basados en la nube, están haciendo que las soluciones de gestión de vulnerabilidades sean cada vez más accesibles, y que “la penetración de este tipo de soluciones sea cada vez mayor”, dice Ascensio Chazarra, Security Services Leader de IBM España

No con la velocidad necesaria, apunta Héctor Sánchez, director de tecnología de Microsoft Ibérica. “Por lo general, se mantiene en muchos casos en funcionamiento tecnologías obsoletas, fuera de soporte, con más de 10 o 15 de años de antigüedad, que por definición no se encuentran preparadas para responder con eficacia a las amenazas actuales”, dice el directivo, para después añadir que la obsolescencia tecnológica, junto con la ausencia de mecanismos de actualización, son sin duda dos de los riesgos de mayor impacto en ciberseguridad.

David Sánchez, responsable de soporte técnico de ESET España, asegura que en el mercado pyme el índice de adopción es sorprendentemente bajo y que si nos centramos en las grandes corporaciones, “la concienciación al respecto es mucho mayor pero aun así hay que mejorar”.

Para Javier Múgica, SE Leader Spain, F5 Networks, el nivel de adopción refleja una amalgama de posicionamientos y prácticas. “Sorprende, a veces, ver como grandes compañías descuidan claramente la gestión de sus vulnerabilidades y, sin embargo, algunas otras compañías de menor entidad adoptan posiciones mucho más proactivas en lo que a la gestión de la seguridad se refiere”, dice.

En todo caso lo que parece quedar claro es que queda camino por recorrer. Las herramientas están ahí, ¡úsenlas!

### Enlaces de interés...

- Análisis de riesgos en tiempo real, el papel de los escáneres de vulnerabilidades
- La nueva generación de ransomware ha llegado, ¿quieres conocerla?
- El coste de Wannacry supera los 4.000 millones de dólares

INTRODUCING

# CHECK POINT
# INFINITY

## THE CYBER SECURITY ARCHITECTURE OF THE FUTURE

CLOUD

MOBILE

THREAT PREVENTION

# El Valor de un SIEM

**Gestión y correlación de logs, eventos e información de seguridad, eso es lo que hace un SIEM. Es la capa de gestión imprescindible por encima de los sistemas y controles de seguridad. Capaz de conectar y unificar la información repartida entre los sistemas, analizarla y referenciarla desde una interfaz, las soluciones SIEM ayudan a realizar detecciones y respuestas ante amenazas más efectivas.**

Las soluciones SIEM, Security Information and Event Management, no son nuevas. Llevan en el mercado bastantes años y fueron desarrolladas con el objetivo de ayudar a las organizaciones en la detección temprana de ataques dirigidos y brechas de seguridad.

En los varios lustros que han pasado desde su aparición, las necesidades de seguridad de las empresas modernas han cambiado. Por una parte, el volumen y variedad de los datos ha crecido; por otra el malware antes estático y más predecible, se ha vuelto mucho más sofisticado, multi vector, y polimórfico.

¿Significa eso que los SIEM no valen frente a la situación actual? No. De hecho, son más necesarios que nunca. No sólo porque el número de amenazas crece, sino porque aún se tarda demasiado en detectar una brecha de seguridad.

Un informe de Technavio prevé que el mercado SIEM crecerá una media anual superior al 12% entre 2017 y 2021. Explica la consultora que los SIEM combinan las herramientas de gestión de la seguridad de la información (SIM - security information management), que son las encargadas de recopilar logs y generar reportes, con las herramientas de gestión de eventos de seguridad (SEM - security

## Las grandes empresas ya han adoptado solucioens SIEM, mientras que las pequeñas están optando por la prestación de un servicio de SIEM gestionado o de SOC-as-a-Service

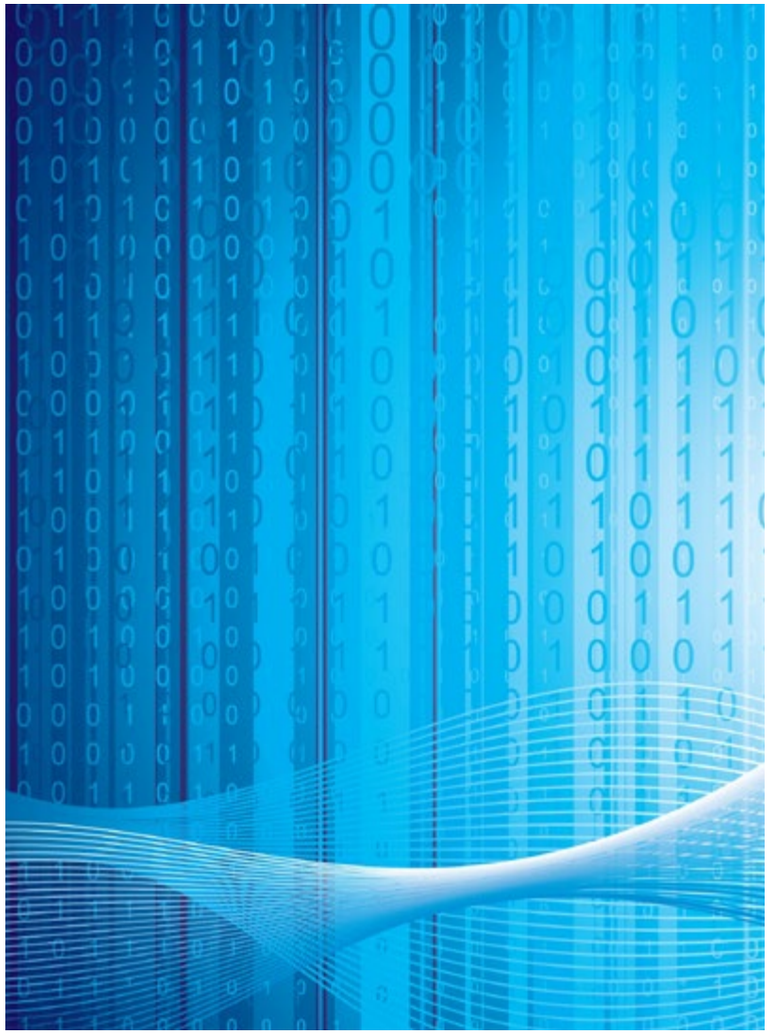
Eduardo Argüeso, Director de IBM Security en España, Portugal, Grecia e Israel

event management), centradas en analizar, correlacionar y alertar de eventos en tiempo real.

Convertidos en parte fundamental de las estrategias de seguridad modernas, los SIEM modernos han evolucionado para centralizar toda la actividad de red, para lo que incluyen capacidad para enviar alertas basadas en ajustes predefinidos, facilitar la auditoría y cumplimiento y tener la habilidad de mirar un dato en varios niveles de detalle. Por cierto que  aunque el objetivo de los SIEM no es el de satisfacer necesidades regulatorias específicas, es importante tener en cuenta que son capaces de recoger y analizar el tipo de dato que exigiría una auditoría.

**¿Cuál es el valor real de un SIEM?**

En opinión de Rafael Esteban, responsable de ventas para el Sur de Europa de LogRhythm, un SIEM funciona “como el sistema nervioso central de una organización”. Asegura el directivo que el enfoque tradicional de ciberseguridad ha sido utilizar una estrategia centrada en la prevención en-



focada en bloquear ataques, y que, si bien eso es importante, “muchos de los ataques y amenazas avanzados actuales están eludiendo las defensas basadas en el perímetro con ataques creativos, furtivos, selectivos y persistentes que a menudo pasan desapercibidos durante periodos de tiempo significativos”.

De forma que los SIEM, “ayudan a prevenir infracciones antes de que sucedan” gracias a una visión unificada de todas las amenazas, lo que permite detectarlas y neutralizarlas rápidamente. “Una solución SIEM verdaderamente efectiva sirve mucho más que para recopilar datos de registro y alarmas superficiales; ofrece a las organizaciones información valiosa sobre análisis avanzados, datos forenses y capacidades de respuesta a incidentes”, dice el ejecutivo de LogRhythm.

Para Joaquín Malo de Molina, BDM - Enterprise Security de Ireo, mayorista de Trustwave, el valor real de un SIEM es el de poder tener trazabilidad sobre las actividades de usuarios y de los diferentes sistemas y aplicaciones presentes en la red corpo-

## Qué tener en cuenta a la hora de escoger un SIEM

Considerando un SIEM como el sistema nervioso central en el que analizar alertas, realizar investigaciones, diseñar e implementar contramedidas y respaldar el análisis forense, Frost and Sullivan identifican cuatro factores críticos que hay que tener en cuenta a la hora de escoger el SIEM correcto.

VELOCIDAD

La velocidad a la que se pueden detectar e investigar alertas de seguridad, así como tomar contramedidas basadas en un incidente de seguridad para reducir su impacto en el negocio es un elemento crítico de un SIEM. El tiempo que transcurre entre el momento de la intrusión y hasta que el atacante ha comprometido el sistema es el tiempo en que los analistas deben realizar una serie de actividades para frenar el ataque.

PRODUCTIVIDAD

Con las alertas verificadas automáticamente, el analista de seguridad puede dedicarse a investigar y determinar la gravedad, urgencia, causa y las contramedidas a tomar.

Hay varios atributos que Frost y Sullivan recomienda para contribuir a la productividad de los analistas de seguridad: una interfaz de sistema unificada, flujo de trabajo intuitivo, desarrollo de scripts instantáneos y búsqueda rápida y precisa.

COLABORACIÓN

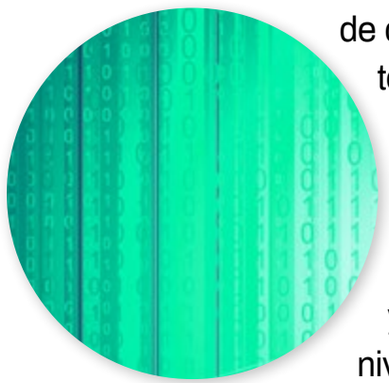
Aunque su trabajo sea crítico, los analistas no pueden hacer su trabajo de manera aislada. La gestión de riesgos La gestión del riesgo es un esfuerzo comunitario, y los flujos de trabajo colaborativos respaldados por el SIEM crean sinergias beneficiosas entre las entidades que tienen intereses creados.

Hay tres categorías de flujos de trabajo colaborativos que los SIEM deben soportar: flujos de trabajo entre analistas, supervisores y otras entidades con derechos.

MULTIPLES OBJETIVOS

Aunque el SIEM sea un instrumento importante para la herramienta de seguridad, no es su única función.

Una empresa puede necesitar un SIEM con capacidades adicionales para análisis forense de res, monitorización de endpoint, UEBA (User and Entity Behavioral Analytics) o respuesta ante incidentes. De forma que los SIEM de alto nivel deberían poder estar equipados con estos servicios adicionales.



rativa, con el fin de identificar posibles agujeros de seguridad y prevenirlos.

Nicola Esposito, director de Risk Advisory de Deloitte, dice que el valor de una solución SIEM varía en función de los objetivos y necesidades de las compañías, así como del nivel de madurez de la misma. Entre los objetivos menciona la centralización de la auditoria de los sistemas de seguridad, que obliga a construir un flujo de trabajo dentro de la compañía a la hora de provisionar los sistemas, ya que como parte del proceso de provisión es necesario la inclusión de la auditoria en el SIEM.

También se refiere el directivo al establecimiento de controles de seguridad básicos, ya que “casi todos los SIEM incluyen set de reglas por defecto que ayudan a obtener visibilidad de lo que ocurre en la red”, así como a introducir el concepto SOC en la compañía, “ya que las alertas deben ser tratadas en tiempo y forma”. Ahora bien, en empresas con un nivelo de madurez mayor “las soluciones SIEM

Es importante asumir este tipo de proyectos desde un ámbito global dentro de la empresa y no solo desde el Departamento de Seguridad

Nicola Esposito, Director de Risk Advisory de Deloitte

ayudan al apoyo del cumplimiento normativo como PCI DSS, SOX, LOPD, etc.”.

El valor real de un SIEM es, para Eduardo Argüeso, director de IBM Security en España, Portugal, Grecia e Israel, es el de “consolidar toda la información respecto a posibles incidentes que estás captando de las distintas plataformas de gestión específica de cada uno de los dominios que va a tener una empresa normalmente”. Habla el ejecutivo de Consolidar la información, así como Relacionar los distintos inputs que por sí solo pueden dar o no indicio de una posible amenaza o ataque, o al revés que por sí solas sí parece que sea un ataque pero en conjunción con otros inputs no.

En resumidas cuentas, los SIEM recopilan información de eventos que ayudan a las empresas a determinar lo que es una amenaza y lo que no, ayudando a reducir los falsos positivos.

**Configuración y mantenimiento**

Mientras que unos mencionan la configuración y mantenimiento de los SIEM como uno de los gran-

## Consecuencia de la GDPR veremos cómo la monitorización, la detección y la respuesta se convierten en un componente mucho más fundamental de la estrategia de ciberseguridad de una compañía

Rafael Esteban, Responsable de Ventas para el Sur de Europa de LogRhythm

des problemas de estas soluciones, para el responsable de Risk and Advisory de Deloitte se trata únicamente los conocimientos técnicos. “No se trata solo de un tema de configuración y mantenimientos, se trata de un de gobierno del proyecto”, asegura Nicola Esposito.

“Desde nuestro punto de vista y en base a la experiencia que tenemos, hemos comprobado que lo que penaliza este tipo de proyectos no son únicamente los conocimientos técnicos”, dice el directivo, añadiendo que es importante asumir este tipo de proyectos desde un ámbito global dentro de la empresa que terminan impactando y requiriendo apoyo de muchos departamentos, como el de comunicaciones, sistemas, recursos humanos o de ingeniería. “Es necesario que todos los actores tengan claras sus tareas y sobre todo que el alcance en las primeras interacciones esté ajustado al nivel de madurez de la empresa”.

Desde Ireo prefieren apuntar hacia la herramienta en sí cuando hablamos de configuración y mantenimiento de los SIEM como uno de los grandes problemas de estas soluciones. Y es que en realidad será la solución y su capacidad para tratar con la información que se pretende buscar, así como del grado de correlación que se desea con el fin de conectar eventos de distintas fuentes para ser alertado, de lo que dependerá la mayor o menos dificultad para trabajar con un SIEM. “El conocimiento por anticipado de estos aspectos pueden hacer más o menos sencilla la tarea de detectar agujeros de seguridad, a la par que el disponer de una herramienta con entorno gráfico intuitivo facilitará es tarea”, dice el mayorista de Trustwave.

En todo caso parece que la evolución de las propias herramientas SIEM han limado muchos problemas. Así lo considera el responsable de ventas para el Sur de Europa de LogRhythm al recordar que “tradicionalmente, la instalación de estas herramientas requería meses, además de la participación de un profesional cualificado para configurarlas. Ahora, las soluciones SIEM están completamente integradas con casi cualquier solución de software, lo que minimiza el esfuerzo de configuración, brinda mayor flexibilidad y reduce los costes de mantenimiento”.

De igual parecer es Eduardo Argüeso de IBM, quién recuerda que el mundo de los SIEM ha evolucionado a partir de sistemas de gestión de logs. “Un gestor de logs es una herramienta que permite gestionar grandes cantidades de información, pero por el contrario no suele estar preparado para hacer cosas más específicas de seguridad, como puede

## El valor de un SIEM es poder tener una trazabilidad de las actividades de los usuarios, sistemas y aplicaciones para identificar posibles agujeros de seguridad

Joaquín Malo de Molina, BDM - Enterprise Security de Ireo, mayorista de Trustwave

ser integrarse con fuentes específicas de seguridad, con sistemas de protección de entornos de seguridad, etc. No suele estar preparado para integrar directamente la información sobre vulnerabilidades que está disponible en este mundo, y tampoco para integrarse con la información de amenazas; e igualmente, no suele estar preparado de forma nativa para configurar reglas que permitan precisamente hace esa cualificación de los diferentes eventos o la distinta yuxtaposición de eventos en información sobre amenazas. Esa configuración reglas, si la tengo que hacer a mano, suele ser costosa".

Y habla el director de IBM Security de las herramientas que más que evolucionar, han nacido con "vocación de SIEM e incorporan esas capacidades de forma nativa". Se requiere la configuración de reglas, pero la transformación de esas reglas conceptuales en reglas físicas en el sistema es mucho más sencilla, porque la propia herramienta cuenta con una maquinaria de configuración y de despliegue de las mismas.

### Machine learning

El valor de un SIEM parece estar claro, así como que la evolución de este tipo de soluciones han impacto en una mayor facilidad de uso. Aun así, la cantidad de datos que hay que analizar, la propia evolución de las amenazas hace que estas herramientas sean costosas de manejar. Surge entonces la opción de una solución de monitorización de red animada por machine learning como sustituto del SIEM. Entre las ventajas, no tener que andar creando reglas.

Nuestros expertos están de acuerdo en el valor del machine learning, pero no como sustituto, sino como el perfecto complemento del SIEM. Y es que si bien las soluciones de monitorización de red con machine learning "están aportando mucho valor a la hora de detectar anomalías, no tienen un rol de orquestación como un SIEM", dice Nicolás Espósito, de Deloitte.

Para Rafael Esteban, de LogRhythm, aunque "la monitorización de la red con machine learning e inteligencia artificial es sin duda el futuro, SIEM todavía tiene un papel que desempeñar". Asegura el directivo que la abrumadora cantidad de alertas de seguridad que estas soluciones pueden generar a diario dificulta su capacidad de operar, pero que la aparición de soluciones de SIEM de última generación, que combinan aprendizaje automático, análisis de Big Data e inteligencia artificial "son una gran herramienta para ayudar a las organizaciones a mejorar la detección y la mitigación de los enormes volúmenes de amenazas que enfrentan actualmente".

Desde Ireo, mayorista de Trustwave, dicen que "las herramientas con machine learning ayudarán a una toma de decisiones más rápida o automatizada ante patrones de comportamiento anómalos en redes", aunque "el SIEM siempre tendrá su valor como repositorio general de eventos para realizar un análisis forense una vez producida la anomalía".

Igual que al resto de sus colegas, a Eduardo Argüeso, el machine learning le parece “una nueva capacidad que los SIEM pueden y deberían incorporar para ser más efectivos”. Sin embargo, el directivo va más allá, porque IBM está empezando a utilizar ya la Inteligencia artificial, “no para sustituir al analista, que siempre será el que tome la última decisión, pero como los analistas son escasos y parece que van a serlo cada día más, estamos viendo cómo podemos automatizar la parte del trabajo del analista que un sistema realmente inteligente pueda hacer”.

**Adopción del SIEM en España**

En España estamos “absolutamente al día” en lo que a adopción de SIEM se refiere, asegura Eduardo Argüeso. Cualquier gran empresa tiene ya un sistema SIEM funcionando desde hace años y las pequeñas empiezan a entender que “necesitan consolidar la información y analizarla de forma unificada y de forma correlada; lo que están optando muchas veces estas empresas más pequeñas es por la prestación de un servicio de managed SIEM o de SOC-as-a-service”.

Joaquín Malo de Molina, BDM - Enterprise Security de Ireo, mayorista de Trustwave, también está de acuerdo en que la adopción de soluciones SIEM en España es alta. Dice el directivo que “cada vez hay una preocupación mayor por los delitos de Ciberseguridad y que, además de medidas a nivel de protección perimetral y de End-Point, se requiere de herramientas que monitoricen/auditen las actividades dentro de la red para identificar posibles problemas”.

La adopción de este tipo de soluciones también se verá impulsada por normativas como la GDPR, la regulación sobre protección de datos que será de obligado cumplimiento a partir del 25 de mayo de 2018. A este respecto Rafael Esteban, de LogRythm. dice que como resultado de la implementación de la regulación GDPR de la UE, “veremos cómo la monitorización, la detección y la respuesta se convierten en un componente mucho más fundamental de la estrategia de ciberseguridad de una compañía. De hecho, las empresas requerirán un enfoque más coordinado y eficiente para la detección de amenazas que va más allá del simple despliegue de firewalls o antivirus”.

Para el portavoz de Ireo, “el hecho de que haya una normativa que obligue de forma estricta (con sanciones importante) a establecer procedimientos seguros de obtención y procesamiento de datos personales, obligará a las empresas a invertir en herramientas que les permite controlar las posibles actividades fraudulentas en relación con dichos datos”.

**Enlaces de interés...**

- W SIEM para principiantes
- W Gestión de seguridad Unificada vs SIEM, ¿quién da más?
- W Consideraciones para la creación de un SOC

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.

www.eset.es

ESET
ENJOY SAFER TECHNOLOGY™

# Por una Transformación Digital Segura

**Ahora que las compañías adoptan todo tipo de tecnologías, la seguridad debe ir por delante teniendo en cuenta que ya no se trata de proteger el perímetro de red, sino los datos a través de los sistemas, de los dispositivos y de la nube.**

No nos cansamos de hablar de Transformación Digital. Llevamos años haciéndolo. Hablamos sobre las ventajas de subir al cloud, de lo ventajoso que resulta pagar por lo que se consume en un modelo as-a-service, de lo conveniente que es poner al cliente en el centro de toda nuestra estrategia o de cómo la movilidad aumenta la productividad.

De lo que hablamos menos es de seguridad. De cómo adoptar la nube de manera segura, de mantener los datos de los clientes a salvo, estén donde estén, o de cómo es cada vez más necesario gestionar correctamente la cantidad y variedad de dispositivos que se conectan a nuestras redes para hacer de la Transformación Digital una realidad.

Todos estos aspectos y algunos más son los que abordaremos en el webinar en el que participan Eusebio Nieva, Director Técnico Check Point España y Portugal; David Sanz, EMEA Solutions Principal de Commvault; José de la Cruz, Director Técnico de Trend Micro España y Portugal; César Moro, Sales consultant de Quest Software; Bosco Espinosa de los Monteros, Preventa de Kaspersky Lab y Rubén Muñoz, Iberia Country Lead Security Advisory Services de DXC.

**Check Point Software**

Para Eusebio Nieva la Transformación Digital tiene que pensarse siempre con seguridad, porque no hacerlo así “sería añadir problemas”. Lo cierto es que hoy en día se pide que las tecnologías sean flexibles, adaptables y más rápidas, y teniendo en cuenta que todo está conectado, las medidas de seguridad son vitales.

Tenemos que proteger todas las plataformas de negocio, y no tenemos un perímetro por lo que los ataques están en cualquier punto, incluidos en los móviles que tienen una escala muchísimo mayor. “Es la hora de implementar un nuevo modelo de seguridad adaptado a nuevas tecnologías, como la nube”, explica el director técnico de Check Point

"La empresa española sí que tiene en cuenta la seguridad en un Proyecto de Transformación Digital, pero no forma parte de todo el proceso, sino que se ejecuta de forma paralela"

Rubén Muñoz, Iberia Country Lead Security Advisory Services de DXC

diciendo que a veces el cloud es un facilitador de la seguridad. Las políticas, dice también el directivo, deben ser dinámicas para incorporar nuevas soluciones y además centralizadas. "Proponemos un servicio capaz de escalar y gestionada de manera centralizada", dice Nieva.

Siendo la movilidad uno de los pilares de la Transformación Digital, es importante tener en cuenta a los móviles en las políticas de seguridad de las empresas. Dice Eusebio Nieva que los móviles son la nueva generación de amenazas y habla de smishing, de ataques por bluetooth y que se detectan mucho más tarde que los ataques tradicionales. Tomen nota, señores, porque "aunque los ataques de ransomware son una industria en sí mismos, se saca mucho más dinero de los ataques a móviles que del ransomware", dice.

¿Habrá más concienciación sobre la seguridad en 2018? "Yo creo que sí porque están aumentando el número de ataques, pero el problema es que nos olvidamos de todo demasiado rápido. Hay que concienciar a los usuarios".

**Commvault**

La Transformación Digital ha supuesto, en opinión de David Sanz, EMEA Solutions principal de Commvault, un giro hacia los datos; "vivimos en un mundo basado en datos, y las empresas quieren capturarlos, gestionarlos y protegerlos de la mejor manera".

Clave en este "tratar el dato como se merece", la propuesta de la compañía, experta en backup y recuperación, es una plataforma capaz de controlar los datos estén donde estén. Su misión es capturar los datos, deduplicarlos, comprimirlos e indexarlos, generando una enorme visibilidad y ofreciendo una capa de valor a disposición de los clientes.

Identifica David Sanz cuatro grandes retos a la hora de abordar una Transformación Digital. Por un lado, hacer que IT se alinee más con negocio; por otro lado, todo lo que tiene que ver con las ciberamenazas, y en particular las de tipo ransomware; luego están los retos de tipo normativo y por último la nube y la movilidad

¿Qué nos reclama el negocio? Continuidad. A pesar de ellos un tercio de nuestros servidores

"GDPR es una normativa que ha traído un nuevo paradigma a la privacidad de los datos personales porque lo que dice es que el dueño de los datos es el ciudadano"

David Sanz, EMEA Solutions principal de Commvault

tiene una tolerancia de paradas o pérdida de datos inferior a 15 minutos otros tercio una tolerancia de entre 15 minutos y dos horas, y sólo un 14% de los servidores a nivel mundial tiene una tolerancia de más de seis horas, que es lo que nos da un backup tradicional, explica David Sanz en el Webinar.

El directivo se apresura a aclarar que eso no significa que el backup no valga, sino que hay que dar un paso más y establecer puntos de recuperación, o snapshots "pare reducir el intervalo de recuperación a horas, e incluso minutos".


POR UNA TRANSFORMACIÓN DIGITAL SEGURA

CLICAR PARA VER EL VÍDEO

De cara al reto de las amenazas de seguridad, dice David Sanz que hay que entender las fases de una brecha de seguridad: Prevención, detección y recuperación. Mientras que en la primera fase inicial de prevención juegan los proveedores de seguridad clásicos, y es lógico contar con un plan de recuperación en el que juega un papel importante contar con una copia de seguridad, "la fase de detección es crítica para poder reducir el impacto". Y aunque Commvault no es una empresa de seguridad clásica, "somos capaces de detectar anomalías" que dan la voz de alarma.

El reto normativo que mencionaba al comienzo de su ponencia el directivo de Commvault le lleva a hablar de GDPR, una normativa "que ha traído un nuevo paradigma a la privacidad de los datos personales porque lo que dice es que el dueño de los datos es el ciudadano". De nuevo habla David Snaz de visibilidad de los datos, la que tienen que tener las empresas si un usuario quiere ejercer su derecho al olvido. Que la plataforma de Commvault sea capaz de indexar los datos, estructurados o no, con un motor de búsqueda muy similar a los buscadores de Internet "nos permite buscar lo que queramos, cualquier tipo de datos".

En cuanto al cloud y la movilidad, dice el directivo de Commvault que "el dato puede estar donde queramos, pero es conveniente que el control lo tengamos nosotros" y explica que la plataforma de la compañía permite hacer backup de la nube, en la nube y desde la nube, utilizarla como un datacenter de recuperación de desastres o para la portabilidad de cargas…, "al final se trata de darle libertad al cliente".

Y con respecto a la movilidad, "no es más que la demanda de los usuarios de acceder a sus datos desde donde quieran". Y eso es también lo que hace la plataforma de Commvault, una plataforma abierta "que permite el acceso al dato de forma segura integrado en las capacidades de identidades de la compañía", de forma que el usuario pueda acceder con sus credenciales desde un móvil o un navegador y consultar sus datos, descargárselo, compartirlo, analizarlo, etc. "Fomentamos la movilidad controlando el dato corporativo y creemos mucho en el modelo autoservicio, y así las empresas pueden adoptar la movilidad", dice David Sanz.

"Queremos hacer una Transformación Digital y tenemos que hacerla con la seguridad imbuida, porque hay agujeros de seguridad difícilmente subsanables"

Bosco Espinosa de los Monteros, Preventa de Kaspersky Lab

**Trend Micro**

Para José de la Cruz, Director Técnico de Trend Micro, la Transformación Digital consiste en la incorporación de nuevas tecnologías para mejorar la eficiencia o la rentabilidad, y las tres grandes áreas en que más influencia está teniendo la Transformación Digital son el cloud, la movilidad y la conectividad

Explica el directivo que, desde un punto de vista de ciberseguridad, si nos vamos diez o quince años atrás, nos encontramos con que anteriormente recibíamos un fichero que podía tener dos estados: legítimo y bueno o ilegítimo y peligroso, "y ante esta situación los fabricantes intentábamos lanzar cuanto antes una firma que bloqueaba la amenaza", dice José de la Cruz. Ahora existe un nuevo tipo de amenaza que es el fichero desconocido, que puede estar relacionado con un ataque de día cero, con el BEC, un ransomware… es decir algo que no tenemos la certeza de que sea bueno, pero no podemos descartar que sea malo.

Ante esta nueva situación que José de la Cruz califica de "híbrida" se necesita una solución adaptable y estratégica. La propuesta de Trend Micro es una solución multicapa basada en más de 25 años de historia. Además de multicapa, la propuesta de la compañía es "seguridad conectada", porque según José de la cruz, "es importante proteger todos y cada uno de los vectores de entrada de una empresa, desde el endoint al correo, y nosotros disponemos de soluciones para cada uno de estos ámbitos y distribuimos estas soluciones en tres grandes áreas", que son el endpoint, el cloud y la red, proporcionando algo que Trend Micro considera muy importante: la visibilidad, "saber lo que está ocurriendo en nuestras redes". Además, la compañía cuenta con soluciones para el ámbito industrial.

"Cuando iniciaba mi presentación hablaba de la importante que tenía la transición a la nube", recuerda José de la Cruz. Explica el directivo que sea del tipo que sea -privada, pública o híbrida, lo que tenemos es lo mismo: Datos, aplicaciones, sistemas y redes, y añade que Trend Micro tiene una propuesta específica que es para proteger el entorno de servidor, que es Deep Security, una solución modular que incorpora protección antimalware con características de machine learning, análisis de comportamiento o reputación web; así como monitorización del directorio y que el contenido no sea modificado sin permiso; supervisión de logs que nos permite ver qué es lo que está ocurriendo en nuestro entorno y detectar eventos sospechosos, así como un control de aplicaciones que permite bloquear una máquina para que sólo se ejecuten procesos permitidos.

Por último, la parte de protección de red, que para José de la Cruz es "la parte estrella de este producto" porque junto con un módulo de firewall a nivel de host muy interesante o un módulo IPS, "tiene la capacidad de aplicar políticas de parcheado virtual".

Recuerda el director técnico de Trend Micro que Wannacry "puso de manifiesto que el parchado tradicional es ineficiente" y que una estrategia más rápida a la hora de parchear es el parcheado virtual. A las pocas horas de conocerse la vulnerabilidad Trend Micro genera un parche virtual que consiste en una regla que se aplica en el endpoint para detectar el comportamiento asociado a esa vulnerabilidad.

José de la Cruz cierra su ponencia hablando de software-as-a-service, y de propuestas para añadir una capa de seguridad a Office 365, Box, Dropbox, etc.

"La evaluación continua nos podría dar respuesta a quién ha accedido a qué y de qué manera, lo que nos permite saber quién tiene permisos y qué sistemas son vulnerables"

César Moro, Sales Consultant de Quest Software


**Quest**

César Moro, Sales consultant de Quest Software, iniciaba su ponencia en este webinar Por una Transformación Digital Segura explicando que muchas empresas que se mueven a la nube lo hacen por reducir costes, dar la posibilidad de operar libremente desde cualquier dispositivo, además incrementar la escalabilidad y continuidad de negocio.

En los entornos Microsoft, las empresas se mueven hacia Office 365 y hacia Azure, pero muchas empresas apuestan por entornos híbridos "porque es difícil abandonar el legacy". Explica César Moro que el 90% de las compañías tienen entornos de directorio activo on-premise, al tiempo que mantienen ratios de adopción de la nube del 70%, y estas compañías se encuentran con el reto de que tienen que sincronizar esos usuarios. El reto, asegura el directivo de Quest, "está en cubrir los entornos de directorio activo híbridos".

Los entornos híbridos amplían la superficie de ataque y por tanto también es un reto saber si se producen filtraciones de datos, a lo que se unen los problemas de cumplimiento normativo, o de la propia continuidad de negocio. Pero las empresas también se enfrentan a retos técnicos, explica César Moro, haciendo referencia al hecho de contar con una línea base de permisos establecidos dentro de nuestra organización que tenga en cuenta quién accede, a qué, cómo se estructuran los grupos de dan permisos. "La auditoría es clave", asegura el directivo de Quest, porque nos va a permitir hacer un análisis forense en cado de problemas.

Las diferentes propuestas de Quest Software permite establecer un ciclo desde la evaluación continua de la información y poder conocer y alertar en tiempo real de lo que está ocurriendo con esa auditoría detallada; remediar y mitigar cuando se detectan problemas y finalmente poder investigar y recuperar.

Esa evaluación continua nos podría dar respuesta a quién ha accedido a qué y de qué manera, lo que nos permite saber quién tiene permisos y qué sistemas son vulnerables. "En la parte de detección y alertas lo que intentamos es ser reactivos con una auditoría detallada, que nos va a dar información sobre quién está accediendo a un determinado documento en tiempo real, saber si alguien hizo algo crítico o ha accedido al buzón del correo del director", explica César Moro, añadiendo que saber lo que pasa en mi entorno y poder detectar un ataque interno es crítico.

La parte de remediación y mitigación requiere ir un paso más allá y permite, por ejemplo, limitar los permisos, establecer un rollback para que nadie tenga permisos en exceso. Y la investigación y recuperación es lo último. "En lugar de días nosotros podemos hacer que dure un par de horas. Y cuando ves que tu parada es de dos horas en lugar de cuatro días, el retorno de la inversión no se puede rebatir", asegura César Moro.

**Kaspersky Lab**

La empresa Española no está teniendo en cuenta la seguridad cuando aborda un proyecto de Transformación Digital, "lo están viendo como una

"Es hora de implementar un nuevo modelo de seguridad adaptado a nuevas tecnologías, como la nube"

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

segunda fase, y creemos que un proyecto de esta envergadura debería ir imbuida la seguridad", dice Bosco Espinosa de los Monteros, preventa de Kasperky Lab.

Recomienda el directivo de la empresa de seguridad que primero debe hacerse un estudio de lo que hay que hacer, y no "embarcarnos en un proyecto todo de golpe sino saber dónde queremos llegar, las necesidades que tenemos y saber que si digitalizamos todo estamos ampliando los posibles vectores de ataque y por tanto tenemos que securizar muchos más puntos".

Hace unos años cuando se hablaba de seguridad, se hablaba de un perímetro, que desapareció con los móviles y las tabletas. Pero ahora los usuarios pueden acceder a nuestra información siempre que quieran y desde donde quieran, y eso requiere un minucioso control del dato, esté donde esté.

Explica Bosco Espinosa de los Monteros que los datos se mueven y que la movilidad hace que tengamos que saber quién accede y desde dónde. "Tenemos que saber lo que está ocurriendo dentro de nuestra red y tenemos que saber responder antes un ataque", explica el directivo de Kaspersky. Y tan importante es saber lo que está ocurriendo dentro de nuestra red como tener un plan de seguridad y un plan de respuesta que esté preparado y probado.

Con la evolución de la industria, con la Transformación Digital, llegan también nuevas tecnologías que ayudan a tener todo bajo cierto control como son las soluciones de Endpoint Detection and Response. "La posibilidad de que automáticamente seamos capaces de hacer rollback a las acciones que haga el malware, ya sea que me ha levantado un servicio, que se haya conectado a una página web china, etc." Cobren mucha importancia hoy día. Y añade Bosco Espinosa de los Monteros que cuanto más automático todo mejor, "porque hoy en día los recursos que tienen las empresas son limitados".

También habla el directivo de Kaspersky de predicción, de saber lo que puede ocurrir, saber qué agujeros de seguridad tengo en mi red mediante un pentesting. "Queremos hacer una transformación digital y tenemos que hacerla con la seguridad imbuida, porque hay agujeros de seguridad difícilmente subsanables", concluye Bosco Espinosa de los Monteros.

**DXC**

Para Rubén Muñoz, Iberia Country Lead Security Advisory Services de DXC, la empresa española sí que tiene en cuenta la seguridad en un Proyecto de Transformación Digital, "pero no forma parte de todo el proceso, sino que se ejecuta de forma paralela".

Entiende DXC la transformación Digital como un proceso que se apoya en cinco pilares: Applications, Cloud, Workplace, Analytis y Security. "Una Transformación Digital se produce en un contexto en el que todos estos pilares se entremezclan para llevar a la empresa a una nueva dimensión, a una nueva esencia", explica el directivo de DXC

En la parte de seguridad hay que tener en cuenta que el panorama de amenazas ha cambiado, que el perímetro ha desaparecido, que el tiempo medio de detección de una brecha es de 99 días que el tiempo de respuesta puede alcanzar los 46 días…

"Wannacry puso de manifiesto que el parchado tradicional es ineficiente, y que una estrategia más rápida a la hora de parchear es el parcheado virtual"

José de la Cruz, director técnico de Trend Micro

el panorama obliga a contar con un departamento de seguridad con conocimientos específicos adaptados a este nuevo entorno.

Explica Rubén Muñoz que el grupo de seguridad de DXC ha detectado que se debe tener en cuenta temas de cumplimiento normativo, inteligencia de seguridad para detectar anomalías, gestión del riesgo, de las vulnerabilidades y de los accesos e identidades, sin olvidar la infraestructura de seguridad clásica. No se olvida el directivo de DXC de mencionar la protección de la privacidad del dato, que está totalmente asociado a GDPR y la fuga de información, así como el cifrado de datos; "pasaríamos por un plano que sería la gestión de identidades hasta lo que sería la implantación tecnológica y salvaguarda de esas identidades y luego pasaríamos a un área específica de seguridad cloud, en el que nos centramos en ese control, de acceso a las aplicaciones y controlar lo que pasa en la nube".

Explica a continuación Rubén Muñoz en estas siete áreas de conocimiento "hemos diseñado el arte de seguridad de DXC", y que estas áreas de conocimiento se ven correspondidas por un conjunto de capacidades que se reúnen en tres pilares: Consultoría, Tecnología y Servicios Gestionados.

Uno de los valores añadidos de DXC en cuanto a servicios gestionados "es que tenemos una capacidad dual local", y explica Rubén Muñoz que DXC es una empresa internacional que cuenta con una dualidad de SOC Global Regional. La compañía cuenta con cinco SOC globales y al mismo tiempo centros regionales que dan soporte a empresas locales.

"Por ejemplo nuestro SOC en Madrid cubre España y Portugal. Tengo un SOC para ofrecer servicios gestionados By Design, que me permite adaptarme a las necesidades locales pero sin perder esa capa global que nos va a proveer de inteligencia a nivel global. Y eso nos da un potencial que hoy en día en el mercado no abunda mucho".

Y así es como DXC ha orientado su área de seguridad para acompañar esa transformación digital y hacerla segura, explica Rubén Muñoz.

Concluye el directivo que la mayoría de las Transformaciones Digitales que se están viendo están tratando la seguridad de manera paralela; "es una manera de hacerlo, pero en DXC no pensamos que sea la manera correcta y por eso hemos montado todas estas capacidades".

**Compartir en RRSS**

**Enlaces de interés...**

- Nueve buenas prácticas para la seguridad del directorio activo
- Bad Bot Report
- Gestión de accesos con privilegios
- Cómo conseguir el mejor ADC para la Transformación Digital
- La Transformación Digital abre nuevas posibilidades a la economía del cibercrimen
- Sin seguridad, imposible avanzar en Transformación Digital

# NUEVO.
# PERO NO NACIDO AYER.

**CSC Y HPE ENTERPRISE SERVICES AHORA SON DXC TECHNOLOGY.**

**DXC.technology/GetItDone**

DXC.technology | THRIVE ON CHANGE.

# Recuperación ante desastres, ¿estás preparado?

**Parece obvio pensar que las empresas tienen planes de backup, disaster recovery y continuidad de negocio. Pero lo obvio deja de serlo cuando un informe tras otro indica que la mayoría de los responsables de TI no están seguros de la habilidad de sus organizaciones para recuperarse de una incidencia o un ataque.**

Si algo hay que agradecerle al ransomware es poner de manifiesto, con su éxito imparable, que las empresas no cuentan con una copia de seguridad adecuada. Falta de soporte, bajos presupuestos o que el retorno de la inversión no es inmediato, están detrás del problema.

La empresa española, ¿adopta políticas de backup y recuperación? ¿Qué aportan los modelos as-a-service? ¿Cómo impacta el cloud o la vitualización en los procesos de Backup y Disaster Recovery? ¿Qué impacto tendrá el IoT? ¿y la GDPR?

Estas y otras preguntas se han planteado en un desayuno en el que han participado César Moro, Consultor preventa de Quest Software; Bosco Espinosa de los Monteros, consultor preventa de Kaspersky Lab; Eusebio Nieva, Director Técnico de Check Point para España y Portugal; y Mario Muñoz, EMEA South Region DPP Lead de DXC.

Para César Moro, la implantación de políticas de backup y recuperación depende de muchas cosas. A veces es no contar con los conocimientos o ganas de incorporarse a la tecnología, a veces se trata de un tema de costes y también hay dejadez.

Para Bosco Espinosa de los Monteros, en la gran cuenta a nadie se le ocurre decir que no tiene una política backup y recuperación, “otra cosa es que luego a alguien se le ocurra comprobar que funciona”. Respecto a la pyme coincidía el directivo que la implantación es menor por desconocimiento y a veces hasta despreocupación; “hay gente que piensa que al tener cloud ya tiene una copia de seguridad, que al sincronizar mis datos ya lo tengo todo hecho. Hay que decirles que eso no es válido porque si sufro un ransomware se te va a sincronizar todo automáticamente, y por tanto queda todo cifrado y es imposible de recuperar”.

Eusebio Nieva mantiene la línea de que las grandes empresas suelen tener los dispositivos y sistemas muy profesionalizados, pero con matices, porque si bien a veces se tienen controlado el tiempo que se tarda en hacer un backup, “nadie se ha preocupado de dimensionar cuánto voy a tardar en

"No hay ninguna gran compañía que se pueda permitir una parada de negocio o una recuperación no correcta de su directorio activo"

César Moro, Consultor preventa de Quest Software

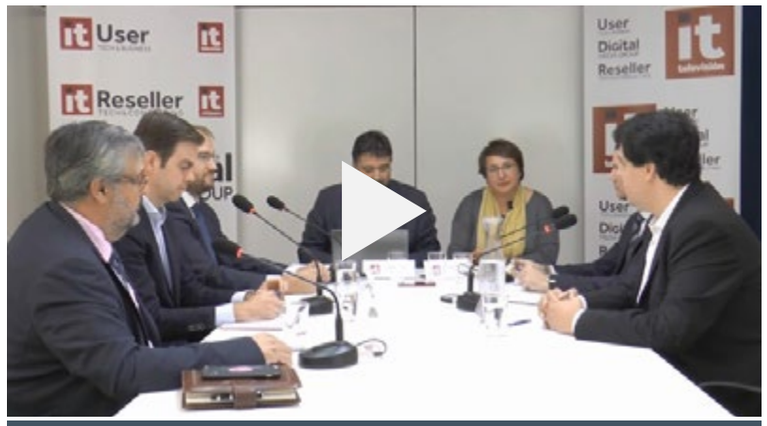
hacer el 'restore'. A veces tardas tres días es hacer el backup de un día, y eso es que algo va mal".

Mario Muñoz coincide, y asegura que, en teoría, en las grandes empresas está todo muy definido, "pero en cuanto llega la hora de la verdad y hay un problema, o una infección de ransomware, o hay que volver a recuperar datos, o máquinas, o sistemas operativos, te das cuenta de que los tiempos no corresponden con lo que se plantificó, que los datos no están o son versiones obsoletas… y cuesta bastante dejarlo todo como estaba". Añade el directivo de DXC el reto que supone hacer un backup correcto del directorio activo y apunta que a veces en la pequeña y mediana se utilizan herramientas o servicios en la nube que te hace copia de lo bueno, y también de lo malo, y no puedes ir hacia atrás.

César Moro, Consultor preventa de Quest Software, recogía el guante sobre la recuperación del directorio activo al contar su compañía con una solución que lo permite, y coincidía con Eusebio en que el tiempo de recuperación es clave porque "no hay ninguna gran compañía que se pueda permitir una parada de negocio o una recuperación no correcta de su directorio activo. Ahí es donde estoy viendo que muchas empresas sí que están apostando por tener no sólo las soluciones de backup sino las de restauración".

**Backup y Disaster Recovery como servicio**

Las propuestas as-a-service facilitan la adopción de soluciones de copia de seguridad y recuperación. Pero el directivo de Kaspersky ve un 'gap', "porque cuando hablamos de backup y de recuperación de datos, vamos a hablar de recuperación ante desastres, y no podemos recuperarlo así como así. Si hemos tenido una brecha de seguridad quizá debamos también investigar qué es lo que ha ocurrido, porque lo podemos recuperar, pero mañana va a volver a pasar, y si no mañana, dentro de dos meses". Es decir que no sólo hay que hablar de esas herramientas de backup y recuperación, sino de saber qué es lo que pasa por nuestra red.




RECUPERACIÓN ANTE DESASTRES, ¿ESTÁS PREPARADO? CLICAR PARA VER EL VÍDEO

Para César Moro ofrecer el backup o la recuperación como servicio "va a facilitar mucho que la pyme sean más conscientes de poder utilizar este tipo de soluciones, sobre todo por precio".

"El factor humano también es un coste", apuntaba Eusebio Nieva. "A veces te pones en la piel de un pequeño empresario y, dependiendo de qué sistemas… Hay que hacer un análisis que no se hace. No se trata de backup para todo, a lo mejor no hace falta. Se tiene que hacer un análisis previo de qué es lo que quiero hacer y las ofertas de tipo nube facilitan mucho este ejercicio".

Mario Muñoz, EMEA South Region DPP Lead de DXC, coincidía en que el modelo as-a-aservice

# "En la gran cuenta la adopción de backup y recuperación está madura. Otra cosa es que luego a alguien se le ocurra comprobar que funciona"

Bosco Espinosa de los Monteros, Consultor preventa de Kaspersky Lab

permite a las pequeñas empresas ocuparse de estas necesidades de una manera fácil, sencilla y con menos coste de una grande, pero al mismo tiempo puede generar un problema "que se desentienden de todo y creen que este servicio lo dejan configurado y se pueden olvidar. Y volvemos a lo de siempre, no hacen pruebas y no comprueban". Y añadía, como recordatorio, que a lo mejor se les está pidiendo que inviertan en el backup cuando lo que es la base, como la seguridad en el endpoint no lo tienen".

Apuntaba el ejecutivo de Quest que cuando pensamos en backup, pensamos más en la protección del dato como tal, pero que la oferta está yendo hacia el backup y restauración de dato, aplicación y servicio.

En todo caso, el servicio también hay que saber contratarlo correctamente. Y es que según Bosco Espinosa de los Monteros, "el servicio puede ser backup pero tienes que restaurarlo tú. Hay muchos tipos de servicios y en el cloud no hay costes ocultos siempre y cuando te leas bien el contrato. Hay que buscar al proveedor adecuado, y si hay algo que cuesta menos es porque hay algo que te estarán haciendo de menos".

"Yo creo que en algunas grandes empresas estamos ante el síndrome del checkbox y no se va más allá, no se comprueba si el backup funciona cada cierto tiempo", decía Eusebio Nieva, añadiendo que tampoco se comprueba "si el datacenter de respaldo se actualizad veinte días después de que se actualice el primario; si los sistemas de alta disponibilidad se han probado". Se necesita un procedimiento a seguir en caso de desastre, porque se puede tener un backup, pero cuando ocurre algo se tiene que saber qué hacer; "cada cosa tiene su forma de trabajar y si no tienes procedimientos tienes un problema".

El ejemplo a seguir es el de una empresa cuyo nombre permanece en el anonimato que cuenta con un procedimiento en el que cada N meses su centro de respaldo se convierte en su centro activo. Cuanta con dos CPD completamente espejados, y el primero deja de ser el primario para ser el segundo. "Siempre saben que van a poder volver de un lado a otro", explica Nieva.

César Moro apunta que es bueno tener un procedimiento, siempre y cuando se pruebe, algo que realizan menos del 50% de las empresas.

Cloud y virtualización

Las tecnologías cambian, las herramientas se modifican, las necesidades evolucionan. Hace unos años tener un backup en un disco duro conectado a la red era una opción razonable, pero eso ahora ha dejado de serlo con el ransomware. Los desastres cambian, tienen orígenes diferentes, y tu sistema se tiene que adaptar a ello.

Cuando hablamos de backup y recuperación, ahora hay que hacer frente a la movilidad y los servicios cloud, a la deslocalización de los datos, a la virtualización.

Los retos, la situación, es más compleja. "Sí, pero el tema de la virtualización, por ejemplo, está facilitando las soluciones", aseguraba César Moro. La

"El procedimiento es fundamental porque puedes tener tu backup, pero cuando ocurre algo hay que saber qué se tiene que hacer"

Eusebio Nieva,

Director Técnico de Check Point

propia evolución hace que ya no sólo se hable de protección o backup del dato, sino del aplicativo y del servicio, algo que se facilita mucho más con la virtualización; incluso subir al cloud también puede reducir el coste de almacenamiento. Quest ya cuenta con soluciones encargadas de todo el tema de virtualización, que con un click te recuperan todo un entorno virtualizado, y lo mismo en cuanto al cloud. "El almacenamiento está siendo más barato y ya empezamos a encontrarnos empresas que empiezan a almacenar una parte en el cloud. Lo que sí es cierto es que nos encontramos mucha diversidad y que las empresas no se atan a una única tecnología", decía el ejecutivo durante el encuentro.

Mario Muñoz apuntaba el tema de la localización, de dónde están localizados los servidores donde se realiza el backup, "porque dependiendo de las empresas, de las políticas que tengan, el CPD tiene que estar en territorio nacional, o en Europa, o fuera, etc. Ese es otro caso que hay que tener en cuenta".

En todo caso parece que lo imprescindible es realizar un análisis previo, porque no es lo mismo una gran cuenta que una pequeña, tienen diferentes necesidades. Repetía Eusebio Nieva que "a algunos les vale con hacer un backup del dato y otros que necesitan una implementación muy diferente. La tecnología en la nube está ayudando, pero también ha habido una evolución de la tecnología en función de la necesidad del servicio".

Bosco Espinosa de los Monteros rompía una lanza a favor de la seguridad, porque lo cierto es que "está muy bien tener unas herramientas de recuperación, pero lo principal creo que para todas las empresas es no tener que utilizarlo nunca, a poder ser. Yo invierto lo que haga falta, pero para no utilizarlo. Y por eso es difícil defender esos presupuestos".

Para César Moro "el backup es un seguro de vida. Nosotros siempre ponemos el ejemplo de un airbag; nadie quiere utilizarlo, pero nadie se plantea ahora mismo ir al concesionario a pedir que se lo quiten".

**Backup y recuperación integrados**

Se planteaba a continuación durante el desayuno si el backup y la recuperación deberían trabajar de manera conjunta e de manera integrada. La posición no es clara, y según César Moro depende mucho del servicio y del tipo de aplicación o dato que se quiera recuperar. "Nosotros por ejemplo tenemos muchas herramientas de recuperación que no se casan con un backup, somos agnósticos. Y luego tenemos soluciones de backup y restauración. ¿Qué es lo mejor?, pues básicamente depende del escenario del cliente".

Eusebio. Hay muchas herramientas de backup que tienen la herramienta de recuperación asociado, que es importante, pero sigo insistiendo en que hay que hacer un análisis previo y en base a eso te saldrá los productos y capacidades que debes tener.

Para Eusebio Nieva, de CheckPoint, la clave está en el procedimiento; "hay muchas herramientas de backup que tienen la herramienta de recuperación asociado. Pero sigo insistiendo en que hay que hacer un análisis previo, y en base a eso te saldrá los productos y capacidades que debes tener".

La integración de backup y recuperación en una misma herramienta, también es cuestionable para

Mario Muñoz. Según explicaba el ejecutivo, una cosa está asociada a la otra, pero independientemente también son importantes. Planteaba además que a veces se quieren hacer cosas sencillas, como una recuperación de un NAS, y resulta que está asociado a un procedimiento que exige una recuperación del sistema complejo; “hay que pensar qué se quiere hacer; tener en cuenta caídas parciales del servicio, o no…”.

**Internet de las Cosas, Backup y Recuperación**

Se planteaba también durante el encuentro si el IoT tendrá un impacto en lo que a backup y recuperación se refiere. “Tendrá un impacto en el volumen de lo que tengas que almacenar”, aseguraba Bosco Espinosa de los Monteros, Consultor preventa de Kaspersky, pero además, y teniendo en cuenta que los datos del IoT se reportan, y a veces consumen, en tiempo real, lo mismo ya no vale con hacer un backup una vez a la semana, o al mes. “Hay que pensar en herramientas flexibles, mayor sensibilización y mayor rapidez a la hora de determinar qué quiero recuperar y cuándo, en tiempo real”.

“No sé si el Iot lo complica, pero lo hace más interesante”, aseguraba el ejecuto de Kaspersky antes de Eusebio Nieva planteara que cuando se habla de IoT el backup no está tanto en el dato como en el servicio, y que hay que aplicar tecnologías de recuperación ante desastres en tiempo real.

El foco que en DXC están haciendo en relación con el IoT está relacionado con los dispositivos móviles, explicaba Mario Muñoz. “La gente suele hacer uso personal de dispositivos profesionales y además de los datos que se pueden perder, también hay que hacer foco en controlar lo que se ejecuta en los dispositivos fuera de lo que es el entorno cerrado de una empresa, y que la gente pueda hacer un uso más libre de ellos”.

Para César Moro el IoT está más relacionado con el Big Data, “y lo único que se me ocurre en el futuro es que nos vayamos encontrando situaciones en las que a lo mejor sí que sea necesario una recuperación del sistema y tengamos que hacer una recuperación de la propia configuración del dispositivo. Que al final tengamos tantos dispositivos que sea necesario hacer un backup de esos dispositivos, y tendríamos que empezar a trabajar o tener otras soluciones que permitan, en caliente, recuperar desde el sensor al dispositivo móvil con soluciones de endpoint management o lo que sea”.

"El backup y recuperación como servicio permite a las pequeñas empresas desentenderse de una manera fácil, sencilla y con menos coste"

Mario Muñoz, EMEA South Region DPP Lead de DXC

“No es recuperar físicamente el sensor, sino la tecnología que hace funcionar el sensor, lo que se llama proyectos en PLC, llámalo BIOS, software. Otro problema grande es la problemática que tenemos a nivel de seguridad y a nivel de estándares”, apunta Bosco Espinosa de los Monteros.

**Propuesta**

Para concluir pedimos a los participantes del desayuno que plantee lo que cada una de sus empresa propone de cara a la necesidad de contar con una política de backup y recuperación.

Quest Software cuenta con una línea de Data Protection donde hay soluciones de almacenamiento en la nube, entornos en virtualización o on-premise. Relacionado con el directorio activo, la compañía cuenta con una herramienta, que César Moro asegura


## Enlaces de interés...

- Las seis principales obligaciones que hay que cumplir con GDPR
- Nueve buenas prácticas para la seguridad del directorio activo
- Por qué la protección del dato es clave en los programas de seguridad modernos
- Guía para la prevención de amenazas móviles

que es la única en el mercado que permite recuperar el entorno ante cualquier desastre. “Hay muchas empresas que la están adoptando este tipo de soluciones porque no se pueden permitir una parada de días para recuperar su entorno de directorio activo. Y cuando comparas días con horas, y el RI está compensando. Ese tipo de soluciones es lo más puntero del mercado y es donde estamos haciendo mucho foco”, aseguraba el ejecutivo de Quest.

Lógicamente Kaspersky habla de protección del dato, pero añadiendo el poder saber lo que ha ocurrido y por qué ha ocurrido ese desastre. Bosco Espinosa de los Monteros planteaba por tanto un producto para poder comprobar incluso amenazas desconocidas y ataques dirigidos, y por otro lado servicios de investigación ante incidentes de seguridad y incluso análisis forense.

Para Eusebio Nieva lo fundamental es que “nuestros clientes al menos desde el punto de vista de seguridad no necesitaran un backup. Y luego si te ha ocurrido saber y analizar qué es lo que ha ocurrido. Pero lo principal es eso, que no ocurra”. Insiste el director técnico de Check Point que se realicen análisis, que el backup o la recuperación respondan a las necesidades del negocio, que se adapten los métodos y los procedimientos a lo que necesitas y que no se deje en un cajón, hay que estar comprobando.

Para Mario Muñoz, lo bueno de DXC es que “al ser una empresa de consultoría y seguridad global somos agnósticos en software y analizamos en cada cliente qué es lo que mejor le vendría dependiendo de sus necesidades. Abarcamos todo el mercado, cada cliente es diferente para nosotros y analizando cómo es cada uno de ellos y las necesidades concretas que tiene. Podemos ofrecerles diferentes servicios y combinaciones de varios”.

# 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

# Ataques DDoS, del pánico al reto

**El ataque de denegación de servicio distribuido es una de las actividades delictivas más antiguas de la web. Sin embargo, a pesar de su edad, los ataques DDoS han resistido los años sorprendentemente bien. La razón de esto es bastante simple: aunque en su núcleo, cada ataque DDoS hace lo mismo, han evolucionado significativamente en las últimas décadas**

Desde que los primeros ataques de Denegación de Servicio, DoS, empezaron a funcionar fuera de entornos de investigación en la década de los '90, los ataques de Denegación de Servicio Distribuido, o DDoS, se han convertido en un arma común entre los ciberdelincuentes. Este tipo de ataques han sido utilizados contra empresas y organismos gubernamentales porque son una manera efectiva de interrumpir servicios con un coste reducido y bajos requerimientos. En un mundo cloud basado en servicios, se han convertido en una verdadera amenaza para la que muchas empresas no están preparadas.

Parece haber consenso en que el primer ataque DDoS ocurrió en 1999 contra la Universidad de Minnesota. Afectó a 227 sistemas y dejó fuera de servicio los servidores de la universidad durante varios días. Los atacantes utilizaron una herramienta llamada Trinoo consistente en una red de máquinas comprometidas a las que se enviaban instrucciones para lanzar el ataque; la dirección IP de las mismas no estaba oculta y cuando se contactó con los dueños de las máquinas afectadas estos no tenían ni idea de que


**CÓMO FUNCIONAN LOS ATAQUES DDOS QUE PUEDEN DESTRUIR INTERNET**

**CLICAR PARA VER EL VÍDEO**

sus sistemas habían sido utilizados para lanzar un ataque.

Otras herramientas utilizadas en los primeros días de esta plaga fueron Stacheldraht, que ya podía actualizarse de manera remota y que incorporaba la suplantación de la IP, junto con Shaft y Omega, que podían recopilar estadísticas de los ataques de las víctimas. Esto último fue de gran importancia, según un documento de RSA, porque permitió a los ciberdelincuentes entender mejor el efecto de ciertos tipos de ataques y saber cuándo un ataque DDoS era detectado y detenido, lo que les permitió ir mejorando.

Al año siguiente empresas de talla de CNN, eBay o Amazon sufrieron ataques similares, lanzados por un adolescente canadiense conocido como Mafiaboy, que los organizó convirtiendo los ordenadores host en zombies y utilizándolos para propagar esos ataques.

Quedó así demostrada la efectividad de los ataques DDoS y empezó a aparecer malware como MyTob, un gusano que se auto propagaba para infectar los ordenadores de una red de forma que los hackers podían luego enviarles las instrucciones de ataques. La naturaleza distribuida de los ataques, que pasaron de ser DoS a DDoS, multiplicó su potencia y complicó su detección, convirtiéndose en armas formidables que los ciberdelincuentes han ido mejorando con el tiempo utilizando herramientas y métodos mejorados.

De atacar a sites de comercio electrónico, instituciones financieras y agencias gubernamentales, se pasó poco después a los ataques contra DNS (Domain Name System). Sólo en el año 2002 se detectaron un total de trece ataques contra servidores DNS, que son esenciales para dar servicio a Internet porque son los encargados de traducir los nombres de los sites, la URL, en una dirección IP. Sin ellos no seríamos capaces de navegar por internet, de acceder a una página web o contactar con un dispositivo específico.

Hoy en día los ataques DDoS han crecido en escala y complejidad. Las empresas nunca saben cuándo van a ser víctimas de este tipo de ataques, por eso conviene contar con estrategia y servicios que frenen o limiten el impacto de un ataque de este tipo.

**Retos de los ataques DDoS actuales**

Afrontar su crecimiento y afrontar la creciente capacidad de los ciberdelincuentes a la hora de coordinar recursos en todo el planeta con el fin de lograr el máximo impacto con sus ataques son algunos de los retos que generan los actuales ataques de

"Los dispositivos IoT resultan muy atractivos para los ciberdelincuentes que preparan ataques tipo DDoS, ya que les agilizan el trabajo sin costes extra"

Ález López del Atxer,
director general de F5 Networks

# Infoblox y el desafío del DNS

En sus orígenes Infoblox era conocido por sus servicios de red, era líder en la categoría de DDI, en servicios de DNS, que son los que permiten navegar por Internet. Y durante un tiempo lo hicieron lo suficientemente bien "como para convertir en el líder del mercado", explica a IT Digital Security Jesper Andersen, CEO de Infoblox a su paso por Madrid.

Aprovechamos su visita no sólo para hablar de la evolución de la compañía, sino para hablar de ataques de denegación de servicio distribuido que son, en opinión del directo, "baratos de realizar y costosos de defender". El DDoS como servicio ha puesto este tipo de ataques al alcance de cualquiera, sólo se necesita un sitio web desde el que ordenar el ataque, pero construir una infraestructura capaz de soportarlo es otro cantar.


Los ataques DDoS tienen una relación especial con el Sistema de nombres de dominio: los ataques DDoS atacan y explotan los servidores DNS; un ataque DDoS exitoso contra ellos hará que sus clientes no puedan visitar su sitio web o enviarle un correo electrónico. Todas las organizaciones con presencia en Internet deben tener un conjunto de servidores DNS autorizados, e incluso la información más básica (por ejemplo, una de sus direcciones de correo electrónico o el nombre de dominio de su sitio web), un posible atacante puede encontrar los nombres y direcciones de esos servidores DNS, dándoles una lista de objetivos.

Hablando con Jesper Andersen sobre DDoS y la propuesta de la compañía para el mercado de la seguridad nos cuenta que Infoblox ha "abordado el tema de la seguridad desde dos puntos de vista, uno externo y otro interno".

El DNS, explica el directo, es el primer lugar realmente importante desde la perspectiva de la seguridad; "evitamos que nuestros clientes sean víctimas de un ataque DDoS, algo que es especialmente preocupante para aquellos que están activos en el comercio electrónico, porque si alguien no se puede conectar y comprar cosas, eso significa perder millones". De forma que el primer paso fue ayudar a los clientes a prevenir ataques DDoS, y no ser víctimas de redireccionamientos fraudulentos, manteniendo seguros los datos confidenciales, como las credenciales de acceso o los datos de las tarjetas de crédito, gracias a Infoblox Advanced DNS Protection.

"La segunda cosa que hicimos en torno a la seguridad está relacionada con el despliegue de un DNS en la red interna", continúa explicando Jesper Andersen. Nos cuenta en directivo que todo el ransomware y el malware que entra en las redes tiene que conectarse a un centro de comando y control, y lo primero que hacen estos centros es realizar una consulta DNS para averiguar cuál es la dirección IP, "de forma conociendo la legitimidad de la URL desde la que se hace la consulta podríamos bloquearla y el ransomware nunca podría llegar a su centro de comando y control para recibir instrucciones". La respuesta de Infoblox ha sido un Firewall DNS, que es una parte de la infraestructura que según el CEO de Infoblox se va a convertir en el centro de atención de los ciberdelincuentes.

"En muchas compañías de todo el mundo hay un gran desafío con el DNS", asegura Jesper Andersen. Se trata del protocolo más atacado. La experiencia del directivo le lleva a asegura que en la mayoría de las compañías las operaciones de red están completamente separadas de las operaciones de seguridad; "a veces ni se hablan entre sí o están en diferentes edificios, y eso es lo que los malos están aprovechando". Y eso es porque cuando vas a hablar con el operador de redes, que es el propietario del DNS te dice que no sabe nada sobre seguridad, que sólo está la actividad y el tiempo de respuesta a la consulta, y cuando vas al equipo de operaciones de seguridad te dicen que ellos no tienen el DNS y que por tanto no son responsables, lo que demuestra que mucho queda por avanzar.

DDoS. Lo dice Álex López DE ATXER, Director general de F5 Networks, que explica que estos ataques ya no se centran solamente en bloquear la prestación del servicio online de una organización a sus clientes. “En la actualidad, muchos hackers utilizan ataques DDoS como pantalla de humo para ocultar un objetivo más dañino, que tiene que ver con comprometer los datos confidenciales de la empresa”, dice el directivo.

El Centro de Operaciones de Seguridad (SOC) de F5, situado en Varsovia, muestra que los ataques DDoS dirigidos a organizaciones europeas están creciendo exponencialmente, y si tenemos en cuenta que para un hacker puede resultar bastante sencillo desde el punto de vista técnico lanzar un ataque DDoS, “es posible que en estos momentos las organizaciones sean más vulnerables que nunca”. Álex López dice también que la parte positiva es que las herramientas necesarias para protegerse adecuadamente, tanto on-premise como en la nube, ya están disponibles, por lo que con independencia del tamaño o actividad de la empresa es posible protegerse adecuadamente.

Para Jose María Cayuela Senior Security Specialist de Akamai Technologies, los retos actuales no han cambiado significativamente con respecto a años anteriores. “El cambio que hemos percibido es la capacidad y la disponibilidad de herramientas de ataque basadas en botnets de dispositivos IoT. Este cambio es el que ha introducido un desafío diferente”. Y explica el directivo que el acceso y la falta de securización de este tipo de dispositivos, combinado con la conectividad a Internet de todos ellos, contribuyen a aumentar el riesgo de forma considerable. Se une que las organizaciones criminales tienen hoy a su disposición una infraestructura de ataque mucho más capilar, asequible y disponible.

> "Hoy todo el mundo se decanta por un modelo de protección compartido, consumiendo modelos de mitigación DDoS-as-a-service"
>
> Jesús Vega, Regional Sales Director de Imperva para Iberia

Alfonso Ramírez, director general de Kaspersky Lab Iberia, tiene claro que los ataques DDoS generan grandes beneficios y su coste no es muy elevado, “por lo que son una buena herramienta para los cibercriminales”. Y asegura que el reto de estos ataques es conseguir el máximo beneficio o hacer el mayor daño posible a la empresa atacada. Al mismo tiempo, están al alcance de cualquiera en un modelo de DDoS-as-a-Service. Según investigaciones de la compañía, el coste de un ataque sobre una página web desprotegida puede ir desde los 46 a los 92 euros; mientras que un ataque a una página protegida sube hasta los 370 euros o más. Así, un ataque DDoS puede costar desde los 4,6 euros por 300 segundos de duración hasta los 370 euros por un ataque de 24 horas. El precio medio de un ataque está en los 23 euros por hora. Los expertos de Kaspersky calculan en 6,5 euros por hora el coste de un ataque de un botnet en la nube de 1000 ordenadores de sobremesa, de forma que los cibercriminales rentabilizan los ataques DDoS a 16 euros por hora.

Jesús Vega, Regional Sales Director para Iberia de Imperva habla de desafíos económicos en cuanto que lanzar ataques se ha convertido en algo tan económico, incluso gratuito, y que “cualquiera puede perpetrar un ataque DDoS letal simplemente alquilando un servicio online”. Añade también que ahora la dirección de un ataque no es igual que la duración del impacto, “lo que significa que incluso una breve explosión/estallido de ataque DDoS puede tener un gran impacto en cualquier actividad comercial y tiempo de actividad”. Explica también Jesús Vega lo que es Hit Wave, una tendencia dentro de este tipo de ataques que consiste en que el atacante lanza un ataque DDoS grande pero de corta duración (de unos pocos segundos) para luego detenerlo. “La repetición de dicho patrón

puede echar abajo rápidamente incluso el servidor web más resistente y, de paso, también los routers", asegura el responsable de Imperva para España.

Por último, menciona Vega un tercer reto, una tendencia conocida como Hit 'n Run (Táctica de Ataque y Retirada) en la que se envía una gran cantidad de tráfico DDoS hacia la IP de la víctima. En la mayoría de los casos, excede el ancho de banda ofrecido por el ISP y colapsa rápidamente las líneas de comunicaciones, dejando la botnet del atacante libre para atacar a otros. Según datos de un informe sobre DDoS Incapsula de Imperva el porcentaje de ataques DDoS de menos de 30 minutos tipo Hit 'n Run fue del 74,3% en el tercer trimestre de 2016, del 78,2% en el cuarto trimestre de 2016 y alcanzó el 90,5% en el primer trimestre de este año.

**Impacto del IoT**

Desde finales del 2014 se viene observando cómo los ataques con origen en dispositivos IoT van tomando protagonismo. Tanto es así, que a finales del 2015 el volumen de tráfico desde estos dispositivos involucrados en un ataque de más de 100Gbps es ya el 75% y ya en 2016 ataques a Krebs y DyN dejan volúmenes de tráfico de más de 600 Gbps y 1 Tbps respectivamente, explica Jose María Cayuela, de Akamai. "A día de hoy tal y como recogemos en nuestro informe SOTI (State of the Internet) vemos como el número de ataques DDoS a infraestructuras aumenta observando una disminución de tráfico. Esto no indica que estemos hoy día más seguros, sino que posiblemente aquellos que orquestan este tipo de actividades maliciosas estén trabajando

"El impacto de un ataque DDoS en el negocio es muy difícil de calcular, pero uno de los elementos principales en el coste de un ataque DDoS es el daño reputacional"

Jose María Cayuela Senior Security Specialist de Akamai Technologies

en nuevas herramientas con nuevas capacidades para coordinar oleadas de ataques".

Para Álex López, los dispositivos IoT "resultan muy atractivos para los ciberdelincuentes que preparan ataques tipo DDoS, ya que les agilizan el trabajo sin costes extra y además son muy fáciles de controlar al presentar, en su mayor parte, unos estándares de seguridad deficientes". Hay que tener en cuenta, dice el directivo, que la mayoría de ellos se comercializa con contraseñas predeterminadas que normalmente nunca se cambian o que, en algunos casos, es imposible cambiar, por lo que para los hackers no resulta complicado introducirse en los sistemas de gestión remota de estos dispositivos –Sistemas Telnet o SSH- e identificar las contraseñas predeterminadas por el fabricante, logrando hacerse con el control de los mismos.

"Los fabricantes de estos productos deben mejorar la seguridad de sus dispositivos a la hora de desarrollarlos y los consumidores deben aprender a mantener su seguridad a la hora de adquirirlos. Los gobiernos también deben tomar cartas en el asunto, legislando para lograr una IoT más segura", asegura el responsable de F5 Networks en España. Y mientras todo eso sucede, cualquier empresa puede ver cómo su negocio corre peligro por un ataque de este tipo, por lo que es necesario que definan sus estrategias de mitigación de ataques DDoS, a fin de estar preparadas ante cualquier incidencia que puede ocurrir de forma inminente.

Igual de crítico se muestra Jesús Vega, de Imperva, al afirmar que "hay muchísimos dispositivos IoT a los que se puede acceder de forma remota a través de credenciales de inicio de sesión fáciles de adivinar, generalmente nombres de usuario y contraseñas predeterminados de fábrica (por ejemplo, admin/admin)". Explica también Vega que esta

# Anonymous y DDoS como forma de protesta

Se esconden tras una careta y son legión. Detrás de Anonymous hay miles de individuos anónimos unidos por la lucha. Protestan contra decisiones políticas, organizaciones como la Iglesia, los lobbies bancarios o las leyes que vayan contra la libertad de expresión o libre disposición de elementos online. Son un grupo libre y sin jerarquías, y aunque también se les puede ver en manifestaciones, sus protestas en la red llegan en forma de ciberataque.

Se esconden tras una careta. Para muchos la de V de Vendetta, el antihéroe del cómiz de Alan More, aunque en realidad es la caricatura de Gy Fawkes, un soldado británico que en en 1605 participó en la llamada conspiración de la pólvora. Fawkes cavó un túnel debajo del Parlamento Británico para tratar de volarlo, pero fue arrestado torturado y condenado a morir en la horca acusado de conspiración el 5 de noviembre de aquel año. Tras su ejecución su cuerpo fue despedazado y sus restos esparcidos por varias partes del país como aviso a futuros conspiradores.

Como parte de su "Operación Cataluña", Anonymous fue el grupo responsable del ataque contra la web del Tribunal Constitucional de España el pasado 21 de octubre, el mismo día en que el Consejo de Ministros del gobierno se reunía para hablar sobre las medidas legales para tomar control de Cataluña. El grupo había declarado a través de la cuenta de Twitter @NamaTikure que lanzaría ataques para defender la "libertad" de Cataluña, cuyo gobierno organizó un referéndum ilegal sobre la independencia de la región a principios del mes.

No ha sido, ni mucho menos, la primera acción realizada por el grupo, que ha convertido los ataques de DDoS en su forma de protesta. Un hecho que ha heredado de otros grupos por The Strano Network, causante del que se considera el primer ejemplo se ataque DDoS como firma de protesta; se produjo en 1995 contra la política nuclear del gobierno francés. También merece la pena mencionar a Electronic Disturbance Theater (EDT) porque fue uno de los primeros grupos en desarrollar sus propias herramientas de ataque: FlooNet.

Anonymous tomó el relevo popularizando la idea de las botnets voluntarias. Mediante un software conocido como Low Orbit Ion Cannon, las personas que quisieran unirse a la protesta podían conectar sus ordenadores a una gran red y donar sus recursos a un ataque DDoS.

El fin de Anonymous es la repercusión social y por eso hacen uso de redes sociales como Twitter para que sus ataques sean bien visibles. La repercusión es más importante que el tiempo que una determinada página web esté técnicamente inaccesible.

situación permite extender y desplegar una nueva botnet, y que una vez que los dispositivos han sido infectados por una botnet, éstos se convierten en esclavos a la espera de recibir órdenes. La unidad de Mando y Control dirige dicha botnet mediante el envío de tareas que serán realizadas por esos agentes. En muchos casos, esas redes bots se utilizan para lanzar ataques DDoS.

**Coste de un ataque de DDoS**

Para medir el coste de un ataque DDoS se tienen en cuenta dos parámetros, según Ález López de Atxer. El primero es el de reputación. No ser capaz de detectar y mitigar un ataque DDoS puede dañar la relación que mantiene una empresa con sus clientes, que pueden percibir en el ataque un signo de debilidad o de desidia. El segundo parámetro es el económico, y aquí habrá que calcular el coste de haber dejado de prestar servicio durante un tiempo determinado. Y recuerda que capítulo aparte es el coste que supone disponer de una infraestructura tecnológica capaz de resistir estos ataques, "no solo con más soluciones de seguridad, servidores, ancho de banda, etc. sino también la disponibilidad de personal especializado y proveedores externos que trabajen para mantener la seguridad o para resolver una incidencia".

Aunque el impacto de un ataque DDoS en el negocio es muy difícil de calcular, pero uno de los elementos principales en el coste de un ataque DDoS es el daño reputacional, dice Jose María Cayuela. "Según la industria también vemos altísimos costes por dejar de dar servicio". Y esto parecer ser espe-

cialmente crítico en el sector Retail. Además, con las nuevas normativas de protección de datos, el coste también se verá afectado considerablemente por las sanciones ante robo de información. De forma que desde Akamai determinan tres factores clave en el coste de un ataque: daño reputacional, pérdidas directas por no dar servicio y posibles sanciones regulatorias.

Para Jesús Vega el coste y los riesgos varían según el mercado vertical y tipo de negocio. "Algunas empresas dependen en gran medida de sus recursos en línea y este es un activo fundamental en la forma en que generan ingresos. A otras les preocupa más la reputación y el impacto en su marca como factor principal". Dice Vega que el impacto reputacional es muy difícil de medir y la investigación ha demostrado que puede durar más de cinco años, pero que además se debe tener en cuenta también el impacto inmediato en los recursos de diferentes departamentos. ¿Cuántos empleados y subcontratistas están involucrados en la mitigación del ataque DDoS y en la actividad de recuperación que tiene lugar justo después? Empleados de IT, Seguridad, Legal, Desarrollo, etc.

Coincide Alfonso Ramírez en identificar lo económico y reputaciones como los costes principales en un ataque DDoS, pero añade que "la recuperación ante un ataque DDoS es también compleja, sobre todo en el caso de entidades financieras, por ejemplo". Y aporta los datos de un estudio que recoge que el coste para una institución financiera puede llegar a superar el millón de euros, frente a los 850.000 euros de otra industria.

**¿Se puede evitar un ataque DDoS?**

Debido a la facilidad para lanzar un ataque, evitarlo está fuera del control del usuario. Sobre lo que sí se puede tener control es sobre las medidas de protección utilizadas en caso de un ataque lanzado contra un sitio web o infraestructura.

De forma que sí se puede evitar un ataque de DDoS, pero ¿cómo? "En primer lugar, sería necesario utilizar tecnologías anti-DDoS basadas tanto en la nube como on-premise, lo que asegurará la protección contra los elementos de un ataque combinado dirigido tanto a la capa de aplicación como a los lanzados desde fuera de la infraestructura, eliminando el tráfico malicioso antes de que llegue a la red. Solo un enfoque híbrido puede brindar a las

organizaciones la flexibilidad necesaria para protegerse contra la amplia gama de armas existentes y a disposición de los hackers", dice Álex López.

Pero no sólo basta con eso, porque también hay que asegurarse de que el proveedor de Internet analiza de forma constante el tráfico de la red e incorpora mejoras de forma continua en sus procesos de análisis. Y finalmente añade el directivo que "contar con la ayuda de un experto también resulta recomendable, con el fin de estar al tanto de las técnicas más recientes". Y es que, en muchas ocasiones, solo los expertos van a ser capaces de identificar los ataques DDoS y de evitar sus consecuencias.

Jesús Vega explica que tradicionalmente, las empresas, hosters y proveedores de servicios de Internet han estado desplegando equipamiento costoso para mitigar el DDos. El problema con el modelo tradicional es que no es escalable desde una

perspectiva económica. Los ataques DDoS siguen la Ley de Moore, se duplican en tamaño y complejidad cada 18 meses, por tanto, las empresas deben duplicar el número de equipos de mitigación e infraestructura al mismo nivel. Además, el proceso de mitigación manual lleva más tiempo del debido a causa de la mayor sofisticación de los ataques, ya que, a diferencia de hace algunos años, se incluyen múltiples vectores de ataque paralelos.

"Hoy todo el mundo se decanta por un modelo de protección compartido, consumiendo modelos de mitigación DDoS-as-a-service. En dicho modelo, los proveedores de mitigación de DDoS invierten mucho en una tecnología y una infraestructura de mitigación DDoS sólida y global, mientras revenden los servicios de protección a un precio fijo a sus clientes", dice el responsable de Imperva para España. Esto permite a los proveedores de mitigación de DDoS hacer crecer su red año tras año y desarrollar tecnología de mitigación de vanguardia gracias a que distribuyen su coste entre todos sus clientes. Con este servicio, las organizaciones obtienen una asistencia de protección DDoS a la que no podrían acceder por sí mismos, sin invertir una gran cantidad para construirlo.

Para Jose María Cayuela, Senior Security Specialist de Akamai, "mantener los equipos, dispositivos IoT o cualquier otro elemento con capacidad para conectarse a internet actualizado y securizado es la única vía que tenemos de evitar que se produzcan este tipo de ataques fácilmente". Añade el directivo que la responsabilidad de esto corresponde a fabricantes, empresas y usuarios y que ya se está tra-

## Mirai, un antes y después

Mirai es un tipo de malware que se dedica a buscar dispositivos IoT para infectarlos e incluirlos en una botnet, una red de dispositivos que pueden controlarse de manera centralizada. Con millones de dispositivo conectados y controlados se pueden montar ataques de denegación de servicio distribuida (DDoS) en los que una ráfaga de tráfico basura inunda los servidores de un destino con tráfico malicioso.

El año pasado Mirai fue capaz de interrumpir el servicio de Internet a más de 900.000 clientes de Deutsche Telekom en Alemania, infectó casi 2.400 routers TalkTalk en el Reino Unido y lanzó un ataque contra OVH.

Pero quizá el que tuvo más repercusión fue el ataque de DDoS contra los servidores de Dyn, una importante empresa de DNS que daba servicio a páginas como Twitter, Spotify, PayPal o Amazon, que quedaron inaccesibles durante horas. Meses después y según una investigación de BitSight Tecnologies se supo que unos 14.500 dominios que utilizaban los servicios de Dyn abandonaron la compañía inmediatamente después del ataque; la cifra representó el 8% de los dominios que dependían de Dyn para la gestión de sus DNS. Ya poco importa, porque la compañía fue adquirida por Oracle en noviembre por 600 millones de dólares.

¿Por qué Mirai fue diferente? Porque según las posteriores investigaciones, fue diseñado desde cero por personas que tenían experiencia previa con la familia de malware gafgyt y por tanto incorporaba muchas de las características de diseño que ya utilizaban las especies de malware más adecuadas en el espacio de IoT. Además, un hacker conocido como "Anna-senpai" eligió abrir su código en septiembre y se une el hecho de que el software de Mirai ha demostrado ser notablemente flexible y adaptable. Como resultado, los hackers pueden desarrollar diferentes cepas de Mirai que pueden hacerse cargo de nuevos dispositivos de IoT vulnerables y aumentar la población (y la potencia de cómputo) de las botnets de Mirai.

No se descuiden, porque Mirai está en manos de unos profesionales.

bajando en la elaboración de normativas, para que cualquier dispositivo puesto en el mercado tenga la garantía de que las medidas de seguridad aplicadas sean las necesarias como para evitar que estos elementos puedan ser hackeados y ser susceptibles de pasar a formar parte de una botnet.

Evitar un ataque de DDoS tampoco es una opción para Alfonso Ramírez. “La pregunta no es si una empresa u organización va a ser atacada, sino cuándo va a producirse ese ataque”, dice el directivo, añadiendo que, ante un problema como este, que no deja de crecer y afecta cada vez a más empresas de todo tipo y tamaño, es importante tomar las medidas adecuadas de protección de infraestructuras TI que impidan ser infiltradas y puedan mantener sus datos seguros. El trabajar con el partner adecuado garantiza a las empresas que puedan enfrentarse a todos los niveles y complejidades de un incidente DDoS, que sólo pueden ser cada vez más fuertes y más sofisticados.

“Para ayudar a las empresas a defenderse antes los ataques DDoS, independientemente de dónde tengan su origen, Kaspersky DDoS Protection ofrece una solución completa e integrada que incluye todo lo que una empresa necesita para minimizar el riesgo de los ataques DDoS”, explica Ramírez. La solución permite que las empresas sigan funcionando con normalidad al protegerles frente a los ataques cada vez más sofisticados y frecuentes.

**Tipos de ataques DDoS**

Existe una gran variedad de este tipo de ataques. Según SOC de F5 Networks de Varsovia, las fragmentaciones del protocolo de usuario (UDP) fueron el tipo de ataque DDoS más común durante el pasado año (23% del total), seguido de DNS Reflections e inundaciones UDP (15%), inundaciones Syn (13%) y NTP Reflections (8%). Los responsables de seguridad de cerca de 300 compañías europeas a los que F5 encuestó hace unos meses afirman que los Blended DDoS son actualmente la mayor amenaza (26%), seguidos por los ataques a nivel de aplicación (25%), ataques volumétricos (19%) y ataques de extorsión (15%).

Akamai coincide al responder que las estadísticas siguen posicionando los vectores de ataque basados en fragmentación UDP, DNS, NTP, UDP/SYN flood y SSDP como los principales. Además, la tendencia en ataques de reflexión se ha mantenido con respecto al año anterior.

Para Alfonso Ramírez, la finalidad de los ataques DDoS es lo que marca la principal diferencia entre ellos. Además de producir problemas inmediatos y visibles en sus operaciones, el 56,5% de las empresas españolas reconoce también que los ataques DDoS se han utilizado como cortinas de humo para otro tipo de acciones que han derivado en importantes daños financieros y reputacionales. Los ataques DDoS se utilizaron en el 37,2% de los casos para esconder ataques de malware, en un 30,2% para el robo o extracción de datos, en un 20,9% para el robo de dinero y hasta en un 44,2% para acceder a la red corporativa o hackearla.

En los últimos meses hemos visto que no solo los cibercriminales expertos en alta tecnología pueden lanzar ataques DDoS pidiendo un rescate. Cualquier persona, incluso sin conocimientos técnicos puede comprar una demostración de ataque para extorsionar. Suelen escoger empresas inexpertas que no protegen sus recursos contra ataques DDoS y, por tanto, pueden pagar el rescate con una simple demostración.

**Ataques DDoS y la empresa española**

“La concienciación sobre los riesgos asociados con los ataques DDoS está aún en sus inicios”, responde Jesús Vega cuando le preguntamos si la empresa española se toma en serio el riesgo que supone sufrir un ataque DDoS. Para el directivo de Imperva, las organizaciones españolas deberían empezar a pensar seriamente sobre su enfoque en cuanto a protección DDoS y sobre cómo asegurar que la economía española sea resistente a este tipo de amenazas.

Con los datos en la mano. F5 publicó hace unos meses los resultados de una encuesta a cerca de 300 responsables de seguridad europeos. La conclusión principal, perfectamente extrapolable al mercado español, fue que a pesar de que el 35% de los encuestados afirmaron haber sufrido o tener la sospecha de haber sufrido un ataque DDoS, en más de un tercio de las organizaciones aún no se ha desarrollado un plan de respuesta frente a ciberataques. “Teniendo en cuenta que no hay semana en la que no se produzca un ataque o un robo de datos, esta situación resulta altamente preocupante”, concluye Álex López.

Más confiado se muestra Jose María Cayuela al asegurar que el riesgo de ser objeto de este tipo de ataques está presente en los comités de dirección de la mayoría de las compañías españolas, “bien porque una pérdida de servicio pueda implicar un impacto negativo con pérdida de ingresos e insatisfacción de nuestros clientes, así como el impacto reputacional que conlleva el sufrir un ataque y dejar en evidencia que no disponíamos de las medidas necesarias para mitigar un ataque de estas características”.

Asegurando que “queda mucho por hacer todavía en este sentido”, Alfonso Ramírez aporta los datos del estudio Global IT Security Risks (edición 2017) que recoge que el 50,6% de las empresas españolas reconoce que la frecuencia y complejidad de los ataques DDoS dirigidos contra organizaciones como la suya están creciendo en número cada año, y el 35,4% ya ha experimentado en 2017 un ataque de este tipo, frente al 25,5% que se vieron afectadas en 2016, demostrando la importancia que tiene una mejor prevención y protección frente a este tipo de ataques.

A nivel global, el 20% de las empresas afectadas por estos ataques fueron empresas muy pequeñas, el 33% pymes y un 41% empresas grandes, lo que demuestra que independientemente del tamaño o clase de las organizaciones, todas están en peligro. Por otra parte, en los últimos 12 meses, el 89% de las empresas españolas que han sido víctimas de un ataque han sufrido más de uno, un 10% más que la media mundial. Las consecuencias son muy importantes, pues el 20,6% de las empresas españolas reconocen haber sufrido una importante reducción del funcionamiento de sus servicios, el 12,7% vio como sus transacciones y procesos fallaban, y un 6,3% reconoce una total interrupción en su actividad.

**DDoS en el tercer trimestre de 2017**

En el tercer trimestre de 2017 el número de ataques de DDoS en China, Estados Unidos, Corea Del Sur y Rusia se incrementó. Según datos de Kaspersky Lab no sólo hubo un incremento en el número, más de 450 ataques diarios, sino en la potencia, más de 15,8 millones de paquetes por segundo.

El mayor logro en la lucha contra los ataques de DDoS fue desactivar la botnet WireX, que secretamente había estado trabajando en dispositivos Android y a través de aplicaciones en Google Play. Las acciones conjuntas de Google, Samsung y otros varios fabricantes de seguridad pudieron echar abajo la botnet.

"El riesgo de ser víctima de un ataque DDoS, aislado o como parte de un ataque combinado, no parece que vaya a disminuir"

Alfonso Ramírez, Director General de Kaspersky para ESoaña y Portugal

la efectividad de sus métodos sea cuestionable. Y es que los dos actos políticos más notables del tercer trimestre (un ataque contra el proveedor de hosting DreamHost y en un sitio libertario) no lograron nada aparte de una mayor publicidad para los recursos atacados.

Como un medio para ejercer presión, los ataques DDoS buscan industrias donde el tiempo de inactividad y las fallas de comunicación generan más pérdidas de ganancias y reputación. De forma que la industria del juego se está volviendo aún más atractiva para los ciberdelincuentes: por un lado, este mercado genera cientos de miles de millones de dólares, mientras que la seguridad aún está lejos de ser perfecta, con plataformas de juegos híbridas vulnerables a los ataques a través de los enlaces entre recursos y aplicaciones. En el tercer trimestre se vieron ataques contra Blizzard Entertainment, que causaron problemas a los jugadores de Overwatch y World of Warcraft; también contra Americas Cardroom, un site de póker online y contra la UK National Lottery, que estuvo sin servicio durante 90 minutos.

El ataque DDoS más largo del tercer trimestre duró 215 horas, un 28% menos que el más largo del trimestre anterior. Pero al mismo tiempo, el porcentaje de ataques que duraron menos de 50 horas permanece estable: un 99,6 por ciento en el tercer trimestre, frente al 99,7% del segundo.

**Lo peor está por llegar**

2017 está siendo un año complicado en lo que ataques de DDOS se refiere. Desde F5 detectan un fuerte incremento en los ataques tipo DDoS y creen que esta tendencia, empujada por la proliferación de dispositivos IoT, va a continuar. “Asimismo, creemos que los ataques DDoS van a seguir evolucionando e incrementando su complejidad. Por ello, las organizaciones de todo tipo y tamaño tendrán ante sí el reto de garantizar que sus aplicaciones críticas y sus redes permanecen protegidas y disponibles bajo las condiciones más exigentes con independencia del volumen, el tipo o la fuente del ataque DDoS”, concluye Álex López de Atxer, director general de F5 Networks España.



Asegurando que no hay un futuro cierto, aseguran desde Akamai que por experiencia saben que este tipo de ataques es crítico y con toda seguridad volverán mucho más potentes contra compañías e instituciones con el objetivo de causar el mayor caos posible en internet. “Desde Akamai vemos como constantemente se testea cualquier elemento conectado a la red y estamos seguros que cualquier vulnerabilidad será aprovechada por hackers con un objetivo malicioso”, dice Jose María Cayuela.

“Cada vez se están popularizando más este tipo de ataques que son sencillos de poner en marcha, así que seguramente se vayan recrudeciendo con el tiempo y acaparen muchos titulares en 2018”, concluye Alfonso Ramírez.

**Enlaces de interés...**

- ¿Eres parte de una botnet?
- Cuatro razones para externalizar tu DNS
- Las Botnets de Linux acaparan el 70% de los ataques DDoS
- Los ataques de DDoS se duplican en seis meses
- Proteged vuestros servidores DNS

# Próximos #ITWebinars

www.ittelevision.es


## El puesto de trabajo productivo:
### dispositivos y tecnologías para potenciar el rendimiento

**Martes, 30 de enero de 2018**


## Definiendo la seguridad de un SDDC

**Martes, 27 de febrero de 2018**


## Gestión de vulnerabilidades

**Martes, 27 de marzo de 2018**

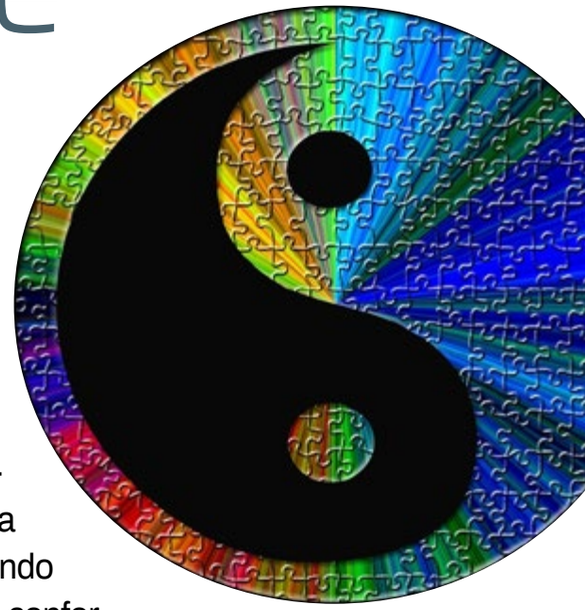

## Estrategias para lograr una experiencia de cliente satisfactoria

**Jueves, 29 de marzo de 2018**

**IGNACIO COBISA**

**Ignacio Cobisa**
**Analista de IDC**
Ignacio Cobisa es analista sénior de investigación en IDC. Con más de 15 años de experiencia en el mercado de TI y telecomunicaciones, antes de unirse a IDC trabajó en diferentes puestos en el Grupo Telefónica, el último como consultor interno en la Oficina del Presidente de Telefónica. Anteriormente estuvo a cargo de Customer Relationship en Ya.com (ISP español de Deutsche Telekom Group). Ignacio es Licenciado en Economía en Complutense (Madrid) y Diplomado en Finanzas en la Universidad de Berkeley.

# La amenaza del cibermal sobre el ciberbien



Cualquiera que esté un poco al tanto de la actualidad o que haga cierto seguimiento de los medios generalistas, se habrá dado cuenta de que cada vez se oyen más noticias relacionadas con ciberdelincuencia, ciberterrorismo, intentos de manipulación de elecciones a través de la red o desinformación online orquestada.

No hace falta ser un gran experto en geopolítica internacional para darse cuenta de que el mundo en el que nos movemos ha cambiado. Que en la próxima gran guerra, que desgraciadamente la habrá, seguramente se pondrá más foco en la seguridad de la red y en evitar amenazas cibernéticas, que en el envío de carros de combate.

Dentro de las predicciones que IDC hace anualmente sobre seguridad, este año nos hemos focalizado, en gran medida, en las amenazas que pueden suponer el cibermal sobre el ciberbien. O el impacto que estas amenazas pueden tener sobre la sociedad globalizada en la que vivimos, incluyendo las empresas que la conforman.

En 2021 el 25% de los datos personales del mundo se verán comprometidos y almacenados en un data lake analizado y utilizado por los ciberdelincuentes organizados

Durante años, los profesionales de la seguridad de la información han discutido un nuevo paradigma de amenazas en el cual los atacantes aprovechan los análisis de una manera similar a la de los proveedores de productos y servicios de seguridad. Lo que no se ha discutido, sin embargo, es que también igual que existe cooperación entre los

# En 2021 el 25% de los datos personales del mundo se verán comprometidos y almacenados en un data lake analizado y utilizado por los ciberdelincuentes organizados


proveedores de seguridad también existe entre los ciberdelincuentes.

Los atacantes están comenzando a adoptar un enfoque más colaborativo, y los resultados podrían ser devastadores. Basta imaginar el poder de combinar algunas de las brechas más grandes de información que se han dado en los últimos años

Si una persona de manera individual se ve atrapada en cada una de estas fugas de información, cedería todos los aspectos privados de su vida. Finalmente, es importante destacar que las miles de pequeñas brechas de datos agregadas servirían para crear un repositorio aún más poderoso que podría usarse para obtener una ventaja competitiva sobre los equipos de seguridad de las empresas y los departamentos de detección de fraude.

En el año 2021 las tensiones geopolíticas, el cibercrimen sin fronteras y un aumento del 30% en el ciber espionaje de Estado impulsarán los esfuerzos para llevar a cabo una “Ciber-Convención de Ginebra”

En un pasado no muy lejano, los gobiernos y las empresas se basaban en límites bien definidos para proteger sus activos más sensibles, ya sean físicos o digitales. Estas defensas comprobadas, reforzadas por una amplia tecnología y supervisadas por profesionales, mantuvieron nuestra información segura y fuera de las manos de espías y criminales. Sabíamos dónde estaban los límites de nuestras redes, y mantuvimos nuestros activos importantes en el lado seguro. Con la popularización del cloud, miles de millones de usuarios acceden a los datos en millones de aplicaciones, sin tener en cuenta la ubicación física de la información. Nuestros perímetros se han desintegrado, y los cibermalos, ya sean criminales, terroristas, delincuentes comunes o estados, se han aprovechado de esta desintegración por obtener sus objetivos de manera ilegal.

El crecimiento económico se verá afectado en la medida en que el desafío a la ciberseguridad continúe causando daños en forma de pérdidas monetarias, trastornos políticos y daños físicos (como resultado de problemas de seguridad en IoT). Esto, a su vez, impulsará a los gobiernos a colaborar en

El crecimiento económico se verá afectado en la medida en que el desafío a la ciberseguridad continúe causando daños en forma de pérdidas monetarias, trastornos políticos y daños físicos

normas y convenciones internacionales aplicables sobre ciberguerra y cibercrimen. Una iniciativa liderada por los gobiernos del G20 buscará establecer pautas formales para las actividades cibernéticas. Las leyes y reglamentaciones internacionales, como la Convención de Ginebra o una extensión del Manual de Tallin, establecerán estándares sobre qué actividades cibernéticas son aceptables y cuáles no, tanto en términos de guerra como de actividades delictivas.

Las empresas tienen la necesidad de adaptarse a este entorno para poder seguir generando valor para sus accionistas. Por tanto, desde IDC creemos que dentro de las prioridades de inversión en estos próximos años, la seguridad debe de seguir siendo una partida destacada. Las empresas deberán poner foco en garantizar distintos niveles de seguridad en función de los niveles de riesgo de los usuarios. La gestión integral de la seguridad será una palanca importante para evitar la complejidad.

En el año 2019, el 75% de los CIO reenfocarán la ciberseguridad en torno a la autenticación y confianza para gestionar los riesgos, iniciando la retirada de sistemas que no pueden garantizar la protección de datos

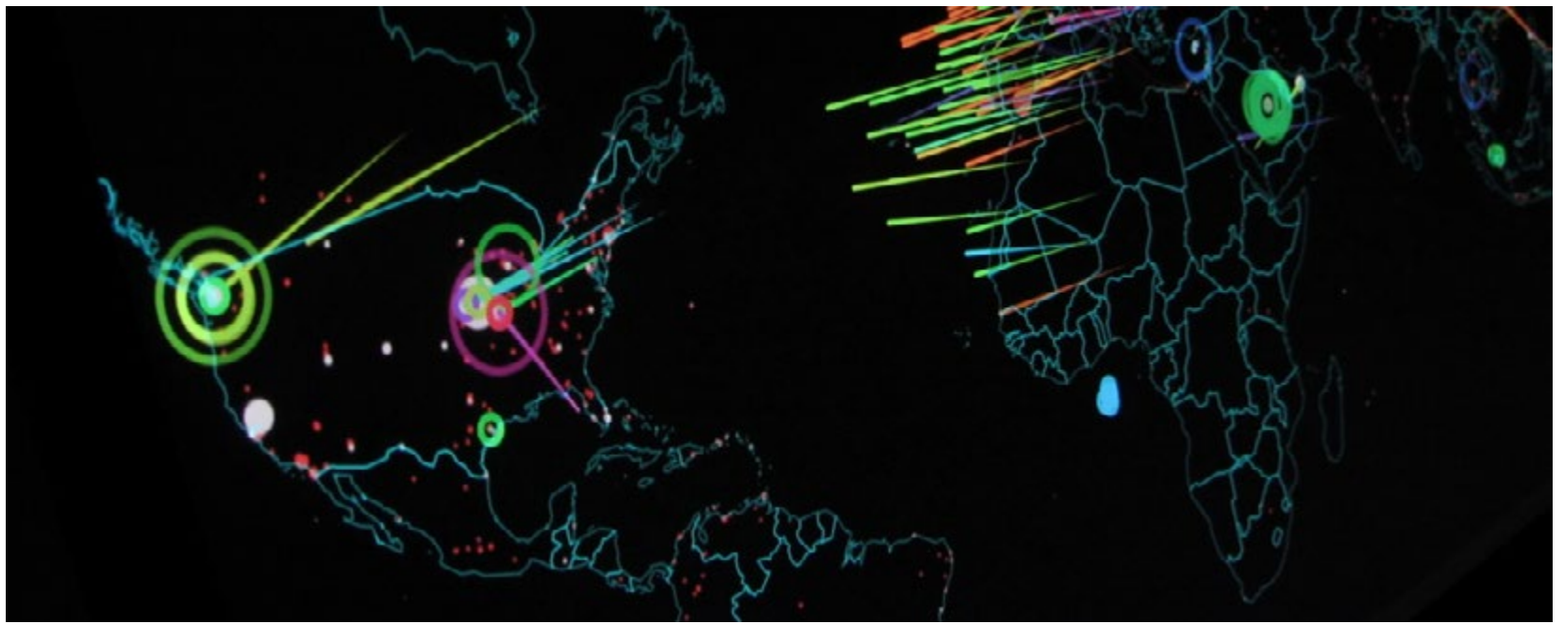
El concepto de una misma seguridad para todos ya no es válido dentro de los departamentos TI. La tendencia es a buscar crear un entorno seguro que proteja los sistemas actuales y futuros de las crecientes amenazas de seguridad, al tiempo que mantiene el nivel de experiencia del usuario. Este equilibrio, requerirá que los sistemas heredados se actualicen, modifiquen o retiren con el objetivo de mejorar la seguridad y permitir la defensa proactiva de la red en general, desde el centro de datos al dispositivo.

Este enfoque se basa cada vez en mayor medida en el concepto de “patch independence” y permitirá puertas de enlace dinámicas para proporcionar datos en tiempo real de actividades sospechosas y medir constantemente la fiabilidad del sistema.

Los niveles de seguridad se ajustarán según sea necesario en función de los niveles de riesgo. Con acciones en tiempo real basadas en el nivel de confianza y el nivel de impacto. Los sistemas que no puedan ajustarse para satisfacer estas necesidades, simplemente serán reemplazados o retirados.

Para el año 2020 el 30% del gasto en seguridad se destinará a proveedores que ofrezcan plataformas integradas de seguridad

# En el año 2019, el 75% de los CIO reenfocarán la ciberseguridad en torno a la autenticación y confianza para gestionar los riesgos



En un futuro, los CIOs promoverán significativamente menos productos de seguridad de TI individuales dentro de la empresa, en parte debido al presupuesto, pero sobre todo debido al impacto en la complejidad. Actualmente, algunas grandes empresas albergan hasta 50 productos de proveedores de seguridad en su entorno. Con el auge de la nube y el software como servicio (SaaS), las organizaciones buscan plataformas integradas para reducir la complejidad y los costes, así como para facilitar la gestión y administración de la infinidad de tecnologías que administran. Reducir la complejidad al pasar a plataformas integradas, ya sea on-premises, en la nube o en un entorno híbrido, también proporciona el entorno adecuado para una mayor seguridad, ya que las empresas no necesitan aplicar parches y actualizar tantas soluciones individuales.

A riesgo de poder sonar pretencioso, desde IDC creemos que si entre todos, empresas, administraciones públicas y organismos supranacionales nos centramos en controlar los riesgos se seguridad que podemos gestionar, las amenazas del cibermal sobre el ciberbien seguirán ahí, pero podremos minimizar su impacto.

**Enlaces de interés...**

- Los cinco grandes mitos de las brechas de seguridad
- Desmitificando el panorama de amenazas
- Lagunas de conocimietno en segurida
- Inteligencia de amenazas, un as en la manga


## Los cinco grandes mitos de las brechas de seguridad

Hemos terminado por asumir que una brecha de seguridad es inevitable y que el enfoque principal debe estar en la detección y la respuesta en lugar de la prevención. Pero en este documento Firemon plantea que esta opinión está promovida sobre la causa de que las brechas y los fallos de la tecnología son en realidad mitos, mitos que oscurecen un camino claro hacia una mayor seguridad y una mejor gestión de riesgos. “Desterrar estos mitos es un paso importante para mejorar la efectividad de nuestras defensas de seguridad contra futuros intentos de violación”. En este documento se exponen cinco de los mayores mitos que existen sobre violaciones de datos, y cómo y por qué ocurren.


## Cómo utilizar la Dark Web para la inteligencia de amenazas

Se habla de la Dark Web como el conjunto de sites en que se puede comprar y vender de todo, desde herramientas personalizadas para ciberdelincuencia hasta datos robados, drogas, armas y más. Este documento analiza cómo los investigadores pueden usar la web oscura para obtener inteligencia de amenazas muy valiosa, a menudo relevante para un amplio espectro de posibles objetivos, tanto organizaciones como individuos, a los que no se puede acceder a través de la monitorización convencional.


## Amenazas de primer nivel y su impacto en las decisiones de seguridad de Endpoint

El panorama de las amenazas continúa evolucionando a medida que los ciberdelincuentes se centran en desarrollar ataques sofisticados y dirigidos. Si bien los ataques perpetrados por ciberdelincuentes a través de métodos de phishing que introducen malware desconocido son primordiales, las organizaciones están preocupadas sobre el espectro diverso del panorama de amenazas. Explore este informe para aprender cómo proteger los puntos finales de su organización contra ataques cibernéticos con estrategias de defensa específicas, incluido el aprendizaje automático.

## Desmitificando el panorama de amenazas

Las empresas de seguridad deben transformar los datos de amenazas globales en inteligencia procesable que ayude a sus clientes a través del quién, cuándo, dónde, por qué y qué es la próxima amenaza. En este Whitepaper se guía a los lectores a través del cambiante panorama de amenazas, mostrándoles dónde es más vulnerable una empresa y proponiendo una guía que explique qué puede hacer para mantenerse a la vanguardia de la seguridad y no salir en los titulares.


# La Seguridad TIC a un solo clic

it Digital MEDIA GROUP

it whitepapers

# Tú eres la clave para la protección de datos

**EVA JARA**

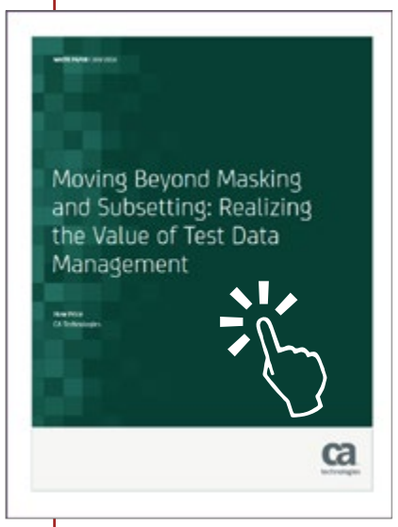
**Jefa de Equipo de Cumplimiento y PBC de EVO banco**

Colegiada por el Ilustre Colegio de Abogados de Madrid. Licenciada en Derecho por la Universidad Autónoma de Madrid. Cursado Master en Asesoría Jurídica de Empresas en el IE. Con experiencia profesional de más de 10 años en áreas relacionadas con el control interno, prevención del riesgo y protección de datos. Actualmente ocupa el puesto de Delegado de Protección de Datos y responsable del área de Cumplimiento Normativo de EVO Banco, S.A.U.

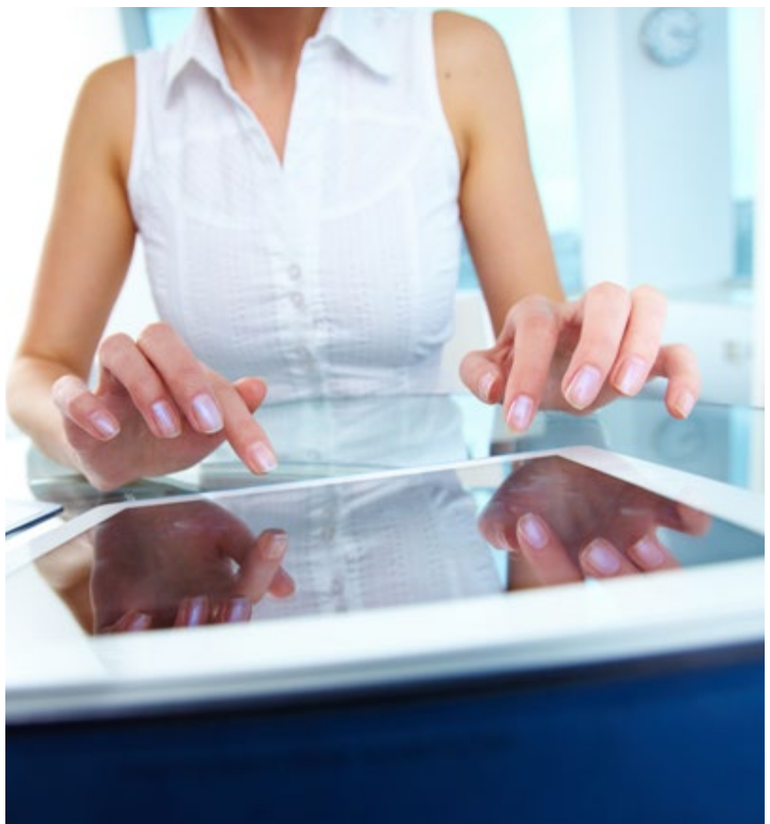
**¿La seguridad ha muerto? ¿La seguridad no existe? En el día de hoy tenemos más normativa que nunca sobre cómo proteger datos, así como controles y medidas de seguridad para ello. Sin embargo, tus datos siguen estando inseguros si tú no haces nada para preservarlos. Siempre oímos que las empresas tienen una serie de obligaciones para preservar tus datos y que tú cuentas con una serie de derechos, pero ojo ¿esto es suficiente? La realidad es que sin tu ayuda la seguridad no es posible.**

## 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.




No estoy hablando de "tu" empresa o empleado, sino el "tú" de persona, un simple usuario de la era digital bien por derecho, devoción u obligación. Cuando entramos en una página web y vemos el mensaje sobre aceptación de cookies, todos las aceptamos sin leerlas. Que tire la primera piedra el que esté libre de culpa. Amén, cuando ves a un padre -o eres el padre- que deja a su hijo una consola, tablet, teléfono o similar sin preocuparse de un control parental (como mucho activamos el de la televisión, por si acaso ven lo que no deben ver a esa tierna edad, claro). Así, un suma y sigue, como cuando se recibe un correo electrónico que aparentemente no se entiende o se desconoce el remitente: cómo dejar de verlo si la curiosidad es un don muy humano.



En la normativa vigente aplicable y aquella que viene, queda claro que los responsables de tratamiento de datos, así como los encargados de ese tratamiento, deben efectuar evaluaciones de impacto y establecer garantías suficientes de seguridad en función de los datos que se traten, según el estado de la técnica. Preocupación máxima que

> Siempre oímos que las empresas tienen una serie de obligaciones para preservar tus datos y que tú cuentas con una serie de derechos

me consta tienen la mayoría de las empresas y que es primordial en EVO Banco, siendo puntera en Transformación Digital. Sin embargo, las amenazas y ataques se volverán más sofisticados, pero las necesidades de cambio/crecimiento para evitarlas en muchas ocasiones no crecerán a la par. Por ello, coincido en que existe una clara necesidad de Transformación Digital, pero como no siempre las tecnologías de las empresas o del mercado pueden cumplir con esas necesidades de forma segura, ni si quiera con recursos ilimitados, debemos poner nuestro granito de arena.

La clave cultural es fundamental para establecer medidas de seguridad eficaces. Una de las tareas y retos fundamentales de los CISO, responsables

**Enlaces de interés...**

- Por qué la protección del dato es clave en los programas de seguridad modernos
- ¿Sabes cómo el GDPR afecta a tu organización?
- Data Protection Officer, el nuevo superhéroe

de seguridad de la información o Delegados de Protección de Datos para fomentar esta cultura será la de involucrar y ayudar lo máximo posible al usuario, siendo capaz de responder u orientar a este a la hora de resolver las siguientes cuestiones: cómo y dónde me informo de medidas de seguridad; quién debe facilitar esa información; cada cuánto tiempo debo refrescar mis conocimientos en estos temas.

El otro día escuché “la ciberseguridad está de moda”. Pues a ver si nos sumamos todos a ese carro, y podemos repetir una letanía parecida a esta: “no debo dejar en manos de otros íntegramente la preocupación de mi seguridad”.

Si bien no puedo despedirme sin lanzar un mensaje de tranquilidad, ya que la realidad actual es que el regulador se preocupa de la seguridad de los datos, las empresas se preocupan por la seguridad de los datos y existen personas especializadas trabajando constantemente en ello. Es cierto que no podemos contar con una ciberseguridad completa, pero lo que sí os puedo asegurar es que el día a día de un Delegado de Protección de datos básicamente responde a esa preocupación. Por ejemplo, ponerse en los zapatos del usuario para tratar de facilitar información útil para asegurar sus datos; revisar iniciativas para que se incorporen medidas de seguridad; velar por el cumplimiento de esas medidas y, en caso de que exista alguna incidencia, actuar con rapidez para ayudar a establecer medidas de acción para su resolución, así como tratar de establecer otras para que no se vuelva a repetir. Y en aquellos casos donde la incidencia pueda afectar gravemente a un usuario, comunicar dicha incidencia para avisar de posibles amenazas y tratar de ayudar a su mitigación en la medida de lo posible.

*Cuando entramos en una página web y vemos el mensaje sobre aceptación de cookies, todos las aceptamos sin leerlas*

**JUAN JOSÉ SALVADOR**

**Responsable de Proyectos de Ciberseguridad y Coordinador Académico en el Campus Internacional de Ciberseguridad**

Técnico Superior en Sistemas Informáticos, con 20 de años de experiencia en el sector de las TICs, en los ámbitos de los Sistemas, las Telecomunicaciones y la Seguridad de estos. Juan José compagina su labor técnica con más de 12.000 horas de formación impartidas, especializado en Ciberseguridad, desde Certificados de Profesionalidad de Seguridad Informática hasta formación in-company.

# Ciberseguridad & Talento: un problema global

**¡Hacen falta millones de profesionales formados en no sé qué tecnología disruptiva!, como nos gusta llamarlas ahora. De forma periódica, durante los últimos 20 años, han aparecido noticias similares que leemos o escuchamos hoy día. Pero el problema de la falta de profesionales formados no es una cuestión nueva dentro del ámbito tecnológico. Como no podía ser de otra forma, hoy las noticias se centran en los millones de profesionales formados que se necesitan con competencias y/o destrezas vinculadas a la ciberseguridad y en la dificultad que supone encontrarles.**

Sin embargo, a diferencia de lo que ha sucedido en otras etapas, la falta de profesionales especialistas en ciberseguridad supone un problema que trasciende a todas las tecnologías, debido entre otras cosas, a la conectividad en la que basan sus servicios todas ellas. Desde las tecnologías basadas en la movilidad, pasando por los servicios en la nube hasta llegar a tecnologías que van a cambiar el futuro, que ya es presente, como puede ser IoT o Blockchain. Todas ellas, son vulnerables a ataques desde cualquier punto del planeta, como se está demostrando día tras día.

Una dificultad como esta parece que no debería tener una solución tan compleja de abordar. Basta-



La inversión en formación sigue muy lejos de donde debería estar y, sin embargo, la ciberseguridad es necesaria hoy en día y lo va a seguir siendo en el futuro

ría con formar a los profesionales que necesitamos. Sin embargo, la solución no es tan trivial y vemos que afecta tanto a países, como a organizaciones y particulares a nivel global.

En primer lugar, la escasa inversión en formación es un hándicap importante, algo que por otro lado ha ocurrido históricamente. Por suerte en España, aunque no tenemos muchos, son referentes a nivel mundial.

En segundo lugar, la falta de formación de calidad. A día de hoy, cada 4 ó 5 años aparece una nueva tecnología que va a cambiar nuestras vidas en un futuro cercano y para las que necesitamos a profesionales que no existen. Con estos plazos de tiempo tan reducidos no se consigue avanzar a la misma velocidad en lo referente a la formación sobre el uso seguro que deben hacer los usuarios de esas tecnologías y en las medidas de seguridad que debemos aplicar para disminuir el riesgo de sufrir un problema relacionado con su uso.

Para finalizar, deberían ser los gobiernos los que "tiraran del carro" a la hora de fomentar y promover

la formación de estos profesionales, aunque solo fuera por interés propio ya que como estamos viendo desde el año 2010, sus infraestructuras críticas son blanco fácil de ataques cada vez más sofisticados.

"Te pueden tirar abajo un Estado", decía hace unos meses Fernando J. Sánchez, director del Centro Nacional de Protección de Infraestructuras Críticas, centro desde donde se protegen doce de los sectores estratégicos en los que un ataque puede llegar a ser catastrófico. Y lo realmente importante, no es si puede llegar a ocurrir sino cuándo va a ocurrir.

La realidad es que la inversión en formación sigue muy lejos de donde debería estar y, sin embargo, la ciberseguridad es necesaria hoy en día y lo va a seguir siendo en el futuro, sea cual sea la tecnología que utilicemos y estemos en el entorno que estemos, tanto público como privado.

Ante algo tan evidente como esto, nuestro Gobierno parece que va a contracorriente cuando hace muy pocos días fijaba oficialmente su posición contraria a la regulación del ejercicio profesional de la informática, argumentando que es algo muy nuevo y que no afecta a la seguridad de las personas. No se entiende muy bien este razonamiento, si hay algo evidente, hoy día, es que los ciberproblemas derivados del uso de la tecnología afectan tanto a personas físicas como jurídicas.

Por lo tanto, necesitamos cambiar de mentalidad y crear nuevos modelos educativos que permitan reducir los tiempos de creación de novedosos programas de formación que se adecuen a las necesidades reales de cada momento. Los campus de ciberseguridad online o de otras disciplinas, plataformas virtuales de formación en formato e-learning, tanto oficiales como privados, están creciendo rápidamente debido a la posibilidad que les ofrecen a los alumnos de realizar la formación ajustándose a su disponibilidad horaria. Algunos de los más innovadores van más allá, permitiendo al alumno elegir las materias que cubran su necesidad formativa concreta, sin obligarle a seguir un programa formativo concreto, en el que la mitad de los contenidos no le aporten nada.

Y es el e-learning es la gran herramienta educativa de este siglo XXI porque permite acceder al conocimiento desde cualquier lugar, eliminando muchas de las barreras tradicionales que impedían el acceso a formación de calidad.

Para que nos demos cuenta del punto en el que estamos, sólo hay que reflexionar sobre la afirmación de Dan Levy, profesor e investigador de Políticas Públicas en la Universidad de Harvard, que

> Necesitamos cambiar de mentalidad y crear nuevos modelos educativos que permitan reducir los tiempos de creación de programas de formación que se adecuen a las necesidades reales

La principal recomendación es comenzar por programas transversales que te permitan tener una visión de 360º de la ciberseguridad


decía recientemente que “cientos de universidades no existirán dentro de 20 años”, porque ya no ofrecerán nada que no podamos aprender sin ellas, ya que los recursos que hay en la red son ilimitados.

Estamos asistiendo a un cambio en el que el alumno es el que organiza su proceso de capacitación y el docente pasa a asumir el rol de mentor, de orientador.

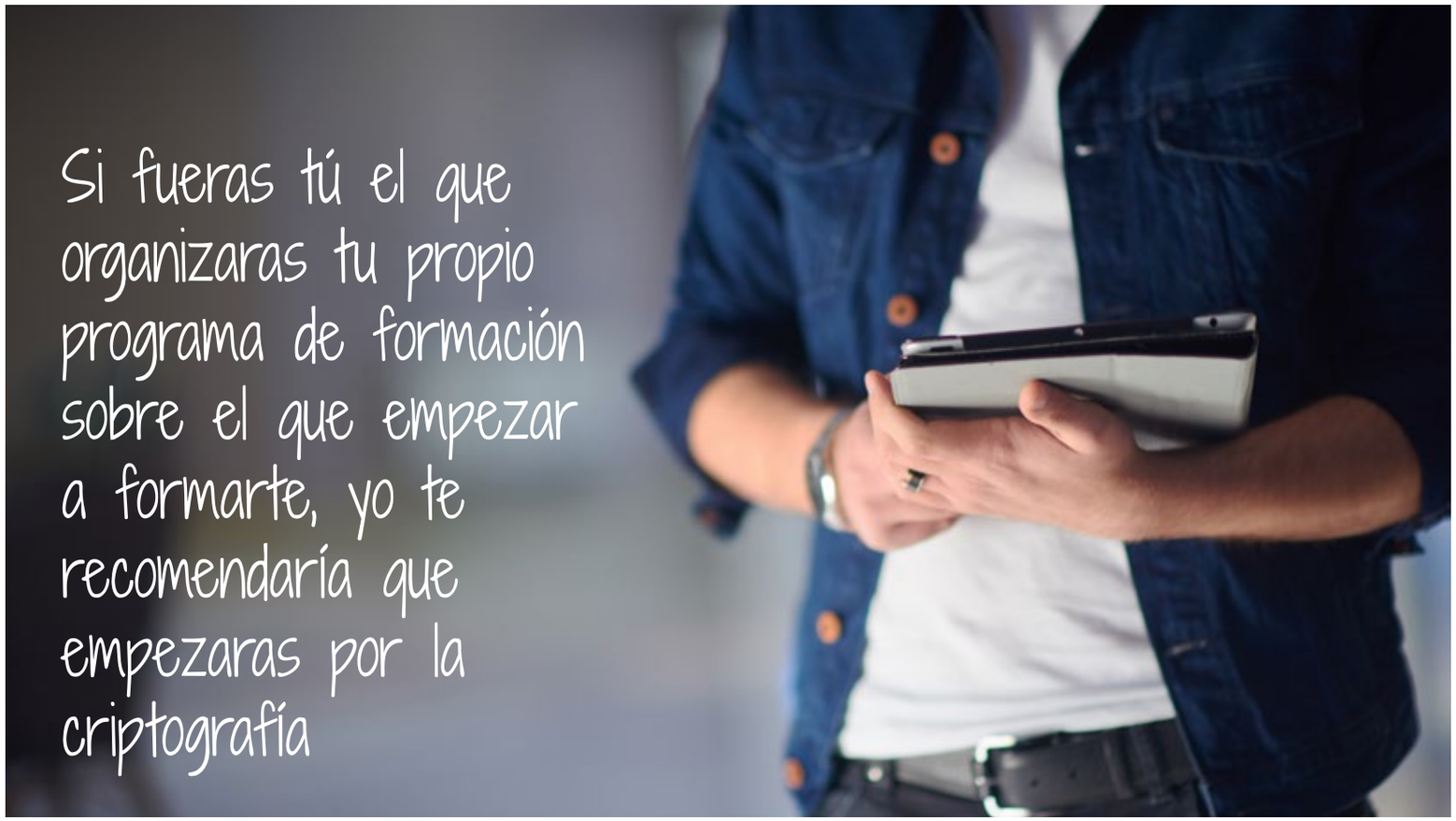
En el ámbito de la ciberseguridad tenemos que tener en cuenta otro detalle importante, y es que la realidad socioeconómica de nuestro país no ayuda especialmente, con más del 90% de las empresas siendo pymes, micropymes y autónomos. Los problemas de ciberseguridad que estas empresas presentan son los mismos que los que puede sufrir una gran organización, pero con una gran diferencia: los recursos humanos y económicos de los que disponen cada uno para hacer frente al problema, son diferentes.

Y que nadie piense que por ser una pequeña empresa o un particular no se puede llegar a ser un objetivo interesante para un ciberdelincuente. La máxima de “o te sacan el dinero o te convierten en dinero” es real para todos, y más para los que menos recursos pueden dedicar a implementar en ciberseguridad ya que, al final son el blanco más fácil de atacar.

En este sentido, el INCIBE está haciendo un gran trabajo diseñando programas de formación gratuitos para micropymes y autónomos, entre otras actividades.

Ahora bien, soy ese alumno que acaba de finalizar sus estudios universitarios o no universitarios; o soy un profesional en activo y quiero adentrarme en el mundo de la ciberseguridad. La pregunta que se hace todo el mundo es: ¿Por dónde empiezo?

La principal recomendación es comenzar por programas transversales que te permitan tener una visión de 360º de la ciberseguridad. Luego te especializarás en alguna de las muchas áreas que forman el conjunto de la ciberseguridad a través de programas más específicos que se adapten a tus gustos, tu formación o tu perfil profesional.




Como decía antes, si fueras tú el que organizaras tu propio programa de formación sobre el que empezar a formarte, yo te recomendaría que empezaras por la criptografía, esa gran apartada de los programas formativos porque es la base de todas las comunicaciones y transacciones que se realizan en la actualidad, aparte de estar detrás de más procesos de los que puedas imaginar.

Sería interesante que siguieras con la Seguridad Web ya que, prácticamente todo lo que hacemos hoy día se realiza a través de la Web y sus vulnerabilidades son aprovechadas para explotar muchos de los ciberataques que sufrimos a diario. Entender bien la Web, más allá de su uso, y cómo protegerla es fundamental.

A continuación, pasaría por los Sistemas Operativos, en plataformas Microsoft y Linux, tanto a nivel de servidor como de puesto de trabajo y continuaría con la seguridad de las redes corporativas, trabajando además las vulnerabilidades específicas que se producen en cada entorno. Tendrás una visión completa del entorno de trabajo tradicional de cualquier organización.

La investigación en fuentes abiertas (OSINT), la seguridad de los entornos IoT y la gestión de identidades son otras tres ramas con un potencial de contratación enorme y complementan perfectamente el temario que estás preparando.

Para finalizar, no me olvidaría de la regulación de la seguridad de la información y la normativa. En general, otro entorno con un potencial de contratación grande, sobre todo a partir del año que viene cuando sea de obligado cumplimiento el nuevo Reglamento General de Protección de Datos (RGPD), un Delegado de Protección de Datos interno o externo.

Algún purista podría decirme que me he dejado fuera ciertas áreas importantes, y no lo discuto, pero para tener una visión trasversal de la ciberseguridad creo que es una buena base sobre la que comenzar a formarse.

Lo que te puedo garantizar es que, una vez que comiences esta aventura ya no podrás dejarlo ¡Es como una droga!

### Enlaces de interés...

- Haciendo fácil el cifrado y la rotación de claves
- SIEM para principiantes
- Lagunas de conocimiento en ciberseguridad
- Realidad virtual para atraer a los expertos en ciberseguridad

# Sumario No Solo IT

## Management y Canal

Carta de un partner a los Reyes Magos para 2018

**Por José Luis Montes Usategui,**

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

## Psicobusiness

El equipo de trabajo para la Transformación

**Por Asier de Artaza,**

*director de www.yesmanagement.es*

## En la nube

La explosión en el almacenamiento de datos

**Por Kevin L. Jackson,**

*experto en Cloud y fundador de Cloud Musings*

## Tecnología y Negocio

Digitalizar España añadiría 2 puntos más al PIB

**Por Jorge Díaz-Cardiel,**

*socio director general*
*de Advice Strategic Consultants*

## Desde mi análisis

Cómo la tecnología cambia el sector retail

**Por Fernando Maldonado,**

*analista principal de Delfos Research*

## Social & Business

El nuevo director de marketing en la empresa

**Por Juan Merodio,**

*experto en Marketing 2.0, redes sociales 2.0*
*y web 2.0*

# Carta de un Partner a los Reyes Magos para 2018

*Queridos Reyes Magos, este año 2017 que ahora termina he sido todo lo bueno que se puede ser en este sector un poco canalla que me ha tocado vivir. En consecuencia, y pidiéndoos que tengáis en cuenta que sigo creyendo en vosotros y no como esos que le escriben a Santa Claus, os quiero pedir que me concedáis durante el 2018 la siguiente lista de cositas sencillas y de apenas importancia. Bueno, vale, de sencillas no tienen nada, pero para eso sois Magos, ¿no? Pues eso, que de lo sencillo ya me encargo yo, y hasta de muchas cosas complejas, pero una manita no me vendría mal con todo lo que llevo encima. Vamos al grano…*

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

"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".

Lo primero que quiero pediros es un cable para avanzar en la transición de mi negocio de venta de infraestructura TI on premise en CAPEX hacia un modelo más de pago por uso, en OPEX, o al menos en modo servicio, aunque sea en cuotas lineales. Ya sé que me la voy a pegar si simplemente intento pasar de revender infraestructura en la forma tradicional a revender servicios de otros, y que no hay rentabilidad ni futuro en escuchar los cantos de sirena de los proveedores de nuble pública. Y ya sé que tengo que construir servicios gestionados del mayor valor añadido que pueda, que quedarme solamente en el outsourcing de personas se me puede convertir en una carrera de ratas. Hasta ahí ya he llegado solo, lo

## *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.


que necesito de vosotros es que me ayudéis a entender cuál es mi modelo de negocio futuro de verdadero valor y sostenible, diferencial en lo posible, y cómo construir la evolución.

En relación con eso, os pido que me echéis una mano también (sois tres, tenéis seis manos, a ver si os da para todo lo que pido) con mi equipo comercial. Mirad, gestionan de narices los clientes que tenemos con los contactos que tenemos, en el tipo de oferta tecnológica que tenemos. Y eso está muy bien… pero no es suficiente. De nuevo, si fuera fácil ya lo habría hecho yo solo, pero lo que necesito es como soplar y aspirar al mismo tiempo, y encima mientras tienes un polvorón en la boca. O sea, difícil, a veces contradictorio, y con riesgo de montar un buen pollo. Porque quiero que sigan haciendo bien todo lo anterior y, además, que naveguen dentro de las organizaciones de nuestros clientes para encontrar nuevos interlocutores y establecer contacto con ellos convenciéndoles de que somos la bomba en tecnologías diferentes de las que hoy nos están comprando. Es decir, ampliando el campo de juego y reposicionándonos. Y si, ya en el colmo de vuestra generosidad, además hacéis que mis comerciales traigan nuevos clientes, soy capaz hasta de tejerles unas mantitas nuevas a vuestros camellos.

Como después de conseguirme esas dos cositas estaréis ya en caliente, ¿qué tal si después de eso me ayudáis a meterle mano a mi margen medio? Me he leído todos los libros de esos tíos tan espabilados que pontifican sobre lo que hay que hacer, pero sin haberlo hecho en su vida, y tengo la cosa clara: tengo que vender cosas del mayor valor añadido posible, tengo que buscar clientes que valoren más lo que la tecnología les aporta y estén dispuestos a invertir en ello, tengo que conseguir diferenciarme de mis competidores, y vender el máximo posible de servicios. La recetita está clara, ahora necesito ayuda con los ingredientes y con el cocinero, porque de la teoría a la práctica creedme que hay un bueeeeeeeeeeeen trecho. Me he leído también algunos libros sobre venta consultiva, venta de soluciones de valor a mercados B2B, y sobre challenge selling. De teoría ya voy servido, echadme una mano con la práctica, sed buenos.


Una pregunta quería haceros: ¿alguno de vosotros está puesto en eso de la inteligencia emocional? Porque me hace falta una ayudita también en eso. Mirad, los fabricantes con los que tengo alianzas son gente rara y cambiante. No nos entendemos, o al menos no todo lo que querría. Ellos se quejan de que yo voy a mi bola,

Queridos Reyes Magos, necesito de vosotros que me ayudéis a entender cuál es mi modelo de negocio futuro de verdadero valor y sostenible, diferencial en lo posible, y cómo construir la evolución

y yo me quejo de que ellos van a la suya. Total, que parece que ambos vamos a nuestra bola, pero luego andamos por ahí dándonos abrazos y llamándonos "Partner". Tampoco se trata de que estemos siempre de acuerdo en todo, pero intuyo que o no nos lo contamos todo, o no nos escuchamos de forma suficientemente activa, o decimos lo contrario de lo que pensamos, o vete a saber qué, pero el caso es que una miajita de mejor entendimiento y mayor confianza mutua nos iría bien a todos.

Ya con esto tengo la impresión de que he llenado el capazo, pero me vais a permitir abusar un poquito más de vuestra paciencia, y voy a pediros que me echéis una última mano con mi marketing. A ver, no es que sea malo, al menos no es peor que el de mis competidores, pero muy mejorable sí que lo es. Para empezar, no tenemos un plan, ni unos objetivos más allá de gastarnos los pocos fondos que los fabricantes nos dan. Nuestra web, ¡qué contaros de ella!, que menos mal que pocos clientes van a verla. Al cabo del año habremos hecho una serie de acciones de marketing, pero tengo que confesar que bastante erráticas y un poco a salto de mata. Mis comerciales no creen mucho en que lo que hacemos les de algún resultado, así que viven medio de espaldas a eso y a mí me gustaría que fueran ellos los primeros impulsores de nuestras acciones de marketing, que las pidieran y hasta que nos guiaran en ellas. Ya de nuestras redes sociales ni hablamos, una pena, la verdad, y no sé cómo meterle mano para que nos sirvan para mejorar el negocio y no solamente para compartir tal cual nos llegan, con una listita pequeña de contactos, los mensajes de nuestros fabricantes. Para algo más tienen que servir, espero.

Si os parece, vamos a dejarlo aquí, que igual me he pasado un poquito. Pero es que muchas de estas cosas hace tiempo que vienen coleando, y ya la situación se está poniendo que no da para muchas dilaciones más. Yo prometo seguir poniéndole ganas y mucho esfuerzo, pero igual por separado cada una de estas cosas me vería con capacidad de ponerle remedio yo solo, pero todas juntas como que se me hace bola.



## Enlaces relacionados

- Modelo de consumo de TI como servicio para la innovación empresarial
- Beneficios del consumo de TI como servicio

¿Te avisamos del próximo IT Reseller?

# TU CANAL DE VÍDEOS IT

INFORMATIVO IT


DIÁLOGOS IT

IT WEBINARS

CASO DE ÉXITO IT


MESA REDONDA IT

# TU PRODUCTORA DE CONTENIDOS AUDIOVISUALES

WEBINARS

ENTREVISTAS


EVENTOS


VÍDEOS

INFORMATIVOS

www.ittelevision.es

# El equipo de trabajo para la transformación

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

***(segunda parte)***

**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

realmente influyen y movilizan a la gente. Así, tendremos líderes formales, es decir, el director del departamento y similares, y líderes informales.

Atención a este último grupo. Los líderes informales son aquellos cuyas opiniones pesan y la gente les sigue, con lo que son los potenciales tractores de la organización. Esto puede ser por diferentes motivos: su carisma, atractivo, simpatía, conocimiento experto, historia en la compañía... Así que debemos reparar bien en quiénes son; no podemos olvidar que la compañía tiene unos organigramas formales, oficiales y luego una realidad, compuesta por lo oficial y lo extraoficial.

Identificadas estas personas clave, toca pedir su integración en este equipo con un compro-

## El equipo tampoco funciona solo, sino que habrá que invertir en la generación de equipo

Para llevar a cabo cualquier proyecto transversal en la organización, es muy interesante crear un equipo de trabajo responsable, en primera instancia, de la transformación, sea del tipo que sea.

Este elemento será crítico para el éxito del proyecto y por ello no puede estar compuesto de cualquier manera, sino que su composición es un aspecto crítico, ya que determinará su eficacia en gran parte.

¿Qué es lo que vamos a hacer? Pues, en primer lugar, identificar a los auténticos líderes de la organización, es decir, aquellos que

— JOHN KOTTER´S GUIDING COALITION —


CLICAR PARA VER EL VÍDEO


## *La realidad de las empresas españolas sobre competencias y Transformación Digital*

Directores y managers de recursos humanos, formación, tecnología y transformación digital han participado en este estudio de B-Talent, Soft Skills & Digital Mindset, que analiza, desde el prisma de Recursos Humanos, el grado de sensibilización de las empresas frente al reto de la digitalización. Pues bien, de él se desprende que las empresas españolas todavía tienen importantes hitos que alcanzar en materia de transformación digital.

miso emocional. Este compromiso puede venir respaldado por el sentido de urgencia (ver artículo relacionado, transformación sin el efecto colchón), por la presentación de una gran oportunidad para la organización, y por la consideración y confianza en ellos como agentes del cambio.

Sigamos, porque el equipo tampoco funciona solo, sino que habrá que invertir en la generación de equipo, el remanido “team building” en el que el equipo vaya cogiendo personalidad, confianza, espíritu y sentido de dirección en la misión. Las actividades fuera de la oficina contribuyen a establecer conexiones más fuertes racionales y emocionales que darán confianza y química personal, lo que será el pegamento que les mantendrá unidos.

Además, debemos fijar un objetivo común, que sea realmente inspirador y convierta la finalidad del equipo de trabajo en una actividad apasionante, complementaria a sus puestos y actividades diarias en la organización.

Una vez compuesto y vistos los primeros pasos, revisa el equipo para detectar áreas débiles. No olvides que se necesita una buena combinación de gente de diferentes departamentos y niveles en la compañía. Las cualidades de este equipo son fundamentales.

Entremos entonces a repasar qué cualidades requiere nuestro equipo para la transformación. Este comité debe tener una posición de poder, así que se necesitan suficientes miembros con

## Los líderes informales son aquellos cuyas opiniones pesan y la gente les sigue, con lo que son los potenciales tractores de la organización

poder, recordemos oficial y extraoficial, para que los que se quedan fuera no sean más fuertes y puedan bloquear las iniciativas de nuestro “dream team”.

Necesitan tener un nivel de expertise a lo largo y ancho, es decir, representar

todos los puntos de vista de la empresa. Desde las disciplinas profesionales u “oficios”, caracteres sociales y culturales, miembros expertos multifuncionales de diferentes ubicaciones y realidades... todo debe estar presente para que



consideremos que permita tomar decisiones inteligentes e informadas.

El equipo en conjunto, y a través de sus componentes, debe tener credibilidad. Hablamos de gente percibida y respetada dentro de la empresa y que conseguirán que sus futuros pronunciamientos sean considerados y tomados en serio por todos los empleados (por su credibilidad… por ¡su reputación!)

Hay otros dos conceptos interesantes de este equipo que, en ocasiones, se confunden, uno es liderazgo y otro la capacidad de gestión (management). Aportemos cierto detalle a estos términos. Por un lado, el equipo debe tener suficientes líderes constatados. Lo hemos comentado ya suficientemente, pero realmente es ahora cuando lo estamos completando, en el sentido de que tiene que haber líderes capaces de conducir el proceso de cambio (una parte del equipo que conduce, inspira y establece dirección al proceso). Por otro lado, el tándem se equilibra con, sigamos llamándoles, líderes con capacidad de gestión, es decir, responsables de que las cosas se lleven a cabo, se ejecuten; éste será el management que controla el proceso y consigue hacerlo realidad.

Llegados a este punto, necesitarán, finalmente, capacitación en sintonización personal, técnicas de comunicación y persuasión, cambio de actitudes y gestión de conflictos entre otras; así como conocer en detalle el proyecto que tienen entre manos.

Con este equipo seremos capaces de llevar un proceso complejo como es el cambio en una organización; ya sea una transformación estratégica, cultural, digital, innovadora o de orientación a mercado. A partir de aquí tendrán que seguir un proceso en su desarrollo, pero esto ya lo dejamos para el próximo artículo.

Una vez más, personas y gestión, psicobusiness, porque, como vemos, ningún plan o proyecto tendrá éxito si no se considera a las personas. Y viceversa, las personas necesitan de gestión, herramientas, procesos y planes inspiradores, para aportar el máximo a su empresa.

## Enlaces relacionados

- The guiding coalition
- John Kotter´s Guiding coalition
- Inteligencia Artificial y robótica
- Tendencias 2017: Inteligencia Artificial. El impacto del Deep learning en verticales e IoT
- Inteligencia Artificial y estadística

# La explosión en el almacenamiento de datos

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

La innovación en cloud computing será el motor de la transformación de las empresas en 2018. El crecimiento de la nube está produciendo una rápida expansión del mercado del almacenamiento, por lo que su coste y su complejidad se convierten en cuestiones cada vez más acuciantes para la actividad de negocio. La causa de esta situación es el volumen cada vez mayor de datos generados en tiempo real en internet, dispositivos móviles, redes sociales, sensores, archivos de registro y aplicaciones transaccionales. El Big Data, por su parte, ha encontrado su sitio como elemento integrante de la operativa de un gran número de sectores, y con aplicaciones prácticas muy diversas, desde la detección del fraude hasta el procesado de imágenes.

El concepto original de Big Data fue acuñado para describir conjuntos de datos demasiado grandes para las bases de datos convencionales, aunque se ha ampliado con el tiempo de manera muy significativa, para incluir ahora aquellas tecnologías y servicios que capturan, almacenan, gestionan y analizan grandes conjuntos de datos para la resolución de problemas complejos. La inversión global en Big Data si-

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.

gue creciendo, a pesar de las objeciones que pueden surgir sobre su nivel de privacidad o a las reticencias frente a su uso. Las últimas previsiones de los analistas indican que el mercado global en estas soluciones superará los 57.000 millones de dólares, sólo en 2017, con in crecimiento anual agregado de un 10% durante los próximos tres años.

Cuanto más tiempo esperemos para mover nuestro almacenamiento a la nube, más complicado nos será mantener nuestra actividad al ritmo al que aumentan las demandas de almacenamiento

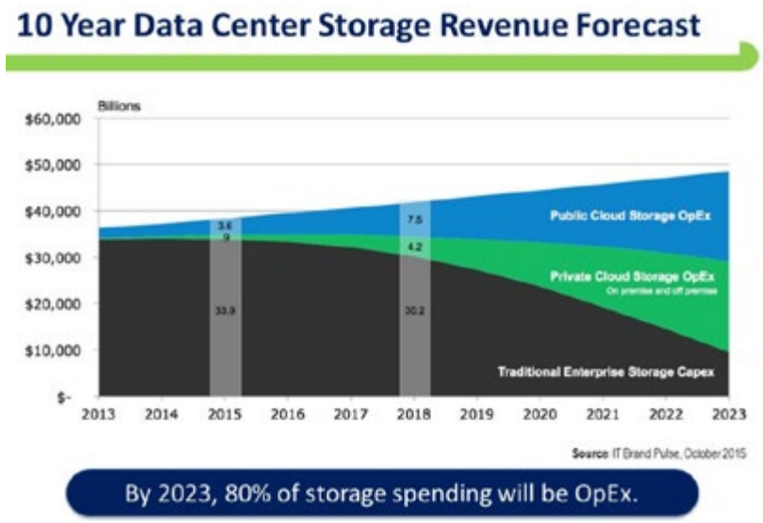
Este tipo de inversiones de negocio no planificadas habría supuesto, en el pasado, acometer proyectos de mejora muy largos y costosos en tecnologías de almacenamiento, con el riesgo añadido de olvidar -por accidente- datos almacenados en equipos obsoletos, y el consiguiente impacto negativo sobre el nivel de disponibilidad de las aplicaciones o de las copias de seguridad de datos. En este sentido, la maduración del cloud ha permitido, afortunadamente, ofrecer nuevas opciones de servicio. Los servicios de nube pública han cambiado por completo la forma en la que las empresas consumen tecnología, mientras que la analítica avanzada, el machine learning, el Internet de las Cosas y los nuevos servicios de base de datos y de edge computing han hecho que las decisiones sobre modernización del almacenamiento sean aún más críticas que antes.

Las empresas se están enfrentando al reto del almacenamiento con un uso cada vez mayor de modelos de soluciones de TI híbrida, en las que se combinan la flexibilidad del almacenamiento en una nube pública con la seguridad y la estabilidad del almacenamiento en un centro de datos convencional, y donde las inversiones se trasladan desde la adquisición de capital hacia gastos operativos más fáciles de gestionar. Las proyecciones muestran que los gastos operativos comenzarán a superar en breve a los gastos de capital, una situación que en muchas organizaciones ha sido la clave para minimizar

## *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.




**Previsiones a 10 años del volumen global de ingresos por almacenamiento de datos**

el riesgo, incrementar la eficiencia y modernizar los procesos a la velocidad que requiere la actividad de negocio.

Si bien es cierto que estas nuevas opciones de almacenamiento híbrido ayudan al equipo de sistemas a evolucionar desde un modelo táctico y reactivo hacia un enfoque mucho más estratégico, como verdaderos partners de negocio, la elección del proveedor de almacenamiento más adecuado es crucial. Esto implica, en aplicaciones de Big Data, consumir almacenamiento de objetos en la nube, donde la elasticidad y la capacidad prácticamente ilimitada de esta opción la convierten en la alternativa ideal para la resolución de problemas de almacenamiento corporativo de Big Data. Por otro lado, aunque el almacenamiento en la nube pueda percibirse como la mejor solución posible, será necesario tener en cuenta que la velocidad de respuesta de los servicios, el precio, y el coste de los servicios adicionales -como las llamadas a API- en el cloud pueden añadir dificultad al proceso de elección del partner más adecuado. En cualquier caso, cuanto más tiempo esperemos para mover nuestro almacenamiento a la nube, más complicado nos será mantener nuestra actividad al ritmo al que aumentan las demandas de almacenanamiento. Si busca de verdad el éxito en sus objetivos de negocio, empiece a buscar ya a un partner de almacenamiento que le permita cubrir sus necesidades, mejorar la eficiencia, y mantenerse al frente del mercado al que se dirige.




(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)

## Enlaces relacionados

- El almacenamiento empresarial creció un 2,9% en el segundo trimestre, según IDC
- Forbes: The State of Storage
- Cuotas de mercado de almacenamiento empresarial externo desde 2008 a 2017
- Las lagunas de conocimiento en ciberseguridad
- Ciberamenazas y tendencias. Informe CCN-CERT edición 2017
- 4 formas de protegerse y recuperarse de ataques de ransomware
- Como utilizar la Dark Web para la inteligencia de amenazas

# Digitalizar España añadiría 2 puntos al PIB

*Para que una economía desarrollada esté sana, necesita tener no menos de un 20% de su producto interior bruto en la industria, como sucede en Alemania y en Estados Unidos. Las economías "solo de servicios", como la española, son más susceptibles de ser afectadas por los vaivenes de los ciclos económicos. Hoy, la industria está fuertemente vinculada al conjunto de nuevas tecnologías que conforman la llamada "Digitalización".*

Jorge Díaz-Cardiel
*Socio director general de Advice Strategic Consultants*

"Hemos pasado de la era de la Computación a la de la Digitalización", afirma Jorge Díaz Cardiel en su último libro "Digitalización y éxito empresarial". Las grandes empresas han sido pioneras. La obra trata de compañías que, como Amazon, Apple, Google, Salesforce, Microsoft, Facebook, Sage… han creado las tecnologías digitales. También del ecosis-

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

Cellnex Telecom, líder europeo en gestión de infraestructuras de telecomunicaciones inalámbricas; Gas Natural Fenosa es la primera compañía energética de Europa; El Corte Inglés lidera la transformación digital en su sector; Bankinter, primer banco innovador por teléfono e Internet; Sage España ayuda a las pymes a digitalizarse; Vodafone España ha creado el Observatorio Vodafone y es punto de referencia de la Digitalización empresarial y del sector público.

Los 3,2 millones de pymes españolas (99,88% de nuestro tejido empresarial) tienen el ejemplo de las grandes empresas de todos los sectores para digitalizarse. Y aquí está el gran reto que tiene la economía española y los responsables de la política económica española. En sus manos está avanzar la Agenda Digital. A finales de 2012, el Gobierno fijó una hoja de ruta específica para digitalizar España, consiguiéndose

tema tecnológico norteamericano que hace posible que esas herramientas tecnológicas lleguen a empresas y familias: HP Inc. HPE, IBM, Oracle, Intel, Dell... Es decir, del Silicon Valley, cuyo PIB equivale al de Irlanda. En economías desarrolladas, la Digitalización puede añadir 2% al PIB.

"En España, tenemos el ejemplo de la gran empresa", asevera Díaz Cardiel. La Fundación Bancaria La Caixa, con el liderazgo de su presidente, Isidro Fainé; Telefónica y su apuesta por la convergencia digital, Big Data y la fibra óptica, con José María Álvarez-Pallete; CaixaBank, primer banco digital del mundo; Abertis, líder mundial en gestión de infraestructuras;

Los 3,2 millones de pymes españolas (99,88% de nuestro tejido empresarial) tienen el ejemplo de las grandes empresas de todos los sectores para digitalizarse

## *La realidad de las empresas españolas sobre competencias y Transformación Digital*

Directores y managers de recursos humanos, formación, tecnología y transformación digital han participado en este estudio de B-Talent, Soft Skills & Digital Mindset, que analiza, desde el prisma de Recursos Humanos, el grado de sensibilización de las empresas frente al reto de la digitalización. Pues bien, de él se desprende que las empresas españolas todavía tienen importantes hitos que alcanzar en materia de transformación digital.

grandes logros en el sector de las Administraciones Públicas, donde la digitalización del ámbito público generó ahorros de 31.000 millones de euros entre 2013 y 2014 y de 22.000 millones de euros entre 2015 y 2016. Éste ha sido uno de los motivos por los que el déficit público ha estado bajo control. Pero éste no debe ser el único objetivo.

En sentido positivo -tenemos como ejemplo el caso de Estados Unidos- sabemos que la productividad de las pyme y autónomos (no me cansaré de repetirlo: el 99,88% del tejido empresarial español) aumenta un 20% cuando se introducen las tecnologías de la información en los procesos internos de la empresa y en los externos, como ventas y marketing. Éste es el caso norteamericano durante los últimos ocho años y los frutos han sido evidentes: crecimientos del PIB del 2,6% de media anual y tasa de paro del 4,4% -dependiendo del mes oscila entre el 4,1 y el 4,5%- o, lo que es lo mismo, pleno empleo.



En cambio, en Europa se ha apostado en estos últimos ocho años por la moderación salarial como fórmula para aumentar la productividad empresarial. Los frutos también son evidentes: aumentos de productividad del 3,5% (versus el 20% estadounidense), crecimiento del PIB medio en la Unión Europea del 1,4% y tasa de paro media del 10%, con excepciones como Grecia y España, donde el paro es más elevado.

Una fuerte apuesta de los poderes públicos por la digitalización de la economía y las empresas daría un empujón fuerte al crecimiento del PIB y del empleo.

Una fuerte apuesta de los poderes públicos por la digitalización de la economía y las empresas daría un empujón fuerte al crecimiento del PIB y del empleo




## Enlaces relacionados

- [Instituto Nacional de Estadística. PIB español]
- [Efecto del sector TI estadounidense en el PIB]
- [Sector tecnológico en el PIB de la UE]
- [Cómo debe ser el centro de datos de nueva generación]
- [La empresa digital]
- [El impacto de la automatización en las operaciones de IT]
- [El reto de la Cultural Digital]
- [Innovación a nivel global]

[Fernando Maldonado]
*Analista asociado a Delfos Research*

# Cómo la tecnología cambia al sector Retail

*No cabe duda de que el entorno en el que operan las empresas del sector retail es cada vez más complejo. Parte del origen y de la solución se encuentra en la adopción de nuevas tecnologías. Esto no es algo nuevo. En el pasado ha habido cambios tecnológicos con un fuerte impacto dentro de su actividad.*

Por ejemplo, la incorporación de los códigos de barra y sus lectores no sólo generó una mejora en la eficiencia de distintos procesos a lo largo de la cadena de valor, sino que también rompió el equilibrio de poder dentro del sector. Las grandes superficies se beneficiaron,

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

## *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.


de una mayor eficiencia y agilidad a escala, en detrimento del pequeño comercio para el que esta tecnología resolvía un problema que no tenían.

Esto se traduce, por ejemplo, en una mayor presión hacia el autoservicio por parte del cliente, ya sea en el mundo físico como en el virtual. De este modo, en algunas tiendas físicas, aunque todavía en una fase piloto, el autoservicio puede llegar a que los clientes no tengan ninguna interacción con los empleados – ej. cajeros-. En el mundo virtual, tanto los asistentes personales virtuales como los chatbots prometen,

**La incorporación de los códigos de barra y sus lectores no sólo generó una mejora en la eficiencia de distintos procesos a lo largo de la cadena de valor, sino que también rompió el equilibrio de poder dentro del sector**

Hoy hablamos de un cambio tecnológico sí, pero esta vez es diferente. No hay una única tecnología a la que señalar, sino que se trata más bien de un conjunto de ellas que interactúan entre sí para crear una innovación por combinación de consecuencias imprevisibles.

Robotización, inteligencia artificial, movilidad, cloud, block-chain o IoT son tendencias que por sí solas prometen redefinir la cadena de valor del sector. Pero, qué no harán cuando comiencen a combinarse unas con otras. Quizá esta sea la razón por la que resulta tan difícil asomarse al futuro de este sector y, por extensión, a cualquier otro.

Lo que sí que sabemos es que el equilibrio existente en el mercado se ha vuelto romper. Pero, esta vez entre empresas y clientes. Estos últimos, fuertemente tecnificados ahora tienen el poder.  Y lo que demandan es inmediatez y personalización.

## Hay tantas combinaciones de tecnologías que solo mediante la experimentación, por prueba y error puede detectar cuál será el próximo giro de este sector

una vez integrada la inteligencia artificial, un nuevo paradigma de comercio donde el cliente pueda entablar un dialogo por medio de voz o texto con un “Personal Shopper Virtual” que lo guíe en su proceso de compra, incluso una vez comprado recibir (sin salir de la aplicación de mensajería utilizada) confirmación del pedido. Por su puesto esto también permite gestionar

incidencias o proporcionar recomendaciones en tiempo real.

Esto es solo un ejemplo de la promesa de cómo la tecnología está permeando el negocio de retail. Lo dicho, hay tantas combinaciones de tecnologías que solo mediante la experimentación, por prueba y error puede detectar cuál será el próximo giro de este sector.

Sea como fuere todos los escenarios llevan a un mundo en el que sólo podrán competir aquellos capaces de ofrecer personalización a escala. Una vez allí habrá que reinventarse constantemente y abrazar todas las tecnologías que están por venir, para experimentar, para combinarlas, para aprender.

Eso sí, sin olvidar que el cliente es el que tiene el poder.



### Enlaces relacionados

- Impacto del código de barras en el sector
- Impacto de block-chain en Retail
- Primera mención del término de “comercio conversacional”
- US Social Commerce 2017: Influencing and Driving Sales
- eShopper Barometer
- La verdad sobre el ecosistema de IoT
- La reinvención digital: una oportunidad para España

**Juan Merodio**
*Experto en Marketing 2.0, Redes Sociales y Web 2.0*

# El nuevo director de marketing en la empresa

*El marketing del futuro más cercano va a trabajar alrededor de 2 conceptos: Tecnología y datos.*

En el mundo que estamos viviendo todo evoluciona, los consumidores evolucionan, la tecnología lo hace y, por lo tanto, la figura y roles de un director de marketing debe hacerlo también, pasando a convertirse en un director de marketing tecnológico o head of marketing technology. Este nuevo rol lo leí en un artículo publicado.

Entre otras cosas presentaban un gráfico de cómo debe dividirse un nuevo departamento

Uno de los principales expertos en España en Marketing Digital, Redes Sociales y Web 2.0. Ponente habitual en congresos de reconocido prestigio internacional así como profesor de las mejores Escuelas de Negocio y Universidades, entre las que destacan la Rey Juan Carlos, Cesma o el Instituto de Empresa.

## *Marketing digital y pymes, un mundo de oportunidades*

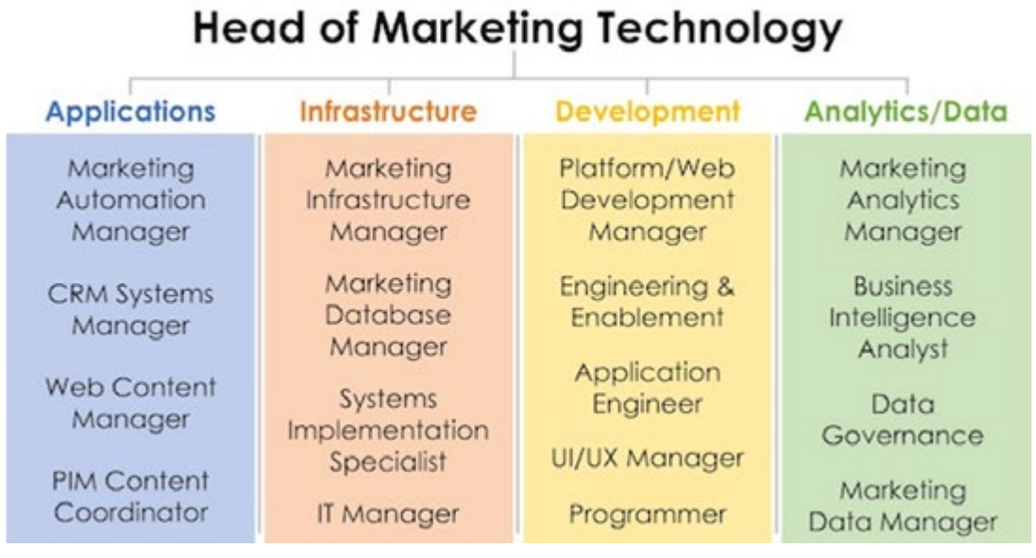
Las nuevas tecnologías, los nuevos servicios multimedia, se han convertido en la mejor oportunidad para salir de la crisis y, sobre todo, para dotar a las pymes de nuevas herramientas que les permitan ganar en competitividad y diferenciación. QDQ media explica en el siguiente libro digital cómo mejorar la función de marketing digital en las pequeñas y medianas empresas.


# Tenemos que olvidarnos de hacer un marketing por impulsos probando campañas para saber cuál consideramos que va a funcionar mejor

de marketing liderado por esta figura y el cual se dividiría en cuatro subgrupos: aplicaciones, infraestructura, desarrollo y análisis de datos (Ver imagen)

Como puedes ver en este gráfico que te muestro, cada uno de los grupos tiene sus diferentes profesionales, los cuales reportarían al Director de Marketing tecnológico. Puedes ver que dentro de su grupo aplicaciones tenemos un responsable de automatización de marketing, responsable de sistemas de CRM, el responsable de contenidos web y un responsable de la gestión de información de los productos.

Dentro de la parte inferior nos encontraríamos con los responsables de bases de datos, implementación y TI. En la zona desarrollo tendríamos los





CLICAR PARA AMPLIAR

# Los consumidores evolucionan, la tecnología lo hace y, por lo tanto, la figura y roles de un director de marketing debe hacerlo también

## BI O INTELIGENCIA DE NEGOCIO


CLICAR PARA VER EL VÍDEO

desarrolladores de plataformas, ingenieros, y aplicaciones irresponsables de experiencia de usuario. Y, por último, en el Grupo de Análisis de Datos tenemos los responsables de analítica en marketing y de inteligencia de negocio.

Visto esto está claro que este tipo de organigrama está pensado para una gran organización que necesite de todo ello y de los recursos; es cierto, pero la idea es extrapolable a una pequeña empresa en términos de hacia dónde debemos dirigir nuestros esfuerzos de marketing. Lo que quiero decir es que tenemos que olvidarnos de hacer un marketing por impulsos probando campañas para saber cuál consideramos que va a funcionar mejor, y basar todas nuestras acciones tácticas en el uso de la tecnología dirigida por los insights que nos dan los datos, o dicho de otro modo lo que se define como Data Driven Marketing, hacer a los datos el jefe de todo el marketing.

¿TE HA GUSTADO ESTE REPORTAJE?

***Compártelo en tus redes sociales***

## Enlaces relacionados

- El nuevo rol del CMO
- BI o inteligencia de negocio
- Automatización de marketing
- Inteligencia de negocio
- 5 grandes tendencias del marketing moderno
- Las lagunas de conocimiento en ciberseguridad
- Ciberamenazas y tendencias. Informe CCN-CERT edición 2017
- 4 formas de protegerse y recuperarse de ataques de ransomware


it User
TECH & BUSINESS

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